



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ (ИБРР-2017)

**ЮБИЛЕЙНАЯ X САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ
КОНФЕРЕНЦИЯ**

Санкт-Петербург, 1-3 ноября 2017 г.

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

**Санкт-Петербург
2017**

<http://spoisu.ru>



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ (ИБРР-2017)

**ЮБИЛЕЙНАЯ X САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ
КОНФЕРЕНЦИЯ**

Санкт-Петербург, 1-3 ноября 2017 г.

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

**Санкт-Петербург
2017**

<http://spoisu.ru>

УДК (002:681):338.98

И 74

ISBN 978–5–906931–64–1

И 74 **Информационная безопасность регионов России (ИБРР-2017).**
Юбилейная X Санкт-Петербургская межрегиональная конференция.
Санкт-Петербург, 1-3 ноября 2017 г.: Материалы конференции / СПОИСУ. –
СПб., 2017. – 580 с.

Сборник охватывает широкий круг направлений: Государственная политика обеспечения информационной безопасности регионов России, Правовые аспекты информационной безопасности, Безопасность информационных технологий, Современные средства защиты информации, Информационная безопасность телекоммуникационных сетей, Информационно-экономическая безопасность, Информационная безопасность и импортозамещение в критических инфраструктурах, Информационная безопасность транспортных систем, Информационная безопасность объектов морской техники и морской инфраструктуры, Информационно-психологическая безопасность, Информационная безопасность Арктического региона, Информационная безопасность в экологии, Информационная безопасность в социокompьютинге, Информационная безопасность киберфизических систем, Подготовка и переподготовка кадров в области обеспечения информационной безопасности, а также материалы молодежных научных школ «Информационная безопасность и проблемы устойчивого развития» и «Безопасные информационные технологии». Предназначен для широкого круга руководителей и специалистов органов государственной власти, академических учреждений, высших учебных заведений, научно-исследовательских и научно-производственных предприятий и организаций Санкт-Петербурга и других регионов, специализирующихся в области информатизации, связи и защиты информации.

УДК (002:681):338.98

Редакционная коллегия: *Р.М. Юсупов, Б.Я. Советов, В.В. Касаткин*
Компьютерная верстка: *А.С. Михайлова*

Публикуется в авторской редакции

Подписано в печать 20.10.2017. Формат 60х84 $\frac{1}{8}$. Бумага офсетная.
Печать – ризография. Усл. печ. л. 67,42. Тираж 400 экз. Заказ № 1057
Отпечатано в ООО «Политехника-принт»
190005, Санкт-Петербург, Измайловский пр., 18-д

ISBN 978–5–906931–64–1

© Санкт-Петербургское Общество информатики,
вычислительной техники, систем связи и
управления (СПОИСУ), 2017 г.
© Авторы, 2017 г.



INFORMATION SECURITY OF RUSSIAN REGIONS (ISRR-2017)

ANNIVERSARY X ST. PETERSBURG INTERREGIONAL CONFERENCE

St. Petersburg, November 1-3, 2017

PROCEEDINGS OF THE CONFERENCE

**St. Petersburg
2017**

<http://spoisu.ru>



УЧРЕДИТЕЛИ КОНФЕРЕНЦИИ «ИБРР-2017»

- Правительство Санкт-Петербурга
- Законодательное Собрание Санкт-Петербурга
- Правительство Ленинградской области
- Министерство связи и массовых коммуникаций Российской Федерации
- Министерство образования и науки Российской Федерации
- Российская академия образования
- Отделение нанотехнологий и информационных технологий Российской академии наук
- Санкт-Петербургский научный центр Российской академии наук
- Санкт-Петербургский институт информатики и автоматизации Российской академии наук
- Санкт-Петербургская территориальная группа Российского национального комитета по автоматическому управлению
- Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления

СОУСТРОИТЕЛИ КОНФЕРЕНЦИИ «ИБРР-2017»

- Российский фонд фундаментальных исследований
- Макрорегиональный филиал «Северо-Запад» ПАО «Ростелеком»
- СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
- ФГУП «ЦентрИнформ»
- Филиал ФГУП ЦНИИС - ЛО ЦНИИС
- АО «Концерн «НПО «Аврора»
- АО «НПО «Импульс»
- АО «НТЦ «Фрактал»
- АО «Центр компьютерных разработок»
- Группа компаний «Омега»
- ЗАО «Институт инфотелекоммуникаций»
- ЗАО «Институт телекоммуникаций»
- ООО «Ассоциация специалистов безопасности»
- ООО «Геонавигатор»
- ООО «Компания «Марвел»
- ООО «Лаборатория инфокоммуникационных сетей»
- ООО «НеоБИТ»
- Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
- Государственный университет морского и речного флота имени адмирала С.О. Макарова
- Петербургский государственный университет путей сообщения Императора Александра I
- Санкт-Петербургский политехнический университет Петра Великого
- Санкт-Петербургский государственный университет аэрокосмического приборостроения
- Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
- Санкт-Петербургский государственный университет промышленных технологий и дизайна
- Санкт-Петербургский государственный экономический университет
- Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
- Санкт-Петербургский государственный морской технический университет
- Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
- Санкт-Петербургский университет МВД России
- Партнерство для развития информационного общества на Северо-Западе России
- Санкт-Петербургская инженерная академия
- Санкт-Петербургское отделение Академии информатизации образования



КООРДИНАЦИОННЫЙ СОВЕТ КОНФЕРЕНЦИИ «ИБРР-2017»

Полтавченко Георгий Сергеевич	Губернатор Санкт-Петербурга
Макаров Вячеслав Серафимович	Председатель Законодательного собрания Санкт-Петербурга
Дрозденко Александр Юрьевич	Губернатор Ленинградской области
Алферов Жорес Иванович	Председатель Президиума Санкт-Петербургского научного центра Российской академии наук, член президиума Российской академии наук, Лауреат Нобелевской премии
Балыбердин Александр Леонидович	Заместитель директора Административного департамента аппарата Правительства Российской Федерации
Васильева Ольга Юрьевна	Министр образования и науки Российской Федерации
Никифоров Николай Анатольевич	Министр информационных технологий и связи Российской Федерации
Сергеев Алексей Иванович	Генеральный секретарь Совета Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств
Стемпковский Александр Леонидович	Академик-секретарь Отделения нанотехнологий и информационных технологий Российской академии наук
Федоров Александр Вячеславович	Заместитель Председателя Следственного комитета Российской Федерации

ПРЕЗИДИУМ КОНФЕРЕНЦИИ «ИБРР-2017»

Советов Борис Яковлевич	Председатель Президиума, сопредседатель Научного совета по информатизации Санкт-Петербурга
Юсупов Рафаэль Мидхатович	Председатель Организационного Комитета, директор Санкт-Петербургского института информатики и автоматизации Российской академии наук
Говорунов Александр Николаевич	Вице-губернатор Санкт-Петербурга - руководитель Администрации Губернатора Санкт-Петербурга
Кучерявый Михаил Михайлович	Вице-губернатор Ленинградской области - руководитель аппарата Губернатора и Правительства Ленинградской области
Степура Сергей Николаевич	Руководитель Управления ФСТЭК России по Северо-Западному федеральному округу
Чамара Денис Петрович	Председатель Комитета по информатизации и связи Санкт-Петербурга
Максимов Андрей Станиславович	Председатель Комитета по науке и высшей школе Санкт-Петербурга
Пешехонов Владимир Григорьевич	Генеральный директор ГНЦ «Центральный научно-исследовательский институт «Электроприбор»

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ КОНФЕРЕНЦИИ «ИБРР-2017»

Председатель Организационного Комитета

Юсупов Рафаэль Мидхатович	Директор Санкт-Петербургского института информатики и автоматизации Российской академии наук, член-корреспондент Российской академии наук

Заместитель председателя Организационного Комитета

Майоров Владимир Владимирович	Начальник Управления информационной безопасности и технической защиты информации Комитета по информатизации и связи Санкт-Петербурга

Члены Организационного Комитета

Антохина Юлия Анатольевна	Ректор Санкт-Петербургского государственного университета аэрокосмического приборостроения
Алейник Ярослав Александрович	Руководитель Группы компаний «Омега»
Балаценко Андрей Владимирович	Вице-президент – директор макрорегионального филиала «Северо-Запад» ПАО «Ростелеком»
Барышников Сергей Олегович	Ректор Государственного университета морского и речного флота имени адмирала С.О. Макарова
Басков Вячеслав Дмитриевич	Генеральный директор ООО «НеоБИТ»
Бачевский Сергей Викторович	Ректор Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
Блажис Анатолий Константинович	Генеральный директор АО «НТЦ «Фрактал»
Бобрович Владимир Юрьевич	Директор по развитию и внешним связям АО «Концерн «НПО «Аврора»
Богданов Владимир Николаевич	Директор ФГУП «ЦентрИнформ»
Борисов Николай Валентинович	Профессор с возложенными обязанностями заведующего кафедрой информационных систем в искусстве и гуманитарных науках Санкт-Петербургского государственного университета
Васильев Владимир Николаевич	Ректор Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, вице-президент Российского Союза ректоров
Вус Михаил Александрович	Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук
Гаценко Олег Юрьевич	Генеральный директор АО «Научно-исследовательский институт программных средств»
Герус Евгений Валерьевич	Директор СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Гирдин Сергей Алексеевич	Президент ООО «Компания «Марвел»
Гоголь Александр Александрович	Заведующий кафедрой телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
Григорьев Владимир Александрович	Заведующий кафедрой «Беспроводные телекоммуникации» Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, генеральный директор ООО «Лаборатория инфокоммуникационных сетей»
Давыдов Евгений Борисович	Главный конструктор, первый заместитель генерального директора АО «НИИ «Масштаб»

Демидов Алексей Вячеславович	Ректор Санкт-Петербургского государственного университета промышленных технологий и дизайна, председатель Совета ректоров вузов Санкт-Петербурга и Ленинградской области
Жданов Сергей Николаевич	Заместитель генерального директора АО ВТБ Девелопмент
Жигадло Валентин Эдуардович	Директор Филиала ФГУП ЦНИИС - ЛО ЦНИИС
Заборовский Владимир Сергеевич	Директор Института компьютерных наук и технологий, заведующий кафедрой телематики Санкт-Петербургского политехнического университета Петра Великого
Захаров Юрий Никитич	Первый заместитель директора СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Зегжда Петр Дмитриевич	Руководитель отделения «Кибербезопасность», профессор кафедры информационной безопасности компьютерных систем» Санкт-Петербургского политехнического университета Петра Великого
Идрисов Рустам Фидайович	Директор Центра исследований проблем безопасности Российской академии наук
Ипатов Олег Сергеевич	Заместитель проректора по научной работе, заведующий кафедрой программно-аппаратных комплексов реального времени» Санкт-Петербургского политехнического университета Петра Великого
Искандеров Юрий Марсович	Заведующий лабораторией информационных технологий на транспорте Санкт-Петербургского института информатики и автоматизации Российской академии наук
Касаткин Виктор Викторович	Ученый секретарь Научного совета по информатизации Санкт-Петербурга, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук
Кирсанов Игорь Петрович	Генеральный директор ООО «Выставочное Объединение «РЕСТЭК»
Корниенко Анатолий Адамович	Заведующий кафедрой информатики и информационной безопасности Петербургского государственного университета путей сообщения Императора Александра I
Кузичкин Александр Васильевич	Заместитель генерального директора по информационным технологиям АО «НИИ телевидения»
Кузьмин Юрий Григорьевич	Ученый секретарь Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления
Кутузов Владимир Михайлович	Ректор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина)
Марков Вячеслав Сергеевич	Ученый секретарь Объединенного научного совета по проблемам информатики, управления и телекоммуникаций Санкт-Петербургского научного центра Российской академии наук
Максимцев Игорь Анатольевич	Ректор Санкт-Петербургского государственного экономического университета
Михайлов Николай Семенович	Технический директор Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления
Михайлова Анна Сергеевна	Заместитель директора Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления по связям с общественностью
Молдовян Александр Андреевич	Заведующий научно-исследовательским отделом проблем информационной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук

Никулин Евгений Николаевич	Ректор Санкт-Петербургского института экономики и бизнеса
Нырков Анатолий Павлович	Профессор кафедры комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова
Оводенко Анатолий Аркадьевич	Президент Санкт-Петербургского государственного университета аэрокосмического приборостроения
Остапенко Александр Николаевич	Президент Специализированного холдинга «Лаборатория ППШ», советник АО «Лаборатория ППШ», заместитель генерального директора ООО «Лаборатория ППШ»
Панычев Александр Юрьевич	Ректор Петербургского государственного университета путей сообщения Императора Александра I
Присяжнюк Сергей Прокофьевич	Генеральный директор ЗАО «Институт телекоммуникаций»
Пухов Геннадий Георгиевич	Директор ООО «Геонавигатор»
Рунеев Анатолий Юрьевич	Генеральный директор АО «Научно-исследовательский институт «Рубин»
Силла Евгений Петрович	Ученый секретарь Санкт-Петербургского института информатики и автоматизации Российской академии наук
Симонов Михаил Владимирович	Главный консультант директора ФГУП «ЦентрИнформ»
Солодяников Александр Владимирович	Генеральный директор ООО «Ассоциация специалистов безопасности»
Тихомиров Сергей Григорьевич	Генеральный директор АО «Центр компьютерных разработок»
Ткач Анатолий Федорович	Заместитель директора Санкт-Петербургского института информатики и автоматизации Российской академии наук
Туричин Глеб Андреевич	И.о. ректора Санкт-Петербургского государственного морского технического университета
Устинов Игорь Анатольевич	Генеральный директор АО «НПО «Импульс»
Федоров Андрей Евгеньевич	Директор института – заместитель генерального директора АО «Концерн «НПО «Аврора»
Федорченко Людмила Николаевна	Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук
Цыулев Сергей Валентинович	Главный специалист отдела информационно-компьютерной безопасности Комитета по информатизации и связи
Черешкин Дмитрий Семенович	Заведующий лабораторией Института системного анализа Российской академии наук
Чугунов Андрей Владимирович	Заведующий кафедрой управления государственными информационными системами, директор Центра технологий электронного правительства Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики
Шерстюк Юрий Михайлович	Генеральный директор ЗАО «Институт инфотелекоммуникаций»
Шилов Константин Юрьевич	Генеральный директор АО «Концерн «НПО «Аврора»

ПРОГРАММНЫЙ КОМИТЕТ КОНФЕРЕНЦИИ «ИБРР-2017»

Председатель Программного Комитета

Советов Борис Яковлевич	Сопредседатель Научного совета по информатизации Санкт-Петербурга, академик Российской академии образования

Заместители председателя Программного Комитета

Жигадло Валентин Эдуардович	Директор Филиала ФГУП ЦНИИС - ЛО ЦНИИС
Молдовян Александр Андреевич	Заведующий научно-исследовательским отделом проблем информационной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук

Члены Программного Комитета

Алексеев Анатолий Владимирович	Исполнительный директор НП «Институт автоматизации процессов борьбы за живучесть корабля, судна», профессор кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета, д-р техн. наук, проф.
Азаров Артур Александрович	Старший научный сотрудник лаборатории теоретических и междисциплинарных проблем информатики Санкт-Петербургского института информатики и автоматизации Российской академии наук, канд. техн. наук
Афанасьев Александр Васильевич	Полковник полиции, начальник научно-исследовательского отдела Санкт-Петербургского университета МВД России, канд. юрид. наук, доц.
Бариков Леонид Николаевич	Доцент кафедры вычислительных систем и сетей Санкт-Петербургского государственного университета аэрокосмического приборостроения, канд. техн. наук, доц.
Бобрович Владимир Юрьевич	Директор по инновациям и развитию АО «Концерн «НПО «Аврора», д-р техн. наук, проф.
Бессонова Екатерина Евгеньевна	Ассистент кафедры безопасных информационных технологий Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, канд. техн. наук
Беззатеев Сергей Валентинович	Заведующий кафедрой безопасности киберфизических систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, д-р техн. наук, доц.
Бирюков Михаил Александрович	Адъютант Военной академии связи им. С.М. Буденного
Бузников Анатолий Алексеевич	Заслуженный профессор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), заслуженный деятель науки Российской Федерации, д-р техн. наук, проф.
Вассоевич Андрей Леонидович	Профессор кафедры политической психологии факультета психологии Санкт-Петербургского государственного университета, д-р филос. наук, проф.
Воробьев Владимир Иванович	Главный научный сотрудник лаборатории информационно-вычислительных систем и технологий программирования Санкт-Петербургского института информатики и автоматизации Российской академии наук, д-р техн. наук, проф.
Вус Михаил Александрович	Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук
Горохов Владимир Леонидович	Профессор кафедры инновационного менеджмента Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), д-р техн. наук, проф.
Домбровская Лариса Александровна	Профессор кафедры математики и информатики Санкт-Петербургского университета МВД России, канд. пед. наук, доц.

Заколдаев Данил Анатольевич	декан факультета информационной безопасности и компьютерных технологий, заведующий кафедрой проектирования и безопасности компьютерных систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, канд. техн. наук, доц.
Зикратов Игорь Алексеевич	Декан факультета информационных систем и технологий Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, д-р техн. наук, проф.
Зегжда Петр Дмитриевич	Руководитель отделения «Кибербезопасность», профессор кафедры информационной безопасности компьютерных систем Санкт-Петербургского политехнического университета Петра Великого, заслуженный деятель науки Российской Федерации, д-р техн. наук, проф.
Ивлева Людмила Евгеньевна	Заведующая лабораторией электронных информационно-образовательных технологий им. проф. Ю.М. Кулибанова
Игнатъев Михаил Борисович	Заслуженный профессор Санкт-Петербургского государственного университета аэрокосмического приборостроения, заслуженный деятель науки Российской Федерации, д-р техн. наук, проф.
Игумнов Владимир Вячеславович	Первый заместитель генерального директора, главный конструктор АО «НПО «Импульс», канд. техн. наук
Искандеров Юрий Марсович	Заведующий лабораторией информационных технологий на транспорте Санкт-Петербургского института информатики и автоматизации Российской академии наук, д-р техн. наук, проф.
Касаткин Виктор Викторович	Ученый секретарь Научного совета по информатизации Санкт-Петербурга, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, канд. техн. наук, доц.
Кефели Игорь Федорович	Директор Центра геополитической экспертизы Северо-Западного института управления – филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, заслуженный работник высшей школы Российской Федерации, д-р филос. наук, проф.
Колбанёв Михаил Олегович	Профессор Санкт-Петербургского государственного экономического университета, д-р техн. наук, проф.
Коноплёв Георгий Асадович	Доцент кафедры квантовой электроники и оптико-электронных приборов Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), канд. техн. наук, доц.
Корниенко Анатолий Адамович	Заведующий кафедрой информатики и информационной безопасности Петербургского государственного университета путей сообщения Императора Александра I, д-р техн. наук, проф.
Коршунов Игорь Львович	Заведующий кафедрой информационных систем и технологий Санкт-Петербургского государственного экономического университета, канд. техн. наук, доц.
Котенко Игорь Витальевич	Заведующий лабораторией проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, д-р техн. наук, проф.
Лебедев Илья Сергеевич	Ведущий научный сотрудник лаборатории информационных технологий на транспорте Санкт-Петербургского института информатики и автоматизации Российской академии наук, д-р техн. наук, доц.

Левкин Игорь Михайлович	Профессор кафедры информационных систем и технологий Санкт-Петербургского государственного экономического университета, д-р воен. наук, проф.
Литвинов Владислав Леонидович	Доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А.Бонч-Бруевича, канд. техн. наук, доц.
Майоров Владимир Владимирович	Начальник Управления информационной безопасности и технической защиты информации Комитета по информатизации и связи
Микадзе Сергей Юрьевич	Проректор Санкт-Петербургского государственного экономического университета, канд. экон. наук
Митько Арсений Валерьевич	Доцент кафедры радиотехнических и оптоэлектронных комплексов Санкт-Петербургского государственного университета аэрокосмического приборостроения, председатель Совета молодых учёных Севера Арктической общественной академии наук, канд. техн. наук, доц.
Митько Валерий Брониславович	Советник директора Ленинградского отделения Центрального научно-исследовательского института связи, президент Арктической общественной академии наук, д-р техн. наук, проф.
Молдовян Николай Андреевич	Заведующий лабораторией криптологии Санкт-Петербургского института информатики и автоматизации Российской академии наук, заслуженный изобретатель Российской Федерации, д-р техн. наук, проф.
Мусатенко Роман Иванович	Руководитель Центра ранговой партнерской сертификации НП «Институт автоматизации процессов борьбы за живучесть корабля, судна»
Новикова Евгения Сергеевна	Доцент кафедры информационных систем Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), канд. техн. наук, доц.
Нырков Анатолий Павлович	Заведующий кафедрой комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова, д-р техн. наук, проф.
Паращук Игорь Борисович	Профессор кафедры автоматизированных систем специального назначения Военной академии связи им. С.М. Буденного, д-р техн. наук, проф.
Плебанек Ольга Васильевна	Заведующая кафедрой социально-гуманитарных наук Межрегионального института экономики и права, профессор кафедры социально-гуманитарных наук глобалистики и геополитики Национального государственного Университета физической культуры, спорта и здоровья имени П.Ф.Лесгафта, Санкт-Петербург, д-р филос. наук, доц.
Полежаева Ольга Дмитриевна	Директор проекта Северо-Западного института управления – филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации
Примакин Алексей Иванович	Полковник полиции, начальник кафедры специальных информационных технологий Санкт-Петербургского университета МВД России, д-р техн. наук, проф.
Путилин Алексей Николаевич	Заместитель главного конструктора АО «НПО «Импульс», д-р техн. наук, проф.
Разживин Никита Сергеевич	Магистрант кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета

Саенко Игорь Борисович	Ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, д-р техн. наук, проф.
Согонов Сергей Александрович	Заведующий кафедрой судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета, канд. техн. наук, доц.
Соколов Сергей Сергеевич	Проректор по учебной работе Государственного университета морского и речного флота имени адмирала С.О. Макарова, д-р техн. наук, доц.
Созинова Екатерина Николаевна	Доцент кафедры проектирования безопасных компьютерных систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, канд. техн. наук
Татарникова Татьяна Михайловна	Профессор кафедры информационных систем и технологий Санкт-Петербургского государственного экономического университета, д-р техн. наук, доц.
Трофимов Валерий Владимирович	Заведующий кафедрой информатики Санкт-Петербургского государственного экономического университета, заслуженный деятель науки Российской Федерации, д-р техн. наук, проф.
Тулупьев Александр Львович	Заведующий лабораторией теоретических и междисциплинарных проблем информатики Санкт-Петербургского института информатики и автоматизации Российской академии наук, д-р физ.-мат. наук, доц.
Тюрин Иван Сергеевич	Системный аналитик НП «Институт автоматизации процессов борьбы за живучесть корабля, судна»
Устинов Игорь Анатольевич	Генеральный директор АО «Научно-производственное объединение «Импульс», канд. техн. наук
Цехановский Владислав Владимирович	Заведующий кафедрой информационных систем Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), канд. техн. наук, доц.
Цыулёв Сергей Валентинович	Главный специалист отдела информационно-компьютерной безопасности Управления информационной безопасности и технической защиты информации Комитета по информатизации и связи
Чечулин Андрей Алексеевич	Старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, канд. техн. наук
Шакин Дмитрий Николаевич	Заместитель руководителя Управления ФСТЭК России по Северо-Западному федеральному округу, канд. воен. наук, доц.
Шишкин Владимир Михайлович	Старший научный сотрудник лаборатории информационно-вычислительных систем и технологий программирования Санкт-Петербургского института информатики и автоматизации Российской академии наук, канд. техн. наук, доц.
Яковлева Наталья Александровна	Полковник полиции, начальник кафедры математики и информатики Санкт-Петербургского университета МВД России, канд. психол. наук

Ученый секретарь Конференции

Заболотский Вадим Петрович

Главный научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук

Координатор Конференции

Касаткин Виктор Викторович

Ученый секретарь Научного совета по информатизации Санкт-Петербурга, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук

Информационное обеспечение Конференции

«Компьютер Информ»

Газета о передовых инфокоммуникационных и телекоммуникационных технологиях, продуктах, решениях для руководителей предприятий и организаций, отделов автоматизации, телекоммуникационного и информационного обеспечения, ведущих специалистов служб ИТ, студентов и школьников <http://www.ci.ru>



ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ

УДК 35.078.42

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СЕВЕРО-ЗАПАДНОМ ФЕДЕРАЛЬНОМ ОКРУГЕ КАК ПРИМЕР РЕАЛИЗАЦИИ РЕГИОНАЛЬНОЙ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ

Кучерявый Михаил Михайлович, Вовенда Юлия Владимировна

Администрация Ленинградской области

Россия, Санкт-Петербург, Суворовский пр., 67

emails: apparat@lenreg.ru, vovenda-yv@sziiu.ru

Аннотация: В статье рассматривается деятельность органов государственной власти Северо-Западного федерального округа по обеспечению безопасности информации. Освещаются вопросы формирования и функционирования системы защиты информации в Северо-Западном федеральном округе. Особое внимание уделено государственным информационным системам, процессам регулирования и контроля обеспечения безопасности информации Управлением ФСТЭК по СЗФО.

Ключевые слова: Органы государственной власти, обеспечение информации, система защиты информации, государственные информационные системы, техническая защита информации.

INFORMATION SECURITY IN THE NORTH-WEST FEDERAL DISTRICT AS AN EXAMPLE OF IMPLEMENTATION OF REGIONAL STATE POLICY

Kucheryavyi Mikhail, Vovenda Julia

Administration of the Leningrad Region

Russia, St. Petersburg, Suворovsky pr., 67

emails: apparat@lenreg.ru, vovenda-yv@sziiu.ru

Abstract: The article is considered the activities of public authorities of the North-West Federal District to ensure information security. Highlightsthe issues of formation and functioning of the information security system in the North-West Federal District. The main attention is paid to the state information systems, control and monitoring of security information by the FSTEC Office for the North-West Federal District.

Keywords: Public authorities, providing information, information security system, state information systems, technical protection of information.

Сегодняшний мир, в котором мы живем – это мир, который характеризуется глобальным развитием, усовершенствованием информационно-коммуникационных технологий и сложившаяся к настоящему времени новая политическая реальность характеризуется трансформацией разрозненных и суверенных информационных систем в единое глобальное пространство.

Надёжная работа информационных ресурсов, систем управления и связи имеет исключительное значение для обороноспособности страны, для устойчивого развития экономики и социальной сферы, для защиты суверенитета России.

Доктриной информационной безопасности Российской Федерации [1] предусматривается повышение эффективности функционирования системы государственного управления, обеспечение информационного взаимодействия между органами власти при решении задач в области обороны и безопасности.

Определяя в качестве приоритетов построение в Российской Федерации информационного общества, государственная политика нацелена на усиление внимания к защите государственных информационных ресурсов.

Существующие современные угрозы в информационной сфере направлены, в первую очередь, против действующих органов государственной власти и управления всех регионов Российской Федерации.

В государственных и муниципальных информационных системах органов власти субъектов Российской Федерации Северо-Западного федерального округа обрабатываются значительные массивы информации ограниченного доступа.

Зарегистрированных государственных информационных систем в округе около четырехсот, муниципальных более пятисот. В более чем четырех с половиной тысячах информационных систем персональных данных обрабатывается информация о населении округа. Такие данные очень привлекательны для технических разведок иностранных государств.

При этом официально, в соответствии с «Договором по открытому небу» [2], осуществляется детальная фотосъемка объектов по маршруту полета.

Так же легально, в рамках международных научно-исследовательских программ, ведется разведка с использованием иностранных технических средств наблюдения и контроля, которые позволяют получать сведения об экономическом и военном потенциалах Северо-Западного региона. Такие средства размещены в Республике Коми, Мурманской и Ленинградской областях, в Санкт-Петербурге.

Технические средства более двадцати стран НАТО объединены в систему глобального контроля международных линий связи «Эшелон». Наибольшую угрозу для государственных информационных систем Северо-Западного федерального округа представляет техническая компьютерная разведка, реализованная в системе электронного наблюдения PRISM.

Для обеспечения своевременной и адекватной реакции на возникающие и прогнозируемые угрозы утечки информации ограниченного доступа в округе сформирована и функционирует система защиты информации, которая охватывает все уровни и ветви органов власти Северо-Западного федерального округа.

Управление ФСТЭК России по Северо-Западному федеральному округу осуществляет координацию деятельности по защите информации в пределах федерального округа, организует функционирование сформированной системы защиты информации.

Управление ФСТЭК России по Северо-Западному федеральному округу осуществляет реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам: обеспечения безопасности информации; противодействия иностранным техническим разведкам на территории Российской Федерации; обеспечения защиты информации, содержащей сведения, составляющие государственную тайну и т.д.

Система органов государственной власти и управления в Северо-Западном федеральном округе является центральным звеном обеспечения информационного противоборства в регионе.

Важное значение имеет обеспечение защиты информации в государственных информационных системах. В информационных системах органов власти циркулирует информация, имеющая значение для деятельности государства и региона, в том числе в социальной сфере, здравоохранении и образовании, преждевременное раскрытие которой может привести к нежелательному, негативному общественному резонансу. Безопасность информации в государственных информационных системах достигается путем проведения большого комплекса работ, в том числе по аттестованию ГИС и созданию систем по технической защите информации.

Работа по определению статуса информационных систем в органах власти находится на начальном этапе, в то время как решениями Межведомственного совета по защите информации в Северо-Западном федеральном округе руководителям органов власти рекомендовалось выполнить данные работы в 2014 году. При этом необходимая правовая база, определяющая порядок и содержание работ по защите информации в государственных информационных системах, уже сформирована.

Фактическое состояние работ по защите информации в государственных информационных системах органов государственной власти и органов местного самоуправления оценивается в ходе контроля, проводимого Управлением ФСТЭК России по СЗФО.

За последнее время проверены на соответствие требованиям законодательства Российской Федерации, нормативных и методических документов ФСТЭК России информационные системы органов государственной власти Санкт-Петербурга, Мурманской и Архангельской областей.

Результаты контроля показали, что основные организационные и технические требования приказа ФСТЭК России от 11 февраля 2013 г. № 17 [4] в полном объеме выполнены только в проверенных государственных информационных системах Санкт-Петербурга.

Уровень защищенности информационных систем в органах государственной власти не в полной мере соответствует существующим угрозам и масштабам информатизации.

Темпы совершенствования региональных систем защиты информации отстают от возрастания и усложнения требований в области информационной безопасности.

Без усиления внимания руководства к подбору, подготовке специалистов и необходимому финансированию работ, эффективность по обеспечению безопасности информации будет недостаточной.

СПИСОК ЛИТЕРАТУРЫ:

- 1 Доктрина информационной безопасности Российской Федерации. Новая редакция. [Электронный ресурс]. URL: http://infosystems.ru/assets/files/files/doktrina_IB.pdf

- 2 Договор по открытому небу. [Электронный ресурс] // Организация по безопасности сотрудничеству в Европе. URL: <http://www.osce.org/ru/library/14131>
- 3 Сведения о полномочиях ФСТЭК России; перечень нормативных правовых актов, определяющих эти полномочия. [Электронный ресурс] // ФСТЭК России. URL: <http://fstec.ru/obshchaya-informatsiya/polnomochiya>
- 4 Приказ Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [Электронный ресурс] // ФСТЭК России. URL: <http://fstec.ru/normativnye-pravovye-akty-tzi/110-deyatelnost/tekushchaya/tekhnicheskaya-zashchita-informatsii/normativnye-pravovye-akty/prikazy/703-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17>

УДК 323

КОНЦЕПЦИЯ СЕКЬЮРИТИЗАЦИИ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ ПОЛИТИКИ РОССИИ

Баранов Николай Алексеевич

Санкт-Петербургский государственный университет,
Санкт-Петербург, ул. Смольного, 1-3, 7-й подъезд
Северо-Западный институт управления – филиал РАНХиГС
199178, Санкт-Петербург, В.О., Средний пр. В.О., 57/43
email: nicbar@mail.ru

Аннотация: В статье рассматривается деятельность государства в информационной сфере, которая может способствовать распространению процесса секьюритизации, подвергая опасности права и свободы человека. В результате ценность безопасности начинает превалировать над всеми остальными политическими ценностями, детерминируя все сферы жизни.

Ключевые слова: информатизация, секьюритизация, угрозы безопасности, экстремальная политика.

THE CONCEPT OF SECURITIZATION IN THE CONTEXT OF INFORMATION POLICY OF RUSSIA

Baranov Nikolai

St. Petersburg State University,
Russia, St. Petersburg, Smolny St., 1-3, 7th entrance,
Northwest institute of management – RANEPA branch,
Russia, St. Petersburg, V.O., Sredny Ave. V.O., 57/43
email: nicbar@mail.ru

Abstract: In article activity of the state in the information sphere which can promote securitization process distribution is considered, endangering the right and freedom of the person. As a result the value of safety begins to prevail over all other political values, determining all spheres of life.

Keywords: informatization, securitization, threats to security, extreme policy.

Введение. В современных обществах на первый план выходят проблемы безопасности, что вполне объяснимо с точки зрения социальных приоритетов. Включение проблематики безопасности в новые сферы жизни общества – экологическую, экономическую, культурную, информационную – способствует легитимации чрезвычайных мер, предпринимаемых государством, что сказывается на ограничениях демократических процедур. В результате ценность безопасности начинает превалировать над всеми остальными политическими ценностями, детерминируя все сферы жизни.

В академической среде появилась потребность обосновать новые тенденции политических изменений в мире. Так, в последнее десятилетие стала актуальной концепция секьюритизации, предложенная Б. Бузаном, О. Уивером и Я. Де Вилдом [1], связанная с восприятием новых угроз безопасности обществом. Исследователями Копенгагенской школы международных отношений была предложена новая структура в исследовании безопасности, предполагающая раскрытие механизма актуализации данного феномена: каким образом некий объект начинает рассматриваться в качестве угрозы, как он привносится в политический дискурс и утверждается в качестве угрозы, т. е. секьюритизируется.

Процесс, в ходе которого объект представляется в качестве проблемы безопасности и начинает рассматриваться как угроза, американский политолог Барри Бузан называет секьюритизацией [2]. В качестве объекта может выступать государство, национальный суверенитет, экономика, экологическая сфера, идентичность, биологические виды. Объект становится вопросом безопасности после принятия решения о его важности по сравнению с другими. В этом случае объекту придается статус чрезвычайного приоритета, что выводит его из области обычной политики. Такой статус может быть определен акторами, утверждающими, что объект находится под угрозой его существованию. В качестве акторов могут быть как государственные институты, так и гражданские, не относящиеся к сфере политики.

Массовая информатизация общества способствует возникновению новых угроз безопасности, которые распространяются как на частную жизнь, так и на социальную, политическую, экономическую

сферы. В сложившихся условиях высокую значимость приобретает деятельность государства в информационной сфере, которая включает в себя совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, связанных с формированием и обработкой информации, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

Значимость любого произошедшего события зависит, в первую очередь, от его интерпретации в средствах массовой информации. А если эта информация имеет политический подтекст, выгодный одним и не выгодный другим акторам мирового политического процесса, то возникает потребность в соответствующем объяснении событий. Поэтому информационная политика «как особая сфера жизнедеятельности людей, связанная с распространением информации в интересах государства и гражданского общества» [3, с. 103] занимает особое место в современном обществе.

Информационное воздействие в XXI веке приобретает еще большую значимость, так как его направленность влияет на поведение большого количества людей, у которых под влиянием той или иной информации могут возникать потребности как конструктивного, так и деструктивного характера, что существенным образом влияет на политическую ситуацию в стране и в мировом пространстве в целом. Недаром средства информационного воздействия называют информационным оружием, так как по своим разрушительным силам оно сопоставимо с обычными средствами вооружения, а иногда по своим последствиям превосходит их. В современном научном дискурсе под информационным оружием понимается «совокупность информации, а также специальных методов, устройств и средств манипуляции ею для скрытого воздействия на информационный ресурс противника с целью достижения поставленных целей и решения задач информационной борьбы (войны)» [4, с. 53].

В целях предотвращения угрозы такого воздействия Россия предпринимает необходимые меры для обеспечения национальной и международной информационной безопасности, противодействия угрозам государственной, экономической и общественной безопасности, исходящим из информационного пространства, для борьбы с терроризмом и иными угрозами с применением информационно-коммуникационных технологий, добивается выработки под эгидой ООН универсальных правил ответственного поведения государств в информационной сфере, в том числе посредством интернационализации на справедливой основе управления информационно-коммуникационной сетью «Интернет».

В Стратегии национальной безопасности Российской Федерации высказывается озабоченность тем, что «все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории» [5]. В Стратегии отмечается, что появляются новые формы противоправной деятельности с использованием информационных коммуникационных и высоких технологий. В целях осуществления государственной и общественной безопасности совершенствуется система выявления и анализа угроз в информационной сфере, противодействия им; принимаются меры для повышения защищенности граждан и общества от деструктивного информационного воздействия со стороны экстремистских и террористических организаций, иностранных спецслужб и пропагандистских структур.

Важнейшей задачей государства в рамках информационного противоборства является контроль информационного пространства, интегрированного в глобальное информационное пространство и являющегося его частью; создание специальных сил, в функции которых входит ведение информационного противоборства; разработка средств информационного воздействия; принятие нормативно-правовых актов, обосновывающих и определяющих информационную политику страны.

Агрессивная информационная политика, проводимая западными странами против России, вынуждает российское политическое руководство принимать адекватные меры, и прежде всего в концептуальном плане. 5 декабря 2016 г. Президентом России была утверждена Доктрина информационной безопасности Российской Федерации, представляющая собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере на основе анализа основных информационных угроз и оценки состояния информационной безопасности [6].

В условиях тотального проникновения информационных технологий во все сферы жизни общества возникает потребность в создании соответствующей инфраструктуры в целях формирования общества знаний, в котором преобладающее значение для развития гражданина, экономики и государства имеют получение, сохранение, производство и распространение достоверной информации с учетом стратегических национальных приоритетов Российской Федерации. Такая цель перед государством поставлена в Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы, утвержденной Указом Президента России от 9 мая 2017 г., в которой определены задачи и меры по реализации внутренней и внешней политики страны «в сфере применения информационных и коммуникационных технологий, направленные на развитие

информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов» [7].

В сложившихся условиях национальными интересами страны становятся развитие человеческого потенциала, обеспечение безопасности граждан и государства, повышение роли России в мировом гуманитарном и культурном пространстве, развитие свободного, устойчивого и безопасного взаимодействия граждан и организаций, органов государственной власти Российской Федерации, органов местного самоуправления, повышение эффективности государственного управления, развитие экономики и социальной сферы, формирование цифровой экономики.

Заключение. Таким образом, в Российской Федерации произошла секьюритизация информационной сферы. В качестве акторов выступили как государство, так и часть гражданского общества, в основном патристично настроенное, признавшее высокую значимость информационных технологий и их способность оказывать влияние на все стороны жизнедеятельности общества. Необходимость защиты от проникновения в частную сферу, служебную переписку, деятельность государственных и муниципальных учреждений было признано гражданами, обществом и государством, что привело к легитимации угрозы в информационной сфере. Поэтому принятые меры в виде вышеперечисленных государственных нормативно-правовых документов создали условия для экстремальной политики, логически завершив процесс секьюритизации.

СПИСОК ЛИТЕРАТУРЫ

1. Buzan B., Wæver O., de Wilde J. Security: A New Framework for Analysis. L.: Lynne Rienner Publishers, 1998. 239 p.
2. Агапеева К. Теория секьюритизации Барри Бузана // Информационно-аналитический портал «Геополитика». URL: <https://www.geopolitica.ru/article/teoriya-sekyuritizacii-barri-buzana> (дата обращения: 11.06.2017).
3. Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно-психологической войны. М.: Горячая линия – Телеком, 2012. 542 с.
4. Анненков В. Информационно-психологическое противоборство: современные аспекты // Современный мир и геополитика / Отв. ред. М.А. Неймарк. М.: Издательство «Канон+» РООИ «Реабилитация», 2015. С.116-126.
5. Указ Президента Российской Федерации «О Стратегии национальной безопасности Российской Федерации» от 31 декабря 2015 г. №683 // Официальный сайт Президента России. URL: <http://kremlin.ru/acts/bank/40391> (дата обращения: 11.06.2017).
6. Доктрина информационной безопасности Российской Федерации. URL: <http://kremlin.ru/acts/bank/41460> (дата обращения: 15.01.2017).
7. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы. URL: <http://www.kremlin.ru/acts/bank/41919> (дата обращения: 11.06.2017).

УДК 004.9

УПРАВЛЕНИЕ БЕЗОПАСНОЙ ИНТЕЛЛЕКТУАЛЬНОЙ СРЕДОЙ ОБИТАНИЯ НА ПРИМЕРЕ ЖИЛИЩНО-КОММУНАЛЬНОЙ СФЕРЫ САНКТ-ПЕТЕРБУРГА

Груздева Мария Николаевна¹, Шарипов Роман Радикович²

¹ Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Россия, Санкт-Петербург, В.О., Биржевая линия, 14

² Санкт-Петербургский информационно-аналитический центр, Россия, Санкт-Петербург, ул. Черняховского, 59
emails: gruzdevamariia@ya.ru, sharipov@iac.spb.ru

Аннотация: В докладе рассмотрены основы формирования безопасной интеллектуальной среды обитания, ее характеристики и проблема отсутствия технологии управления интеллектуальной средой обитания в жилищно-коммунальной сфере.

Ключевые слова: технологии; информационная система, интеллектуальная среда обитания; жилищно-коммунальная сфера, умный город.

MANAGEMENT OF THE INTELLECTUAL ENVIRONMENT AMONG THE EXAMPLE OF THE HOUSING AND MUNICIPAL SPHERE OF SAINT PETERSBURG

Gruzdeva Maria¹, Sharipov Roman²

¹ ITMO University, Department of Government Information Systems Management, Russia, St. Petersburg, Birzhevaya linia, 14

² St. Petersburg Information and Analytical Centre, Russia, St. Petersburg, Cherniahovskogo, 59
emails: gruzdevamariia@ya.ru, sharipov@iac.spb.ru

Abstract: The report considers the foundations of the formation of an intellectual environment among, its characteristics and the lack of technology for managing the intellectual environment in the housing and communal sphere.

Keywords: technologies; information system, intellectual environment among; housing and communal sphere, smart city.

Введение. В настоящее время активно развиваются умные города, посредством внедрения и применения информационных технологий, интеллектуальных систем, технологий интернет вещей и т.д. Стремительное развитие научно-технического прогресса привело к тому, что во все отрасли внедряются инновации [1]. Научно-технический прогресс выступает как важнейшее средство решения социально-экономических задач, повышения качества жизни граждан, повышения производительности и интерактивности городских служб, снижения расходов и потребления ресурсов, повышения эффективности взаимодействия между городскими жителями и государством, охраны окружающей среды, а также комплексной безопасности [2]. Это служит формированию интеллектуальной среды обитания.

Целью научного исследования является изучение основ формирования безопасной интеллектуальной среды обитания и применимость технологии управления на примере жилищно-коммунальной сферы.

Интеллектуальная среда обитания (далее – ИСО) – это сложная система, параметры которой (комфорт, физическая безопасность, энергоэффективность, экологическая безопасность и др.), определяют ее состояние с помощью датчиков (периферийных устройств), определяющих и измеряющих параметры отдельных объектов во времени и анализа измеряемых параметров для принятия управляющих решений и автоматического воздействия на объекты.

Применительно к жилищно-коммунальной сфере объектами ИСО являются дома, субъектами – граждане, проживающие в этих домах, управляющие организации и органы государственной власти, осуществляющие контроль и управление за деятельностью.

ИСО активно использует алгоритмы и устройства, которые способны воспринимать и изменять окружающее пространство, развивать себя. Развитие происходит с помощью методов самообучения на основе окружающей среды.

В жилищно-коммунальной сфере на сегодняшний день существуют такие проблемы, как ненадлежащее качество состояния объектов (домов) и отсутствие полной информации о текущем состоянии объектов. Но основной проблемой, применительно к управлению над объектами интеллектуальной среды обитания, является отсутствие возможных технологий и инструментов для принятия управляющих решений и автоматического воздействия на объекты.

Проблемы были выделены на основе изучения Государственной информационной системы Санкт-Петербурга «МТС МКД» и данных об объектах, содержащейся в ней [3]. Назначением системы является автоматизация управленческой деятельности, учет технического состояния объектов жилищного фонда, а также обследование, хранение, обработка и актуализация технико-экономических параметров объектов жилищного фонда [5].

В рамках научного исследования предлагается внедрить комплексную технологию управления ИСО на основе модернизации Государственной информационной системы Санкт-Петербурга «МТС МКД».

ИСО в жилищно-коммунальной сфере имеет свои характеристики, такие как комфортность – автоматизация принятия и исполнения решений по воздействию на окружающие объекты; энергоэффективность – рациональное использование энергетических ресурсов; коммуникационность – общение на различных уровнях между объектами, входящими в ИСО; безопасность – важнейшим условием обеспечения комплексной безопасности является максимальная незаметность средств, используемых для ее обеспечения, что безусловно связано с интеллектуализацией системы.

Интеллектуальные системы внедряются в объекты среды. Примером служит автоматическая система обеспечения технической безопасности квартиры или дома. Система технической безопасности может совмещаться с системой защиты от проникновения, системой учета расходов воды, энергии и т.п. Важнейшей частью интеллектуальных систем является обеспечение информационной безопасности, сохранение целостности и доступности данных, собираемых с помощью периферийных устройств. Необходимо чтобы были меры и действия, направленные на предупреждение нарушения целостности и функциональности систем. Уровень уязвимости может быть высоким, сформированный множеством факторов внешней и внутренней среды [5].

Работа выполнена в рамках проекта № 417007 «Исследование факторов, влияющих на развитие «умных городов» и их эффективность».

СПИСОК ЛИТЕРАТУРЫ

1. Груздева М.Н., Павловская М.А. Концепция "умных" городов: развитие и тренды цифровых трансформаций // Информационные ресурсы России, 2017. № 4 (158). С. 33
2. Жанназарова Г. К., Талипова Р. Н. Научно-технический прогресс – положительные и отрицательные стороны // Молодой ученый. 2016. №21.1. С.16
3. Государственная информационная система Санкт-Петербурга «Мониторинг технического состояния многоквартирных домов в Санкт-Петербурге» [Электронный ресурс] – URL: <http://test.dice.spb.ru/NotLogged.aspx?SpecifyArguments> (дата обращения: 15.06.2017)
4. Портал «Открытые данные» [Электронный ресурс] – URL: <http://data.gov.spb.ru> (дата обращения: 15.09.2017)
5. Сиражова З.Г. Обзор технологии, средств обеспечения и политики компьютерной безопасности интеллектуальных систем // Автоматизация и управление в технических системах (АУТС), 2014. №1.1 (8). С.58

УДК 004.056

АКТУАЛЬНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОСУЩЕСТВЛЕНИИ ГОСУДАРСТВЕННОЙ МИГРАЦИОННОЙ ПОЛИТИКИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Клечиков Александр Владимирович
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, В.О., Биржевая линия, 14
email: od@mail.ifmo.ru

Аннотация: В докладе рассмотрено действующее законодательство в сфере государственной миграционной политики, представлен пример информационного продукта для электронного тестирования трудовых мигрантов на территории РФ. Автором обозначена значимость информационных технологий в данной сфере и перспектив их развития, выявлена и обоснована необходимость поддержания высокого уровня информационной безопасности при обмене данными.

Ключевые слова: миграционная политика; автоматизация процессов; информационная безопасность; обмен данными.

ACTUAL ASPECTS OF INFORMATION INFRASTRUCTURE IN THE IMPLEMENTATION OF STATE MIGRATION POLICY IN THE RUSSIAN FEDERATION

Klechikov Aleksandr
ITMO University
Russia, St. Petersburg, Birzhevaya linia, 14
email: od@mail.ifmo.ru

Abstract: The report considers the current legislation in the sphere of state migration policy, provides an example of an information product for electronic testing of labor migrants in the territory of the Russian Federation. The author outlined the importance of information technologies in this area and the prospects for their development, identified and justified the need to maintain a high level of information security in the exchange of data.

Keywords: migration policy; automation of processes; information security; data exchange.

Введение. Процесс глобализации, достигший серьезных масштабов в XXI веке, открыл новые проблемы перед современным мировым сообществом. На сегодняшний день одной из наиболее резонансных проблем стала проблема миграции, которая особенно остро охватила страны Западной Европы. После распада СССР наиболее экономически-привлекательным регионом, притягивающим мигрантов из стран Восточной Европы и Средней Азии, стала Россия.

Благодаря утвержденной в июне 2012 года Концепции государственной миграционной политики [1], со сроком реализации до 2025 года, стали формироваться механизмы привлечения (отбора) иностранных граждан с востребованными в стране профессионально-квалификационными и образовательными навыками. Данная концепция также тесно связана с Концепцией долгосрочного социально-экономического развития Российской Федерации до 2020 года, Концепцией демографической политики Российской Федерации на период до 2025 года и стратегией национальной безопасности Российской Федерации до 2020 года.

В рамках исполнения пунктов Концепции государственной миграционной политики был проведен целый ряд мероприятий. Принципиальной задачей привлечения (отбора) и использования иностранной рабочей силы стала автоматизация процесса тестирования трудовых мигрантов. Таким образом, в 2012 году одним из первых в России был создан программный комплекс «ЭЛТЕРУС» [2], позволяющий проводить тестирование мигрантов по русскому языку на базе уполномоченных ВУЗов страны с выдачей соответствующих государственных сертификатов. В настоящее время программа позволяет также проводить тестирование на знания русского языка, истории России и законодательства РФ путем предоставления доступа к современной информационной среде тестирования при помощи терминалов с сенсорными экранами. «ЭЛТЕРУС» позволяет создавать и обрабатывать материалы для проведения тестирования, включая аудиограммы, использовать обезличенные данные тестируемых, результаты тестирования, архивы методических материалов. Программный комплекс поддерживает процесс оценки знаний тестируемых путем анализа их ответов с последующим формированием регламентированных документов с результатами тестирования.

Однако, несмотря на большую работу по автоматизации процесса электронного тестирования трудовых мигрантов, существует ряд значимых и проблемных моментов развития данной области.

Ключевым направлением развития должно стать внедрение системы оценки знаний потенциальных мигрантов непосредственно в странах исхода. Это позволит сократить поток неквалифицированных мигрантов, не прошедших отбор на территориях своих стран, кроме того, сократит их финансовые затраты по временному и необходимому нахождению на территории РФ для прохождения тестирования. Главной проблемой в данном направлении является необходимость

формирования и защиты трансграничных потоков данных, позволяющих организовать юридически-значимый документооборот со странами исхода. Для этого требуется не только создать межгосударственную нормативно-правовую базу, но и обеспечить реализацию высокого уровня информационной безопасности во избежание фальсификации или потери данных.

Следующим направлением развития может стать создание единого межведомственного электронного взаимодействия (МВД, Минобрнауки РФ, Пограничная служба ФСБ РФ, региональные органы государственной власти) при обеспечении информационной безопасности, то есть всех ключевых структур, участвующих в государственном миграционном регулировании на территории РФ.

Также представляется целесообразной разработка информационной системы предварительного тестирования знаний иностранных граждан, которая позволила бы бесплатно и быстро оценить свои знания для определения уровня подготовки перед сдачей основных тестов. При этом уровень информационной безопасности при прохождении даже таких, предварительных тестов должен сохраняться на высоком уровне.

Заключение. Необходимость развития государственной миграционной политики обозначена в Концепции, утвержденной Президентом Российской Федерации. В настоящее время уже запущены процессы автоматизации тестирования иностранных граждан на территории РФ, для обеспечения легитимности которых необходимо поддержание высокого уровня информационной безопасности. А также выявлены направления развития данной области, требующие консолидированных юридических и технологических решений.

СПИСОК ЛИТЕРАТУРЫ

1. Концепция государственной миграционной политики Российской Федерации на период до 2025 года. – URL: <http://kremlin.ru/events/president/news/15635> (дата обращения на 03.10.2017).
2. Элтерус [описание программного комплекса] // Сайт ООО «Агентство электронного тестирования» – URL: <http://spbeta.ru/elterus> (дата обращения на 03.10.2017).

УДК 004.624, 351\354

ИСПОЛЬЗОВАНИЕ ПОЧТОВЫХ АКТИВОВ В СОЗДАНИИ ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА УМНОГО ГОРОДА

Павловская Мария Александровна, Кононова Ольга Витальевна
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Биржевая линия, 14,
emails: pavlovskayamaria@gmail.com, kononolg@yandex.ru

Аннотация: В статье рассмотрены возможности участия почтовых служб в проектах умного города, применимости подхода в российских реалиях и за рубежом. Основная идея заключается в интеграции информационных систем умного города и активов почтовых служб и подразделений для более эффективного и повсеместного сбора городских данных. Интеграция позволит улучшить результаты управления умным городом, обеспечит безопасность использования информационных ресурсов. В статье приведен анализ международных источников.

Ключевые слова: *умный город; город, управляемый данными; почтовые активы; информационная безопасность; защищенное информационное пространство*

THE POSTAL ASSETS IN THE CREATION OF A SMART CITY PROTECTED INFORMATION SPACE

Pavlovskaya Maria, Kononova Olga
ITMO University,
Russia, St. Petersburg, Birzhevaya linia, 14,
pavlovskayamaria@gmail.com, ovkonon@yandex.ru

Abstract: The article presents the possibilities of participation of postal services in the smart city projects, an applicability of the approach in Russian realities and abroad. The main idea is to integrate smart city information systems and the assets of postal services and units for more efficient and ubiquitous urban data collection. The integration will improve the results of a smart city management, ensure the safety of the information resources using. The article gives an analysis of international sources.

Keywords: *smart city; data-driven city; post assets; information security; protected information space*

Введение. В настоящее время наблюдается рост интереса к проектам Умных городов у Российских властей. Большинство проектов находятся на начальных этапах. Это обусловлено, помимо отсутствия достаточного финансирования и неполнотой нормативной базы, проблемами организации сбора, хранения, обработки, безопасности использования городских данных, генерируемых всеми участниками городской среды. Городские власти выстраивают отношения с ключевыми организациями, предоставляющими необходимую информацию, однако подобные взаимодействия развиты

недостаточно. Сбор данных о состоянии городской инфраструктуры в концепциях умных городов в большинстве случаев возлагается на транспортные и специализированные государственные предприятия и службы. Государственные почтовые службы, в частности Почта России, остаются вне концепций и моделей Умных городов. Между тем материально-техническая база почтовых служб большинства стран мира является серьезным материальным активом. Об использовании почтовых активов в городских умных проектах при условии обеспечения сохранности, конфиденциальности, безопасности передачи данных ведутся дискуссии и исследования [1], [2], [3], [4], [5], [6], [7], [8], [9], [10].

Среди направлений развития цифровой экономики в Российской Федерации на период до 2025 года выделено направление «Умный город» – комплекс технических решений и организационных мероприятий, направленных на достижение максимально возможного качества управления городской средой. Городская область становится умнее, когда инфраструктура городских информационно-коммуникационных технологий может обеспечить функциональные потребности Умного города и безопасность информационного обмена. Сложность городских систем и процессов информационного обмена между ними, воплощенная в архитектуре умного города, является фактором непосредственного влияния на обеспечение защиты информации информационных и телекоммуникационных систем умного города.

В большинстве развитых стран почтовые службы играют решающую роль в организации взаимодействия между всеми уровнями государственного управления и гражданами как в физической, так и в цифровой сферах. Традиционная посредническая функция почтовых операторов, географическая плотность их розничных сетей и их растущий технологический потенциал – это активы, на которые правительства полагаются для предоставления эффективных, безопасных и доступных услуг. Для организации безопасной работы с данными, требуется выделение и формализация описания информации, необходимой органам государственной власти и/или местного самоуправления для повышения эффективности принятия управленческих решений. Каждый определенный таким образом тип и источник данных предъявляет особые требования к получению, хранению, безопасности [11]. В настоящее время отсутствует рекомендованный перечень источников данных, закрепленный нормативно или представляющий собой свод лучших мировых практик. Выделенные в научной литературе и нормативно-регламентирующей документации источники, как правило, не эквивалентны по составу, качеству и количеству обрабатываемых данных. В частности, возможности государственных почтовых служб не рассматривались до недавнего времени, таким образом они остаются в стороне от вовлечения в инициативы умных городов [8].

Многие почтовые службы предоставляют услуги местных органов власти через почтовые отделения. Например, Poste Italiane предлагает службу «Sportello Amico», с помощью которой жители могут проводить различные транзакции, включая различные виды местных платежей [3]. «Почта России» также предоставляет возможности для получения государственных и муниципальных услуг, осуществления платежей, выдачи идентификаторов для доступа к электронным услугам в почтовых отделениях. Кроме того, некоторые почтовые службы, например, Норвегии и Португалии, помогают городам развивать эффективность транспортировки пассажиров с использованием экологичных транспортных средств, таких как электромобили и велосипеды, используемые курьерами [4] [5]. Swiss Post напрямую участвует в повышении мобильности в городах посредством своего сервиса PostBus – это система общественного транспорта, использующая электрические и автономные автобусы для перевозки пассажиров между городами. Swiss Post также предлагает программу проката велосипедов PubliBike [6].

Некоторые из почтовых служб начинают изучать возможность сбора данных на основе датчиков. Уже в 2014 году испанская почта Correos участвовала в разработке датчиков контроля качества воздуха для размещения на почтовых транспортных средствах [8]. Финская почтовая служба Posti начинает проводить эксперименты по использованию собранных датчиками данных для анализа дорожных условий, транспортного потока и силу беспроводного сигнала [9]. Французский почтовый оператор La Poste через свою дочернюю компанию Docapost придерживается другого подхода – организация разрабатывает платформу, на которой сенсорные данные из разнородных источников могут быть размещены с обеспечением достаточного уровня надежности и легкости доступа. В рамках такой модели La Poste играет роль брокера данных, предлагая услуги по их хранению и аналитике [10]. Почтовая служба США (USPS) признана лучшей почтовой службой в 20 крупнейших экономиках мира. Тем не менее, даже такая развитая почтовая служба, как USPS, только на начальной стадии рассмотрения возможности участия в проектах Умных городов [1].

Заключение. В исследовании был обобщен взгляд на мировой опыт вовлечения почтовых служб в социально-значимые инициативы городов. Данные исследования показали, что полностью спектр социально значимых инициатив не реализован ни в одной из рассмотренных стран. При этом сбору, хранению и анализу и тем более защите данных уделяется наименьшее внимание.

На основании анализа и данных, предложенных М. Ravnitzky в статье [12], была описана модель для описания городских данных, сбор которых возможен с использованием активов Почты России при применении датчиков, сенсоров и прочих считывающих устройств. Модель была применена к данным, сбор которых возможен с использованием активов Почты России. Показано, что посредством

использования почтовых активов сбор данных может реализовываться с большей периодичностью и охватом по сравнению с текущей ситуацией, что приведет к повышению их качества и актуальности.

СПИСОК ЛИТЕРАТУРЫ

1. The Postal Service and Cities: A "Smart" Partnership RARC Report Report Number RARC-WP-16-017 September 26, 2016 Available at: <https://www.uspsig.gov/sites/default/files/document-library-files/2016/RARC-WP-16-017.pdf>
2. OIG, "E-Government and the Postal Service: A Conduit to Help Government Meet Citizens' Needs" RARC-WP13-003, January 7, 2013. Available at: https://www.uspsig.gov/sites/default/files/document-library-files/2015/rarc-wp-13-003_0.pdf
3. Poste Italiane, "Sportello Amico". Available at: <http://www.poste.it/ufficio-postale/sportello-amico.shtml>.
4. Post and Parcel "Norway Post to add 330 Electric Vehicles to Fleet," June 18, 2015. Available at: <http://postandparcel.info/65771/news/environment-news-2/norway-post-to-add-330-electric-vehicles-to-fleet/>
5. Post and Parcel "CTT Group Invests €5m in Green Fleet," 2014. Available at: <http://postandparcel.info/60290/uncategorized/ctt-group-invests-e5m-in-green-fleet/>.
6. Swiss Post, The Pleasure of Simple Solutions: Annual Report 2015. Available at: http://annualreport.swisspost.ch/15/ar/downloads/geschaeftsbericht_konzern/en/E_Post_GB15_Geschaeftsbericht_WEB.pdf
7. The Postal Service and Cities: A "Smart" Partnership <https://www.uspsig.gov/sites/default/files/document-library-files/2016/RARC-WP-16-017.pdf>.
8. Docapost, "Digital Hub and IOT," Available at: <http://en.docapost.com/solutions/digital-hub-iot>
9. Grupo Correos, "2014 Integrated Annual Report: Innovation and Technology, Our Present, Our Future," 2014. Available at: <http://www.correos.es>, p. 36.
10. Posti, Annual Report 2015. Available at: http://annualreport2015.posti.com/filebank/1229-POSTI_Annual_Report_2015.pdf, p. 39.
11. Data-Driven City: from the concept to application-oriented decisions. 2016. Available at: https://www.pwc.ru/government-and-public-sector/assets/ddc_rus.pdf
12. Michael J. Ravnitzky, "Offering Sensor Network Services Using the Postal Delivery Vehicle Fleet" 2010, p. 2. Available at: http://www.prc.gov/sites/default/files/papers/Ravnitzky%20Postal%20Sensors%20Paper%20070910-MJR-1_1191.pdf

УДК 323

ИНФОРМАЦИОННАЯ ПОЛИТИКА РОССИИ В КОНТЕКСТЕ СТРАТЕГИИ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Попов Павел Валентинович

Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова,
Россия, Санкт-Петербург, 1-я Красноармейская ул., д. 1,
email: pa052vel@rambler.ru

Аннотация: Статья посвящена анализу «Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы».

Ключевые слова: информационное общество; информационная политика; информационное пространство.

RUSSIAN INFORMATION POLICY IN THE CONTEXT OF THE INFORMATION SOCIETY DEVELOPMENT STRATEGY

Popov Pavel Valentinovich

The Baltic State Technical University, named after D.F. Ustinov,
Russia, St. Petersburg, 1-st Krasnoarmeyskaya Street 1,
email: pa052vel@rambler.ru

Abstract: The article is devoted to the analysis of the "Strategy of information society development in Russian Federation to 2017 - 2030".

Keywords: information society; information policy; information space.

В мае 2017 г. Президентом Российской Федерации В.В. Путиным утверждена «Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы» [1].

Документ определяет приоритетный сценарий развития информационного общества, задачи по обеспечению национальных интересов в области цифровой экономики, а также цели и стратегические национальные приоритеты по формированию информационного пространства с учётом потребностей граждан и общества в получении качественных и достоверных сведений, развитию информационной и коммуникационной инфраструктуры Российской Федерации, созданию и применению российских информационных и коммуникационных технологий, обеспечению их конкурентоспособности на международном уровне, формированию новой технологической основы для развития экономики и социальной сферы.

В прежнем варианте «Стратегии развития информационного общества в РФ», которая была утверждена в феврале 2008 года говорилось о необходимости поддерживать отечественные информационные технологии, обеспечивать доступность информационных и телекоммуникационных услуг для населения, осуществлять защиту информации и т.д. Нынешний документ говорит о необходимости укреплении интеллектуального суверенитета страны в киберпространстве (т.е. отстаивании суверенного права государства «определять информационную, технологическую и

экономическую политику в национальном сегменте сети») и создании цифровой экономики. При этом чётко отмечено, что «международно-правовые механизмы» для этого не установлены.

Известно, что над новой Стратегией работали на протяжении всего 2016 года, подготовлена она была при участии рабочей группы помощника президента РФ Игоря Щёголева "Интернет + экономика". В документ вошли предложения, которые обсуждались на самом высоком уровне, в том числе на встречах президента РФ Владимира Путина с представителями IT-индустрии, а также положения Посланий главы государства Федеральному собранию и Доктрины информационной безопасности России [2].

По мнению экспертов «Ассоциации электронных коммуникаций» настоящая редакция Стратегии обладает преемственностью, комплиментарностью и непротиворечивостью по отношению к международным принципам построения информационного общества, определённым Окинавской хартией и другими международными документами [3].

Основными принципами Стратегии названы обеспечение прав граждан на доступ к информации, свободы выбора средств получения знаний, сохранение традиционных и привычных для граждан (отличных от цифровых) форм получения товаров и услуг, а также приоритет «традиционных российских духовно-нравственных ценностей» и соблюдение основанных на этих ценностях «норм поведения».

Такие приоритеты, как обеспечение конкурентоспособности России, совершенствование системы государственного управления, развитие экономической, социально-политической, культурной и духовной сфер жизни общества на основе использования информационных и телекоммуникационных технологий, также декларировались в Стратегии-2008.

В Стратегии вводятся новые для официальных документов понятия Интернета вещей, Больших данных и других составляющих Цифровой экономики, как деятельности, ключевым фактором в которой является внедрение технологии обработки данных, что позволит уменьшить затраты при производстве товаров и оказании услуг.

Уточняется понятие «критической информационной инфраструктуры» России. К её объектам относятся информационные системы, телекоммуникационные сети и автоматизированные системы управления технологическими процессами, которые используются государственными органами, а также в оборонной промышленности, в сфере здравоохранения, транспорта, связи, в кредитно-финансовой сфере, энергетике, топливной, атомной, ракетно-космической, горнодобывающей, металлургической и химической промышленности. Эту инфраструктуру необходимо защищать «с использованием государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы». Объясняется в стратегии и что такое «облачные» и «туманные вычисления», «общество знаний».

В Стратегии чётко говорится о необходимости обеспечить формирование Национальной электронной библиотеки и иных государственных информационных систем, включающих в себя объекты исторического, научного и культурного наследия народов. Кроме того, необходимо "создать условия для популяризации русской культуры и науки за рубежом, в том числе для противодействия попыткам искажения и фальсификации исторических и других фактов".

При этом в документе справедливо указывается, что усилия многих государств направлены на приоритетное развитие национальной информационной инфраструктуры в ущерб формированию и распространению знаний, что не в полной мере соответствует целям, продекларированным на Всемирной встрече на высшем уровне по вопросам информационного общества, проходившей в Женеве в 2003 году [4].

В Стратегии указывается необходимость обеспечения использования российских средств шифрования при электронном взаимодействии федеральных органов власти, замены импортного оборудования, программного обеспечения и электронной компонентной базы отечественными аналогами, а также обеспечение комплексной защиты информационной инфраструктуры РФ в том числе с использованием государственной системы обнаружения, предупреждения и ликвидации последствий атак на информационные ресурсы.

Согласно документу, в области электронной торговли для иностранных участников на российском рынке должен быть введён ряд ограничений. Поставщики товаров, программного обеспечения и услуг должны выполнять требования российского законодательства, в противном случае доступ к ним будет ограничен. В то же время иностранным предприятиям, оказывающим услуги на территории РФ будет обеспечена возможность создания собственных представительств в России.

Сотрудничество российских организаций с зарубежными компаниями в сфере цифровой экономики возможно при определённых условиях. В частности, при взаимодействии российских и иностранных организаций все данные должны храниться в базах данных и обрабатываться на серверах, размещённых на территории РФ, а платежи осуществляться через российские платёжные системы. Оказание финансовых услуг иностранными предприятиями на территории России не допускается.

Согласно указу, Правительству Российской Федерации необходимо утвердить перечень показателей реализации Стратегии и план её реализации, а также внести изменения в документы стратегического планирования.

Выводы: В новой Стратегии первостепенное внимание уделено самой информации, а не средствам накопления и передачи данных и она призвана способствовать обеспечению таких национальных интересов, как развитие человеческого потенциала; обеспечение безопасности граждан и государства; повышение роли России в мировом гуманитарном и культурном пространстве. Этот документ прежде всего указывает приоритеты, на которые могут ориентироваться органы законодательной и исполнительной власти при разработке нормативных актов по информационной политике России.

СПИСОК ЛИТЕРАТУРЫ:

1. О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы : указ Президента Российской Федерации от 09.05.2017 г. № 203 [Электронный ресурс]. URL: <http://kremlin.ru/acts/bank/41919>.
2. «Щёголев собрал первое заседание рабочей группы, занимающейся вопросами развития интернета» // ТАСС [Электронный ресурс]. URL: <http://tass.ru/politika/2660075> (дата обращения: 19.09.2017).
3. «Официальная позиция РАЭК по Стратегии развития Информационного общества в Российской Федерации 2017-2030 годы» [Электронный ресурс]. URL: <http://raec.ru/live/position/9411/> (дата обращения: 19.09.2017).
4. Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии» // Отчёт о женевском этапе всемирной встречи на высшем уровне по вопросам информационного общества, Женева, 10–12 декабря 2003 года [Электронный ресурс]. URL: <http://www.lawtrend.org/wp-content/uploads/2014/07/OTCHET-O-ZHENEVSKOM-ETAPE-VSEMIRONOJ-VSTRECHI.pdf> (дата обращения: 19.09.2017).

УДК 339.746

ИМПОРТОЗАМЕЩЕНИЕ КАК ПУТЬ ОБЕСПЕЧЕНИЯ ТЕХНОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИИ

Советов Борис Яковлевич¹, Касаткин Виктор Викторович²

¹Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», Россия, Санкт-Петербург, ул. Профессора Попова, 5,

²Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Россия, Санкт-Петербург, 14 линия, 39,
emails: bysovetov@mail.ru, v.v.kasatkin@iiias.spb.su,

Аннотация: Реализация стратегии импортозамещения в ИТ-сфере должна быть нацелена на поддержку разработки и продвижения российского программного обеспечения, результатов научной, научно-технической, инновационной деятельности и развития инновационной инфраструктуры в сфере информационно-коммуникационных технологий, что нашло отражение в требованиях к модернизации государственных образовательных стандартов высшего образования нового поколения. Обсуждается стратегия импортозамещения в области информационных технологий, реализуемая в Санкт-Петербурге на основе инновационных предложений научных, образовательных и коммерческих организаций и промышленных предприятий, представленных в Научном совете по информатизации Санкт-Петербурга.

Ключевые слова: импортозамещение, технологическая безопасность, информационные технологии.

IMPORT SUBSTITUTION AS WAY OF ENSURING TECHNOLOGICAL SAFETY OF RUSSIA

Boris Sovetov¹, Victor Kasatkin²

¹ The St. Petersburg State Electrotechnical University «LETI»,
Russia, St. Petersburg, Professor Popov str., 5,

² St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,
Russia, St. Petersburg, 14 Line, 39,
emails: bysovetov@mail.ru, v.v.kasatkin@iiias.spb.su,

Abstract: Implementation of strategy of import substitution in the IT sphere shall be aimed at support of development and promotion of the Russian software, results of scientific, scientific and technical, innovative activities and development of innovative infrastructure in the sphere of information and communication technologies that found reflection in requirements to upgrade of the state educational standards of the higher education of new generation. The strategy of import substitution in the field of information technologies realized in St. Petersburg on the basis of innovative sentences of the scientific, educational and commercial organizations and the industrial enterprises provided in Scientific council on informatization of St. Petersburg is discussed.

Keywords: import substitution, technological safety, information technologies.

В истории России проблема импортозамещения вставала в середине XIX века, когда спрос на российский товар прекратился, ряд стран отказался от ввоза в Россию некоторых сырьевых продуктов,

а импорт готового иностранного товара в Россию усилился. В ряде работ того времени было установлено, что необходимо обеспечение защитных мер в ситуации, когда отечественный производитель не имеет достаточного объема инвестиций для расширения своего производства и Российская промышленность сталкивается с демпингом иностранных производителей. В этот период были успешно реализованы проекты импортозамещения в условиях протекционистских мер со стороны иностранных государств в таких областях как добыча российской нефти, производство керосина, зеркал, металла и зерна.

Ситуация повторилась в конце XX века, а также в новейшей истории, когда в 2012 году в полном объеме встала проблема экономической безопасности России и исключительно своевременной мерой оказалась разработка Государственной программы развития сельского хозяйства и регулирования рынков сельскохозяйственной продукции, сырья и продовольствия на 2013–2020 годы, принятой постановлением Правительства РФ от 14.07.2012 № 717, ход и результаты реализации которой были утверждены в 2016 году [1]. Продолжением реализации политики импортозамещения явилась Государственная программа Российской Федерации «Развитие промышленности и повышение ее конкурентоспособности», утвержденная распоряжением Правительства РФ от 27.12.2012 № 2539-р [2]. Были определены перспективные направления развития импортозамещения до 2020 года, среди которых в качестве приоритетных были определены сельское хозяйство, информационные технологии, машиностроение и т.д. Особое внимание было уделено информационным технологиям в связи с подготовкой и принятием 24.12.2017 постановления Правительства РФ № 57 «О создании Российского фонда развития информационных технологий» [3]. Целью создания фонда является поддержка разработки и продвижения российского программного обеспечения, поддержка научной, научно-технической, инновационной деятельности и развития инновационной инфраструктуры в сфере информационно-коммуникационных технологий, что нашло отражение в требованиях к модернизации государственных образовательных стандартов высшего образования нового поколения.

В докладе обсуждается стратегия импортозамещения в области информационных технологий, реализуемая в Санкт-Петербурге на основе инновационных предложений научных, образовательных и коммерческих организаций и промышленных предприятий, представленных в Научном совете по информатизации Санкт-Петербурга.

СПИСОК ЛИТЕРАТУРЫ

1. Об утверждении национального доклада о ходе и результатах реализации в 2016 году Государственной программы развития сельского хозяйства и регулирования рынков сельскохозяйственной продукции, сырья и продовольствия на 2013–2020 годы // <http://government.ru/docs/27573/> 26.09.2017.
2. Государственная программа «Развитие промышленности и повышение ее конкурентоспособности» // <http://www.gosprog.ru/gosprog-016/> 26.09.2017.
3. Постановление Правительства РФ от 24.01.2017 № 57 «О создании Российского фонда развития информационных технологий» // <http://government.ru/docs/26221/> 26.09.2017.

УДК 378.046.4

МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ФОРМИРОВАНИЯ СИСТЕМЫ РАСПРЕДЕЛЕННЫХ СИТУАЦИОННЫХ ЦЕНТРОВ

Соколов Борис Владимирович, Салухов Владимир Иванович
Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия, 39,
email: spiiras@iias.spb.su

Аннотация: Проведен краткий анализ формирования системы распределенных ситуационных центров (СРСЦ), центров компетенций, показана потребность и особенности подготовки специалистов, отвечающих требованиям цифровой экономики. Сформулированы общие подходы для успешной интеграции инновационных технологий в решение разнообразных социально-экономических задач.

Ключевые слова: цифровая экономика, информационное общество, ситуационный центр, центр компетенций

METHODOLOGICAL ASPECTS OF FORMATION OF SYSTEM OF DISTRIBUTED SITUATIONAL CENTERS

Sokolov Boris, Salukhov Vladimir
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,
Russia, St. Petersburg, 14 Line, 39,
email: spiiras@iias.spb.su

Abstract: A brief analysis of the formation of a system of distributed situational centers (SRSC), centers of competence, shows the need and features of preparation of specialists, meeting the requirements of the digital economy. Formulated common approaches to the successful integration of innovative technologies in the solution of various socio-economic problems.

Keywords: *digital economy, information society, the situation centre, the competence centre*

Введение. В настоящее время информационные технологии и накопленные человеком знания все в большей мере становятся стратегическим ресурсом общества, его движущей производительной силой. Индустриальный этап развития общества постепенно переходит к новой эволюционной фазе и соответствующей общественно-экономической формации – информационному обществу. Оно предполагает наиболее эффективное и динамичное развитие на основе максимально полного использования имеющихся информационных ресурсов и средств их обработки.

Информационное общество создает объективные предпосылки перехода к цифровой экономике, как наиболее эффективной и управляемой форме совершенствования производственной и социальной сферы деятельности человека. Ведущее место в цифровой экономике отводится новым информационным и коммуникационным технологиям (ИКТ), которые уже фактически являются технологиями общего назначения, также как технологии, например, производства тепла и электроэнергии. Следует ожидать, что в процессе развития цифрового производства и в целом цифровой экономики получат широкое распространение самые разнообразные классы киберфизических систем (КФС). Не исключено, что их повсеместное внедрение приведет к гораздо большим изменениям в обществе, чем появление компьютеров и Интернета.

В перспективных КФС, наряду с функциями позиционирования, контроля и диагностики также будут реализованы функции автоматического составления отчетов о состоянии соответствующей подсистемы контролируемого оборудования, в том числе, данных о всех возникающих неисправностях; об остатке ресурса изнашиваемых деталей; о ресурсе расходных материалов; загрузке оборудования и режиме его эксплуатации [1,2]. Указанные возможности открывают широчайшие перспективы по автоматизации и интеллектуализации как самого цифрового производства продукции, так и ее обслуживания и эксплуатации во время послепродажного функционирования. Ключевым элементом предлагаемого электронного обслуживания (e-maintenance) будет являться базирующееся на Web-технологиях дистанционное администрирование, мониторинг, тестирование, диагностика, прогнозирование состояния эксплуатируемых программных и технических средств, реконфигурация их структур, в случае возникновения аварийных и нештатных ситуаций и отсутствии необходимых резервов.

При безусловной важности всех этих инновационных направлений, необходимо проработанное с учетом специфики нашей страны определение как стратегических, так и текущих (тактических) целей и задач, стоящих перед нашей экономикой и государством в целом. Важная роль в решении перечисленных проблем отводится формируемой в настоящее время системе распределенных ситуационных центров (СРЦ), работающих по единому регламенту взаимодействия, которая руководством страны рассматривается в качестве устойчивого фундамента долгосрочного совершенствования системы государственного, отраслевого, муниципального управления и корпоративного управления. Процессы разработки, совершенствования и дальнейшего развития СРЦ требуют реализации комплексных междисциплинарных интеграционных подходов, базирующихся на соответствующей регламентированной проектной деятельности, которую следует осуществлять согласно отечественному законодательству в Центрах компетенций федерального, регионального и муниципального уровнях государственного управления [1].

Создаваемые ситуационные центры и центры компетенции призваны минимизировать и упредить потенциальные риски самой разнообразной природы. Вместе с тем, многолетний опыт их эксплуатации и применения позволил выделить целый ряд недостатков и недоработок. Среди них можно выделить причины, имеющие методологический характер, модельно-алгоритмические, технологические и организационные.

Методология формирования СРЦ. Методологический характер существующих недостатков обусловлен главным образом тем, что при разработке СЦ зачастую игнорируются требования системного подхода к проектированию сложных организационно-технических комплексов. Это, в частности, проявляется в осуществлении автоматизации лишь отдельных этапов процесса сбора и обработки информации или в решении на ЭВМ некоторых расчётных задач без рассмотрения проблемы автоматизации процессов управления в целом. Модельно-алгоритмические связаны с недостаточной проработкой фундаментальной теоретической базы. Технологические причины во многом определяются существующими подходами к проектированию и созданию сложных организационно-технических систем, когда большое число специалистов практически вручную формируют облик будущей перспективной системы.

Среди причин организационного характера следует указать то, что многие руководители организаций, где осуществлялась разработка и внедрение СЦ осознанно или неосознанно их структуру и функции подгоняли под существующую организационно-технологическую структуру, говоря другими словами, – автоматизировался непроизводительный труд.

Перечисленные причины во многом обуславливают основные требования к навыкам и компетенциям специалистов, пригодных для плодотворной работы в системе распределенных ситуационных центров и центрах компетенций федерального, регионального и муниципального уровнях государственного управления.

Учитывая высокие темпы развития процессов цифровой экономики, навыки характеризуются динамикой своего жизненного цикла, привязанного к жизненному циклу рабочего места, что отличает их от традиционных компетенций, сформулированных в действующих образовательных стандартах. Поэтому формирование конкретных навыков должно осуществляться, во-первых, в возможно сжатые сроки пока они еще актуальны, и, во-вторых, с учетом того, что они смогут адаптироваться к новым условиям и развиваться.

Совершенствование и дальнейшее развитие СРСЦ и центров компетенций неизбежно потребуют реализации комплексных междисциплинарных интеграционных подходов от специалистов и персонала этих центров [2-3]. Специалисты центров должны быть готовы к методологическому разнообразию инструментально-моделирующих средств, необходимости использования широкого спектра аппаратно-программных средств. Существующее методологическое разнообразие позволяет разрабатывать и проигрывать различные варианты развития ситуаций и выбирать наиболее предпочтительные решения. Чаще всего, они характеризуются следующими особенностями [3]:

- многокритериальность принятия решений;
- итерационный характер подготовки и принятия решений;
- необходимость визуализации информации;
- коллективный характер пользовательского интерфейса.

Сложность, многоаспектность, междисциплинарность требуемых навыков для персонала СЦ и центров компетенций, а также крайне жесткие сроки для обучения и переподготовки специалистов вынуждают находить инновационные образовательные технологии, широкое использование сетевых методов обучения, выбор гибких шаблонов построения учебных программ, обеспечивающих широкие возможности для их диверсификации, а также многообразные формы дополнительного образования и самообразования, плюс методы и средства поддержки контрольно-измерительных и аттестационных процессов.

Специалисты центров должны быть готовы к методологическому разнообразию инструментально-моделирующих средств, необходимости использования широкого спектра аппаратно-программных средств от специализированных баз данных, киосков данных до моделей различных типов. При подготовке и принятии управленческих решений потребуются навыки использования следующих методов: информационный поиск в базах данных, интеллектуальный анализ данных, поиск знаний в базах знаний и данных, имитационное моделирование, нейронные сети и экспертные системы, когнитивное моделирование, информационно-аналитические системы и др.

Существующее методологическое разнообразие позволяет разрабатывать и проигрывать различные варианты развития ситуаций и выбирать наиболее предпочтительные решения. Чаще всего, они характеризуются следующими особенностями [4]:

– Многокритериальность принятия решений. Практические задачи, которые решаются в СРСЦ, являются многокритериальными. Все используемые критерии (или значительная их часть) нечисловые, в частности имеют вербальные (словесные) шкальные оценки. Методы выявления относительной важности критериев, свертки критериев должны учитывать реальные возможности человеческого мозга по представлению и переработке информации при сравнении, ранжировании вариантов решений и выбора наиболее предпочтительного.

– Итерационный характер подготовки и принятия решений. В процессе подготовки и принятия решений в ситуационном центре (СЦ) можно выделить следующие этапы: мониторинг предметных областей; формирование «дерева» целей; обоснование множества критериев, включая методики их свертки; генерация альтернативных вариантов достижения целей; оценка вариантов по системе критериев; классификация вариантов решений по отдельным критериям или по обобщенному сводному критерию; обоснование и выбор рационального (наиболее эффективного) варианта решения; доведение принятых решений до исполнителей и контроль исполнения.

– Необходимость визуализации информации. Значительные объемы разнотипных данных, поступающих в СЦ, делают необходимым преобразование этой информации в некоторое пространственное представление, которое должно сохранять его информационные характеристики. В этой ситуации только визуализация информации позволяет повысить качество оценки и выбора решений. Лицо, принимающее решение (ЛПР) и эксперты должны иметь возможность работать как с видеоматериалами, картографическими, анимационными, имитационными моделями реальных объектов, так и с графиками, таблицами, многомерными диаграммами, мультимедийными продуктами.

– Коллективный характер пользовательского интерфейса. Экраны коллективного пользования СЦ становятся ядром пользовательского интерфейса, обстановка на экранах технологически настраивается на мгновенную реакцию ЛПР. Чтобы пользовательский интерфейс мог обладать указанными свойствами, создают соответствующие архитектуры студийных технологий и средств отображения.

Методологическое разнообразие в формировании и становлении системы распределенных ситуационных центров определяется еще и тем, что в структуре центров компетенции предусмотрено подразделение с функциями координации образовательной деятельности. Такими функциями являются:

– подготовка и переподготовка специалистов по программам дополнительного образования и программам повышения квалификации в области комплексной обработки, интеграции и анализа

разнотипных данных информации и знаний о социально-экономической, общественно-политической сферах, в области комплексного упреждающего моделирования и принятия управленческих решений в кризисных ситуациях, связанных с природными катаклизмами, техногенными катастрофами, социально-экономическими и военно-политическими кризисами;

– координация работ, проводимых в региональных высших учебных заведениях по подготовке специалистов для Регионального ситуационного центра по программам высшего профессионального образования (бакалавриат и программы магистратуры);

– организация и проведение научно-практических конференций, семинаров, сборов и мастер-классов с представителями региональных органов государственного и муниципального управления для их ознакомления с новейшими достижениями в области цифровой экономики и управления.

Существующий опыт, несомненно, заслуживает внимания специалистов, но его не следует расценивать как исчерпывающий. Очевидно, что только коллективные, систематические и целенаправленные усилия всех заинтересованных сторон смогут уверенно продвигать подготовку специалистов в области цифровой экономики

Закключение. В настоящее время подготовку специалистов, пригодных для успешной работы в СРСЦ и центрах компетенций, целесообразно строить на базе научно-образовательных центров, создающих основу механизма широкого внедрения инновационных технологий решения социально-экономических задач, позволяет на практике реализовать идею интеграции науки, образования и производства, достичь минимальных затрат времени на организацию образовательного процесса и использовать все преимущества этой интеграции в такой высокотехнологичной и наукоемкой сфере, как цифровая экономика.

Исследования, выполненные по данной тематике, проводились при финансовой поддержке ведущих университетов Российской Федерации: СПбГПУ (мероприятие 6.1.1), ИТМО (субсидия 074–U01), Программы НТС Союзного государства «Мониторинг-СГ» (проект 1.4.1-1), грантов РФФИ №№15-07-08391, 15-08-08459, 15-07-01230, 16-07-00779, 16-08-00510, 16-08-01277, гранта РНФ №16-19-00199, Программы фундаментальных исследований ОНИТ РАН (проект №2.11).

СПИСОК ЛИТЕРАТУРЫ

1. Распоряжение Правительства РФ от 15.10.2016 №2165-р «Об утверждении плана первоочередных мероприятий по организации проектной деятельности в Правительстве Российской Федерации на 2016 и 2017 годы».
2. Салухов В.И., Шевченко О.И. Моделирование и управление рисками при проектировании и строительстве сетей связи/ Проблемы анализа риска, 2014. Т. 11. № 3. С. 48-67.
3. Ильин Н.И., Демидов Н.Н., Новикова Е.В. Ситуационные центры. Опыт, состояние, тенденции развития/ М.: МедиаПресс, 2011 – 336с.
4. Салухов В.И., Соколов Б.В. Образовательная компонента в формировании и становлении распределенных ситуационных центров и центров компетенции/ Стратегические приоритеты №2 (14) 2017, С 138-148

УДК 378.147

ОСОБЕННОСТИ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕВЕРО-ЗАПАДНОМ ФЕДЕРАЛЬНОМ ОКРУГЕ

Сторожик Виктор Сергеевич
Управление ФСТЭК России по Северо-Западному федеральному округу,
Россия, Санкт-Петербург,
email: szfo@fstec.ru

Аннотация: В Доктрине информационной безопасности Российской Федерации определены стратегические цели и основные направления обеспечения информационной безопасности государства с учетом его стратегических национальных приоритетов. К основным направлениям обеспечения информационной безопасности в области науки, технологий и образования в документе отнесено «развитие кадрового потенциала в области информационной безопасности и применения информационных технологий». Обсуждаются вопросы развития кадрового обеспечения безопасности в области информационной безопасности и координации кадрового обеспечения безопасности в информационной сфере в Северо-Западном федеральном округе.

Ключевые слова: информационная система, кадровое обеспечение в области информационной безопасности.

FEATURES OF TRAINING IN THE FIELD OF INFORMATION SECURITY IN THE NORTH-WEST FEDERAL DISTRICT

Victor Storozhik
Department of FSTEC of Russia Northwestern Federal District,
Russia, Saint-Petersburg,
email: szfo@fstec.ru

Abstract: In the Doctrine of information security of the Russian Federation strategic objectives and the main directions of ensuring information security of the state taking into account his strategic national priorities

are defined. "development of personnel potential in the field of information security and use of information technologies" is referred to the main directions of ensuring information security in the field of science, technologies and education in the document. Issues of development of staffing in the field of information security and coordination of staffing of safety in the information sphere in the Northwestern Federal District are discussed.

Keywords: *information system, staffing in the field of information security.*

В Концепции внешней политики Российской Федерации, утвержденной Указом Президента Российской Федерации от 30 ноября 2016 г. № 640 сформулирована позиция государства по отношению к использованию информационно-коммуникационных технологий в современном мире. В документе отмечено, что Российская Федерация принимает необходимые меры для обеспечения национальной и международной информационной безопасности, и противодействия угрозам государственной, экономической и общественной безопасности, исходящим из информационного пространства [1].

В Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, определены стратегические цели и основные направления обеспечения информационной безопасности государства с учетом его стратегических национальных приоритетов. При этом к основным направлениям обеспечения информационной безопасности в области науки, технологий и образования в документе отнесено «развитие кадрового потенциала в области информационной безопасности и применения информационных технологий» [2].

В настоящее время эта задача решается в рамках функционирующей системы подготовки, переподготовки и повышения квалификации кадров в указанной сфере деятельности [3] - [10].

Комплексность и взаимосвязанность задач по совершенствованию кадрового обеспечения безопасности в информационной сфере требует также принятия дополнительных мер нормативно-правового, организационного и методического характера. В рамках реализации государственной политики по развитию кадрового потенциала в области обеспечения информационной безопасности разработана Концепция развития кадрового обеспечения в области информационной безопасности в Российской Федерации на долгосрочную перспективу, определен порядок повышения квалификации специалистов по защите информации, осуществляется разработка федеральных государственных образовательных стандартов в области информационной безопасности и комплекса мер для закрепления специалистов по информационной безопасности в органах государственной власти и организациях. В настоящее время дополнительное профессиональное образование осуществляется на базе высшего [11] - [13] или среднего профессионального образования [14], [15] и направлено на непрерывное профессиональное развитие специалистов в области информационной безопасности.

Дополнительное профессиональное образование в области информационной безопасности включает в себя профессиональную переподготовку и повышение квалификации [16], [17].

В рамках реализации Концепции развития кадрового обеспечения в области информационной безопасности в Российской Федерации на долгосрочную перспективу в Федеральной службе по техническому и экспортному контролю (ФСТЭК России) сформирована группа по координации кадрового обеспечения безопасности в информационной сфере, а при Управлении ФСТЭК России по Северо-Западному федеральному округу организована деятельность координационного методического Совета по вопросам подготовки специалистов в области информационной безопасности.

Выводы. 1. Развитие кадрового потенциала в области информационной безопасности и применения информационных технологий является одним из определяющих направлений реализации государственной политики обеспечения информационной безопасности в области науки, технологий и образования.

2. В рамках реализации Концепции развития кадрового обеспечения в области информационной безопасности в Российской Федерации на долгосрочную перспективу ФСТЭК России реализуется комплекс дополнительных мер по методическому обеспечению подготовки, переподготовки и повышения квалификации кадров.

3. При решении задач по формированию прогноза баланса трудовых ресурсов и прогноза подготовки кадров по информационной безопасности ФСТЭК России выполняет полномочия центра ответственности, осуществляющего подготовку и представление в Минобрнауки России предложений о контрольных цифрах приема по укрупненной группе направлений подготовки «Информационная безопасность» для обучения по образовательным программам бакалавриата, специалитета и магистратуры за счёт бюджетных ассигнований федерального бюджета.

4. В Северо-Западном федеральном округе основные направления государственной политики по подготовке, профессиональной переподготовке и повышению квалификации специалистов осуществляются путем реализации решений координационного методического Совета по вопросам подготовки специалистов в области информационной безопасности при Управлении ФСТЭК России по СЗФО, которые принимаются с участием представителей ведущих образовательных организаций округа.

СПИСОК ЛИТЕРАТУРЫ

1. Концепция внешней политики Российской Федерации (утв. Указом Президента Российской Федерации от 30 ноября 2016 г. № 640).
2. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646).
3. Федеральный закон «Об образовании в Российской Федерации» от 29 декабря 2012 г. № 273-ФЗ.
4. Федеральный закон «О государственной и гражданской службе Российской Федерации» от 27 июля 2004 г. № 79 (редакция от 05.10.2015 № 285-ФЗ).
5. Постановление Правительства Российской Федерации «Об организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса» от 6 мая 2016 г. № 399.
6. Положение о лицензировании деятельности по технической защите конфиденциальной информации (утв. постановлением Правительства Российской Федерации от 3 февраля 2012 г. №79).
7. Постановление Правительства Российской Федерации «О внесении изменений в некоторые акты Правительства Российской Федерации по вопросам лицензирования отдельных видов деятельности» от 15 июня 2016 г. № 541.
8. Указ Президента Российской Федерации «Вопросы Федеральной службы по техническому и экспортному контролю» от 16 августа 2004 г. № 1085 (с изменениями и дополнениями от 20.01.2015 № 26-ФЗ).
9. Постановление Правительства Российской Федерации «Об утверждении Правил установления организациям, осуществляющим образовательную деятельность, контрольных цифр приема по профессиям, специальностям и направлениям подготовки и (или) укрупненным группам профессий, специальностей и направлений подготовки для обучения по образовательным программам среднего профессионального и высшего образования за счет бюджетных ассигнований федерального бюджета, а также о признании утратившими силу некоторых актов Правительства Российской Федерации» от 27 марта 2015 г. № 285 (редакция от 02.11.2015).
10. Постановление Правительства Российской Федерации «О порядке заключения и расторжения договора о целевом приеме и договора о целевом обучении» от 27 ноября 2013 г. № 1076.
11. Приказ Министерства образования и науки Российской Федерации «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры» от 19 декабря 2013 г. №1367.
12. Приказ Министерства образования и науки Российской Федерации «Об утверждении перечней специальностей и направлений подготовки высшего образования, применяемых при реализации образовательных программ высшего образования, содержащих сведения, составляющие государственную тайну или служебную информацию ограниченного распространения» от 12 сентября 2013 г. №1060.
13. Приказ Министерства образования и науки Российской Федерации «Об утверждении перечней специальностей и направлений подготовки высшего образования» от 12 сентября 2013 г. №1061.
14. Приказ Министерства образования и науки Российской Федерации «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования» от 14 июня 2013 г. №464.
15. Приказ Министерства образования и науки Российской Федерации «Об утверждении перечней профессий и специальностей среднего профессионального образования» от 29 октября 2013 г. №1199.
16. Приказ Министерства образования и науки Российской Федерации «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам» от 1 июля 2013 г. №499.
17. Приказ Министерства образования и науки Российской Федерации «Об утверждении Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности» от 5 декабря 2013 г. №1310.

УДК 681.3

**ИНФОРМАЦИЯ КАК ВАЖНЕЙШИЙ РЕСУРС ДЛЯ ПРИНЯТИЯ ЭФФЕКТИВНЫХ
УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ**

Тарашнина Светлана Ивановна
Санкт-Петербургский информационно-аналитический центр,
Россия, Санкт-Петербург, Транспортный пер., 6,
Санкт-Петербургский государственный университет,
Россия, Санкт-Петербург, Университетская наб., 7/9,
email: tarashnina@gmail.com

Аннотация: В статье отмечена значимость информации и других составляющих процесса информатизации при принятии управленческих решений. Приведено несколько методов получения сведений о социально-экономическом развитии региона (на примере Санкт-Петербурга). Обозначена необходимость хранения и накопления данных, использования информации для глубокой аналитики и выявления скрытых закономерностей как в целях оперативного реагирования, так и долгосрочного планирования.

Ключевые слова: информационно-экономическая безопасность, эффективность управленческих решений, информационно-аналитическая работа.

**INFORMATION AS THE MOST IMPORTANT RESOURCE FOR MAKING EFFECTIVE
MANAGERIAL DECISIONS**

Tarashnina Svetlana
Saint-Petersburg Information and Analytical Centre,
Russia, Saint-Petersburg, Transportnyi per., 6,
Saint-Petersburg State University,
Russia, Saint-Petersburg, Universitetskaya nab., 7/9,
email: tarashnina@gmail.com

Abstract: The article highlights the importance of information and other components of the informatization in making managerial decisions. Several methods for obtaining information on the socio-economic development of the region (on the example of St. Petersburg) are given. The paper notes the need for storage and accumulation of information to perform in-depth analysis and identify hidden patterns for a rapid response and a long-term planning.

Keywords: *digitalization, information and economic threats, especially the implementation.*

В современных условиях процесс успешного функционирования и экономического развития региона (страны) зависит от принятия качественных и своевременных управленческих решений, которые формируются на основе всестороннего анализа информации, поступающей как из внутренней, так и из внешней среды. В последние десятилетия, в связи с развитием информационных технологий и всеобщей информатизацией социально-экономических отношений, возросло значение информации как для экономики, так и для общества в целом. Информация стала одним из важных управленческих ресурсов, наравне с человеческими, финансовыми и материальными ресурсами. Ее накопление и потребление заложено в основу планомерного развития экономики.

Эффективное управление невозможно без информационного обеспечения, необходимого для принятия решений по важнейшим направлениям и сферам деятельности органов государственной власти. Значимым аспектом в этом процессе является поиск данных различной природы о социально-экономическом развитии региона, дальнейшее их накопление, хранение и грамотное использование.

В реальной жизни информация о любом объекте (явлении) в полном объеме в отдельно взятый момент времени не существует. Она носит отрывочный разрозненный и противоречивый характер. Поэтому сущность информационно-аналитической работы заключается в создании на базе собираемых сведений и материалов обобщенной, качественно новой информации об объектах (явлениях) наблюдения [1].

Другой важной составляющей информационно-аналитической работы является наличие аналитических программных продуктов, позволяющих выявлять скрытые закономерности в данных, выполнять анализ больших данных, а также оперативно предоставлять результаты решения прогнозно-аналитических задач.

В Санкт-Петербурге функционирует государственная информационная система «Интегрированная система информационно-аналитического обеспечения исполнительных органов государственной власти Санкт-Петербурга» (далее ИС ИАО). Система подключена к сети единой мультисервисной телекоммуникационной сети исполнительных органов государственной власти Санкт-Петербурга (ЕМТС) и обеспечивает информационно-аналитическую поддержку всем специалистам и руководителям ИОГВ Санкт-Петербурга. Информационным базисом ИС ИАО является Хранилище данных, которое систематически пополняется информацией из различных источников: ведомственная статистика, государственная федеральная и региональная статистика, социологические опросы населения, данные мониторинга ГЛОНАСС и др.

Каким образом собирается необходимая для понимания и решения возникающих городских проблем информация? Основным источником данных является государственная и ведомственная статистика. Данные собираются путем проведения мониторингов по различным сферам социально-экономического развития Санкт-Петербурга. Однако для глубокого анализа ситуации необходима дополнительная информация о происходящих в городе процессах.

Учитывая тот факт, что определенные сферы жизнедеятельности не описываются статистическими показателями, важным источником информации является само население. На средствах ИС ИАО проводятся социологические опросы населения Санкт-Петербурга, целевые опросы отдельных групп населения, экспертные опросы, фокус-группы. К числу анализируемых аспектов относятся удовлетворенность населения работой жилищно-коммунальных служб, общественного транспорта, качеством школьного образования, медицинским обслуживанием в рамках ОМС, благоустройством и озеленением, работой правоохранительных органов.

Проводятся мониторинги межнациональных отношений, распространенности здорового образа жизни населения (табакокурение, употребление алкоголя, обеспеченность населения внутривидовыми спортивными площадками, доступность медицинской помощи), положения инвалидов, пенсионеров, семей с детьми, оценки населения по преступности, безопасности, коррупции и др.

Альтернативным способом получения данных об экономическом развитии региона является использование технологии ГЛОНАСС и информационно-навигационных систем для мониторинга деятельности государственных служб, обеспечивающих работу городского пассажирского транспорта, организаций жилищно-коммунального хозяйства, скорой медицинской помощи, грузоперевозчиков. Фиксируются нарушения транспортной работы (расписаний перевозок, отклонения от маршрута, простои, длительность доставки пациента в больницу, происшествия с участием специальных транспортных средств и др.).

Полученная информация анализируется методами корреляционного и регрессионного анализа, кластерного анализа и другими методами интеллектуальной обработки данных (Data Mining). Анализ

результатов позволяет отслеживать проблемные зоны и оперативно реагировать на происходящие в городе системные нарушения, предпринимая меры превентивного характера.

Несмотря на проводимую аналитическую работу, вопрос информационно-экономической безопасности региона на сегодняшний день стоит достаточно остро. Сущность информационно-экономических угроз заключается в использовании информации циркулирующей или создаваемой на объекте микро (личность, хозяйствующий субъект), мезо (регион, отрасль, социальная группа) и макро (страна, группа стран) уровня или вокруг него для нанесения экономического ущерба этому объекту [2].

Уничтожение или повреждение информации может привести к серьезным проблемам в управлении регионом. Необходимо разрабатывать и внедрять специальные системы защиты информации, модели предотвращения информационно-экономических угроз с целью обеспечить состояние защищенности региона и его информационной среды от негативного влияния дестабилизирующих факторов, что гарантируют стабильное и прогрессивное развитие региона [3].

В работе предлагается для обеспечения информационно-экономической безопасности использовать комплексный интеграционный подход к вопросам сбора, хранения, накопления и анализа информации в интересах органов государственной власти. Интеграция ресурсов, например, на основе единой платформы Центра обработки данных (как это сделано в Санкт-Петербурге) способствует повышению степени защищенности информационных ресурсов. Современные технологии добычи информации и аналитической обработки целесообразно реализовывать на базе государственных информационно-аналитических центров.

СПИСОК ЛИТЕРАТУРЫ

1. Левкин И.М. Теория и практика информационно-аналитической работы. НИЦ (г. Курск) в/ч 11135, 2013. – 417 с.
2. Технологические аспекты информационно-экономической безопасности / В.В. Касаткин, А.М. Колбанёв, И.Л. Коршунов, И.М. Левкин, С.Ю. Микадзе. – СПб.: Изд-во СПбГЭУ, 2016. – 193 с.
3. Тимаев Р.А. Понятие информационно-экономической безопасности предприятия / Р.А. Тимаев // Культура народов Причерноморья. 2014. — No 278. — С. 64— 69.

УДК 004:005.21

ПРОГРАММА «ЦИФРОВАЯ ЭКОНОМИКА» В КОНТЕКСТЕ РАЗВИТИЯ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ИНФОРМАТИЗАЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Чугунов Андрей Владимирович

Санкт-Петербургский национальный исследовательский университет

информационных технологий, механики и оптики,
Россия, Санкт-Петербург, В.О., Биржевая линия, 14.

email: chugunov@corp.ifmo.ru

Аннотация: В докладе представлен анализ развития государственных программ развития информатизации в контексте нового этапа, связанного с принятием Программы «Цифровая экономика Российской Федерации» и соответствующей Дорожной карты. Рассмотрены новации и организационные механизмы, призванные стимулировать процессы цифровых трансформаций в основных сферах экономики и государственного управления, в том числе меры по обеспечению организационной и правовой защиты личности, бизнеса и государственных интересов при взаимодействии в новых условиях.

Ключевые слова: государственная политика информатизации; цифровая экономика, информационная безопасность; блокчейн-технологии.

DIGITAL ECONOMY PROGRAM: RUSSIAN FEDERATION INFORMATIZATION POLICY CONTEXT

Chugunov Andrei

ITMO University

Russia, St. Petersburg, Birzhevaya linia, 14

email: chugunov@corp.ifmo.ru

Abstract: The paper presents an analysis of informatization state programs' development in the context of a new stage connected with the adoption of the "Digital Economy in the Russian Federation" Program and its Roadmap. Novations and organizational mechanisms designed to stimulate the processes of digital transformations in the main spheres of the economy and public administration, including the organizational and legal protection of personal, business and state interests in interaction under new conditions, are considered.

Keywords: information policy; digital economy, information security; blockchain technology.

Введение. В конце 2016 г. в Российской Федерации была актуализирована задача развития цифровой экономики. В своем обращении к Федеральному Собранию Президент России Владимир Путин заявил о необходимости в собственных передовых разработках и научных решениях, направленных на развитие экономики и социальных отраслей. Было сказано о необходимости

сосредоточиться на так называемых «сквозных» технологиях - цифровых технологиях, с мощным технологическим потенциалом, которые сегодня определяют облик всех сфер жизни [16]. Так же президент предложил запустить масштабную системную программу развития экономики нового технологического поколения, так называемой «цифровой экономики», отметив, что этот вопрос является вопросом национальной безопасности и технологической независимости России. Именно с этими заявлениями экспертное сообщество связывает начало проработки государственного курса на развитие цифровой экономики в России [2]. Программа «Цифровая экономика» была утверждена распоряжением Правительства РФ в июле 2017 г. [3]

Программа была разработана Минкомсвязью России во исполнение перечня поручений Президента России по реализации Послания Федеральному Собранию [4]. Для разработки программы была сформирована рабочая группа, состоящая из подгрупп по базовым направлениям. Программой определены цели, задачи, направления и сроки реализации основных мер государственной политики по созданию необходимых условий для развития в России цифровой экономики, в которой данные в цифровом виде являются ключевым фактором производства во всех сферах социально-экономической деятельности, что является необходимым условием повышения конкурентоспособности страны, качества жизни граждан, обеспечения экономического роста и национального суверенитета. Определены пять базовых направлений развития цифровой экономики в России на период до 2024 года: нормативное регулирование, кадры и образование, формирование исследовательских компетенций и технических заделов, информационная инфраструктура и информационная безопасность. Цифровая экономика была включена в перечень основных направлений стратегического развития России до 2025 года по итогам заседания Совета по стратегическому развитию и приоритетным проектам при Президенте России, которое состоялось в июле 2017 г. В обзорной публикации РБК, посвященной данному вопросу обобщаются основные показатели, которые необходимо достичь в результате реализации программы [5]. Согласно документу, в России к 2024 году должны работать не менее десяти конкурентоспособных на мировом рынке высокотехнологичных компаний и десяти индустриальных цифровых платформ, а именно цифровые медицинские учреждения, «умные города» и другие.

К 2024 году, согласно программе, в России должно работать не менее 500 средних и малых предприятий «в сфере цифровых технологий». Вузы к данному сроку должны будут ежегодно выпускать не менее 120 тыс. IT-специалистов, а в сфере высоких технологий должно быть реализовано не менее 30 исследовательских проектов с объемом бюджета 100 млн руб. Для работающих в данной сфере компаний планируется ввести «особый» правовой режим. Уделено внимание и теме импортозамещения, в частности, доля иностранного оборудования, закупаемого госорганами, должна снизиться до 50%, а программного обеспечения - до 10%. В каждом федеральном округе должны будут работать Центры обработки данных (ЦОД), которые будут поступать в госорганы от граждан и организаций на территории России. Кроме того, программа предусматривает развитие интернет-безопасности, в частности, создание национальной системы фильтрации интернет-трафика для ограничения доступа несовершеннолетних в Сеть.

Необходимо отметить, что программа «Цифровая экономика» была утверждена параллельно с действующей государственной программой «Информационное общество», что вызывает серьезные проблемы с ресурсным обеспечением новой программы. Не исключен вариант реформирования двух программ, либо новая программа останется некой политической декларацией не подтвержденной финансовыми ресурсами.

Предварительная версия программы «Цифровая экономика» содержала «отраслевые» разделы (здравоохранение, образование, госуправление) и раздел, посвященный созданию «умных городов», однако из финальной версии программы они были изъяты. Можно предположить, что это связано именно с нерешенностью вопроса о бюджетировании всей программы. При этом в тексте программы, утвержденной распоряжением Правительства указано, что «реализация отдельных направлений по отраслям экономики (сферам деятельности), в первую очередь в сфере здравоохранения, создания «умных городов» и государственного управления, включая контрольно-надзорную деятельность, будет осуществляться на основе дополнения настоящей Программы соответствующими разделами, а также разработки реализации соответствующих планов мероприятий («дорожный карт»), сформированных в рамках системы управления реализацией настоящей Программы» [3].

При этом следует отметить, что сам процесс обсуждения в профессиональных сообществах, экспертных структурах и советах весьма позитивно сказался на актуализации задач и приоритизации проектов в сфере цифровой трансформации и институционализации таких новаций, как «интернет вещей», блокчейн-технологии, онлайн-сервисы в различных сферах экономики и управления.

В частности, многие позиции Дорожной карты программы «Цифровая экономика» создают возможности для использования блокчейна, например, планируется обеспечить правовые условия для внедрения и использования технологий децентрализованного ведения реестров и удостоверения прав (п. 1.2). Предполагается создать открытую общественную сетевую платформу для управления результатами интеллектуальной деятельности (п. 3.3.5). Зарубежный и российский опыт использования блокчейн-технологий в различных сферах управления демонстрирует ряд эффектов [6],

однако требуются специальные исследования при оперировании сверхбольшими массивами информации (в масштабах региона и страны).

Важное значение имеет ориентация Программы на разработку технических стандартов и адаптацию системы стандартизации целям внедрения цифровой экономики.

Заключение. В 2017 году наступил новый этап развития программ информатизации в Российской Федерации. Принятие программы «Цифровая экономика» приведет к переформатированию региональных программ информатизации, в частности можно предположить, что будут внесены изменения и в Концепцию региональной информатизации и аналогичные региональные нормативные правовые акты.

СПИСОК ЛИТЕРАТУРЫ

1. Послание Президента Федеральному Собранию [1.12.2016] // Президент России. – URL: <http://kremlin.ru/events/president/news/53379> (дата обращения на 03.10.2017).
2. Путин объявил переход России на «цифровую экономику» [1.12.2016] // CNews. – URL: http://www.cnews.ru/news/top/2016-12-01_poslanie_federalnomu_sobraniyu_putin_nastaivaet (дата обращения на 03.10.2017).
3. Об утверждении программы «Цифровая экономика Российской Федерации». Распоряжение Правительства РФ от 28 июля 2017 года №1632-р. – URL: <http://government.ru/docs/28653/> (дата обращения на 03.10.2017).
4. Перечень поручений Президента России по реализации Послания Федеральному Собранию (№Пр-2346 от 5 декабря 2016 года) – URL: <http://www.kremlin.ru/acts/assignments/orders/53425> (дата обращения на 03.10.2017).
5. Цифровая экономика вошла в список направлений стратегического развития [19.07.2017] // РБК. – URL: <http://www.rbc.ru/rbcfreenews/596f76a59a794733a47de689> (дата обращения на 03.10.2017).
6. Пряников М.М., Чугунов А.В. Блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы // International Journal of Open Information Technologies. 2017. № 6 (5). С. 49-55.

УДК 004.62

ДОВЕРИЕ МЕЖДУ КОНТРАГЕНТАМИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Шугай Антон Андреевич

Исследовательская лаборатория brdt.pro,
Россия, Санкт-Петербург, о. Новая Голландия, 2, офис 403
email: anton@brdt.pro

Аннотация: В докладе представлен анализ применения технологии blockchain для решения проблемы доверия в процессе обеспечения безопасности информации. Рассматриваются традиционные подходы по достижению доверия, их слабые стороны и высокая стоимость. Технология blockchain позволяет обеспечить полную прозрачность и математическую доказуемость целостности данных и источников ввода. Невозможность изменения записанной информации полностью исключает атаку направленную на целостность данных и снимает затраты на поддержание информационной безопасности архивов и реестров. Встроенные алгоритмы подтверждения аутентичности участников взаимодействия упрощают интеграцию с системами идентификации и аутентификации, контроля доступа и защиты соединений.

Ключевые слова: технология blockchain, проблема доверия, государственные информационные системы, информационная безопасность

TRUST BETWEEN COUNTERPARTIES IN INFORMATION SYSTEMS

Shugay Anton

Research Laboratory brdt.pro,
Russia, St. Petersburg, New Holland island, 2, of. 403
email: anton@brdt.pro

Abstract: The paper presents an analysis of the blockchain technology application for the purpose of solving problem of trust in the process of ensuring information security. Traditional approaches of achieving trust, their weaknesses and high cost are considered. The blockchain technology allows to provide full transparency and mathematical provability of data integrity and origin of data input. An impossibility of changing recorded information completely excludes attacks aimed at the integrity of the data and removes the costs of maintaining the information security of archives and registers. Built-in algorithms of the interaction participants' authenticity confirmation simplify integration with identification, authentication, access control and connection security systems.

Keywords: blockchain technology, problem of trust, state information systems, information security.

Введение. Доверительные механизмы, надежность и общедоступность данных, лежащие в основе технологии blockchain, обеспечивают ее эффективность, низкую стоимость и высокую безопасность. Эти характеристики широко обсуждаются и исследуются экспертами самых разных областей. Сейчас технология входит в стадию активного тестирования для создания новых бизнес-моделей как в частном секторе экономики, так и в государственном.

Технология blockchain имеет потенциал для создания третьей великой системы доверия, наряду с государственными силами и социальными группами, основанными на этнической и/или гражданской солидарности, вере, школьных связях и другими. blockchain предлагает новый способ личной и социальной уверенности, необходимой при любой транзакции. На этой основе появилось множество новых сервисов: академические сертификаты, электронные медицинские записи, информация о гарантии для покупок, отчеты о клинических испытаниях, проверка цепи поставок и происхождения товара, подтверждение авторского права и многое другое. Понятие смарт-контракты приобрело новый смысл с появлением возможности их независимого исполнения. Также blockchain может избавить от проблемы ложной информации.

На сегодняшний день, ведется активная дискуссия о регулировании использования технологии. Фактически, технология blockchain может дополнять или же полностью заменять правоприменение. Поэтому, жесткое регулирование инновации со стороны государства может привести к отказу в возможности применять технологию blockchain для достижения целей государственной политики.

Концепция доверия, на которой основан практически любое транзакционное взаимодействие между объектами, необходима для обеспечения сотрудничества в условиях неопределенности. Значимость и роль доверия может меняться в зависимости от объекта, но оно необходимо для формирования прозрачных взаимоотношений между объектами экономической и социальной деятельности. Пользователи информационных систем сталкиваются с проблемой доверия, например, при использовании кредитной карты, при предоставлении персональных данных или при заказе и потреблении продукта. Доверие может стать продуктом само по себе. Технология blockchain благодаря своей прозрачности может увеличить доверие к производителям товаров и услуг практически в любой отрасли.

Технология также дает пользователям уверенность в том, что они могут безопасно хранить и обмениваться ценностями. И все же если, blockchain полностью ликвидирует необходимость доверия людям и компаниям с помощью программного кода и криптографии, не создаст ли она что-то, что будет противоположно концепции доверия? Если blockchain будет единственным гарантом исполнения договоренностей и обязанностей сторон, могут возникнуть проблемы из-за ограничений самой технологии. Вот тут и нужен механизм, способный работать совместно с инновационной технологией. И этот механизм – закон. [3, р. 23]. И, хотя многие считают, что участие государства замедлит развитие технологии blockchain и криптоэкономики, стоит помнить, что государство было создано не только как механизм заставляющий людей верить друг другу из-за страха мифического Левиафана Томаса Гоббса, иначе бы Сатоши Накамото уже решил эту проблему.

Заключение. Стоит отметить, что технология blockchain может успешно применяться и в государственных информационных системах. Внедрение технологии в государственные системы приведет к повышению эффективности государственного управления, уменьшению стоимости транзакций; сделает взаимодействие с государственными органами более простым, быстрым, комфортным и эффективным. Разработка единой информационно-аналитической системы для мониторинга и контроля, создание цифровых платформ для интеллектуального управления ресурсами, развитие интеллектуальных систем поддержки принятия решений, использование беспилотных и интеллектуальных робототехнических комплексов, создание инфраструктуры для сбора и хранения информации в симбиозе с технологией Blockchain приведет к отличным результатам. Некоторые эксперты считают, что с появлением этой технологии, полностью изменится транзакционное взаимодействие между объектами: люди, организации, государства, роботы.

СПИСОК ЛИТЕРАТУРЫ

1. National Security Implications of Virtual Currency, December 2015 https://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1231/RAND_RR1231.pdf
2. Бутырин В., Проблема Доверия (Ч.2) // Cryptoscope, 27 апреля 2015 https://cryptoscope.blogspot.ru/2016/05/2_51.html
3. Werbach K. Trust, But Verify: Why the Blockchain Needs the Law // Technology Law Journal, Berkeley, 2017.
4. DiStefano J., Blockchain: 'A novel solution to the problem of trust' beyond Bitcoin // Philly.com, February 2, 2017 <http://www.philly.com/philly/blogs/inq-phillydeals/Blockchain-.html>
5. Seppälä J., The role of trust in understanding the effects of blockchain on business models // Aalto University School of Science, Helsinki, October 7, 2017 https://aaltodoc.aalto.fi/bitstream/handle/123456789/23302/master_Sepp%C3%A4l%C3%A4_Jane_2016.pdf?sequence=1
6. Qian DJ., Op Ed: The Fourth Industrial Revolution: Blockchain Tech and the Integration of Trust // Bitcoin Magazine, February 15, 2017 <https://bitcoinmagazine.com/articles/op-ed-fourth-industrial-revolution-blockchain-tech-and-integration-trust/>
7. Bauerle N., What are Blockchain's Issues and Limitations? // Coindesk <https://www.coindesk.com/information/blockchains-issues-limitations/>
8. Macaulay T., Blockchain limitations: Is the distributed ledger technology overhyped? // Tech World, November 9, 2016 <https://www.techworld.com/startups/what-are-limitations-of-blockchain-experts-from-odi-explain-3648881/>
9. Цифровая экономика России, 10 апреля, 2017 http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D1%8F_%D1%8D%D0%BA%D0%BE%D0%BD%D0%BE%D0%BC%D0%B8%D0%BA%D0%B0_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8
10. Маркушевский Д., Рябова Н., Кухарчик В. Технологии «блокчейн» для электронного правительства / Школа молодых менеджеров публичного администрирования, Белорусский институт реформы и трансформации публичного администрирования, 2016 http://sympa-by.eu/sites/default/files/articles/blockchain_v_elektronnom_pravitelstve.pdf
11. Авдеев М., Блокчейн-технологии в госуправлении. Мировой опыт // Forbes, 25 апреля, 2017 <http://www.forbes.ru/tehnologii/343203-blokcheyn-tehnologii-v-gosupravlenii-mirovoy-opyt>



ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 621.396.62

ПРИНЦИПЫ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ СЕТЕЙ ПОДВИЖНОЙ РАДИОСВЯЗИ ПРАВООХРАНИТЕЛЬНОЙ СФЕРЫ НА ОСНОВЕ СОВЕРШЕНСТВОВАНИЯ ЧАСТОТНО-ТЕРРИТОРИАЛЬНОГО ПЛАНИРОВАНИЯ

Бабкин Александр Николаевич
Воронежский институт МВД России
emails: alex_babk@mail.ru

Аннотация: В статье рассмотрены вопросы обеспечения качества связи и защищенности информации в сетях подвижной радиосвязи правоохранительной сферы на основе совершенствования их частотно-территориального планирования. Совершенствование частотно-территориального планирования включает в себя оптимальное присвоение частот, оптимальное территориальное расположение радиосетей, применение современных методов проектирования, направленных на выполнение требований по формированию показателя эффективности функционирования сетей радиосвязи.

Ключевые слова: сеть радиосвязи, качество связи, защищенность информации, частотно-территориальное планирование

PRINCIPLES OF INCREASE IN SECURITY OF INFORMATION OF NETWORKS MOBILE RADIO COMMUNICATION OF THE LAW-ENFORCEMENT SPHERE ON THE BASIS ENHANCEMENTS OF FREQUENCY AND TERRITORIAL PLANNING

Babkin Alexander Nikolaevich
Voronezh institute of the Ministry of Internal Affairs of the Russian Federation
emails: alex_babk@mail.ru

Abstract: In article questions of support of communication quality and security of information on networks of a mobile radio communication of the law-enforcement sphere on the basis of enhancement of their frequency and territorial planning are considered. Enhancement of frequency and territorial planning includes optimum assignment of frequencies, optimum territorial layout of radio networks, application of the modern design methods directed to execution of requirements for formation of an index of efficiency of functioning of networks of a radio communication.

Keywords: radio communication network, communication quality, security of information, frequency and territorial planning

Введение. Возрастающие требования к защищенности информации сетей радиосвязи (СРС) правоохранительной сферы, связанные с количественным ростом радиоэлектронных средств (РЭС), совершенствованием существующих и необходимостью организации новых радиосетей, увеличением интереса к ним со стороны криминальных структур, организаций антиконституционной направленности, спецслужб иностранных государств, стремящихся использовать для своих целей оперативно-служебную информацию, приводят к необходимости совершенствования частотно-территориального планирования (ЧТП) СРС.

Основная часть. В настоящее время под ЧТП понимают комплекс мероприятий, направленный на обеспечение электромагнитной совместимости (ЭМС) РЭС и СРС, вопросы защищенности информации не рассматриваются. В то же время, частотно-территориальное планирование должно быть одним из важнейших этапов проектирования защищенных СРС, обеспечивающее их организацию на заданной территории в условиях противодействия угрозам информационной безопасности, выполнение установленных требований по электромагнитной совместимости.

Основным требованием по обеспечению ЭМС РЭС и СРС является выполнение функциональных задач в реальной электромагнитной обстановке с заданным качеством функционирования. Все размещаемые в радиосети РЭС должны функционировать, не оказывая друг на друга мешающего воздействия. За критерий ЭМС принимается допустимое отношение сигнал/помеха на входе приемника при условии, что его численное значение определяется по

допустимому эффекту влияния помехи на полезный сигнал на выходе приемника, т.е. по допустимому численному значению отношения сигнал/помеха на выходе приемника [1, 2].

Совершенствование ЧТП состоит в проведении дополнительных мероприятий, связанных с обеспечением защищенности информации на основе оптимального присвоения частот защищенным СРС, оптимальном территориальном расположении радиосетей, применении современных методов частотно-территориального планирования, направленных на выполнение требований по формированию показателя эффективности функционирования СРС. В качестве показателя эффективности функционирования СРС в условиях защищенности информации может использоваться вероятность доведения сообщения до легальных пользователей за время меньше требуемого значения при обеспечении требуемых показателей качества связи и защищенности информации [3]. В качестве показателя качества связи может выступать достоверность передачи информации и один из показателей надежности СРС (например, коэффициент оперативной готовности), в качестве показателя защищенности информации – вероятность обеспечения её защиты в сети радиосвязи при воздействии угроз информационной безопасности. Показатель защищенности информации является комплексным критерием и в свою очередь включает в себя такие показатели, как показатели конфиденциальности, целостности, доступности и скрытности.

Оптимальное присвоение частот защищенным СРС необходимо для повышения эффективности использования радиочастотного спектра, расчета предельной загрузки частотных диапазонов, определения технических характеристик РЭС СРС, влияющих на электромагнитную обстановку (ЭМО) в территориальных районах, оценки характеристик складывающейся ЭМО в долгосрочной перспективе, обеспечения защищенности передаваемой информации. Оптимальным считается такое присвоение частот, которое максимизирует число СРС, получивших частотные присвоения (если полоса частот задана), или минимизирует полосу частот (если задана исходная группа СРС) [4, 5].

При оптимальном присвоении частот необходимо учитывать защитные отношения и назначать сетям радиосвязи частоты работы с учетом:

1. Совместимости в отношении помех по совмещенным, соседним и побочным каналам приема, а также интермодуляционным искажениям.

2. Обеспечения заданной зоны покрытия при соответствии показателей доступности и скрытности требуемым значениям.

Задачей оптимального территориального размещения СРС является формирование таких территориальных размещений радиосетей, которые исключали бы перекрытие зон обслуживания и зон помех.

Одним из эффективных способов решения данной задачи является применение радиально-углового метода, основанного на применении полярной системы координат [5]. Данный метод позволяет значительно упростить расчеты, связанные с определением возможных перекрытий зон обслуживания и зон помех, вводимых в существующую группировку СРС новых радиосетей.

Одним из возможных способов обеспечения качества связи и защищенности информации является контроль радиоканала, как основного элемента сети радиосвязи, в реальных условиях эксплуатации СРС [6]. В СРС качество связи между элементами сети радиосвязи зависит прежде всего от условий распространения радиоволн. Условия распространения радиоволн могут изменяться от однолучевого распространения между приемником и передатчиком в условиях прямой видимости до многолучевого распространения при многократных отражениях от препятствий (особенно в городских условиях и внутри зданий) при отсутствии прямой видимости. Количественной мерой обеспечения качества связи может служить или вероятность ошибочного, или вероятность правильного приема информации. При этом вероятность ошибочного или вероятность правильного приема информации может определять также такие показатели защищенности информации как доступность и скрытность. Сети радиосвязи, в которых осуществляется контроль радиоканала в реальных условиях эксплуатации, можно отнести к сетям с обратной связью.

Закключение. Совершенствование частотно-территориального планирования СРС можно рассматривать как концепцию построения защищенных сетей радиосвязи, предполагающую:

- оптимизацию их частотного ресурса;
- оптимизацию расположения РЭС и СРС на территории;
- оптимизацию энергоресурсов РЭС;
- обеспечение показателя эффективности функционирования СРС в реальных условиях эксплуатации.

СПИСОК ЛИТЕРАТУРЫ

1. Бабкин А.Н. ЧТП сетей подвижной радиосвязи специального назначения / А.Н. Бабкин, А.В. Леншин // Теория и техника радиосвязи. – 2013 – 3. – С.17-22
2. Сети мобильной связи. Частотно-территориальное планирование: учебное пособие для вузов / В.Ю. Бабков, М.А. Вознюк, П.А. Михайлов. – М.: Горячая линия – Телеком, 2007. – 224 с.
3. Бабкин А.Н. Постановка задачи проектирования защищенных сетей радиосвязи органов внутренних дел / А.Н. Бабкин, Э.А. Бардаев // Вестник ВИ МВД России. – 2015. – №3. – С.16– 22.
4. Бабкин А.Н. Способ частотно-территориального планирования сетей радиосвязи специального назначения / А.Н. Бабкин, И.В. Атласов // Вестник ВИ МВД России. – 2014. – №4. – С.165– 177.
5. Бабкин А.Н. Радиально-угловой метод частотно-территориального планирования сетей подвижной радиосвязи ОВД / А.Н. Бабкин, И.В. Атласов // Вестник ВИ МВД России. – 2013. – №3. – С.12– 118.
6. Бабкин А.Н. Способ контроля радиоканала / А.Н. Бабкин, А.В. Эсауленко // Вестник ВИ МВД России. – 2013. – №1. – С.8 – 13.

УДК 681.142

ЗАДАЧА ВИЗУАЛИЗАЦИИ МАРШРУТОВ ВЫПОЛНЕНИЯ КОМПЬЮТЕРНЫХ ПРОГРАММБезруков Вячеслав Алексеевич¹, Синешчук Юрий Иванович², Синешчук Максим Юрьевич³¹ Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский пр-т, 49² Санкт-Петербургский университет МВД России
Россия, Санкт-Петербург, ул. Летчика Пилутова, 1³ Санкт-Петербургский университет ГПС МЧС России
Россия, г. Санкт-Петербург, Московский просп., 149

emails: bezrukov.1950@mail.ru, sinegal@rambler.ru, smaxim@inbox.ru

Аннотация: Рассмотрена проблема разработки инструментальных средств позволяющих визуализировать маршруты выполнения программ защиты информации.

Ключевые слова: защита информации, программное обеспечение, сертификация, граф, визуализация.

THE PROBLEM OF VISUALIZING ROUTES RUN COMPUTER PROGRAMS¹Bezrukov Vjacheslav, Sineshchuk Yuri² Sineshchuk Maxim³¹Saint - Petersburg national research University of information technologies, mechanics and optics
Russia, St. Petersburg, Kronverksky broad street, 49² Saint-Petersburg University of MIA of Russia
Russia, Saint-Petersburg, letchika Pilyutova Street 1,³Saint-Petersburg university of State fire service of EMERCOM of Russia
Russia, St. Petersburg, Moscow broad street, 149.

emails: bezrukov.1950@mail.ru, sinegal@rambler.ru, smaxim@inbox.ru

Abstract: The problem of development of tools allowing you to visualize the routes of program execution of information protection.

Keywords: information security, software certification, graph, visualization.

Введение. Научно-технический прогресс, создание и глобальное распространение электронных технологий, особенно сети Интернет, стало основной причиной появления и распространения киберугроз. Чтобы обеспечить превосходство над потенциальными противниками(конкурентами), специальные подразделения ищут слабые звенья и уязвимые места в их компьютерных системах.

Для предотвращения кибератак, реализующих соответствующие киберугрозы создаются системы защиты информации (СЗИ), при этом особую актуальность приобретает вопрос обеспечения контроля отсутствия недеklarированных возможностей программного обеспечения(ПО) СЗИ. Эта проблема обусловлена большим количеством разработчиков и разнообразием ПО, при разработке которого, зачастую основное внимание уделяется его функциональности, и, в значительно меньшей степени, - его безопасности. Вместе с тем, существующая статистика неумолимо свидетельствует о большом количестве уязвимостей, выявляемых в ПО. Указанные обстоятельства обуславливают необходимость сертификации ПО СЗИ на соответствие требованиям безопасности [1]. Процедура сертификации, как эффективное средство управления безопасностью, предполагает осуществление контроля отсутствия недеklarированных возможностей (НДВ).

Одним из важных инструментов в этой системе является статический анализ исходных текстов программ, который предполагает формирование перечня маршрутов выполнения функциональных объектов. В качестве функциональных объектов могут выступать процедуры, функции, ветви, операторы и т.п. элемент программы, осуществляющий выполнение действий по реализации законченного фрагмента алгоритма программы [2].

Процедура формирования маршрутов выполнения функциональных объектов и ветвей программного обеспечения характеризуется высокой сложностью, обусловленной большими временными затратами, сложностью аналитической работы эксперта, что в ряде случаев делает сертификацию недоступной для разработчиков ПО. Одним из решений, в рамках решения указанной проблемы, может служить снижение требований к автоматизированному рабочему месту эксперта за счет возможности взаимодействия с результатом визуализации маршрутов [3], [4]. Визуализация графов представляет собой отдельную дисциплину на стыке теоретической информатики и математики. Данная дисциплина получила широкое развитие в силу разнообразия областей практического применения.

Архитектуры инструментального комплекса, реализующего поставленную задачу отражает два этапа формирования изображения графа: присваивания координат и вывод полученной укладки, что реализуется в рамках следующих модулей:

- модуль получения и обработки входных данных;

- модуль формирования укладки графа;
- модуль формирования интерфейса пользователя;
- модуль визуализации графа.

Передача данных на модуль формирования укладки графа осуществляется через модуль получения и обработки входных данных, или результатов анализа. На сторону конечного пользователя подается результат работы модуля формирования укладки графа, представляющий собой сериализованный объект, содержащий информацию о вершинах графа (функциональных объектах или ветвях) и их связях, а также координаты вершин. Модуль формирования интерфейса, получая на вход сериализованный объект, передает его модулю визуализации, который создает окончательное изображение, являющееся частью графического интерфейса.

Заключение. Задача уменьшения требований к автоматизированному рабочему месту эксперта при сохранении возможности взаимодействия с результатом визуализации решена благодаря архитектурному разделению программного комплекса на две компоненты, первая из которых формирует укладку графа и передает её в виде сериализованного объекта, а вторая выполняется независимо от первой, принимает на вход укладку графа и формирует средствами браузера искомое изображение, а также обеспечивает возможность взаимодействия пользователя с графом.

СПИСОК ЛИТЕРАТУРЫ

1. Беляков И. А., Еремеев М. А. Применение интеллектуальных технологий в процессе сертификации программного обеспечения // Молодой ученый. — 2011. — №11. Т.1. — С. 23-31.
2. Graph Drawing [Electronic resource] // Graph Drawing Symposium [Official website]. URL: <http://www.graphdrawing.org/>
3. Documentation [Electronic resource] // Graphviz – Graph Visualization Software [Официальный сайт]. Режим доступа: <http://www.graphviz.org/Documentation.php>
4. З.В. Апанович. Методы визуализации информации при помощи графов. Часть 2. Методы визуализации ориентированных и неориентированных графов [Электронный учебник] // Электронная образовательная среда НГУ [Официальный сайт]. Режим доступа: http://193.124.209.204/?db=book_apanovich2&int=VIEW&class=ROOT&templ=VIEW

УДК 004.05

АЛГОРИТМ СИНТЕЗА ЭФФЕКТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Вилков Валерий Борисович¹, Сычев Сергей Евгеньевич², Черных Андрей Климентьевич²

¹ Военная академия материально-технического обеспечения им. генерала армии А.В. Хрулёва, Россия, Санкт-Петербург, наб. Макарова, 8,

² Санкт-Петербургский институт войск национальной гвардии Российской Федерации, Россия, Санкт-Петербург, ул. Лётчика Пилютова, 1, emails: amirusha@rambler.ru, s75sichev@mail.ru

Аннотация: В статье рассматривается подход к созданию информационных систем, обеспечивающих информационную безопасность обрабатываемых данных. Предложен оптимальный алгоритм, синтезирующий указанные системы. Приведён иллюстративный пример. Указаны направления, развивающие подход к созданию указанных систем.

Ключевые слова: информационная безопасность системы, надежность системы, теория нечетких множеств, нечеткая логика, максимальный остов.

SYNTHESIS ALGORITHM OF EFFECTIVE INFORMATION SYSTEMS

Vilkov Valeriy¹, Sychev Sergey², Chernykh Andrey²

¹ Military academy of logistics behalf of the army general A. V. Khrulyov, Russia, St.-Petersburg, nabereznaya Makarova, 8,

² St.-Petersburg institutes of armies of national guards of Russian Federation, Russia, St.-Petersburg, Pilot Pilutova str. 1, emails: amirusha@rambler.ru, s75sichev@mail.ru

Abstract: In article approach to creation of the information systems ensuring information security of the processed data is considered. The optimum algorithm synthesizing the specified systems is offered, the illustrative example is given. The directions developing approach to creation of the specified systems are specified

Keywords: information security of system, reliability of system, theory of indistinct sets, fuzzy logic, maximum skeleton.

Введение. В статье рассмотрена задача по созданию наиболее эффективной, по критерию информационной безопасности (в дальнейшем надежной) информационной системы. Эта задача является модификацией известной задачи о кратчайшем соединении [1], [2], [3], [4]. Отличие состоит в том, что в качестве характеристики линии передачи данных используется не её стоимость, а её надежность, для чего привлекается теория нечетких множеств и нечеткая логика [5], [6], [7], [8], [9], [10], [11], [12], [13].

Доказано, что некоторые задачи приводят к необходимости построить сеть не минимального, а максимального веса. К этой задаче также применим алгоритм Краскала, если изменить знак веса каждого ребра на противоположный. Если требуется найти сеть с минимальным произведением весов ребер, то, учитывая, что $\log(ab) = \log(a) + \log(b)$, минимальное остовное дерево графа, в котором веса ребер заменены их логарифмами, дает нужное решение. Правда, вес ребер обязательно должен быть положительным.

Дана формулировка рассматриваемой задачи на языке теории графов [2] [3].

Показана актуальность сформулированной задачи при создании сетей, когда важно минимизировать доступ хакеров к информации в них циркулирующей.

Определено понятие надежности кабельной линии связи, показателя надежности кабельной линии связи.

Предложено для определения надежности кабельных линий связи и всей сети использовать теорию нечетких множеств.

Определен вид функции принадлежности [14].

Следуя [15], [16], [17], введены понятия нечеткой логики.

Над нечеткими высказываниями введены различные логические операции.

В постановке задачи указан связный взвешенный граф $G = (E, V)$, его ребра соответствуют кабельным линиям связи, каждому из них соотнесено число - степень истинности нечеткого высказывания «кабельная линия связи надежна».

Требуется найти остов этого графа, для которого степень истинности нечеткого высказывания «все кабельные линии связи надежны» максимальна.

Сформулированы теоремы 1 и 2.

Предложен алгоритм, реализующий указанную задачу.

Пусть дан связный граф $G = (V, E)$, имеющий n вершин и m ребер, пусть для любого ребра $e \in E$ определен его вес $d(e)$ (его надежность).

Начинаем с графа $G_0 = (V, \emptyset)$, который состоит только из вершин графа $G = (V, E)$ и не имеет ребер. Этот граф можно рассматривать как n компонент связности, каждая из которых состоит из одной вершины.

В дальнейшем алгоритм состоит из последовательности этапов. На этапе с номером k ($k = 1, 2, \dots, n-1$) строится граф $G_k = (V, T_k)$, для этого к множеству ребер T_{k-1} графа G_{k-1} добавляется одно ребро, которое выбирается по следующему правилу:

- в графе $G = (V, E)$ выбираем ребро максимального веса из числа ребер, не принадлежащих T_{k-1} ;
- если добавление этого ребра к T_{k-1} не приводит к образованию цикла, то присоединяем это ребро к T_{k-1} , получаем T_k и граф $G_k = (V, T_k)$;
- если цикл образуется, то из оставшихся ребер графа $G = (V, E)$ не принадлежащих T_{k-1} , выбираем ребро максимального веса и т.д.

Граф G_{n-1} является остовом графа G максимального веса.

Заключение. В заключении отмечено, что в статье предложен легко программируемый алгоритм создания информационной системы, в максимальной степени обеспечивающей информационную безопасность, реализуемого в её рамках информационного обмена.

СПИСОК ЛИТЕРАТУРЫ

1. Белоусов А. И., Ткачев С. Б. Дискретная математика. – М., 2006. – 744 с.
2. Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К. Минимальные остовные деревья // Алгоритмы: построение и анализ / Под ред. И. В. Красикова. 2-е изд. – М., 2005. – 1296 с.
3. Таха Т. Введение в исследование операций. – М.: Вильямс, 2005. – 912 с.
4. Kruskal B. On the Shortest Spanning Subtree of a Graph and the Traveling Salesman Problem. – Proc. AMS. 1956. Vol 7, No. 1.
5. Черных А. К., Вилков В. Б. Управление безопасностью транспортных перевозок при организации материального обеспечения сил и средств МЧС России в условиях чрезвычайной ситуации // Пожаровзрывобезопасность. 2016. Т. 25. № 9. С. 52-59.
1. DOI: 10.18322/PVB.2016.25.09.52-59.
6. Вилков В. Б., Черных А. К., Гарькушев А. Ю., Зайцев А. И. Алгоритм поиска оптимального маршрута выдвижения подразделения войск национальной гвардии // Известия Российской академии ракетных и артиллерийских наук. 2017. № 1 (96). С. 29-33.
7. Вилков В. Б., Черных А. К., Флегонтов А. В. Теория и практика оптимизации решений на основе нечетких множеств и нечёткой логики. – СПб.: Изд. РГПУ им. А.И. Герцена, 2017. – 160 с.
8. Заде Л. Понятие лингвистической переменной и его применение к принятию приближенных решений. – М., 1976. – 166 с.
9. Кофман А. Введение в теорию нечетких множеств. – М.: Радио и связь, 1982. – 429 с.
10. Леоненков А. В. Нечеткое моделирование в среде MATLAB и fuzzyTECH. – СПб.: БХВ-Петербург, 2005. – 725 с.
11. Орловский С. А. Проблемы принятия решений при нечеткой исходной информации. – М., 1981. – 206 с.
12. Яхьяева Г. Э. Нечеткие множества и нейронные сети. – М.: Бином, 2006. – 315 с.
13. Zadeh L. Fuzzy sets // Information and Control. –1965. – № 8. P. 338-353.
14. Борисов А.Н., Крумберг О.А., Федоров И.П. Принятие решений на основе нечетких моделей: Примеры использования. – Рига: Зинатне, 1990. – 184 с.
15. Заде Л. Понятие лингвистической переменной и его применение к принятию приближенных решений. – М.: Мир, 1976. – 166 с.
16. Тэрано Т., Асаи К., Сугэно М. Прикладные нечеткие системы. – М.: Мир, 1993. – 368 с.
17. Штовба С.Д. Введение в теорию нечетких множеств и нечеткую логику. – Винница: УНИВЕРСУМ-Винница, 2001. – 71 с.

УДК 343

НЕКОТОРЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РЕАЛИЗАЦИИ ПОЛИЦИЕЙ ФУНКЦИИ ГОСУДАРСТВЕННОЙ ЗАЩИТЫГалушко Валерий Анатольевич¹, Воронов Анатолий Федорович², Малахов Александр Сергеевич³¹ Омская академия МВД России, Россия, Омск, пр. Комарова, 7,² УМВД России по Омской области, Россия, Омск, ул. Ленина, 2,³ Омская академия МВД России, Россия, Омск, пр. Комарова, 7,

emails: vgalushko@yandex.ru, omskbox@mail.ru

Аннотация: В статье рассмотрены отдельные проблемы информационной безопасности, связанные с защитой полицией участников уголовного судопроизводства и предложения по их решению.

Ключевые слова: информационная безопасность; государственная защита участников уголовного судопроизводства, информационно-коммуникационная сеть Интернет.

SOME ASPECTS OF ENSURING INFORMATION SECURITY DURING THE IMPLEMENTATION OF THE POLICE FUNCTIONS OF THE STATE PROTECTIONGalushko Valery¹, Voronov Anatoly², Malakhov Alexander³¹The Omsk Academy of the Interior, Russia, Omsk, Komarova str. 7,² Department of Internal Affairs of Russia in Omsk region, Russia, Omsk, Lenin str., 2,³ The Omsk Academy of the Interior, Russia, Omsk, Komarova str. 7

emails: vgalushko@yandex.ru, omskbox@mail.ru

Abstract: the article considers some problems of information security related to the protection of the police participation in criminal proceedings and proposals for their solution.

Keywords: information security; state protection of participants of criminal proceedings, communication in the Internet.

Введение. Отсутствие кардинальных позитивных изменений в количественных и качественных характеристиках преступности в России позволяет констатировать, что комплекс осуществляемых мероприятий по борьбе с ней недостаточно эффективен. Особую тревогу вызывает тенденция к учащению противоправного воздействия на участников уголовного судопроизводства, латентность которого позволяет лишь с условностью судить о действительных его масштабах. Анализ ситуации в сфере государственной защиты должностных лиц и участников уголовного судопроизводства в Российской Федерации свидетельствует об устойчивой тенденции увеличения числа защищаемых лиц. Это говорит с одной стороны о том, что преступное воздействие на них растет, а с другой – о том, что люди больше стали доверять правосудию и гарантированной помощи со стороны государства. В этих условиях возрастает актуальность вопросов, связанных с совершенствованием информационной безопасности при осуществлении государственной защиты, которые выступают предметом нашего внимания.

Анализ законодательных и ведомственных нормативных правовых актов [1], [2] свидетельствует об отсутствии подробной регламентации вопросов обеспечения информационной безопасности лица, к которому применяются меры государственной защиты. Научные исследования [3], [4] и практика деятельности подразделений по обеспечению государственной защиты МВД России свидетельствует, что преступники, стремясь оказать криминальное воздействие на участников уголовного судопроизводства, самостоятельно либо при помощи квалифицированных специалистов ведут поиск и анализ информации о них в информационно-телекоммуникационной сети Интернет, применяют программные и технические средства [5] несанкционированного получения интересующих сведений. Высокая степень проникновения в повседневную жизнь современного человека сервисов информационно-телекоммуникационных сетей [6], электронных платежей, средств мобильной связи [7], [8], [9] и привыкание к ним пользователя объективно затрудняет обеспечение сотрудниками полиции безопасности лица, к которому применяются меры государственной защиты. В ряде случаев защищаемое лицо затрудняется указать все социальные сети, интернет-магазины, электронные платежные системы и иные ресурсы, где была оставлена информация о нем. И если сотрудники подразделений полиции по обеспечению государственной защиты проходят специальную подготовку и обладают необходимыми навыками по недопущению утечки информации о защищаемых ими лицах в этой сфере, имеют соответствующие нормативно закрепленные обязанности и ответственность, то вовлеченные в орбиту уголовного судопроизводства граждане, как правило, не только не обладают такими знаниями и навыками, но и в ряде случаев пренебрегают разъясняемыми им элементарными правилами по обеспечению личной безопасности. В этих условиях несоблюдение защищаемым лицом запретов и рекомендаций сотрудников подразделений органов внутренних дел, осуществляющих государственную защиту, по использованию вышеназванных технических средств и сетей передачи

данных может создать реальную угрозу выявления правонарушителями этого лица и совершения в отношении него преступления.

Заключение. Представляется необходимым при заключении органом, осуществляющим меры безопасности, договора с защищаемым лицом, фиксировать в нем в числе обязанностей защищаемого лица ограничение пользования ресурсами информационно-телекоммуникационной сети Интернет, электронными платежами, средствами мобильной связи. Это повысит эффективность информационной безопасности при выполнении полицией функции государственной защиты участников уголовного судопроизводства и будет способствовать укреплению правопорядка в Российской Федерации.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 20 августа 2004 г. N 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства». Доступ из СПС КонсультантПлюс.
2. Приказ МВД РФ от 21 марта 2007 г. N 281 "Об утверждении Административного регламента МВД России по исполнению государственной функции обеспечения в соответствии с законодательством Российской Федерации государственной защиты судей, должностных лиц правоохранительных и контролирующих органов, безопасности участников уголовного судопроизводства и их близких".
3. Вормсбехер И.А. Проблемные вопросы применения государственной защиты в отношении граждан, участвующих в проведении оперативно-розыскных мероприятий // Деятельность органов внутренних дел по обеспечению безопасности лиц, подлежащих государственной защите в современных условиях: вопросы теории и практики. 2016. № 3. С. 333 – 337.
4. Таова Л.Ю. Обеспечение безопасности лиц, участвующих в уголовном судопроизводстве, и их близких как средство реализации принципа охраны прав и свобод человека и гражданина // Общество и право. 2007. № 4(18). С. 231-234.
5. Парадников А.Г., Щеглов И.В., Дубинин А.С., Шаламов Г.В. Специальные технические средства органов внутренних дел. Учебное наглядное пособие. Омск, 2011. 87 с.
6. Першин А.Н., Сидорова К.С. Использование ресурсов информационно-телекоммуникационной сети «Интернет» в розыскной деятельности следователя // Научный журнал «Библиотека криминалиста» Вып. 4, 2017. С. 320-325.
7. Шеховцова Л.С. Об участии специалиста при производстве обыска, сопряженного с изъятием электронного носителя информации // Раскрытие и расследование преступлений: наука, практика, опыт. Сборник научных статей преподавателей и адъюнктов кафедр криминалистики Московского университета МВД им. В.Я. Кикотя. Тула, 2015. С. 205-209.
8. Дерий Е.А., Шебалин А.В. Электронный кошелек как элемент способа незаконного сбыта наркотических средств, совершенного с использованием сети Интернет // Проблемы правовой и технической защиты информации. Сборник научных статей под ред. В.В. Полякова. Барнаул, 2015. С. 136-138.
9. Рясов А.В., Лапунова Ю.А. Способы противодействия вовлечению лиц в совершение преступлений террористического характера в информационно-телекоммуникационных сетях // Вестник СевКавГТИ. 2016. №2 (25). С. 121-123.

УДК 681.518 (004.031.42)

ПОДХОД К РАЗРАБОТКЕ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА ДЕЖУРНОГО ПО УНИВЕРСИТЕТУ

Иванов Николай Николаевич, Потехин Владимир Семенович
Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, ул. Летчика Пилютова, 1,
emails: kolya-domovoi@mail.ru, vsp1945@gmail.com

Аннотация: Излагается подход, позволяющий определить облик автоматизированного рабочего места, ориентированного на автоматизацию должностных функций дежурного по учреждению.

Ключевые слова: автоматизированное рабочее место; информационные системы; компьютерные технологии.

THE APPROACH TO THE DEVELOPMENT WORKSTATION ON DUTY AT THE UNIVERSITY

Ivanov Nikolay, Potekhin Vladimir
St. Petersburg University at Russian Ministry of Internal Affairs (MIA),
Russia, St. Petersburg, Pilot Pilyutov str., 1,
emails: kolya-domovoi@mail.ru, vsp1945@gmail.com

Abstract. An approach that allows to determine the appearance of the workstation, oriented on automation of the official functions of a duty officer at the institution is presented.

Keywords: automated workstation, information systems, computer technologies.

Введение. Следуя ГОСТу 34.003-90 [1] под автоматизированным рабочим местом (АРМ) будем понимать программно-технический комплекс (ПТК), обеспечивающий автоматизацию деятельности определенного вида. Как следует из анализа работ [2], [3], [4] и [5]:

– техническая часть ПТК, может представлять собой универсальную или специализированную ЭВМ с необходимым набором устройств ввода-вывода. Для случая дежурного по университету достаточно универсальной офисной ЭВМ;

– наиболее крупными компонентами программной части ПТК являются операционная система (ОС) и функциональное программное обеспечение (ФПО). При этом в качестве ОС возможно использование наиболее распространенной ОС MS Windows в любой современной комплектации. Что

касается ФПО, то оно должно разрабатываться специально для должностного лица, функции которого предполагается автоматизировать (в нашем случае — функции дежурного по университету).

Для выявления функций, подлежащих автоматизации, был выполнен анализ действующих нормативов [1], [2], [3] и учтен опыт разработки АРМ [4] и [5], что позволяет рекомендовать следующую последовательность действий:

- изучить основополагающие руководящие документы, регламентирующие функционирование объекта автоматизации (в нашем случае — должностные инструкции дежурного по университету);

- собрать и проанализировать данные о реальном функционировании объекта, как соответствующие функциональным обязанностям дежурного, так и обусловленные традициями университета или указаниями командования, не вошедшими пока в функциональные обязанности;

- собрать и проанализировать данные об организационной структуре объекта управления (в данном случае университета с детализацией элементов структуры в объеме, предусмотренном функциональными обязанностями дежурного);

- выявить функции, выполняемые каждым должностным лицом, участвующим в выбранном для автоматизации процессе, и порядок взаимодействия между ними до автоматизации (до внедрения разрабатываемого АРМа);

- определить какие из этих функций можно и целесообразно возложить на АРМ, а какие — оставить за человеком;

- определить состав должностных лиц, которые (исходя из выбранных функций, подлежащих автоматизации) будут оснащаться соответствующими техническими средствами (в частности АРМами);

- выявить новые задачи, которые можно решаться только после внедрения автоматизированной технологии работы (например, для организации оповещения личного состава в случае чрезвычайных ситуаций или тревоги до автоматизации по традиции могут использоваться списки «оповестителей», стационарные телефонные аппараты и «бумажный» учет личного состава по прибытии. В случае внедрения средств автоматизации, оповещение можно организовать иначе: путем автоматизированной рассылки SMS-сообщений по заранее составленным спискам личного состава и учета прибытия личного состава на основе данных, считываемых с турникетов, осуществляющих допуск на территорию университета по пластиковым пропускам. При этом, конечно, должна быть предусмотрена автоматизированная многоуровневая визуализация собранных данных с ориентацией на руководителей всех уровней, начиная от начальников структурных подразделений, до руководства организации);

- определить состав элементов, существенных для описания функционирования системы;

- определить функции каждого АРМа, включая АРМ дежурного по университету.

Заключение. Выполнение перечисленных действий, по мнению авторов, позволит собрать необходимые исходные данные, определить цели разработки, функций автоматизации, необходимые для построения функциональной структуры автоматизированного рабочего места исследуемого объекта автоматизации. На основании собранных данных, как следует из работ [6], [7] и [8], возможно построение функциональных моделей, необходимых для создания АРМ с учетом специфики функций, возлагаемых на дежурного по университету.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения. URL: <http://www.docload.ru/Basesdoc/32/32114/index.htm> (дата обращения 13.09.2017).
2. РД 50-680-88. Методические указания. Автоматизированные системы. Основные положения. М.: "Издательство стандартов", 1989.
3. Р 50-34. 126-92. Рекомендации. Информационная технология. Правила проведения работ по созданию автоматизированных систем. М.: "Издательство стандартов", 1993.
4. Потехин В.С., Кадулин В.Е. Об уточнении понятия и классификации автоматизированных рабочих мест, используемых в информационных системах и компьютерных технологиях Санкт-Петербургского университета МВД России // Вестник СПб университета МВД № 4 (68), 2015. С. 207 – 210.
5. Потехин В.С. Опыт разработки методических рекомендаций на основе компьютерных технологий для слушателей-заочников, готовящих дипломы по техническим специальностям // Вестник СПб университета МВД № 4, (60), 2013. С. 149 – 155.
6. Горбаченко В. И., Убиенных Г. Ф., Бобрышева Г. В. Создание функциональной модели информационной системы с помощью CASE-средства CA ERwin Process Modeler 7.3. / Пенза: ПГУ, 2010. 66 с. URL: <http://window.edu.ru/resource/658/72658/files/stup552.pdf> (дата обращения 11.09.2017).
7. Дубейсковский В.И. Практика функционального моделирования с AllFusion Process Modeer 4.1. Где? Зачем? Как? / М.: Изд. Диалог-МИФИ, 2008. 464 с. ISBN 5-86404 192-0.
8. Маклаков С.В. Моделирование бизнес-процессов с AllFusion PM. 2-е изд., испр. и дополн. / М.: Изд. Диалог-МИФИ, 2008 – 224 с. ISBN 5-86404-179-3.

УДК 681.518 (004.031.42)

ПОДХОД К АДАПТАЦИИ ТИПОВЫХ РЕШЕНИЙ ПРИ РАЗРАБОТКЕ СИСТЕМЫ КОНТРОЛЯ УПРАВЛЕНИЯ ДОСТУПОМ НА ОБЪЕКТЫ ОСОБОЙ ВАЖНОСТИ

Калачев Максим Сергеевич, Потехин Владимир Семенович, Саратов Дмитрий Николаевич
Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, ул. Летчика Пилютова, 1,
emails: cala4yov.maks@yandex.ru, vsp1945@gmail.com, saratovdn@mail.ru

Аннотация: Излагается подход, позволяющий адаптировать типовые решения, рекомендованные к использованию при проектировании систем контроля управления доступом (СКУД) на особо важные объекты МВД России. Учитываются новые угрозы, выявленные за время эксплуатации СКУД, разработанных ранее.

Ключевые слова: *система контроля управления доступом, функциональные модели СКУД, алгоритмы СКУД, адаптация типовых решений.*

APPROACH TO ADAPTATION OF TYPICAL SOLUTIONS AT THE DEVELOPMENT OF THE ACCESS MANAGEMENT CONTROL SYSTEM FOR SPECIAL IMPORTANCE OBJECTS

Kalachev Maksim, Potekhin Vladimir, Saratov Dmitrij
St. Petersburg University at Russian Ministry of internal Affairs (MIA),
Russia, St. Petersburg, Pilot Pilyutov str., 1,
emails: cala4yov.maks@yandex.ru, vsp1945@gmail.com, saratovdn@mail.ru

Abstract: The An approach, allowing to adapt the typical solutions, which recommended for use in the design of access management control systems (AMCS) for the most important objects of the Ministry of Internal Affairs of Russia, is presented. New threats detected during the operation of the AMCS developed earlier are taken into account.

Keywords: *the control system of access management, functional models of AMCS, AMCS algorithms, adaptation of typical solutions.*

Введение. Проникновение на объекты особой важности системы МВД России весьма привлекает террористов тем, что может привести к тяжким последствиям не только в масштабе охраняемого объекта, но и региона, и даже страны. Именно поэтому преступники пытаются применять все новые и новые средства и способы, способствующие реализации их преступных замыслов. В свою очередь государственные структуры, включая МВД России, вынуждены постоянно адаптировать (совершенствовать) средства и приемы защиты объектов. Поэтому тема данной работы, направленная на адаптацию типовых решений, используемых при разработке систем управления контролем доступом (СКУД), обречена на актуальность.

Для обеспечения должной адаптации (к изменяющимся условиям) типовых решений, рекомендованных руководством [1], разработанным НИЦ «Охрана» МВД России, при проектировании каждой новой СКУД представляется целесообразной следующая последовательность выполнения работ:

- изучить уже используемые типовые системные и технические решения построения систем контроля управления доступом [1], а также требования, предъявляемые основными руководящими документами [2], [3] и [4];
- проанализировать выявленные новые средства и способы, которые преступники предполагают использовать, противодействуя СКУД, и сформулировать новые угрозы;
- проанализировать возможности современной номенклатуры преграждающих управляемых устройств, включая простые и укрепленные двери, калитки, трехштанговые турникеты (триподы), полуростовые, полноростовые турникеты, автоматизированные проходные, шлюзовые кабины (тамбур-шлюзы) [5], [6] и [7];
- выполнить анализ возможностей устройств, обеспечивающих ввод идентификационных признаков в виде карт, брелоков, браслетов, меток, биопараметров человека, которые служат для определения прав владельца [8];
- скорректировать функциональные модели, которые использовались ранее в созданных СКУД, учтя опыт их эксплуатации и новые угрозы [9], [10], [11], [12];
- построить поведенческие модели (алгоритмы), обеспечивающие не только учет полномочий лиц, допущенных на объект, но и алгоритмы, обеспечивающие доступ на объект в условиях выбранных преграждающих управляемых устройств и устройств, обеспечивающих ввод идентификационных признаков [13]. При этом должна обеспечиваться визуализация информации состояния в принятой системе обозначений, которая предоставляется личному составу охраны на пультах контроля или автоматизированные рабочие места (АРМы). Причем должно быть обеспечено автоматическое протоколирование всех существенных действий личного состава объекта, применяемых аппаратно-программных средств при использовании ИТ с целью последующего анализа и выявления «узких мест»

системы охраны объекта. Кроме того, должна обеспечиваться возможность дистанционной передачи командной информации на исполнительные механизмы контролируемых объектов на основе современных средств коммуникаций (в частности, локальной вычислительной сети), позволяющих интегрировать перечисленные компоненты в единую систему защиты объекта;

– предусмотреть создание резервной схемы защиты, обеспечивающей достаточный уровень дублирования основных элементов охраняемого объекта (включая источники резервного питания).

В заключение заметим, что, по мнению авторов, выполнение перечисленных работ позволит поддерживать рассмотренную информационную технологию на приемлемом уровне и тем самым обеспечивать решение задачи охраны особо важных объектов с помощью СКУД в условиях появляющихся новых угроз.

СПИСОК ЛИТЕРАТУРЫ

1. Р 78.36.018-2011. Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности. НИЦ «Охрана» МВД России, 2011. [Электронный ресурс] URL: <http://docs.cntd.ru/document/1200102115> (дата обращения 13.09.2017).
2. Р 50-34. 126-92. Рекомендации. Информационная технология. Правила проведения работ по созданию автоматизированных систем. М.: "Издательство стандартов", 1993.
3. ГОСТ Р 52435-2005: Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний [Электронный ресурс]. URL: https://ohranatruda.ru/ot_biblio/normativ/data_normativ/46/46831/index.php#48320 (дата обращения 13.09.2017).
4. Национальный стандарт РФ ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний (утв. приказом Федерального агентства по техническому регулированию и метрологии от 17 декабря 2008 г. N 430-ст). [Электронный ресурс]. URL: <http://www.vashdom.ru/gost/51241-2008/#13560> (дата обращения 13.09.2017).
5. Система контроля и управления доступом // Википедия. [Электронный ресурс]. URL: <http://ru.wikipedia.org/?oldid=84466477> (дата обращения: 13.09.2017).
6. Тамбуры-шлюзы // ООО «ТЕХЗАЩИТА». [Электронный ресурс] URL: <http://www.radiosonar.ru/tourniquet/tourniquetnov1.html> (дата обращения: 13.09.2017).
7. Шлюз на базе двух дверей // ООО «ЕС-пром». [Электронный ресурс] URL: <http://www.trevog.net/decisions/passport/1529/> (дата обращения: 13.09.2017).
8. Мальцев А. Современные биометрические методы идентификации // Хабрахарб [Электронный ресурс] URL: <https://habrahabr.ru/post/126144/> (дата обращения 13.09.2017).
9. Горбаченко В. И., Убиенных Г. Ф., Бобрышева Г. В. Создание функциональной модели информационной системы с помощью CASE-средства CA ERwin Process Modeler 7.3. – Пенза: ПГУ, 2010. – 66 с. [Электронный ресурс]. <http://window.edu.ru/resource/658/72658/files/stup552.pdf> (дата обращения 13.09.2017).
10. Горохов А. Ю. Теория информационных процессов и систем // ПНИПУ. [Электронный ресурс] URL: http://vmm.pstu.ru/index.php?option=com_content&view=article&id=375&Itemid=224 (дата обращения 13.09.2017).
11. Дубейсковский В. И. Практика функционального моделирования с AllFusion Process Modeler 4.1. Где? Зачем? Как? М.: Изд. Диалог-МИФИ, 2008 – 464 с. ISBN 5-86404 192-0.
12. Маклаков С. В. Моделирование бизнес-процессов с AllFusion PM. 2-е изд., испр. и дополн. М.: Изд. Диалог-МИФИ, 2008. 224 с. ISBN 5-86404-179-3.
13. ГОСТ 19.701-90 (ИСО 5807-85). Единая система программной документации. Схемы алгоритмов, программ, данных и систем. Условные обозначения и правила выполнения. М.: "Издательство стандартов", 1991.

УДК 347.78: 023.1

О ПРАВОВЫХ АСПЕКТАХ ЭЛЕКТРОННОЙ БИБЛИОТЕКИ

Кононов Олег Александрович, Кононова Ольга Васильевна
Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Россия, Санкт-Петербург, ул. Большая Морская, 67,
emails: o2kon@mail.ru

Аннотация: В статье рассмотрены актуальные вопросы организации работы электронных библиотек в части регулирования правовых отношений авторов, издателей, библиотекарей и пользователей.

Ключевые слова: электронная библиотека; правовые аспекты; информационные ресурсы; информационно-коммуникационные технологии.

ABOUT LEGAL ASPECTS OF ELECTRONIC LIBRARY

Oleg Kononov, Olga Kononova
Saint-Petersburg State University of Aerospace Instrumentation,
Russia, Saint-Petersburg, Bolshaya Morskaya street 67,
e-mails: o2kon@mail.ru

Abstract: In article topical issues of the organization of work of electronic libraries regarding regulation of legal relations of authors, publishers, librarians and users are considered.

Keywords: electronic library; legal aspects; information resources; information and communication technologies.

Введение. Сегодня, благодаря развитию информационных технологий и средств телекоммуникаций повышается мобильность обновления и доставки информации, и, прежде всего, технической, библиографической, учебной, научной и т.п. к субъектам профессиональной деятельности. Поэтому библиотека постепенно превращается из хранилища знаний в информационный центр, способный не только предоставлять потенциальным пользователям и читателям целесообразно организованную информацию из книг, учебников, монографий и периодических изданий, но и обеспечивать доступ к гипертекстовым обучающим и контролирующим системам, полнотекстовым документам, видео- и аудиодокументам, а также к оперативной информации внутри организации или учебного заведения [1].

Расширение функций библиотек, достигаемое за счет использования средств вычислительной и телекоммуникационной техники, позволяет:

- оперативно обновлять фонды справочной, научной, технической, и учебной литературы, особенно в таких быстро развивающихся отраслях науки и техники, как электроника, биотехнологии, информатика и др.;

- обеспечивать читателей информацией в режиме удаленного доступа, что особенно важно, например, при организации всех форм дополнительного, послевузовского и очно-заочного образования;

- экономить средства, затрачиваемые на выпуск, закупку и хранение больших тиражей литературы, например, научной или учебной;

- обеспечивать кооперативный доступ к максимально широкому спектру любых периодических изданий.

Электронная библиотека должна опираться на открытость архитектуры, поддержку сетей, надежность, защищенность, простоту, удобство работы читателей и работников библиотеки, а также на возможность подключения к российскому и международному библиотечному пространству [1].

Развитие информационных ресурсов в библиотеках, музеях, архивах, способствующих созданию и использованию электронных документов, автоматизированных информационных центров, электронных библиотек, служб электронной доставки документов, доступных через электронную почту, через глобальные телекоммуникационные системы и сеть Интернет происходит в условиях, когда правовое обеспечение не соответствует потребностям общества. В этой ситуации библиотеки, музеи, архивы, с одной стороны, обязаны соблюдать права авторов произведений, с другой, обеспечить широкое использование их произведений в целях образования, просвещения и научной деятельности читателей и посетителей. Эти вопросы постоянно возникают в повседневной деятельности этих учреждений и имеют юридический и практический характер.

Правовая основа функционирования электронных библиотек заложена в соответствующих законах Российской Федерации. Создание электронной библиотеки, обслуживание пользователей электронными ресурсами предусмотрено в Федеральном законе «О библиотечном деле». Отдельные аспекты, связанные с созданием и использованием электронными библиотеками входящих в них баз данных, электронных каталогов и картотек, регулирует Федеральный закон «Об информации, информатизации и защите информации» [2].

Процесс разработки и совершенствования соответствующих правовых актов значительно отстает от бурного развития и внедрения новых информационных технологий и не позволяет зачастую библиотекам оперативно решать возникающие вопросы. Поэтому российские библиотеки самостоятельно разрабатывают локальные нормативно-правовые документы, обеспечивающие защиту деятельности электронных библиотек. При этом в структуру правового регулирования, наряду с действующими федеральными законами, активно включаются следующие внутренние нормативно-правовые акты: организационные, технические, технологические, методические и инструктивные документы, а также концепции создания электронных библиотек. Каждая библиотека подходит к составлению этих документов, исходя из целей и задач электронной библиотеки, ее структуры, содержательного и программного обеспечения.

Особую актуальность приобретают отношения, возникающие между создателем информации, библиотекой, имеющей права на предоставление этой информации, и пользователем. Эти отношения регулируются действующими ГОСТами, ОСТами, стандартами предприятий по библиотечному делу и информации, внутренними технологическими и методическими документами.

Урегулирование правоотношений, касающихся авторских прав и предоставления пользователям электронных текстовых документов, библиотеки решают на основе авторских договоров или лицензионных соглашений.

Однако, при решении этих вопросов важна роль государства в установлении правильного правового режима регулирования отношений, который стимулировал бы создание произведений авторами и обеспечивал бы их широкое распространение в обществе, в том числе и через библиотеки, т.е. удовлетворял бы интересы авторов, издателей, библиотекарей и пользователей. Поэтому дальнейшее совершенствование законодательства по получению и использованию информации через электронные библиотеки должно проводиться комплексно во взаимодействии и взаимопонимании всех проблем, гармонизации с национальным и международным законодательством в соответствии с

развитием средств телекоммуникации, современными достижениями науки и техники, с учетом особенностей информатизации общества.

Заключение. Таким образом, сегодня особую актуальность приобретают вопросы организационно-правового обеспечения конкретных направлений функционирования электронных библиотек, освоение специалистами библиотечно-информационных служб обширного массива законодательных и иных нормативных актов, регулирующих оптимальные формы взаимоотношений и взаимодействия с пользователями и партнерами.

СПИСОК ЛИТЕРАТУРЫ

1. Кононов О.А. Кононова О.В., Попенко Н.В. Правовые вопросы электронной библиотеки. VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013)»: материалы конференции. – СПб.: СПОИСУ, 2013. С.32.
2. Кононов О.А. Кононова О.В. О правовых вопросах использования информационных технологий. Актуальные проблемы экономики и управления. Научный журнал. – СПб.: ГУАП, 2016, №3(11), С.97-103.

УДК 004.773.3: 174

ОБ ЭТИКЕ ЭЛЕКТРОННОЙ ПЕРЕПИСКИ

Кононов Олег Александрович, Кононова Ольга Васильевна
Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Россия, Санкт-Петербург, ул. Большая Морская, 67,
emails: o2kon@mail.ru

Аннотация: В статье рассмотрены актуальные вопросы этики электронной переписки, показано её значение для установления и поддержки правильных взаимоотношений между участниками инфокоммуникационного взаимодействия.

Ключевые слова: этика; электронная почта; электронная переписка; информационно-коммуникационные технологии.

ABOUT ETHICS OF ELECTRONIC CORRESPONDENCE

Oleg Kononov, Olga Kononova
Saint-Petersburg State University of Aerospace Instrumentation,
Russia, Saint-Petersburg, Bolshaya Morskaya street 67,
emails: o2kon@mail.ru

Abstract: In article topical issues of ethics of electronic correspondence are considered, its value for establishment and support of the correct relationship between participants of infocommunication interaction is shown.

Keywords: ethics; e-mail; electronic correspondence; information and communication technologies.

Введение. Широкое использование инфокоммуникационных технологий в повседневной жизни, несомненно, влияет на социальную природу человека, социальную организацию общества, на его социальные коммуникации в части изменения и значительного роста роли социально-экономических отношений между субъектами инфокоммуникационного взаимодействия [1].

Следствием этого является изменение и значительный рост роли социально-экономических отношений между субъектами инфокоммуникационного взаимодействия таких областей социологии как социальный контроль, социальные нормы и санкции, агенты формального и неформального контроля, номенклатура, мафия, закрытая группа и ряд других областей [2].

Одним из наиболее распространенных способов инфокоммуникаций является электронная почта – первый и наиболее распространенный из сервисов Интернета.

Изобретателем электронной почты считается Рэй Томлинсон, соединивший в 1971 г. с помощью специальной почтовой программы пользователей удаленных компьютеров электронной сети «Aranet». Таким образом, уже в 70-е годы прошлого века были заложены основные возможности и механизмы работы электронной почты, которые совершенствуются и используются в современных почтовых программах и серверах.

Наряду со значительными достоинствами, такими как оперативность и легкость использования, доступность практически в любом месте, универсальность форматов писем и вложений, дешевизна сервиса, надежность и скорость доставки, электронная почта имеет и ряд недостатков [2]:

- привязка к домену почтового портала и невозможность получения желательного и запоминаемого адреса;
- ограничение объема почтового ящика или объема пересылаемого сообщения;
- негарантированное время пересылки электронного сообщения и самой доставки;
- наличие зачастую большого количества спама;
- опасность поступления вирусов;
- возможность несанкционированного доступа третьих лиц;

- не интерактивность;
- и другие.

К счастью за прошедшие десятилетия накоплен богатый опыт борьбы с различными видами мошенничества при использовании электронной почты.

В то же время при подготовке электронного письма существуют определенные правила этикета, которые регламентируются «сетикетом» и обеспечивают достоверное понимание передаваемой информации и эффективность ее использования [3].

Главное правило «сетикета», такое же, как и в любом другом этикете: ведите себя так, чтобы вас было легко понять, не создавайте проблемы другим и не мешайте нормальному диалогу. Всегда следует вести себя так, чтобы не обидеть человека, с которым ведется переписка по Интернету. Правила «бизнес-сетикета» появились как руководство для установления и поддержки правильных взаимоотношений между коммерческой деятельностью и ее клиентами.

При всей неформальности электронного общения необходимо помнить и выполнять одно из самых важных правил при составлении электронных писем – соблюдение принципов грамотности и логичности. Тот факт, что электронная почта – быстрый способ связи, вовсе не означает, что она должна быть небрежной.

Заключение. В докладе рассматриваются вопросы этики электронной переписки, определяющие стиль общения, оформление электронного письма, размер электронного письма, использование адресной книги, ответ на электронное сообщение, применение смайликов и электронной подписи.

СПИСОК ЛИТЕРАТУРЫ

1. Кононов О.А. Кононова О.В. О правовых вопросах использования информационных технологий. Актуальные проблемы экономики и управления. Научный журнал. СПб.: ГУАП, 2016, №3(11), С.97-103.
2. Кононов О.А. Кононова О.В., Попенко Н.В. Правовое обеспечение электронной почты. VIII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013)»: материалы конференции. – СПб.: СПОИСУ, 2013. С.33.
3. Кононов О.А. Кононова О.В., Попенко Н.В. Об этике электронной почты. XIII Санкт-Петербургская международная конференция «Региональная информатика – 2014 (РИ-2014)»: материалы конференции. – СПб.: СПОИСУ, 2014. С.403-404.

УДК 004.056

ПОДХОДЫ К ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

Костюк Анатолий Владимирович

Санкт-Петербургский военный институт войск национальной гвардии Российской Федерации
Россия, Санкт-Петербург, улица Летчика Пилютова, 1,
email: kostyuk.anatoliy.2015@mail.ru

Аннотация: В статье рассмотрены проблемы информационно-психологической безопасности личности в условиях информатизации общества. Анализируются два подхода к пониманию информационно-психологической безопасности личности. Формулируются задачи информационного и психологического образования в сфере информационно-психологической безопасности личности.

Ключевые слова: *информационно-психологическая безопасность личности, подходы и задачи информационно-психологической безопасности личности.*

APPROACHES TO INFORMATION-PSYCHOLOGICAL SECURITY OF THE PERSON

Kostyuk Anatoliy

St. Petersburg military institute of troops of national guard of the Russian Federation
Russia, St. Petersburg, Pilot Pilyutov Street, 1,
email: kostyuk.anatoliy.2015@mail.ru, sbobon@mail.ru

Abstract: The article considers the problems of information and psychological security of an individual in the context of informatization of society. Two approaches to understanding the information-psychological security of an individual are analyzed. The tasks of information and psychological education in the field of information and psychological security of the individual are formulated.

Keywords: *information-psychological security of the person, approaches and tasks information-psychological security of the person.*

Современное общество в эпоху информатизации характеризуется существенной зависимостью его естественного функционирования и тенденций развития от созданной им же информационной среды, которая является сложным системным образованием.

Наибольшее влияние информационно-коммуникативные процессы оказывают на духовную сферу социума, создавая зачастую негативные последствия и деструктивные изменения в форме психоэмоциональной и социальной напряженности, ложных ориентаций и ценностей и т. п. [1]. Существенное влияние информационная среда оказывает также на эмоциональные составляющие и процессы во всех основных сферах общественной жизни.

Основной процессуальной составляющей информационной среды являются информационно-коммуникативные процессы, активно воздействующие на эмоциональные составляющие индивидуального, группового и массового сознания. Одной из характерных особенностей процессов, протекающих в информационной среде, является их динамизм.

Проблема информационной безопасности различных производственных, общественных, государственных объектов относится к сфере государственной политики и уже продолжительное время является актуальной как в теоретическом, так и в прикладном плане. Пересмотр приоритетов и акцентов в интерпретации проблемы безопасности и перенос их с интересов государства, которые воспринимались в отрыве от нужд и потребностей человека, на интересы самого человека поставил науку и практику перед необходимостью разработки совершенно нового аспекта этой проблемы – информационно-психологической безопасности личности [2,3].

В настоящее время в условиях информатизации общества все больше ученых и практиков выделяют данную проблему и отмечают необходимость ее разработки (В.Д. Аносов, Г.В. Грачев, А.К. Грязнов, Е.Л. Доценко, А.А. Жулин, М.Л. Князева, Т.И. Колесникова, В.Е. Лепский, И.К. Мельник, А.В. Непомнящий, Е.П. Прохоров, С.К. Рощин, Г.Л. Смолян, А.А. Стрельцов и др.).

В научной литературе информационно-психологическая безопасность (ИПБ) личности рассматривается как состояние защищенности ее психики от воздействия разнообразных информационных факторов, мешающих или затрудняющих создание и функционирование соответствующей информационно-ориентировочной основы жизнедеятельности человека в обществе, а также адекватной системы его персональных отношений к окружающему миру и самому себе [2].

Узловые источники угроз ИПБ по отношению к личности рассматриваются, в основном, как внешние и внутренние. К внешним угрозам следует отнести соответствующие воздействия разнообразных организаций и людей, средства массовой информации и пр. С этих позиций формирование информационно-психологической безопасности требует создание надлежащей системы противостояния по отношению к внешним угрозам. Такая система должна состоять из нормативно-правовой, организационной и технологической составляющих [4].

Внутренние источники угроз ИПБ личности лежат в самой биосоциальной природе психики человека, в особенностях ее формирования и функционирования [2], а также в индивидуально-личностных характеристиках человека (например, внушаемости, критичности, импульсивности). Наличие внутренних факторов, а также понимание того, что и внешние угрозы оказывают воздействие не напрямую, а посредством «преломления» через внутренний мир человека побуждает исследователей рассматривать человека не только как объекта, но и как субъекта личной безопасности.

Объективная неосуществимость уберечь человека от всех отрицательных информационно-психологических воздействий сдвигает «центр тяжести» проблемы обеспечения информационно-психологической безопасности личности на развитие ее «иммунитета» и устойчивости к таким воздействиям, что переводит эту проблему в психолого-педагогическую плоскость.

Информационно-психологическая безопасность определяется В.Е. Лепским как научно-практическое направление, которое сформировано для того чтобы обеспечить защищенность индивидуумов и сообществ от противозаконных информационных угроз и формирования информационной сферы, соответствующей задачам стимулирования и поддержки рефлексивного способа существования человека (группы) как субъекта жизни (деятельности) [5]. Две цели, разделенные автором с помощью союза «и», по сути, обозначают два подхода к пониманию информационно-психологической безопасности и, соответственно, к ее обеспечению.

Как следует из определений информационно-психологической безопасности личности, которые даются в работах Г.В. Грачева, И.К. Мельник, С.Ю. Решетиной, Г.Л. Смолян и др., проблема ИПБ личности подменяется проблемой ее защищенности от отрицательных информационно-психологических угроз. Психологическая защита личности трактуется как применение различных психологических средств и способов трансформации процессов информационно-психологического взаимодействия человека с информационной средой в целом для устранения и нейтрализации угрожающих факторов, способных нанести ему ущерб [2,5]. Следовательно, подготовка человека в области информационно-психологической безопасности должна быть нацелена на формирование мотивации, знаний и умений, которые обеспечили бы безопасность человека, и включала бы обучение личности знанию возможных опасностей, внешних и внутренних угроз, способов защиты, оказывала бы содействие в понимании потребности и возможности защиты, а также способствовала бы овладению необходимыми умениями. В границах данного подхода можно также предложить формы психологической подготовки специального назначения, в частности, тренинги, направленные на приобретение опыта противодействия информационно-психологическому воздействию.

Другой подход основан на понимании безопасности как состоянии жизнедеятельности человека, при котором не снижается во времени вероятность достижения им жизненных целей и обеспечивается его развитие [2]. С позиции данного подхода одним из основных условий ИПБ личности является наличие устойчивой системы жизненных ценностей и их осуществление.

Понятие «наличие» предусматривает знание и понимание себя, самоопределение, а понятие «осуществление» предполагает принятие себя, подлинность проявлений, реализацию своих отношений, смыслов, ценностей. Самоопределение, как процесс, предполагает осознание человеком своих целей, идеалов, личностных и физических свойств, творческое познание себя истинного, соотнесение своих возможностей и желаний с социальными нормами, построение личной ценностно-смысловой картины мира, а как результат – становление субъекта собственной жизни. С этих позиций обеспечение информационно-психологической безопасности личности есть развитие ее ценностно-смысловой сферы, субъектных качеств, поддержка процесса духовно-нравственного становления.

Эти идеи согласуются с общей направленностью современного образования, в частности, с тенденцией его гуманизации, а задачи этого процесса во многом совпадают с целями общего психологического образования. Последнее рассматривается нами как предметная отрасль образования, направленная на формирование базисной информационной и психологической культуры личности.

Задачи информационного и психологического образования в сфере ИПБ личности можно сгруппировать в три блока:

- 1) помощь растущему человеку в самопознании, формирование умений самоконтроля, саморегуляции, самоорганизации;
- 2) помощь в постижении своей системы ценностей, содействие процессу выработки индивидуального подхода к преодолению жизненных противоречий, выбора жизненной стратегии;
- 3) помощь в формировании взглядов, которые содействовали бы становлению положительного эмоционально-ценностного отношения к себе, другим людям, своей безопасности и саморазвитию.

Выделенные нами подходы не противоречат друг другу, а соотносятся как два уровня. Формируя отдельные стороны личности (знания, умения, эмоционально-ценностные отношения), способствующие ее защищенности (первый подход), мы переходим в обеспечении информационно-психологической безопасности личности от превентивных мер к профилактическим, а заботясь о развитии личности (второй подход) — от профилактических к созидательным. Как первый, так и второй подходы предполагают познание психологической реальности и реализуются в сфере специального и общего психологического образования соответственно.

Таким образом, можно сделать вывод о том, что решение теоретико-методологических и практических проблем психологического образования внесет существенный вклад в обеспечение информационно-психологической безопасности личности.

СПИСОК ЛИТЕРАТУРЫ

1. Костюк А.В., Бобонец С.А., Флегонтов А.В. Информационные системы и технологии. Информационные технологии. Базовый курс. Учебник. Часть 2.— СПб.: Изд. РГПУ им. А.И. Герцена, 2014. — 308 с.
2. Грачев Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. URL: <http://bookap.by.ru/psywar/grachev>. (дата обращения: 18.09.2017)
3. Бобонец С.А., Костюк А.В. Обеспечение безопасности электронного обучения // Направления и перспективы развития образования в военных институтах внутренних войск МВД России: материалы VII Международной научно-практической конференции: в 2 ч. / Изд-во НВИ войск национальной гвардии. — Новосибирск, 2017. — С.102-104 сЛызь Н.А., Непомнящий А.В. Безопасность как характеристика личности // Известия ТРТУ. Таганрог, 2002. № 5 (28). С. 168–173.
4. Костюк А.В., Бобонец С.А. Информационные технологии в науке и образовании. Часть 1. — Учебник. СПб.: Астерион, 2017.— 256 с.
5. Лепский В.Е. Информационно-психологическая безопасность субъекта в изменяющемся обществе /Индивидуальный и групповой субъекты в изменяющемся обществе. М., 1999. С.98-99.

УДК 37.062

ОСОБЕННОСТИ ПЕДАГОГИЧЕСКИХ КОММУНИКАЦИЙ В УСЛОВИЯХ ИНФОРМАТИЗАЦИИ ОБРАЗОВАНИЯ

Костюк Анатолий Владимирович, Бобонец Сергей Алексеевич
Санкт-Петербургский военный институт войск национальной гвардии Российской Федерации
Россия, Санкт-Петербург, улица Летчика Пилютова, 1,
emails: kostyuk.anatoliy.2015@mail.ru

Аннотация: В работе рассмотрены необходимость и возможность профессиональных педагогических коммуникаций в среде интернет. Проанализированы особенности коммуникаций при отсутствии непосредственного визуального контакта, выявлены особенности профессиональных педагогических коммуникаций и обусловлена необходимость формирования определенных ИКТ-компетенций для педагогов.

Ключевые слова: информационные и педагогические коммуникации; вербальная (языковая) коммуникация; ИКТ-компетенции для коммуникации.

PECULIARITIES OF PEDAGOGICAL COMMUNICATIONS IN THE CONDITIONS OF EDUCATION INFORMATIZATION

Kostyuk Anatoliy, Bobonets Sergey

St. Petersburg military institute of troops of national guard of the Russian Federation
Russia, St. Petersburg, Pilot Pilyutov Street, 1,
emails: kostyuk.anatoliy.2015@mail.ru, sbobon@mail.ru

Abstract: The paper considers the necessity and possibility of professional pedagogical communications in the Internet environment. Features of communications are analyzed in the absence of direct visual contact, features of professional pedagogical communications are revealed and the necessity of forming certain ICT competences for teachers is determined.

Keywords: *information and pedagogical communications; verbal (language) communication; ICT competence for communication.*

Современные коммуникационные технологии и среда интернета существенно расширили возможности коммуникаций в профессиональной области. Открытость, и демократизм интернет-взаимодействия с одной стороны обеспечивают [1], [2]:

- высокую скорость взаимодействия, образующую мобильную обратную связь с партнерами (при условии их активного участия во взаимодействии);
- расширение круга единомышленников не только в своей стране, но и за рубежом;
- дополнительные возможности преподавателям для удовлетворения своих информационно-образовательных и профессиональных потребностей;
- экспертную оценку своих публикаций и достижений, собственную оценку публикаций и достижений других участников взаимодействия в сети Интернет (самовыражение, самоутверждение, самореализация);
- возможность анонимного участия во взаимодействии (снятие страхов, фобий и других психопатических ограничений).

С другой стороны, профессиональное педагогическое взаимодействие посредством интернета с учетом особенностей сетевого этикета требуют ответственности за процесс и результат взаимодействия, поскольку оно подвергается публичной оценке и критике. Эти риски отрицательно влияют на мотивацию к взаимодействию. Как показывает анализ форумов, сайтов педагогических сообществ, интернет-семинаров и конференций, педагогическое сообщество в целом пока недостаточно готово к публичности и объективности на этой стадии [2], [3].

Участники профессионального педагогического взаимодействия посредством сети интернет могут иметь персонифицированные интернет-сервисы с различными потребительскими и технологическими характеристиками или общие для всех участников взаимодействия интернет-сервисы, предоставляемые со стороны организаторов информационного взаимодействия [3]. Поэтому при формировании пространства целей, конкретизации целей и задач следует учитывать особенности персонифицированных интернет-сервисов.

Особое значение для профессионального педагогического взаимодействия в сети интернет имеют медиалингвистические особенности сообщений. По сравнению с традиционным взаимодействием информационная (содержательная) и коммуникативная (процессуальная) составляющие взаимодействия в сети интернет являются более существенными [4].

В сети интернет как информационно-коммуникационной среде информационное взаимодействие зачастую сводится к обмену текстовыми сообщениями, поэтому основой взаимодействия является вербальная (языковая) коммуникация и преимущественно в письменной форме [4]. При взаимодействии средствами письменно-речевой коммуникации, реализуемой текстами сообщений электронной почты, чатов, содержанием веб-страниц и пр., существенным образом акцентируются различные роли пишущего, автора (отправитель, адресант) и читателя (получатель, адресат) [5]. При этом отсутствие непосредственного визуального контакта существенным образом изменяет процесс взаимодействия. Субъекты взаимодействия могут и не иметь личных контактов до взаимодействия, например, взаимодействие участников формируемого сетевого педагогического сообщества или взаимодействие сетевого педагога и сетевого обучающегося.

Отсутствие личного контакта затрудняет взаимодействие, так как достаточно сложно через письменную коммуникацию «спроектировать» личность, определить ее творческие и профессиональные интересы и психологические особенности. Отсутствие личного контакта, а в будущем и невозможность его установления, упрощает взаимодействие, поскольку снимает большинство существующих при реальном взаимодействии психологических барьеров.

Во втором случае, отсутствие личного контакта ограничивает степени свободы взаимодействующих и создает условия для более тонкой настройки на виртуального, но известного, адресата. Взаимопонимание между преподавателями, как правило, основывается на общности профессиональных интересов и проблем, причем последнее является наиболее существенным. Именно эти проблемы и их обсуждение инициируют обмен опытом.

В тоже время потребность установления взаимопонимания и предисловия взаимодействия между преподавателями и обучающимися актуализирует необходимость использования особенностей письменно-речевой коммуникации, принятой в молодежной среде.

Выделенные особенности педагогического взаимодействия в сети интернет обуславливают необходимость формирования определенных ИКТ-компетенций, которые в иных случаях соприкосновения с информационно-коммуникационными технологиями (ИКТ) или их применения в обучении не являются существенными (например, умения подготовить сообщение для различных категорий субъектов взаимодействия, умения использовать метафоры, сленг, паралингвистические приемы и т. д.). Эти и другие специальные ИКТ-компетенции необходимо формировать как у работающих в рамках повышения квалификации, так и у будущих педагогов.

СПИСОК ЛИТЕРАТУРЫ

1. Костюк А.В. Использование информационно-коммуникационных технологий для подготовки офицеров национальной гвардии // Направления и перспективы развития образования в военных институтах войск национальной гвардии Российской Федерации. / Сборник научных статей VIII Межвузовской научно-практической конференции с международным участием. 2017. С. 462-466.
2. Костюк А.В., Бобонец С.А. Информационные технологии в науке и образовании. Учебник. Часть 1.– СПб.: Астерион, 2017. – 256 с.
3. Костюк А.В., Бобонец С.А. Проблемы информационной безопасности в технологиях дистанционного обучения / Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 2 / СПОИСУ. – СПб., 2016. – 491 с. (стр. 100-102)
4. Бобонец С.А., Костюк А.В. Информационно-образовательная среда как фактор повышения эффективности образовательного процесса. // В сборнике: Эффекты реализации исследовательских проектов в военных институтах внутренних войск материалы научно-методического семинара. Санкт-Петербургский военный институт внутренних войск МВД России. 2016. С. 74-78.
5. Костюк А.В., Бобонец С.А. Информационное обеспечение образовательного процесса. Научный альманах. 2016. № 5-2 (19). ООО «Консалтинговая компания Юком» С. 165-168.

УДК 004.056

ОРГАНИЗАЦИОННЫЕ СТРУКТУРЫ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Костюк Анатолий Владимирович, Бобонец Сергей Алексеевич
Санкт-Петербургский военный институт войск национальной гвардии Российской Федерации
Россия, Санкт-Петербург, улица Летчика Пилютова, 1,
emails: kostyuk.anatoliy.2015@mail.ru, sbobon@mail.ru

Аннотация: В работе рассмотрены важнейшие виды структур учреждений (организаций), их влияние на информационную безопасность, управление в функциональной организационной структуре, а также сделаны выводы по применимости этих структур в организациях различного типа.

Ключевые слова: *информационная безопасность, типы организационных структур, управление в организационной структуре, информационная безопасность организации.*

ORGANIZATIONAL STRUCTURES AND INFORMATION SECURITY

Kostyuk Anatoliy, Bobonets Sergey
St. Petersburg military institute of troops of national guard of the Russian Federation
Russia, St. Petersburg, Pilot Pilyutov Street, 1,
emails: kostyuk.anatoliy.2015@mail.ru, sbobon@mail.ru

Abstract: The paper considers the most important types of institutions (organizations) structures, their impact on information security, management in the functional organizational structure, and also draws conclusions on the applicability of these structures in organizations of various types.

Keywords: *information security, types of organizational structures, management in the organizational structure, information security of the organization.*

Необходимость и важность решения вопросов информационной безопасности в настоящее время осознается как обществом, так и гражданами. В первую очередь проблемы информационной безопасности затрагивают юридических лиц, учреждения и организации.

Проведенный анализ показывает, что структурная организация управления оказывает существенное влияние на информационную безопасность организации в целом. В зависимости от характера связей между подразделениями организации различают следующие типы организационных структур: линейную, функциональную, штабную и матричную [1].

В линейной структуре каждое структурное подразделение возглавляется соответствующим руководителем, который наделен необходимыми правами и осуществляет единоличное руководство своими подчиненными. Он лично реализует все функции управления. Следовательно, вся ответственность за поступки подчиненных лежит на руководителе [2,3].

Основными достоинствами такого управления являются:

- один канал связи, что в конечном итоге снижает вероятность утечки информации;
- персональная ответственность руководителя, что способствует улучшению контроля выполнения мероприятий по информационной безопасности;
- высокая оперативность в принятии решений при выявлении каких-либо нарушений информационной безопасности.

Основными недостатками линейной структуры являются:

- высокая загруженность руководителя информацией, большое количество контактов с подчиненными и вышестоящими структурами, следовательно, с точки зрения обеспечения информационной безопасности руководитель является самым слабым звеном;
- сосредоточение власти в верхних ветвях системы управления может привести к выходу из строя всей ветви, следующей за ним, либо хищение практически всей информации по организации;
- загруженность каналов связи между инстанциями зачастую ведет к продолжительному или неполному обмену информацией.

Управление в функциональной организационной структуре реализуется некоторой группой подразделений, которые специализируются на выполнении конкретных видов работ, требуемых для принятия решения в системе линейного управления [3,4].

Основными преимуществами функциональной структуры с точки зрения ИБ являются:

- полная информация о деятельности организации (предприятия) сосредоточена только у руководителя в отличие от линейной системы;
- посредством изъятия процессов дублирования в реализации управленческих функций и обладании информацией снижается количества вероятных каналов утечки специализированной информации;
- стандартизация и формализация явлений и процессов, связанных с управлением организацией.

Основные недостатки:

- затруднения в реализации устойчивых взаимосвязей между разными функциональными службами, что приводит к затруднениям обмена информацией и снижению производительности;
- достаточно закостеневшая организационная форма, с трудом реагирующая на изменения (длительная процедура принятия решения);
- значительное число каналов связи, которые требуют защиты, как следствие увеличение расходов на обеспечение безопасности информации.

При штабной организационной структуре управления все полномочия по управлению сосредоточены у линейного руководителя, который возглавляет конкретный коллектив. Помощь руководителю в ходе разработки конкретных вопросов и подготовки соответствующих решений, оказывает специальный аппарат, который функционально состоит из нескольких подразделений [3].

Основными преимуществами штабной структуры с точки зрения ИБ являются:

- высвобождение главного линейного руководителя от глубокого анализа проблем,
- существенное повышение качества обработки специализированной информации и выработка более объективных решений, в сравнении с линейной и функциональной структурами;
- полная информация по организации сосредоточена преимущественно у главного руководителя, следовательно, число каналов возможной утечки информации существенно ограничено.

Основные недостатки:

- отсутствие информационно обмена и установившихся взаимосвязей между функциональными подразделениями или группами на горизонтальном уровне, что ведет к ухудшению работы организации, но повышает информационную безопасность;
- низкая персональная ответственность, поскольку разработчики решений, как правило, не принимают участие в его выполнении.

Формируемая в матричной структуре управления управляющая информация обеспечивает решение конкретной целевой задачи, в выполнении которой принимают участие все звенья организации. Структурно процесс управления по вертикали базируется на отдельных сферах деятельности организации (производство, сбыт и т.д.). По горизонтали процесс управления базируется на управлении проектами, темами и т.д. Поэтому руководитель проекта преимущественно устанавливает, что и когда должно быть сделано по конкретной программе и сотрудничает не со специалистами, которые структурно подчинены не ему, а линейным руководителем. В дальнейшем линейные руководители принимают решение, кто и как будет исполнять ту или иную работу [3,5].

Основными преимуществами матричной структуры с точки зрения ИБ являются:

- высокая оперативность реагирования на изменяющиеся условия (устойчивость работы);
- целесообразное применение кадрового ресурса за счет специализации разных видов деятельности;
- усиление контроля над важными задачами проекта;
- увеличение персональной ответственности за реализацию программы в целом и ее элементов.

Основные недостатки:

- децентрализация управления, передача ряда полномочий вышестоящих руководителей нижестоящим;
- сложная структура соподчинения (возможность противоречий между приоритетами заданий, противоречий между управляющими инстанциями),

— наличие значительного количества возможных каналов утечки информации за счет большого количества связей в организации.

Штабная структура повышает производительность организации и уменьшает возможность утечки информации. Матричная структура, повышая производительность организации, вызывает рост числа каналов утечки информации, а, следовательно, и ухудшает состояние ИБ организации. Матричная структура более предпочтительна для крупных организаций, которые смогут выделить средства на комплексное решение задач обеспечения ИБ и обеспечения безопасности каналов связи.

Линейная структура для таких организаций не пригодна, так как в этом случае необходимо наличие значительного числа универсальных управляющих, которые потенциально опасны как каналы утечки информации. В тоже время для небольших организаций линейная структура экономически более выгодна. И для таких организаций вопрос ИБ и безопасности информации стоит не так остро, как для крупных предприятий. Следовательно, для малых организаций целесообразно применение линейной структуры управления.

СПИСОК ЛИТЕРАТУРЫ

1. Типы организационных структур, их характеристика. URL: http://www.e-reading.club/chapter.php/97486/46/Mihaleva_-_Menedzhment_konspekt_lectiii.html (дата обращения: 12.09.2017)
2. Костюк А.В., Бобонец С.А., Флегонтов А.В. Информационные системы и технологии. Информационные технологии. Базовый курс. Учебник. Часть 2. – СПб.: Изд. РГПУ им. А.И. Герцена, 2014. – 308 с.
3. Костюк А.В., Бобонец С.А. Анализ влияния типов организационных структур на информационную безопасность. // В сборнике: Региональная информатика и информационная безопасность. Сборник трудов. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. 2016. С. 102-104.
4. Бобонец С.А., Костюк А.В. Обеспечение безопасности электронного обучения // Направления и перспективы развития образования в военных институтах внутренних войск МВД России: материалы VII Международной научно-практической конференции: в 2 ч. / Изд-во НВИ войск национальной гвардии. – Новосибирск, 2017. – С.102-104 с.
5. Костюк А.В., Бобонец С.А. Синтез структуры межсетевого экрана // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 2 / СПОИСУ. – СПб., 2016. – 491 с.

УДК 681.3.067

РАЗРАБОТКА ТРЕБОВАНИЙ К ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В СРЕДСТВАХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Куватов Валерий Ильич, Примакин Алексей Иванович
Санкт-Петербургский университет МВД России,
emails: kyb.valery@yandex.ru, a.primakin@mail.ru

Аннотация: Рассматривается задача формирования требований к конфиденциальности, целостности и доступности данных в системе защиты информации средств вычислительной техники и автоматизированных систем. Показано, что для решения этой задачи может быть использован метод анализа иерархий и кластерный анализ. Разработана методика решения этой задачи.

Ключевые слова: конфиденциальность; целостность; доступность; защита информации; матрица парных сравнений; собственное число; собственный вектор.

MODEL FOR FORMATION OF REQUIREMENTS FOR CONFIDENTIALITY OF INTEGRITY AND ACCESSIBILITY OF DATA IN THE SYSTEM OF INFORMATION PROTECTION OF MEANS OF COMPUTER ENGINEERING AND AUTOMATED SYSTEMS

Kuvatov Valery Ilyich, Primakin Alexey Ivanovich
St. Petersburg University of the Ministry of Internal Affairs of Russia,
Russia, St. Petersburg, st. pilot Pilutov, 1,
emails: kyb.valery@yandex.ru, a.primakin@mail.ru

Abstract: Considers the problem of formation of requirements to the confidentiality, integrity and availability of data in the system of information security of computer equipment and automated systems. It is shown that for solutions of this task can be used analytic hierarchy process and cluster analysis. The developed method of solving this problem.

Keywords: confidentiality; integrity; availability; data protection; matrix of paired comparisons; eigenvalue; eigenvector.

Введение. Проблема обеспечения информационной безопасности средств вычислительной техники (СВТ) и автоматизированных систем (АС) становится все более и более важной. Поэтому раздел теории информационной безопасности, направленный на разработку систем защиты информации в СВТ и АС, является одним из наиболее востребованных.

Основная часть. Наибольшую сложность при разработке системы защиты информации в СВТ и АС представляет задача формирования требований к защите каждого вида используемой в системе конфиденциальной информации, ее носителей и процессов обработки. Классический подход к решению этой задачи основан на учете только одного свойства безопасности информации – ее

конфиденциальности. Такой подход правомерен, если важность конфиденциальности много выше важности целостности и доступности. В общем случае это не всегда так. Иногда важнейшими могут быть такие качества как целостность или доступность.

Современный подход [1] предполагает, наряду с требованиями по обеспечению конфиденциальности информации, формирование требований по обеспечению целостности и доступности информации (последнее – только для санкционированных пользователей). Для каждого типа требований разрабатывается несколько уровней. Порядок определения уровня принято описывать следующим образом:

1. Данные делятся на типы по тематике, по функциональному назначению, по одинаковости информационных технологий и др. признакам.

2. Для каждого типа данных и каждого свойства безопасности определяются: 1) перечень и важность субъектов (важность незначительная, малая, средняя, высокая, очень высокая), интересы которых затрагиваются при нарушении данного свойства безопасности информации; 2) уровень наносимого ущерба (незначительный, малый, средний, большой, очень большой) и соответствующий уровень требований к защищенности.

3. Для каждого типа информации с учетом значимости субъектов и уровней наносимого им ущерба устанавливается степень необходимой защищенности по каждому из свойств безопасности информации. В качестве уровней защищенности могут выступать: отсутствие требований по данному свойству, низкий, средний, высокий, очень высокий уровень требований. При равенстве значений для разных субъектов, в итоге выбирается максимальное значение уровня. Наиболее важный недостаток такого подхода связан с использованием ранговой шкалы для оценки величины каждого свойства [2]. Методы, изложенные в докладе, позволяют в значительной степени устранить этот недостаток.

В докладе изложен:

– метод сравнительной оценки важности субъектов, важности показателей конфиденциальности, целостности и доступности информации для каждого из субъектов;

– метод разделения субъектов информационных отношений на классы с одинаковыми требованиями к конфиденциальности, целостности и доступности информации.

В идейном отношении метод базируется на схеме анализа иерархий [3] и кластерном анализе [4]. С помощью метода анализа иерархий для каждого субъекта формируется вектор, компонентами которого являются: важность субъекта и требования к конфиденциальности, целостности и доступности информации каждого типа, используемой данным субъектом. С помощью кластерного анализа множество субъектов делится на классы, каждый из которых характеризуется близкими значениями важности конфиденциальности, целостности и доступности информации каждого типа.

Заключение. Метод анализа иерархий позволяет в данном случае получать более объективные экспертные оценки, чем оценки, получаемые другими методами, а кластерный анализ – делить множество субъектов на классы близкие по требованиям конфиденциальности, целостности и доступности информации.

СПИСОК ЛИТЕРАТУРЫ

1. М. А. Борисов, И. В. Заводцев, И. В. Чижов. Основы программно-аппаратной защиты информации. — М.: URSS, 2015 — 412 с.
2. Куватов В. И., Синешук Ю. И., Синешук М. Ю. Проблемы выбора рационального состава системы защиты информации. // Труды Юбилейной XV Санкт-Петербургской международной конференции «Региональная информатика «РИ-2016». С. 219-220.
3. Куватов В. И., Величко Г. А. Исследование операций. – Петродворец: ВВМУРЭ, 2005 – 425 с.
4. Неслухов Д.С. Использование кластерного и регрессионного анализа в изучении экономической деятельности судостроительных и судоремонтных предприятий //Интернет-журнал «НАУКОВЕДЕНИЕ» Том 8, №4 (2016) <http://naukovedenie.ru/PDF/78EVN416.pdf> (доступ свободный).

УДК 342.51, 341.1

ПРЕСТУПЛЕНИЯ В ОБЛАСТИ ИТ-ИНФОРМАТИЗАЦИИ В РОССИИ И МИРЕ

Лядов Алексей Олегович, Евсеев Алексей Викторович

Санкт-Петербургский университет технологий управления и экономики,
Россия, 190103, г. Санкт-Петербург, Лермонтовский проспект, 44, литер А
emails: lyadov-62@mail.ru avespb@gmail.com

Аннотация: в статье представлен обзор определений и составов преступлений в области информационной и коммуникационной инфраструктуры; утверждается необходимость совершенствования законодательства в данной области на основе новейшей официальной концепции 2017 года и ее проработки научно-экспертным сообществом.

Ключевые слова: право, государство, современная Россия, IT-технология, компьютерная информация, юридическая сфера, правонарушение, юридическая ответственность

ABOUT THE THEORETICAL UNDERSTANDING OF LEGAL REGULATION IN THE FIELD OF IT INFORMATIZATION

Lyadov Aleksey, Evseyev Aleksey

Saint-Petersburg University of Management Technologies and Economics

Russia, 190103, Saint-Petersburg, Лермонтовский проспект, 44, литер А

emails: lyadov-62@mail.ru, avespb@gmail.com

Abstract: the article presents an overview of the definitions and offences in the field of information and communication infrastructure; the need to improve legislation in this area based on the latest official concept, 2017 and development of the scientific-expert community.

Keywords: law, state, modern Russia, IT-technology, computer information, legal sphere, offence, legal responsibility

Наличие в России и мире компьютерных правонарушений, в частности, кибер-преступности, берет свое начало с 1990-х годов и за последние десятилетия остается довольно устойчивым трендом, демонстрируя при этом свое качественное развитие. Существенными являются не только социальные и экономические потери, но и политические риски, исходящие от кибер-атак. Неслучайно Правительство США отчаянно противодействует разоблачениям, которые публикуются на сайте <https://wikileaks.org/>. В России еще в 2011 г. доморощенные хакеры сумели временно заблокировать сайты Президента и Правительства РФ. При этом кибер-атаки происходят в самых разнообразных формах: блокировки правительственных веб-сайтов, перенаправления URL, DDos-атаки, кражи или подлоги компьютерной информации и т.д. В последние 10-12 лет кибер-преступления с политическими целями зачастую организуются и проводятся на государственном уровне, приобретая характер кибер-шпионажа, либо становятся средством ведения настоящих информационных войн - "кибер-оружием".

В ответ на эти реальные угрозы национальной безопасности России Президент РФ еще в 2013 году издал Указ "О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации"[1], в соответствии с которым возложил на Федеральную службу безопасности РФ полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и за рубежом (посольства и консульства).

В международном праве известны несколько определений кибернетических преступлений.

На 10-м Конгрессе ООН по предупреждению преступности и обращению с правонарушителями были выработаны два определения. «Кибер-преступность в узком смысле («компьютерная преступность») – это любое противозаконное поведение в форме электронных операций, направленное против безопасности компьютерных систем и обрабатываемых ими данных. Кибер-преступность в более широком смысле («преступления, связанные с применением компьютеров») – это любое противозаконное поведение, осуществляемое посредством или в связи с компьютерной системой или сетью, включая такие преступления, как незаконное владение, предложение или распространение информации посредством компьютерной системы или сети.

В российском законодательстве нет легального определения для понятия «компьютерное преступление» («кибер-преступление»). Но есть гл. 28 («Преступления в сфере компьютерной информации») Уголовного кодекса РФ [2], которая содержит ряд составов компьютерных преступлений. Одновременно есть и иные составы, которые могут дополнять либо охватывать компьютерные правонарушения, например, ст. 159.6 («Мошенничество в сфере компьютерной информации»), ст. 205.2. («Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма»), ст. 285.3. («Внесение в единые государственные реестры заведомо недостоверных сведений»), и многие другие. После внесения изменений в нормативно-правовые акты, регулирующие деятельность средств массовой информации, необходимость соблюдения специальных требований, предназначенных ранее для традиционных СМИ (газеты, журналы, телевидение, радио), теперь была распространена и на сетевые издания, и на блогеров. При этом квалифицирующий признак объективной стороны преступления "совершение преступления с использованием средств массовой информации" распространился еще на 12 составов преступлений [2 ст. 137, ст. 185.3, ст. 205.2, ст. 228.1, ст. 242, ст. 242.1, ст. 280, ст. 280.1, ст. 282, ст. 354, ст. 354.1].

Однако перечень видов преступлений, связанных с компьютерами, на практике неуклонно растет. Это - и подставные сайты («фейки»), и удаление защиты с программного обеспечения («крекинг»), и незаконное пользование лицензионными программами и базами данных («пиратство»), и злонамеренная Интернет-реклама или ее рассылка на электронные почтовые адреса («черный пиар») и многие другие.

Конвенция Совета Европы о кибер-преступности [5 1.39] определила 4 вида компьютерных преступлений:

– ст. 2 (противоправный умышленный доступ к компьютерной системе либо ее части);

- ст. 3 (противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах);
- ст. 4 (противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных);
- ст. 5 (серьезное противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных).

Именно эти четыре вида преступлений являются собственно «компьютерными», остальные — это либо связанные с компьютером (computer-related), либо совершаемые с помощью компьютера (computer-facilitated) преступления.

Широкое распространение получила также уголовно-правовая классификация компьютерных преступлений по способу их совершения, принятая Генеральным Секретариатом Интерпола еще в 1991 г. [цит. по: 6 с. 96 - 98.]:

Вместе с тем, остаются и иные риски, которые несут в себе общественную опасность, но до сих пор не запрещены уголовными или административными законами в нашей стране. Так, Уполномоченный по правам человека в РФ в своем отчете за 2016 год [3] отмечает возрастающее число суицидов среди детей (в 2016 г. – 772 случая), ставших жертвами деятельности «групп смерти» в социальных сетях. В этом докладе также отмечается, что меры, провозглашенные в Концепции информационной безопасности детей [4], пока еще далеки от своего юридического закрепления и практического воплощения.

Обобщая вышесказанное, при квалификации компьютерных преступлений считаем целесообразным учитывать не только их общие признаки – место совершения правонарушения («информационно-коммуникационная инфраструктура»), способ и нанесенный вред («уничтожение, блокирование, модификация, копирование компьютерной информации или нейтрализация средств защиты»), но и характер последствий компьютерной преступности, затрагивающие уже не только частные, но и публичные интересы социума и государства. На этой основе мы предлагаем дополнить УК РФ новой статьей 274.1 с новым составом уголовного преступления, которая бы имела следующее содержание: «Создание, распространение или использование компьютеров, компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации в информационных и коммуникационных системах Российской Федерации, - наказывается лишением свободы - до 10 лет или, в случае наступления тяжких или особо тяжких последствий для безопасности личности, общества и/или государства - до 25 лет».

СПИСОК ЛИТЕРАТУРЫ

1. Указ Президента РФ от 15.01.2013 N 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // Собрание законодательства РФ, 2013, N 3, ст. 178.
2. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 17.04.2017) / URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 30.04.2017).
3. Доклад о деятельности Уполномоченного по правам человека в Российской Федерации за 2016 год // Российская газета, 2017, 17 мая / URL: <https://rg.ru/2017/05/17/doklad-dok.html> (дата обращения 13.06.2017).
4. Распоряжение Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р «Об утверждении Концепции информационной безопасности детей» / URL: <http://government.ru/media/files/mPbAMyJ29uSPhL3p20168GA6hv3CtBxD.pdf> (дата обращения 13.06.2017).
5. Европейская Конвенция по киберпреступлениям (преступлениям в киберпространстве). Будапешт, 23 ноября 2001 года / URL: <http://mvd.gov.by/main.aspx?guid=4603> (дата обращения 13.06.2017).
6. Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность / В.Д. Курушин, В.А.Минаев. - М.: Новый Юрист, 2012.- 216 с.

УДК 34.096

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ ОПЕРАТИВНО-РОЗЫСКНЫХ ТЕХНОЛОГИЙ В ПРОТИВОДЕЙСТВИИ ТЕРРОРИЗМУ

Нигметов Николай Александрович
Санкт-Петербургский университет МВД России
Россия, Санкт-Петербург, ул. Летчика Пилютова, 1
email: iamvladr@gmail.com

Аннотация. В статье автор рассматривает природу терроризма, нетрадиционные подходы и технологии по профилактике и выявлению данной преступной деятельности. Автор утверждает о необходимости использования специального программного обеспечения, применения аналитического поиска элементов террористической деятельности.

Ключевые слова: терроризм; нетрадиционные подходы, прогнозирование, специальное программное обеспечение, оперативно-аналитический поиск, компьютерные базы

PROBLEMS OF THE MODERN OPERATIVE-INVESTIGATIVE TECHNOLOGIES USING IN THE TERRORISM COUNTERACTION

Nigmatov Nikolay

The St. Petersburg University of the Ministry of the Internal Affairs,
Russia, St. Petersburg, letchika Pilyutova str. 1
email: iamvladr@gmail.com

Abstract: In the article the author researches the terrorism nature and non-traditional approaches and technologies of it's discovery and prevention. The author consider the necessity of the special program core and analytical methods to find terror activity salient features.

Keywords: *terrorism, non-traditional approaches, special program core, analytical methods.*

На основе раздела IX Уголовного кодекса Российской Федерации «Преступления против общественной безопасности и общественного порядка» [2], Федерального закона «О противодействии терроризму» [3] и ряда международных конвенций, касающихся проблемы борьбы с террористическими актами терроризм является одной из главных проблем современного общества.

Терроризм – «это идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устранением насилия и (или) иными формами противоправных насильственных действий» [6, стр.223].

Пленум Верховного Суда РФ в постановлении от 9 февраля 2012 г. № 1 определяет, что терроризм представляет угрозу международному миру и безопасности, развитию дружественных отношений между государствами, сохранению территориальной целостности государств, их политической, экономической и социальной стабильности, а также осуществлению основных прав и свобод человека и гражданина, включая право на жизнь [5]. Как правило, все действия, связанные с данным явлением, носят латентный, скрытый характер, поэтому их выявление документирование и дальнейшее использование для привлечения к ответственности лиц составляют достаточно сложный комплекс подготовки и проведения оперативно-розыскных мероприятий.

Оперативные подразделения органов внутренних дел осуществляют комплекс организационных, правовых, оперативно-розыскных и поисковых мероприятий, направленных на выявление, предупреждение и минимизацию вредных последствий очагов угрозы возникновения террористической опасности, а также своевременное пресечение любой террористической деятельности. Это подтверждает верность выбора негласных мер и современных оперативно-розыскных технологий в борьбе с данным видом правонарушений и обуславливает необходимость использования, разработки и реализация на практике современных теоретических моделей борьбы с данным видом преступности в ее новейших проявлениях, применение необходимых научно-технических возможностей.

Сущность использования нетрадиционных подходов в деятельности оперативных подразделений органов внутренних дел в борьбе с преступлениями террористической направленности включает в себя по мимо проведения оперативно-розыскных мероприятий и применение регистраторов психосоматического состояния; гипноза; нетрадиционных средств контроля за перемещением материальных ценностей; информационно-психологическое воздействие; создание и использование специальных предприятий; использование идентификационно-поисковых и диагностико-поисковых систем, основанных на мультимедийных компьютерных технологиях Важнейшим элементом успешного решения задач противодействия терроризму является прогнозирование – это познавательно-исследовательская деятельность субъектов управления и специализированных подразделений МВД, которые оперируют либо вероятностными закономерностями, либо категорически- определенной структурой закономерностей прошлого опыта, тенденциями, проблемными ситуациями, факторами, влияющими на криминальную ситуацию в будущем, обосновывают выводы, предлагают выбор наиболее эффективных форм, методов и средств реализации задач и принятия на этой основе управленческих решений по борьбе с преступлениями террористической направленности и планирование – целенаправленная мыслительная деятельность субъектов управления по выработке комплексных, обоснованных, реальных, динамичных оперативно-розыскных мероприятий организационно-управленческого (перспективные и текущие планы), организационно-тактического (планы комплексных операций, комплексные планы по борьбе с преступлениями террористической направленности), оперативно-тактического (планы по делам оперативного учета) характера, и иных оперативно-розыскных мероприятий гласного и негласного характера, выполняемая на основе анализа оперативной обстановки и складывающейся оперативной ситуации, изучения текущей информации о замышляемых, подготавливаемых, либо совершенных преступлениях или иных правонарушений с признаками террористической деятельности. С этой целью для выявления потенциальных источников оперативно значимой информации в деятельности оперативных подразделений органов внутренних дел может использоваться как универсальное, так и специальное программное обеспечение. Универсальные программы (информационно-поисковой системы, редакторы, электронные таблицы и т.п.) общего назначения не только повышают производительность труда и эффективность работы по выявлению, раскрытию и расследованию преступлений террористического характера, но и поднимают

ее на качественно новый уровень. Специализированные программы могут быть ориентированы на непосредственное их применение при осуществлении оперативно-розыскных мероприятий в направлении борьбы с преступлениями террористической направленности и выявлению лиц причастных к данному виду деятельности как непосредственно, так и опосредованно. При этом определённые программные продукты и так называемый оперативно-аналитический поиск позволяют:

- проводить оперативно-розыскной мониторинг;
- негласно применять специальное программное обеспечение и оборудование;
- определять индивидуальный почерк работы фигуранта (лицо причастное к террористическим проявлениям) и идентификационные характеристики разработанных им программ;
- определять перечень электронных адресов и сайтов Интернет, с которыми работал фигурант;
- негласно регистрировать перечень программ, с которыми работает фигурант;
- определять путь, а в некоторых случаях и конкретный адрес, исходящей угрозы;
- осуществлять негласный контроль над фигурантом, определяя характер разрабатываемых продуктов;
- обнаружить латентную и закодированную информации в компьютерной системе;
- проводить идентификацию компьютерных систем по следам применения на различных материальных носителях информации;
- осуществлять исследование следов деятельности фигуранта в целях его идентификации;
- исследовать материальные носители с целью поиска заданной информации;
- применять аналитическое программное обеспечение.

Оперативно-розыскной процесс состоит из превентивно-поискового этапа и трёх взаимообусловленных и одновременно достаточно самостоятельных стадий (проверка, разработка, контроль). На этапе оперативно-аналитического поиска существует возможность использования компьютерного моделирования для раскрытия преступлений в сфере террористической составляющей. Одним из перспективных направлений компьютерной инженерии является использование имитационных моделей. Такая модель предусматривает организацию информационных потоков внутри моделируемых систем, воспроизведение на компьютере операций подмены, перераспределения, взаимодействия между отдельными структурными элементами системы и поэтому является достаточно эффективным средством изучения и прогнозирования в том числе и преступлений террористической направленности.

По результатам оперативно-аналитического поиска в оперативных подразделениях целесообразно формировать компьютерные базы данных, используемые:

- для последующей оперативной проверки лиц, преступных групп и организаций; для проведения оперативной-профилактических мер;
- для проведения негласных методов и использования негласных сил в криминальной среде с целью углубления оперативных позиций, необходимых для успешного проведения так называемой стратегической разведки.

В оперативно-розыскной деятельности в области выявления и документирования преступлений в том числе с террористической окраской целесообразно применять и оперативно-криминологическое прогнозирование индивидуального или преступного группового поведения. Определённую информацию можно извлечь, анализируя сетевой трафик локальных и региональных компьютерных сетей. Полезную информацию могут дать и анализ платежей клиентов за услуги. Прогнозирование может успешно осуществляться в основе первичных материалов оперативного характера, так как его банки информации создаются на основе прогноза вероятности преступного поведения определённых контингентов. Все это в совокупности является элементами методики оперативного прогнозирования, которое вплетается в оперативно-розыскные мероприятия при реализации форм ОРД (поиске, профилактике, разработке). Естественно, вопросы моделирования и прогнозирования необходимо решать, используя современные технологии.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 12 августа 1995 года №144-ФЗ «Об оперативно-розыскной деятельности» (с изменениями от 6 июля 2016 года №374-ФЗ).
2. Федеральный закон от 3 апреля 1995 г. N 40-ФЗ «О федеральной службе безопасности» // «Собрание законодательства Российской Федерации» от 10 апреля 1995 г.
3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63 - ФЗ (принят Государственной Думой Федерального Собрания Российской Федерации 24.05.1996 г., редакция от 125.02.2012 г.) // «Собрание законодательства Российской Федерации», 17.06.1996 г.
4. Федеральный закон Российской Федерации от 6 марта 2006 г. N 35-ФЗ «О противодействии терроризму» от 10 марта 2006 г. в «Российская Газета» - Федеральный выпуск № 4014.
5. Федеральный закон № 321-ФЗ от 30.12.2008 года «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам противодействия терроризму» от 30.12.2008.
6. Постановление Пленума Верховного Суда Российской Федерации от 9 февраля 2012 г. N 1 г. Москва «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» // «Российская Газета» - Федеральный выпуск № 5708.
7. Тимченко А.А., Берекет В.М., Бородин С.С. «Административная деятельность органов внутренних дел»: учебное наглядное пособие // СПб ун-т МВД России, 2010.

УДК 004.056:61

**КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ
В СОВРЕМЕННЫХ УСЛОВИЯХ**

Парфенов Николай Петрович, Алексеев Сергей Алексеевич
Санкт-Петербургский университет МВД России «СПБУ МВД России»,
Россия, Санкт-Петербург, ул. Летчика Пилютова, 1
emails: parfenov-nikolai@mail.ru, ksgati@yandex.ru

Аннотация: В статье рассмотрены комплексные методы защиты информации в органах внутренних дел в современных условиях.

Ключевые слова: защита информации; техническая защита информации; служба безопасности; комплекс мероприятий по защите информации; организационные меры (методы) защиты информации.

COMPLEX DEFENCE OF INFORMATION IN ORGANS OF INTERNAL AFFAIRS IN MODERN TERMS

Nikolay Parfenov, Sergey Alekseev
Saint-Petersburg University of MIA of Russia
Russia, St. Petersburg, Letchika Pilyutova str. 1
emails: parfenov-nikolai@mail.ru, ksgati@yandex.ru

Annotation: In the article the complex methods of defence of information are considered in the organs of internal affairs in modern terms.

Keywords: defence of information; technical defence of information; security service; complex of events on defence of information; organizational measures (methods) of defence of information.

Введение. Быстрое развитие человечества в последние годы привело к переходу от индустриального к информационному обществу. В современном информационном обществе необходимо, чтобы каждый член общества владел информацией, умел производить, распространять, хранить и использовать ее. Сотрудники органов внутренних дел, являясь в то же время, членами информационного общества обязаны в большей степени удовлетворять вышеперечисленным требованиям. Полиция обязана использовать в своей деятельности современную информационно-телекоммуникационную структуру, информационные системы, передовые достижения науки и техники, а также системы связи. В то же время органы внутренних дел обязаны защитить информацию от несанкционированного доступа (НСД), техническую защиту от утечек информации и техническое противодействие разведкам противников.

Для организации эффективной защиты информации необходимо анализировать, классифицировать и перекрывать всевозможные пути утечки служебной информации. Для решения этих задач в органах внутренних дел создается система безопасности, далее в тексте служба безопасности. Чаще всего служба безопасности создается на базе структурных подразделений секретариата и технической защиты информации. Сотрудники данных подразделений обеспечивают режим секретности и техническую защиту конфиденциальной информации. К комплексу мероприятий, которые обеспечивают информационную безопасность, можно отнести: предупреждение внутренних и внешних угроз; выявление внутренних и внешних угроз; обнаружение внутренних и внешних угроз; локализация преступных посягательств и преступных действий; ликвидация последствий угроз и преступных посягательств, а также восстановление прежнего состояния.

Комплексная защита информации в органах внутренних дел в современных условиях включает следующие мероприятия по защите информации:

1. Предупреждение внутренних и внешних угроз – это упреждающие, до их возникновения, действия по защите информации, например, создание осознанного климата внутри коллектива сотрудников органа внутренних дел по защите информации; защита информации криптографическими, аппаратными, физическими и аппаратно-программными средствами; работа с информаторами по предупреждению утечек конфиденциальной информации; упреждающая информационно-аналитическая работа службы безопасности органа внутренних дел по текущему и прогнозируемому состоянию криминогенной обстановки.

2. Выявление внутренних и внешних угроз – это систематическая работа по выявлению и предупреждению потенциальных и/или реальных внутренних и внешних угроз безопасности информации, например, внедрение тайных информаторов в среду криминальной структуры и получение упреждающих сведений о подготовке преступных посягательств и преступных действий.

3. Обнаружение внутренних и внешних угроз – систематическая деятельность по определению явных внутренних и внешних угроз и реальных преступных действий. Результатом этой деятельности может быть: обнаружение фактов хищения и разглашения конфиденциальной информации; фактов НСД к служебной информации.

4. Использование охранного телевидения, видеокамер, а также датчиков сигнализации предназначено для обнаружения угроз.

5. Локализация преступных посягательств и преступных деяний – систематическая деятельность по устранению реальной угрозы явных преступных посягательств и преступных деяний, например, пресечение подслушивания служебной информации во время совещания по звуковым каналам их утечки.

6. Ликвидация последствий угроз и преступных посягательств, а также восстановление прежнего состояния - систематическая работа по восстановлению состояния, предшествовавшего наступлению угроз и преступных деяний.

По функциональному признаку классификация средств технической защиты выглядит следующим образом:

1. Аппаратные средства защиты информации – устройства, приборы и приспособления для защиты служебной информации.

2. Физические средства защиты информации – механические конструкции и изделия, защищающие служебную информацию путем ограничения доступа злоумышленников на объекты защиты.

3. Криптографические защиты информации – специальные алгоритмические и математические средства, защищающие служебную информацию методом шифрования.

4. Программные средства защиты информации – специальные программные комплексы программы и системы защиты служебной информации в информационных системах органов внутренних дел.

5. Организационно-технические мероприятия защиты информации – комплекс мер, блокирующих разглашения и утечки служебной информации с помощью технических средств и режима.

6. Технические мероприятия по защите служебной информации подразделяются следующие:

1) скрывание – это применение радиомолчания и конструирование пассивных помех техническим средствам криминальных структур;

2) подавление – это конструирование активных помех техническим средствам криминальных структур;

3) дезинформация – это чаще всего предоставление ложной информации криминальным структурам, злоумышленникам, т.е. использование в работе информационных технологий и средств ложной информации.

7. Организационные мероприятия – ограничительные мероприятия к регламенту доступа конфиденциальной информации и технологий обработки и переработки служебной информации:

1) установление надежного пропускного режима;

2) установление надежного контроля над сотрудниками органа внутренних дел, работающими со служебной информацией;

3) установление отдельных зон в соответствии с уровнями конфиденциальной информации и режимными системами допуска;

4) установление регламента допуска и работы с конфиденциальной информацией, включая операции их учета, перемещения, исполнения, хранения и уничтожения.

В органах внутренних дел служат множество сотрудников, которые имеют различные формы допуска к конфиденциальной информации, поэтому для эффективной защиты информации необходимо провести классификацию объектов защиты по уровням секретности информации; т.е. установить категорию объекта защиты информации. В зависимости от важности и конфиденциальности информации устанавливается минимальный комплекс мер по ее защите. Соответствующую категорию информации присваивает специальная комиссия, которая также утверждает необходимый и достаточный комплекс технических и режимных мер и мероприятий по защите конфиденциальной информации. Кроме этого, специальная комиссия подтверждает, что объект защиты соответствует всем требованиям нормативно-правовых документов и стандартов по технической защите информации.

Заключение. Подводя итоги рассмотренных в статье вопросов необходимо подчеркнуть, что основными путями защиты информации являются лицензирование деятельности органов внутренних дел в области информации, аттестование объектов защиты по степени секретности, сертификация средств защиты информации и категорирование объектов защиты информации.

СПИСОК ЛИТЕРАТУРЫ:

1. Алексеев С.А., Гончар А.А., Стахно Р.Е. Направления интеллектуализации системы управления качеством тренажерной подготовки специалистов органов внутренних дел. / Научный журнал. № 6 (19) Москва. изд. «Проблемы науки». 2017 С.15-18
2. Парфенов Н.П., Стахно Р.Е. Вопросы правового регулирования обработки и защиты персональных данных. / Проблемы современной науки и образования № 19 (101). Москва.изд. «Проблемы науки». 2017. С. 29-32.

УДК 004.056:61

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ ОВД ПОСРЕДСТВОМ СПЕЦИАЛЬНОЙ ОБРАБОТКИ

Парфенов Николай Петрович, Алексеев Сергей Алексеевич
Санкт-Петербургский университет МВД России
Россия, Санкт-Петербург, ул. Летчика Пилютова, 1
emails: parfenov-nikolai@mail.ru, ksgati@yandex.ru

Аннотация: В статье рассмотрены специальные методы защиты персональных данных сотрудников ОВД при выполнении ими служебных обязанностей.

Ключевые слова: *персональные данные; защита персональных данных; обезличивание персональных данных; система защиты информации; организационные меры (методы) защиты информации.*

PERSONAL DATA PROTECTION EMPLOYEES ATS BY SPECIAL TREATMENT

Nikolay Parfenov, Sergey Alekseev
Saint-Petersburg University of MIA of Russia
Russia, St. Petersburg, Letchika Pilyutova str. 1
emails: parfenov-nikolai@mail.ru, ksgati@yandex.ru

Abstract: In the article the special methods of protection of the personal data of employees of ОВД are considered at implementation by them official duties.

Keywords: *personal information, protection of personal information, depersonalization of personal information, information security system, organizational measures (methods) of information security.*

Введение. В современных условиях развития общества защита информации приобретает актуальное значение. Одной из важнейших задач в МВД России является обеспечение надежной защиты информации различных уровней конфиденциальности (секретности), а также информации, содержащей сведения ограниченного распространения (служебной, персональных данных).

В настоящее время основным звеном в системе защиты информации организации становится технология защиты персональных данных его работников. На существующий момент времени ужесточены нормы законодательства по защите персональных данных работников. Поэтому необходимо позаботиться о соблюдении установленных в этой сфере требований. Необходимо отметить, что согласно Федеральному закону «О службе в органах внутренних дел Российской Федерации» от 30.11.2011 № 342-ФЗ для сотрудников внутренних дел отдельно прописана защита их персональных данных, что означает дополнительное предоставление гарантий при защите их персональных данных:

1) обработка персональных данных проводится для соблюдения требований Конституции Российской Федерации, настоящего Федерального закона и других нормативных правовых актов;

2) защита персональных данных сотрудников МВД от неправомерного применения или утраты, осуществляется средствами федерального органа исполнительной власти в сфере внутренних дел в соответствии с требованиями настоящего Федерального закона и других нормативных правовых актов.

В структурных подразделениях ОВД проходят службу сотрудники, которые имеют различные формы допуска к конфиденциальной информации. В связи с этим, для обеспечения требований по защите и допуску различных групп к информации разной степени секретности предварительно разделяют объекты информатизации по важности и присваивают категории. Категории определяются конфиденциальностью информации, обрабатываемой на соответствующем объекте информатизации. При этом для каждой категории определяется соответствующий набор требований по ее защите. После присвоения объекту информатизации соответствующей категории специальная комиссия проводит комплекс режимных и технических мероприятий. Защита персональных данных сотрудников полиции имеет свои специфические особенности, и этому обстоятельству нам бы хотелось уделить особое внимание. В основном, специфические особенности защиты персональных данных обусловлены условиями прохождения службы сотрудниками правоохранительных органов и вытекают из положений нижеперечисленных основных нормативных правовых документов:

1. Конституция РФ (Статьи 23, 24);
2. Трудовой кодекс РФ (Глава 14);
3. Федеральный закон «О полиции»;
4. Федеральный закон № 152-ФЗ «О персональных данных» от 27 июля 2006г.;
5. Положение «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утверждено постановлением Правительства Российской Федерации № 781 от 17 ноября 2007 г.;

6. «Порядок проведения классификации информационных систем персональных данных», утвержден приказом ФСТЭК России, ФСБ России Мининформсвязи России № 55/86/20 от 13 февраля 2008 г.

Персональные данные – в общепринятом смысле термина, это - сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность. Как правило, идентификация личности проводится по сведениям, содержащимся в паспорте. Кроме этого, идентифицировать личность позволяют и дактилоскопические данные. Для сотрудников правоохранительных органов, предназначенных для борьбы с преступностью, эти данные имеют непосредственное значение. В настоящее время защита информации на предприятиях, в организациях, органах внутренних дел приобретает актуальное значение. Ключевое место в технологии защиты персональных данных работников занимает разработка положения. Положение о защите персональных данных работника – это основной документ, регламентирующий порядок защиты персональных данных работника на конкретном предприятии. Положение о защите персональных данных работника - это внутренний (локальный) документ предприятия. Данный документ разрабатывает кадровая служба предприятия. На сегодняшний день закон не установил строгой формы этого документа, но он должен соответствовать требованиям, которые предъявляет к защите персональных данных работника Трудовой кодекс РФ. Работодатель разрабатывает перечень мер, необходимых для выполнения обязанностей по обработке персональных данных. Обезличивание персональных данных представляет собой совокупность специальных действий (специальной обработки) их, в результате которых нельзя установить принадлежность защищаемых персональных данных их конкретному носителю. В статье рассматриваются свойства, специальные методы обработки (обезличивания) персональных данных и проведем их оценку. Обезличивание персональных данных необходимо не только для их защиты от несанкционированного использования, но и для дальнейшей обработки. Поэтому обезличенные данные должны сохранять основные характеристики обезличиваемых персональных данных. Назовем основные свойства обезличенных данных:

1) полнота – это сохранение информации в полном объеме о конкретных носителях персональных данных, которая имела до обезличивания;

2) структурированность – это сохранение структуры обезличенных данных конкретных носителей, имевшейся до обезличивания;

3) семантическая целостность – это сохранение семантики персональных данных конкретных субъектов в процессе их обезличивания;

4) анонимность – это неспособность однозначной идентификации носителей персональных данных, полученных в процессе обезличивания, без использования дополнительной информации.

Наиболее практичными считаются следующие специальные методы обработки (обезличивания):

1) метод введения идентификаторов – это замена персональных данных идентификаторами, путем создания каталогов соответствия идентификаторов исходным персональным данным;

2) метод изменения состава или семантики – это изменение состава или семантики персональных данных конкретных субъектов методом замены их результатами статистической обработки, объединения или исключения части сведений;

3) метод декомпозиции – это разделение множества персональных данных конкретных субъектов на подмножества с дальнейшим обособленным хранением их;

4) метод перемешивания – это перемещение и перестановка отдельных записей в множестве персональных данных конкретных субъектов.

5) Необходимо подчеркнуть и отметить, что методы обезличивания данных постоянно развиваются, совершенствуются.

Заключение. Резюмируя рассмотренные вопросы, необходимо отметить, что применение рассмотренных в статье специальных методов обработки (обезличивания) данных позволит повысить качество обработки персональных данных и обеспечит более высокую степень защиты персональных данных сотрудников ОВД.

СПИСОК ЛИТЕРАТУРЫ:

1. Алексеев С.А., Гончар А.А., Стахно Р.Е. Основы квалиметрии, автоматизации и интеллектуализации систем организационного управления практической подготовкой в вузах МВД. / Научный журнал. № 5 (35) Москва. изд. «Проблемы науки». 2017. С.29-32.
2. Парфенов Н.П., Стахно Р.Е. Ужесточение требований к обработке персональных данных - основа повышения безопасности государства / Наука, техника и образование. №5 (35). Том 2. Изд-во «Проблемы науки», г. Иваново. 2017.С.13-15.

УДК 343

О НЕКОТОРЫХ АСПЕКТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ШКОЛЬНИКОВ

Поправко Анна Сергеевна
Омская академия МВД России,
Россия, Омск, пр. Комарова, 7,
email: almera5451@yandex.ru

Аннотация: в статье отражены отдельные проблемы информационной безопасности школьников, обусловленные переменами в социальной, политической и экономической жизни общества под влиянием глобальной информатизации и некоторые пути их решения.

Ключевые слова: информационная безопасность; ребенок, школьник, информационно-коммуникационная сеть Интернет.

SOME ASPECTS OF INFORMATION SECURITY OF THE SCHOOLCHILDREN

Popravko Anna
The Omsk Academy of the Interior,
Russia, Omsk, Komarova str. 7,
email: almera5451@yandex.ru

Abstract: the article describes some problems of information security of the **schoolchildren**, caused by changes in the social, political and economic life under the influence of global information and some solutions to them.

Keywords: *information security; child, schoolchildren, information and communication the Internet.*

Введение. Существующие проблемы информационной безопасности школьников [1] обусловлены переменами в социальной, политической и экономической жизни общества под влиянием глобальной информатизации. Значительный объем информации школьники узнают не через теоретический материал учебника, а на практике, оформляя свои исследования, осуществляя поиск и структурирование информации, полученной в сети Интернет [2].

Учитывая несформировавшуюся систему личностных ценностей ребенка, отсутствие регулирования доступа к средствам информационного воздействия, психологические особенности детского возраста, индивидуальные особенности ребенка, неразвитость информационной культуры школьников, отсутствие должной помощи школьникам со стороны педагогов, психологов и родителей, Интернет может представлять реальную угрозу для детей школьного возраста. Ребенок школьного возраста, выходящий в Интернет, в процессе поиска нужной ему информации может просматривать любые материалы. А это могут быть сайты, содержащие информацию о насилии, наркотиках, порнографии, страницы, подталкивающие молодежь к самоубийствам, страницы с националистической или откровенно фашистской идеологией. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна, содержащие любую информацию [3].

Все чаще и чаще злоумышленники используют каналы сети Интернет для того, чтобы заставить детей выдать личную информацию. В других случаях это могут быть педофилы, которые ищут новые жертвы. Помимо указанного, существует угроза заражения устройства вредоносным программным обеспечением.

Из многообразных факторов риска к наиболее распространенным и разрушительным для физического, психического и нравственного здоровья школьников относятся некоторые разновидности компьютерных игр. Смысл многих игр сводится к убийству, совершению преступлений разного рода. Под предлогом борьбы со злом дети программируются на жестокость и садизм. У некоторых школьников появляются признаки компьютерной наркомании.

Не смотря на существующие проблемы, педагоги и родители не могут просто запретить ребенку посещать Интернет, так как в современном обществе это просто необходимо.

Поэтому, на наш взгляд, в первую очередь, педагоги и родители, как значимые в жизни школьника взрослые, должны способствовать обеспечению информационной безопасности детей школьного возраста. Процесс просвещения в области безопасности при работе с информацией в сети Интернет целесообразно начинать с начальной школы. Всем обозначенным видам проблем может противостоять педагог, обучающий информационной безопасности. Грамотный в рассматриваемой области специалист должен проводить уроки медиаобразования, на которых давать самые необходимые знания по соблюдению безопасности в информационном пространстве, готовить сознание детей к противодействию негативным информационным воздействиям, формировать информационную грамотность, развивать способности к самоблокированию информации, учить отличать качественную информацию от некачественной [4]. В воспитательной работе педагогам также необходимо уделять внимание воспитанию информационной культуры учащихся.

Заключение. Таким образом, родителям необходимо контролировать поведение детей в информационных сетях при помощи специализированных компьютерных программ. Таким образом может отслеживаться время, проводимое за компьютером, запрещаться доступ к отдельным ресурсам, компьютерным играм и иным программам. Функцию контроля также должны осуществлять образовательные учреждения, что минимизирует возможность причинения вреда ребенку неконтролируемой информацией. Поэтому обеспечение информационной безопасности школьников должно стать одним из первоочередных направлений работы современной школы.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Доступ из СПС КонсультантПлюс.
2. Малых Т.А. Педагогические условия развития информационной безопасности младшего школьника: Автореф. дисс. канд. пед. наук. - Иркутск, 2008. 56 с.
3. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. - М.: ЮНИТИ-ДАНА, 2013. 239 с.
4. Саттарова Н.И. К вопросу об информационной безопасности школьников // Информационные и коммуникационные технологии в образовании: Межвузовский сборник научных трудов. СПб.: Изд-во БАН, 2002. 115 с.

УДК 681.518

ОБ АПРОБАЦИИ ТЕХНОЛОГИИ ГИПЕРССЫЛОК ПРИ РАБОТЕ С ДОКУМЕНТАМИ, РАЗМЕЩЕННЫМИ В ХРАНИЛИЩЕ ПОДРАЗДЕЛЕНИЯ

Гореленко Константин Евгеньевич, Потехин Владимир Семенович
Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, ул. Летчика Пилютова, 1,
emails: kost32kost@yandex.ru, vsp1945@gmail.com

Аннотация: Излагается подход, позволяющий построить модель и апробировать технологию гиперссылок при работе с электронными документами. При этом документы размещаются в электронном хранилище подразделения. Целью работы является вынесение решения о целесообразности применения предложенного подхода.

Ключевые слова: электронные документы, электронное хранилище документов, технологии гиперссылок.

ON APPROBATION OF HYPERLINKS TECHNOLOGY AT WORK WITH DOCUMENTS, LOCATED IN THE SUBDIVISION DEPARTMENT

Gorelenko Konstantin, Potekhin Vladimir
St. Petersburg University at Russian Ministry of internal Affairs (MIA),
Russia, St. Petersburg, Pilot Pilyutov str., 1,
emails: kost32kost@yandex.ru, vsp1945@gmail.com

Abstract: An approach that allows to build a model and to test the hyperlinks technology at work with electronic documents is presented. The documents are placed in electronic subdivision storage. The aim of this work is to make the decision on expediency of the proposed approach application.

Keywords: *electronic documents, electronic document repository, hyperlinks technology*

Введение. В каждом современном учреждении России работают с электронными документами. Для хранения и использования документов, изданных на федеральном уровне и региональном уровнях, часто используют справочно-правовые системы, например, «ГАРАНТ» [1], «Консультант-Плюс» [2] и др. Однако для документов, изданных на локальном уровне (в каком-либо учреждении) использование подобных систем затруднено из-за необходимости содержания большого штата сотрудников. Поэтому на практике документы локального уровня размещают в иерархическую структуру папок, созданную средствами операционной системы, например, в «Проводнике» OS MS Windows. Но при этом «навигация» и между документами, и внутри документа требует много времени. Кроме того фильтрационные возможности «Проводника» не в полной мере удовлетворяют пользователей. Положение можно изменить, если обеспечить навигацию на основе гиперссылок в сочетании с фильтрационными возможностями пакета MS Excel. Теоретические основы такого подхода изложены в статье [3], но требуется апробация (практическая проверка) этого замысла.

Для обеспечения апробации представляется целесообразным:

1) выбрать предметную область, в рамках которой будет проводиться исследование. Например, это может быть документация, которую должны вести на кафедре Санкт-Петербургского университета МВД России по дисциплине 10.05.05 – Безопасность информационных технологий в правоохранительной сфере [4];

2) проанализировать требования руководящих документов [5] и [6] с целью выявления функций, подлежащих реализации в части организации хранения документов, их фильтрации и навигации, как между документами, так и внутри документов;

3) проанализировать опыт автоматизации подобных функций [7], [8], [9], [10], [11] и возможности современных средств из числа инструментария, входящего в MS Office, выбрав такие инструментальные средства, которые обеспечат реализацию функций, выявленных в п. 2);

4) построить функциональную модель исследуемого процесса с детализацией до наиболее важных подпроцессов, функций и задач, используя соответствующие CASE- средства, например, [12], [13], [14];

5) построить поведенческие модели (алгоритмы), соответствующие функциональной модели, выбрав те из них, в которых наиболее полно могут быть показаны возможности навигации на основе гиперссылок на основе требований [15];

6) построить действующую модель, используя инструментальные средства пакетов прикладных программ (выбранных в п. 3), для демонстрации работы возможным потенциальным пользователям.

В заключение заметим, что, по мнению авторов, выполнение изложенного плана исследований и оценка полученных результатов потенциальными пользователями позволит составить объективное суждение о целесообразности применения подобного подхода.

СПИСОК ЛИТЕРАТУРЫ

1. Справочно-правовая система «ГАРАНТ». [Электронный ресурс] URL: <http://www.garant.ru/> (дата обращения 13.09.2017).
2. Справочно-правовая система «Консультант-Плюс». [Электронный ресурс] URL: <http://consultant29.ru/> (дата обращения 13.09.2017).
3. Чудаков О.Е., Куватов В.И., Потехин В.С. Опыт разработки электронного хранилища документов учебно-методического обеспечения образовательных программ на основе компьютерных технологий // Вестник СПб университета МВД № 2, (74), 2017. С. 184 – 191. [Электронный ресурс] URL: [http://www.univermvd.ru/files/other-files/%D0%92%D0%B5%D1%81%D1%82%D0%BD%D0%B8%D0%BA_2_\(74\)_2017.pdf](http://www.univermvd.ru/files/other-files/%D0%92%D0%B5%D1%81%D1%82%D0%BD%D0%B8%D0%BA_2_(74)_2017.pdf) (дата обращения 13.09.2017).
4. Федеральный государственный образовательный стандарт высшего образования по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере (уровень специалитета). Утвержден Приказом Минобрнауки России от 19.12.2016 N 1612. Сайт «КонсультантПлюс» [Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_210993/ (дата обращения 13.09.2017).
5. Положение об учебно-методическом обеспечении образовательных программ. Утверждено приказом начальника Санкт-Петербургского университета МВД России № 68 от 12.02.2016 г. СПб: Изд-во Санкт-Петербургского университета МВД России. 2016. – с. 24.
6. Положение об образовательной деятельности федерального государственного казенного образовательного учреждения высшего профессионального образования «Санкт-Петербургский университет Министерства внутренних дел Российской Федерации». Утверждено приказом начальника Санкт-Петербургского университета МВД России № 610 от 10.11.2014 г. СПб: Изд-во Санкт-Петербургского университета МВД России. 2014. – с. 132.
7. Современные образовательные технологии в учебном процессе вуза [Текст]: методическое пособие / авт.-сост. Н. Э. Касаткина, Т. К. Градусова, Т. А. Жукова, Е. А. Кагакина, О. М. Колупаева, Г. Г. Солодова, И. В. Тимонина; отв. ред. Н. Э. Касаткина. – Кемерово: ГОУ «КРИПО», 2011. – 237 с. [Электронный ресурс] URL: <http://portal.tpu.ru:7777/SHARED/k/KAV47/education/Tab2/%D0%A1%D0%BE%D0%B2%D1%80%D0%B5%D0%BC%D0%B5%D0%BD%D0%BD%D1%8B%D0%B5%20%D0%BE%D0%B1%D1%80%D0%B0%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5%20%D1%82.pdf> (дата обращения 13.09.2017).
8. Малышева М.А. Современные технологии обучения в вузе (опыт НИУ ВШЭ в Санкт-Петербурге). Методическое пособие. – Отдел оперативной полиграфии НИУ ВШЭ – Санкт-Петербург, 2011. – 134 с. http://portal.tpu.ru:7777/SHARED/k/KAV47/education/Tab2/%D1%83%D1%87%D0%B5%D0%B1_%D0%BC%D0%B5%D1%82_%D0%BF%D0%BE%D1%81%D0%BE%D0%B1_%D0%A1%D0%BE%D0%B2%D1%80_%D1%82%D0%B5%D1%85%D0%BD_%D0%BE%D0%B1%D1%83%D1%87_11.pdf
9. Кривошеев А. О., Голомидов Г. С., Таран А. Н. Перспективные Internet-технологии информационного обеспечения образовательных услуг. Сайт «МГТУ им. Н.Г. Баумана». [Электронный ресурс] URL: <http://technomag.bmstu.ru/doc/52838.html> (дата обращения 13.09.2017).
10. Потехин В.С. Опыт разработки методических рекомендаций на основе компьютерных технологий для слушателей-заочников, готовящих дипломы по техническим специальностям // Вестник СПб университета МВД № 4, (60), 2013. С. 149 – 155.
11. Кадулин В.Е., Потехин В.С. Об уточнении понятия и классификации автоматизированных рабочих мест, используемых в информационных системах и компьютерных технологиях. Вестник СПб университета МВД № 4 (68), 2015. С. 207 – 210.
12. Горбаченко В. И., Убиенных Г. Ф., Бобрышева Г. В. Создание функциональной модели информационной системы с помощью CASE-средства CA ERwin Process Modeler 7.3. – Пенза: ПГУ, 2010. – 66 с. [Электронный ресурс]. URL: <http://window.edu.ru/resource/658/72658/files/stup552.pdf> (дата обращения 13.09.2017).
13. Дубейковский В.И. Практика функционального моделирования с AllFusion Process Modeler 4.1. Где? Зачем? Как? М.: Изд. Диалог-МИФИ, 2008 – 464 с. ISBN 5-86404 192-0.
14. Маклаков С.В. Моделирование бизнес-процессов с AllFusion PM. 2-е изд., испр. и дополн. – М.: Изд. Диалог-МИФИ, 2008 – 224 с. ISBN 5-86404-179-3.
15. ГОСТ 19.701-90 (ИСО 5807-85). Единая система программной документации. Схемы алгоритмов, программ, данных и систем. Условные обозначения и правила выполнения. М.: "Издательство стандартов", 1991.

УДК 004.056.53

ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Редковников Владислав Александрович
Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, ул. Летчика Пилютова, 1,
email: iamvladr@gmail.com

Аннотация: В статье затронуты вопросы обеспечения информационной безопасности информационных систем, используемых в органах внутренних дел Российской Федерации, а также рассмотрены основные направления обеспечения информационной безопасности данных систем.

Ключевые слова: *информационные системы и технологии; информационная безопасность; обеспечение информационной безопасности; органы внутренних дел; ЕИТКС.*

ISSUES OF ENSURING THE INFORMATION SECURITY OF INFORMATION SYSTEMS OF LAW-ENFORCEMENT BODIES OF RUSSIAN FEDERATION

Redkovnikov Vladislav

The St. Petersburg University of the Ministry of the Internal Affairs,
Russia, St. Petersburg, Pilot Pilutov str. 1,
email: iamvladr@gmail.com

Abstract: In article the issues of ensuring information security of information systems used in law-enforcement bodies of Russian Federation are raised. The directions of ensuring information security of these systems are also considered.

Keywords: *information systems and technologies; information security; ensuring the information security; law-enforcement bodies; UITS.*

Введение. В настоящее время органы внутренних дел Российской Федерации испытывают острую необходимость в применении информационных систем и технологий в своей деятельности. Значительную долю в используемых системах и технологиях занимают различные автоматизированные информационно-поисковые системы (АИПС), а также Единая информационно-телекоммуникационная система органов внутренних дел Российской Федерации (ЕИТКС ОВД) [1]. В связи с данным обстоятельством возникает проблема обеспечения информационной безопасности данных систем.

Основным нормативно-правовым актом, разрешающим применение в полиции современной информационно-телекоммуникационной инфраструктуры, информационных систем и сетей связи является федеральный закон «О полиции» [2]. Основными АИПС, используемыми в полиции, являются:

- АИПС «Опознание»;
- АИПС «Автопоиск»;
- АИПС «Антиквариат»;
- АИПС «Досье»;
- АИПС «Папилон»;
- АИПС «Криминал и ДТП»;
- АИПС «Насилие»;
- АИПС «Криминал и Адмпрактика».

При этом доступ к вышеперечисленным АИПС сотрудник полиции может получить через своё рабочее место, подключенное соответствующим образом к ЕИТКС ОВД.

ЕИТКС ОВД состоит из региональных интегрированных мультисервисных телекоммуникационных систем, которые соединяются друг с другом собственными или арендованными каналами связи, используя распространённый протокол TCP/IP.

Вопрос обеспечения информационной безопасности вышеперечисленных информационных систем и технологий следует рассматривать по трём основным направлениям [3]:

1. Правовая защита.
2. Организационная защита.
3. Инженерно-техническая и аппаратно-программная защита.

Первое направление заключается в создании такой нормативно-правовой базы, которая бы в полной мере обеспечивала защиту информации на правовой основе. Также к данному направлению относится совершенствование нормативно-правовых документов, регламентирующих защиту информации, в том числе федерального закона № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации», федерального закона № 152-ФЗ от 27.07.2006 г. «О персональных данных», федерального закона № 5485-1 от 21.07.1993 г. «О государственной тайне», федерального закона № 98-ФЗ от 29.07.2004 г. «О коммерческой тайне».

Второе направление подразумевает регламентацию производственной деятельности сотрудников органов внутренних дел, использующих перечисленные информационные системы и технологии в своей деятельности, на нормативно-правовой основе, исключающей нанесение ущерба, а именно:

- разглашение или утрата информации, составляющей государственную тайну, или информации, предназначенной для служебного пользования, а также носителей данной информации;
- разглашение или утрата сотрудником своих данных, дающих право на доступ к ресурсам АИПС и компьютерной технике, обеспечивающей доступ к АИПС (логины и пароли учётных записей);

– неквалифицированные действия сотрудников, приводящие к ошибкам и отказам в работе компьютерной техники, связанной с использованием АИПС.

Достаточно эффективными мерами, способствующими исключению ущерба по данному направлению, являются:

– разработка специальных инструкций для сотрудников, регламентирующих их работу с компьютерной техникой и АИПС;

– разработка локальных политик информационной безопасности в подразделениях, в которых применяются АИПС;

– проведение с сотрудниками практических занятий, разъясняющих им основы работы на компьютерной технике, обеспечивающей использование АИПС.

Третье направление представляет собой комплекс технических и аппаратно-программных средств, препятствующих нанесению ущерба.

К техническим средствам можно отнести специальные системы тушения пожаров, устанавливаемые в помещениях с компьютерной техникой, системы поддержания требуемого климата и влажности воздуха, а также системы, препятствующие проникновению посторонних лиц в данные помещения.

К аппаратно-программным средствам можно отнести криптомодемы и криптографические программы, предназначенные для шифрования передаваемой информации, системы защиты информации от несанкционированного доступа такие, как «Dallas Lock», а также системы разграничения доступа к информации разной категории. При этом целесообразно обратить внимание на средства резервирования и дублирования информации: данные средства позволят возобновить работу информационных систем при глобальных ошибках и отказах.

Заключение. Вопрос обеспечения информационной безопасности информационных систем, используемых в органах внутренних дел является крайне актуальным. Это обусловлено тем, что в настоящее время в органах внутренних дел Российской Федерации применяется всё большее число различных информационных систем и технологий. Решение данного вопроса позволит более эффективно использовать упомянутые системы и технологии, что в свою очередь положительно отразится на работе сотрудников органов внутренних дел.

СПИСОК ЛИТЕРАТУРЫ

1. Об утверждении новой редакции Программы МВД России «Создание единой информационно-телекоммуникационной системы органов внутренних дел» [Электронный ресурс]: приказ Министерства внутренних дел Российской Федерации от 20.05.2008 № 435 ред. от 02.03.2011. – Режим доступа: КонсультантПлюс.
2. Федеральный закон Российской Федерации от 07.02.2011 № 3-ФЗ «О полиции» (ред. от 03.02.2014) // Собрание законодательства Российской Федерации, 14.02.2011, № 7, ст. 900.
3. Ярочкин В.И. Информационная безопасность: Учебник для студентов ВУЗов / В.И. Ярочкин. – М.: Академический Проект; Гаудеамус, 2-е изд. – 2004. – 544 с.

УДК 681.518 (004.031.42)

ПОДХОД К РАЗРАБОТКЕ СРЕДСТВ ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ ПРИ САМОСТОЯТЕЛЬНОЙ ПОДГОТОВКЕ ОБУЧАЕМЫХ К ЗАЧЕТУ И ЭКЗАМЕНУ НА ПРИМЕРЕ ОДНОЙ ИЗ ДИСЦИПЛИН, СВЯЗАННЫХ С ОБЕСПЕЧЕНИЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рыжова Валентина Сергеевна, Потехин Владимир Семенович
Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, ул. Летчика Пилютова, 1,
emails: valjlepleu@yandex.ru, vsp1945@gmail.com

Аннотация: Излагается подход к созданию средств информационной поддержки, обеспечивающих процесс самостоятельной работы на автоматизированном рабочем месте обучаемого

(АРМ-О) при подготовке к зачету или экзамену.

Ключевые слова: средства информационной поддержки процесса, самостоятельная подготовка, зачет, экзамен.

AN APPROACH TO DEVELOPMENT OF INFORMATION SUPPORT TOOLS AT THE INDEPENDENT TRAINING OF TRAINED TO EXERCISE AND EXAMINATION ON THE EXAMPLE OF ONE OF THE DISCIPLINES RELATED TO SECURING INFORMATION SECURITY

Ryzhova Valentina, Potekhin Vladimir
St. Petersburg University at Russian Ministry of internal Affairs (MIA),
Russia, St. Petersburg, Pilot Pilyutov str., 1,
emails: valjlepleu@yandex.ru, vsp1945@gmail.com

Abstract: The article describes the approach to the creation of information support tools that provide the process of independent work on the student's automated workplace (AWP-O) in preparation for a test or exam.

Keywords: *modeling; means of information support of the process, independent preparation, test, exam.*

Введение. В соответствии с федеральным государственным стандартом высшего образования (ФГОС ВО) по специальности 10.05.05 – Безопасность информационных технологий в правоохранительной сфере [1] предусматривается:

- использование всей совокупности ресурсов материально-технического и учебно-методического обеспечения, включая не только традиционные учебно-методические материалы (УММ) в «бумажном» исполнении, но и электронные УММ, размещенные в, электронной информационно-образовательной среде организации, а также в электронных библиотеках Интернет;

- использование специальных помещений для проведения всех видов занятий, включая промежуточную аттестацию, а также помещения для самостоятельной работы (включая подготовку к экзаменам и зачетам).

Однако курсантами и слушателями использование упомянутых средств связано с рядом сложностей:

- «бумажные» УММ хранятся в библиотечном фонде, который даже по нормам ФГОС ВО предусматривает укомплектование печатными изданиями из расчета не менее 1 издания на двоих обучаемых по основной литературе, а по дополнительной литературе и того хуже (1 издание на четверых). Это приемлемо, когда речь идет о текущем изучении дисциплины, но крайне неудобно в период подготовки к зачету или экзамену. Устранить эту сложность можно, если обеспечить хранение и доступ копий «бумажных» УММ наряду с другими электронными изданиями (но для этого потребуются работы по созданию соответствующих средств информационной поддержки);

- УММ, хранящиеся в электронной информационно-образовательной среде университета, могут использоваться с помощью электронных киосков, установленных в коридорах университета. Однако таких киосков не много, да и сложно вести подготовку к экзамену, стоя в коридоре;

- УММ, хранящиеся в электронных библиотеках Интернет, могут использоваться лишь в компьютерных классах, имеющих выход в Интернет.

Устранить упомянутые сложности можно, если на основе современных информационных технологий, обеспечить возможность комплексного использования всех доступных УММ с автоматизированного рабочего места обучаемого (АРМ-О), оснащенного средствами информационной поддержки самостоятельной подготовки к зачету или экзамену. Но для этого следует выполнить дополнительные исследования, предусматривающие:

- анализ руководящих документов, регламентирующих процесс контроля знаний в ходе промежуточной аттестации, включая зачеты и экзамены [2], [3];

- анализ имеющихся достижений в исследуемой области и выявление тех средств, которые могут оказаться полезными при организации самостоятельной работы обучаемых в ходе подготовки к зачетам (экзаменам) [4], [5], [6], [7];

- построение на основе работ [8], [9], [10], [11] функциональной и поведенческой моделей, учитывающих специфику комплексного использования всех УММ, предусмотренных к использованию учебной программой изучаемой дисциплины, обеспечивая доступ (по желанию обучаемого) и к копиям «бумажных» УММ, и к УММ, хранящиеся в электронной информационно-образовательной среде университета, и к УММ, хранящиеся в электронных библиотеках Интернет;

- разработку диалога «ЭВМ-обучаемый», отвечающего современным требованиям реализации средств информационной поддержки в процессе изучения УММ, предусмотренных учебной программой [6], [7].

В заключение заметим, что реализация перечисленных направлений исследований, не претендуя на полноту, позволяют, по мнению авторов, составить общее впечатление о возможном подходе к созданию средств информационной поддержки, обеспечивающих процесс самостоятельной работы на автоматизированном рабочем месте обучаемого (АРМ-О) при подготовке к зачету или экзамену.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный государственный образовательный стандарт высшего образования по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере (уровень специалитета). Утвержден Приказом Минобрнауки России от 19.12.2016 N 1612. Сайт «КонсультантПлюс» URL: http://www.consultant.ru/document/cons_doc_LAW_210993/ (дата обращения 13.09.2017).
2. Положение об учебно-методическом обеспечении образовательных программ. Утверждено приказом начальника Санкт-Петербургского университета МВД России № 68 от 12.02.2016 г. / СПб: Изд-во Санкт-Петербургского университета МВД России. 2016 . 24 с.
3. Положение об образовательной деятельности федерального государственного казенного образовательного учреждения высшего профессионального образования «Санкт-Петербургский университет Министерства внутренних дел Российской Федерации».

- Федерации». Утверждено приказом начальника Санкт-Петербургского университета МВД России № 610 от 10.11.2014 г. / СПб: Изд-во Санкт-Петербургского университета МВД России. 2014. 132 с.
4. Иванников А.Д., Иванов Ю.Л., Кулагин В.П. Перспективы использования WWW-технологии в высшей школе России / Информационные технологии, 1996. № 2. С. 24-29.
 5. Кривошеев А. О., Голомидов Г. С., Таран А. Н. Перспективные Internet-технологии информационного обеспечения образовательных услуг / Сайт «МГТУ им. Н.Г. Баумана». URL: <http://technomag.bmstu.ru/doc/52838.html> (дата обращения 13.09.2017).
 6. Потехин В.С. Опыт разработки методических рекомендаций на основе компьютерных технологий для слушателей-заочников, готовящих дипломы по техническим специальностям // Вестник СПб университета МВД № 4, (60), 2013. С. 149 – 155.
 7. Кадулин В.Е., Потехин В.С. Об уточнении понятия и классификации автоматизированных рабочих мест, используемых в информационных системах и компьютерных технологиях // Вестник СПб университета МВД № 4 (68), 2015. С. 207 – 210.
 8. Горбаченко В. И., Убиенных Г. Ф., Бобрышева Г. В. Создание функциональной модели информационной системы с помощью CASE-средства CA ERwin Process Modeler 7.3. – Пенза: ПГУ, 2010. 66 с. [Электронный ресурс]. <http://window.edu.ru/resource/658/72658/files/stup552.pdf> (дата обращения 13.09.2017).
 9. Дубейковский В.И. Практика функционального моделирования с AllFusion Process Modeer 4.1. Где? Зачем? Как? / М.: Изд. Диалог-МИФИ, 2008 –464 с. ISBN 5-86404 192-0.
 10. Маклаков С.В. Моделирование бизнес-процессов с AllFusion PM. 2-е изд., испр. и дополн. / М.: Изд. Диалог-МИФИ, 2008. 224 с. ISBN 5-86404-179-3.
 11. ГОСТ 19.701-90 (ИСО 5807-85). Единая система программной документации. Схемы алгоритмов, программ, данных и систем. Условные обозначения и правила выполнения / М.: "Издательство стандартов", 1991.

УДК 681.142.

УЧЕБНО – ТРЕНИРОВОЧНЫЙ КОНТРОЛЬНО – ПРОПУСКНОЙ ПУНКТ, КАК ЭЛЕМЕНТ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ «БОЕВОЙ СИСТЕМЫ» МВД

Саликов Александр Васильевич, Синешчук Юрий Иванович
Санкт-Петербургский университет МВД России
Россия, Санкт-Петербург, ул. Летчика Пилютова, 1,
emails: salikov.aleksandr92@mail.ru , sinegal@rambler.ru

Аннотация: Авторами обоснована роль мероприятий физической защиты в системе информационной безопасности. Показано место системы информационной безопасности в структуре боевой системы, предложены технические решения для отработки навыков обеспечения пропускного режима на основе учебно-тренировочного комплекса.

Ключевые слова: боевая система; информационная безопасность; физическая защита; обучение; пропускной режим.

TRAINING CHECKPOINT, AS PART OF THE INFORMATION SECURITY SYSTEM "BATTLE SYSTEM" OF THE MINISTRY OF INTERIOR

Salikov Alexander, Sineshchuk Yuri
Saint-Petersburg University of MIA of Russia
Russia, Saint-Petersburg, letchika Pilyutova Street 1,
emails: salikov.aleksandr92@mail.ru, sinegal@rambler.ru

Abstract: The authors explain the role of measures of physical protection in the system of information security. Shown place information security systems in the structure of the combat system, the proposed technical solution is to practice skills provide admission on the basis of the training complex.

Keywords: combat system; information security; physical protection; training; access control.

Введение. Развитие общества в последнее время приобрело так называемый постиндустриальный характер и характеризуется глобальной информатизацией общества, как новой система взглядов, ценностей, законов и правил, позволяющей говорить об "информационной эре", которая сопровождается и рядом новых проблем. К совокупности таких проблем можно отнести обострившийся вопрос защиты информации, ставшей одновременно и более уязвимой, и значимой практически для всех сфер жизнедеятельности, включая и деятельность правоохранительных органов. Информация перестает быть абстрактной, неуправляемой характеристикой, она обретает исчисляемую стоимость и принадлежность определенным субъектам. Приобретая все свойства товара и собственности, информация становится объектом интересов самого различного характера (коммерческого, социального, криминального и т.д.). В этих условиях становится актуальной задача обеспечения эшелонированной(рубежной) защиты информации подразделений, органов внутренних дел(ОВД).

Эффективность решения задачи обеспечения защиты информации в ОВД предполагает рассмотрение МВД, в целом, и отдельных ее структурных элементов с позиций системного подхода в виде сложной организационно-технической системы. Из всего многообразия типов систем для описания системы противоборствующих сторон (силовых ведомств) используют так называемые боевые системы (БС).

Под боевой системой будем понимать сложную организационно-техническую совокупность взаимосвязанных элементов(подсистем), предназначенных для сдерживания или поражения (воздействия) на противоборствующую систему [1].

В структуре боевой системы, как правило, выделяют: ударную(функциональную), управляющую и подсистему обеспечения и обслуживания. Одним из элементов последней является система обеспечения информационной безопасности(СОИБ).

Создание комплексной(интегрированной) СОИБ предусматривает следующие формальные и неформальные меры (методы, средства) защиты информации[2]: правовые (законодательные); административные или организационные; физические; инженерно-технические; аппаратно-программные.

Учитывая специфику силовых ведомств, особую роль в СОИБ играют физические меры защиты информации. К физическим мерам относятся разного рода механические электро- и электронно-механические, радиотехнические и другие устройства или сооружения для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, воспрепятствования несанкционированного доступа (входа, выхода), проноса (выноса) средств и материалов и других возможных видов преступных действий.

Одним из направлений деятельности сотрудников ОВД является обеспечение безопасности при проведении пропускного режима на объекте. В 2018 году Санкт-Петербург примет часть футбольных матчей финальной части XXI чемпионата мира по футболу, где вопросы обеспечения безопасности, проведение досмотровых мероприятий должны решать подготовленные специалисты.

Для успешного выполнения указанных задач требуется совершенствовать и развивать тактическую грамотность сотрудников в различных экстремальных ситуациях. Необходимо получить навыки оперативной оценки обстановки и выработки последовательности действий, для достижения максимально положительного результата с минимальными негативными последствиями. Эти навыки нарабатываются с помощью систематического моделирования ситуаций. Знание и правильное применение таких алгоритмов является неотъемлемой частью подготовки квалифицированных специалистов ОВД [3].

В Санкт-Петербургском университете МВД России планируется возведение Учебно-тренировочного контрольно-пропускного пункта (далее – КПП). КПП предназначается для осуществления практической подготовки, переподготовки и повышения квалификации сотрудников и работников различных государственных и коммерческих организаций, обеспечивающих мероприятия по усилению безопасности на особо важных объектах, объектах транспорта и массового пребывания людей при проведении общественно - политических, спортивных и культурных мероприятий, проводимых в Санкт-Петербурге.

Сооружение монтируется на готовом фундаменте и представляет собой сборно-разборную конструкцию, состоящую из отдельных модулей, общей площадью 332,3 м².

Предусмотренный проектом набор помещений и оборудования позволяет проводить занятия одновременно для учебной группы, состоящий из 30 человек с разделением на две подгруппы. Первая подгруппа проходит практическое обучение работе на стационарном и переносном досмотровом оборудовании в зале досмотра; одновременно, вторая подгруппа располагается в учебном классе, отделенным от зала досмотра стеклянной перегородкой, через которую обучающиеся имеют возможность наблюдать, анализировать и оценивать действия первой подгруппы.

Для получения оперативной видеоинформации об обстановке в выделенных зонах объекта с возможностью получения детальной картины крупным планом, в зале досмотра предусмотрена установка системы телевизионного наблюдения (6 IP камер Hikvision, современное цифровое IP оборудование TRASSIR) с выводом сигналов на мониторы, расположенные в учебном классе. Предусмотрено дублирование информации, поступающей на экраны трех интроскопов «Инспектор 65/75ZX» и одной установки персонального досмотра человека «Номо – scan» на мониторы, расположенные в учебном классе.

В процессе обучения на объекте вырабатываются практические навыки и умения по осуществлению установленного режима доступа людей, обеспечения досмотра, выявления запрещенных к проносу предметов и веществ. Опыт сотрудников профессорско-преподавательского состава, принявших непосредственное участие в обеспечении безопасности пропускного режима во время проведения XXII Олимпийских зимних игр и XI Паралимпийских зимних игр 2014 года в городе Сочи позволяет проводить занятия на высоком уровне.

Кроме того, помимо обучения, на КПП может осуществляться пропускной режим переменного состава.

Закключение. Создание учебно-тренировочного контрольно-пропускного пункта с новейшими техническими средствами позволит значительно повысить качество теоретической и практической подготовки по усилению безопасности на особо важных объектах, объектах транспорта и массового пребывания людей при проведении общественно - политических, спортивных и культурных мероприятий. В зависимости от решаемых задач, КПП можно рассматривать как элемент «боевой системы» Санкт – Петербургского университета МВД, так и всей системы МВД в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Синешук Ю.И., Синешук М.Ю., Примакин А.И., Пантиховский О.В. Правовые аспекты безопасности единого информационного пространства силовых ведомств (МВД, МЧС, МО) . «Вестник Санкт-Петербургского университета МВД». – № 2. – 2012. с. 234-240
2. Синешук Ю.И., Синешук М.Ю., Пантиховский О.В. Информационно-логическая модель анализа и обеспечения устойчивости функционирования систем управления сложными организационно-техническими объектами. Научно-аналитический журнал Проблемы управления рисками в техносфере №2(22), 2012, с.6-12, СПбУ ГПС МЧС России
3. Тактическая подготовка сотрудников ОВД к действиям в экстремальных ситуациях: проблемы и пути совершенствования URL: [http:// publikacia.net/archive/2015/3/2/22](http://publikacia.net/archive/2015/3/2/22).

УДК 519.2

**КОМПЛЕКСНАЯ ОЦЕНКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ИНФОРМАЦИОННЫХ СИСТЕМ САНКТ-ПЕТЕРБУРГСКОГО УНИВЕРСИТЕТА МВД РОССИИ
ПОСРЕДСТВОМ ПРИМЕНЕНИЯ МЕТОДОВ МНОГОМЕРНОГО АНАЛИЗА
(НА ПРИМЕРЕ КЛАСТЕРНОГО И ДИСКРИМИНАНТНОГО АНАЛИЗА)**

Саратов Дмитрий Николаевич, Козлов Михаил, Хухкха Кристина
Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, ул. летчика Пилютова, 1,
email: saratovdn@mail.ru

Аннотация: В статье затронуты вопросы обеспечения информационной безопасности информационных систем, используемых в органах внутренних дел Российской Федерации, а также рассмотрены основные направления обеспечения информационной безопасности данных систем.

Ключевые слова: *информационные системы и технологии; информационная безопасность; обеспечение информационной безопасности.*

**COMPREHENSIVE ASSESSMENT OF SECURITY ASSURANCE
INFORMATION SYSTEMS OF THE ST. PETERSBURG UNIVERSITY OF THE MOI OF RUSSIA
THROUGH THE APPLICATION OF METHODS OF MULTIDIMENSIONAL ANALYSIS
(ON THE EXAMPLE OF CLUSTER AND DISCRIMINANT ANALYSIS)**

Saratov Dmitry, Mikhail Kozlov, Huhkha Christina
St. Petersburg University of the Ministry of Internal Affairs of Russia,
Russia, St. Petersburg, st. pilot Pilutov, 1
email: saratovdn@mail.ru

Abstract: The article touches upon the issues of ensuring information security of information systems used in the internal affairs bodies of the Russian Federation, as well as the main directions of ensuring information security of these systems.

Key words: *information systems and technologies; Information Security; ensuring information security.*

СПБУ МВД России готовит специалистов в области защиты информации. Перед лицом данного специалиста стоит непростая задача - обезопасить информацию от утечек, потерь, злоумышленников и шпионов. Он должен обладать навыками обработки статистических данных, уметь применить математические основы для решения поставленных перед ним задач.

Информационной безопасности в нашем Университете отводится не малозначимая роль. Она отвечает таким принципам, как целостность данных, обеспечение конфиденциальности, доступность, достоверность.

В данном тезисе хотелось бы продемонстрировать на основе кластерного и дискриминантного анализов разделение информационных угроз, непосредственно влияющих на работу кадров данного учреждения, и отнесение новой возникшей угрозы в системе к определенному кластеру.

Для проведения указанных анализов в первую очередь необходимо определить виды информационных угроз, которые могут нанести существенный вред образовательной организации. Для этого мы прибегнем к классификации их по уровням эталонной модели взаимодействия открытых систем, а именно:

- угрозы на физическом уровне;
- угрозы на канальном уровне;
- угрозы на сетевом уровне;
- угрозы на транспортном уровне;
- угрозы на сеансовом уровне;
- угрозы на представительном уровне;
- угрозы на прикладном уровне.

Далее непосредственно хотелось бы продемонстрировать применение кластерного анализа, а затем плавно перейти к дискриминантному. У кластерного анализа стоит задача разделения

неоднородной совокупности, элементы которой характеризуются множеством признаками, на однородные или близкие по определенным критериям кластеры.

Основными этапами кластерного анализа являются:

1. Отбор выборки объектов для кластеризации.
2. Выделение признаков, характеризующих каждый объект данной совокупности, получение их числовых значений. При необходимости – нормализация значений признаков.
3. Определение меры близости между объектами и группами объектов.
4. Создание групп сходных объектов (кластеров).
5. Представление результатов кластеризации.
6. Анализ результатов кластеризации и при необходимости корректировка выбранной метрики (п. 3) и метода кластеризации (п. 4) до получения оптимального результата.

Дискриминантный анализ включает в себя методы классификации многомерных наблюдений по принципу максимального сходства при наличии обучающих признаков, здесь кластеры не образуются, а формулируется правило, по которому объекты подмножества подлежащего классификации относятся к одному из уже существующих (обучающих) подмножеств (классов), на основе сравнения величины дискриминантной функции классифицируемого объекта, рассчитанной по дискриминантным переменным, с некоторой константой дискриминации.

Основными этапами дискриминантного анализа являются:

1. Выбор данных, конкретно заданных переменных.
2. Выбор данных для дискриминации.
3. Интерпретация полученных результатов.

Итак, перейдем к проведению кластеризации информационных угроз, имеющих возможность нанести существенный вред.

На первом этапе применяется выборочный метод математической статистики, с помощью которого формируется выборка объектов для дальнейшего исследования. Для комплексной оценки информационных угроз в качестве объектов мы используем уровни эталонной модели взаимодействия открытых систем.

На втором этапе происходит выбор признаков, по которым будет проводиться кластеризация. В качестве признаков мы используем средние показатели нанесенного ущерба для организации.

На третьем этапе определяется метрика или мера близости между объектами и мера близости между группами объектов. Расстояние между кластерами может определяться по нескольким правилам, например: принцип «ближайшего соседа», принцип «дальнего соседа», принцип «средней связи».

На четвертом этапе из объектов образуем кластеры: по оси x отчается средний показатель по нанесенному ущербу, по оси y отображается средний показатель по затратам образовательного учреждения на реализацию защиты от информационных угроз.

На пятом этапе, на основании кластеров, мы определяем 3 группы информационных угроз, непосредственно их влияние на реализацию учебного процесса и способность организации защитить себя от нанесенного ущерба:

- информационные угрозы, повлекшие значительный ущерб;
- информационные угрозы, нанешие только частичный вред учреждению;
- информационные угрозы, не повлиявшие на работу организации.

По результатам кластеризации делаем вывод, что угрозы, которые могут повлечь значительный ущерб и частичный вред учреждению, гораздо ниже, чем не повлиявшие на работу организации. Для усиления защиты информации нужно проводить мероприятия и доработки нынешней системы безопасности.

При проведении первого этапа дискриминантного анализа мы имеем на входе угрозы информационной безопасности, разбитые на уровни OSI. Каждый уровень можно охарактеризовать несколькими угрозами, имеющими определенные классифицирующие признаки.

На втором этапе определяются данные, по которым можно было бы разделить наши исходные данные на две группы объектов. Вопрос состоит лишь в том, по какому же признаку нам их разбить? Все гораздо проще, чем думалось бы. Продвинутый пользователь ПК прекрасно знает, что эталонная модель взаимодействия открытых систем делится на:

- два самых низших уровня эталонной модели OSI, которые реализуются аппаратным и программным обеспечением;
- пять высших уровней, как правило, реализующиеся методом сетевого доступа.

На третьем этапе определяем угрозы, которые могут нанести ущерб для каждого уровня, их конкретное поражение программного и аппаратного обеспечения, возможные риски при их не обнаружении и способы обеспечения безопасной эксплуатации. В случае возникновения новых угроз, мы сможем отнести к определенной группе рисков и найти способы защиты от них.

Методы кластерного анализа и дискриминантного анализа позволяют разделить неоднородную совокупность наблюдаемых объектов на однородные группы и классифицировать эти группы. Подводя итог, мы делаем вывод о том, что с помощью данных методов можно выделить группу угроз, борьба с

которой имеет наиболее важное значение для обеспечения информационной безопасности в СПБУ МВД России.

СПИСОК ЛИТЕРАТУРЫ

1. Большакова Л.В., Примакин А.И., Яковлева Н.А. Применение кластерного и дискриминантного анализов в процессе обработки и интерпретации статистических данных при обеспечении экономической и информационной безопасности хозяйствующего субъекта // Вестник Санкт-Петербургского университета МВД России. - С.-Пб.: Изд-во С.-Петербург. ун-та МВД России, 2014, № 2 (62). - С. 148-156
2. Кремер Н.Ш., Теория вероятностей и математическая статистика. [Текст]: Учебник. /ЮНИТИ. / Н.Ш. Кремер. – М., 2007. -474 с.
3. Калинина, В.Н. Введение в многомерный статистический анализ [Текст]: Учебное пособие / В.Н. Калинина.- ГУУ. - М., 2010. - 66 с.

УДК 378

СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ МЧС РОССИИ

Саратов Дмитрий Николаевич¹, Подружжина Татьяна Александровна²

¹ Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, ул. летчика Пилутова, 1,

² Санкт-Петербургский университет ГПС МЧС России,
Россия, Санкт-Петербург, Московский пр. 149,
emails: pta_73@list.ru.ru, saratovdn@mail.ru

Аннотация: В тезисе затронуты вопросы подготовки специалистов в области информационной безопасности, а также рассмотрены проблемные вопросы обеспечения кадрами подразделений МЧС России.

Ключевые слова: информационная безопасность; обеспечение информационной безопасности; подготовка кадров.

MODERN CONDITION AND PROSPECTS FOR DEVELOPMENT OF THE TRAINING SYSTEM OF SPECIALISTS IN FIELDS OF INFORMATION SECURITY FOR EMERGENCY RUSSIA

Saratov Dmitry¹, Podrzhkina Tatyana²

¹St. Petersburg University of the Ministry of Internal Affairs of Russia,
Russia, St. Petersburg, st. pilot Pilutov, 1,

²St. Petersburg State University of Emergency Situations Ministry of Russia,
Russia, St. Petersburg, Moscow Ave, 149,
emails: pta_73@list.ru.ru, saratovdn@mail.ru

Abstract: The thesis touches upon the issues of training specialists in the field of information security, as well as the problematic issues of providing the personnel of the subdivisions of the Ministry of Emergencies of Russia.

Key words: information security; ensuring information security; personnel training.

Мы с вами живём в век практически тотальной информатизации. Интенсивное развитие и использование современных информационных технологий привели в настоящее время к серьезным качественным изменениям в экономической, социально-политической и духовной сфере общественной жизни. Человечество фактически переживает этап формирования нового информационного общества, несущего новые возможности. Вместе с тем это приводит и к росту угроз национальной, коллективной и личной безопасности, связанных с нарушением установленных режимов использования информационных и коммуникационных систем, ущемлением конституционных прав граждан, распространением вредоносных программ, а также с использованием возможностей современных информационных технологий для осуществления враждебных, террористических и других преступных действий.

01.10.2014 состоялось Заседание Совбеза РФ по проблеме информационной безопасности, на котором его секретарь – Николай Платонович Патрушев – отметил, что, начиная с 2010 года было совершено более 90 млн. атак на информресурсы РФ. Он уточнил, что только в 2014 году таких атак в отношении российского сегмента интернета было зафиксировано более 57 миллионов, особенно в период Олимпиады в Сочи, присоединения Крыма и во время событий на Донбассе. По опубликованным данным ежедневно в мире формируется около 7200 вредоносных программ, в год – более 2 миллионов; появились программы – шпионы. Указанные обстоятельства указывают на то, что особую остроту сегодня приобретает проблема обеспечения информационной безопасности (ИБ).

Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента России от 5 декабря 2016 г. № 646, констатирует, что информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности России.

При этом в качестве одного из приоритетных направлений государственной политики в области обеспечения ИБ определяется совершенствование подготовки кадров, развитие образования в этой сфере. Если рассматривать сегодняшнее состояние кадрового обеспечения ИБ, то следует отметить, что данный вопрос применительно к защите информации имеет в стране достаточную практическую реализацию и устойчивую тенденцию к положительной динамике. На сегодняшний день уже функционирует организованная система подготовки молодых специалистов и повышения квалификации специалистов, работающих в области защиты информации. Дальнейшая задача в этой сфере заключается в создании четкой государственной системы прогнозирования потребности в специалистах, разработке методологии формирования государственного заказа на их подготовку, развитии новых направлений и образовательных программ подготовки кадров, учитывающих принципиально междисциплинарный характер данной области деятельности.

Более того, обучение основам ИБ и защиты информации должно стать инвариантной составляющей информационной подготовки в рамках всех без исключения специальностей и направлений профессионального образования, служащей формированию информационной культуры личности на этапе перехода от постиндустриального к информационному обществу. Решение всех этих задач должно быть основано на системном подходе, учитывающем методологические, организационные, содержательные, дидактические и технологические аспекты.

Некоторые подходы к решению наиболее острых проблем, стоящих сегодня перед системой кадрового обеспечения ИБ, и являются предметом доклада, так как все вышеприведенные обстоятельства в полной мере относятся и к МЧС России.

МЧС является обладателем значительного объема информационных ресурсов, информационно-телекоммуникационных систем, систем сбора, хранения и обработки и передачи различных баз данных. Указанные виды информации и системы должны быть надёжно защищены от деструктивных воздействий. В качестве деструктивных воздействий могут выступать хищение, блокирование, модификация, уничтожение, несанкционированный доступ к информационным и системным ресурсам.

Деятельность по обеспечению безопасности информации возлагается на штатные подразделения (штатных специалистов) по защите информации. К сожалению, по результатам проведённых проверок соответствующими регуляторами отмечено, что в составе подразделений МЧС специалистов с профильным образованием в области информационной безопасности практически нет.

Удовлетворить потребность в высококвалифицированных специалистах в области обеспечения ИБ можно только на основе комплексного использования всех возможностей среднего, высшего и дополнительного профессионального образования. Кроме этого, необходимо отметить, что на сегодняшний день фактически нетронутым остается такой пласт, как подготовка кадров в области второй составляющей ИБ – защиты личности и общества от разрушающего воздействия информации. Справедливости ради надо сказать, что вторая составляющая ИБ гораздо сложнее, неопределеннее первой, что порождает особые трудности при решении соответствующих задач. Обеспечение сколько-нибудь эффективной защиты от негативной информации возможно лишь при наличии развитой законодательной и нормативно-правовой базы, процесс создания которой в России еще далеко не завершен.

Сегодня подготовка кадров в области ИБ имеет существенные особенности, поскольку выступает не только как реакция на спрос рынка в отношении таких специалистов, но и как важная составляющая комплекса мероприятий государства по противодействию угрозам в информационной сфере. Этими особенностями определяются и содержание подготовки указанных специалистов, и особые требования, предъявляемые к образовательным учреждениям при организации такой подготовки. В общей системе обеспечения ИБ государства кадровое сопровождение является самостоятельной подсистемой, а сама система подготовки специалистов выступает в качестве основы такого сопровождения.

Как было сказано выше, к настоящему времени в России сложились основы дееспособной системы подготовки и повышения квалификации специалистов, способных решать задачи обеспечения ИБ страны. Немаловажно и то, что российская система подготовки кадров в области ИБ занимает по ряду позиций ведущее положение, по крайней мере среди европейских стран, о чем свидетельствуют материалы регулярно проводимых конференций по образованию в области информационной безопасности.

На сегодняшний день эта система включает в себя следующие составляющие:

- пять ФГОС ВПО и разработанных на их базе ООП подготовки специалистов в области ИБ по специальностям: «Компьютерная безопасность», «Информационная безопасность автоматизированных систем», «Информационная безопасность телекоммуникационных систем», «Информационно-аналитические системы безопасности», «Безопасность информационных технологий в правоохранительной сфере»;

- два ФГОС ВПО по направлению «Информационная безопасность» (подготовка бакалавров и магистров);

- три ГОС среднего профессионального образования по специальностям: «Информационная безопасность телекоммуникационных систем», «Информационная безопасность автоматизированных систем», «Организация и технология защиты информации»;
- образовательные программы дополнительного образования и соответствующие курсы переподготовки и повышения квалификации;
- образовательные программы послевузовского профессионального образования в данной области (включая подготовка кадров высшей квалификации по специальности «Методы и системы защиты информации, информационная безопасность»);
- учебно-методическое объединение вузов России по образованию в области ИБ;
- более 150 вузов России (государственных и негосударственных), которые готовят специалистов по указанным специальностям;
- 29 региональных учебно-научных центров по проблемам ИБ в системе высшей школы.

К сожалению, в структуре образовательных учреждений МЧС проблеме подготовки кадров в области ИБ уделено недостаточное внимание.

В настоящее время только один вуз системы МЧС готовит специалистов по Информационной безопасности Санкт-Петербургский университет Государственной противопожарной службы МЧС России в Институте безопасности жизнедеятельности: ФГОС ВПО по направлению «Информационная безопасность» (подготовка бакалавров); ГОС ВПО по специальности: «Организация и технология защиты информации».

Решить проблему нехватки специалистов по ИБ с помощью только подготовки новых кадров с высшим и средним профессиональным образованием практически невозможно. Основными причинами такого положения являются:

- большой временной интервал процесса подготовки;
- явно недостаточное количество выпускаемых специалистов (среднее количество специалистов в области ИБ, выпускаемых в год высшими учебными заведениями страны, оценивается примерно в 1,7 тыс. человек, тогда как лишь государственным учреждениям ежегодно требуется порядка 3,5 тыс. человек);
- инерционность обучения, связанная с долговременной (в пределах одного цикла обучения) стабильностью учебных программ и планов (за это время требования к содержанию обучения существенно изменяются);
- сложность организации целевой подготовки специалистов в интересах конкретного органа власти или предприятия (к сожалению, в настоящее время не каждая организация может сформулировать требования к уровню знаний и умений специалиста в области ИБ);
- сложности с профессиональной ориентацией поступающих на обучение из-за проблем с реализацией принципа тщательного отбора кадров, обучающихся по специальностям и направлениям подготовки в области ИБ.

Последнее имеет очень важное значение. В то же время при существующей системе подготовки предполагается обучение молодых людей в возрасте 17–18 лет. Даже если кроме проверки знаний устраивать проверку психофизиологических характеристик (возможность практической реализации этого весьма сомнительна), то это вряд ли обеспечит эффективность отбора, так как за длительное время обучения данные параметры могут кардинально поменяться. Кроме того, выпускники могут пойти работать не по специальности или, что еще хуже, будут выполнять функции, противоположные защите.

В этой связи представляется, что развитие в области кадрового обеспечения ИБ для нужд МЧС в ближайшей перспективе должно получить дополнительное профессиональное образование. Среди несомненных достоинств этой формы обучения можно отметить малую длительность подготовки, гибкость учебных программ, простоту реализации целевой подготовки в интересах конкретных подразделений и структур МЧС, возможность наиболее полного удовлетворения потребности в специалистах различного уровня квалификации. Тем более, что ФСТЭК России разработаны типовые программы повышения квалификации практически по всем направлениям: «Администратор безопасности информации в автоматизированных системах», «Организация технической защиты информации в органах государственной власти», «Организация мероприятий по обеспечению безопасности информации в ключевых системах информационной инфраструктуры», «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных».

Однако здесь требуется дифференцированный подход к обучению, учитывающий различные категории обучающихся. Следует также соблюдать принцип, заключающийся в том, что специалист должен знать и уметь только то, что ему положено знать и уметь. Учитывая характер знаний и навыков у специалистов в области ИБ, можно сделать вывод, что знания в этой области должны получать только те, кому это необходимо, а круг обучаемых определяется исключительно потребностями подразделений МЧС, тем самым и реализуется целевой характер дополнительного профессионального образования.

Таким образом, подводя итоги можно сделать следующие основные выводы:

– во-первых, следует предпринять решительные шаги по формированию системы подготовки специалистов в области обеспечения ИБ в структуре МЧС, в противном случае можно оказаться в роли «догоняющих»,

– во-вторых, совершенно очевидно, что удовлетворить потребность в высококвалифицированных специалистах в области обеспечения ИБ в структуре МЧС можно только на основе комплексного использования всех возможностей среднего, высшего и дополнительного профессионального образования. Именно сочетание всех этих форм позволяет построить единую стройную систему подготовки кадров на основе непрерывности образовательного процесса и удовлетворить широкий спектр предъявляемых требований, как в содержательном, так и в квалификационном аспекте.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646)
2. Подружкина, Т. А. Проблемные вопросы подготовки кадров в области информационной безопасности в условиях стандартизации профессиональной деятельности / Т.А. Подружкина, Д.Ю. Федоров // Информационная безопасность регионов России (ИБРР-2015): матер. IX Санкт-Петербургской межрегион. конф., Санкт-Петербург, 28-30 октября 2015 г. – СПб.: СПОИСУ, 2015. – С. 349-350. (0.1 п.л.)

УДК 681.142

ОБЛАЧНЫЕ ТЕХНОЛОГИИ, КАК СРЕДСТВО ПРЕДУПРЕЖДЕНИЯ ПОТЕРИ ДАННЫХ

Синешук Юрий Иванович, Трубин Игорь Романович
Санкт-Петербургский университет МВД России
Россия, Санкт-Петербург, ул. Летчика Пилутова, 1,
emails: salikov.aleksandr92@mail.ru, sinegal@rambler.ru

Аннотация: Авторами рассматриваются технологии резервного копирования данных, позволяющие предотвратить катастрофическую потерю данных. Показано место и возможности применения облачных технологий в решении поставленных задач. Сформулированы проблемы и намечены пути их решения.

Ключевые слова: информационная безопасность; устойчивость; резервирование; облачная технология.

CLOUD TECHNOLOGY AS A MEANS OF PREVENTING THE LOSS OF DATA

Sineshchuk Yuri, Trubin Igor
Saint-Petersburg University of MIA of Russia
Russia, Saint-Petersburg, letchika Pilyutova Street 1,
emails: salikov.aleksandr92@mail.ru, sinegal@rambler.ru

Abstract: The authors consider technology data backup to prevent catastrophic loss of data. The place and possibilities of application of cloud technologies in solving the problems. Formulated the problems and ways of their solution.

Keywords: information security; stability; backup; cloud technology.

Введение. Одной из форм угроз информационной безопасности являются различные бедствия, влекущие за собой потерю данных. К числу бедствий можно отнести все, что влечет за собой потерю данных в сети. Причины бедствий самые разнообразные – от дел рук человеческих, до природных катаклизмов. Остановка сети, вызванная чрезвычайными причинами, всегда бедствие, всегда серьезное уменьшение производительности, устойчивости функционирования, другие непредсказуемые последствия с сопутствующими финансовыми потерями.

Существуют традиционные методы и системы, предупреждающие катастрофическую потерю данных: резервное копирование; отказоустойчивые системы; источники бесперебойного питания (UPS). В зависимости от ценности данных и бюджета организации могут использоваться все эти системы или любая из них,

Считается, что система резервного копирования – первая линия обороны. Надежная стратегия резервирования сводит к минимуму риск потери данных, поддерживая текущую резервную копию в таком состоянии, при котором файлы легко восстанавливаются в случае повреждения оригинальных данных. Выбор объектов для резервного копирования – целые диски, отдельные каталоги или файлы – зависит от того, насколько быстро нужно продолжить работу после потери важных данных, восстановив их. Критические данные должны резервироваться с разной периодичностью, в зависимости от степени их важности и от того, насколько часто они обновляются. Накопитель должен иметь емкость, превышающую емкость наибольшего сервера в сети. Он также должен обеспечивать поиск и коррекцию ошибок в течение всего процесса резервирования и восстановления.

Эффективная политика резервирования использует комбинацию методов.

Выделяют два способа планового сохранения всех или части данных, накапливаемых и используемых в автоматизированных системах, с целью восстановления их после возможной утраты в результате возникновения в компьютерной системе сбоев или отказов. Это архивирование и резервное копирование. Архивированием называют сохранение данных, которые не требуются в постоянном оперативном использовании. Возможно это программные продукты или пользовательские документы в электронном виде. Определение данных, подлежащих архивированию, осуществляется пользователем и выполняется в произвольные моменты времени по мере возникновения необходимости. В отличие от архивирования резервное копирование – это процесс сохранения избыточных копий данных, используемых оперативно. Цель получения резервных копий состоит в их использовании для восстановления данных в случае утери повреждения текущей копии (оригинала). С точки зрения обеспечения отказоустойчивости системы резервное копирование выглядит более важной операцией по сравнению с архивированием.

Организация этого процесса требует предварительного планирования для нахождения компромисса между актуальностью сохраняемых данных и загруженностью системы. С одной стороны, данные, сохраняемые в резервной копии, должны быть максимально приближены к текущим данным. С другой стороны, минимизация периода активизации процедуры резервного копирования может послужить серьезной помехой процессу решения задач пользователей.

Все множество процедур резервного копирования можно представить в виде трех классов: полное, наращиваемое и дифференцированное копирование.

Полное копирование. При его выполнении весь заданный набор данных (файлы, каталоги) регулярно переносится на альтернативный носитель. Такой метод резервирования наиболее надежен, так как сохраняется 100 % данных, и прост в аварийной ситуации, потому что восстанавливается полностью и сразу вся использовавшаяся информация. Издержками метода являются длительность получения резервной копии и ее значительный объем.

Наращиваемое (инкрементальное) копирование. Первое копирование данных происходит в полном объеме. В каждую последующую копию помещаются только те данные, которые подверглись модификации с момента сохранения предыдущей. После завершения некоторого цикла (например, раз в неделю) вновь реализуется полное копирование и процесс повторяется. Резервные копии имеют небольшой объем (кроме полной копии), сам процесс копирования осуществляется довольно быстро. Однако своеобразной платой за эти преимущества является относительно долгое восстановление данных: сначала восстанавливается полная копия, затем последовательно все остальные. К тому же в некоторых случаях при неверно выбранном критерии модифицирования данных, возможен пропуск некоторой их части.

Дифференцированное копирование (копирование по методу различий). При использовании этого подхода к резервному копированию стартовая копия также является полной. Последующие копии содержат только те данные, которые были модифицированы со времени создания первой. В известной мере это компромиссное решение относительно двух ранее рассмотренных подходов. В данном случае время создания резервируемых данных, равно как и их объем, существенно меньше, чем при полном копировании, но больше, чем при наращиваемом копировании. Однако для восстановления данных после возникновения нештатных ситуаций требуются только первая и последняя копии.

В начале 2000 годов появилась облачная технология, при которой пользовательская информация постоянно хранится на интернет-серверах и лишь временно кэшируется на стороне пользователя. При этом доступ к сервису можно получить используя не только стационарные компьютерные системы, но и любые другие вычислительные средства: ноутбуки, планшеты, смартфоны и т.д. Облачная технология обладает рядом достоинств: облачные технологии обеспечивают общий доступ и совместную обработку информационных ресурсов благодаря их синхронизации через сетевые сервера; обработка информации может осуществляться не локально, поэтому снижаются требования к подготовленности операторов различных функциональных систем; снимается вопрос дискового пространства на ЭВМ конечных пользователей; резервирование и синхронизация информации через облачные сервисы с их территориально распределенной структурой позволяет обеспечить необходимую репликацию циркулирующих данных между серверами и повысить устойчивость вычислительной системы.

Вместе с тем, как и любые другие компьютерные технологии, облачные технологии тоже имеют ряд уязвимостей: неправомерное использование облачных технологий; небезопасные программные интерфейсы (API); внутренние нарушители; уязвимости в облачных технологиях; утечка данных и др.

Заключение. Облачные технологии являются перспективным средством решения задачи предупреждения катастрофической потери данных в вычислительных системах. Их эффективное применение предполагает интеграцию в комплексную систему обеспечения информационной безопасности, что позволит исключить большую часть уязвимостей.

СПИСОК ЛИТЕРАТУРЫ

1. Синешук Ю.И., Синешук М.Ю., Пантиховский О.В. Информационно-логическая модель анализа и обеспечения устойчивости функционирования систем управления сложными организационно-техническими объектами. Научно-аналитический журнал Проблемы управления рисками в техносфере №2(22), 2012, с.6-12, СПбУ ГПС МЧС России

2. Запечников С.В. Обеспечение безопасности восстановительного резервирования информации в системах распределенного хранения данных – М.: МИФИ, 2005. –325с.
3. Джордж Риз. Облачные вычисления.- БХВ-Петербург. 2011. - 288с.

УДК 681.518

ОБ АВТОМАТИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ ДВИЖЕНИЕМ СПЕЦТРАНСПОРТА НА ПЕРЕКРЕСТКЕ С ИСПОЛЬЗОВАНИЕМ РАДИОМЕТОК

Смоленцева Линда Александровна, Потехин Владимир Семенович
Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, ул. Летчика Пилютова, 1,
emails: linda-smolenceva@mail.ru, vsp1945@gmail.com

Аннотация: Излагается подход, позволяющий обеспечить беспрепятственный проезд перекрестков спецтранспортом. Подход предполагает установку на спецтранспорт радиометок и разработку подсистемы управления светофором, считывающей данные с радиометок.

Ключевые слова: спецтранспорт, управление движением, радиометки.

ON AUTOMATION OF THE MOVEMENT MANAGEMENT PROCESS OF THE SPECIAL VEHICLES AT THE CROSSROADS WITH THE RFID USE

Smolentseva Linda, Potekhin Vladimir
St. Petersburg University at Russian Ministry of internal Affairs (MIA),
Russia, St. Petersburg, Pilot Pilyutov str., 1,
emails: linda-smolenceva@mail.ru, vsp1945@gmail.com

Abstract: An approach that will allow for the unobstructed passage of crossroads by special vehicles is presented. The approach assumes the RFID installation on special vehicles and the development of subsystem management of the traffic light that reads the data from RFID tags

Keywords: special vehicles, movement management, RFID (Radio Frequency Identification).

Введение. Статистика МВД свидетельствует о том, что количество нарушений правил дорожного движения в части блокирования беспрепятственного проезда транспортных средств, оснащенных специальными сигналами, год от года растет [1]. Поэтому руководство МВД России требует использования для организации эффективного управления автотранспортом всех доступных средств и способов, в том числе применения и современных информационных технологий [2, ст. 11]. Одна из идей, предполагающая использование радиометок [3] для автоматизации процесса управления спецтранспортом, родилась в московском Департаменте транспорта и Центре организации дорожного движения (ЦОДД) [4]. В этой связи тема данной работы представляется актуальной.

Для обеспечения приоритетного движения через светофоры автомобилей «скорой помощи», пожарных, полиции и других спецслужб, а также общественного транспорта предполагается использование радиометок. Светофоры предполагается оборудовать считывателями, которые смогут распознавать сигнал от RFID-меток, установленных на специальном и общественном транспорте, и максимально быстро – в течение 10-15 секунд — включать зелёный свет. Цена специальных RFID-меток для автомобилей сейчас составляет около 35-40 рублей, но при оптовых поставках она может существенно снижаться. Попадая в зону действия антенны, метки просто сообщают свой номер. RFID-метки должны быть вандало- и метеоустойчивы. Конструкция должна быть такова, чтобы её было нельзя снять с машины, не разрушив внутренний контур с микроантенной, что делает радиометку непригодной для установки ее на другой автомобиль. Антенна считывателя монтируется на определенном расстоянии от светофора. Считыватель ставится в закрытый ящик, а сервер, который принимает данные, может находиться где угодно. Один мощный считыватель может обслуживать до 10 антенн без особенной потери мощности, его пиковая скорость считывания — 150 меток в секунду [4].

Таков замысел ЦОДД, но для его реализации необходимо решение ряда организационно-технических задач, к числу которых, на наш взгляд, в частности, относятся:

- выбор радиометок, в наибольшей степени пригодных для автоматизации рассматриваемого процесса, и определение порядка установки радиометок на спецтранспорт [5], [6], [7];
- организация централизованного учета (создание интегрированной базы данных учета — ИБД-У) радиометок, установленных на спецтранспорт, путем дополнения сведениями о радиометках «Реестра регистрации транспортных средств», ведущегося в настоящее время, и содержащим пока лишь традиционные параметры, фиксируемые при регистрации автотранспорта [8], [9];
- установка стационарных считывателей на перекрестках в точках наиболее интенсивного потока автомобилей, где планируется автоматическое управление движением [10], [11];
- обеспечение возможности получения данных со считывателя и автоматического формирования запросов к ИБД-У с целью подтверждения принадлежности транспортного средства, оснащенного радиометкой, к спецтранспорту или общественному транспорту;

– обеспечение автоматического переключения светофора с целью предоставления возможности проезда спецтранспорта (общественного транспорта) в соответствующем направлении. При этом возможно, что для определения запланированного направления движения спецтранспорта, может потребоваться дополнение данных радиометки соответствующими сведениями, считываемыми с указателя поворота спецтранспорта.

Отметим, что большая часть перечисленных организационно-технических задач ранее решалась применительно к другим объектам исследований (например, к процессу въезда на охраняемую стоянку [12]) и требуется лишь адаптация выработанных решений к условиям управления спецтранспортом на перекрестках, но есть и задача, определяющая новизну данной работы. Это задача автоматической выработки управленческого решения переключения светофора в условиях конкуренции за проезд перекрестка двух и более спецтранспортов, одновременно пребывающих к перекрестку. Осуществление как адаптации ранее выработанных решений, так решение новой задачи требует проведения дополнительных исследований.

Закключение. Названный перечень организационно-технических задач возможно не является исчерпывающим, но все же позволяет составить общее впечатление о возможном подходе к автоматизации процесса управления спецтранспортом на перекрестках на основе использования радиометок. Решение перечисленных задач будет способствовать повышению эффективности работы правоохранительных органов с помощью внедрения в систему МВД технических и программных средств автоматизации, реализующих современные информационные технологии.

СПИСОК ЛИТЕРАТУРЫ

1. Сайт Госавтоинспекции. URL: <http://www.gibdd.ru/> (дата обращения: 12.09.2017).
2. Федеральный закон Российской Федерации от 7 февраля 2011 года № 3-ФЗ «О полиции» URL: http://www.consultant.ru/document/cons_doc_LAW_110165/ (дата обращения: 12.09.2017).
3. RFID // Википедия. URL: <http://ru.wikipedia.org/?oldid=80440746> (дата обращения: 12.09.2017).
4. RFID в транспортных системах / Сайт «Наука, технологии, инновации, консалтинг». URL: <http://altkonsalt.ru/rfid-v-transportnyih-sistemah/> (дата обращения: 12.09.2017).
5. Дальняя идентификация // Parsec URL: http://www.parsec.ru/rfid/?gclid=CjwKEAju97K_BRCwmNTK26iM-hMSJABrkNtbv0BQhIL9-PhLmj9lyTxlw2Wa28VER6fGKEpTBRs6RoCpSvw_wcB (дата обращения: 12.09.2017).
6. Активные радиометки // АО «СОКБ «Вектор» URL: <http://sokb-vektor.ru/produkcija/aktivnye-radiometki/> (дата обращения: 12.09.2017).
7. Багдасарян А., Багдасарян С., Бутенко В., Карапетян Г. Радиочастотные метки на ПАВ. Особенности конструкции технологии // Элементная база электроники. URL: http://www.electronics.ru/files/article_pdf/3/article_3459_509.pdf (дата обращения: 12.09.2017).
8. Приказ МВД России от 07.08.2013 № 605 «Об утверждении Административного регламента МВД РФ по предоставлению государственной услуги по регистрации автотранспортных средств и прицепов к ним». URL: http://www.consultant.ru/document/cons_doc_LAW_152842/ (дата обращения: 12.09.2017).
9. Регистрация автотранспортного средства в Госавтоинспекции // Портал госуслуг. URL: https://www.gosuslugi.ru/pgu/service/10000466914_10000027170.html#!description (дата обращения: 12.09.2017).
10. Власов М. RFID: 1 технология – 1000 решений: Практические примеры использования RFID в различных областях. М.: Альпина Паблишер, 2014. 218 с. ISBN 978-5-9614-4879-5.39.
11. RFID-оборудование ISBC для "Систем контроля и учета автотранспорта" // Сайт компании ISBC RFID. URL: <http://www.isbc-rfid.ru/applications/auto/> (дата обращения: 12.09.2017).
12. Технологии RFID идентификации // Сайт компании ISBC RFID. URL: <http://www.isbc-rfid.ru/applications/auto/> (дата обращения: 12.09.2017).

УДК 004.056

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ ЗАЩИТА СОТРУДНИКОВ СИЛОВЫХ СТРУКТУР

Ярмоленко Наталия Владимировна

Санкт-Петербургский военный институт внутренних войск МВД России

Россия, Санкт-Петербург, ул. Летчика Пилутова, 1

e-mail: nv_yarmolenko@mail.ru

Аннотация: В статье поясняется содержание информационно-психологической защиты сотрудников силовых структур и раскрываются основные источники угроз информационно-психологической безопасности.

Ключевые слова: безопасность личности; социальные практики безопасного поведения; личность как объект безопасности.

INFORMATION-PSYCHOLOGICAL PROTECTION OF EMPLOYEES OF POWER STRUCTURES

Yarmolenko Natalia

St. Petersburg Military Institute of the Russian Interior Troops

Russia, St. Petersburg, ul. Flyer Pilyutova, 1

Annotation: The article explains the content of information and psychological protection of law enforcement officers and reveals the main sources of information and psychological security threats.

Keywords: personal security; social practices of safe behavior; personality as an object of safety.

Повсеместное использование различных коммуникационных средств и информационных технологий связывают с разнообразными информационными воздействиями на психику человека, поэтому изучение механизмов действия угроз информационно-психологической безопасности личности является постоянной потребностью не только в повседневной жизни человека и его социальной практики, но и в профессиональной деятельности.

Угроза рассматривается как целенаправленные действия конкретных носителей враждебных намерений, воздействуя на объект – личность человека и его психическое состояние.

Манипуляции человеком, общественным мнением и массовым сознанием деструктивного характера могут наряду с межнациональными конфликтами, экологическими бедствиями и демографическими катастрофами превратиться в глобальную проблему для человечества современной эпохи.

Если свойства объекта безопасности ухудшаются посредством насильственного изменения, то угроза выступает в качестве возможности разрешения противоречия во взаимодействии объекта безопасности с другими объектами. Для защиты от внешних угроз разрабатываются специальные меры и локализация их ущерба. Основными характеристиками угроз представляются не только место проявления источника, но и его форма, вероятность предполагаемого ущерба, а также тип объекта безопасности. Для защиты от внешних угроз разрабатываются специальные меры, а также локализация их ущерба. Под психологической защитой личности подразумевается сложная система личностных механизмов предотвращения или нейтрализации угрожающих факторов, которые наносят ущерб человеку посредством использования различных средств и способов изменения процессов его информационно-психологического взаимодействия с различными социальными субъектами и информационной средой в целом. Благодаря интенсивному развитию открытых компьютерных сетей и новых информационно-коммуникационных технологий, размещение информационного ресурса на электронных носителях и увеличение концентрации информации в информационных системах различного рода, проблема защиты личных информационных ресурсов становится более актуальной.

Развитие сетевых технологий и технологий мультимедиа дало появлению еще одного вида воздействия на личность индивидуума как виртуальная реальность. Она предлагает новые возможности не только в сфере досуга и культуры, обещая новые несуществующие миры и переживания; интересные идеи «путешествий», но не географического плана. Такие виртуальные путешествия, как правило, небезопасны для личности. Такая технология таит в себе опасность манипулирования личностью и экспериментов над сознанием, апробируя новые методики психотренинга. Конечно, визуальные системы предлагают человеку легкий доступ к событиям и сюжетам, которые могут быть деструктивными для психики. Погружаясь в такие виртуальные реальности, человек не отдает себе отчета, куда это повлияет на состояние его психики.

Угрозы безопасности личности информационно-психологического характера, осуществляя разрушающие воздействия на психологическое состояние сотрудника, препятствуют полноценно развиваться ему и приспосабливаться к сложным социальным условиям, но при этом удовлетворяют его потребности и реализовывая гарантированные Конституцией, нормами федерального законодательства и международного права гражданские права и свободы. Угрозы информационно-психологической безопасности личности воздействуют не только на сознание человека, но и на систему его ценностей, психическое здоровье и свободу воли человека. Потребность в безопасности является необходимым условием нормального существования и развития. Поэтому человек так нуждается в ощущении своей связи с окружающим миром, другими людьми, в принадлежности к определенным социальным группам и общественным структурам. Рекомендуемые способы обеспечения информационно-психологической безопасности предлагают уход (отказ, отклонение от негативного воздействия), не восприятие негативной информации, блокирование критического восприятия или маскировка проявления своих эмоций. Таким образом, формируется информационная культура сотрудника, что и обеспечивает информационно-психологическую безопасность личности.

Источниками воздействия информационно-психологического характера на личность могут быть:

- государство (в том числе – иностранные государства), органы власти и управления и другие государственные структуры и учреждения;
- общество (различные общественные, экономические, политические и иные организации, в том числе зарубежные);
- различные социальные группы (формальные и неформальные, устойчивые и случайные, большие и малые по месту жительства, работы, учебы, службы, совместному проживанию и, проведения досуга и т.д.);
- отдельные личности (в том числе представители государственных и общественных структур, разнообразных социальных групп и т.п.) [1].

Отечественные исследователи, такие как Г.В. Грачев, Д.А. Ершов, С.К. Рощин, В.А. Соснин, предлагают различные меры защиты личности от информационно-психологического воздействия и поддерживают правовые формы решения проблемы на законодательном уровне, перенося ответственность на провайдеров или потребителей информации. К важным правовым актам

противодействия угрозам информационно-психологической безопасности необходимо считать следующие:

1. Защита информации, представляющей угрозу интересам всех субъектов и объектов РФ, от несанкционированного доступа.
2. Мониторинг информации о субъектах и объектах экстремисткой и террористической деятельности.
3. Мониторинг анонимных денежных потоков в сети Интернет.
4. Противодействие пропагандистским устремлениям экстремисткой и террористической идеологии.
5. Рассмотрение технической и правовой возможности привязки пользователя (или технического средства) к информации, выложенной в Интернете [3].

Но процессы информационно-психологического воздействия на человека могут изменяться как им самим, так и в его интересах другими людьми и социальными субъектами различного уровня сложности, системно-структурной и функциональной организации. Иными словами, психологическая защита личности – это использование разнообразных средств и способов изменения процессов информационно-психологического взаимодействия человека с различными социальными субъектами и информационной средой в целом для предотвращения или нейтрализации угрожающих факторов, способных нанести ему ущерб.

Для сотрудника может представлять информационно-психологическую опасность деятельность различных группировок и объединений людей, в частности, некоторых политических партий, общественно-политических движений, националистических и религиозных организаций, финансово-экономических и коммерческих структур, лоббистских и мафиозных групп.

Таким образом, благодаря развитию информационных технологий расширяются методы негативного информационно-психологического воздействия на личности военнослужащих, наблюдается эволюция различных форм терроризма, где огромное значение приобретает информационно-психологическая составляющая. Средства психологической защиты личности связаны с изменением процессов ее информационно-психологического взаимодействия с информационной средой для предотвращения или нейтрализации угрожающих факторов, способных нанести ущерб человеку. Важнейшим и приоритетным направлением деятельности правоохранительных органов должно стать обеспечение необходимого уровня безопасности обрабатываемой информации, надежная защита сознания и психики личности от негативного информационного воздействия.

СПИСОК ЛИТЕРАТУРЫ

1. Грачев Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты / Г.В. Грачев. – М.: 2003.
2. Манойло А.В. Государственная информационная политика в особых условиях. Монография, М. 2003.
3. Примакин А.И. Куватов В.И., Якушев Д.И. Противодействие террористическим и экстремистским организациям в сети Интернет [Текст] // Вестник Санкт-Петербургского университета МВД России. 2015. № 1 (65) – С. 91-95.



БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

УДК 621.39

БЕЗОПАСНОСТЬ ДОСТУПА К ОБРАЗОВАТЕЛЬНЫМ РЕСУРСАМ ПРИ ИСПОЛЬЗОВАНИИ УДАЛЕННОГО ДОСТУПА

Анисимов Андрей Владимирович

Смольный Институт РАО Россия, Санкт-Петербург, Полюстровский пр., 59

email: avanisimov@yandex.ru

Аннотация: В статье рассматриваются вопросы информационной безопасности: конфиденциальность, целостность и доступность. Обязательное условие использования образовательного ресурса – это его защита и возможность администрирования, как преподавателями, так и техническим персоналом образовательного учреждения. Получены требования к доступу в интернет на скоростях, необходимых в соответствии с техническими условиями.

Ключевые слова: информационная безопасность, конфиденциальность, целостность, доступность, пользователь образовательный ресурс.

SECURITY OF ACCESS TO EDUCATIONAL RESOURCES BY REMOTE ACCESS

Anisimov Andrey Vladimirovich

Smolny Institute of RAO, Russia, Sankt-Peterburg, Polyustrovskiy pr., 59

email: avanisimov@yandex.ru

Abstract: the article considers the questions of information security: confidentiality integrity, and availability. Obligatory use of the educational resource is his defense and ability to administer both teachers and technical staff of the educational institution. Derived requirements for the Internet access at the speeds required in accordance with the technical conditions.

Keywords: information security, confidentiality, integrity, availability, user, educational resource.

Введение. Под безопасностью будем подразумевать следующие аспекты аспекта информационной безопасности: конфиденциальность целостность и доступность. Доступ к образовательным ресурсам – это как избирательный, так и обязательный подходы к обеспечению безопасности данных.

Пользователь образовательного ресурса запрашивает данные путем обращения к программе, установленной на устройстве клиента. Различными устройствами клиента могут быть как стационарные компьютеры, так и портативные мобильные телефоны. Таким образом, средства подготовки запросов и обработки ответов обращаются к набору коммуникационных программ в составе клиента. Избирательный подход к обеспечению безопасности – пользователи обладают различными правами, или привилегиями, и полномочиями при работе. Обязательный подход к обеспечению безопасности - каждому присваивается некий квалификационный уровень и пользователю предоставляются права если есть права доступа. Такие системы проще в управлении. Электронная образовательная среда при этом ведет себя как тематическое приложение, созданное разработчиком с использованием стандартов, функций и инструментальных средств. Клиент обращается к аппаратным средствам коммуникаций с использованием технологии сетевого соединения в процессе проведения сеанса связи через беспроводные сетевые адаптеры в соответствии со стандартами IEEE. Обязательное условие реализации такой сети – это защита образовательного ресурса и возможность администрирования как преподавателями, так и техническим персоналом образовательного учреждения, поэтому в составе сети должна быть предусмотрена базовая станция, объединяющая действия этих категорий пользователей. Тем самым обеспечивается доступ в интернет через беспроводное объединение компьютеров сети на скоростях, необходимых в соответствии с техническими условиями.

В беспроводных ЛВС технология IEEE 802.1x применяется при использовании оборудования компании Cisco, которая разработала протокол LEAP как реализацию EAP-аутентификации для беспроводных ЛВС, основанную на передаче дайджеста (hash) вызов-пароль. Этот протокол обеспечивает взаимную аутентификацию клиентского устройства и точки доступа, на основе динамического WEP-ключа. Тестирование эффективности доступа можно осуществить с помощью беспроводной платы с точкой доступа к оборудованию компании Cisco, при этом необходимо

использование протоколов RADIUS, выбор конкретной реализации этого протокола зависит от требований по качеству обслуживания. Конфигурация поддержки LEAP на точке доступа, осуществляется через порт, используемый сервером RADIUS. Права доступа определяются при помощи разделяемого ключа при активизировании режима EAP. На сервере RADIUS регистрируется точка доступа Cisco в качестве клиентского устройства.

Для тестирования протоколов доступа к электронной образовательной среде на базе беспроводных сетей можно воспользоваться алгоритмом EAP-TLS со службами IAS (RADIUS-сервер) и Active Directory. Для взаимной аутентификации в EAP-TLS используются цифровые сертификаты, которые можно получить в соответствии с существующими стандартами. При этом в процессе тестирования сервер RADIUS используется для передачи цифрового сертификата клиентской станции. В конце процедуры тестирования аутентификация обучаемого и технического персонала позволяет получить необходимую защиту данных, используемых в учебном процессе. Пользователь программы образовательной среды, установивший у себя на компьютере соответствующее программное обеспечение, становится зарегистрированным пользователем. Каждый зарегистрированный пользователь имеет свой уровень доступа, определяемый договором, и секретности.

При использовании специализированной реализации RADIUS сервера, выполняющей функции аккаунтинга, можно обеспечить получение информации о MSISDN и других атрибутах пользователей, вошедших в сеть и получивших IP-адрес, и сохранить ее в базе данных (MySQL). Специализированная реализация RADIUS-сервера имеет возможность обработки RADIUS-пакетов пользователей: добавления/изменения атрибутов по заданным условиям и пересылки таких пакетов на другие RADIUS-сервера. Гибкость конфигурирования обеспечивается применением XML-технологий. Особенность такого подхода по сравнению с аналогами - условная обработка атрибутов пакетов, расширенная система рассылки пакетов, TCP интерфейс быстрого доступа к сессионной информации. Другие модули системы получают информацию путем подключения по TCP к модулю идентификации пользователей. В случае использования серверов RADIUS сторонних производителей имеется возможность запроса атрибутов непосредственно из базы данных MySQL. Proxy-сервер, находящийся между WAP-шлюзами и Internet, управляет доступом пользователей образовательной среды на Internet-ресурсы с возможностью запрета доступа конкретным пользователям на определенные ресурсы. Электронная образовательная среда при этом ведет себя как тематическое приложение, ведет запись журнала доступа в Internet, а также журнал для отдельных пользователей или ресурсов.

Модуль мониторинга электронной образовательной среды как тематического приложения позволяет удаленно (с помощью web-интерфейса) контролировать наличие IP-трафика между модулями системы. Для каждого модуля контролируется количество процессов, занимаемая ими память и загрузка процессора. Дополнительно контролируется свободное место на диске. При возникновении критических ситуаций аварийные модули могут быть перезапущены. Модуль мониторинга в соответствии с конфигурационными файлами собирает информацию о состоянии системы и может отдать эти параметры по запросу через сетевой интерфейс. Модуль мониторинга должен быть запущен с привилегиями, позволяющими запускать скрипты, которые фигурируют в его файле конфигурации. При запуске электронной образовательной среды открывается серверный сокет, в соответствии с параметрами конфигурации, который ожидает запросов от модуля WEB/WAP интерфейсов. Помимо инструкций и распоряжений руководства учебного центра администрирование основывается на стандартах, описанных в RFC [1], [2]. Статистика электронной образовательной среды формируется в соответствии с конфигурацией. Для подсчета статистики по трафику, модуль мониторинга запускает tcpdump (местонахождение файла tcpdump описывается в файле конфигурации). Система статистики электронной образовательной среды предназначена для формирования статистических отчетов по запросам пользователей, обработанных с помощью WAP Gateway. Источником информации для сбора статистики служат log-файлы модулей, входящих в состав WAP Gateway. Система статистики формирует ежедневные технологические отчеты, ежедневные отчеты по производительности WAP Gateway, а также подробные ежемесячные отчеты.

Заключение. Образовательная система в информационном обществе нуждается в эффективной защите, которая может быть обеспечена на основе современных информационных технологий.

СПИСОК ЛИТЕРАТУРЫ

1. Beadles M., Mitton D., "Criteria for Evaluating Network Access Server Protocols", RFC 3169, September 2001
2. Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

УДК 004.056

ОРГАНИЗАЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Барышникова Надежда Юрьевна, Егоров Александр Николаевич, Крупенина Наталия Викторовна
Государственный университет морского и речного флота имени адмирала С.О. Макарова,
Россия, Санкт-Петербург, ул. Двинская, 5/7,
emails: baryshnikova.n.yu@gmail.com, eanspb@rambler.ru, nvkrup@rambler.ru

Аннотация: В статье рассмотрены проблемы организации информационной безопасности, возникающие в информационной системе. Приводятся основные инструменты для поиска уязвимостей.

Ключевые слова: информационная безопасность; поиск уязвимостей; защита информации; информационная система

ORGANIZATION OF INFORMATION SECURITY IN THE INFORMATION SYSTEM

Baryshnikova Nadezhda, Egorov Aleksandr, Krupenina Nataliya
Admiral Makarov State University of Maritime and Island Shipping,
Russia, St. Petersburg, Dvinskaya str., 5/7,

emails: baryshnikova.n.yu@gmail.com, eanspb@rambler.ru, nvkrup@rambler.ru

Abstract: The article considers the problems organization of information security arising the information system. The main tools with search for vulnerabilities are provided.

Keywords: information security; vulnerability search; data protection; information system

Введение. В последнее время участились случаи атаки на информационные системы (ИС), в частности, на ИС банков. При этом одной из основных целей злоумышленников является хищение денежных средств пользователей посредством, например, подмены данных в файлах, выгружаемых из учетной системы и передаваемых в другие системы при дистанционном обмене данными между несколькими филиалами банка. Подмену осуществляет вредоносное программное обеспечение, которым заражаются компьютеры клиентов. В связи с этим определяются основные требования к эффективной организации информационной безопасности не только для ИС банков, но и для остальных типов ИС. В частности, обеспечение защищенного исполнения запросов пользователей, предоставление требуемой информации из базы данных, обработка полученных данных [1] и безопасный дистанционный обмен данными. Следовательно, задача поиска возможных уязвимостей в ИС является актуальной и требует более детального анализа с последующим решением обнаруженных проблем. Следует отметить, что указанная задача не потеряет актуальность и на ближайшую перспективу в виду постоянного совершенствования методов хищения информации и появления нового вредоносного программного обеспечения [2].

На практике уязвимости ИС в основном связаны с возникновением следующих угроз информационной безопасности:

- несанкционированный доступ к информации, хранящейся в таблицах базы данных;
- несанкционированный доступ к сети;
- умышленное причинение вреда злоумышленником и т.д.

Возникновение описанных угроз чаще всего связано с выбранным разработчиком вариантом реализации ИС [3], который может повлечь за собой следующие проблемы, связанные с информационной безопасностью:

- инъекция кода;
- SQL-инъекция;
- подделка запросов в клиент-серверном варианте работы пользователя;
- ошибки ввода данных пользователем и т.д.

Большинство из существующих проблем информационной безопасности можно решить еще на этапе разработки ИС, а именно во время проектирования и построения архитектуры и составляющих ее компонент. Для этого предлагается сразу включить соответствующий требуемому уровню организации общей безопасности набор функций и методик таких как:

- применение шифрованных протоколов обмена данными между клиентской и серверной частью;
- использование перед началом работы ИС процедуры проверки хэш-функции исполняемого приложения и библиотек с целью защиты ИС от возможных инъекций кода и SQL-инъекций;
- использование защиты от дизассемблирования;
- контроль памяти и возможных утечек памяти;
- защита от переполнения буфера;
- анализ вводимых пользователем данных;
- экранирование спецсимволов, служебных слов, идентификаторов и ключевых слов языка запросов ИС во вводимых пользователем запросах;
- своевременный контроль закрытия соединений с базой данных и завершения работы пользователя и т.д.

После завершения проектирования и построения архитектуры и составляющих ее компонент, осуществляется применение разработчиком защитных функций и методик. При этом анализ безопасности зачастую осуществляется с использованием готовых разработок или коммерческих программных продуктов. Поиск уязвимостей в программном коде ИС сводится к следующим двум основным действиям:

- выявление переполнения буфера с целью защиты от выполнения произвольного вредоносного кода уязвимой программой, выполнившей переполнение памяти;
- выявление ошибок ввода с целью защиты от инъекций кода и SQL-инъекций.

В настоящее время существует достаточно большое количество готовых инструментальных средств, предназначенных для автоматизации поиска уязвимостей. Они основаны либо на использовании методов статического анализа, который анализирует исходный программный код всей ИС без его последующего исполнения, либо на использовании методов динамического анализа, который позволяет производить отладку во время исполнения программного кода. К основным статическим анализаторам можно отнести:

- ITS4;
- RATS;
- PScan;
- Flawfinder и т.д.

Принцип работы базируется на применении лексического и синтаксического анализов программного кода, поэтому результаты поиска уязвимостей, предоставленные данными анализаторами, могут быть некорректными. Тогда в дополнение к ним применяют следующие основные динамические анализаторы:

- BOON;
- MOPS;
- Viva64 и т.д.

В их основе используется глубокий семантический анализ, автоматизирующий процессы сканирования исходных программных кодов. Применение всех вышеперечисленных методов анализа в совокупности позволяет эффективно и быстро осуществлять поиск уязвимых мест в ИС.

Также в последнее время для уменьшения количества расходов, направленных на закупку готовых инструментальных средств для поиска уязвимостей, все чаще используют современные методы принятия решений, например, применение нечеткой логики при решении задач оценки уровня информационной безопасности на этапе реализации ИС.

Заключение. В статье рассмотрены проблемы информационной безопасности, возникающие в ИС. Существует огромное количество инструментов и способов анализа для организации поиска возможных уязвимостей. Но только их комплексное применение позволит получить наиболее лучший результат в области достижения безопасности ИС.

СПИСОК ЛИТЕРАТУРЫ

1. Барышникова Н.Ю. Организация интеллектуально диалога с пользователем в среде «1С: Предприятие» / Н.Ю. Барышникова, А.Н. Егоров, Н.В. Крупенина // Новые информационные технологии в образовании: Сборник научных трудов XVII международной научно-практической конференции «Новые информационные технологии в образовании» (Инновации в экономике и образовании на базе технологических решений «1С»). М.: ООО «1С-Пабблишинг». 2017. Ч. 1. С. 522–525.
2. Андреев Н.О. Современные проблемы безопасности корпоративных сетей // Прикладная информатика. 2008. № 1. С. 25–31.
3. Тимофеев А.Э. Типовые уязвимости в программном обеспечении, предоставляющем защиту информации с помощью криптографических методов / А.Э. Тимофеев, И.В. Лунегов // Фундаментальные и прикладные проблемы механики, математики, информатики: сборник трудов научно-практической конференции. Пермь: ФГБОУ ВПО «Пермский государственный национальный исследовательский университет». 2015. С. 335.

УДК 004.056

НЕБЕЗОПАСНОСТЬ МОБИЛЬНЫХ УСТРОЙСТВ

Башмаков Алексей Васильевич

Государственный университет морского и речного флота имени адмирала С.О. Макарова,
Россия, Санкт-Петербург, ул. Двинская, 5/7,
email: abashm@mail.ru

Аннотация: В статье рассмотрены актуальные угрозы информационной безопасности, вызванные применением мобильных устройств, и даны рекомендации по их минимизации.

Ключевые слова: мобильные устройства; угрозы информационной безопасности; мобильные приложения; киберпреступления.

INSECURITY OF MOBILE DEVICES

Bashmakov Alexey

Admiral Makarov State University of Maritime and Inland Shipping,
Russia, Saint-Petersburg, Dvinskaya st., 5/7,
email: abashm@mail.ru

Abstract: The article presents current information security threats of mobile devices and recommendations for their minimization.

Keywords: *mobile devices; information security threats; mobile apps; cybercrime.*

Введение. Мобильные устройства стремительно проникают во все сферы жизни человека, становясь основным способом нашего взаимодействия с окружающим миром и внушительным хранилищем личной информации. Как известно, обратной стороной популярности любой технологии является ее использование в противоправных целях. К сожалению, ситуация с мобильными устройствами не является исключением из этого правила и возможности современных мобильных устройств широко используются киберпреступниками.

Типовое мобильное устройство представляет собой довольно мощный компьютер, обладающий малым размером и весом, как минимумом одним беспроводным интерфейсом доступа к Сети, встроенной несъемной памятью, операционной системой и возможностью установки приложений [3].

Мобильное устройство может многое «рассказать» о своем владельце, ведь в его памяти хранятся: контакты коллег, друзей и близких, зачастую содержащие большой объем их личных данных; журнал звонков; корпоративная переписка; параметры точек доступа Wi-Fi, которые расположены в пределах ареала обитания владельца; приложения социальных сетей с сохраненными паролями; банковские реквизиты или мобильный банкинг, фотоснимки, видеозаписи, заметки и пр. Абстрактная стоимость хранимой деловой и личной информации может превышать цену самого устройства [7].

Сами же мобильные устройства издавна являются «идеальными» средствами подслушивания. Ещё в 1998 руководитель службы госбезопасности Швеции (SEPO) Андре Эрикссон публично предупредил граждан страны, чтобы они не брали мобильные телефоны на те деловые встречи, где обсуждается конфиденциальная информация. По свидетельству Эрикссона, все сотовые телефоны можно использовать для подслушивания даже тогда, когда они находятся в нерабочем состоянии [6]. Ситуация с тех пор в лучшую сторону не поменялась. Привести современное мобильное устройство в «нерабочее» состояние не так уж просто. Нажимая на кнопку выключения, мы лишь переводим устройство в режим ожидания (stand-by), но оно продолжает функционировать с теми возможностями, которые в них заложены не только на аппаратном, но и на программном уровне. В связи с тем, что аккумуляторы подавляющего большинства мобильных устройств без отвертки не извлекаются, такие устройства невозможно гарантированно отключить.

Если дополнительно принять во внимание то, что мобильные устройства мы всегда носим с собой и переживаем, когда их забываем, регулярно заражаем аккумуляторы, берем на все важные мероприятия, то становится неудивительным, что злоумышленники разных мастей проявляют к ним повышенный интерес.

Причем «злоумышленниками» не обязательно должны быть спецслужбы, обладающие судя по откровениям Эдварда Сноудена [2] и последним утечкам из ЦРУ [4] беспрецедентными возможностями по контролю самих мобильных устройств и отслеживанию их местоположения [1]. Возможности злоумышленного взаимодействия с нашими мобильными устройствами значительно расширились благодаря развитию рынка мобильных приложений. Многие из них регулярно передают значительное количество данных третьим сторонам. Таким образом, для получения доступа к мобильному устройству необязательно взламывать операционную систему смартфона, достаточно убедить пользователя установить «полезное» приложение.

Отдельную проблему для безопасности хранимых на мобильных устройствах данных составляют установленные на них операционные системы. Во-первых, операционные системы, судя по пользовательским соглашениям, на вполне законных основаниях щедро собирают информацию и следят за действиями пользователей для благой цели - «улучшения качества обслуживания» и показа таргетированной рекламы. Во-вторых, в операционных системах мобильных устройств практически еженедельно выявляются серьезные уязвимости. Ситуация усугубляется тем, что даже если разработчики оперативно выпускают обновления, закрывающие уязвимость, нет никакой уверенности что обновления дойдут до конечных пользователей и их мобильных устройств. Выпуск обновлений (в том числе и критических), ложится на плечи производителей устройств, а им порой требуются месяцы, чтобы выпустить даже самые экстренные обновления. Обновления для мобильных устройств, произведенных более 1,5 лет назад, могут вообще не выпускаться.

Для защиты от рассмотренных угроз правильнее всего не использовать мобильные устройства вообще. Если данный вариант неприемлем, то целесообразно следовать следующим базовым рекомендациям, отранжированным по их эффективности:

1. Не накапливать и не обрабатывать на мобильных устройствах ту информацию, которую не хотите предоставлять 3 лицам.

2. Использовать самые простые мобильные устройства с ограниченным функционалом (например, вместо смартфонов применять сотовые телефонные аппараты) или применять сотовые телефонные аппараты в защищенном исполнении, оснащенные средствами защиты, предназначенными для предотвращения возможной утечки акустической и визуальной информации (например, изделие «Телефон-В» производства ЦБИ МАСКОМ [5]).

3. Не устанавливать мобильные приложения из недоверенных источников. Вероятность загрузки вредоносных приложений из официальных интернет-магазинов приложений от разработчиков

мобильных операционных систем невысока. При установке приложений обращайте внимание на запрашиваемые ими разрешения. Остерегайтесь тех приложений, которые запрашивают избыточный доступ.

4. Своевременно устанавливать исправления безопасности операционных систем и приложений мобильных устройств.

Заключение. Мобильные устройства в настоящее время для большинства людей являются основным способом взаимодействия с окружающим миром и внушительным хранилищем личной информации. Соблюдение приведенных в статье базовых рекомендаций позволит уменьшить риски информационной безопасности и снизить возможные негативные последствия от их использования.

СПИСОК ЛИТЕРАТУРЫ

1. How the NSA is tracking people right now // The Washington Post. 2013. [Электронный ресурс] // URL: <https://apps.washingtonpost.com/g/page/national/how-the-nsa-is-tracking-people-right-now/634/> (дата обращения 18.09.2017).
2. Marcel Rosenbach, Laura Poitras, Holger Stark How the NSA Accesses Smartphone Data // SPIEGEL ONLINE. 2015. [Электронный ресурс]. URL: <http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html> (дата обращения 11.09.2017).
3. Murugiah Souppaya, Karen Scarfone. Guidelines for Managing the Security of Mobile Devices in the Enterprise // NIST Special Publication 800-124 Revision 1 [Электронный ресурс]. URL: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf> (дата обращения 11.09.2017).
4. Vault 7: Projects // Wikileaks. 2017. [Электронный ресурс]. URL: <https://wikileaks.org/ciav7p1/> (дата обращения 18.09.2017).
5. Каталог оборудования и программного обеспечения // Группа компаний МАСКОМ. 2017. [Электронный ресурс]. URL: <http://www.mascom.ru/catalog/#p=87> (дата обращения 18.09.2017).
6. Киви Берд Гигабайты власти. Информационные технологии между свободой и тоталитаризмом. – М: Бестселлер, 2004 – 105 с.
7. Маньшин Г.Г., Артамонов В.А. Проблемы безопасности мобильных устройств и систем. Фундаментальные проблемы системной безопасности: материалы II школы-семинара молодых ученых (02 - 04 июня 2015). – Елец: Елецкий государственный университет им. И.А. Бунина, 2015. – 270с.

УДК 004.056; 003.26

ПРИМЕНЕНИЕ АЛГОРИТМА РЕШЕНИЯ КУБИЧЕСКИХ УРАВНЕНИЙ В КОНЕЧНОМ БИНАРНОМ ПОЛЕ В ОТРИЦАЕМОМ ШИФРОВАНИИ

Будчан Дарья Сергеевна

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5,
email: daria.budchan@mail.ru

Аннотация: В статье рассмотрены протокол отрицаемого шифрования и алгоритм решения кубических уравнений в конечно бинарном поле. Рассмотрены алгоритм решения кубических уравнений в простом конечном поле и алгоритм решения квадратных уравнений в бинарном конечном поле, на основе которых может быть разработан необходимый алгоритм.

Ключевые слова: отрицаемое шифрование, конечное бинарное поле.

ADAPTATION OF THE ALGORITHM FOR SOLVING CUBIC EQUATIONS IN A FINITE BINARY FIELD FOR DENIED ENCRYPTION

Budchan Darya

The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
email: daria.budchan@mail.ru

Abstract: The article presents the denied encryption protocol and the algorithm for solving cubic equations in a finite binary field. An algorithm for solving cubic equations in a simple finite field and an algorithm for solving quadratic equations in a binary finite field are considered, a necessary algorithm can be developed on the basis of algorithms.

Keywords: denied encryption, finite binary field.

Введение. В настоящее время имеется ряд работ, в которых предлагается способ отрицаемого шифрования, суть которого состоит в генерации шифртекста в виде набора коэффициентов уравнений второй, третьей и четвертой степеней. Разработка алгоритма решения кубических уравнений в конечном бинарном поле позволит увеличить криптостойкость протоколов, в основе которых будет лежать данный алгоритм.

В современном мире одним из системообразующих факторов жизни общества является интенсивное развитие информационной сферы с постепенным переходом к информационному обществу. При этом одной из ключевых составляющих сферы является безопасность личных, коммерческих и государственных данных.

Информационная безопасность включает в себя обеспечение конфиденциальности, целостности и доступности информации. Всё это достигается применением различных алгоритмов шифрования исходных данных.

Существуют различные методы шифрования: симметричные и асимметричные, блочные и потоковые. Одним из новых способов криптографического преобразования является отрицаемое шифрование.

В современных каналах связи используются многобитовые последовательности, которые можно интерпретировать как элементы конечных полей. Важной задачей становится поиск решений уравнений в полях больших степеней и представление их в виде битовых строк [1].

Ранее был разработан алгоритм решения кубических уравнений в простом конечном поле [2]. В таком случае процедура расшифрования состоит в решении кубического уравнения в конечном поле и получении однозначного ответа, благодаря чему устраняется проблема неоднозначности расшифрованного текста.

На основе разработанного алгоритма был предложен способ отрицаемого шифрования. Отрицаемое шифрование представляет собой способ криптографического преобразования, в котором зашифровываются совместно два или более различных сообщения на двух или более различных ключах [3]. Этот метод обеспечивает возможность правдоподобного отрицания наличия одного или группы сообщений как таковых.

Однако возникла задача повысить криптостойкость такого протокола. Для этого было предложено проводить вычисления не в простом, а в бинарном конечном поле.

Имеются определённые отличия в задачах решения уравнений в полях различной характеристики. Решение квадратных уравнений в простых полях нечётной характеристики приводит к задаче вычисления символа Лежандра [4]. В свою очередь решение квадратных уравнений в полях характеристики «два» имеет свою специфику, поскольку решаемое уравнение в стандартном виде оказывается линейным.

В ряде работ, посвящённых решению уравнений различной степени в конечных полях, имеются алгоритмы решения квадратных уравнений в бинарном конечном поле. Для рассмотрения подобных алгоритмов важно знать ряд теоретических понятий, таких как след, полуслед. Имеются способы приведения квадратного уравнения в поле характеристики два к стандартному виду. Для решения такого квадратного уравнения в конечных бинарных полях используется формула полуследа [1].

На основе имеющихся алгоритмов и способа решения кубических уравнений в простом конечном поле необходимо разработать алгоритм решения кубических уравнений в бинарном поле. Такой алгоритм упростит процедуру расшифровки и сократит временные затраты, а также повысит криптостойкость протокола шифрования. После представления полученных решений в виде битовых строк их можно передавать по каналам связи. Это позволяет унифицировать и оптимизировать процесс решения.

Алгоритмы решения кубических уравнений в конечном поле могут быть использованы для построения протокола отрицаемого шифрования, который может применяться в защищённых распределённых вычислениях, тайном электронном голосовании и защите от скупки голосов.

Закключение. Имеющиеся в настоящее время алгоритмы решения кубических уравнений в простом конечном поле и квадратных уравнений в бинарном конечном поле позволяют разработать алгоритм решения кубических уравнений в конечном поле характеристики два. Такой алгоритм может лежать в основе протокола отрицаемого шифрования. Составленный таким образом протокол может применяться в различных системах и технологиях, повышая криптографическую безопасность.

СПИСОК ЛИТЕРАТУРЫ

1. Глуско Кр.Л. Арифметический алгоритм решения квадратных уравнений в конечных полях характеристики два / Кр.Л. Глуско, С.С. Титов // Доклады ТУСУРа. – № 1 (25), ч. 2. – С. 148–152.
2. Молдовян Н. А., Молдовян Д. Н., Вайчикаускас М. А. Генерация кубических уравнений как способ открытого шифрования // Вопросы защиты информации. 2015. №2. С. 3–7.
3. Молдовян Н. А., Вайчикаускас М. А. Расширение криптосхемы Рабина: алгоритм отрицаемого шифрования по открытому ключу // Вопросы защиты информации. 2014. № 2. С. 12–16.
4. Болотов А.А. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых / А.А. Болотов, С.Б. Гашков, А.Б. Фролов. – М.: КомКнига, 2006. – С. 76–81.

УДК 004.056

РАЗРАБОТКА ТЕХНОЛОГИИ УПРАВЛЕНИЯ ПРОЦЕССОМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ WEB – ПРИЛОЖЕНИЯ

Бурлов Вячеслав Георгиевич, Петров Сергей Вадимович, Грозмани Елена Сергеевна
Санкт-Петербургский политехнический университет Петра Великого,
Россия, Санкт-Петербург, ул. Политехническая, 29,
emails: burlovvg@mail.ru, c.petrov@gmail.ru, grozmani.el@yandex.ru

Аннотация: Обеспечение информационной безопасности web-приложения — это деятельность, направленная на предупреждение угроз разрушения информационного процесса и его последствий. Человек осуществляет свою деятельность на основе модели [1]. В основе деятельности лежит решение ответственного лица. Поэтому для осуществления деятельности адекватной объективной обстановке (в нашем случае враждебной) необходимо располагать адекватной математической моделью решения человека. Без математической модели решения весьма сложно гарантировать достижения цели управления ИБ. Аналогичная ситуация имеет место с построением системы обеспечения ИБ, так как отсутствует критерий синтеза правильно построенной системы. Данная совокупность факторов определяет актуальность настоящей работы.

Ключевые слова: *информационная безопасность, web – приложение, модель процесса, управленческое решение, синтез.*

DEVELOPMENT OF TECHNOLOGY MANAGING THE PROCESS SECURING INFORMATION ON THE EXAMPLE WEB – APPLICATIONS

Burlov Viacheslav, Petrov Sergey, Grozmani Elena
St. Petersburg Polytechnic University of Peter the Great (SPbPU),
Russia, St. Petersburg, st. Polytechnic, 29,
emails: burlovvg@mail.ru, c.petrov@gmail.ru, grozmani.el@yandex.ru

Abstract: Ensuring information security of a web application is an activity aimed at preventing threats to the destruction of the information process and its consequences. A person carries out his activity on the basis of the model [1]. The basis of the activity is the decision of the responsible person. Therefore, to implement an adequate objective situation (in our case, hostile), it is necessary to have an adequate mathematical model for the solution of a person. Without a mathematical model of the solution, it is very difficult to guarantee the achievement of the IS management goal. A similar situation occurs with the construction of an IS system, since there is no criterion for the synthesis of a correctly constructed system. This set of factors determines the relevance of.

Keywords: *information security, web application, process model, management decision, synthesis.*

Введение. В настоящее время web-приложения стали играть ключевую роль в большинстве государственных и коммерческих организаций. Работая в режиме 24/7, они как правило, являются элементами ключевой инфраструктуры, обеспечивая критически важные бизнес-процессы. Обеспечение защищенности существующих в них информационных процессов является необходимым условием для успешного ведения деятельности соответствующими структурами.

Основная часть. Безопасность информации – это свойство информационного процесса сохранять своё предназначение в процессе жизненного цикла. Обеспечение информационной безопасности – это деятельность, направленная на предупреждение угроз разрушения информационного процесса и его последствий.

В основе деятельности лежат решения, принимаемые ответственным лицом. Следовательно, для принятия решений, соответствующих объективной обстановке, необходимо обладать адекватной математической моделью решения человека.

Для синтеза модели целесообразно применить естественно-научный подход (ЕНП), базирующийся на законе сохранения целостности объекта (ЗСЦО).

ЕНП определяется интеграцией свойств Мышления человека, окружающего Мира и Познания [2,3,4]. Реализуется научно-педагогической школой «Системная интеграция процессов государственного управления» [5].

Существует два подхода к разработке системы (модели):

- 1) На основе анализа;
- 2) На основе синтеза.

Анализный подход обладает существенным недостатком: он не позволяет формировать процессы с наперед заданными свойствами, что особенно важно в условиях обеспечения безопасности Web – приложения. Подход, основанный на синтезе, позволяет получать гарантию достижения цели обеспечения ИБ.

Руководствуясь принципами Трёхкомпонентности познания, Целостности и Познаваемости Мира осуществим синтез модели.

На 1-ом уровне, применяя метод декомпозиции, расчленим решение именно на три элемента «обстановка», «решение» и «информационно-аналитическая работа», которые соответствуют «объекту», «предназначению» и «действию». На 2-ом уровне используя метод абстрагирования мы отождествляем «объект» («обстановка») с периодичностью проявления проблемы перед человеком. «Предназначение» («Решение») отождествляем с периодичностью нейтрализации проблемы (средним временем адекватным реагированием на проблему) человеком. «Действие» («Информационно-аналитическая работа») отождествляем с периодичностью идентификации проблемы (средним временем распознавания ситуации).

Временные характеристики обоснованы тем, что только временные ресурсы для человека невосполнимы.

В результате применения методов декомпозиции, абстрагирования и агрегирования мы преобразовали понятие «управленческое решение» в агрегат – математическую модель управленческого решения. Это и есть условие существования процесса управления безопасностью web – приложения

Вывод. В работе предложен метод управления ИБ. Модель управления, в частности граф состояний, может быть далее усложнена, введением дополнительных обратных связей и учётом других условий. В свою очередь для адекватной оценки интенсивностей λ , v_1 и v_2 целесообразно использовать методы сетевого планирования.[6,7].

СПИСОК ЛИТЕРАТУРЫ

1. Анохин П.К. Системные механизмы высшей нервной деятельности. М. "Наука", 1979, 453 стр.
2. Бурлов В.Г. Основы моделирования социально-экономических и политических процессов (Методология. Методы) СПб: Факультет Комплексной Безопасности, СПбГПУ.2007г.-265 с.
3. Бурлов В.Г. Математические методы моделирования в экономике. Часть 1, - СПб. СПб ГПУ, Факультет безопасности, НП «Стратегия будущего», 2007. - 330с.
4. Бурлов В.Г. О концепции гарантированного управления устойчивым развитием арктической зоны на основе решения обратной задачи. Информационные технологии и системы: управление, экономика, транспорт, право. 2015. № 2 (16). С. 99-111.
5. Реестр ведущих научных и научно-педагогических школ Санкт-Петербурга. <http://is.ifmo.ru/aboutus/2013/science-schools.pdf>
6. Burlov V.G., Grobitski A.M. Development of a model for social system management in the construction process taking into account manager's qualification // Humanities&Science University Journal. 2015. No. 15. Pp. 45-57.
7. Burlov V.G., Grobitski A.M., Grobitskaya A.M. Construction management in terms of indicator of the successfully fulfilled production task. Magazine of Civil Engineering. 2016. No. 3. Pp. 77–91. doi: 10.5862/MCE.63.5

УДК 004.056

МОДЕЛИРОВАНИЕ СИСТЕМЫ НА ОСНОВЕ ЗАКОНА СОХРАНЕНИЯ ЦЕЛОСТНОСТИ

Бурлов Вячеслав Георгиевич, Долгирева Елена Сергеевна, Мокеева Татьяна Олеговна
Государственный университет морского и речного флота имени адмирала С.О. Макарова,
Россия, Санкт-Петербург, ул. Двинская, 5/7
emails: burlovvg@mail.ru, lena-baglaeva91@yandex.ru, soiye@mail.ru

Аннотация: В статье разрабатывается модель управленческого решения на основе синтеза, что позволяет заранее знать результаты выполнения задач. На основе такой модели становится возможным гарантированное выполнение задачи.

Ключевые слова: Система, управление, безопасность, целостность, модель, адекватность.

MODELING OF SYSTEM BASED ON THE INTEGRITY CONSERVATION LAW

Burlov Vyacheslav, Dolgireva Elena, Mokeeva Tatyana
Admiral Makarov State University of Maritime and Inland Shipping,
5/7 Dvinskaya str., Saint Petersburg, Russia
emails: burlovvg@mail.ru, lena-baglaeva91@yandex.ru, soiye@mail.ru

Abstract: The article considers the model of the administrative decision based on synthesis. It allows knowing the results of task implementation in advance. With this model it is possible to create conditions for a guaranteed solution to the task.

Keywords: System, management, security, integrity, model, adequacy.

Введение. Процесс обеспечения ИБ строится на основе управленческого решения администратора ИБ. Современная литература не предоставляет нам математической модели формирования управленческого решения, а только лишь методы обоснования этого решения. Без математической модели решения весьма сложно гарантировать достижения цели обеспечения информационной безопасности. Эта проблема определяет актуальность настоящей работы.

Естественно-научный подход к синтезу модели решения человека.

Проблема любого процесса - это несоответствие полученных результатов требуемым, которые основаны на противоречивых выводах. Чтобы исключить противоречивые выводы, используется аксиоматический метод.

Аксиоматический метод предполагает существование следующих компонентов:

- основные допущения и утверждения, которые обычно выражаются в некоторых основных принципах;

- основные понятия, ключевые слова, аксиомы, правила вывода, теоремы;

- основные принципы должны характеризовать суть процесса в ходе работы.

В эту деятельность входят три компонента: человек (его сознание), внешний мир (объект) и всеобщая связь, позволяющая осуществлять познание.

Соответственно, эти три компонента отражены в следующих трех принципах:

- принцип трехкомпонентности познания (Абстрактное представление, абстрактно-конкретное, конкретное представление)
- принцип целостности мира. Реализуется законом сохранения целостности объекта. Это устойчивая, объективная, повторяющаяся связь свойств объекта и свойств действия при фиксированном предназначении, проявляется в взаимном преобразовании свойств объекта и свойств его действия при фиксированном предназначении.
- принцип познаваемости мира. Он реализуется тремя методами научного знания: декомпозицией, абстрагированием, агрегированием.

Принцип трехкомпонентности познания состоит в том, что человек в процессе своей жизнедеятельности неосознанно принимает решения в трех уровнях представления окружающей обстановки.

Чтобы решить поставленную задачу, необходимо понять, какова должна быть модель правильно построенной системы. Модель представляет собой описание или представление объекта, соответствующего данному объекту, и позволяющая получить необходимые характеристики этого объекта.

Актуальной проблемой при моделировании является проблема адекватности модели моделируемому процессу.

Адекватность модели можно оценить тремя подходами,

- сравнивая ее с эталоном,
- сравнивая с результатами эксперимента;
- полнотой учёта основных закономерностей предметной области.

Наиболее полно удовлетворяет нашей задаче третий подход из перечисленных. Предметная область – исследование системы. Поэтому целесообразно для нашей предметной области взять закон сохранения целостности – это как раз и есть закон построения и функционирования системы.

Известны два подхода к проектированию систем – это проектировании на основе анализа и проектирования на основе синтеза.

Моделируя объект методом анализа, мы имеем совокупность физических элементов, с помощью которых необходимо предсказать возможный результат работы системы – выходные характеристики.

Моделируя объект методом синтеза напротив имеем набор выходных характеристик, а целью является определить количественный и качественный состав системы.

При разработке на основе синтеза выдается набор выходных характеристик проектируемой системы, и требуют определить количественный и качественный состав системы.

Руководствуясь принципом «трёхкомпонентности познания исследуемый процесс мы должны рассмотреть в трех уровнях: методологическом (условие существования процесса); методическом (условие перевода объекта из настоящего состояния в требуемое); технологическом (условия реализации перевода объекта из настоящего состояния в требуемое).

Руководствуясь принципом целостности, на каждом из трёх уровней представления процесс представляется связь в виде «цепочки» объект-предназначения-действие.

Руководствуясь принципом познаваемости применяем методы «декомпозиция», «абстрагирование», «агрегирования».

Процесс «Управленческое решение» должен соответствовать закону сохранения целостности в связке: объект – предназначение – действие. Для того, чтобы процесс «Управленческое решение» существовал, необходимо и достаточно установить связь между категориями «объект», «действие», «предназначение». С другой стороны, применяя принцип познаваемости, мы должны расчленить процесс «Управленческое решение» на эти три базовых элемента.

Интерпретируем «объект», как элемент модели «решения», в виде «обстановки».

«Действие» интерпретируем, как элемент модели «решения», в виде «информационно-аналитической работы (непрерывное добывание, сбор, изучение, отображение и анализ данных об обстановке)».

«Предназначение» мы должны интерпретировать как элемент модели «решения» в виде «реализации» решения.

На среднем уровне (методическом), необходимо представить причинно-следственную связь, согласованную с тремя базовыми принципами. Для этого необходимо, применяя метод абстрагирования, интерпретировать математической категорией «обстановку» (модель объекта), «информационно-аналитическая работа» (модель действия), «реализация» (предназначение).

Заключение. Изложив суть подхода к решению задачи управления информационной безопасностью в будущем необходимо построить последовательность преобразований вербальной модели к формальной, математической.

СПИСОК ЛИТЕРАТУРЫ

1. Анохин П.К. Системные механизмы высшей нервной деятельности. М. "Наука", 1979, 453 стр.
2. Бурлов В.Г. О концепции гарантированного управления устойчивым развитием арктической зоны на основе решения обратной задачи. Информационные технологии и системы: управление, экономика, транспорт, право. 2015. 3. Бурлов В.Г.

Синтез модели управления информационной безопасностью. Труды IV Международной научно-практической конференции «Информационные управляющие системы и технологии» (ИУСТ -ОДЕССА -2015). С. 147-151. № 2 (16). С. 99-111.

3. Бурлов В.Г. Гробицкий А.М. Интеллектуализация процесса управления трудовым коллективом при выполнении производственного задания. В сборнике: ИНФОРМАЦИОННЫЕ УПРАВЛЯЮЩИЕ СИСТЕМЫ И ТЕХНОЛОГИИ. Материалы V Международной научно-практической конференции (ИУСТ-ОДЕССА-2016). 2016. С. 192-195.
4. Бурлов В.Г. МЕТОДОЛОГИЯ ОЦЕНИВАНИЯ И УПРАВЛЕНИЯ РИСКАМИ ВОЗНИКНОВЕНИЯ ЧС В ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ И СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ СИСТЕМАХ. В сборнике: Региональные риски чрезвычайных ситуаций и управление природной и техногенной безопасностью муниципальных образований. Материалы девятой Всероссийской научно-практической конференции по проблемам защиты населения и территорий от чрезвычайных ситуаций. Центр стратегических исследований гражданской защиты МЧС России. 2004. С. 220-233.

УДК 004.056

СТАТИЧЕСКИЙ АНАЛИЗ БЕЗОПАСНОСТИ ANDROID-ПРИЛОЖЕНИЙ

Дремов Андрей Сергеевич, Павленко Евгений Юрьевич
Санкт-Петербургский политехнический университет Петра Великого,
Россия, Санкт-Петербург, ул. Политехническая, 29,
emails: dremov.asx@gmail.com, pavlenko@ibks.spbstu.ru

Аннотация: Исследована задача определения вредоносных приложений для операционной системы Android. Рассмотрены существующие подходы к анализу вредоносных Android-приложений. Предложен подход к анализу Android-приложений, основанный на использовании графов потоков управления и потоков данных. В работе даны формальные определения отношения зависимости, которые используются для построения графов, а также описан алгоритм, определяющий вредоносные участки кода с помощью полученных графов. Приведены результаты экспериментальной оценки качества работы предложенного подхода, демонстрирующие высокую вероятность обнаружения вредоносных участков кода Android-приложений.

Ключевые слова: информационная безопасность; Google Android; безопасность мобильных устройств; вредоносное программное обеспечение; анализ приложения.

STATIC ANALYSIS OF ANDROID-APPLICATIONS SECURITY

Dremov Andrei, Pavlenko Evgeny
Peter the Great St.Petersburg Polytechnic University,
Russia, St. Petersburg, Polytechnicheskaya str. 29,
emails: dremov.asx@gmail.com, pavlenko@ibks.spbstu.ru

Abstract: The article presents the problem of identifying malicious Android applications. The main approaches to the analysis of malicious Android-applications are considered. A method for analyzing Android applications is proposed, based on using graphs of control flows and data flows. The article formally describes the dependency relationships that are used to construct graphs, and also describes an algorithm that allows you to identify malicious sections of code using the received graphs. The results of an experimental evaluation of the effectiveness of the proposed method are presented, demonstrating a high probability of detecting malicious portions of the code of Android applications.

Keywords: information security; Google Android; mobile security; malware; application analysis.

Введение. На сегодняшний день операционная система Google Android завоевала наибольшую популярность на рынке мобильных технологий. За последний год рыночная доля использования данной операционной системы превысила аналогичные показатели для платформы Windows [1]. Число пользователей данной операционной системы стремительно растет, поэтому злоумышленники создают и распространяют вредоносное программное обеспечение, применяя различные техники для их маскировки. В результате, задача определения Android-приложений, в которых содержатся вредоносные функции, становится актуальной и востребованной при обеспечении безопасности пользователей мобильных систем.

Для обнаружения вредоносных приложений существуют два основных подхода: статический и динамический анализ [2]. В ходе статического анализа исследуются исходные коды приложения без его реального исполнения. Методы динамического анализа позволяют собирать различную информацию о приложении, которое выполняется в специальной операционной среде. Такой информацией могут быть данные о сетевом трафике, системные вызовы, записи в журналах событий и др. В последнее время большую популярность получили методы обнаружения вредоносных приложений, основанные на алгоритмах машинного обучения, которые комбинируют подходы статического и динамического анализа для составления векторов-признаков [3].

Перечисленные способы обнаружения вредоносного программного обеспечения выполняют анализ Android-приложения как единой системы, в которую могут быть включены как вредоносные, так и легитимные участки кода, а в результате исследователю дается вероятностная оценка содержания вредоносных функций без указания конкретных участков кода, в которых они содержатся.

В данной работе предлагается подход к анализу Android-приложений, который основывается на извлечении различных участков кода приложения, определения их характеристик безопасности, в результате чего можно установить, какие участки кода содержат вредоносные функции. Полученные данные можно использовать в качестве сигнатур для идентификации опасных Android-приложений или устранить вредоносные участки кода из приложения, уменьшив риск нарушения безопасности пользователя.

Для оценки содержания вредоносных функций в Android-приложении используются графы двух типов: графы зависимостей классов и графы вызовов методов, способы построения которых учитывают многие особенности Android-приложений. Графы зависимости классов позволяют извлечь участки кода приложения и строятся на основе межкомпонентных взаимодействий и преобразований с данными. Графы вызовов методов необходимы для получения признаков участков кода, влияющих на свойства безопасности приложения, и строятся на основе связей между методами. В результате взаимно-однозначного соответствия между графами различных типов можно установить, какие участки кода являются вредоносными.

Чтобы автоматизировать процесс анализа Android-приложений, было разработано специальное программное обеспечение, включающее модули построения графов, извлечения участков кода по полученным графам зависимости классов, расчет значений критериев легитимности, которые необходимы для формирования итоговой оценки вредоносности участка кода. При значении итоговой оценки больше единицы, участок кода считается вредоносным и выдается результат пользователю.

Заключение. Рассмотренный подход к анализу безопасности Android-приложения позволяет эффективно оценить содержание вредоносных функций в приложении и определить участки кода, в которых они содержатся. В ходе экспериментальной оценки качества разработанного подхода использовались 1000 приложений, из которых 475 являлись вредоносными. В результате 91% составила доля истинно распознанных вредоносных Android-приложений, а 93% – доля истинно распознанных образцов безопасных Android-приложений, что говорит о достаточно высокой точности обнаружения и возможности применения данного подхода на практике.

СПИСОК ЛИТЕРАТУРЫ

1. StatCounter Global Stats [Электронный ресурс] – Режим доступа: <http://gs.statcounter.com/press/android-overtakes-windows-for-first-time>, свободный.
2. A. Kapratwar. Static and Dynamic Analysis for Android Malware Detection: [Электронный ресурс]. URL: http://scholarworks.sjsu.edu/cgi/viewcontent.cgi?article=1488&context=etd_projects / A. Kapratwar // San Jose State University, 2014.
3. Павленко Е. Ю. Применение методов кластеризации для анализа безопасности Android-приложений [Текст] / Павленко Е. Ю., Ярмач А. В., Москвин Д. А. Проблемы информационной безопасности. Компьютерные системы. №3 2016. С. 119-126.

УДК 51.76

ОБОСНОВАНИЕ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ОПАСНОГО ВЗРЫВООБРАЗНОГО РАЗВИТИЯ ПОПУЛЯЦИОННОГО ПРОЦЕССА ДЛЯ ИНВАЗИОННОГО ТАКСОНА

Дубровская Виктория Андреевна, Переварюха Андрей Юрьевич
Санкт-Петербургский институт информатики и автоматизации РАН,
Россия, Санкт-Петербург, ул. 14 линия, 39,
emails: madelf@pisem.net, torry_2902@mail.ru

Аннотация: В работе нами рассмотрено обоснование имитационной модели на основе дифференциального уравнения для описания так называемой продолжительной пилообразной вспышки популяции опасного насекомого фитофага, возникающей при появлении нерегулярных флуктуаций численности большой амплитуды. Флуктуации моделируются в форме затухающих релаксационных колебаний при серии отстоящих друг от друга во времени пиков численности.

Ключевые слова: моделирование; популяционная динамика; инвазии видов

IMITATIVE MODELING OF HAZARDOUS EXPLOSIVE PROJECTION OF THE POPULATION PROCESS FOR THE INVASION TAXON

Dubrovskaya Victoria, Perevaryukha Andrey,
St. Petersburg Institute of Informatics and Automation of RAS,
Russia, St. Petersburg, st. 14 line, 39,
emails: madelf@pisem.net, torry_2902@mail.ru

Abstract: The article considers the justification of the simulation model on the basis of the differential equation for describing the so-called prolonged sawtooth flare of the phytophagous insect population that occurs when irregular fluctuations in the abundance of large amplitude occur. Fluctuations are modeled in the form of damped relaxation oscillations with a series of spacing peaks in time.

Keywords: *modeling; population dynamics; invasive species*

В контексте мер поддержания экологической безопасности и сохранения биоразнообразия весь комплекс задач по информационному мониторингу, прогнозированию, учету последствий и выработке методов противодействия такому явлению как массовые размножения насекомых представляет особый интерес для развития методов имитационного моделирования. Объяснение генезиса и формализация масштабных нестационарных состояний у уязвимых видов в естественной среде, к которым относится подавляющее большинство насекомых Hemiptera и Lepidoptera, одновременно одна из актуальных нерешенных проблем для математической экологии как междисциплинарного научного направления. С точки зрения системной экологии постановка задачи формального описания стремительных изменений в популяционной динамике у вредителей-фитофагов представляет теоретический интерес из-за необходимой модификации представлений о действующих механизмах, точнее о диапазонах их действия и выключения, в регуляции эффективности воспроизводства популяций в качественно различных состояниях.

Многие наблюдаемые ситуации при массовых размножениях связаны с явлениями инвазий и адаптаций чужеродных видов – глобальной современной проблемой. В некоторых случаях вид-вселенец, представленный изначально малой группой особей, не встречает конкурентного противодействия со стороны автохтонного биологического окружения. Тогда у образующейся популяции происходит максимизация репродуктивного потенциала, который на самом деле является агрегированной и отнюдь не независимой характеристикой. В работах по моделированию деградации осетровых рыб мы успешно отказались от расчетов пополнения при фиксированном репродуктивном параметре.

Инвазия далеко не всегда переходит в стадию вспышки. В некоторых случаях инвазия может оказаться даже полезной для питания ценных потребителей, как в случае с донной фауной Каспийского моря, где проникновение средиземноморских моллюсков повысило продуктивность кормовой биомассы рыб во время падения уровня моря. Наихудший вариант инвазионного процесса реализовался после обнаружения в 2012 г. самшитовой огневки *Cydalima perspectalis* на побережье Краснодарского края. Выживание гусениц после обработки посадочного материала фосфорорганическим инсектицидом повлекло сплошное поражение массивов реликтового самшита Имеретинской низменности огневкой в 2013 г. Естественные патогены «олимпийской бабочки» отсутствовали полностью. За два года очаги поражения самшитовых рощ распространились до долин Абхазии [1]. По скорости развития последствий для экосистемы появление *Cydalima perspectalis* превзошло даже вселение полифага непарного шелкопряда *Lymantria dispar* в леса восточного побережья США.

Вспышки численности свойственны и неизмеримо давно присутствующим в экосистеме видам. В некотором смысле они становятся частью круга последовательных перестроений в растительных сообществах. О цикличности или стохастичности причин таких явлений ведется длительная дискуссия биологов и математиков. В работах на примере полифага лугового мотылька *Loxostege sticticalis* приводятся указания в пользу цикличности. Из известной работы Л.Р. Кларка [2] скорее можно сделать вывод о случайном сбое в механизме регуляции и действии пороговых состояний численности при сложном межвидовом взаимодействии группы видов, составляющих трехуровневую систему «паразиты-хозяин»: псиллид и конкурирующих наездников.

Основной аспект, выделяемый нами в комплексной проблеме исследования вспышек в том, что по-видимому, нереально выделить общий путь развития процесса именно с позиций теории метаморфозов фазовых портретов нелинейных динамических систем, аппарата для описания резких изменений. Данные ряда примеров указывают на различия в типах бифуркаций. Наиболее оправданным видится сценарный подход к моделированию ситуаций с некоторым множеством вариантов дальнейшего развития.

В настоящей работе мы предлагаем непрерывную модель бифуркационного запуска сценария специфически осциллирующей вспышки на основе концепции запаздывания в действии регулирующих факторов. Модельный сценарий актуален по имеющимся данным наблюдений для случаев поражения вредителем лесов Канады и позволяет оценивать временную эволюцию характеристик пилообразных колебаний численности.

Традиционными методами математической экологии описать нелинейность завершения и спонтанность выхода из хаотических флуктуаций представлялось невозможным. Был выбран подход в форме непрерывно-дискретной динамической системы, строившейся на формализации выживаемости поколения. Изменения непрерывной системы в выделенные условиями моменты времени были соотнесены с переходами между тремя стадиями развития онтогенеза *Psyllidae*.

Первая разработанная нами базовая модель [2] формулировалась переопределяемой правой частью дифференциального уравнения для убыли численности $N(t)$ на трех последовательных временных субинтервалах с включением условий завершения активности.

Таким образом, мы получили сложную зависимость для дискретной составляющей траектории, которая демонстрирует спонтанное преодоление порогового равновесия из переходного хаотического

режима. Изначально при анализе наблюдений предполагалась вариативность на стадии завершения вспышки, что не было учтено нами в предыдущей статье, но вполне можно отразить в модели просто уменьшив вклад функционала ответственного за эффект Олли. Для описания завершения вспышки был введен триггерный функционал, редуцирующий притягивающую стационарную точку, что резко переводило популяцию в следующий период хаотических флуктуаций. Порог запуска вспышки не может быть монотонно достижим из любого состояния системы, все же вспышка численности с дефолиацией – это эпизодическое явление, потому несвязные границы областей притяжения аттракторов в нашей модели хорошо описывают данный экологический аспект. Существование порога, отраженного в модели граничным неустойчивым положением равновесия, объясняется сложными взаимоотношениями различных видов паразитических наездников при выборе предпочтительного объекта для кладки. После превышения пороговой численности возрастает роль перепончатокрылых подсемейства Encyrtinae, в основном *Coccidoctonus psyllae*, эти осы активно начинают паразитировать на других размножившихся паразитических наездниках семейства Encyrtidae – основных врагов для яиц псиллид.

Необходимо отметить, что регуляция эффективности воспроизводства посредством гиперпаразита достаточно специфическая ситуация. Существование порогового перехода не может быть единственным или даже главенствующим объяснением механизма запуска вспышки. Вполне логично, что в бореальных лесах Северной Америки действуют некоторые другие механизмы, вызывающие не менее масштабные вспышки у других таксономических групп насекомых.

В контексте ситуации с поражениями эвкалиптовых лесов вредоносным инвазионным видом оказался именно гиперпаразит *Coccidoctonus psyllae*, после появления которого в Новой Зеландии в местных лесах участились вспышки видов семейства Psyllidae. В семействах Ichneumonidae, Encyrtidae встречаются сверхпаразиты и более высоких, третьего и даже четвертого порядков, паразитические осы поражающие других перепончатокрылых паразитов.

Работа выполнена при обобщении результатов проектов РФФИ: № 17-07-00125 (СПИИРАН), №15-04-01226 (совместно с Всероссийским институтом защиты растений РАН). №16–37–00028 (СПИИРАН) для Молодых ученых (руководитель доц. Соловьева Т.Н.).

СПИСОК ЛИТЕРАТУРЫ

1. Лукмазова Е.А., Тания И.В. Самшитовая огнёвка *Cydalis perspectalis* (Walker, 1859) в Республике Абхазия // Труды Ботанического института. 2014. №1. С. 110–122.
2. Переварюха А.Ю. Модель развития спонтанной вспышки численности насекомого с аperiodической динамикой // Энтомологическое обозрение. 2015. Т. 94. № 1. С. 203–215.

УДК 004.056.5

РАЗРАБОТКА ЗАЩИЩЕННОГО ПРОТОКОЛА ТАЙНОГО ГОЛОСОВАНИЯ В ТВОРЧЕСКОМ КОНКУРСЕ

Дмитриева Лариса Михайловна, Макарова Таисья Васильевна
Омский государственный технический университет «ОмГТУ»
Россия, г. Омск, пр. Мира, 11,
emails: dmlara@yandex.ru, tajam@mail.ru

Аннотация: В статье рассмотрены вопросы создания защищенного протокола голосования, обеспечивающего анонимность и корректность учета голосов членов жюри творческого конкурса: актуальность, требования к протоколу, описание протокола, возможные сферы его применения.

Ключевые слова: электронное голосование; тайное электронное голосование; протокол слепой подписи

DEVELOPMENT OF SECURE PROTOCOL FOR SECRET E-VOTING IN CREATIVITY COMPETITION

Larisa Dmitrieva, Taisya Makarova
Omsk State Technical University «OmSTU»,
Russia, Omsk, pr. Mira 11,
emails: dmlara@yandex.ru, tajam@mail.ru

Abstract: The article discusses the creation of a secure voting protocol that ensures anonymity and correct accounting of jury members votes in creative competitions, actuality, protocol requirements and possible areas of its application

Keywords: electronic voting; secret electronic voting; blind signature protocol

Творческая жизнь деятелей культуры насыщена разного рода конкурсами, в ходе которых выявляются наиболее яркие, с профессиональной точки зрения, личности или наиболее качественные авторские работы. Победители гордо несут звание «лучшего», прославляя тем самым свою школу и своих учителей.

Кафедра «Дизайн и технологии медиаиндустрии», занимаясь воспитанием творческих личностей, также проводит конкурсные мероприятия, одним из которых является Всероссийская студенческая творческая лаборатория «Регионы, города: ракурсы и параллели».

Для информационной поддержки конкурсов создаются интернет-ресурсы, позволяющие удаленно принимать работы участников и организовывать удаленное голосование членов жюри.

Не имея большого бюджета на проведение мероприятия, кафедра ДТМ, как и многие другие организаторы, для создания сайта выбирает бесплатные CMS-платформы с простым интерфейсом и большим количеством встроенных функций, в том числе функции голосования. Однако все подобные системы управления контентом предоставляют администратору полные права на доступ к любой информации, в том числе, открытый доступ к результатам голосования каждого эксперта. Это обстоятельство лишает членов жюри уверенности в сохранении тайны поставленной конкурсанта оценки, разглашение которой может внести разлад в отношения коллег по цеху, имеющих многолетние творческие связи.

Данная проблема актуализировала вопрос создания механизма анонимного голосования в творческом конкурсе, достаточно простого, чтобы быть реализованным в рамках бюджетного проекта, и, вместе с тем надежно обеспечивающего анонимную подачу и корректную обработку голосов судей.

Задача обеспечения конфиденциальности решений участников голосования и корректности учета голосов членов жюри может быть решена применением защищенного протокола голосования.

Протокол электронного голосования в творческом конкурсе должен обеспечивать выполнение ряда требований: обеспечение тайны (анонимности) выставления оценки; доступность информации об участниках голосования; строгая однозначная идентификация участников голосования; одноразовый учет голоса эксперта; корректность подсчета конечного результата; возможность проверки любым из участников, что его голос правильно учтен; работоспособность протокола в случае, когда некоторые из его участников нечестны.

Исходя из данных требований, разработан защищенный протокол голосования в творческом конкурсе. В его основу положены алгоритм создания электронной цифровой подписи ЭЦП и асимметричная криптосистема шифрования RSA. Участниками протокола являются: эксперт (член жюри) и счетная комиссия.

Разработанный протокол позволяет раздавать бюллетени членам жюри, при этом не нарушает принцип тайны голосования.

Нечестный эксперт не сможет обмануть эту систему. Не имеющий право голосовать, не получит бюллетень для подачи голоса, так как его личность проверяется на основании его ЭЦП при подаче заявки на получение бюллетеня. Протокол слепой подписи обеспечивает единственность его бюллетеня. Если нечестный эксперт попытается отправить один бюллетень дважды, счетная комиссия обнаружит дублирование идентификационных номеров, и не будет учитывать второй бюллетень. Если эксперт попытается получить несколько бюллетеней, избирательная комиссия также обнаружит это на соответствующем этапе и при публикации результатов. Также нечестный эксперт не сможет создать свои собственные бюллетени, так как не знает закрытого ключа комиссии. По этой же причине он не может перехватить и изменить чужие бюллетени.

Организаторы выборов не могут узнать, как голосовал конкретный эксперт. Так как протокол слепой подписи маскирует последовательные номера бюллетеней до момента подведения итогов, счетная комиссия не сможет установить связь между подписанными ею замаскированным бюллетенем и подытоживаемым бюллетенем. Опубликование перечня последовательных номеров и связанных с ним бюллетеней позволяет экспертам убедиться, что их бюллетени были правильно учтены.

Разработанный протокол проверен на корректность работы и будет использован для обеспечения защиты голосования при проведении конкурсного отбора на модернизированном сайте мероприятия Всероссийская студенческая творческая лаборатория «Регионы. Города. Ракурсы и параллели».

СПИСОК ЛИТЕРАТУРЫ

1. Галицкий А. В., Рябо С. Д., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях – М.: ДМК Пресс, 2012. – 592 с.
2. Шнайер Б. Прикладная криптография (Applied Cryptography). – М.: Триумф, 2002. – 816 с.

УДК 681.518.5:004.052.32

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ КЛАССА ДВУХМОДУЛЬНЫХ КОДОВ С СУММИРОВАНИЕМ ПРИ СИНТЕЗЕ ДИСКРЕТНЫХ СИСТЕМ С ОБНАРУЖЕНИЕМ ОТКАЗОВ

Ефанов Дмитрий Викторович, Щагина Владислава Александровна

Петербургский государственный университет путей сообщения Императора Александра I,
Россия, Санкт-Петербург, Московский пр., 9,
emails: TrES-4b@yandex.ru, vladislava1997@inbox.ru

Аннотация: Описываются достоинства нового подхода к построению кода, отличного от известных. Анализируются свойства новых кодов в сравнении с известными кодами с суммированием.

Ключевые слова: *техническое диагностирование; функциональный контроль; код с суммированием; код Бергера; двухмодульный код.*

PROSPECTS OF USING THE CLASS OF TWO-MODULUS CODES WITH SUMMATION SYNTHESIS OF DISCRETE SYSTEMS WITH ERROR DETECTION

Efanov Dmitry, Schagina Vladislava
The Emperor Alexander I St. Petersburg State Transport University,
Russia, St. Petersburg, Moscow ave., 9
emails: TrES-4b@yandex.ru, vladislava1997@inbox.ru

Abstract: Describes the advantages of a new approach to constructing code that is different from known ones. The properties of new codes are analyzed in comparison with known codes with summation.

Keywords: *technical diagnostics; concurrent error-detection; sum code; Berger code; two-modulus code.*

Введение. Для организации надежных дискретных устройств автоматики и вычислительной техники используются системы функционального контроля, позволяющие в режиме работы объекта диагностирования производить процедуру диагностирования (не требуется отключения объекта диагностирования от работы, а все входные воздействия одновременно являются и тестовыми) [1], [2]. Часто такие системы строятся с использованием помехоустойчивых кодов, которые имеют простые правила построения и небольшую избыточность. Одними из широко используемых являются классические коды с суммированием и их модификации [3].

Классический код с суммированием (код Бергера) строится путем записи в контрольный вектор веса информационного вектора r , то есть количество единичных разрядов, в двоичном виде. Обозначается код Бергера как $S(m,k)$ -код, где m – длина информационного вектора, k – длина контрольного вектора [4]. Достоинством кода Бергера является то, что он обнаруживает все монотонные ошибки в информационном векторе. Однако, кодом Бергера не обнаруживается достаточно большое общее количество ошибок, это объясняется тем, что контрольные слова распределены между информационными неравномерно. Так же, системы функционального контроля, построенные на основе кода Бергера имеют большую сложность технической реализации. Для улучшения свойств кодов Бергера, используемых при построении надежных дискретных систем используются его различные модификации.

Одной из таких модификаций является разбиение разрядов информационного вектора на подмножества и формирование отдельных контрольных частей для каждого подмножества [5]. То есть в информационном векторе длиной m выделяются два подмножества разрядов $D1$ и $D2$, причем при их пересечении должно образовываться полное множество разрядов Q . Стоит отметить, что данное условие является главным, иначе нарушается помехоустойчивость кода в виду неконтролируемости некоторых разрядов. В [6] рассмотрены такие коды, которые строятся путем разбиения множества информационных разрядов на два подмножества и образуются два подвектора $V1$ и $V2$, затем определяются наименьшие неотрицательные вычеты по модулю 4 весов подвекторов, а получаемые числа в двоичном виде записываются в контрольный вектор.

В зависимости от выделения подмножеств, образуется целое семейство двухмодульных кодов, обозначаемых как $TM(m,k,D1/D2)$ -коды, где $D1/D2$ – количество разрядов информационного вектора в первом и во втором подмножествах. Двухмодульные коды всегда будут иметь длину контрольного вектора $k=4$, поэтому могут быть сравнимы с кодом Бергера при длинах информационных векторов $m=8÷15$. Число способов построения двухмодульных кодов значительно, к примеру, для информационного вектора длиной $m=8$ возможно 39 различных вариантов построения двухмодульного кода. Некоторые из них будут иметь одинаковые свойства, а некоторые – уникальные для каждого вида разбиения.

$TM(m,k,D1/D2)$ -коды могут эффективно использоваться при организации систем функционального контроля.

При сравнительном анализе обнаруживающей способности и структурной избыточности систем функционального контроля, организованных на основе кода Бергера и частного случая двухмодульного кода, используя пакет контрольных комбинационных схем из базы LGSynth`89, MCNC, было выявлено, что системы функционального контроля на основе двухмодульного кода обнаруживают большее общее количество ошибок в информационном векторе, однако, не обнаруживают некоторое количество монотонных ошибок кратностью $d=4,8, \dots$ Также был произведен сравнительный анализ структурной избыточности систем функционального контроля, построенных на основе кодов Бергера, известных модифицированных кодов с суммированием единичных разрядов, дублирования и двухмодульных кодов. Было получено, что для 85% испытуемых контрольных схем, системы функционального контроля, построенные по двухмодульному коду с "половинным" разбиением разрядов на

подмножества, имеют меньшую сложность технической реализации, чем для всех остальных структур. Поэтому было принято решение об исследовании свойств двухмодульных кодов с различными соотношениями разрядов в каждом из подмножеств.

В результате эксперимента с контрольными комбинационными схемами из базы MCNC было установлено, что системы функционального контроля, построенные на основе двухмодульных кодов для 80% вариантов разбиений, имеют меньшую структурную избыточность в сравнении и с применением схем контроля по кодам Бергера и с использованием дублирования. Были установлены некоторые закономерности, проявляющиеся при увеличении разрядов в одном из подмножеств. Так, например, при фиксированном первом подмножестве разрядов D1 с увеличением количества разрядов во втором подмножестве D2 возрастает сложность технической реализации системы функционального контроля.

Заключение. Системы функционального контроля организованные на основе ТМ(m,k,D1/D2)-кодов гораздо эффективнее обнаруживают ошибки в информационных векторах, а также имеют невысокую структурную избыточность (меньшую, чем при использовании как дублирования, так и известных кодов с суммированием). Это делает их использование перспективным для решения задач технической диагностики и при синтезе надежных дискретных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Nicolaidis M., Zorian Y. On-Line Testing for VLSI – A Compendium of Approaches // Journal of Electronic Testing: Theory and Applications. – 1998. – Vol. 12, issue 1-2. – Pp. 7-20.
2. Göessel M., Ocheretny V., Sogomonyan E., Marienfeld D. New Methods of Concurrent Checking: Edition 1. – Dordrecht: Springer Science+Business Media B.V., 2008, 184 p.
3. Piestrak S.J. Design of Self-Testing Checkers for Unidirectional Error Detecting Codes. – Wrocław: Oficyna Wydawnicza Politechniki Wrocławskiej, 1995. – 111 p.
4. Berger J.M. A Note on Error Detection Codes for Asymmetric Channels // Information and Control. – 1961. – Vol. 4. – Issue 1. – Pp. 68-73. – DOI: 10.1016/S0019-9958(61)80037-5.
5. Efanov D., Sapozhnikov V., Sapozhnikov V.I. Generic Two-Modulus Sum Codes for Technical Diagnostics of Discrete Systems Problems // Proceedings of 14th IEEE East-West Design & Test Symposium (EWDTS'2016), Yerevan, Armenia, October 14-17, 2016, pp. 256-260, doi: 10.1109/EWDTS.2016.7807713.
6. Efanov D., Sapozhnikov V., Sapozhnikov V.I., Schagina V. The Analysis of Two-Modulus Codes Detection Ability with Summation of Unit Data Bits Compared to Classical and Modified Berger Codes // Proceedings of 15th IEEE East-West Design & Test Symposium (EWDTS'2017), Novi Sad, Serbia, September 29 – October 2, 2017.

УДК 004.056

ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ВЫЯВЛЕНИЯ ВРЕДНОСНЫХ ANDROID-ПРИЛОЖЕНИЙ

Игнатьев Глеб Юрьевич, Павленко Евгений Юрьевич
Санкт-Петербургский политехнический университет Петра Великого
Россия, Санкт-Петербург, ул. Политехническая, 29,
emails: glebignatieff@gmail.com, pavlenko@ibks.spbstu.ru

Аннотация: Исследована возможность создания высокопроизводительного анализатора Android-приложений, который бы позволял обрабатывать большое количество приложений за короткие промежутки времени. Предложен метод анализа безопасности Android-приложений, основанный на применении статического анализа с использованием методов машинного обучения. В работе подробно описаны: выборка, используемое пространство признаков, а также алгоритмы машинного обучения, используемые для построения классификатора. Приведены результаты экспериментальной оценки эффективности программной реализации предложенного метода, демонстрирующие его высокую производительность и высокую точность определения вредоносных Android-приложений.

Ключевые слова: информационная безопасность; Google Android; вредоносное программное обеспечение; статический анализ приложения; машинное обучение.

USING MACHINE LEARNING FOR DETECTION OF MALICIOUS ANDROID-APPLICATION

Ignatiev Gleb, Pavlenko Evgeny
Peter the Great St.Petersburg Polytechnic University,
Russia, St.Petersburg, Polytechnicheskaya, 29,
emails: glebignatieff@gmail.com, pavlenko@ibks.spbstu.ru

Abstract: This article explores the problem of developing a high-performance Android applications analyzer, which capable of processing a large number of applications in a very short period of time. A method for analyzing security of Android applications is proposed, based on the use of machine learning algorithms in static analysis. The paper describes dataset, application features and machine learning algorithms used to build a classifier. The results of an experimental evaluation of effectiveness of the proposed method are presented, demonstrating it high performance and high accuracy of detecting malicious Android applications.

Keywords: information security; Google Android; malware; static analysis, machine learning.

Введение: На сегодняшний день самой распространенной операционной системой для мобильных устройств является Google Android, по последним данным установленная на более чем 85% устройств. Стремительный рост числа пользователей привлек разработчиков вредоносного программного обеспечения (ВПО) по всему миру, что, в свою очередь, привело к колоссальному росту количества ВПО для Android в начале второго десятилетия XX века, который продолжается и по сей день. Одним из основных подходов выявления вредоносных приложений является статический анализ, позволяющий анализировать приложения без их непосредственного запуска, и основной задачей которого является извлечение некоторых характерных для данного приложения свойств, по которым можно было бы сказать, является данное приложение вредоносным или нет.

Ежедневно в магазины Android-приложений поступают тысячи и десятки тысяч приложений, многие из которых являются вредоносными. Очевидно, что в таких условиях крайне необходимо наличие некоторого метода, который бы позволил бы достаточно быстро и с большой долей уверенности отсеивать вероятно вредоносные приложения из общего числа приложений. Кроме того, желательно, чтобы этот метод не требовал больших вычислительных мощностей и ресурсов памяти. И наконец, что даже более важно, метод должен иметь возможность распознавать новые семейства и виды ВПО и противостоять шифрованию и полиморфизму старых.

В работе [1] представлен общий подход к созданию классификатора, он включает в себя следующие три условные стадии: формирование признакового описание файла (feature selection), выбор признаков (feature selection) и построение математической модели – классификатора, который использует разреженный вектор признаков, полученный на второй стадии. В целом, все исследования в этой области строятся подобным образом, меняется только пространство используемых признаков и алгоритмы. В работе [2] авторы показали, что использование комплексного набора признаков способствует повышению точности классификации, а именно, в работе классификатор был сначала построен на основе разрешений, затем на основе API вызовов, и, наконец, на основе их совокупности. В результате два первых классификатора показали худшую точность классификации по сравнению с последним. В работе [3] авторы также показали преимущество классификатора, построенного на комплексном наборе признаков (в данном случае это разрешения и users-feature), провели исследование различных алгоритмов машинного обучения применительно к данной задаче и показали, что и без использования API вызовов можно достичь достаточно высокой точности определения, что важно, поскольку их анализ является дорогостоящей задачей.

Авторами данной работы предлагается метод статического анализа безопасности Android-приложений с использованием алгоритмов машинного обучения, который сочетает в себе высокую точность определения вредоносных Android-приложений посредством использования комплексного набора признаков и в то же время является высокопроизводительным решением, позволяющим проанализировать большое количество приложений в короткие сроки.

Для обеспечения максимальной скорости работы необходимо использовать признаки, не требующие дополнительных вычислений для извлечения, поэтому в данном случае автоматически отбрасываются признаки, требующие декомпиляции Android-приложения, в итоге остается файл манифеста Android-приложения и файлы метаданных. Таким образом, для обеспечения максимальной точности определения, необходимо извлечь максимум из данных файлов.

Таким образом, из всего содержимого файла манифеста было сформировано пространство признаков, содержащее разрешения приложения, фильтры Intent, теги uses-feature и множество коэффициентов, показывающих процент использования в анализируемом приложении определенных компонентов (операций, сервисов и т.д.) по отношению к общему количеству, а также общее количество разрешений и процент использования определенных видов разрешений к общему количеству. Множество коэффициентов было построено на основании источника **[Ошибка! Источник ссылки не найден.]**.

Помимо этого, из файлов метаданных в методе используется файл сертификата приложения, а именно, его серийный номер. После анализа большого количества вредоносных приложений был составлен «черный список» серийных номеров, поскольку, как показали исследования [5], разработчики программного обеспечения часто имеют неосторожность использовать один и тот же сертификат для разработки своих приложений. Таким образом, данный «черный список» позволяет быстро определить подмножество приложений недобросовестного разработчика.

С использованием выбранного пространства признаков, строится вектор каждого приложения выборки, и полученная совокупность векторов дает набор данных для обучения классификатора. Перед обучением пространство признаков предварительно сокращается путём использования алгоритмов отбора признаков, это позволяет сократить объем вычислений и, следовательно, увеличить производительность классификатора без потери точности. Обученный классификатор способен, используя вектор признаков поданного на вход приложения, определить, является ли оно легитимным или вредоносным.

В итоге, с учетом разработанного классификатора и «черного списка» номеров, система реализует следующий алгоритм принятия решений: в случае, если приложение было классифицировано как вредоносное, то это решение окончательное, иначе вероятно легитимное

приложение проходит проверку серийного номера: если он обнаруживается в черном списке, то приложение считается подозрительным, поскольку произведено разработчиком ВПО, иначе приложение признается легитимным.

Заключение: Представленный в данной работе метод позволяет определять вредоносные Android-приложения с использованием классификатора на основе алгоритмов машинного обучения, построенного на комплексном пространстве признаков, извлечение которых не требует дорогостоящей с точки зрения ресурсов и времени декомпиляции приложения. Таким образом, разработанный подход позволяет классифицировать Android приложения на легитимные и вредоносные приложения с высокой производительностью и большой точностью, показатель AUC = 0.98.

СПИСОК ЛИТЕРАТУРЫ

1. Путин Е., Тимофеев А. Классификатор для статического обнаружения компьютерных вирусов, основанный на машинном обучении // Information Technologies & Knowledge. – 2014. – Т. 8. – № 2. – С. 103-112.
2. –Sahs J., Khan L. A Machine Learning Approach to Android Malware Detection // Intelligence and Security Informatics Conference (EISIC). 2012 [Электронный ресурс]. URL: <http://www.utdallas.edu/~lkhan/papers/06298824.pdf>.
3. Sanz B., Santos I., Laorden C., Ugarte-Pedrero X., Nieves J., P. Bringas P. G., Alvarez G. MAMA: Manifest Analysis for Malware Detection in Android // Cybernetics and Systems. – 2013. – Т. 44. – С. 469-488.
4. Павленко Е.Ю., Дремов А.С. Обнаружение вредоносных участков кода Android-приложений на основе анализа графов потоков управления и графов потоков данных // Проблемы информационной безопасности. Компьютерные системы. – 2017. – № 2. – С. 109-126.
5. Kang H., Jang J., Mohaisen A., Kim H. Detecting and Classifying Android Malware Using Static Analysis along with Creator Information // International Journal of Distributed Sensor Networks. – 2015. DOI: 10.1155/2015/479174.

УДК 004.056.2

ПОСТАНОВКА ЗАДАЧИ О РАЗРАБОТКЕ СИСТЕМЫ МЕТРИК ЗАЩИЩЕННОСТИ БАЗ ДАННЫХ

Мария Феликсовна Исаева, Михаил Леонидович Глухарев

Петербургский государственный университет путей сообщения императора Александра I

Россия, г. Санкт-Петербург, Московский пр., 9

emails: isaeva.mf@gmail.com, mlgluharev@yandex.ru

Аннотация: В данной работе предлагается общая структура системы метрик защищенности баз данных, обосновывается необходимость ее разработки, раскрывается роль метрик защищенности в оценивании качества баз данных и информационных систем в целом.

Ключевые слова: базы данных; безопасность информации; метрики защищенности.

PROBLEM STATEMENT OF DEVELOPING OF DATABASE SAFETY METRICS SYSTEM

Maria Isaeva, Michael Gluharev

Emperor Alexander I St. Petersburg State Transport University

Russia, St. Petersburg, Moskovsky Prospekt, 9

emails: isaeva.mf@gmail.com, mlgluharev@yandex.ru

Abstract: The article presents a common structure of database safety metrics system, substantiates the necessity to its development, reveals the role of security metrics in estimating the quality of databases and information systems in general.

Keywords: databases; information safety; safety metrics.

Введение. Защищенность информации в информационно-управляющих системах (ИИУС) – одно из необходимых условий ее безопасной эксплуатации, которая позволяет организациям избегать экономических и репутационных потерь, связанных с нарушением конфиденциальности, целостности и доступности информации, обеспечивать пользователей достоверной и актуальной информацией, а во многих случаях – предотвращать угрозы здоровью и жизни людей. Важным компонентом ИИУС является база данных (БД). В настоящее время существует множество моделей данных различных степеней сложности, предложено множество способов реализации технологии активных БД, что неизбежно приводит к увеличению числа возможных угроз, реализуемых через БД и СУБД, следовательно, возрастает роль защищенности БД в обеспечении безопасности ИИУС и их качества в целом. Эффективность работы ИИУС может быть значительно снижена при наличии ошибок в процессе проектирования системы защиты информации и при неправильной оценке обеспечиваемого уровня защиты информации до ввода в эксплуатацию данной системы.

Все методы защиты информации в базе данных (БД) можно классифицировать на несколько больших групп: организационные, аппаратные, программные, процедурные и структурные.

Организационные методы защиты используются для ограничения числа лиц, которые получают право доступа в помещение, где происходит работа с базой данных. Процедурные методы делают возможным доступ к данным и передачу их только тем пользователям, которые имеют соответствующие разрешения. Структурные методы защиты применяются на этапах проектирования структуры баз данных. Аппаратные средства защиты информации представляют собой различные

электронные устройства, встраиваемые в состав технических средств вычислительной системы. Программные методы играют важнейшую роль при создании эффективных систем защиты информационных ресурсов БД – они позволяют реализовать большинство функций защиты: идентификацию пользователей БД, проверку подлинности пользователей, проверку полномочий пользователей на совершение того или иного действия в системе, реагирование на попытку несанкционированного доступа (НСД) к системе и другие.

При разработке БД во время активного развития информационных технологий очень важно получить высококачественный продукт. В связи с этим возникает вопрос об оценивании качества БД и, в частности, оценивании уровня защищенности. Известно, что для оценивания качества программного обеспечения АИУС на различных стадиях жизненного цикла используется разветвленная система метрик, являющаяся результатом работы большого числа специалистов в течение нескольких десятилетий [1]. Представляется целесообразным оценивать качество БД аналогичным образом, т. е. основываясь на системе метрик для БД. Однако вопросам оценки качества БД уделяется намного меньше внимания. Показатели качества информации в БД предложены в работах В. В. Липаева (например, [2]). Оценка проекта БД на соответствия требованиям к схеме данных и программным механизмам поддержки целостности информации предложены в работе [3]. Тем не менее, существует потребность в более глубокой проработке этих вопросов, в частности, создании системы метрик защищенности БД.

Система метрик имеет иерархическую структуру. Корнем иерархии является качественный показатель – уровень защищенности – со значениями «высокий», «средний», «низкий». Защищенность складывается из обеспеченности таких свойств информации, как конфиденциальность, целостность и доступность, плюс подотчетность и подлинность ресурсов БД (второй уровень иерархии). На третьем уровне иерархии расположены интегральные показатели, отражающие соответствие БД требованиям нормативных документов и стандартов по каждому свойству защищенности. Более низкие уровни включают конкретные количественные и качественные характеристики, каждая из которых отражает отдельное свойство, частную особенность БД. Сюда могут относиться технико-экономические показатели – затраты, производимые на разработку и в процессе эксплуатации; безопасное время (математическое ожидание времени «взлома» метода защиты путем опробования множества вариантов проникновения) [4]; для определения уровня защищенности информации от несанкционированного доступа и одновременно доступности информации для легитимных – сложность иерархии субъектов доступа (пользователей и ролей), сложность, детализированность, безызыбочность и непротиворечивость правил разграничения доступа, эффективность применения различных моделей доступа в БД и т. п.

Заключение. Система метрик защищенности позволит не только оценивать уровень защищенности БД и ее качество в целом, но и принимать решения о создании новых методов и механизмов защиты с целью улучшения основных показателей.

СПИСОК ЛИТЕРАТУРЫ

1. Баранов С.Н., Тележкин А.М. Метрическое обеспечение программных разработок. Труды СПИИРАН. Выпуск № 5(36), 2014. ISSN 2078-9599, с.5-27
2. Липаев В.В. Обеспечение качества программных средств. Методы и стандарты. Серия «Информационные технологии». М.: СИНТЕГ, 2001. – 380 с. ISBN 5-89638-044-5.
3. Разработка показателей и методов оценивания корректности реляционных баз данных/ М. Л. Глухарев //Известия Петербургского университета путей сообщения/ Отв. ред. В. И. Ковалев. - СПб.: ПГУПС, 2008. - Вып.1. - С. 135-148.
4. Кульба В.В., Курочка Н.П. Математическая модель обеспечения безопасности информации в базах данных // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 7, №2 (2015) <http://naukovedenie.ru/PDF/108TVN315.pdf> (доступ свободный). Загл. с экрана. Яз. рус., англ. DOI: 10.15862/108TVN315.

УДК 004.457

ЗАЩИТА ИНФОРМАЦИИ ОТ СКРЫТЫХ УГРОЗ В СРЕДЕ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

Марков Вячеслав Сергеевич, Сидоренко Татьяна Владимировна
Санкт-Петербургский научный Центр Российской академии наук,
Россия, Санкт-Петербург, Университетская наб., 5
emails: markov@spbrc.nw.ru, puma@spbrc.nw.ru

Аннотация: Рассматривается метод обеспечения защиты информации в среде облачных вычислений, учитывающий контроль процессов выделения ресурсов по результатам идентификации потенциальных угроз, возникающих на уровне контроля взаимодействия системных процессов, реализуемых в гипервизоре. Данный подход позволяет оценить различные аспекты защищенности системы с учетом её топологии, режима работы и другой информации.

Ключевые слова: информационная система; облачные вычисления; защита компьютерных систем и сетей; информационная безопасность.

PROTECTION OF INFORMATION FROM HIDDEN THREATS IN THE ENVIRONMENT OF CLOUD COMPUTING

Markov Vyacheslav, Sidorenko Tatiana

The St. Petersburg scientific centre of the Russian Academy of Sciences,

Russia, Saint-Petersburg, Universitetskaya emb., 5

emails: markov@spbrc.nw.ru, puma@spbrc.nw.ru

Abstract: The method of information security in the cloud computing environment, taking into account the process control resource allocation according to the results identifying potential threats on the level of control of interaction the system processes implemented in the hypervisor. This approach allows us to evaluate various aspects of system security taking into account its topology, operating mode and other information.

Keywords: *information system; cloud computing; protection of computer systems and networks; information security.*

Введение. Применение традиционных средств защиты информации, основанных на анализе событий безопасности в компьютерных сетях, в силу специфики угроз является недостаточным [1]. Одним из актуальных направлений решения этой проблемы является совершенствование сервисов защиты информации, которые осуществляют интегральную оценку состояния сети, управление её защитой.

Атаке могут подвергаться как элементы сетевой инфраструктуры провайдера, который представляет облачные услуги, так и сама среда виртуализации [2].

Защита от таких деструктивных воздействий должна осуществляться на уровне процессов управления системными вызовами или контроля недекларированных возможностей прикладного программного обеспечения, что требует создания новых методов противодействия попыткам внешних и внутренних пользователей изменить состояние защищенности информационных ресурсов среды облачных вычислений.

Анализ защищенности информационных систем.

Применение технологий облачных вычислений определяет необходимость рассмотрения возможных способов функционирования компонентов информационной среды. Распределенные вычислительные мощности системы облачных вычислений могут быть использованы для защиты, как других систем, так и компьютеров отдельных пользователей.

Потребности в защите определяются не только объемами и важностью защищаемой информации, но и условиями при использовании, хранении и её обработки, а также рассмотрением возможных способов дестабилизирующих воздействий, приводящих к нарушению функционирования компонентов информационной среды.

Особую опасность предоставляют угрозы, которые реализуются внутри периметра безопасности компьютерной сети, так как их локализация с применением современных средств защиты информации, например, с использованием антивирусов и сканеров безопасности, встречает существенные трудности [3]. Поэтому для создания эффективных механизмов защиты виртуальной инфраструктуры необходимо обеспечить безопасность не только физической среды, включая непосредственные серверы виртуализации, но и сети передачи данных, что позволит оперативно идентифицировать скрытые и потенциально опасные процессы информационного взаимодействия.

Традиционные средства обеспечения информационной безопасности такие, как средства разграничения доступа, межсетевые экраны, системы обнаружения вторжений, контролируют только те информационные потоки, которые проходят по каналам, предназначенным для их передачи, поэтому угрозы, реализуемые посредством скрытых каналов передачи информации, с их помощью не могут быть блокированы [4].

При этом динамический характер процессов информационного взаимодействия компьютерной сети затрудняет возможности оперативной оценки рисков программных и инфраструктурных ресурсов, предоставляемых в режиме удаленного доступа. В этих условиях важное значение приобретают технологии защиты от угроз, которые формируются с использованием скрытых каналов информационного воздействия или внутри периметра безопасности компьютерной сети [5].

В статье рассматривается один из подходов обеспечения защиты информации в среде облачных вычислений, который основан на контроле процессов выделения ресурсов в соответствии с результатами оперативной идентификации потенциальных угроз, возникающих на уровне доступа к прикладным информационным сервисам.

Заключение. Защита компьютерных сетей предполагает применение новых подходов к построению систем защиты информации, способных осуществлять непрерывный мониторинг защищенности сетей.

Предложено решение оперативной оценки идентификации скрытых и потенциально опасных процессов информационного взаимодействия компьютерной сети. Выделение анализируемых ресурсов между виртуальными машинами в соответствии с оценкой потенциальных угроз повысит безопасность виртуальной инфраструктуры.

СПИСОК ЛИТЕРАТУРЫ:

1. Бердник А. В., Бойко А.К. Методы защиты виртуальной среды // Всероссийский журнал научных публикаций, 2013, № 3 (18), С. 24-27.
2. Joint Task Force. Managing Information Security Risk. Organization, Mission and Information System View. -Gaithersburg: NIST 2011.
3. З.Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А. Технологии управления информацией и событиями безопасности для защиты компьютерных сетей // проблемы информационной безопасности, Компьютерные системы. №2, 2012.
4. Сычев А.М. Обоснование требований к межсетевым экранам и системам управления безопасностью в распределенных информационных системах: диссертация на соискание ученой степени кандидата технических наук: 05.13.19 / Сычев А.М. – М:МИФИ, 2002. – 149с.
5. Моляков, А.С. Модель скрытых угроз информационной безопасности в среде облачных вычислений Текст]. / А.С. Моляков, В.С.Заборовский, А.А. Лукашин// Проблемы информационной безопасности, Компьютерные системы, - СПб.: Изд-во Политех. Ун-та, 2014. - №2. – С.41-46

УДК 004.6

**СПОСОБ УМЕНЬШЕНИЯ СЛУЖЕБНОГО ТРАФИКА В СЕТИ ПЕРЕДАЧИ ДАННЫХ
С КОММУТАЦИЕЙ ПАКЕТОВ**

Курашев Заур Валерьевич

Военная академия связи имени маршала Советского Союза С.М. Буденного,
Россия, Санкт-Петербург, Тихорецкий проспект, 3
emails: Frankilou@yandex.ru

Аннотация: Рассмотрена сеть передачи данных с коммутацией пакетов. Особенности служебного трафика циркулируемого в сети. Предложен способ уменьшения служебного трафика и выигрыш.

Ключевые слова: Трафик, сеть передачи данных, коммутация пакетов.

A METHOD FOR REDUCING THE OVERHEAD IN A PACKET DATA NETWORK

Zaur Kurashhev

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny,
Russia, St. Petersburg, Tikhoretsky avenue 3,
emails: Frankilou@yandex.ru

Abstract: Considered a network of data transmission with packet switching. Features of the service traffic circulating in the network. A method for reducing the service traffic and gaining.

Keywords: Traffic, communication network, packet switching.

Важной подсистемой системы связи является сеть передачи данных (СПД). Для определения места и роли СПД обратимся к РД 45.128 - 2000 «Сети и службы передачи данных». Согласно руководящего документа «Службой ПД называется служба электросвязи, позволяющая пользователям получать от оператора связи набор услуг передачи данных на базе одной или нескольких сетей данных». Сети ПД не включают в себя окончное оборудование данных (ООД), в роли которого может выступать ЭВМ. С распространением ЭВМ повысилась потребность в передаче данных. Протоколы определяют правила обмена на различных уровнях функциональной архитектуры ЭМВОС. Основными аспектами функционирования протокола является эффективность и надежность. Эффективность связана с производительностью, задержкой, избыточностью и другими количественными характеристиками. Надежность обусловлена правильностью функционирования протокола при передаче данных [1]. Основными показателями эффективности традиционно являются производительность и задержка. Производительность оценивается скоростью передачи полезной информации между процессами с учетом всей управляющей информацией и повторных передач. Задержка характеризуется временем начала передачи пакета передатчиком до момента успешного поступления всего пакета в приемник или прихода подтверждения в передатчик при оценке полной задержки.

При передаче больших объемов информации между процессами данные могут иметь различный размер пакета. В сетях с коммутацией пакетов задержка будет меньше для небольших пакетов, поскольку время передачи на каждом переприемном участке между узлами коммутации пропорционально длине пакета. Избыточность в коротких пакетах увеличивается, так как каждый пакет содержит заголовок фиксированной длины и для одного и того же объема информации потребуется большой объем обработки и подтверждений. При коротких пакетах максимальная производительность уменьшается, а эффективность линии возрастает. При использовании длинных пакетов уменьшается избыточность и повышается производительность из-за увеличения задержки [2,3].

Трафик сети передачи данных делится на два класса. К первому классу относится трафик реального времени (передача голосовых сообщений), ко второму классу относятся информационные потоки (пересылка файлов или данных). Способ уменьшения служебного трафика, относящийся к классу информационных потоков, заключается в формировании на передающей стороне сообщения,

которое в процессе передачи делится на пакеты различной длины и принимается адресатом на приемной стороне. В свою очередь адресат получивший пакет должен отправить пакет с подтверждением. Данный пакет он прикрепляет к передаваемому пакету и посылает в канал связи. Вопросы достоверности информации реализованы на другом уровне функциональной архитектуры. Предлагаемый способ может быть использован в сети передачи данных, который увеличивает пропускную способность линий в два раза, для использования в интересах других услуг.

СПИСОК ЛИТЕРАТУРЫ

1. Протоколы и методы управления в сетях передачи данных: Пер. с англ. / Под ред. Ф.Ф. Куо. -М.: Радио и связь, 1985. -480 с.
2. Forney, G.D., Jr., «Convolutional Codes III: Sequential Decoding», Information and Control, 25, pp.267-297, July 1974.
3. Robinson, J.P., «Error Propagation and Definite Decoding of Convolutional Codes», IEEE Transactions on Information Theory, IT-14, pp. 121-128, January 1968.
4. Чуднов А.М., Кирик Д.И., Курашев З.В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений/ Радиотехнические и телекоммуникационные системы. - 2017. -№2. с.41-49.
5. Брунилин А.А., Бирюков М.А., Саенко И.Б. Модель и метод использования онтологий для управления разграничением доступа в едином информационном пространстве // Математические методы в технике и технологиях – ММТТ. 2016. № 6 (88). С. 122-124.
6. Башкирцев А.С., Михайличенко Н.В., Ренсков А.А., Парашук И.Б. Совершенствование объема и номенклатуры множества контролируемых параметров, принадлежащих пространству управления информационными системами и сетями // Успехи современной науки 2017, №1, Т.4, С.46-52.
7. Неижмак А.В., Орешина М.А. Методы защиты облачных хранилищ // Образование и информационная культура: теория и практика. Материалы Межрегионального форума. Под редакцией В.Г. Шубовича. 2016. С. 88-92.
8. Неижмак А.В., Орешина М.А. Направления по защите облачных хранилищ // Информационная и компьютерная безопасность материалы Межрегионального форума «Кибердружина». 2016. С. 30-31.
9. Модель системы связи с управляемыми структурами в конфликтных условиях/ П.Н. Барашков, А.П. Родимов, К.А. Ткаченко, А.М. Чуднов. – Л.: ВАС, 1986. – 52 с.

УДК 004.056.5

ЗАЩИТА ИНФОРМАЦИИ И ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Карташов Павел Николаевич

Санкт-Петербургский государственный экономический университет, кафедра информационных систем и технологий (ИСИТ),

Россия, 191023, Санкт-Петербург, улица Садовая, 21.

email: torgul@bk.ru

Аннотация: С каждым годом всё большее количество информации сохраняется и обрабатывается в цифровом виде. Разнообразные «девайсы» и «гаджеты» стали неотъемлемой частью жизни большинства людей. Помимо рабочей или финансовой информации устройства стали нести в себе и огромное количество личных, конфиденциальных данных. В связи с этим активно развиваются различные программные и аппаратные средства защиты информации. А потому в системе человек-компьютер всё более уязвимым звеном становится не машина, а сам человек. В статье рассмотрены проблемы защиты информации, связанные именно с человеческим фактором.

Ключевые слова: защита информации; безопасность; социальная инженерия; человеческий фактор.

DATA PROTECTION AND THE HUMAN FACTOR

Kartashov Pavel

The St. Petersburg State Economical University

Russia, St. Petersburg, Sadovaya str. 21,

email: torgul@bk.ru

Abstract: From year to year more and more information is stored and processed in digital forms. A variety of "devices" and "gadgets" have become an integral part of most people's lives. Besides working or financial data, the devices now carry a huge amount of personal, confidential information. For that matter various software and hardware methods of information protection are actively developing. Therefore, in the human-computer system, the increasingly vulnerable component is not the machine, but the person himself. The article deals with the problems of data protection, in the context of the human factor.

Keywords: data protection; security; social engineering, human factor.

В современном мире информация является одним из ценнейших ресурсов. Утечка данных может привести к весьма печальным последствиям, начиная от крупных финансовых потерь и заканчивая человеческими жертвами. Согласно ISO/IEC 2382:2015 информационная система представляет собой систему, предназначенную для хранения, поиска и обработки информации, к которой также относятся организационные ресурсы (человеческие, технические, финансовые и т.д.), которые обеспечивают и распространяют информацию.

По мере развития технологий всё больше информации хранится и обрабатывается именно в электронном виде. Разнообразные «девайсы» и «гаджеты» могут иногда поведать о человеке больше, чем его окружение. Столь привычные и уже незаменимые в обычной жизни устройства сохраняют в себе фотографии, видеозаписи, переписки, рабочие документы, различную финансовую и прочую конфиденциальную информацию. Они как будто «впитывают» и несут в себе часть жизни своего владельца. А потому неудивительно, что эту оцифрованную информацию человек стремится защитить максимально надёжно. И со временем пользователю начинает казаться, что если он надёжно защитит свой компьютер (планшет, телефон, локальную сеть – неважно), то его информация будет в безопасности. Однако не стоит забывать, что в системе человек-компьютер уязвимым звеном всегда будет оставаться не машина, а сам человек.

При подготовке и обучении специалистов в информационной сфере, особое внимание надо уделять человеческому фактору и его роли в информационных системах. Так, предлагая своим студентам подготовить выступления по темам «угрозы информационной безопасности» и «методы защиты информации», я неоднократно сталкивался с тем, что наиболее подробно они рассматривали всю техническую сторону вопроса: системы контроля доступа, персональную идентификацию, ключи и шифрование данных, защиту сетей, программно-технические методы и т.д. Дыры в безопасности, связанные с человеческим фактором, обычно комментировались дежурной фразой «применять организационные методы защиты». Примеры подобных уязвимостей обычно приводились с трудом, не хватало понимания того, как через слабости человека пробивается брешь в информационной безопасности.

Если провести анализ известных случаев взломов и проникновений в защищённые информационные системы, то вы увидите, что большинство из них были связаны именно с человеческим фактором. Случаи умышленной кражи, порчи или уничтожения информации сотрудниками внутри своей организации мы сейчас рассматривать не будем. Такие проблемы чаще всего решаются на уровне подбора кадров и жёсткого разграничения доступа. Последствия же разбираются постфактум с привлечением ответственных за безопасность внутри организации, а также соответствующих служб органов внутренних дел.

Для нас интерес представляют ситуации, когда человек неумышленно оставляет «открытые двери» в информационной безопасности и не придаёт должного значения произошедшему с целью минимизации последствий. Как примеры можно упомянуть потерю рабочего пропуска или банковской карты без дальнейшей их блокировки, удаление или изменение какой-либо информации по неосторожности, оставление в доступных местах записанных паролей, ключей доступа, конфиденциальной информации и т.п.

В подобных случаях сотрудникам должна изначально по всем ключевым моментам разъясняться ситуация с личной ответственностью за информацию, с которой они работают. Должны быть составлены соответствующие инструкции. Необходимо проводить беседы и разъяснять порядок действий в той или иной ситуации для минимизации негативных последствий.

Отдельным пунктом стоит упомянуть случаи, когда злоумышленники проникают внутрь защищенной информационной системы, пользуясь обычными слабостями человеческого характера. Чаще всего это связано с тем, что на многие события люди реагируют автоматически, привычным для них способом. Об этом писал в своей книге «Психология влияния» Роберт Чалдини. Серьезно и аналитически человек реагирует только на ту информацию, на которую у него есть время и желание, в остальных случаях реакция обычно идёт по типу «щёлк, зажужжало». Также у сотрудников, чья работа однообразна, утомительна и предполагает обработку большого количества информации, часто срабатывает рефлекс: позвонили и сказали, что надо сделать – делаем. В качестве примера подобных действий Роберт Чалдини упоминает эксперимент, проводившийся психологами, которые обзванивали медсестёр в больницах и, представившись врачом, давали распоряжение ввести смертельную дозу препарата пациенту. Медсёстры понимали, что делают, но в силу загруженности по работе и давления авторитета позвонившего, шли выполнять поставленную задачу. Останавливали их уже на входе в палату. Подобные методы воздействия получили название социальная инженерия.

Одним из родоначальников социальной инженерии был Кевин Митник, который в своей книге «Искусство обмана» прямым текстом говорит о том, что намного проще получить доступ, воздействуя на людей, чем пытаться взломать систему.

Задача с проникновением в чужую информационную систему намного упрощается, если провести предварительную разведку и запастись сведениями, находящимися в открытом доступе: имена сотрудников или знакомых (особенно руководства, друзей, родственников), номера телефонов, род занятий, увлечения и т.д. Всё это может быть использовано как для проникновения на объект, так и для последующего воздействия через телефон, смс, электронную почту и т.д.

Выбрав «жертву», злоумышленник попытается втереться в доверие, ссылаясь на доступную ему информацию. После чего он может уговорить или сообщить ему что-то, или же выполнить какие-то действия. Подобным образом сейчас работают мошенники, действующие через социальные сети или телефон, выманивая у доверчивых людей деньги.

Для проникновения в организации чаще всего используются рядовые сотрудники, которые хоть и не обладают высоким уровнем допуска, но могут открыть доступ к «следующей ступени». Полученные сведения собираются, анализируются и используются для воздействия на сотрудника более высокого ранга.

Для противодействия подобным мошенническим действиям необходимо регулярно проводить инструктажи сотрудников. Стоит разъяснить им, что информация, которую легко найти в открытом доступе, не может служить для авторизации.

Разрабатывая «организационные методы защиты информации», необходимо понимать, что, даже обнаружив какую-то угрозу и проинструктировав о ней сотрудников или просто близких вам людей, нельзя быть до конца уверенным, что эта информация останется навсегда усвоенной. Регулярные инструктажи по защите информации должны быть частью вашей системы безопасности наравне с программно-техническими методами.

СПИСОК ЛИТЕРАТУРЫ:

1. Верзун Н.А., Колбанев М.О., Татарникова Т.М. Аспекты безопасности информационно-экономической деятельности // Технологии информационно-экономической безопасности: сб. статей сотр. каф. ИС и Т. – СПб.: Изд-во СПбГЭУ, 2016. – С.52–56.
2. Митник К. Д., Саймон В. Л. Искусство обмана. М.: Компания АйТи, 2004. 359 с.
3. Чалдини Р, Психология влияния. СПб: Питер, 2011. 304 с.

УДК 811.116.1

ИНФОРМАЦИОННО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИН ЛИНГВИСТИЧЕСКОГО ЦИКЛА

Колоколова Лидия Петровна

Стерлитамакский филиал Башкирского государственного университета

Россия, Республика Башкортостан, Стерлитамак, пр. Ленина, 49

emails: kollidia@rambler.ru

Аннотация: В статье рассмотрены информационно-технические средства, активно применяемые в учебной деятельности при изложении нового материала, на этапе закрепления изученного материала, при контроле и проверке, а также при самостоятельной работе. Процесс технологизации ускоряет передачу и освоение знаний, способствует формированию языковых корпусов, обеспечивает взаимодействие преподавателя и обучаемого в современных системах открытого и дистанционного образования.

Ключевые слова: информационные средства; компьютерное обучение программное обеспечение, книговедение, библиография.

INFORMATION-TECHNICAL SUPPORT DISCIPLINES OF LINGUISTIC CYCLE

Lidia Kolokolova

Sterlitamak Branch of Bashkir state university

Russia, Republic of Bashkortostan, Sterlitamak, Lenin Prospect, 49

emails: kollidia@rambler.ru

Abstract. The article presents information technologies, actively used in the educational activity in describing new material, at the stage of consolidation of the material, at controls and examination, as well as independent work. Process technologizing accelerate the transfer of knowledge and learning, promotes formation of a language corps, provides interaction the teacher and the student in modern systems of open and distance education.

Keywords: information technologies; computer education; software; bibliography, bibliography.

Введение. В настоящее время существует довольно большое число языковых корпусов, которые отличаются друг от друга по самым разным параметрам, поэтому в учебном процессе наблюдается устойчивый интерес исследователей к привлечению информационных технологий в преподавание корпусной лингвистики. Внедрение информационных технологий (ИТ) в образовательный процесс не столько насущная необходимость, сколько осознанный процесс технологизации рутинных процессов с целью проведения лингвистического анализа компьютеризированных библиографических источников. Информационные технологии в обучении русскому языку позволяют интегрировать в рамках одной программы тексты, графику, звук, высококачественные фотоизображения.

Таким образом, одной из наиболее важных задач, стоящих перед российской системой образования, является обеспечение доступности и качества образовательного процесса, итогом которого должно быть формирование конкурентоспособного выпускника. Данная цель не может быть достигнута без широкого внедрения, без опоры на современные информационные технологии в образовании.

В рамках дисциплины «Книговедение и библиография» информационные технологии позволяют решить следующие задачи: сформировать в сознании специалистов гуманитарного профиля

необходимые для научной и педагогической деятельности базовые представления о книговедении и библиографии; освоить научное знание о книге, социальные функции книги, виды и типы книжных изданий, современные классификации книжных изданий.

Методологически внедрение ИК в процесс обучения ускоряет передачу и освоение знаний и способствует формированию книговедения и библиографии. Важным качеством современных ИТ является их универсальность: они могут быть основой в организации любой деятельности, связанной информационным обменом, основой в создании общего информационного языкового пространства.

Наибольшую популярность среди технических приложений лингвистики получило компьютерное обучение. Компьютер является многофункциональным помощником, хорошим методическим инструментом наряду с другими средствами обучения. Актуальность компьютерных технологий в преподавании русской словесности налицо, так как новые условия, непринужденная обстановка, общение с компьютером, одобрение электронного помощника результатов труда имеют позитивную оценку. Студенты с разной степенью грамотности сосредотачиваются на ключевых моментах, так как машина идет вместе со студентом от незнания к знанию, акцентируя внимание на неусвоенном материале. Компьютерное обучение даёт возможность представить состав книговедения, книговедческую типологию, электронную книгу, книгопроизводство, основные процессы и продукцию, внешние и внутренние элементы книги.

Информационные технологии позволяют представить в объёме национальный корпус, его размер, хронологический охват языка, репрезентативность корпуса, филологическую экспертизу, типы аннотирования, а также метаразметку как часть поискового аппарата корпуса, различные технологии разметки (автоматическая, полуавтоматическая ручная разметка).

Технические средства успешно находят применение при составлении словарей, созданных на базе корпуса (традиционные словари, электронные словари, частотные словари разного типа: с входной единицей – лексемой, с входной единицей – словоформой; частотный словарь словоформ русского языка). Например, по теме «Библиография» важно учитывать следующие этапы работы: 1) предмет, объект, задачи изучаемой проблемы, 2) библиографические сведения, 3) понятие словарной статьи, структура словарной статьи, 4) издательство, 5) лексикографический анализ слова. Технические средства дают возможность представить исследовательскую работу в целом и затем поэтапно рассматривать каждый отдельный информационный блок. Особенно этот вид деятельности характерен при анализе схемы комплексного лексикографического анализа, включающего следующие виды деятельности: 1) дать полное название словаря, 2) указать, выходные данные (автор (ы), год издания, место издания, издательство), 3) определить объект описания, 4) охарактеризовать структуру словарных статей и их содержание, 5) определить принцип построения словаря, 6) определить структуру словаря, 7) определить, на кого рассчитан словарь, 8) охарактеризовать объём словаря и специфику его оформления: таблицы, схемы, карты, иллюстрации, фото ит.п., 9) описать словарную статью.

Совершенно очевидно, что информационные технологии (ИТ) – это широкий спектр цифровых технологий, используемых для создания, передачи и распространения информации и оказания услуг (компьютерное оборудование, программное обеспечение, телефонные линии, сотовая связь, электронная почта, сотовые и спутниковые технологии, сети беспроводной и кабельной связи, мультимедийные средства).

Примером успешной реализации ИКТ в современном учебном процессе стало появление Интернета – всемирной компьютерной передачи с ее практически неограниченными возможностями сбора и хранения информации, передачи ее индивидуально каждому пользователю. Технология Интернет как среда коммуникации является посредником во включении студента в сетевые структуры, на основе которого он получает возможность эффективно использовать информацию, предоставляя ее заинтересованным людям в кратчайшие сроки.

Совершенно очевидно, в рамках дисциплин лингвистического цикла эффективность обучения может быть значительно повышена с помощью ИТ, применяемых в различных, оптимальных для данных занятий сочетаниях с другими средствами обучения.

СПИСОК ЛИТЕРАТУРЫ

1. Коган Е. И. Библиография, отражающая статус вуза // журнал «Библиография и книговедение». 2015. № 1.
2. Сафиуллина З. А. Концепт социальной памяти в библиографоведении // журнал «Библиография и книговедение». 2015. № 2.

УДК 004.89

РЕШЕНИЕ БАЗОВОЙ ВЫЧИСЛИТЕЛЬНОЙ ЗАДАЧИ МЕТОДАМИ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ

Мельников Александр Владимирович, Нарушев Илья Романович
Воронежский институт Министерства Внутренних Дел Российской Федерации,
Россия, Воронеж, пр-т. Патриотов, 53,
emails: meln78@mail.ru, nar_i@bk.ru

Аннотация: В статье рассматривается метод погружения базовой вычислительной задачи сравнения технических объектов в экспертную оболочку в классе методов data mining.

Ключевые слова: data mining, экспертные системы, кластеризация.

THE SOLUTION OF THE BASIC COMPUTATIONAL PROBLEM BY METHODS OF INTELLECTUAL DATA ANALYSIS

Melnikov Aleksander, Narushev Ilya
The Voronezh Institute of the Ministry of Interior of Russia,
Russia, Voronezh, Patriotov str. 53,
emails: meln78@mail.ru, nar_i@bk.ru

Abstract: The article deals with the method of immersing the basic computational task of comparing technical objects to the expert shell in the class of data mining methods.

Keywords: data mining, expert systems, clustering.

Введение. Типичной особенностью в современной теории экспертных систем является применение интеллектуальных способов обработки данных (data mining). Data Mining (глубинный анализ данных, интеллектуальный анализ данных) — емкостное понятие, обозначающее совокупность методов обнаружения в множестве данных ранее неизвестных, нетривиальных и доступных интерпретации знаний, необходимых для принятия решений. в различных сферах человеческой деятельности [1], [2], [3].

В основе методов Data Mining лежат методы теории экспертных систем, классификации, моделирования и прогнозирования, основанные на применении нейронных сетей, генетических алгоритмов, многомерного регрессионного анализа, методов кластеризации, метода анализа иерархий, ассоциативной памяти, теории нечетких множеств, факторного анализа, метода главных компонент и др. В общем, упомянутые методы лежат на стыке теории баз данных, статистики и искусственного интеллекта.

Задачи, решаемые методами Data Mining, очень часто разделяют на описательные (descriptive) и предсказательные (predictive). Описательные задачи дают наглядное описание имеющихся скрытых закономерностей, в то время как в предсказательных задачах на первом плане стоит вопрос о предсказании для тех случаев, для которых данных ещё нет. К описательным задачам относятся: поиск ассоциативных правил или паттернов, кластерный анализ, нечетко-множественное описание признаков, построение регрессионной модели. К предсказательным задачам относятся: прогнозирование, регрессия на главные компоненты, метод анализа иерархий, гребневая регрессия, анализ временных рядов и т.д.

Описание метода представления в экспертной оболочке задачи сравнения технических объектов. Метод предназначен для совершенствования решения класса вычислительных задач оценки и сравнения технических объектов (систем, приборов, устройств) как по чисто техническим характеристикам, так и по показателям «качество-цена».

Предлагаемая процедура реализуется в несколько этапов.

1. К множеству сравниваемых объектов применяется принцип теории экспертных систем — выделения наиболее информативных признаков и разделения признаков на количественные, качественные, наличия определенных свойств, признаки общей инженерной оценки, признаки критической оценки [4]. В зависимости от влияния на обобщенный показатель качества объекта выделяют признаки положительного эффекта (ППЭ) и признаки отрицательного эффекта (ПОЭ).

Сформированное множество данных образует признаковое (факторное) пространство, которое в задачах многомерного статистического анализа часто называют множеством референтных данных [5].

2. Применение к полученному множеству методов интеллектуального анализа (data mining): метода анализа иерархий, теории нечетких множеств, модели множественной линейной регрессии, метода главных компонент, гребневой (ridge) регрессии, метода ассоциативного обучения нейронной сети, алгоритмов классификации, кластеризации, прогнозирования значений обобщенного показателя на основе многомерной калибровки, визуализации полученных результатов и др.

Обозначим исходную задачу сравнения технических объектов, к которой мы собираемся применить методы интеллектуального анализа, базовой задачей. Погружение в экспертную оболочку предполагает, во-первых, подготовку входных данных для базовой задачи (метод анализа иерархий, метод главных компонент, нечетко-множественные представления и др.). Во-вторых, необходимо представить итоговые результаты базовой задачи в наиболее полном и качественно интерпретируемом виде (метод ассоциативного обучения, классификация объектов экспертизы, алгоритмы кластеризации и др.).

Здесь важен выбор наиболее рациональных приемов визуализации результатов. Как известно, проблема визуализации является далеко не тривиальной [6].

3. Применение большинства из перечисленных выше методов интеллектуального анализа осуществляется на основе теории нейронных сетей [7], [8]. Так, для прогнозирования значений обобщенного показателя качества объекта используется нейронная сеть прямого распространения сигнала с обратным распространением ошибки (feed-forward backprop), для реализации ассоциативного обучения — нейронная сеть с функцией активации softmax. Для решения задачи классификации используется нейронная сеть персептрон, а для кластеризации объектов экспертизы — самоорганизующаяся сеть Кохонена с функцией активации compelayer.

Заключение. В целом, предлагаемый метод погружения вычислительной задачи сравнения технических объектов в экспертную оболочку в классе программ реализации методов искусственного интеллекта представляется эффективным средством повышения надежности принимаемых управленческих решений. Дальнейшее расширение экспертной оболочки по сравнению с представленным выше примером целесообразно на основе методов теории нейронных сетей, например, кластеризации объектов экспертизы с помощью самоорганизующихся нейронных сетей.

СПИСОК ЛИТЕРАТУРЫ

1. Барсегян А.А. и др. Технология анализа данных: Data Mining, Text Mining, OLAP. СПб.: БХВ – Петербург, 2007. – 384 с.
2. Дюк В., Самойленко А. Data mining: учебный курс. СПб.: Питер, 2001. – 368 с.
3. Witten I., Frank E., Hall M. Data Mining: Practical Machine Learning Tools and Techniques. N.Y.: Morgan Kaufmann, 2011. – 664 p.
4. Бухарин С.В., Мельников А.В. Кластерно-иерархические методы экспертизы экономических объектов. Воронеж: Научная книга, 2012. – 276 с.
5. Эсбенсен, К. Анализ многомерных данных. Избранные главы. Черноголовка, Изд-во ИПХФ РАН, 2005. – 160 с.
6. Chambers J. et al. Graphical methods for data analysis. Belmont, CA: Wadsworth, 1983 – 415 p.
7. Хайкин С. Нейронные сети: полный курс. М.– СПб.– Киев: Вильямс, 2006. – 1104 с.
8. Бухарин С.В., Навоев В.В. Методы теории нейронных сетей в экспертизе технических и экономических объектов. Воронеж: Научная книга, 2015. – 256 с.

УДК 004.056

ИЕРАРХИЧЕСКИЙ ПОДХОД К ВЫЯВЛЕНИЮ ВРЕДНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Москвин Дмитрий Андреевич, Павленко Евгений Юрьевич, Ярмак Анастасия Викторовна

Санкт-Петербургский политехнический университет Петра Великого,

Россия, Санкт-Петербург, ул. Политехническая, 29

emails: moskvin@ibks.spbstu.ru, pavlenko@ibks.spbstu.ru, nastyayarmak238@gmail.com

Аннотация: Предложена графово-событийная модель, позволяющая осуществить анализ поведения программы на основе генерируемых в процессе ее функционирования событий. Представлена архитектура системы, а также перечислен список событий, отслеживаемых на каждом уровне. Рассмотрены метрики, которые позволяют проводить оценку подобия полученной структуры графа и структуры графов заданных легитимных приложений. Приведены результаты эксперимента, иллюстрирующие эффективность предложенного подхода.

Ключевые слова: информационная безопасность, вредоносное программное обеспечение, гипервизор, анализ информационной безопасности, технология виртуализации.

HIERARCHICAL APPROACH TO DETECTING MALICIOUS SOFTWARE

Moskvin Dmitry, Pavlenko Evgeny, Yarmak Anastasiya

The St. Petersburg State Polytechnic University of Peter the Great,

Russia, St. Petersburg, Polytechnicheskaya str. 29,

emails: moskvin@ibks.spbstu.ru, pavlenko@ibks.spbstu.ru, nastyayarmak238@gmail.com

Abstract: Proposed the model based on event graph, which can provide the behavior analyses of a program. The graph is built by events generated during program execution. The architecture of the system is presented, and a list of events tracked at each level is listed. The metrics that allow comparing a structure of obtained graph with structure of legitimate program's graphs are also presented. The experiment's results experimental results illustrate the effectiveness of the proposed approach.

Keywords: information security, malware, hypervisor, security management, virtualization technology.

Введение. Процесс обеспечения безопасности информационных систем (ИС) подразумевает постоянный мониторинг событий информационной безопасности, их анализ и принятие решений о состоянии системы, а также обеспечение обратной реакции на обнаруженные отклонения и аномалии. Авторами предложен иерархический подход к обеспечению безопасности ИС, заключающийся в сборе и анализе событий на всех уровнях системы (на уровнях приложений операционной системы (ОС), ядра ОС, гипервизора и SMM и на уровне аппаратного обеспечения) [1].

Целесообразность иерархического подхода основана на исследовании современного вредоносного программного обеспечения (ВПО), в результате которого было установлено, что для ВПО характерна межуровневая миграция, позволяющая ему прочно закрепиться в системе.

При этом, в настоящее время отсутствуют подходы к обнаружению нарушений в ИС, способные анализировать безопасность на нескольких уровнях ИС. Существуют средства, функционирующие на одном, максимум на двух, уровнях, но они не взаимодействуют со средствами обнаружения, работающими на других уровнях. Разработанный подход учитывает особенности действия ВПО на каждом уровне системы, систематизированные в ходе анализа [2].

Для многоуровневого анализа событий в ИС предполагается внедрение специальных программных агентов, собирающих и анализирующих данные о состоянии системы на вышележащем уровне для каждого уровня иерархии. Система, реализующая анализ безопасности ИС на основе предложенного подхода, осуществляет сбор и анализ событий на каждом уровне безопасности, выявляет нарушения ИБ и устанавливает взаимосвязи между событиями с различных уровней.

Многоуровневый подход к анализу безопасности заключается в иерархическом представлении логики событий и выявлении взаимосвязей между событиями разных уровней в процессе функционирования программы. При переходе на более низкий уровень абстракций, частота генерации событий ИС может увеличиваться, поэтому с каждым событием верхнего уровня может быть связано макрособытие (комбинация событий, следующих друг за другом мгновенно) более низкого уровня.

Авторами предлагается строить граф событий, что реализуется в 2 этапа:

1. Выделение процессов и отслеживание событий на каждом уровне с помощью специальных агентов. На основе событий, произошедших на каждом уровне, составляется событийный граф, описывающий поведение программы. Каждому действию программы ставится в соответствие событие или цепочка событий нижележащего уровня.

2. Генерация графа событий программы с использованием полученной информации для установления взаимосвязей между событиями. На основе данного графа принимается решение о наличии вредоносной функциональности.

Закключение. Предлагаемый авторами подход позволяет выразить процесс воздействия на систему через цепочку событий, возникающих на различных уровнях ИС при функционировании ее программ. Использование графа событий позволяет проанализировать поведение программы на основе генерируемых событий и взаимодействия с компонентами ОС. Далее выполняется оценка отличия полученного графа от графов доверенных программ с использованием метрики, основанной на вычислении максимального общего подграфа двух графов.

СПИСОК ЛИТЕРАТУРЫ

1. Zegzhda P.D. A new approach to security evaluation of operating systems / Zegzhda P.D., Zegzhda D.P., Kalinin M.O. // Communications in Computer and Information Science. 2013. Т. 374. № PART II. С. 254-259.
2. Павленко Е.Ю. Иерархический подход к анализу нарушений безопасности в информационных системах/ Павленко Е.Ю., Ярмук А.В., Москвин Д.А. // Проблемы информационной безопасности. Компьютерные системы. 2017. № 1.

УДК 004.056.55

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ БЕЗОПАСНОСТИ В ДЕЦЕНТРАЛИЗОВАННЫХ СИСТЕМАХ ОБЛАЧНОГО ХРАНЕНИЯ ДАННЫХ

Мясников Алексей Владимирович, Москвин Дмитрий Андреевич
Санкт-Петербургский политехнический университет Петра Великого,
Россия, Санкт-Петербург, Политехническая ул., 29
emails: myasnikovalexey@gmail.com, moskvin@ibks.ftk.spbstu.ru

Аннотация: В докладе рассматриваются преимущества конечного пользователя в аспекте хранения конфиденциальных данных при использовании современных сервисов децентрализованного облачного хранения данных, в отличие от традиционных централизованных облачных хранилищ. Приводятся сравнения в организации подхода к безопасности пользовательских данных в каждом из случаев. Рассматривается ряд атак, возможных на децентрализованные системы облачного хранения.

Ключевые слова: децентрализованные сети; облачные хранилища; информационная безопасность; облачные вычисления.

ANALYSIS OF INFORMATION SECURITY MECHANISMS IN DECENTRALIZED SYSTEMS OF CLOUD DATA STORAGE

Miasnikov Alexei, Moskvina Dmitrii
Peter the Great St. Petersburg Polytechnic University
Russia, St. Petersburg, Politekhnikeskaya ul., 29
emails: myasnikovalexey@gmail.com, moskvin@ibks.ftk.spbstu.ru

Abstract: The article discusses the advantages for the end user while storing confidential data with modern decentralized cloud storages in comparison with traditional centralized cloud storages. Comparisons are given in the approaches to keeping security of user data in each of the cases. A number of attacks, possible on decentralized systems of cloud storage, are considered.

Keywords: *decentralized networks; cloud storage; informational security; cloud computing.*

Введение. Безопасность хранения и передачи данных в централизованных облачных средах основана на доверии к владельцу облачной инфраструктуры и доверии к криптографическим средствам защиты, реализованных поставщиком услуг. Кроме того, централизованные облака уязвимы для множества атак, в числе которых атаки типа «человек посередине», атаки на программное обеспечение и инфраструктуру облака, ведущие к раскрытию пользовательских данных.

Стремительное развитие распределенных технологий, произошедшее за последние годы, породило интерес к теме организации децентрализованных облачных хранилищ, в качестве альтернативы традиционным облакам. Такие сервисы как storj.io, sia, maidsafe используют в основе своей архитектуры технологию блокчейн для организации распределенной инфраструктуры передачи данных. Эти облачные системы не предполагают наличие централизованного управления, но при этом архитектурные решения, положенные в их основу, позволяют обеспечить такие требования безопасности, как сохранение конфиденциальности, целостности и доступности передаваемых пользовательских файлов.

Механизмы обеспечения конфиденциальности основаны на использовании шифрования на стороне клиента и разбиении выгружаемого файла на фрагменты. Каждый пользователь децентрализованного хранилища генерирует пару ключей и при выгрузке файлов в облако шифрует все исходящие данные. Таким образом, благодаря криптографическим преобразованиям, ни один из узлов децентрализованной сети, не обладающий нужным ключом, не сможет прочитать чужие данные.

Механизмы обеспечения целостности и доступности основаны на использовании распределенных хэш-таблиц, цифровых подписей, деревьев Меркла и дублирующих узлов. В децентрализованных облачных хранилищах применяется полный или частичный аудит доступности файла с целью получить доказательство возможности загрузки файла из облака. Для повышения доступности файла его фрагменты загружаются в сеть в нескольких экземплярах. Владелец файла через определенные промежутки времени может запросить доказательство возможности скачать фрагмент файла у децентрализованной системы. В случае, если некоторые узлы с фрагментом файла недоступны, (недоступность хранящего узла, нарушение целостности фрагмента), начинается процесс повторного создания экземпляра фрагмента файла. Таким образом, в системе происходит саморегуляция, направленная на постоянное поддержание доступности и целостности файлов.

Применение распределенной архитектуры нивелирует угрозы безопасности, связанные с доверием к третьей стороне. Однако, при данном подходе к организации хранилища появляется класс атак, характерных только для децентрализованных систем. Данные атаки могут нарушить стабильность работы облака при наличии критической массы захваченных нарушителем узлов в сети, например, в случае атаки sybil.

Заключение. Децентрализованные системы облачного хранения данных решают ряд проблем, связанных с безопасностью хранимых данных и доверием к третьей стороне. В скором времени они смогут стать достойной альтернативой традиционным облачным хранилищам. Для того, чтобы эти системы стали полностью пригодными для использования конечными пользователями необходимо усовершенствование методов резервирования файлов и популяризация подобных методов хранения среди обычных пользователей. Кроме того, идея сдачи свободных ресурсов в аренду ограничивается не только дисковым пространством, например, на базе похожей схемы можно на возмездной основе предоставлять вычислительные ресурсы компьютера (CPU, GPU).

СПИСОК ЛИТЕРАТУРЫ

1. Shawn Wilkinson, Tome Boshevski, Josh Brandoff, James Prestwich, Gordon Hall, Patrick Gerbes, Philip Hutchins, Chris Pollard. Storj – A Peer-to Peer Cloud Storage Network v 2.0, Декабрь 2016.
2. David Irvine. MaidSafe Distributed File System, Сентябрь 2010.
3. Nick Lambert, Qi Ma, David Irvine. Safecoin: The Decentralized Network Token, Январь 2015.

УДК 004.89

ИСПОЛЬЗОВАНИЕ КАРТ КОХОНЕНА В СРЕДЕ МАТЛАВ ДЛЯ КЛАСТЕРИЗАЦИИ АНОМАЛЬНОГО ПОВЕДЕНИЯ

Нарушев Илья Романович

Воронежский институт Министерства Внутренних Дел Российской Федерации,
Россия, Воронеж, пр-т. Патриотов, 53
email: nar_i@bk.ru

Аннотация: В статье рассмотрены проблемы и перспективы развития совершенствования алгоритмов выявления аномального поведения с помощью карт Кохонена и алгоритмов машинного обучения в среде Matlab для обеспечения безопасности информации и интерпретации угроз.

Ключевые слова: *машинное обучение; кластеризация; нейронные сети; аномальное поведение.*

APPLICATION OF ALGORITHMS OF NEURAL NETWORKS AND MACHINE LEARNING TO THE DETECTION OF ANOMALOUS BEHAVIOR

Narushev Ilya

The Voronezh Institute of the Ministry of Interior of Russia,
Russia, Voronezh, Patriotov str. 53,
email: nar_i@bk.ru

Abstract: The article deals with problems and development prospects using Kohonen maps and machine learning algorithms in the Matlab environment to provide information security and threat interpretation.

Keywords: *machine learning; clustering; neural networks; abnormal behavior.*

Введение. Использование карт Кохонена [1] для кластеризации аномального поведения может являться одним из наиболее перспективных методов. Для решения задач кластеризации входных векторов можно использовать самоорганизующуюся сеть в виде карты Кохонена обладающую в отличие от слоя Кохонена, следующим топологическим свойством: когда близким кластерам входных векторов соответствуют близко расположенные нейроны [2].

Топология размещения нейронов в слое Кохонена может задаваться М-функциями языка MATLAB gridtop, hextop или randtop, что соответствует размещению нейронов в узлах различных сеток со случайной топологией. Карта Кохонена для определения нейрона-победителя использует ту же процедуру, что применяется и в слое Кохонена, но с изменением весовых коэффициентов соседних нейронов некоторого радиуса в соответствии с правилом Кохонена [3]. В отличие от слоя Кохонена, расстояния между нейронами вычисляются 4 разными способами — с помощью специальных функций вычисления расстояний dist, boxdist, linkdist и mandist.

Карта Кохонена для определения нейрона-победителя использует ту же процедуру, которая применяется и в слое Кохонена. Однако на карте Кохонена одновременно изменяются весовые коэффициенты соседних нейронов в соответствии с соотношением, именуемым правилом Кохонена.

Топология карты расположения нейронов может быть как одномерной так и больших размерностей. В случае одномерной карты Кохонена, когда нейроны расположены вдоль линии, каждый нейрон будет иметь только двух соседей в пределах радиуса 1 или единственного соседа, если нейрон расположен на конце линии. Расстояния между нейронами можно определять различными способами, используя прямоугольные или гексагональные сетки, однако это никак не влияет на характеристики сети, связанные с классификацией входных векторов [3].

Правило обучения слоя Кохонена заключается в том, чтобы настроить нужным образом элементы матрицы весов. Предположим, что нейрон победил при подаче входа на шаг самообучения n , тогда строка g матрицы весов корректируется в соответствии с этим правилом. В пакете nntool настройка параметров сети по правилу Кохонена реализована в виде М-функции learnk.

Нейрон-победитель и все нейроны, лежащие в пределах его окрестности, подвергаются адаптации, в ходе которой их векторы весов изменяются «в направлении» вектора x по правилу Кохонена

Таким образом правило Кохонена представляет собой рекуррентное соотношение, которое обеспечивает коррекцию строки g матрицы весов добавлением взвешенной разности вектора входа и значения строки на предыдущем шаге. Вектор веса, наиболее близкий к вектору входа, модифицируется так, чтобы расстояние между ними стало еще меньше. В конечном счете, если в слое имеется достаточное количество нейронов, то каждая группа близких векторов окажется связанной с одним из нейронов слоя. В этом и заключается свойство самоорганизации слоя Кохонена.

Одна из проблем конкурирующего слоя состоит в том, что некоторые нейроны оказываются незадействованными (мертвые нейроны). Это проявляется в том, что нейроны, имеющие начальные весовые векторы, значительно удаленные от векторов входа, никогда не выигрывают конкуренции, независимо от того, как долго продолжается обучение.

Чтобы исключить такую ситуацию и сделать все нейроны чувствительными к поступающим на вход векторам, используются смещения (biases), которые позволяют нейрону стать конкурентным с нейронами-победителями. Это достигается положительным смещением, которое добавляется к отрицательному расстоянию удаленного нейрона. Соответствующее правило настройки, учитывающее нечувствительность мертвых нейронов, реализовано в пакете nntool в виде М-функции learncon и заключается в следующем.

Увеличение смещений для неактивных нейронов позволяет расширить диапазон покрытия входных значений, и неактивный нейрон начинает формировать кластер. Второе преимущество, связанное с коррекцией смещений, состоит в том, что они позволяют выравнивать значения параметра активности и обеспечить «притяжение» приблизительно одинакового количества векторов входа.

Заключение. Возможности по применению карт Кохонена весьма обширны, например: многомерность, различные виды сеток кластеров, графическая интерпретация и т.д. В связи с этим, их можно рекомендовать для применения сложных задач кластеризации с большим количеством объектов, в том числе для использования в алгоритмах кластеризации аномального поведения.

СПИСОК ЛИТЕРАТУРЫ

1. Хайкин С. Нейронные сети: полный курс / С. Хайкин: Пер. с англ. — 2-ое изд. — М. — СПб. — Киев: Вильямс, 2006. — 1104 с.
2. Кохонен, Т. Самоорганизующиеся карты / Т. Кохонен: Пер. с англ. — 3 изд. — М.: БИНОМ, 2008. — 655 с.
3. Медведев, В.С. Нейронные сети. Matlab 6 / В.С. Медведев, В.Г. Потемкин. — М.: ДИАЛОГ-МИФИ, 2002. — 496 с.

УДК 004.056

НЕ СТРУКТУРИРОВАННЫЕ ДАННЫЕ В ЗАДАЧАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Полтавцева Мария Анатольевна, Печенкин Александр Игоревич
Санкт-Петербургский политехнический университет Петра Великого,
Россия, Санкт-Петербург, ул. Политехническая, 29
emails: poltavtseva@ibks.spbstu.ru, pechenkin@ibks.spbstu.ru

Аннотация: В работе рассмотрены вопросы работы с неструктурированными данными при решении задач информационной безопасности. Приводится специфика и классификация данных с точки зрения автоматизированной обработки. Рассматриваются вопросы соотношения данных с классами онтологии предметной области и формирования экземпляров. Вводятся понятия дискретности и полноты онтологических концептов и определяются необходимые структуры метаданных.

Ключевые слова: неструктурированные данные; анализ; онтологии; информационная безопасность

SEMISTRUCTURED DATA IN INFORMATION SECURITY CHALLENGES

Poltavtseva Maria Anatolevna, Pechenkin Alexander Igorevich
The St. Petersburg State Polytechnical University Petra Velikogo,
Russia, St. Petersburg, Politechnicheskaya str. 29,
emails: poltavtseva@ibks.spbstu.ru, pechenkin@ibks.spbstu.ru

Abstract: The paper presents working with semistructured data due to the solution of information security problems. Given the specificity and classification of these data automated processing. The novelty of the paper is in the questions of data and ontology classes (domains) correlation. We introduce the concepts of discreteness and completeness of the ontological concepts and define the required metadata structure.

Keywords: semistructured data; data analysis; ontology; information security

Введение.

Развитие и расширение применения информационных технологий приводит не только к их проникновению во все сферы жизни, включая здравоохранение, образование и бытовое общение, но и эволюции атак. Одной из основных тенденций является использование методов социальной инженерии и фишинга, причем в том числе, в атаках на промышленные объекты [1]. Самыми распространенными атаками в банковской сфере за период с 01 июня 2015 г. по 31 мая 2016 г. ЦБ РФ признает рассылки электронных сообщений, содержащих вредоносное ПО [2]. Аналогичные тенденции отмечают и другие исследователи [3]. Таким образом, на сегодняшний день особенностью информационной безопасности частных, корпоративных и даже промышленных объектов является обеспечение не только сетевой и технической безопасности, но и безопасности относительно применения злоумышленниками социально-культурных методов.

В то же время, распространенность современных организаций, высокая численность сотрудников, обилие социальных сетей и медиа, электронных профилей и тому подобных решений не позволяет провести какой-либо комплексный анализ безопасности, включающий их как информационно – телекоммуникационный, так и социальный профиль (включая сайт, порталы партнеров и т.д.). Таким образом, возникает задача автоматизированного анализа не только структурированных (компьютерных) данных узкой предметной области, но широко спектра неструктурированных данных для решения различных задач информационной безопасности. Таких, как оценка защищенности, выявление угроз, проведение расследований, тестирование на проникновение и других.

Неструктурированные данные в области информационной безопасности.

К неструктурированным данным относят информацию, в явном виде, без предварительной обработки, не пригодную для выполнения задач анализа. Когда говорят о неструктурированных данных в современных информационных системах, выделяют следующие признаки [4]: разнообразие, неоднозначность, динамичность. В общем случае неструктурированные данные в области информационной безопасности можно представить двумя категориями.

Формализованная информация. Сюда относятся данные, полученные от технических устройств, результаты сканирования, журналы аудита, результаты работы автоматизированных систем. Эти данные имеют четкую структуру (хотя и отличающуюся между собой), ясный источник, и, зачастую, этого набора сведений достаточно чтобы говорить об их семантическом наполнении.

Неформализованная информация. К этой категории отнесем данные, касающиеся не технической сферы, хотя, конечно, они должны быть получены также с помощью автоматизированных средств, учитывая объемы информации. Сюда входят страницы сайтов сети Интернет (самой организации, ее партнеров, мероприятий, личные страницы сотрудников и т.д.), страницы социальных сетей, блоги другие слабо формализуемые источники данных.

При анализе формализованных данных, возможно сразу автоматизированными средствами установить значимые метаданные [5], такие как источник информации, семантическое значение информационного поля. Таким образом, в большинстве случаев возможно однозначно соотнести формализованные данные с экземпляром конкретного класса онтологии. При этом отдельной задачей становится установление связей между объектами. Наличие связи между классами онтологии показывает наличие связи между их экземплярами, однако при подобном анализе в большом числе случаев нельзя однозначно сопоставить экземпляры классов онтологии друг другу.

В большинстве случаев неформализованные данные могут быть единообразно представлены для предварительной обработки в виде плоского текста. При анализе неформализованных данных установление принадлежности к онтологии становится более сложной задачей, так как, зачастую, по имеющимся данным сложно идентифицировать объект и практически невозможно – его связи. Для решения этой задачи онтологическому классу ставится в соответствие формат данных класса (если его можно выделить – например, множество форматов телефонных номеров или электронной почты) и модуль извлечения понятий из данных. Последний, базируясь на известных методах извлечения понятий и именованных сущностей [6], позволит достаточно точно определять сами сущности, хотя применение методов выявления семантических связей в исходном тексте, таких как описанные в [7] и [8], не дает достаточно хорошего результата. Таким образом, возникает оценка достоверности принадлежности i -го экземпляра к j -му классу. Критерии принадлежности – оценки, позволяющие сделать вывод о принадлежности экземпляра классу (например, соответствие формату представления). Однако, не смотря на разную степень значимости, сами по себе эти оценки почти никогда не являются точными.

Также необходимо учесть дискретность большого числа данных. Под дискретностью в данном случае понимается различная степень полноты данных, начиная от самого общего представления и заканчивая детализированным. Возникает понятие полноты концепта, показывающего, на каком уровне детализации он представлен. Для ее оценки и учета описанной дискретной природы данных, с каждым классом онтологии оказывается связан признак дискретности $Discreetness \in \{0,1\}$ и, при $Discreetness=1$, иерархия полноты концепта H . Иерархия H позволяет выделить смысловые составляющие концепта, которые могут быть определены отдельно друг от друга.

Заключение.

В работе рассмотрена проблема обработки неструктурированных данных при решении задач в области информационной безопасности. Выделены основные свойства неструктурированных данных (разнообразие, неоднозначность и динамичность) и определены специфические данные такого рода, характерные для области информационной безопасности. Дано понятие формализованных и неформализованных данных в рассматриваемом контексте.

Для определения семантики неструктурированных данных предлагается использовать онтологию информационной безопасности, как предметной области, по аналогии с задачами интеграции данных из гетерогенных источников. Рассмотрены специфические вопросы определения семантики данных и их соотнесения с классами онтологии. Определены необходимые метаданные для корректного соотнесения данных и экземпляров онтологических классов. Введены понятия дискретности и полноты концептов.

СПИСОК ЛИТЕРАТУРЫ

1. Кибербезопасность 2016-2017: от итогов к прогнозам // <https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-2016-2017-rus.pdf>
2. Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России // http://www.cbr.ru/credit/Gubzi_docs/fincert_survey.pdf
3. Угрозы и тенденции рынка информационной безопасности. Защита от атак «нулевого» дня // Jet Infosystems VII ежегодная конференция Центра информационной безопасности компании «Инфосистемы Джет» «Pro безопасность» 06.2016г.
4. Артем Гришковский Интегрированная обработка неструктурированных данных «Открытые системы», № 06, 2013
5. Коголовский М.Р. Метаданные, их свойства, функции, классификация и средства представления // Труды 14-й Всероссийской научной конференции «Электронные библиотеки: перспективные методы и технологии, электронные коллекции» — RCDL-2012, Переславль-Залесский, Россия, 15-18 октября 2012 г.
6. Grishman R. Information extraction: Techniques and challenges. // Information Extraction. Springer-Verlag, Lecture Notes in Artificial Intelligence, Rome, 1997.
7. Палагин А. В., Кривой С. Л., Петренко Н. Г. Концептуальные графы и семантические сети в системах обработки естественно-языковой информации // Математические машины и системы. 2009. №3(т.1)
8. Белоусов К.И. Деятельностно-онтологическая концепция формообразования текста [Текст]: дис. докт. филол. наук / К.И. Белоусов. – Оренбург, 2005. – 374.

УДК 004.932

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В ГРАФИЧЕСКОМ КОНТЕНТЕ МОБИЛЬНЫХ УСТРОЙСТВ

Попов Борис Николаевич

Государственный университет морского и речного флота имени адмирала С.О.Макарова,
Россия, Санкт-Петербург, ул. Двинская, 5/7,
email: boris.n.popov@gmail.com

Аннотация: В статье рассматривается программная реализация методов стеганографии в пользовательском программном обеспечении на мобильной платформе.

Ключевые слова: программная реализация; цифровые водяные знаки; стеганография; мобильные устройства; метод Куттера-Джордана-Боссена.

USING DIGITAL WATER MARKS IN THE GRAPHIC CONTENT OF MOBILE DEVICES

Popov Boris

Admiral Makarov State University Of Maritime And Inland Shipping,
Russia, St. Petersburg, Dvinskaya str. 5/7,
email: boris.n.popov@gmail.com

Abstract: The article presents software implementation of steganography methods in user software on a mobile platform.

Keywords: software implementation; digital watermarks; steganography; mobile devices; Kutter-Jordan-Bossen method.

Одно из современных направлений в управлении данными – это использование метаданных как средства хранения, передачи дополнительной информации, сопровождающей исходные данные. В таком контексте можно рассматривать применение методов стеганографии к цифровой обработке изображений. Известны несколько способов применения внедрения цифровых водяных знаков, в которых используется метод изменения наименее значащего бита (метод LSB (Least Significant Bit)) для случая, когда контейнером представлено изображение. Отметим метод Куттера-Джордана-Боссена, в котором манипуляции выполняются с синей составляющей изображения. Для канала синего цвета в модели RGB возможно изменение младших бит, так как известно, что человеческое зрение менее чувствительно к перепадам яркости этой цветовой составляющей в сравнении с красной и зеленой.

В рассматриваемом приложении выполняется добавление заданной пользователем информации методом скрытого внедрения в файл изображения, формируемого мобильным устройством при фотографировании. В приложении также обеспечивается считывание такой информации.

Общий алгоритм реализован для мобильных устройств на платформе Android в среде разработки Android Studio. Функциональная схема работы приложения включает в себя две ветви, развивающиеся после стартового экрана.

Первая ветвь включает создание фотографии, считывание данных с матрицы камеры, преобразование сообщения, встраивание сообщения, сохранение изображения. Вторая ветвь развивается при выборе опции "Считывание" на стартовом экране и включает считывание заданных фрагментов кода, обратное преобразование сообщения и вывод внедренного скрытого сообщения на экран приложения.

Области применения рассмотренной реализации: поддержка авторского права, скрытая аннотация графического контента, обнаружение распространения копий изображения, создание условий для защиты от нелегального копирования графического контента.

СПИСОК ЛИТЕРАТУРЫ

1. Конахович Г.Ф., Пузыренко А.Ю. «Компьютерная стеганография. Теория и практика»
2. Шелухин О.И., Канаев С.Д. Стеганография. Алгоритмы и программная реализация. 2017 г.

УДК 004.91

ОЦЕНКА НАДЕЖНОСТИ СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ СИСТЕМ

Свеженцев Игорь Иванович

Санкт-Петербургский Смольный институт,
Россия, Санкт-Петербург, Полюстровский проспект 59,
email: sii6@rambler.ru.

Аннотация: В статье рассмотрены подходы к оценке надежности проектируемых систем.

Ключевые слова: надежность систем; проектирование; теория систем, сложные системы.

ASSESSMENT OF RELIABILITY OF SOCIO-ECONOMIC SYSTEMS

Svezhentsev Igor Ivanovich
St. Petersburg Smolny Institute,
Russia, St. Petersburg, Polyustrovsky Avenue, 59,
email: sii6@rambler.ru.

Abstract: The approaches to the reliability assessment of the systems being designed are considered in the article.

Keywords: *reliability of systems; design; theory of systems, complex systems.*

Введение. Решению проблем проектирования сложных социально-экономических систем всегда уделялось пристальное внимание специалистов. По мере накопления опыта изменялись представления о системах и о путях и методах их проектирования.

Разработка принципиально нового подхода к решению проектных задач приводит к необходимости оценить уровень развития и методологический потенциал теории надежности, а также проблемы, находящиеся на стыке теории надежности, теории массового обслуживания и инженерной психологии.

Попытки дать обобщенное, целостное описание системы «человек - машина» зачастую связано с чрезвычайным упрощением, когда человек рассматривается как одно из звеньев системы. Требования проектировщиков, обращенные к психологам, сводятся к определению набора характеристик, которые следует приписать «человеческому компоненту». Традиционно указанные характеристики этого «компонента» описываются в иных понятиях (внимание, понимание задачи и др.), нежели машинного компонента. А в отношении человека в принципе нельзя построить модель, адекватную модели технического устройства; единственной истинной характеристикой человека является его изменчивость.

Разрешение этой проблемы на сегодняшний день производится на основе следующего постулата. Поскольку в теории надежности единственными понятиями, описывающими функционирование системы, являются «выполнение» или «отказ», то роль человека должна быть записана только с помощью этих двоичных символов. При таком подходе, после проектирования на плоскость технического описания, от психологии остаются только конечные результаты:

- форма деятельности пользователя;
- операции, на которые разбивается деятельность;
- их взаимосвязь;
- внешние параметры выполнения операций (точность, время);
- параметры внутреннего состояния оператора и их влияние на внешние параметры (эмоциональное состояние, направленность).

Эти результаты объединяются с характеристиками технических устройств в общем цикле функционирования системы.

Таким образом, проектировщик системы получает возможность выбрать оптимальную последовательность операций, оценить потребную численность персонала для получения необходимых показателей функционирования систем, решить вопрос о номенклатуре специалистов.

Возвращение на определенном этапе развития научной теории к анализу ее основ вполне закономерно, если эта теория оправдывает себя в области практических приложений. Это относится к теории надежности. Вводившиеся при решении некоторых прикладных задач функционалы надежности, оказывались либо недостаточно универсальными, либо имели эвристический характер, что, безусловно, отражает трудности формализации их оценок.

Строгое формулирование принципа надежности как одного из фундаментальных вариационных принципов проектирования, установление условий его единственности, позволит ввести в практику проектирования сложных систем критерий надежности, провести классификацию систем по надежности, обеспечить математический синтез оптимальных характеристик.

Конечной целью такой работы должна стать возможность решения широкого класса задач синтеза социально экономических систем ограниченной сложности на основе критерия обобщенной надежности, исследование задач синтеза характеристик надежных систем.

Важность и актуальность задач совершенствования теории надежности обусловлена тем, что указанный аспект – это неотъемлемая характеристика проектируемой системы. Любая корректная задача синтеза системы должна опираться на понятие системы данного уровня надежности.

Важное значение имеет также применение понятия надежности и к самому процессу проектирования (в виде надежности проектирования) и его автоматизации, так как оно непосредственно влияет на экономию времени и трудозатрат при создании систем, а также к формированию живучести и других существенных эксплуатационных характеристик систем.

Основные идеи математической теории систем связаны с понятиями состояния, управления, оптимизации и реализации.

Однако представляется необходимым присоединить к ним также понятие надежности социально-экономических систем, которое не только сочетает в себе различные грани указанных фундаментальных понятий, но и служит переходным мостом от теории к практике.

Заключение. Следовательно, решение основных проектных задач может быть основано на обеспечении глубокой взаимосвязи теории надежности с концепцией проектирования. В этом случае появляется возможность трактовать систему проектирования, как систему управления движением в среде, роль которой играет целевое пространство проектирования. Подобная динамическая концепция предполагает, что теория надежности уже потенциально содержит в себе концепцию проектирования.

СПИСОК ЛИТЕРАТУРЫ

1. Каталевский Д.Ю. Основы имитационного моделирования и системного анализа в управлении: Учебное пособие. — М.: Издательство Московского университета, 2011. — 304 с., ил.
2. Карпов Ю.Г. Имитационное моделирование систем. Введение в моделирование с Anylogic 5. - БХВ, Санкт-Петербург, 2006. - 400с.

УДК 004.056:007.51

ЗАЩИТА ОТ АТАК МЕТОДАМИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Солодяников Александр Владимирович¹, Сухостат Валентина Васильевна²,
Антонова Любовь Сергеевна³

^{1,3} ООО «Ассоциация специалистов по безопасности»,
Россия, 194100, Санкт-Петербург, ул. Кантемировская, 7

² Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, 197101, Санкт-Петербург, Кронверкский проспект, 49,
emails: info@spbissa.ru, sukhostat@mail.ru, antonova.ls@mail.ru

Аннотация: Специфичность целенаправленных атак на оператора методами социальной инженерии требует усиленного внимания к обеспечению информационной безопасности (ИБ) современной организации. В статье рассмотрены методы защиты от нетехнических угроз для ИБ и развития компетентности сотрудников противостоять опасностям социальной инженерии.

Ключевые слова: социальная инженерия, информационная безопасность, тестирование на проникновение, обучение сотрудников.

PROTECTION FROM ATTACKS BY METHODS OF SOCIAL ENGINEERING

Solodyannikov Alexander¹, Sukhostat Valentina², Antonova Liubov³

^{1,3} "Association of security professionals" LLC,
Russia, 194100, St. Petersburg, Kantemirovskaya st., 7,

² Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics
Russia, 197101, St. Petersburg, Kronverkskiy pr., 49,
emails: info@spbissa.ru, sukhostat@mail.ru, antonova.ls@mail.ru

Abstract: Specificity of purposeful attacks on the operator by methods of social engineering requires increased attention to the information security (IS) of a modern organization. The methods of protection from non-technical threats for IS and development of competence of employee to resist the dangers of social engineering are considered in the article.

Keywords: social engineering, information security, penetration testing, employee training.

Введение. Потенциальной угрозой ИБ современной организации может быть проявление человеческого фактора. Поэтому важно своевременно усилить политику безопасности компании, учитывающую защиту от нападений, использующих технологии социальной инженерии. Далее описываются общие стратегии ослабления и нейтрализации методов несанкционированного доступа к информационной инфраструктуре предприятия на основе слабостей человеческого фактора.

Меры физической безопасности. Разработанные и внедренные четкие и сжатые политики безопасности требуют периодической проверки, чтобы определить состояние информирования о безопасности среди сотрудников с целью выявления и устранения потенциальных недостатков. Так, постоянное напоминание сотрудникам о реализации реальной угрозы в любое время наряду с всеобъемлющим охватом систем видеонаблюдения в сочетании с четко определенным периметром контролируемой зоны обуславливает обеспечение физической безопасности, закрывает доступ злоумышленников к ценным ресурсам компании.

Применение программных средств. В борьбе с социальной инженерией значимость приобретает и разветвление ряда защитных программных средств. При этом следует учитывать, что использование программных средств, с одной стороны, может быть эффективным в борьбе с некоторыми типами атак методами социальной инженерии, с другой, – может оказаться совершенно бесполезным при других видах атак.

Специальные меры по предотвращению нападений, использующих технологии социальной инженерии. Другие специальные меры могут оказаться очень эффективной стратегией предотвращения атак методами социальной инженерии. Подобные меры включают активный мониторинг, агрессивную аутентификацию и учет пользователей, использование целевых алгоритмов машинного обучения и анализа. Так после проверки системы, допустимо ее самообучение на способность различать законные и незаконные действия пользователя, несоответствие данных. Эффективность систем машинного и поведенческого обучения способствует обнаружению и предотвращению сложных атак методами социальной инженерии. Пример: целевой фишинг.

Таким образом, механизмы внутренней безопасности, а также другие решения безопасности могут служить мощным щитом защиты предприятий от атак методами социальной инженерии.

Постоянно меняющаяся динамика в современном ИТ-мире и разнообразный характер потенциальных угроз требует информирования о них и обучения управленческого и технического штата компаний, включая ведущих менеджеров и правление компании, технический и сервисный персонал, службу поддержки, службу безопасности, бизнес-менеджеров о текущих правилах и процедурах безопасности. Так как политика безопасности содержит процедуры и рекомендации, которые диктуют методы защиты данных и активов организации, то политики также должны быть защищены от несанкционированного доступа, который может помочь злоумышленникам получить представление о внутренней работе компании.

Применение компаний достаточных мер безопасности и уверенность в защите от нападения предопределяют поиск другого мнения об уровне обеспечения информационной безопасности своей организации. Для этого проводится тестирование на проникновение. Основная цель данного мероприятия заключается в установлении технических уязвимостей и слабых мест в сети, системах и приложениях. Значимым становится и тот факт, что многие фирмы наряду с тестированием на проникновение, определяют перспективы безопасности и предприимчивых сотрудников.

Наиболее эффективной стратегией смягчения последствий в сфере социальной инженерии является образование. С периодическим и систематическим обучением по вопросам безопасности и частым напоминанием о необходимости оставаться начеку и проявлять бдительность в отношении подозрительного поведения компании могут эффективно превратить свое слабое звено в сильное.

Формы организации и методы повышения квалификации и информирования сотрудников о разнообразных потенциальных угрозах ИБ организации.

Обучение на месте. Такая форма организации обучения заключается в создании условий для внутри корпоративного обучения, в подготовке кого-либо из сотрудников (или в приглашении внешнего тренера), который сможет проводить регулярное обучение навыкам безопасности для персонала компании.

Инtranет. Инtranет организации может быть применим в реализации программ повышения квалификации и информирования сотрудников по учебному пособию, размещенном в интрасети.

Скринсейверы. Заставки могут играть большую роль в повышении информирования о безопасности среди сотрудников, могут использоваться для отображения коротких напоминаний о сохранении пароля в безопасности, запрете на выезд, сообщении о подозрительном поведении соответствующим отделам и т.д.

Онлайн-курсы. Работодатели могут использовать один из многих онлайн-провайдеров для обучения безопасности. Доступные образовательные ресурсы интернета способствуют развитию знаний сотрудников о рисках, связанных с социальной инженерией.

Таким образом, наличие разнообразных методов обучения обуславливает повышение информирования о разнообразном характере потенциальных угроз социальной инженерии для ИБ предприятия. Следствием является адекватное осознание сотрудниками рисков, создаваемых атакующими. При этом работодатель автоматически получает преимущество в этой битве; у бизнеса меньше шансов пострадать от нападения из-за того, что их обученный персонал проявляет должную осмотрительность, чтобы защитить компанию.

Заключение. Многоуровневая программа защиты от разнообразного характера потенциальных угроз социальной инженерии для ИБ организации может быть эффективной в силу компетентности сотрудников понимать и признавать общие методы эксплуатации, используемые социальными инженерами. Поэтому современные организации должны тратить свое время и силы, чтобы убедиться, что их сотрудники защищены от нападений, использующих технологии социальной инженерии, предпринимая превентивные меры.

СПИСОК ЛИТЕРАТУРЫ

1. Гатчин Ю.А. Методика оценки защищенности оператора информационных систем в условиях деструктивных информационных воздействий / Ю.А. Гатчин, В.И. Поляков, В.В. Сухостат, Н.В. Малков // Вестник компьютерных и информационных технологий. 2015. №2 (128). С. 54-59.
2. Митник К. Искусство вторжения: Пер. с англ. — Семенова А.В. — М.: Компания АйТи, ДМК Пресс, 2005. — 280 стр.
3. Салем М., Хаммуде М. Defense Methods Against Social Engineering Attacks [Электронный ресурс] URL: https://www.researchgate.net/publication/319097404_Defense_Methods_Against_Social_Engineering_Attacks (дата обращения 19.09.2017)

УДК 006.015.2

**ОСОБЕННОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
В ПРОЦЕССЕ ФУНКЦИОНИРОВАНИЯ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ**

Солодянников Александр Владимирович,
ООО «Ассоциация специалистов по безопасности»
Россия, Санкт-Петербург, ул. Кантемировская, д.7, лит. А
emails: info@spbissa.ru

Аннотация: В статье рассмотрены вопросы актуальности обработки персональных данных сотрудников и клиентов предприятия при осуществлении его деятельности.

Ключевые слова: *персональные данные, обработка, сотрудник, трудовой договор.*

**SPECIAL ASPECTS OF PROCESSING PERSONAL DATA IN THE PROCESS OF FUNCTIONING OF
INDUSRTIAL COMPANY**

Solodyannikov Alexander
"Association of security professionals" LLC,
Russia, 194100, St. Petersburg, Kantemirovskaya st., 7,
e-mails: info@spbissa.ru

Annotation: *The questions of actuality of processing personal data of employees and clients of the enterprise at realization of its activity are considered in the article.*

Keywords: *personal data, processing, employee, labor contract.*

Каждое предприятие, и в особенности крупные, собирает и обрабатывает большой объем персональных данных своих сотрудников. В эти данные входит информация, разглашение которой может принести вред субъекту ПДн: это и место проживания, зарплата, режим работы, семейное положение, сведения о детях и т.п. Кроме того, часть этих данных не только обрабатывается внутри предприятия, но и передается в различные государственные структуры. Часто сотрудники предприятия занимаются покупкой билетов и бронированием гостиниц для командировочных. Иногда оформлением виз. А это тоже передача данных. Есть еще один «тонкий момент» - пропуск на территорию посетителей. Особо режимные предприятия не только собирают ФИО, но требуют копию паспорта, телефон, место работы и много другое.

В связи с этим, вопросы обработки ПДн(во всем понимании значения этого термина в соответствии с 152ФЗ) являются актуальными для практически каждой организации.

1. Статус предприятия как «оператора обработки персональных данных».

1.1. Предприятие, обрабатывающее персональные данные только своих сотрудников, является «оператором».

В ряде случаев оператор вправе осуществлять обработку персональных данных без уведомления уполномоченного органа. Это ситуация при обработке персональных данных:

1) обрабатываемых в соответствии с трудовым законодательством;

(п. 1 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

(см. текст в предыдущей редакции)

2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных;

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

4) сделанных субъектом персональных данных общедоступными;

(п. 4 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;

9) обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

(п. 9 введен Федеральным законом от 25.07.2011 N 261-ФЗ).

1.2 Требования к отделу кадров (ОК).

1.2.1 В ОК должны быть следующие документы.

а) документация по организации работы отдела кадров содержит организационно-правовую документацию и включает:

- положение об отделе;
- должностные инструкции работников отдела;
- приказы, распоряжения, указания руководства предприятия, регламентирующие структуру отдела и распределение сфер ответственности между его работниками;
- рабочие инструкции по выполнению основных функций отдела, ведению документации и формированию персональных данных в комплексы (документы, базы данных и т.п.). Сюда относятся также дела с документацией по планированию, учету, анализу и отчетности в части основной деятельности отдела.

б) документация, образующаяся в процессе основной деятельности отдела и содержащая персональные данные в единичном или сводном виде:

- комплексы документов, сопровождающие процесс оформления трудовых правоотношений гражданина (при решении вопросов о приеме на работу, переводе, увольнении и т.п.);
- комплексы материалов по анкетированию, тестированию, проведению собеседований с кандидатами на должность;

- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- дела, содержащие основания к приказам по личному составу;
- дела, содержащие материалы аттестации сотрудников, служебных расследований и т.п.;
- справочно-информационный банк данных по персоналу — учетно-справочный аппарат (картотеки, журналы, базы данных и др.);

— подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству предприятия, руководителям структурных подразделений и служб;

— копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения) документация, образующаяся в процессе основной деятельности отдела и содержащая персональные данные в единичном или сводном виде:

- комплексы документов, сопровождающие процесс оформления трудовых правоотношений гражданина (при решении вопросов о приеме на работу, переводе, увольнении и т.п.);
- комплексы материалов по анкетированию, тестированию, проведению собеседований с кандидатами на должность;

- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- дела, содержащие основания к приказам по личному составу;
- дела, содержащие материалы аттестации сотрудников, служебных расследований и т.п.;
- справочно-информационный банк данных по персоналу — учетно-справочный аппарат (картотеки, журналы, базы данных и др.);

— подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству предприятия, руководителям структурных подразделений и служб;

— копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения.

1.2.2. При работе с документами, делами и базами данных отдела кадров должны соблюдаться следующие основополагающие принципы защиты персональных данных:

- личной ответственности работников за сохранность и конфиденциальность сведений о работе отдела и персональных данных, а также носителей этой информации;

- разбиения знания персональных данных между разными работниками отдела;

- наличия четкой разрешительной системы доступа работников отдела к документам, делам и базам данных;

- проведения регулярных проверок наличия традиционных и электронных документов, дел и баз данных у работников отдела и кадровых документов в подразделениях предприятия.

Главным моментом в защите персональных данных является четкая регламентация функций работников отдела кадров и в соответствии с этим регламентация принадлежности работникам документов, дел, картотек, журналов персонального учета и баз данных. Для реализации этого положения руководителем предприятия должен быть издан приказ или распоряжение о закреплении за работниками отдела определенных массивов документов, необходимых им для информационного обеспечения функций, указанных в должностных инструкциях этих работников, утверждена схема доступа работников отдела кадров и руководящего состава предприятия, структурных подразделений к документам отдела, введена личная ответственность перечисленных должностных лиц и работников за сохранность и конфиденциальность персональных данных.

По каждой функции, выполняемой работником отдела кадров, должен быть регламентирован состав документов, дел и баз данных, с которыми этот работник имеет право работать.

Не допускается, чтобы работник мог знакомиться с любыми документами и материалами отдела. Целесообразно, в целях разграничения доступа и разбиения знания персональных данных между работниками, закрепить за разными работниками:

а) документированное оформление трудовых правоотношений (прием, перевод, увольнение и др.),

б) ведение личных дел и трудовых книжек,

в) составление и хранение приказов по личному составу и контрактов,

г) ведение справочно-информационного банка данных.

Распределение сфер деятельности может быть иным в зависимости от объема работы и штатной численности работников отдела, но разграничение обязанностей и массивов документации должно быть осуществлено в обязательном порядке.

2. Особенности обработки данных, хранящихся в личных делах сотрудников.

2.1 Требования по хранению личных дел.

1) Операции по оформлению, формированию, ведению и хранению личных дел выполняются одним работником отдела кадров, который несет личную ответственность за сохранность документов в делах и доступ к делам других работников.

2) Документы для формирования и ведения личных дел сдаются ему под роспись в передаточном журнале работником, отвечающим за процесс документирования трудовых правоотношений граждан с предприятием.

3) Личное дело должно обязательно иметь опись документов, включенных в дело. Листы дела нумеруются в процессе формирования дела.

4) При помещении в личное дело нового документа данные о нем первоначально вносятся в опись дела, затем листы документа нумеруются и только после этого документ подшивается.

5) На оборотной стороне обложки личного дела может указываться список руководителей, которым дело может быть выдано для ознакомления. Здесь же подклеивается конверт для карточки учета (контрольной карточки) выдачи дела.

6) Изменения и дополнения в персональные данные вносятся в дополнение к личному листку по учету кадров и (или) личную учетную карточку формы Т-2 на основании приказов по личному составу и документов, предоставляемых сотрудниками (свидетельства о браке, диплома и т.д.). Устное заявление сотрудника не является основанием для внесения указанных изменений (кроме второстепенных сведений — изменения номера домашнего телефона, места работы близких родственников и т.п.). Все новые записи в дополнении к личному листку по учету кадров и учетных формах заверяются росписью работников отдела кадров. При переносе сведений из приказа по личному составу работник расписывается против перенесенного пункта.

7) В случае изъятия из личного дела документа в описи дела производится запись с указанием основания для подобного действия и нового местонахождения документа. С документа, подлежащего изъятию, снимается копия, которая подшивается на место изъятых документов. Отметка в описи и копия заверяются росписью работника отдела кадров. Замена документов в личном деле кем бы то ни было запрещается. Новые, исправленные документы помещаются вместе с ранее подшитыми.

8) Приказом руководителя предприятия должен быть установлен порядок выдачи или ознакомления руководящего состава с личными делами сотрудников.

9) Личные дела могут выдаваться на рабочие места только руководителю, его заместителю по кадрам или персоналу и начальника отдела (управления) кадров. Дела выдаются под роспись в контрольной карточке.

10) При возврате дела тщательно проверяется сохранность документов, отсутствие повреждений, включения в дело других документов или подмены документов.

11) Передача личных дел руководителям через их секретарей или референтов не допускается. Другие должностные лица предприятия могут знакомиться с личными делами подчиненных им сотрудников. Ознакомление с делами осуществляется в помещении отдела кадров под наблюдением работника, ответственного за сохранность и ведение личных дел. Факт ознакомления фиксируется в контрольной карточке личного дела.

12) Сотрудник предприятия имеет право знакомиться только со своим личным делом и трудовой книжкой, учетными карточками, отражающими его персональные данные. Факт ознакомления с личным делом также фиксируется в контрольной карточке.

2.2 Требования, выполняемые при организации работ:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных настоящим Кодексом или иными федеральными законами;

- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном настоящим Кодексом и иными федеральными законами;

- осуществлять передачу персональных данных работника в пределах одной организации, у одного индивидуального предпринимателя в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись;

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- передавать персональные данные работника представителям работников в порядке, установленном настоящим Кодексом и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

3 Особенности обработки ПДн в системах контроля доступа (СКУД).

3.1. Если в составе СКУД используются средства автоматизации (АРМ, ЭВМ), то подлежат защите в соответствии с требованиями ФЗ 152 и подзаконных актов.

3.2 Особенности обработки биометрических данных.

1) Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные), могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2) Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, законодательством Российской Федерации об оперативно-розыскной деятельности, законодательством Российской Федерации о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию (в ред. Федерального закона от 25.11.2009 N 266-ФЗ).

В число основных физиологических особенностей человека, влияющих на возможность идентификации его личности, входят: отпечатки пальцев, отпечатки ладони, результаты анализа ДНК, образ лица, сетчатка глаза, особенности строения тела, отдельных органов и тканей, работа желез внутренней секреции, различные отклонения в развитии, атаксии, психическое состояние здоровья и т.п.

3.3 Передача ПДн третьим лицам.

При привлечении третьих лиц к ПДн своих сотрудников в договоре с третьим лицом необходимо прописывать ответственность за обеспечение защиты. А в соглашении сотрудника необходимо конкретно прописывать, каким третьим лицам он (сотрудник) разрешат передавать.

При использовании удаленного доступа канал передачи должен защищаться.

3.4 Сбор у посетителей полных ПДн не является необходимостью, влияющей на функционирование предприятия. Закон не предусматривает обязательный сбор ПДн. Поэтому предприятие, осуществляющее сбор ПДн, обязано получать согласие у посетителей на их обработку.

При обработке ПДн в СКУД с применением средств автоматизации предприятие становится «оператором» обработки ПДн. Соответственно обязано реализовывать требования по защите. Но при этом не обязано уведомлять контролирующий орган.

Согласие сотрудника на обработку ПДн требуется при приеме на работу, даже если предприятие не является «оператором». Согласие подписывается в двух экземплярах при подписании трудового договора. Один экземпляр храниться в личном деле.

3.5 При передаче ПДн третьим лицам предприятие становится «оператором» обработки ПДн. Но при этом не обязано уведомлять контролирующий орган. Сотрудники, задействованные в обработке ПДн (хранении, передаче), должны пройти инструктаж по правилам обеспечения защиты ПДн. А работодатель – организовать данный инструктаж. Пользоваться личной почтой для передачи ПДн другого сотрудника можно только с его письменного разрешения.

Средства защиты ПДн (СрЗИ) выбираются в процессе реализации мероприятий по защите. Существует реестр сертифицированных ФСТЭК СрЗИ, размещенный на сайте ФСТЭК России (fstec.ru). На оборудование и ПО никаких дополнительных требований не накладывается. При обработке ПДн должны быть реализованы мероприятия, включающие в себя разработку документации, внедрение технических и программных средств, контроль эффективности.

СПИСОК ЛИТЕРАТУРЫ

1. Гатчин Ю.А. Методика оценки защищенности оператора информационных систем в условиях деструктивных информационных воздействий / Ю.А. Гатчин, В.И. Поляков, В.В. Сухостат, Н.В. Малков // Вестник компьютерных и информационных технологий. 2015. №2 (128). С. 54-59.

УДК 004.413

ФАКТОРЫ НАСЛЕДОВАНИЯ И ПРОАКТИВНОСТИ В ЖИЗНЕННОМ ЦИКЛЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Соколов Борис Владимирович¹, Мустафин Николай Габдрахманович², Миллер Владимир Евгеньевич³, Савосин Сергей Валентинович²

¹ Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Россия, Санкт-Петербург, 14 линия, 39,

² Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», Россия, Санкт-Петербург, ул. Профессора Попова, 5,

³ СПб филиал ОАО РТИ им. акад. А.Л. Минца, Россия, Санкт-Петербург, Лиговский пр., 254, emails: sokolov_boris@inbox.ru, Nikolay.mustafin@gmail.com

Аннотация: Рассмотрены вопросы развития информационных систем с учетом наследования – использования накопленных знаний и данных об объекте информатизации, процессах принятия решений и опыте использования предыдущих версий систем, проактивности – предвидения изменений внешних и внутренних условий в жизненном цикле информационной системы.

Ключевые слова: наследование, информационная система, унаследованная система, функциональность, аппаратно-программная платформа, проактивность

THE FACTORS OF INHERITANCE AND PROACTIVITY IN THE LIFE CYCLE OF THE INFORMATION SYSTEM

Sokolov Boris Vladimirovich¹, Mustafin Nikolay Gabdrakhmanovich², Miller Vladimir Evgenjevich³, Savosin Sergey Valentinovich²

¹ Saint-Petersburg Institute for Informatics and automation of Russian Academy of Sciences, Russia, St. Petersburg, 14th Line, 39,

² Saint Petersburg Electrotechnical University "LETI", Russia, St. Petersburg, Prof. Popov str., 5,

³ SPb branch of OJSC RTI named after acad. A.L. Mints, Russia, St. Petersburg, Ligovsky pr., 254, emails: sokolov_boris@inbox.ru, Nikolay.mustafin@gmail.com

Abstract: The problems of the development of information systems taking into account inheritance are considered, including the use of accumulated knowledge and data about the object of informatization, decision-making processes and experience in using previous versions of systems, proactivity-foreseeing changes in external and internal conditions in the life cycle of the information system.

Keywords: inheritance, information system, inherited system, functionality, hardware-software platform, proactive

Развитие информационных систем (ИС) различного назначения обуславливается, с одной стороны, постоянным развитием требований пользователей, а, с другой стороны, развитием информационных технологий, включая аппаратно-программные средства, сетевые структуры, диалоговые средства, модели, методы и инструмента систем поддержки принятия решений.

При рассмотрении вопросов развития ИС различного масштаба возникает насущная необходимость использовать всю информацию об объекте информатизации настолько полно, насколько это возможно. В этой связи развитие ИС осуществляется на основе имеющихся знаний об объекте информатизации, процессах принятия решений и опыте использования предыдущих версий ИС, т. е. наследовании накопленных знаний, опыта используемых решений.

К основным факторам развития ИС можно отнести: нарастающую сложность поддержки ИС для обеспечения дополнительной функциональности; увеличение объемов обрабатываемых данных и (или) увеличение числа рабочих мест и, как следствие, недостаточная производительность отдельных элементов системы или системы в целом; неспособность системы обеспечить новые требуемые возможности; проблемы, возникающие при интеграции с другими ИС в рамках единого информационного пространства; появление новых технологий обработки данных (развитие аппаратных и программных средств, новые методологии); моральное устаревание ИС.

С другой стороны, развитие ИС в условиях непрерывных изменений внешних и внутренних факторов – расширение функциональностей, увеличение объемов обрабатываемых данных, развитие аппаратно-программных платформ и т.д., требует проактивности в процессе разработки и сопровождения ИС, т. е. предвидение изменений внешних и внутренних факторов, обеспечивающее экономию затрат на развитие ИС в ее жизненном цикле.

СПИСОК ЛИТЕРАТУРЫ

1. Мустафин Н.Г., Савосин С.В., Подсытник Д.А Унаследованная система в качестве стартовой площадки // Программные продукты и системы. 2004. №3 С.12–16.
2. Охтилев М. Ю., Мустафин Н. Г., Миллер В. Е., Соколов Б. В. Концепция проактивного управления сложными объектами: теоретические и технологические основы // Известия вузов. Приборостроение. 2014. Том 57. №11. С.7–14.

УДК 004.042

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СЕТИ ИНТЕРНЕТА ВЕЩЕЙ СРЕДСТВАМИ НИЗКОРЕСУРСНОЙ КРИПТОГРАФИИ

Супрун Александр Федорович, Царьков Игорь Сергеевич
Санкт-Петербургский политехнический университет Петра Великого
Россия, Санкт-Петербург, Политехническая ул., 29
emails: afs54@inbox.ru, sator_nr@mail.ru.

Аннотация: В статье рассмотрен безопасный протокол взаимодействия между узлами Интернета вещей.

Ключевые слова: Интернет Вещей; взаимодействие; протокол.

THE NETWORK SECURITY OF THE INTERNET OF THINGS MEANS OF LOW-RESOURCE CRYPTOGRAPHY

Suprun Aleksandr, Tsarkov Igor
Peter the Great St.Petersburg Polytechnic University "SPbPU"
Russia, St. Petersburg, Polytechnicheskaya str, 29
emails: afs54@inbox.ru, sator_nr@mail.ru.

Abstract: In article the safe protocol of interaction between nodes of the Internet of things is considered.

Keywords: Internet of Things; interaction; protocol

Введение. IoT (internet of Things, далее – Интернет вещей) представляет собой распределенную мультиагентную сеть, осуществляющую автономный сбор и обработку данных об окружающей среде. Интернет Вещей имеет представление как в реальном, так и в виртуальном пространстве.

В последнее десятилетие наблюдается лавинообразный рост числа агентов ИВ: на февраль 2017 года числа упомянутых агентов составило порядка 10 миллиардов устройств. По прогнозам экспертов, к 2020 году количество агентов ИВ по всему миру может достигнуть 50 миллиардов устройств, а по самым оптимистичным прогнозам развития отрасли – 80 миллиардов. Подобный массив устройств, несмотря на малую среднюю мощность, нельзя оставлять беззащитным: примером последствий пренебрежения безопасностью ИВ являются нашумевшие в СМИ атаки ботнетов BrickerBot, Amnesia и Mirai, объединившие под собой сотни тысяч устройств, которые в последствии были использованы для проведения массированных DDOS атак.

Взаимодействие между узлами Интернета Вещей отличаются требованиями низкой нагрузки на узлы сети, малого объема пересылаемых данных и ограничениями энергопотребления узлов. В рамках исследования создан протокол, отвечающий данным требованиям, предоставляющий возможность построения защищенных каналов общения между узлами сети Интернета вещей.

Заключение. В результате проведенного исследования был разработан протокол, позволяющий устанавливать соединения и обмениваться данными внутри защищенного канала между узлами сети ИВ. Разработанный протокол обладает следующими преимуществами:

- возможность однозначно идентифицировать устройство;
- многоуровневое подтверждение валидности сообщения;
- простота реализации;
- низкие требования к вычислительной мощности компонентов сети;
- низкие требования к пропускной способности канала сети.

СПИСОК ЛИТЕРАТУРЫ

1. Hannes Gross, Marko Holbl, Daniel Slamanig, and Raphael Spreitzer Privacy-Aware Authentication in the Internet of Things. [Электронный ресурс] / IACR Cryptology ePrint Archive. 2015. – Режим доступа: <https://eprint.iacr.org/2015/1110.pdf> свободный (дата обращения: 21.05.2017). – Загл. с экрана. – Яз. англ.
2. Hannes Gross, Marko Holbl, Daniel Slamanig, and Raphael Spreitzer Privacy-Aware Authentication in the Internet of Things. [Электронный ресурс] / IACR Cryptology ePrint Archive. 2015. – Режим доступа: <https://eprint.iacr.org/2015/1110.pdf> свободный (дата обращения: 21.05.2017). – Загл. с экрана. – Яз. англ.
3. Elias Yarrkov Cryptanalysis of XXTEA. [Электронный ресурс] / IACR Cryptology ePrint Archive. 2010. – Режим доступа: <https://eprint.iacr.org/2010/254.pdf>, свободный (дата обращения: 21.05.2017). – Загл. с экрана. – Яз. англ.
4. Zheng Gong, Svetla Nikova, and Yee Wei Law KLEIN: A New Family of Lightweight Block Ciphers. [Электронный ресурс] / School of Computer Science, South China Normal University, China, Faculty of EWI, University of Twente, The Netherlands, Dept. ESAT/SCD-COSIC, Katholieke Universiteit Leuven, Belgium, Department of EEE, The University of Melbourne, Australia. 2012. – Режим доступа: <http://www.smartsantander.eu/downloads/Presentations/gong12klein.pdf>, свободный (дата обращения: 29.05.2017). – Загл. с экрана. – Яз. англ.
5. Wenling Wu and Lei Zhang LBlock: A Lightweight Block Cipher. [Электронный ресурс] / IACR Cryptology ePrint Archive. 2011. – Режим доступа: <https://eprint.iacr.org/2011/345.pdf>, свободный (дата обращения: 29.05.2017). – Загл. с экрана. – Яз. англ.
6. HIGHT Algorithm Specification. [Электронный ресурс] / Korea Internet & Security Agency. 2009. – Режим доступа: <https://seed.kisa.or.kr/html/egovframework/iwt/ds/ko/ref/01.+HIGHT+Algorithm+Specification.pdf>, свободный (дата обращения: 29.05.2017). – Загл. с экрана. – Яз. англ.
7. Christophe De Canniere and Orr Dunkelman, Miroslav Knezevic KATAN & KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers. [Электронный ресурс] / Katholieke Universiteit Leuven, Department of Electrical Engineering ESAT/SCD-COSIC and Interdisciplinary Center for Broad Band Technologies Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium, Ecole Normale Supérieure D'epartement d'Informatique. 2010. – Режим доступа: <https://pdfs.semanticscholar.org/2686/044f8a972325e1b23824430dea731d8e2817.pdf>, свободный (дата обращения: 1.06.2017). – Загл. с экрана. – Яз. англ.
8. Ari Keränen, Carsten Bormann Интернет вещей: Стандарты и рекомендации. [Электронный ресурс] / Информационный сборник «Интернет изнутри». 2017 – Режим доступа: <http://internetinside.ru/internet-veshhey-standarty-i-rekomenda>, свободный (дата обращения: 5.06.2017). – Загл. с экрана. – Яз. рус.

УДК 004.042

ПРОТОКОЛ ВЗАИМОДЕЙСТВИЯ ВНУТРИ СЕТИ ИНТЕРНЕТА ВЕЩЕЙ

Супрун Александр Федорович, Царьков Игорь Сергеевич
 Санкт-Петербургский политехнический университет Петра Великого
 Институт компьютерных наук и технологий
 Россия, Санкт-Петербург, Политехническая ул., д. 29

Аннотация: В статье рассмотрен предлагаемый в рамках научной работы безопасный протокол взаимодействия между узлами Интернета вещей.

Ключевые слова: Интернет Вещей; взаимодействие; протокол.

THE COMMUNICATION PROTOCOL WITHIN THE NETWORK OF THE INTERNET OF THINGS

Suprun Aleksandr, Tsarkov Igor
 Peter the Great St.Petersburg Polytechnic University "SPbPU"
 Russia, St. Petersburg, Polytechnicheskaya str, 29
 Emails: afs54@inbox.ru, sator_nr@mail.ru.

Abstract: In the article proposed in the framework of scientific work secure communication Protocol between the nodes of the Internet of things.

Keywords: Internet of Things; interaction; protocol

Введение. IoT (internet of Things, далее – Интернет вещей) представляет собой распределенную мультиагентную сеть, осуществляющую автономный сбор и обработку данных об окружающей среде. Интернет Вещей имеет представление как в реальном, так и в виртуальном пространстве.

В последнее десятилетие наблюдается лавинообразный рост числа агентов ИВ: на февраль 2017 года числа упомянутых агентов составило порядка 10 миллиардов устройств. По прогнозам экспертов, к 2020 году количество агентов ИВ по всему миру может достигнуть 50 миллиардов устройств, а по самым оптимистичным прогнозам развития отрасли – 80 миллиардов. Подобный массив устройств, несмотря на малую среднюю мощность, нельзя оставлять беззащитным: примером последствий пренебрежения безопасностью ИВ являются нашедшие в СМИ атаки ботнетов BrickerBot, Amnesia и Mirai, объединившие под собой сотни тысяч устройств, которые в последствии были использованы для проведения масштабированных DDOS атак.

Взаимодействие между узлами Интернета Вещей отличается требованиями низкой нагрузки на узлы сети, малого объема пересылаемых данных и ограничениями энергопотребления узлов. В рамках данной работы создан протокол, отвечающий данным требованиям, предоставляющий возможность построения защищенных каналов общения между узлами сети Интернета вещей.

Заключение. На фоне возрастающей вредоносной активности в сети Интернет, необходимо уделить максимальное внимание проблемам безопасности узлов Интернета Вещей, представляющих из себя идеальную базовую площадку для разворачивания вредоносной активности.

СПИСОК ЛИТЕРАТУРЫ

1. Ari Keränen, Carsten Bormann Интернет вещей: Стандарты и рекомендации. [Электронный ресурс] / Информационный сборник «Интернет изнутри». 2017 – Режим доступа: <http://internetinside.ru/internet-veshhey-standarty-i-rekomenda>, свободный (дата обращения: 5.06.2017). – Загл. с экрана. – Яз. рус.

УДК 371.39

ВЫЧИСЛЯЕМЫЙ ВОПРОС КАК ПЕДАГОГИЧЕСКАЯ ТЕХНОЛОГИЯ В ЭЛЕКТРОННОМ ОБУЧЕНИИ

Титова Юлияна Францевна

Смольный институт Российской академии образования

Россия, Санкт-Петербург, Полюстровский пр., 59

email: titova-stud@yandex.ru

Аннотация: В докладе рассмотрен тип вопроса «вычисляемый», представленный в современных LMS, включая, Moodle. Отмечено, что такой тип вопроса в настоящее время мало используется при организации электронного обучения, однако он имеет большие перспективы в обучении естественнонаучным, техническим и экономическим дисциплинам. Позволяет обеспечить индивидуализации при контрольном тестировании. Однако главное применение таких вопросов - это организация электронных практикумов по решению типовых задач. Продемонстрированы примеры вычисляемых вопросов и учебных электронных практикумов.

Ключевые слова: LMS-система; Moodle; методика; электронное обучение; тестовый вопрос; вычисляемый вопрос; компьютерный тест, электронный практикум.

CALCULATED THE QUESTION OF HOW EDUCATIONAL TECHNOLOGY IN E-LEARNING

Titova Yuliayna Frantsevna

Smolny Institute of the Russian Academy of education

Department of information systems, head of department, Associate Professor

Russia, Sankt-Peterburg, Polyustrovskiy PR., d. 59

email: titova-stud@yandex.ru

Abstract: the report examines the type of question calculated, and presented in a modern LMS, including Moodle. Noted that this type of question is currently little used in e-learning, but it has great potential in the teaching of natural-scientific, technical and economic disciplines. Allows you to provide identification in benchmark testing. However, the main application of such issues is the organization of the electronic workshops on solving typical problems. The examples of calculated questions and instructional workshops is presented.

Keywords: LMS; Moodle; methodology; e-learning; the test question; a numerical question given; computer-based test, electronic workshop.

Данный доклад посвящен использованию вычисляемых вопросов в электронном обучении. Практически все современные LMS, включая, Moodle позволяют создавать такие вопросы, но на настоящий момент это практически неиспользуемая форма тестовых вопросов. По своей сути такой вопрос позволяет организовать решение некой вычислительной задачи, в которой традиционно заданы исходные данные и требуется получить результат с использованием одной или нескольких формул. Вычисляемые задачи используются при обучении экономическим, естественнонаучным, в том числе и компьютерным, дисциплинам. В традиционной вычисляемой задаче формулировка включает описание ситуации, набор известных исходных данных и вопрос, что требуется найти. Задача решается в одно или несколько действий. На каждом этапе вычислений применяется формула, связывающая известные и неизвестные величины. В большинстве случаев набор исходных данных является минимально необходимым, т.е. все исходные данные при решении так или иначе должны быть использованы. В любой дисциплине можно выделить типовые задачи, выстроить их в методической последовательности освоения. И самая большая проблема – это научить студентов видеть в формулировке некой конкретной задачи целую категорию, и применять типовой для этой категории метод. Решить эту проблему можно, в том числе, и многократным решением типовых задач, что не позволяет делать современный процесс обучения [1]. Электронный вычисляемый вопрос позволяет на основе одной формулировки сгенерировать целую категорию типовых задач. Во время тестирования к типовой формулировке добавляется случайный набор исходных данных, что делает конкретную задачу уникальной для каждого тестируемого, чем обеспечивается индивидуализация тестирования и невозможность механического запоминания ответа. Наличие электронных вычисляемых вопросов позволит студенту самостоятельно тренироваться решать задачи в том объеме, пока он уверенно не освоит категории типовых задач. И степень его умений будет зависеть только от его прилежности, способностей и упорства.

Создание вычисляемого вопроса включает описание типовой формулировки задачи, программирование формулы правильного ответа и создание наборов исходных данных. Сама формулировка – это, по сути, обобщенное описание некоторого класса однотипных задач, наборы исходных данных позволяют сформировать множество задач с одинаковыми формулировками и с

разными исходными данными. Для создания наборов данных в LMS-среде предусмотрена технология автоматической генерации чисел в заданном диапазоне с заданной погрешностью, что снижает трудоемкость создания вопросов, что избавляет преподавателя от придумывания наборов данных.

Проблемы использования вычисляемых вопросов заключаются в том, что, во-первых, не понятно, как преподаватели узнают о том, что такая форма вопросов есть, во-вторых, кто их научит создавать такие вопросы, и в-третьих, что технология их создания предполагает, хоть и несложное, но программирование формулы [2]. Администраторы системы во многих вузах ограничиваются чисто администраторскими функциями, а именно создание учетных записей, ведение списка групп, общая настройка системы. В их функции не входит исследование возможностей системы и обучение преподавателей, а также методическое обоснование использования элементов системы в учебном процессе. Именно поэтому при организации системы электронного обучения должен быть предусмотрен методист, решающий именно такие методические задачи. Проблема программирования формул решается тем, что, если в дисциплине есть вычислительные задачи, которые предполагают какой-никакой алгоритм решения, значит, и преподаватель способен освоить несложные элементы программирования. У электронных вычисляемых вопросов есть и более важная функция, чем просто организация решения традиционной вычислительной задачи. Повысить обучающий эффект можно также за счет использования разработки так называемых комплексных задач. В данном контексте под комплексной задачей понимается описание в тестовом вопросе ситуации, по которой можно задать несколько вопросов, использующих для ответа разные формулы. Для такой ситуации задается набор исходных данных, необходимый для ответа на все вопросы. С точки зрения одного конкретного вопроса к ситуации этот набор данных будет избыточным. Такой подход позволяет получить вместо одного вопроса несколько тестовых вопросов с использованием одного и того же набора данных.

В докладе будут продемонстрированы примеры вычисляемых вопросов, электронных практикумов и комплексных ситуаций для разных дисциплин. Как известно, решение задач – это один из основных методов усвоения теории. Зачастую аудиторного учебного времени не хватает, для прорешивания всевозможных вариантов постановки задач. Поэтому использование вычисляемых вопросов позволяет продолжить обучение в режиме самостоятельной работы. По мнению автора, вычисляемые вопросы должны составлять основную часть фонда оценочных средств. Это согласуется с современной концепцией образования, направленной на формирование у студентов бакалавриата прикладных навыков. Поэтому необходимо организовать обучение преподавателей, в первую очередь экономических дисциплин, технологии создания таких вопросов в рамках курсов повышения квалификации [3]. При обучении надо обязательно касаться и технологической и педагогической составляющих, что могли бы сделать в большей степени преподаватели компьютерных технологий, а не системные администраторы.

СПИСОК ЛИТЕРАТУРЫ

1. Барабаш П.А., Воробьев С.П., Курносков В.И., Советов Б.Я. Инфокоммуникационные технологии в Глобальной информационной инфраструктуре – Санкт-Петербург: Наука, 2008, 552 с.
2. Титова Ю.Ф. Задачи и проблемы организации электронного обучения и применения дистанционных образовательных технологий // Академия профессионального образования. - 2015 - №6
3. Титова Ю.Ф. Об особенностях труда педагогических работников при использовании электронного обучения.// IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2017)» / Материалы конференции - СПОИСУ. – СПб, 2016.

УДК 004.04

УГРОЗЫ И МЕРЫ ЗАЩИТЫ ПРИ ИСПОЛЬЗОВАНИИ КОНЦЕПЦИИ BYOD

Усатых Ксения Сергеевна
ООО «Ассоциация специалистов по безопасности»
Россия, Санкт-Петербург, ул. Кантемировская, 7
email: usatykh@icloud.com

Аннотация: В статье рассмотрены основные угрозы и способы защиты при использовании в компании концепции BYOD (Bring You Own Device).

Ключевые слова: информационная безопасность, угрозы, BYOD.

THREATS AND PROTECTION MEASURES OF USING THE BYOD CONCEPT

Usatykh Kseniia
LLC «Association of security professionals»,
Russia, St/Petersburg, Kantemirovskaya st. 7
email: usatykh@icloud.com

Abstract: The article describes the main threats and protection methods for use in the company's concept of BYOD (Bring You Own Device).

Keywords: information security, threats, BYOD.

В условиях роста мобильности бизнеса использование девайсов стало неотъемлемой частью развития компаний. С ростом количества мобильных устройств и доступности им информации возникают угрозы информационной безопасности.

Концепция BYOD – Bring Your Own Device дословно переводится, как принеси свое устройство, получила широкое распространение по всему миру. Согласно исследованию компании Microsoft 78% работодателей позволяет использовать личные девайсы для рабочих целей [2]. Преимущественно использование данной концепции распространено в финансовом секторе, PR и IT компаниях. Концепция BYOD позволяет предприятиям повысить производительность, за счет того, что работник, используя личные мобильные устройства: смартфоны, планшетные компьютеры, ноутбуки, расширяет свои рабочие возможности. Доступ к корпоративным ресурсам компании: почте, внутренним документам, конфиденциальной информации может быть получен в любое удобное время и в любом удобном месте (даже во время отпуска сотрудника), а не только в рабочие часы офиса, что позволяет настроить рабочий процесс максимально продуктивно [1]. Для многих компаний преимущество BYOD заключается не только в повышении производительности, но и в сокращении расходов на закупку, обслуживание технических средств и развертывания специального программного обеспечения.

Однако, не смотря на все преимущества BYOD особое внимание необходимо уделить вопросу защиты информации. Бесконтрольное использование девайсов с открытым доступом к внутренним ресурсам компании вне контролируемой зоны влечет за собой риск утраты закрытой или конфиденциальной информации. Угрозы и атаки для мобильных устройств в основном состоят из перенацеленных версий атак, направленных на другие конечные устройства. Эти риски можно разделить на несколько областей:

- вредоносное ПО: вирусы, программы-закладки, которые существуют почти для всех операционных систем. Особенно распространены троянские программы, предназначенные для кражи данных, которые могут работать как в сети мобильного девайса, так и в любой подключенной сети Wi-Fi. Они часто отправляются через SMS (текстовое сообщение) Для нейтрализации угрозы данного типа рекомендуется использование на девайсах специальной операционной системы, которая позволяет изолированно запускать рабочие приложения. Такими ОС являются IOS, Windows Phone.

- наличие уязвимостей и недеklarированных возможностей в ПО устройства;

- перехват коммуникации – угрозы, возникающие при обмене информации по каналам связи: открытые беспроводные точки доступа, перехват между узлами, подмена узлов или данных при передаче, утечка по ПЭМИН;

- Технология взлома беспроводных сетей доступна в Интернете, что упрощает выполнение взломов Wi-Fi и атак типа MITM. Сотовая передача данных также может быть перехвачена и дешифрована. Хакеры могут использовать недостатки в протоколах Wi-Fi и сотовых данных, чтобы подслушивать передачу данных или захватывать сеансы пользователей для онлайн-сервисов, включая электронную почту в Интернете. Мерой по снижению рисков является использование специального клиентского программного обеспечения безопасности. ПО устанавливается на девайс и позволяет создать защищенное VPN соединение, использовать антивирусы [2].

Физический доступ – утрата устройства (кража, поломка, утеря).

Снизить риски позволяет использование системы MDM (Mobile Device Management), которая позволяет удаленно уничтожить информацию на устройстве, которое, например, было украдено, совершать поиск девайса, блокировать устройство до ввода специального уникального пароля, а также восстанавливать данные при получении девайса назад или переустановки системы на другое устройство.

Защита внутренних ресурсов компании (конфиденциальной информации) при использовании концепции BYOD должна рассматриваться, как часть комплексной системы сетевой безопасности. Одним из главных этапов является выработка и закрепление в локальных нормативных актах: правилах, политиках, четкой регламентации:

- обязанностей и ответственности пользователей девайсов;
- порядка действий при утрате устройства;
- порядка подключения девайсов к беспроводным сетям вне офиса;
- списка разрешенного программного обеспечения и порядок его обновления;
- программ защиты информации и двухфакторной аутентификация;
- расчета оценки рисков и постоянного мониторинга.

Таким образом, минимизация рисков при использовании концепции BYOD зависит от степени защиты корпоративной информации. Защита информации должна являться частью комплексной защиты информации на предприятии, и включать в себя не только программные аспекты, но и локальные нормативные акты, которые четко регламентируют и устанавливают обязанности и ответственности пользователей устройств.

СПИСОК ЛИТЕРАТУРЫ

1. Мормуш А.Н. BYOD-дверь в инфраструктуру предприятия. Information security. №5, ноябрь 2016, 28-29.
2. O'Neal D, Zimmermann R. Mobile Device Security in the Workplace: 5 Key Risks and a Surprising Challenge. Forsythe focus, 12 Jule, 2017. <http://focus.forsythe.com/articles/55/Mobile-Device-Security-in-the-Workplace-5-Key-Risks-and-a-Surprising-Challenge>

УДК 004.932

СТРУКТУРА ДАННЫХ ДВУХМАСШТАБНОЙ ДИХОТОМИЧЕСКОЙ ИЕРАРХИИ ОБЪЕКТОВ НА ЦВЕТОВОМ ИЗОБРАЖЕНИИ

Харинов Михаил Вячеславович

Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия, 39,
email: khar@iias.spb.su

Аннотация: В докладе обсуждается модель аппроксимации цветового изображения иерархической последовательностью кусочно-постоянных приближений. Предлагается определение разбиения изображения на вложенные изображения объектов. Описывается структура данных для эффективных вычислений. Проводится сравнение с известными решениями.

Ключевые слова: сегментация изображения; кластеризация пикселей; суммарная квадратичная ошибка; минимизация; иерархия приближений; выпуклая последовательность.

DATA STRUCTURE OF TWO-SCALE DICHOTOMIC HIERARCHY FOR OBJECTS IN A COLOR IMAGE

Kharinov Mikhail

St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,
Russia, St. Petersburg, 14 Line, 39,
email: khar@iias.spb.su

Abstract: The report presents a model of color image approaching by a hierarchical sequence of piecewise constant approximations. The definition of splitting an image into nested images of objects is suggested. A data structure for efficient computations is described. Comparison with known solutions is carried out.

Keywords: image segmentation; pixel clustering; total squared error; minimization; hierarchy of approximations; convex sequence.

Введение. На сегодняшний день, для области обработки изображений остается актуальной проблема создания общеупотребительной модели изображения. Основной трудностью при создании такой модели является определение объектов на изображении без использования априорной информации о конкретных «объектах интереса». Работа [1] отражает современную тенденцию к детектированию на изображении структурированных объектов, которые состоят из некоторых частей и сами объединяются в большие объекты. В рамках указанной тенденции развивается обсуждаемая в докладе модель, в которой структурированные объекты определяются посредством иерархического разделения изображения на вложенные изображения.

Модель двухмасштабной иерархии объектов. В модели дихотомической иерархии объектов изображение аппроксимируется последовательностью приближений в 1, 2, 3... цветах, которые размечают изображение на различные объекты. Цвета упорядочиваются по величине падения суммарной квадратичной ошибки E при разделении надвое множества пикселей данного цвета. При этом детектируемые компьютером объекты, упорядочиваются по дополнительному признаку, который характеризует объекты подобно занимаемой ими площади и в задачах распознавания полезен на этапах последующей обработки.

Модель дихотомической иерархии объектов фактически является моделью применения метода Уорда [2] для кластеризации пикселей изображения и называется двухмасштабной, так как описывает изображение кусочно-постоянными приближениями в двух масштабах — как иерархию объектов и иерархию частей объектов. При этом приближение изображения посредством базовых объектов удовлетворяет трем условиям минимизации суммарной квадратичной ошибки E аппроксимации изображения:

1. Последовательность приближений внутри каждого объекта как самостоятельного изображения описывается выпуклой последовательностью значений E .

2. Максимальное падение E при разделении надвое любого объекта не превышает минимального приращения E при слиянии любой пары объектов в один объект.

3. Реклассификация любой части объекта из одного объекта в другой не повышает E .

Эффективные вычисления обеспечиваются применением метода Уорда по частям изображения и метода K-means [3] в уточненной версии, а также выполнением расчетов в терминах специальной структуры данных.

Структура данных. Все вычисления по иерархической кластеризации и сегментации выполняются в терминах структуры данных динамических деревьев Слэйтора-Тарьяна [4,5], в которой множествам пикселей сопоставляются деревья, а их слияние описывается установлением дуги между корневыми узлами деревьев. Динамические деревья (ациклические графы) дополняются циклами (циклическими графами), заданными в виде кольцевых связных списков, в которых каждый элемент списка ссылается на следующий, а последний элемент ссылается на первый. Динамические деревья и

циклы формируются on-line, непосредственно в процессе вычислений, и образуют динамическую сеть, которая вначале задается на множестве координат пикселей элементарными деревьями и циклами, состоящими из единственного узла. В процессе вычислений деревья и циклы укрупняются или разделяются на компоненты одновременно со слиянием или разделением множеств пикселей, операции с которыми они описывают [4,5].

В вычислительной модели дихотомической иерархии объектов координаты пикселей упорядочиваются в порядке построчной развертки. Кластеры пикселей, в частности, сегменты изображения задаются координатами минимальных начальных пикселей, отнесенных к данному кластеру или сегменту, и деревьями, дуги которых связывают пиксели между собой. Кроме того, те же кластеры или сегменты задаются циклами ссылок пикселей друг на друга, которые задают списки пикселей, отнесенных к данному кластеру или сегменту. По указанным спискам пикселей и деревьям с установленными дугами вычисляются, так называемые, «спрямленные» деревья, дуги которых связывают каждый пиксель с начальным пикселем данного кластера или сегмента. При этом «спрямленные» деревья обеспечивают скоростное вычисление кластера, к которому в данный момент отнесен каждый пиксель.

Порядок слияния кластеров пикселей запоминается благодаря циклам дуг, упорядоченных в порядке установления. Сами кластеры пикселей на момент вычисления задаются в виде циклов начальных пикселей. Поскольку при установлении очередной дуги число кластеров уменьшается на единицу, циклы дуг и циклы начальных пикселей кластеров дополняют друг друга, преобразуются согласованно и физически размещаются в одном и том же массиве. Сдвоенные связные списки установленных дуг и начальных пикселей обеспечивают скоростное воспроизведение последовательности приближений изображения, а также любого приближения с тем или иным числом кластеров в прямом и обратном порядке.

Операция разделения надвое кластера пикселей, определяемая как операция, обратная операции слияния пары кластеров, поддерживается циклами дуг, которые вычисляются для каждого узла дерева и задают списки входящих дуг, упорядоченных в порядке установления. При этом обеспечивается возможность скоростного нахождения дуги, разрыв которой описывает разделение надвое данного кластера пикселей именно на те кластеры, слиянием которых он был получен. Благодаря указанной организации данных оказывается возможным минимизировать суммарную квадратичную ошибку E за счет оптимального выбора порядка разделения кластеров и модификации упомянутых выше сдвоенных списков дуг и начальных пикселей.

Заключение. Судя по нашему опыту, метод Уорда обеспечивает устойчивое выделение на изображении объектов в виде близких по усредненным цветам кластеров пикселей, которые «видит» компьютер [6]. При этом внедрение метода Уорда в практику обработки изображений приводит к модели двухмасштабной дихотомической иерархии объектов, которая благодаря структуре данных динамической сети поддерживает скоростные вычисления с кластерами пикселей и сегментами изображения, а также обеспечивает эффект запоминания миллионов приближений изображения в RAM. Смысл модели дихотомической иерархии объектов прозрачен и сводится к тому, что исходное изображение представляется иерархией структурированных изображений объектов классическим методом Уорда [2], но с учетом особенностей изображения [6]. При этом нетривиальный формализм модели состоит в организации расчетов в терминах специальной структуры данных динамической сети, которая «набрасывается» на пиксели для ускорения вычислений и экономии памяти [5,7,8]. Для эффективного внедрения модели двухмасштабной дихотомической иерархии объектов в практику обработки изображений, вычисления в терминах динамической сети предполагается оформить в виде стандартных утилит обработки, чтобы ими пользовались программисты-инженеры, не вдаваясь в детали математического описания.

СПИСОК ЛИТЕРАТУРЫ

1. Чочиа П.А. Теория и методы обработки видеоинформации на основе двухмасштабной модели изображения / Дис. докт. технич. наук. – М.: ИППИ РАН, 2016. 302 с.
2. Ward J.H., Jr. Hierarchical grouping to optimize an objective function. J. Am. Stat. Assoc. 1963. vol. 58. Issue 301, pp. 236-244.
3. Айвазян С.А., Бухштабер В.М., Енюков И.С., Мешалкин Л.Д. Прикладная статистика: Классификация и снижение размерности // – М.: Финансы и статистика, 1989. 607 с.
4. Tarjan R.E. Efficiency of a Good But Not Linear Set Union Algorithm // Journal of the ACM, 1975. V. 22 (2), P. 215-225.
5. Kharinov M.V. Pixel Clustering for Color Image Segmentation // Programming and Computer Software, 2015, Vol. 41, № 5, pp. 258–266.
6. Ханьков И. Г., Харинов М.В. Модель цифрового изображения на основе модифицированного метода Уорда кластеризации пикселей // Вестник Бурятского государственного университета. Математика, информатика. – Улан-Удэ: Изд-во Бурятского госуниверситета, 2017. №2. С. 61-70.
7. Харинов М.В. Основы модели квазиоптимальных приближений изображения // Вестник Бурятского государственного университета, Математика и информатика, – Улан-Удэ: Изд-во Бурятского госуниверситета, 2016. №1 С. 60-72.
8. Харинов М.В., Ханьков И. Г. Применение метода Уорда для кластеризации пикселей цифрового изображения // Вестник Бурятского государственного университета. Математика, информатика. – Улан-Удэ: Изд-во Бурятского госуниверситета, 2016. №4. С. 34-42.

УДК 51.74

МОДЕЛИРОВАНИЕ УЯЗВИМОСТЕЙ В СИСТЕМЕ БЕЗОПАСНОСТИ

Шипилева Алла Владимировна
Волгоградский государственный университет,
Россия, Волгоград, Университетский проспект, д. 100,
email: ashpileva@mail.ru

Аннотация: В статье представлена модель динамики уязвимостей в системе безопасности, используя предельное поведение ветвящегося процесса с непрерывным временем можно показать, как в многоуровневой системе безопасности можно вычислять потенциал атаки.

Ключевые слова: безопасность; уязвимости; ветвящиеся процессы.

MODELING OF FLAWS WITHIN A SECURITY SYSTEM

Shipileva Alla
Volgograd State University,
Russia, Volgograd, University prospect, 100,
email: ashpileva@mail.ru

Abstract: The article presents a model of the dynamics of vulnerabilities in the security system, using the limiting behavior of a branching process with continuous time can show how in a multi-level security system it is possible to calculate the attack potential.

Keywords: security; flaws; branching processes.

Введение. В настоящее время существует много работ, раскрывающих различные подходы к анализу уязвимостей систем безопасности [1, 2]. В отличие от других программных элементов системы безопасности являются многоуровневыми. Все уровни защиты должны быть преодолены злоумышленниками, чтобы они могли получить неограниченный доступ. В этой статье представлен подход, основанный на ветвящихся процессах с непрерывным временем [5], на расчет потенциального количества уязвимостей в пределах любого элемента защиты в зависимости от времени, в течение которого он подвергался вредоносному вмешательству.

Пусть случайные величины $\xi_0, \xi_1, \xi_2, \dots$ - число уязвимостей в нулевом, первом, втором, и т.д. уровнях защиты системы соответствует числу вершин (состояний) корневого ориентированного дерева уязвимостей (дерева угроз). Дугам дерева уязвимостей приписаны вероятности p_i перехода из состояния i - го уровня защиты в состояние $i+1$ - го уровня. Длительность пребывания в каждом состоянии нулевого, первого, и т.д. уровнях защиты равна соответственно $t_0, t_1, t_2, \dots$ и не является случайной величиной.

При определении вероятности p_i того, что злоумышленник не сможет использовать уязвимости в i - узле дерева уязвимости для проведения атак за заданное время, необходимо учитывать тип дерева уязвимостей.

Заключение. По предложенному дереву атак определяются вероятности, которые можно использовать для вычисления потенциала атаки [5].

СПИСОК ЛИТЕРАТУРЫ

1. Абрамов Е. С., Андреев А. В., Мордвин Д. В. Применение графов атак для моделирования вредоносных сетевых воздействий // Известия Южного федерального университета. Технические науки. 2012. Том 26. Вып.1. С.165 -173.
2. Котенко И. В., Степашин М.В., Богданов В.С. Оценка безопасности компьютерных сетей на основе графов атак и качественных метрик защищенности // Труды СПИИРАН.2006. Вып.3. С.30-39.
3. Котенко И. В., Дойникова Е. В., Чечулин А.А. Динамический перерасчет показателей защищенности на примере определения потенциала атаки // Труды СПИИРАН. 2013. Вып.7. С.26-39.
4. Цыбулин А.М., Шипилева А.В. Математическая модель злоумышленника в корпоративной сети // Сборник трудов. Управление большими системами ИПУ им. В.А.Трапезникова РАН.2007. Вып.19. С.127-133.
5. Харрис Т. Теория случайных ветвящихся процессов. — М: Мир, 1966 — 356с.

УДК 742.012

СИСТЕМНЫЙ ПОДХОД К ТЕОРИИ ИСКУССТВОВЗНАНИЯ

Ярошевич Людмила Ивановна
Санкт-Петербургский государственный институт кино и телевидения
Россия, Санкт-Петербург, ул. Правды, д. 13,
email: ludmila-arttech@rambler.ru

Аннотация: В статье рассмотрена необходимость объединения в единую теорию моделирования изображений точных и гуманитарных наук. Отмечена важность издания учебной литературы для художественных специальностей, объясняющей принадлежность искусства к науке Кибернетике. Введение научно-обоснованной последовательной теории в образовательный процесс.

Ключевые слова: единая система моделирования; моделирование в искусстве; учебники современного образца

A SYSTEM APPROACH TO THE THEORY OF ART

Yaroshevich Ludmila Ivanovna

The St. Petersburg State institute of film and television

Russia, St. Petersburg, Pravda str. 13,

email: ludmila-arttech@rambler.ru

Abstract: This article presents the need to combine the images into a single simulation system. It's importance publishing of information for art specialties. It's necessary to prove the art to science Cybernetics. The introduction of science-based, coherent theory to the educational process.

Keywords: *Unified modeling system; modeling of drawings in Art; textbooks modern sample*

Введение. Путь историко - философского исследования в познании искусства приносит много новых сведений в теорию искусства. Колоссальные возможности в раскрытии тайн художественной практики таит в себе информатика. Научные публикации в этом направлении, раскрывают методику искусствознания, дополняют ее новыми методами. Новое мышление, не отрицая прежних технологий, предлагает взглянуть на обратную связь передачи информации через изображения. С течением времени теория искусства становится неотделимой частью всех видов изображений. Математизированные и нематематизированные изображения это - единая по смыслу система. Не правы те образовательные подразделения, которые исключили из своего состава кафедры Начертательной геометрии. Начертательная геометрия – необходимая составляющая часть науки об изображениях на всех уровнях образовательной системы.

Главное назначение изображений хранить и передавать информацию во времени, во всех видах представления данных...

Всякое изображение это – совмещение проекций восприятия первого, второго, третьего, и т.д. планов в единую композицию, т.е. в суммарную диаграмму восприятия многоуровневого пространства. Единая теория изображений позволит с большим пониманием оценивать терминологию, сложившуюся в естественных условиях, количественно-качественной передачи информации. Подход к вопросу с точки зрения теории систем очевиден.

Примечательно, что Норберт Виннер, создатель Кибернетики, в 17 лет сначала получил искусствоведческое образование, а затем проявил себя как математик. Однако Кибернетика с 1960-х годов начала развиваться, прежде всего, с точных наук, основанных на математических методах, появилась дисциплина – Информатика. Точность - безусловно, важна. Но, именно, кибернетический подход позволяет найти количественно-качественное соответствие и соединить в единую систему точные и гуманитарные науки, создать научную теорию моделирования.

Заключение. Образовательная система сегодня остро нуждается в дальнейшем развитии теории моделирования и качественных учебных пособиях, объясняющих принадлежность художественных изображений к науке Кибернетике.

СПИСОК ЛИТЕРАТУРЫ

1. Норберт Виннер "Кибернетика". Перевод с английского И.В. Соловьева и Г.Н. Пивоварова. Издательство "Наука", 1983г.
2. Ярошевич Л.И. Изобразительная кибернетика как методика кибернетики. Материалы XXIII международной научно-методической конференции "Современное образование: содержание, технологии, качество", 21 апреля 2017г. СПб, "ЛЭТИ" 1т. 298с.



СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.65

СПЕЦИФИЧЕСКИЕ УГРОЗЫ СИСТЕМ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

Бориева Анна Андреевна

Государственный университет морского и речного флота имени адмирала С.О. Макарова, Россия,
г.Санкт-Петербург, ул.Двинская, 5/7,
email: demeneva_a@mail.ru

Аннотация: в данной статье проводится анализ угроз, возникающих вследствие манипулирования данными, а также рассматриваются методы решения этих проблем.

Ключевые слова: база данных; СУБД; защита информации; агрегирование; инференция.

SPECIFIC THREATS OF DATA BASE CONTROL SYSTEMS

Borieva Anna

Admiral Makarov State University of Maritime and Inland Shipping, Russia, St. Petersburg, Dvinskaya st.,
5/7,
email: demeneva_a@mail.ru

Abstract: in this article analyzes the threats arising from the consequences of manipulation, and also considers methods for solving these problems.

Keywords: database; DBMS; data protection; aggregation; inference.

Введение. Сегодня, когда общество находится на стадии перехода от индустриального типа к постиндустриальному, одной из главных особенностей становится повсеместное использование баз данных. Управление их созданием и использованием осуществляется с помощью систем управления базами данных (СУБД). Как и для любой структуры, объектом которой является информация, для СУБД актуальны три основных понятия информационной безопасности – конфиденциальность, целостность и доступность [1].

Понимание происхождения возникающих угроз, является ключом к выстраиванию эффективной политики безопасности. Риски, связанные с базами данных, варьируются от организации к организации, в зависимости от типа информации и той важности, которую она имеет для самой компании. На данный момент наиболее распространенными угрозами СУБД являются: слабая аутентификация; SQL-инъекции; расширенные права, превышающие требования функционала работы сотрудника; вредоносное программное обеспечение, используемое для кражи конфиденциальной информации через законных пользователей с использованием зараженных устройств; экспозиция резервных носителей; эксплуатация уязвимых баз данных; DoS-атаки.

Специфическими угрозами СУБД назовем угрозы, возникающие вследствие манипулирования данными. Наиболее распространенными являются агрегирование и инференция.

Агрегирование данных – это метод получения конфиденциальной информации на основе информации, находящейся в открытом доступе. При этом используются только общепринятые законы математической логики. Простым примером будет являться защита множества C , состоящего из подмножеств A и B . Если мы хотим закрыть доступ к C , то следует ограничить доступ, как минимум, к A или B .

Вторая категория угроз – инференция, включает в себя данные и специализированные знания, которые являются внешними по отношению к системе. Это метод логического вывода, интеллектуального анализа данных, используемый для поиска информации, скрытой от обычных пользователей. Примером может служить аналитика налоговых отчислений по сотрудникам на предприятии. В сочетании с внешними знаниями налогового законодательства можно получить информацию о заработной плате конкретных лиц.

Для решения этих проблем необходимо тщательное проектирование модели данных и максимальное ограничение прав доступа пользователей к информации. Помимо этого, практикуют следующие методы борьбы с угрозами «вывода»:

– Скрытие;

при скрывании некоторые результаты запроса представляют собой случайную выборку или диапазон результатов. При использовании этого метода данные могут быть аппроксимированы, объединены, округлены или представлены в диапазоне или случайной выборке результатов.

- Произвольная пертурбация данных;

произвольная пертурбация данных, путем добавления ложных данных в результат запроса с помощью специальных функций.

- Партиционирование;

состоит из разделения данных на основе их степени уязвимости. Этот метод, хотя и очень эффективен для защиты конфиденциальных данных, имеет недостаток в громоздкости и сложности, которые он доставляет администратору СУБД.

- Многоэкземплярность;

этот метод используется в многоуровневых СУБД. При его использовании данные классифицируются на основе оценок уязвимости, и конечные пользователи могут получить доступ только к тем данным, для которых у них есть необходимое разрешение.

- Средства управления запросами;

этот метод обычно используется для защиты от косвенных атак. Средства управления запросами обрабатывают входящий запрос, результирующий вывод, или, возможно, и то и другое, и отклоняет запросы или результаты, которые не соответствуют политике вывода СУБД.

- Предварительная обработка и анализ результатов;

предварительная обработка запроса выполняется до выполнения запроса и используется для предотвращения сомнительных запросов. И наоборот, анализ результатов запроса выполняется после выполнения запроса и используется для предотвращения слишком точных сомнительных результатов, особенно тех, которые, возможно, были пропущены на этапе предварительной обработки.

- Сохранение истории запросов;

как правило, при сохранении истории запросов для архивирования запросов пользователей или групп используются алгоритмы кластеризации, чтобы гарантировать, что несколько запросов не используются для вывода секретных данных.

Заключение. Специфическими угрозы СУБД могут поставить под вопрос целостность всей базы данных. Чем сложнее база данных, тем выше должна быть обеспечена безопасность, связанная с ней. Если проблемы агрегирования и инференции не решаются эффективно, конфиденциальная информация может быть изъята третьими лицами.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р ИСО/МЭК 17799—2005
2. Maurer R. Top Database Security Threats and How to Mitigate Them [Электронный ресурс] // shrm.org: Society for human resource management. Jul 30. 2015. URL: <https://www.shrm.org/resourcesandtools/hr-topics/risk-management/pages/top-database-security-threats.aspx> (дата обращения: 20.09.2017).
3. Database Inference [Электронный ресурс] // globaltechconsultants.org: Global Tech Consulting Group. <http://globaltechconsultants.org/?q=content/database-inference> (дата обращения: 23.09.2017).
4. Белоусов А.С., Бories З.В., Ныров А.П., Соколов С.С. Разработка эффективной системы управления базами данных ресурсов IT-инфраструктур транспортных объектов: Материалы научно-исследовательской конференции IT: ВЧЕРА, СЕГОДНЯ, ЗАВТРА - 2013. — СПб.: Федеральное государственное бюджетное образовательное учреждение высшего образования Государственный университет морского и речного флота им. адмирала С.О. Макарова, 2013, С. 59-64.

УДК 004.056.53

ТЕСТИРОВАНИЕ СОВРЕМЕННЫХ СРЕДСТВ ЗАЩИТЫ ВИРТУАЛЬНЫХ ИНФРАСТРУКТУР

Бородин Михаил Константинович, Бородина Полина Юрьевна
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский пр., 49,
emails: mikborod@gmail.com, p.y.zaharova@gmail.com

Аннотация: В ходе данного исследования было выполнено тестирование на проникновение на предварительно развёрнутом стенде с виртуальной инфраструктурой на основе VMware vSphere 6 и средством защиты информации vGate R2 4.0. Целью проведенного тестирования являлось обнаружение потенциальных уязвимостей в защите виртуальной инфраструктуры без нанесения вреда непосредственно виртуальным машинам. В данной статье рассмотрены методы тестирования на проникновение методами черного и серого ящиков. Для проведения исследования были использованы различные утилиты и приложения из дистрибутива Kali Linux для сканирования и создания нагрузки на сетевую инфраструктуру. В частности, рассмотрено использование утилиты Nmap не только в качестве средства получения информации о возможных уязвимостях, но и инструмента для осуществления атаки типа «отказ в обслуживании» на используемое средство защиты информации.

Ключевые слова: тестирование на проникновение; виртуализация; CЗИ vGate R2; Kali Linux; VMware

TESTING OF MODERN VIRTUAL DATA PROTECTION SOFTWARE

Borodin Mihail, Borodina Polina

ITMO University,

Russia, St. Petersburg, Kronverkskiy pr., 49,

emails: mikborod@gmail.com, p.y.zaharova@gmail.com

Abstract: A penetration testing is performed on a pre-deployed stand with a virtual infrastructure based on VMware vSphere 6 and vGate R2 4.0 data protection suite. The purpose of this testing is to detect potential vulnerabilities in the virtual infrastructure protection with no sort of damaging directly to virtual machines. In this article, we had discussed penetration testing by the method of black and gray boxes. We will use various utilities and applications from Kali Linux distribution for scanning the network infrastructure and load testing. In particular, the use of Nmap utility is considered not only as a means of information gathering, but also as a tool for implementing a denial-of-service attack on the used information protection suite.

Keywords: *penetration testing; virtualization; vGate R2; Kali Linux; VMware*

Введение. Тестирование на проникновение, как один из элементов аудита информационной безопасности, помогает получить важную информацию о защищенности информационной системы и возможностях её совершенствования. В ходе такого тестирования проводятся мероприятия, позволяющие обнаружить недостаточность средств защиты или их неверную конфигурацию.

Основным отличием тестирования на проникновение от взлома системы злоумышленником являются информированное согласие владельца информационной системы и отчет о результатах испытаний. При тестировании методом черного ящика происходит имитация атаки посторонним лицом, не обладающим правами в системе и не имеющим представления о её внутреннем устройстве. Также было проведено дополнительное исследование методом серого ящика, который позволяет имитировать действия нарушителя, обладающего некоторыми сведениями об устройстве сети и её защите, также нарушитель может обладать пользовательской учётной записью с ограниченными привилегиями.

Для проведения исследования было выбрано СЗИ vGate R2 – сертифицированное средство защиты платформ виртуализации на базе VMware vSphere или Microsoft Hyper-V. Данное средство является одним из самых распространённых решений в области защиты виртуальных инфраструктур на российском рынке. Тестирование проводилось на версии vGate R2 4.0, которая на момент написания статьи прошла сертификацию ФСТЭК и вскоре должна стать доступной для широкого круга пользователей. Среди возможных платформ виртуализации была выбрана наиболее распространенная в корпоративном сегменте – VMware vSphere, в составе кластера серверов виртуализации ESXi и центра управления VMware vCenter.

Ключевым элементом данного исследования выступил Kali Linux – специальный дистрибутив для проведения тестирования на проникновение и «этичного хакинга». Данная операционная система основана на стабильном дистрибутиве Debian и поставляется с широким набором встроенных программ и утилит для исследования защищенности различных информационных систем. В данном исследовании были использованы следующие широко известные инструменты, как: Wireshark, Nmap, Hydra, hping3 и другие.

Заключение. В тексте статьи приведены некоторые методы проведения тестирования на проникновение, кратко описана конфигурация сети, используемые продукты и инструменты. Приведен опыт успешного применения некоторых типов атак на тестируемое средство защиты информации и выявлены существующие уязвимости. Данная статья будет интересна специалистам по аудиту информационной безопасности, интеграторам сложных инфокоммуникационных систем, а также студентам и преподавателям по направлениям, связанным с информационной безопасностью.

СПИСОК ЛИТЕРАТУРЫ

1. Плешков А. С. Тестирование на проникновение как анализ защищенности компьютерных систем / А. С. Плешков, Д. Рудер // Известия Алтайского государственного университета. – 2015. – №1. – С. 174-181.
2. Aileen G. Bacudio. An overview of penetration testing / Aileen G. Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu, Monique Jones // International Journal of Network Security & Its Applications (IJNSA). – 2011. – №6. – С. 19-38.

УДК 007

СЛОЖНОСТЬ ЗАДАЧ УПРАВЛЕНИЯ И СЕТЕЦЕНТРИЗМ

Верзун Наталья Аркадьевна, Колбанев Михаил Олегович

Санкт-Петербургский государственный экономический университет,

Россия, Санкт-Петербург, ул. Садовая, 21

emails: verzun.n@unecon.ru, mokolbanev@mail.ru

Аннотация: В докладе рассматриваются способы преодоления растущей сложности задач управления в современных экономических системах. Благодаря применению информационно-коммуникационных технологий вычислительные возможности объектов управления в экономических системах значительно возросли: они самостоятельно могут обрабатывать большие объемы

информации и принимать обоснованные решения. В связи с этим во всех сферах деятельности перспективными становятся методы и стратегии управления, основанные на взаимодействии равноправных участников.

Ключевые слова: *сетецентризм; экономическая система; информационный барьер; распределенная система; мультиагентная система.*

THE COMPLEXITY OF THE MANAGEMENT TASK AND NETWORK-CENTRIC

Verzun Natalya, Kolbanov Mikhail
The St. Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str. 21,
emails: verzun.n@unecon.ru, mokolbanov@mail.ru

Abstract: The report examines ways of overcoming the growing complexity of management tasks in modern economic systems. Thanks to the use of information and communication technologies, computing capabilities of facilities management in economic systems has considerably increased: they are independently able to process large amounts of information and make informed decisions. In this regard, promising methods are and management strategies based on cooperation of equal participants.

Keywords: *network-centric; the economic system; the information barrier; distributed system; multiagent system.*

При оценке сложности задач управления в реальных больших экономических системах российский кибернетик середины прошлого века академик Глушков В. М. отмечал, что она (сложность) зависит от числа материальных, информационных, энергетических и других видов связи между элементарными объектами, которые в совокупности образуют экономическую систему.

Проведенные Глушковым В. М. исследования показали, в частности, что во второй половине XX века рост числа связей выражается не менее чем квадратичной функцией от числа элементарных объектов экономической системы [1]. Сопоставляя растущую сложность задач управления в экономической системе с пропускной способностью ее организационной системы управления Глушков предположил следующее: с достижением достаточно больших размеров, любая экономическая система проходит два информационных барьера:

- первый барьер – система не может управляться одним человеком;
- второй барьер – для полного решения всех задач управления не хватит всех имеющихся в наличии людей.

Наличие информационных барьеров было обусловлено ограниченными возможностями переработки информации человеком, являвшимся до изобретения средств вычислительной техники единственным ее переработчиком. В процессе роста, объединения существующие системы достигли первого информационного барьера, для преодоления которого было предложено два механизма “распараллеливания” процесса управления:

- возникновение иерархических систем управления;
- вовлечение в процесс управления в равной мере всего взрослого населения планеты (управление в данном случае реализуется косвенно через товарно-денежные отношения).

Однако при достижении второго информационного барьера данные механизмы перестают работать. К началу 70-х гг. минимальная сложность задач управления оценивалась в 1016 арифметических операций. В то время как “вычислительные” возможности человека составляют 106 арифметических операций в год. Соответственно для решения всех задач управления уже недостаточно всех людей, живущих на Земле. Для усиления информационной мощности необходимы были дополнительные “усилители” интеллектуальных возможностей человека, которыми стали средства вычислительной техники и информационные системы.

С достижением второго информационного барьера механизм непосредственного “распараллеливания” процесса управления отошел на второй план, и ключевым фактором повышения эффективности систем управления стало повышение производительности труда управленческого аппарата, т.е. иерархической системы управления, поддерживаемой различными средствами автоматизации, информационными системами на всех уровнях управления [2].

Однако сегодня, с развитием информационно-коммуникационных технологий, вычислительные возможности объектов нижнего уровня иерархии значительно возросли. Конечные узлы (или объекты управления) в современных экономических системах это мощные (в сравнении с прошлым веком) вычислительные устройства, которые самостоятельно могут обрабатывать большие объемы информации и принимать взвешенные решения “на месте” [3]. Поэтому иерархический принцип управления постепенно теряет свою актуальность: число уровней иерархии в системах управления уменьшается. Перспективными становятся методы (и стратегии) управления, основанные на взаимодействии равноправных участников. Последнее утверждение находит свое подтверждение, например, в следующих фактах:

- в появлении концепции сетецентризма, которая становится главной методологией деятельности человека в цифровом обществе [4, 5, 6];

- в принятии решений по уменьшению числа уровней иерархии в различных сферах хозяйственной деятельности;
- в сфере финансовой деятельности – возникновение технологии блокчейн, основанной на отказе от централизованного управления финансовыми операциями и создающей абсолютно новую модель информационного взаимодействия между компаниями и людьми без централизованных платформ и регуляторов при помощи распределенного реестра;
- в информационно-технологической сфере это: развитие различных ИК-технологий, использующих распределенные и мультиагентные системы управления; применение алгоритмов работы, основанных на взаимодействии равноправных участников: туманные вычисления, M2M, Mesh Topology, Peer to Peer, Swarm Intelligence и пр. [7, 8].

СПИСОК ЛИТЕРАТУРЫ

1. Глушков В. М. Кибернетика, вычислительная техника, информатика. Избранные труды: в 3 т. Т. 3: Кибернетика и ее применение в народном хозяйстве. – Киев: Наукова думка, 1990. – 224 с.
2. Левкин И. М., Ковалев А. П., Морозова Е. Ю. Пути совершенствования информационного обеспечения инновационной деятельности предприятия / Управленческое консультирование 2016, №5. С.112–120.
3. Верзун Н. А., Касаткин В. В., Колбанёв М. О. Цифровые технологии: инфокоммуникации и экономика // Сборник: Информационные технологии цифровой экономики: сб. статей. – СПб.: Изд-во СПбГЭУ, 2017. С.29–34.
4. Верзун Н. А., Ипатов О. С., Колбанёв М. О. О сетевых моделях цифровой экономики // Сборник: Информационные технологии цифровой экономики: сб. статей. – СПб.: Изд-во СПбГЭУ, 2017. С.35–41.
5. Новиков Д. А. Кибернетика: Навигатор. История кибернетики, современное состояние, перспективы развития. – М.: ЛЕНАНД, 2016. – 160 с.
6. Верзун Н.А., Колбанёв М.О., Касаткин В.В. Инфокоммуникационная среда, реализующая сетевый подход к управлению деятельностью / Перспективные направления развития отечественных информационных технологий: материалы III межрегиональной научно-практической конференции. Севастополь 19-23 сентября 2017 г. – Севастополь: "РИБЕСТ", 2017. – С.76-78.
7. Верзун Н. А., Колбанев М. О., Омелян А. В. Введение в инфокоммуникационные технологии и сети Future Networks: учебное пособие. – СПб.: Изд-во СПбГЭУ, 2016. – 51 с.
8. Боронин П. Н., Кучерявый А. Е. Интернет вещей как новая концепция развития сетей связи / Информационные технологии и телекоммуникации. 2014. №3(7). С.7–30.

УДК 621.391

ВЛИЯНИЕ ПАРАМЕТРОВ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ НА ПОТРЕБЛЕНИЕ ЭНЕРГИИ АВТОНОМНОЙ СИСТЕМОЙ МОНИТОРИНГА ЭКОСИСТЕМ

Верзун Наталья Аркадьевна¹, Колбанев Михаил Олегович¹, Колбанев Алексей Михайлович²

¹ Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, 21,

²ООО «Перспектива»,
Россия, Санкт-Петербург, Финляндский пр., 4а
emails: verzun.n@unecon.ru, mokolbanev@mail.ru, kolbanev@gmail.ru

Аннотация: В данной работе исследуется влияние параметров беспроводной сенсорной сети на потребление энергии сети в целом. Рассматривается процесс передачи блока данных в БСС от одного узла к другому. Предлагается математическая модель всепроникающей сенсорной сети, позволяющая оценивать энергетические характеристики процесса информационного взаимодействия сенсорных элементов.

Ключевые слова: автономная система мониторинга; беспроводная сенсорная сеть; энергоэффективность; мощность радиосигнала; плотность распределения узлов.

INFLUENCE OF PARAMETERS OF WIRELESS SENSOR NETWORK FOR ENERGY CONSUMPTION AUTONOMOUS SYSTEM OF ECOSYSTEM MONITORING

Verzun Natalya¹, Kolbanev Mikhail¹, Kolbanev Aleksey²

¹ The St. Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str. 21,

²Perspectiva Limited,
Russia, St. Petersburg, Finlyandsky prospect, 4a
emails: verzun.n@unecon.ru, mokolbanev@mail.ru, kolbanev@gmail.ru

Abstract: In this paper we investigate the influence of parameters of the wireless sensor network the energy consumption of the network as a whole. The process of transmitting a data block in BSS from one node to another. We propose a mathematical model of pervasive sensor networks, allowing to estimate the energy characteristics of the process of information interaction of sensor elements.

Keywords: autonomous monitoring system; wireless sensor network; energy efficiency; power radio; the distribution density of nodes.

Объект исследования данного доклада – автономная система мониторинга состояния экосистемы. Экосистемой может быть, например, территория сельскохозяйственных угодий с

посадками, или охраняемая территория (природные заповедники, национальные парки, памятники природы). Автономная система мониторинга представляет собой всепроникающую беспроводную сенсорную mesh-сеть (БСС), покрывающую площадь с посадками (или охраняемую территорию) информационной решеткой, которую составляют многочисленные и разнообразные технические средства наблюдения – датчики, сенсоры – объекты (или узлы) автономной системы [1-3]. В подобных системах, как правило, датчики являются устройствами с автономным питанием. Замена элементов питания во всех объектах БСС, с учетом большого их количества, значительных размеров «накрываемой» территории и малых размеров устройств становится трудновыполнимой задачей [4-6]. Ввиду этого нарастает актуальность необходимости сокращения энергопотребления объектами БСС на всех этапах их работы. Пути повышения энергоэффективности БСС: рациональный выбор параметров узлов, сети; алгоритмов/режимов их функционирования и пр.

В данной работе исследуется влияние параметров беспроводной сенсорной сети на потребление энергии сети в целом [7-10]. Рассматривается процесс передачи блока данных в БСС от одного узла к другому. Предположим, что:

- БСС включает совокупность объектов (или узлов) автономной системы, расположенных на территории конечной площади и образующих пуассоновское поле точек на плоскости;
- при выборе маршрута для передачи блока данных каждый узел передает его ближайшему (по расстоянию) от него «соседу».

С учетом указанных предположений были получены, в частности, выражения для:

- функции распределения (и плотности распределения) случайной величины расстояния от фиксированного узла БСС до ближайшего к нему другого узла в любой момент времени;
- требуемой мощности сигнала на передающей антенне узла, в предположении, что мощность радиосигнала на приемной антенне постоянна;
- математического ожидания случайной величины мощности, затрачиваемой радиопередатчиком фиксированного узла при передаче блока до ближайшего к нему узла в БСС;
- математического ожидания общей мощности сигнала радиопередатчиков узлов БСС при передаче блока от одного фиксированного узла другому через несколько промежуточных узлов.

Применяя вышеперечисленные выражения был проведен численный расчет и анализ влияния параметров рассматриваемой БСС (плотность распределения узлов в ней) и узлов (чувствительность приемника – требуемая мощность принимаемого радиосигнала) на требуемую мощность радиосигнала на передающей антенне объекта БСС [11].

СПИСОК ЛИТЕРАТУРЫ

1. Кучерявый А. Е., Прокопьев А. В., Кучерявый Е. А. Самоорганизующиеся сети. – СПб.: Любавич. – 2011. – 312 с.
2. Росляков А. В., Ванышин С. В., Гребешков А. Ю., Самсонов М. Ю. Интернет-вещей, – Самара: ПГУТИ, ООО «Издательство АсГард». – 2015. – 340 с.
3. Верзун Н. А., Колбанёв М. О., Омелян А. В. Введение в инфокоммуникационные технологии и сети Future Networks: учебное пособие. – СПб.: Изд-во СПбГЭУ, 2016. – 51 с.
4. Колбанев М. О., Пойманова Е. Д., Татарникова Т. М. Физические ресурсы информационного процесса сохранения данных / Изв. вузов. Приборостроение. – 2014. – Т.57, № 9. – 2014. – С.38–42.
5. Верзун Н. А., Колбанев М. О., Колбанев М. О. Энергетическая эффективность помехоустойчивого кодирования в беспроводных сетях интернета вещей / Изв. вузов. Приборостроение. – 2017. – Т.60, № 2. – 2017. – С.143–149.
6. Верзун Н. А., Колбанёв М. О., Омелян А. В. Регулируемый множественный доступ в беспроводной сети умных вещей / Омский научный вестник. Сер. Информатика, вычислительная техника и управление. – 2016. – № 4 (148). – С.147–151.
7. Верзун Н. А., Колбанёв М. О., Шамин А. А. Энергетическая эффективность взаимодействия в беспроводных сенсорных сетях // Информационные технологии и телекоммуникации. 2017. Том 5. № 1. – С.88–96.
8. Кучерявый А. Е., Нуриллоев И. Н., Пармонов А. И., Прокопьев А. В. Обеспечение связности беспроводных сенсорных узлов гетерогенной сети / Информационные технологии и телекоммуникации. – 2015. – №1(9). – С.115–122.
9. Давенпорт В. В., Рут В. Л. Введение в теорию случайных сигналов и шумов. – М.: Издательство иностранной литературы, 1960. – 467 с.
10. Уоллес Р. Максимальная дальность связи по радиоканалу в системе: как этого добиться? – 2015. – № 11. – С.3-13.
11. Верзун Н.А., Колбанёв М.О., Шамин А.А. Исследование влияния параметров беспроводной сенсорной сети на ее энергоэффективность / Перспективные направления развития отечественных информационных технологий: материалы III межрегиональной научно-практической конференции. Севастополь 19-23 сентября 2017 г. – Севастополь: «РИБЕСТ», 2017. – С.119-121.

УДК 004.451

БЕЗОПАСНАЯ ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ ПРОЕКТИРОВАНИЯ КОРПОРАТИВНЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ УНИФИЦИРОВАННОГО ЯЗЫКА МОДЕЛИРОВАНИЯ UML

Дубенецкий Владислав Алексеевич, Кузнецов Александр Григорьевич,
Цехановский Владислав Владимирович

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5,
email: dubvl@list.ru; CHR12@yandex.ru vvcehanovsky@mail.ru

Аннотация: Рассматривается безопасная информационная технология проектирования корпоративных информационно-управляющих систем на основе использования модельного подхода к разработке с использованием case-средства, поддерживающего концепцию на основе унифицированного языка моделирования UML.

Ключевые слова: технология проектирования; case-средство; UML.

SECURE INFORMATION TECHNOLOGY FOR DESIGNING CORPORATE INFORMATION-MANAGEMENT SYSTEMS BASED ON THE USE OF THE UNIFIED MODELING LANGUAGE UML

Dubenetsky Vladislav, Kuznetsov, Aleksandr, Tsehanovsky Vladislav
The St. Petersburg State Electrotechnical University "LETI",
email: dubvl@list.ru; CHR12@yandex.ru vvcehanovsky@mail.ru

Abstract: Considered safe information technology in designing corporate information-management systems on the model-based approach to development using case-tools supporting the concept based on the unified modeling language UML.

Keywords: design technology; case-tool; UML.

В настоящее время в области проектирования корпоративных информационно-управляющих систем (КИУС) широко применяется модельный подход на основе использования унифицированного языка моделирования UML.

Унифицированный язык моделирования (Unified Modeling Language, UML) является графическим языком для визуализации, специфицирования, конструирования и документирования КИУС, включая проектирование программного обеспечения и физическую модель базы данных [1, 2].

С помощью UML можно обеспечить безопасную информационную технологию проектирования КИУС, начиная с разработки концептуальной модели с ее бизнес-функциями и процессами, а также описать особенности реализации системы. Используя модельный подход UML, можно разрабатывать сложные КИУС более качественно, по сравнению с традиционным.

Как язык визуального моделирования UML имеет свою нотацию – принятые обозначения. Нотация обеспечивает семантику языка, является способом унификации обозначений визуального моделирования, обеспечивает всестороннее представление системы, которое сравнительно легко и свободно воспринимается пользователем. Моделирование с помощью UML осуществляется поэтапным построением ряда моделей, каждая из которых отражает какую-то часть или сторону КИУС либо ее замысла.

Модель – это графическое представление множества элементов. Обычно модель изображается в виде графа с вершинами (сущностями) и ребрами (отношениями) [3].

Основные модели UML:

- вариантов использования (use case);
- классов (class);
- кооперации (collaboration);
- последовательности (sequence);
- состояний (statechart);
- деятельности (activity);
- компонентов (component);
- развертывания (deployment).

Разработки и построения этих моделей достаточно для полного построения модели КИУС.

Моделирование с помощью UML предполагает построение ряда взаимосвязанных моделей. Для сопровождения процесса построения, анализа и документирования модели, а также проверки модели и генерации программных кодов разработчики используют специально созданные для этих целей CASE-средства проектирования КИУС.

В общем смысле CASE (Computer-Aided Software Engineering) — это набор инструментов и методов программной инженерии для проектирования КИУС, который помогает обеспечить высокое качество разработки, отсутствие ошибок, генерацию программного кода, а также простоту в обслуживании программных продуктов.

Существует достаточно много CASE-инструментов моделирования и проектирования информационных систем и баз данных (не только с помощью UML). В данной статье выбран программный инструмент моделирования StarUML [1].

Данная программная платформа имеет свободную лицензию и доступна для установки с официального сайта StarUML.

StarUML поддерживает основные модели, принятые в нотации UML, а также модельно-настраиваемую архитектуру. Поддерживает расширения, предоставляет различного рода модули, расширяющие возможности StarUML.

Для того чтобы успешно выполнить проект, объект проектирования должен быть, прежде всего правильно и адекватно описан, то есть необходимо построить полноценные и функциональные

информационные модели объекта проектирования. CASE-средства, поддерживают процесс создания и сопровождения КИУС, включая анализ и формулировку требований, проектирование прикладного ПО и баз данных, генерацию кода, тестирование, документирование, обеспечение качества, конфигурационное управление и управление проектом. Предлагается ряд расширений UML по работе с метаклассами и процессами, позволяющие существенно улучшить технологию проектирования КИУС.

СПИСОК ЛИТЕРАТУРЫ

1. StarUML. The Open Source UML/MDA Platform. Version 5.0.2.1570. Руководство пользователя. Перевод Д. В. Летуновского, 2007, 207 с.
2. Буч Г., Рамбо Д., Джекобсон А. Язык UML. Руководство пользователя. М.: ДМК Пресс, 2007, 489 с.
3. Дубенецкий В.А., Советов Б.Я., Цехановский В.В. Проектирование корпоративных информационных систем. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2013, 191 с.

УДК 004.56

СТРАТЕГИЯ И КУЛЬТУРА БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ СОБСТВЕННОГО АВТОРСКОГО ИНФОРМАЦИОННОГО РЕСУРСА

Виноградов Алексей Борисович, Циголева Марина Андреевна
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
email: vvchehanovsky@mail.ru

Аннотация: Противодействием нарушению авторской информационной безопасности должна служить стратегия киберзащиты и построения защищенной авторской среды - индивидуальной, коллективной, корпоративной. Применение выработанной стратегии и продуманной системы собственной информационной безопасности позволит создать культуру безопасного использования собственного авторского информационного ресурса в стратегически защищенном информационном предметном пространстве компьютерной и информационной безопасности.

Ключевые слова: информационная безопасность, тематические системы поиска, информационные поисковые системы, защита информации.

THE STRATEGY AND CULTURE OF THE SAFE USE OF AN ORIGINAL INFORMATION RESOURCE

Shirokov Vladimir, Schigoleva Marina
The St. Petersburg State Electrotechnical University "LETI",
email: vvchehanovsky@mail.ru

Abstract: Opposition to the violation of copyright of information security should serve as a strategy for cyber security and building a secure copyright environment - individual, collective, corporate. Application-defined strategy and well thought-out system of its own information security allows to create a culture of safe use of personal information resource in a strategically protected information subject area computer and information security.

Keywords: information security, the thematic search system, information search system, information security.

В современном обществе широкой общедоступности информации большое значение для безопасности авторской информации - индивидуальной, коллективной, корпоративной, прежде всего, самим авторам следует принять меры к ограничению неоправданной вседоступности своего информационного продукта. Применение сетевых средств подготовки, согласования и доведения до адресата авторских материалов делает их доступными широкому кругу пользователей электронного ресурса. Существование сетей ограниченного использования и защищенных сетей является предметно- и объектно- ориентированными и защищаемыми политикой государственной информационной безопасности. В сферах науки, производства, образования, культуры, искусства, спорта, корпоративной деятельности, становится уже нормой представление сведений, результатов и отчетов о своей деятельности на сайтах организаций, предприятий, проводимых мероприятий.

Научная, методическая, образовательная, производственная информация выкладывается на сайты и в сеть и становится предметом сравнения со схожим тематическим и терминологическим электронным ресурсом в системах поиска массовых и специализированных информационных систем. Сами системы тематического поиска и тематического моделирования стали самостоятельной областью исследований и разработок с большими перспективами для использования в различных направлениях жизнедеятельности. Созданы специальные новостные системы, проверяющие наличие поисковых слов-маркеров в информационных потоках; составляются тематические словники, включающие наборы специфических для конкретной области слов для избирательного поиска и архивирования тематических рубрик нового информационного ресурса. Системы антиплагиата в науке и образовании стали во многом ловушками для самих добросовестных авторов, вынужденных

искусственно уводить свои результаты от тщательно подобранных и выверенных авторских формулировок, выявляемых системой антиплагиата и включающей счетчик заимствований у самого себя. Тематические системы занимаются текстовым поиском по ключевым словам через системы мониторинга корреспонденции, используя свои разработки и признанные технологии, которые помимо выявления информации делают текстовые вырезки и пересылку по заявленным адресатам.

Подобные технологии широко используются в системах компьютерной безопасности для поиска фактов государственной и террористической угрозы. Помимо компьютерной перлюстрации новой информации аналогичные системы и технологии обладают качеством троянских программ, которые распространяются как модуль программ обнаружения жертвы, установления контакта и вживления в программное обеспечение жертвы с возможным последующим тиражированием трояна. Технологии усовершенствования вредоноса также развиваются на новом качественном уровне и с увеличением ареалов их распространения. Совершенствуются приемы и способы загрузки вредоноса - через защищенный паролем архив или через другие трояны: загрузились, сориентировались и подгрузили дополнительные модули, в том числе со сбором сведений о транзакциях жертвы и пересылкой своих сообщений в базовые адреса сбора захваченной информации. Скачивание выявленной информации может сопровождаться разными способами скрытого или явного разрушения программного обеспечения жертвы.

Противодействием нарушению авторской информационной безопасности должна служить стратегия киберзащиты и построения защищенной авторской среды - индивидуальной, коллективной, корпоративной, которая включает компоненты, отражающие специфику автора и предметной среды информационного ресурса, например:

- обучение безопасным практикам,
- построение систем мониторинга информационного ресурса,
- система реагирования на инциденты,
- восстановление работоспособности после выявленных атак и сбоев,
- распространение информации об инцидентах,
- развитие инфраструктуры на принципах встроенной системы собственной информационной безопасности.

Основным положением стратегии авторской информационной безопасности является наличие системы собственной информационной безопасности с обучением безопасным практикам: со строгим контролем перечня распространяемой информации, широте информирования, глубине и концентрации информации, форме обобщения и представления информации, адресности распространения и доведения информации.

Применение выработанной стратегии и продуманной системы собственной информационной безопасности позволит создать культуру безопасного использования собственного авторского информационного ресурса в стратегически защищенном информационном предметном пространстве, технически и аппаратно поддерживаемом программно-аппаратными технологиями компьютерной и информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Б.Я. Советов, В.В. Цехановский. Информационные технологии: теоретические основы. Учебное пособие. СПб: Лань, 2017 г. 444 с.

УДК 004.056

ПОСТРОЕНИЕ ПРОГРАММНОГО ШЛЮЗА ДЛЯ СЕТЕВОЙ ИЗОЛЯЦИИ ВИРТУАЛЬНЫХ МАШИН

Зегжда Петр Дмитриевич, Никольский Алексей Валерьевич, Алексеев Илья Вадимович
Санкт-Петербургский политехнический университет Петра Великого,
Россия, Санкт-Петербург, ул. Политехническая, 29
emails: kafedra@ibks.spbstu.ru, alexei.nikolsky@ibks.ftk.spbstu.ru, ialexeev@ibks.spbstu.ru

Аннотация: Рассмотрена проблема сетевой изоляции целевой операционной системы от удаленных атак. Проанализированы существующие средства виртуализации и предложено собственное решение для построения программного шлюза для сетевой изоляции виртуальных машин.

Ключевые слова: сеть Интернет; защита от сетевых атак гипервизор; сетевая изоляция

BUILDING A PROGRAM GATEWAY FOR NETWORK INSULATION OF VIRTUAL MACHINES

Zegzhda Petr, Nikolskiy Aleksey, Alekseev Ilya
The St. Petersburg State Polytechnic University of Peter the Great,
Russia, St. Petersburg, Polytechnicheskaya str. 29,
emails: kafedra@ibks.spbstu.ru, alexei.nikolsky@ibks.ftk.spbstu.ru, ialexeev@ibks.spbstu.ru

Abstract: The problem of network isolation of the target operating system from remote attacks is considered. Analyzed existing virtualization tools and offered our own solution for building a software gateway for network isolation of virtual machines.

Keywords: Internet; protection from network attacks; hypervisor; network isolation

Введение. В настоящее время сеть Интернет является самым распространенным способом реализации атак на персональные компьютеры, передачи вредоносного программного обеспечения с целью дальнейшей эксплуатации уязвимостей целевой операционной системы (ОС) и ее компонентов, передачи украденных данных нарушителю, а также удаленного контроля вредоносного программного обеспечения [1]. Следовательно, одной из основных задач обеспечения информационной безопасности ПК является защита от сетевых атак.

Существуют различные решения данной задачи безопасности: средства обнаружения вторжений, средства предотвращения вторжений, межсетевые экраны, DLP-системы, DPI-системы и др. Однако, все данные решения не решают проблему изоляции ОС от существующих сетевых адаптеров. Ведь именно отделение ОС от физического присутствия сетевого адаптера предотвратит любой сетевой доступ как извне к целевой ОС, так и изнутри из целевой ОС в сеть Интернет, однако при этом большинству пользователей необходимо наличие сетевого соединения.

Данная задача может быть успешно решена с использованием технологии аппаратной виртуализации путем создания гипервизора, виртуализирующего хостовую ОС, для которой будет скрыто существование сетевых адаптеров, установленных на компьютере, а доступ к ним будет предоставлен только гостевой виртуальной машине, которая будет запущена впоследствии. В настоящее время существует всего несколько решений, позволяющих передать управление сетевым адаптером напрямую в виртуальную машину: Xen, VirtualBox [2]. Указанные решения рассчитаны на использование в крупных серверах (Xen) или в ОС семейства Linux (VirtualBox), в то время как для пользователей наиболее распространенных ОС семейства Windows подобного решения нет.

В процессорах Intel, начиная с Intel Core, реализована технология Intel Virtualization Technology for Directed I/O [3]. Данная технология позволяет осуществлять виртуализацию DMA запросов, формируя для каждого PCI устройства собственное виртуальное адресное пространство, что позволит разграничить и изолировать виртуальные машины не только между собой, но и между различными периферийными устройствами.

Таким образом, можно полностью скрыть наличие физического сетевого адаптера для хостовой виртуальной машины, при этом гостевая виртуальная машина будет иметь полный доступ к сетевому адаптеру. Такое разграничение между хостовой ОС и гостевой ОС возможно благодаря контролю вложенной виртуализации. Разработанный гипервизор представляет собой программный шлюз, разделяющий аппаратное обеспечение, в том числе и сетевые адаптеры, между хостовой ОС и гостевой ОС.

Заключение. Предложенный подход к построению программного шлюза для сетевой изоляции виртуальных машин позволяет защититься от сетевых атак, изолируя все их последствия внутри виртуальной машины с гостевой ОС, при этом все действия происходят прозрачно для пользователя, решение универсально относительно хостовой ОС, гостевой ОС, системы виртуализации и оборудования.

СПИСОК ЛИТЕРАТУРЫ

1. Платонов В.В. Программно-аппаратные средства защиты информации - М.: Издательский центр «Академия», 2013, 336 с.
2. Спецификация «Oracle VM VirtualBox User Manual Version 5.1.26», 2017, 361 с.
3. Спецификация архитектуры «Intel Virtualization Technology for Directed I/O», 2016, 276 с.

УДК 004.056

АНАЛИЗАТОРЫ ПРОТОКОЛОВ ДЛЯ КОНТРОЛЯ НАД ПАКЕТАМИ ДАННЫХ МЕЖДУ УСТРОЙСТВАМИ СЕТИ

Зорин Кирилл Михайлович, Гурьянов Денис Юрьевич, Щиголева Марина Андреевна
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
emails: kirillzorin@gmail.com; rightx@gmail.com; vvchehanovsky@mail.ru

Аннотация: С целью эффективного управления и защиты данных в корпоративной информационной сети организуется контроль над пакетами данных, передающимися между устройствами сети. Для возникающих задач в сегментах сети предлагается вариант мониторинга сетевого трафика с серверным приложением и использованием ресурса базы данных сети.

Ключевые слова: корпоративная информационная сеть; коммуникационное обслуживание информационной системы; пакеты данных; сетевой трафик данных.

PROTOCOL ANALYZERS FOR MONITORING DATA PACKETS BETWEEN NETWORK DEVICES

Zorin Kirill, Guryanov Denis, Shigoleva Marina
The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
emails: kirillzorin@gmail.com; rightx@gmail.com; vvchehanovsky@mail.ru

Abstract: Effective management and protection of data in corporate information network organized control over data packets transmitted between network devices. For emerging challenges in network segments, the program is monitoring the network traffic with the server application and use of the database resource network.

Keywords: *corporate communication network, communication service information system, data packets, network traffic data.*

Для организации эффективного управления и защиты данных в корпоративной информационной сети требуется возможность контроля над пакетами, передающимися между устройствами сети. Острота и актуальность вопроса возрастают при обеспечении нарастающей пропускной способности сети, необходимом уровне качества обслуживания, защите передаваемых данных. Применяемые архитектурные решения организации коммуникационного обслуживания информационной системы при наращивании нагрузки сети должны функционально сопровождаться анализом работы сети и диагностикой состояния её информационного ресурса. Для пакетного режима обработки данных в информационных компьютерных сетях требуется организация контроля над трафиком пакетов, передающихся между устройствами сети. Системное администрирование сети, анализ параметров сети, выявление уязвимостей и хакерских атак помогают реализовать анализаторы протоколов пакетов данных. В распределенных информационных системах с сетевым программным обеспечением и приложениями типа клиент-сервер анализаторы протоколов выступают как мощное средство для отладки и диагностики программ обработки данных и обслуживания ресурса сети.

По сочетанию задач: регистрации данных, передаваемых в сегментах сети; записи и хранении информации в базах данных сети; выдачей пользователю данных в удобной для него форме; возможностью анализа сетевого трафика и фильтрации трафика; контроля и декодирования захваченных пакетов; разрабатывается программа мониторинга сетевого трафика с серверным приложением и использованием ресурса базы данных сети.

При контроле за продвижением пакетов данных, приемом, выдачей их в удобном для пользователя форме, логика работы анализатора протоколов между устройствами сети решает задачи контроля над пакетами данных, функционального обеспечения доведения пакетов данных между устройствами сети, сбора и отображения архитектуры сети и исполнения сетевого трафика. Пользовательский интерфейс и сервисное обеспечение обеспечивают сбор и отображение статистики на основании сведений, полученных из принятого сетевого трафика; регистрацию данных, передаваемых в сегментах сети; анализ захвата и фильтрации сетевого трафика по задаваемым пользователем параметрам; запись и хранение информации о перехваченных пакетах; выделение вложенности пакетов протоколов разных уровней с возможностью расшифровки содержания отдельных полей пакета. В архитектуре корпоративной информационной сети возможно отображение компьютеров, подключенных к локальной сети в динамике режимов их использования; подключение и отключение интернет-соединения на клиентском компьютере; отображение форм применения сервисного ресурса и пользовательского интерфейса.

Программно-вычислительный ресурс сети может предоставить графическое представление полученной статистической информации в виде графиков и диаграмм загрузки сети. По информационному ресурсу сети производится регистрация данных и пакетов данных, их трафика, адресность доведения, обеспечение сохранения целостности пакетов данных, фрагментарное декодирование пакетов данных по задаваемым пользователем параметрам.

Анализатор протоколов для контроля над пакетами данных между устройствами сети включает алгоритмы анализа передаваемого трафика по сети с контролем пользовательского трафика с помощью структуры клиент-серверного приложения, выбора сетевого интерфейса, сканирования дерева сети, перехвата сетевых пакетов, фильтрации сетевых пакетов, анализа передаваемого трафика.

СПИСОК ЛИТЕРАТУРЫ

1. Б.Я. Советов, В.В. Цехановский. Информационные технологии: теоретические основы. Учебное пособие. СПб: Лань, 2017 г. 444 с.

УДК 004.5

**МОДЕЛИ КОРРЕКЦИИ ФУНКЦИОНАЛЬНОГО СОСТОЯНИЯ, ОСНОВАННЫЕ НА
ТИПОЛОГИЧЕСКИХ ОСОБЕННОСТЯХ ЧЕЛОВЕКА-ОПЕРАТОРА В РАМКАХ УЛУЧШЕНИЯ
ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ИНДИВИДА**

Колмаков Сергей Александрович

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5,
email: s.kolmakov1992@gmail.com

Аннотация: Рассматриваются способы представления функционального состояния человека, выделяются факторы, которые необходимо учитывать для достоверного отображения функционального состояния. Предлагаются модели для коррекции функционального состояния человека, основанные на типологических особенностях человека-оператора.

Ключевые слова: функциональное состояние; психологическая безопасность; работоспособность; типологические особенности.

**MODEL OF CORRECTION FUNCTION STATE BASED ON THE TYPOLOGICAL FEATURES OF THE
HUMAN OPERATOR IN THE FRAMEWORK OF IMPROVING THE INFORMATION-PSYCHO LOGICAL
SECURITY OF THE INDIVIDUAL**

Sergey Kolmakov

The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
email: s.kolmakov1992@gmail.com

Abstract: The report deals with ways to represent the functional state of a person, identify factors that must be taken into account for a reliable mapping of the functional state. Also in this report, models for the correction of a person's functional state, based on the typological features of the human operator, are proposed.

Keywords: functional state; phichological safety; working capacity; typological features.

Введение. Психологическая безопасность – одно из наиболее актуальных направлений в исследованиях ученых, представляющих науки о труде. Мы можем понимать информационно-психологическую безопасность человека как состояние защищенности личности, обеспечивающее ее целостность как активного социального субъекта и возможностей развития в условиях информационного взаимодействия с окружающей средой [1]. Основываясь на этом можно сделать вывод, что информационно-психологическая безопасность неотрывно связана с понятием функционального состояния человека-оператора.

На сегодняшний день функциональное состояние (ФС) рассматривают с различных сторон:

– С точки зрения психофизиологии функциональное состояние рассматривают как фоновую активность нервной системы человека.

– С точки зрения эргономики и инженерной психологии функциональное состояние рассматривают в рамках деятельностного подхода, т.е. оценки эффективности труда в конкретной деятельности человека [2].

Ввиду отсутствия единого подхода к пониманию ФС, следует рассматривать как набор характеристик разных направлений, включающих в себе сразу несколько основ:

1. Физиологическую (ЧСС, ЭКГ).
2. Деятельностную (количество ошибок в единицу времени).
3. Психологическое само восприятие субъекта (бальная оценка на основе опросников об утомляемости).

Соответственно ФС человека можно представить кортежем, который содержит в себе выше перечисленные показатели. При этом следует учитывать, что интегральные оценки функциональных состояний не должны выходить за рамки установленных норм для конкретной деятельности, т.е. реализовывать методы адаптивного анализа отклонения показателей от нормы[3].

Однако при возможности оценки ФС человека не менее важным для информационно-психологической безопасности индивида стоит вопрос о возможности управления этим состоянием.

Если обратиться к диаграмме работоспособности человека-оператора (Ч-О), то можно увидеть, что работоспособность оператора имеет несколько ярко выраженных периодов: период мобилизации, устойчивой работоспособности, утомляемости. Любая из фаз связана со своей собственной задачей по коррекции ФС, но каждая из них тем или иным способом связана с активацией или же релаксацией нервной системы [4].

Можно выделить множество способов коррекции ФС, но особый интерес представляют методы прямого воздействия: ароматерапия, музыкотерапия, электростимуляция тканей, цветотерапия, мультимедийные воздействия, вибростимуляция и т.д. [5]. Каждый из этих методов работает с разной

эффективностью. Ответ на вопрос «почему?» стоит искать в области дифференциации психологического и психофизиологического строения человека. Соответственно, при нормализации функционального состояния человека-оператора необходимо учитывать индивидуальные особенности строения его нервной системы: психофизиологический тип, соматотип, функциональную асимметрию [6, 7, 8].

Можно выдвинуть следующую гипотезу: все сигналы, воздействующие на Ч-О, можно разделить на две категории – активизирующие и релаксирующие. Активизирующие сигналы можно пометить знаком «+», они отвечают за мобилизацию резервов организма, а также повышают количественные показатели характеристик, отображающих ФС. Релаксирующие сигналы можно пометить знаком «-», они отвечают за снижение активности и количественное уменьшение показателей отображающих ФС. Соответственно, мы можем представить само оптимальное ФС человека как некий коридор из допустимых значений. При выходе из коридора допустимых значений необходимо применять методы коррекции.

Так же, как было сказано выше, типологические особенности человека-оператора важны при определении и выборе программы воздействия на индивида, однако данный момент современной наукой мало изучен. Отсутствуют единые алгоритмы для составления программ воздействия, а также малоизучено влияние типологических характеристик человека-оператора и различных параметров сигналов отличных модальностей на функциональное состояние человека-оператора. Однако, воздействие на человека можно было бы представить в виде иерархической структуры, которая имеет три уровня: уровень характеристики человека, уровень характеристик сигналов, уровень функционального состояния. Соответственно описать воздействие на человека-оператора можно при помощи нескольких кортежей, содержащих как характеристические данные по сигналам, так и весовые коэффициенты зависимостей [9].

Однако, данная модель имеет ряд сложностей, которые еще предстоит решить. Одной из основных сложностей является отсутствие в достаточном количестве проведенных исследований, а соответственно, необходимость разработать методологию исследования искомых зависимостей. Так же из задач, которые будет необходимо решить – подбор характеристик сигналов, которые могли бы выражаться в количественном эквиваленте, а не в качественном [10].

Заключение. Несмотря на то, что в области коррекции функционального состояния человека методами прямого воздействия имеется множество вопросов, на которые до сих пор не найдены ответы, данное направление является крайне перспективным. Оно открывает огромные возможности для создания методов повышения работоспособности человека, разработок методологии для снятия психологических нагрузок, стрессов и депрессий, что в конечном итоге будет способствовать повышению информационно-психологической безопасности личности. В данной работе приведены иерархические модели коррекции функционального состояния человека-оператора, а также отмечены имеющиеся проблемы в реализации данных моделей, которые и являются следующими этапами для изучения проблемной области.

СПИСОК ЛИТЕРАТУРЫ

1. Грачев Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты – М.: Изд-во РАГС, 1998 – 125 с.
2. Леонова А.Б., Психодиагностика функциональных состояний человека, изд. МГУ, 1984г.
3. Ушаков И.Б., Богомолов А.В. Паттерны функциональных состояний оператора – М.: Наука, 2010. – 390 с.
4. Данилова Н.Н., Крылова А.Л. Физиология высшей нервной деятельности. М.: изд. Моск. ун-та, 1989, 231 с.
5. Колмаков С.А. Методы коррекции функционального состояния человека-оператора и его типологические особенности// Человеческий фактор в сложных технических системах и средах, труды Второй Международной научно-практической конференции. 2016, Издательство: Межрегиональная эргономическая ассоциация, С. – 325 – 331.
6. Богомаз С.А. Психологические типы К.Г.Юнга, психофизиологические типы и интертипные отношения. – Т.: Издательский дом ТГУ, 2000, 71 с.
7. Антропова Л.К. Функциональная асимметрия мозга и индивидуальные психофизиологические особенности человека// Медицина и образование в Сибири. – 2011. – №3. – С. 81 – 93.
8. Шутова С.В. Влияние обонятельного сенсорного притока на время и точность сенсомоторных реакций у юношей разных конституциональных типов // Вестник ТГУ – 2001. – Вып. 1 – С. 69 – 71.
9. Психологические основы профессиональной деятельности: хрестоматия / Сост. В.А. Бодров. – М.: ПЕР СЭ; Логос, 2007, 511 с.
10. Леонова А.Б. Психологические технологии управления состоянием человека – М.: Изд-во Моск. ун-та, 2007. – 380 с.

УДК 004

ТЕОРИЯ СОЗДАНИЯ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ АВТОМАТИЗИРОВАННОГО ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

Кривоногов Сергей Вячеславович

Нижегородский государственный инженерно-экономический университет,
Россия, Княгинино, ул. Октябрьская, 22 а.

emails: ksvkn@mail.ru

Аннотация: В статье проводится анализ теоретического материала для разработки распределенной системы автоматизированного обнаружения уязвимостей в программном обеспечении. Проводится обзор литературных источников, занимающихся данными проблемами. Поставлены цели и задачи разработки. Непосредственно выполнена сама разработка указаны ее

плюсы и минусы. Разработка строится на технологии фаззинга, применяемого в задаче поиска уязвимостей в ПО.

Ключевые слова: анализ безопасности; информационная безопасность; методы защиты; программирование; распределенная система; системы защиты; уязвимости.

THE THEORY OF THE CREATION OF A DISTRIBUTED SYSTEM FOR AUTOMATED DETECTION OF SOFTWARE VULNERABILITIES

Krivosnogov Sergey

Nizhny Novgorod state engineering-economic University

Russia, knyaginino, ul Oktyabrskaya, D. 22.

emails: ksvkn@mail.ru

Abstract: In article the analysis of theoretical material to develop a distributed system of automated detection of vulnerabilities in software. A review of the literature dealing with these problems. The goals and objectives of the development. Directly implemented development itself indicated its pros and cons. The development is based on technology fuzzing used in the task of searching vulnerabilities in the software.

Keywords: security analysis; information security; protection methods; programming; distributed system; protection systems; vulnerability.

Введение. Постановка задачи обнаружения уязвимостей в компьютерных системах получается в процессе актуализации и проектирования возможностей для получения незаконного доступа работниками госорганов или разведок, частных или государственных, а также при работе органов слежения либо хакерами. О значимости данной проблемы можно определять по данным которые размещают в интернет сетях за оплату, эти данные также можно обменять на информацию о багах и возможностях взлома, которые предлагаются на «внутреннем рынке хакеров» рынке в обмен на информацию об уязвимостях – для часто используемых систем эта сумма может достигать миллиона долларов США [1, с. 31]. Для примера можно взять программу для очистки системы CCleaner. Данная программа была модифицирована злоумышленниками для получения данных пользователя при помощи вредоносного кода маскируясь под сертификат антивирусного обеспечения.

Трудность нахождения багов в программном коде обозначается важнейшей проблемой разработчиков нового программного обеспечения так как недостатки программного обеспечения проблематично обнаружить. Важно то что многие разработчики программного обеспечения применяют всевозможные средства внедрения вредоносного, когда в основном это пассивная защита программного обеспечения. Так или иначе разработчики вынуждены постоянно находить и устранять баги своих проектов, которые так или иначе влияют на безопасность системы. Для разработчиков лучше получать сведения об ошибках и багах в процессе тестирования приложения, а не при атаке на информационную систему или программный продукт [2, с. 44].

У разработчиков для стимула поиска уязвимости разрабатываемого программного обеспечения есть фонд компаний таких как VISA, PayPal, Facebook или Google, в которых имеются программы поощрения специалистов информационной безопасности в обмен на финансовое вознаграждение и ошибки других программ, в такие организации вложены миллионы долларов США. [3, с. 51].

Такие фонды позволяют поощрять ученых, занимающихся информационной безопасностью, а также «дырами» в программном обеспечении, в связи с этим ученые проявляют высокую заинтересованность при поиске ошибок, а также разрабатывать инструменты, позволяющие более точно проводить поиск и анализ систем безопасности.

Данными вопросами контроля качества и поиска уязвимостей в информационных системах и программном обеспечении становились предметом изучения многих отечественных ученых, таких как Иванков А.В., Курюмов Д.В., Миноженко А.В., Нетесов В.С., Маликов О.Р., Козлов Д. Д., Курицин А. А. [4, с. 38]

Рассматриваемый в данной работе способ поиска ошибок изучался только зарубежными учеными, такими как Таканен Ари, ДеМотт Джаред, Миллер Чарльз и Ламберт Скот. В работе используется метод модульности [4, с. 40].

Целью выполняемой работы является проектирование и эксплуатация общей распределенной системы полного контроля для автоматического поиска багов и дыр в программном обеспечении.

На основании цели были сформулированы такие задачи как:

- создать скелет разделительной(распределенной) системы поиска мест взлома;
- спроектировать модель системы при помощи программного обеспечения;
- создать такую систему использующую нетривиальный фаззер, которая будет выполнять все работы в пределах распределенной системы;
- провести оценку эффективности спроектированной системы и апробировать ее в реальных условиях на примере часто используемых приложений, тем самым подтвердив ее практическую значимость.

В качестве объекта исследования выбраны процессы отбора уязвимостей программного обеспечения на уровне программного кода.

Предметом исследования в работе являются технологии деления на фазы программного кода и оболочки программного обеспечения, применяемые в задаче поиска уязвимостей в системах.

В качестве методологической и теоретической основы работы использовались разработки многих русских и зарубежных ученых безопасников, которые рассматривали анализ систем безопасности программного обеспечения в динамическом формате.

Теоретическая значимость исследования заключается в анализе существующих методов автоматического обнаружения уязвимостей и определении наиболее оптимальных методов, корреляция между сложностью развития и эффективностью.

Практическая значимость работы определяется способностью полностью использовать построенную систему как один из важных инструментов исследователя ИС. Прозрачная масштабируемость и разделенная структура системы в то же время позволяют использовать ее в течение всего времени работы.

Новшество исследования – это создание легко развертываемой и расширяемой системы для обнаружения багов, связанных с безопасностью, с уделением особого внимания браузеру в качестве цели (отражающей тот факт, что браузер является наиболее используемым и тем самым привлекает злоумышленников). Аналогов данного программного обеспечения среди свободного ПО не имеется.

Суть деления на фазы (модули) рассматривается таким образом, что каждая неделимая на модули фаза имеет способность обнаруживать в каждом отрывке программного кода неучтенные баги и способы взлома.

Проведенное исследование позволило получить важные результаты такие как:

- предложена и спроектирована модель каскадной системы обнаружения черных дыр в «системе защиты», на основании данной модели лежит фазная (модульная) технология.
- разработан модуль, с помощью которых можно провести оценку безопасности таких компонентов браузера, как расширения, представление и интерфейс пользователя;
- работоспособность полученной системы показана на опыте тестирования часто используемого программного обеспечения.

Заключение. В исследовании разработана распределенная система автоматического обнаружения багов в программном обеспечении в частности интернет технологиях. На первом этапе была проведена классификация уязвимостей и проанализированы методы и технологии их обнаружения. На основе этого анализа была выбрана технология поиска уязвимостей, сформулированы требования и определена модель системы.

На этапе проектирования модель была протестирована. Кроме того, был разработан модуль, который функционирует в рамках созданной системы. Впоследствии была проведена оценка эффективности, которая показывает что система работоспособна.

СПИСОК ЛИТЕРАТУРЫ

1. Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. – 2-е изд., испр. и доп. – М. : Издательство Юрайт, 2017. – 261 с.
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. – М. : Издательство Юрайт, 2017. – 312 с.
4. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. – М. : Издательство Юрайт, 2017. – 321 с.
5. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. – М. : Издательство Юрайт, 2017. – 325 с.

УДК 004.5

КОМПРОМИСС БЕЗОПАСНОСТИ И ЮЗАБИЛИТИ СОВРЕМЕННЫХ ПОЛЬЗОВАТЕЛЬСКИХ ИНТЕРФЕЙСОВ

Леонов Антон Викторович

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5,
emails: anton.leonov18@gmail.com

Аннотация: Рассматриваются вопросы безопасности сложных технических систем - конфиденциальной информации, персональных данных, обеспечение безопасности самой системы от риска принятия неправильных решений конечным пользователем. Взаимодействие с системой происходит при помощи пользовательского интерфейса, тем самым возникает необходимость нахождения компромисса между требованиями безопасности и удобства работы с системой, баланса между безопасностью и юзабилити пользовательских интерфейсов.

Ключевые слова: пользовательские интерфейсы; безопасность технических систем; юзабилити.

COMPROMISE BETWEEN SECURITY AND USABILITY OF THE MODERN USER INTERFACES

Leonov Anton

The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
emails: anton.leonov18@gmail.com

Abstract: Providing the security of complex technical systems is an important problem for modern society – confidential information, personal data, which is used in technical systems, must be protected. Moreover, it is necessary to ensure the security of the system itself from the risk of making the wrong decisions by the end-user. Interaction with the system takes place through the user interface, thus there is a need to find a compromise between the security requirements and the convenience of working with the system.

Keywords: *user interfaces; security; usability.*

Обеспечение безопасности сложных технических систем – важная проблема современного общества. С развитием Интернета все большее и большее количество конфиденциальной информации, персональных данных, которое необходимо защищать, используется в технических системах. Более того, необходимо обеспечивать безопасность самой системы от риска принятия неправильных решений конечным пользователем.

Взаимодействие с любой технической системой происходит при помощи пользовательского интерфейса, который обладает определенными критериями удобства использования. С другой стороны, техническая система должна быть безопасной (удовлетворять критериям безопасности). При этом безопасность системы должна оказывать минимальное влияние на ее юзабилити, чтобы не вызывать раздражения и эффекта отталкивания у конечных пользователей. Следовательно, возникает задача интеграции аспектов безопасности на всех этапах проектирования пользовательских интерфейсов, а также необходимость нахождения компромисса между требованиями безопасности и удобства работы с системой.

В ходе проведенного исследования:

- сформулированы основные критерии юзабилити и безопасности пользовательских интерфейсов;
- проведены исследования, которые показывают возможность реализации баланса между безопасностью и юзабилити на примере различных форм аутентификации пользователей;
- показаны примеры работы систем безопасности, которые влияют на удобство использования;
- подготовлен обзор существующей литературы, посвященной проблеме поиска компромисса между безопасностью и юзабилити пользовательских интерфейсов;
- предложены вопросы и проблемы для дальнейшего исследования в данной области.

Термин «юзабилити» применен как «способ разработки и проверки систем с использованием экспериментальных методов для достижения эффективности и удовлетворенности конкретных пользователей, которые выполняют определенную задачу в определенной среде» [1]. Цель юзабилити состоит в установлении компромисса между удовлетворением пользователя и его эффективностью.

Помимо создания безопасного программного обеспечения, предполагается правильная интеграция действий и политик безопасности в процесс разработки программного обеспечения. Подходы, основанные на оценке только юзабилити программных интерфейсов, не вполне подходят для оценки систем, ориентированных на обеспечение их безопасности [2]. Во многих исследованиях [5], отсутствует анализ реакции и поведения пользователей на нарушения в системе безопасности, хотя рассмотрение таких вариантов использования поможет лучше разработать безопасный интерфейс. Согласно Меллеру и др. [3], причина, по которой пользователи не могут эффективно использовать защищенные системы, заключается в том, что такие системы не учитывают принципы юзабилити в своем дизайне и вред может быть нанесен не только пользователю системы, но и самой системе в целом. В качестве примера можно привести традиционные графические формы для ввода пароля) и требования, которые система безопасности предъявляет к паролям (например, система требует ввести старый пароль, который ни разу не использовался для системы, повторить новый пароля, тем самым формирует конфликт между памятью человека и требованиями безопасности).

Проведенный анализ [1-12], показал недостатки проектирования существующих пользовательских интерфейсов с точки зрения аспектов безопасности и удобства использования, а также необходимость интеграции системы безопасности на всех этапах проектирования пользовательских интерфейсов. Предложена и показана возможность нахождения компромисса между безопасностью и юзабилити без снижения общего качества технической системы.

СПИСОК ЛИТЕРАТУРЫ

1. Weir C. S., Douglas G., Carruthers M., Jack M. User perceptions of security, convenience and usability for ebanking authentication tokens // *Computers & Security*, 2009, №28, P. 47-62.
2. Ugochi O. N., Beverly A. O., Babak B. R. Usability and Security in User Interface Design: A Systematic Literature Review // *I.J. Information Technology and Computer Science*, 2016, № 5, P. 72-80.
3. Moller S., Ben-Asher N., Engelbrecht K.-P., Englert R., Meyer J. Modeling the behavior of users who are confronted with security mechanisms // *Computers & Security*, 2011, № 30, P. 242-256.

4. Crano rL. F., Buchler N. Better together: Usability and security go hand in hand // IEEE Security & Privacy, 2014, P. 89-93.
5. Mihajlov M., Blažič B. J., Josimovski S. Quantifying Usability and Security in Authentication, 2011, P. 626-629.
6. Gunson N., Marshall D., Morton H., Jack M. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking // Computers & Security, 2011, № 30, P. 208-220.
7. Mihajlov M., Jerman-Blazic B., Josimovski S. A conceptual framework for evaluating usable security in authentication mechanisms-usability perspectives, 2011, P. 332-336.
8. Chiasson S., Forget A., Biddle R., Van Oorschot P.C. User interface design affects security: Patterns in click-based graphical passwords // International Journal of Information Security, 2009, № 8, P. 387-398.
9. Furnell S. Usability versus complexity—striking the balance in end-user security // Network Security, 2010, № 2010, P. 13-17.
10. Dhamija R., Dusséault L. The seven flaws of identity management: Usability and security challenges // Security & Privacy, IEEE, 2008, № 6, P. 24-29.
11. Habiba U., Masood R., Shibli M. A., Niazi M. A. Cloud identity management security issues & solutions: a taxonomy // Complex Adaptive Systems Modeling, 2014, № 2, P. 1-37.
12. Renaud K. Evaluating authentication mechanisms // Security and Usability: Designing Secure Systems That People Can Use, 2005, P. 103-128.

УДК 681.3

О ЗАДАЧЕ ПОИСКА НОВЫХ КОНЕЧНЫХ АССОЦИАТИВНЫХ АЛГЕБР ДЛЯ ПОСТРОЕНИЯ КРИПТОСХЕМ С ОТКРЫТЫМ КЛЮЧОМ

Молдовян Николай Андреевич¹, Ковалева Ирина Владиславовна²

¹ Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Россия, Санкт-Петербург, 14 линия, 39,

² Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», Россия, Санкт-Петербург, ул. Профессора Попова, 5.
emails: nmold@mail.ru, IrVKov@gmail.com

Аннотация: в статье рассмотрена проблема поиска новых вычислительно трудных задач для разработки доказуемо стойких постквантовых криптосхем. Изучен метод построения постквантовых криптосхем с открытым ключом на основе задачи поиска сопрягающего элемента в некоммутативных группах. Проанализированы работы по разработке алгоритмов на основе задачи конгруэнц логарифмирования. На основе проведенного исследования сделан вывод о необходимости расширения класса конечных алгебраических структур, в которых можно задать задачу конгруэнц логарифмирования. Предложен вариант поиска конечных ассоциативных алгебр различной размерности.

Ключевые слова: постквантовая криптография; криптографические протоколы; конечная алгебра; ассоциативная алгебра; задача дискретного логарифмирования.

ABOUT THE PROBLEM OF FINDING NEW FINITE ASSOCIATIVE ALGEBRAS FOR CONSTRUCTING PUBLIC KEY CRYPTOSCHEMES

Moldovyan Nikolay¹, Kovaleva Irina²

¹ Federal state budgetary institution of Science of St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences
Russia, St. Petersburg, 14-th Linia, VI, No. 39,

² The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5.
emails: nmold@mail.ru, IrVKov@gmail.com

Abstract: the article deals with the problem of searching for new computationally difficult problems for the development of provably secure post-quantum cryptoschemes. A method for constructing post-quantum public key cryptosystems based on the problem of searching for a conjugating element in noncommutative groups was studied. The work on the development of algorithms based on the congruence logarithm problem was analyzed. Based on research it was concluded that it is necessary to extend the class of finite algebraic structures in which the congruence logarithm problem can be specified. A variant of the search for finite associative algebras of various dimensions is proposed.

Keywords: post-quantum cryptography; cryptographic protocols; finite algebra; associative algebra; discrete logarithm problem.

Наиболее широкое практическое применение для открытого распределения ключей, открытого шифрования и аутентификации информации в автоматизированных информационных системах получили протоколы криптографии с открытым ключом, основанные на вычислительно трудных задачах факторизации и дискретного логарифмирования. Безопасность протоколов данного вида основана на том, что в настоящее время лучшие алгоритмы решения указанных задач имеют субэкспоненциальную (задача факторизации) и задача дискретного логарифмирования в конечных полях) или экспоненциальную сложность (задача дискретного логарифмирования в группе точек эллиптической кривой над конечным полем). В связи со значительным прогрессом в развитии квантовых вычислений возник интерес к оценке сложности дискретного логарифмирования и

факторизации при решении этих задач на квантовом компьютере. Было показано, что обе эти задачи имеют полиномиальную сложность в модели квантовых вычислений [1]. Этот результат означает, что в случае появления практически значимых квантовых вычислителей действующие в настоящее время стандарты, регламентирующие использование двухключевых криптографических алгоритмов и протоколов, должны быть отменены как не обеспечивающие требуемый уровень стойкости. Последнее порождает проблему развития арсенала алгоритмов ЭЦП, протоколов открытого распределения ключей и открытого шифрования, которые были бы безопасными в случае появления возможности практического использования квантовых вычислителей для выполнения атак на криптосхемы. Большинство алгоритмов криптографии с секретным ключом, например, блочные шифры, по мнению специалистов останутся стойкими и при возможности осуществления криптоанализа с использованием квантовых вычислителей. Однако для обеспечения достаточной стойкости алгоритмов и протоколов двухключевой криптографии требуется положить в их основу вычислительно трудные задачи другого типа, для которых сложность решения имела бы сверхполиномиальную сложность как при решении на компьютерах обычного типа, так и при их решении на квантовых компьютерах. Актуальность разработки алгоритмов и протоколов постквантовой криптографии обусловила появление регулярно проводимых тематических конференций. Для упреждения потенциально возможной критической ситуации Национальный институт стандартов и технологий (НИСТ, National Institute of Standards and Technology, NIST) объявил конкурс на разработку криптографических алгоритмов, основанных на новых вычислительно трудных задачах. В настоящее время не предложена задача, которая позволила бы обеспечить возможность разработки на ее основе всех типов криптосхем, которые реализованы на основе задачи дискретного логарифмирования или на основе задачи факторизации. В случае постквантовых криптосхем является ценным нахождение решения для каждого отдельного типа криптосхем.

В качестве алгебраических структур для задания новых вычислительно трудных задач, которые могут быть положены в основу криптосхем с открытым ключом, представляют значительный интерес некоммутативные группы. В известной зарубежной литературе опубликовано достаточно много работ по разработке двухключевых криптосхем на основе трудности задачи поиска сопрягающего элемента в группах переплетения (группах кос). В работе [2] сделана попытка построения криптосхем с открытым ключом на основе задачи нахождения сопрягающего элемента в конечных кольцах матриц. Однако оказалось, что задача поиска сопрягающего элемента в некоммутативных группах может быть решена методами линейной алгебры, т.е. не обладает высокой вычислительной сложностью, требуемой для разработки на их основе криптосхем с открытым ключом.

Следующим существенным шагом в направлении применения некоммутативных конечных групп и колец является предложение комбинирования задач дискретного логарифмирования и поиска сопрягающего элемента. Технические проблемы задания выбора различными пользователями коммутирующих между собой элементов некоммутативной группы были решены в работах [3], [4], [5], [6], где были предложены алгоритмы открытого распределения ключей, открытого шифрования, коммутативного шифрования на основе задачи дискретного логарифмирования в скрытой циклической конечной группе (называемой также задачей конгруэнц логарифмирования). Данные криптосхемы обладают субэкспоненциальной стойкостью к атакам с использованием традиционных компьютеров. Тем не менее было определено, что для обеспечения достаточной стойкости к атакам с использованием квантовых компьютеров следует найти некоммутативные конечные алгебры с ассоциативной операцией умножения, которые отличны от использованных в [3], [4], [5], [6] конечных некоммутативных колец, поскольку в последних решение задачи конгруэнц логарифмирования может быть сведено к решению задачи дискретного логарифмирования в конечном поле.

Закключение. Таким образом, вычислительно трудная задача конгруэнц логарифмирования (дискретного логарифмирования в скрытой циклической группе конечной некоммутативной алгебры) представляется перспективной для разработки протоколов и алгоритмов постквантовой криптографии. Однако для построения постквантовых алгоритмов и протоколов с открытым ключом требуется существенно расширить класс конечных алгебраических структур, в которых можно задать задачу конгруэнц логарифмирования, который в настоящее время является достаточно ограниченным и включает конечные некоммутативные. Значительный интерес представляет поиск конечных ассоциативных алгебр различной размерности, которые не являются коммутативными кольцами. Нахождение новых способов задания таких алгебр и исследование их свойств является базовым этапом предлагаемого проекта. На основе решения этой задачи будут разработаны способы задания новых типов конечных ассоциативных алгебр и разработаны криптографические алгоритмы и протоколы, представляющие интерес для расширения арсенала постквантовой криптографии.

СПИСОК ЛИТЕРАТУРЫ

1. Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer // *SIAM Journal of Computing*. 1997. Vol. 26. P. 1484–1509.
2. Grigoriev D., Shpilrain V. Authentication from Matrix Conjugation // *Groups-Complexity-Cryptography*. 2009. Vol. 1. № 2. P. 199-205.
3. Sakalauskas E., Tvarijonas P., Raulynaitis A. Key Agreement Protocol (KAP) Using Conjugacy and Discrete Logarithm Problems in Group Representation Level // *INFORMATICA*. 2007. Vol. 18. № 1. P. 115–124.

4. Moldovyan D.N. Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes // Quasigroups and Related Systems. 2010. Vol. 18. P. 165–176.
5. Moldovyan D.N., Moldovyan N.A. A New Hard Problem over Non-Commutative Finite Groups for Cryptographic Protocols // Springer Verlag LNCS. 2010. Vol. 6258. P. 183–194.
6. Горячев А.А., Молдовян Д.Н., Куприянов И.А. Выбор параметров задачи скрытого дискретного логарифмирования для синтеза криптосхем // Вопросы защиты информации. 2011. № 1. С. 19–23.

УДК 681.3

ПОСТРОЕНИЕ КОНЕЧНЫХ АЛГЕБР ДЛЯ РЕАЛИЗАЦИИ ПОСТКВАНТОВЫХ ПРОТОКОЛОВ ЗАЩИТНЫХ ПРЕОБРАЗОВАНИЙ ИНФОРМАЦИИ

Молдовян Николай Андреевич¹, Абросимов Иван Константинович²

¹ Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия, 39,

² Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5
emails: nmold@mail.ru, ivnabr@yandex.ru

Аннотация: рассмотрена проблема построения конечных алгебраических структур, с операциями над которыми связаны вычислительно трудные для квантового компьютера задачи. Изучен подход к построению некоммутативных колец конечномерных векторов с операциями перемножения векторов и автоморфного отображения векторов. На основании проведенного исследования сделаны выводы о способах построения таблиц умножения базисных векторов. Предложены варианты построения таких таблиц и показана применимость некоммутативных алгебр конечномерных векторов с введенной операцией умножения для построения постквантовых криптографических протоколов.

Ключевые слова: постквантовая криптография; криптографические примитивы; криптографические протоколы; конечные алгебраические структуры.

CONSTRUCTION OF FINITE ALGEBRAS FOR IMPLEMENTATION OF POST-QUANTUM PROTOCOLS OF PROTECTIVE TRANSFORMATIONS OF INFORMATION

Moldovyan Nikolay¹, Abrosimov Ivan²

¹ Federal state budgetary institution of Science of St. Petersburg Institute
for Informatics and Automation of the Russian Academy of Sciences
Russia, St. Petersburg, 14-th Linia, VI, No. 39,

² The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5.
emails: nmold@mail.ru, ivnabr@yandex.ru

Abstract: the problem of constructing finite algebraic structures with operations involving computationally difficult problems for a quantum computer is considered. An approach to the construction of non-commutative rings of finite-dimensional vectors with operations of multiplication of vectors and automorphic mapping of vectors is studied. Conclusions about the methods of constructing tables of multiplication of basis vectors are made on the basis of the study. Variants for constructing such tables are proposed and the applicability of non-commutative algebras of finite-dimensional vectors with the multiplication operation introduced for constructing post-quantum cryptographic protocols is shown.

Keywords: post-quantum cryptography; cryptographic primitives; cryptographic protocols; finite algebraic structures.

Введение. Широко применяемые алгоритмы асимметричного шифрования основываются на вычислительно сложных для классического компьютера задачах факторизации и дискретного логарифмирования. Безопасность криптосхем, основанных на этих задачах, связана с тем, что алгоритмы их решения имеют субэкспоненциальную или экспоненциальную сложность. Развитие квантовых вычислений и возможность появления квантовых компьютеров привело к необходимости оценки сложности данных задач в случае, когда атакующая сторона может использовать для атаки на криптосхему квантовый компьютер. Было показано [1], что данные задачи решаются на квантовом компьютере за полиномиальное время, что делает криптосхемы, основанные на задачах факторизации и дискретного логарифмирования нестойкими к атакам нарушителя, имеющего в своем распоряжении квантовый компьютер. В связи с этим, имеет место потребность в вычислительно трудных задачах, сложность решения которых оставалась бы сверхполиномиальной даже при наличии у нарушителя квантового компьютера.

Для формирования новых вычислительно трудных задач требуется использование конечных алгебраических структур, отличных от «традиционных» конечных полей. В качестве таких структур и вычислительно сложных задач соответственно предлагались группы переплетений и поиск сопрягающего элемента, кольца матриц и поиск сопрягающего элемента, конечные циклические группы

и комбинация задач дискретного логарифмирования и поиска сопрягающего элемента и др. Однако, в настоящее время не предложена алгебраическая структура и вычислительно трудная задача, которая позволила бы обеспечить возможность разработки на ее основе всех типов криптосхем, реализуемых в классической двухключевой криптографии.

В качестве алгебраической структуры, на основе которой можно было бы сформировать вычислительно трудную для квантового компьютера задачу, предлагается конечное некоммутативное кольцо векторов со специальной операцией умножения векторов. Результат умножения векторов в этом кольце определяется по правилу перемножения каждой компоненты первого вектора с каждой компонентой второго вектора с последующей заменой в каждом слагаемом произведения пар базисных векторов на однокомпонентный вектор в соответствии с так называемой таблицей умножения базисных векторов [2]. Строкам и столбцам данных таблиц соответствуют базисные вектора, а ячейкам – результат их перемножения. Результатом перемножения является некоторый базисный вектор, умноженный на структурный коэффициент. Структурные коэффициенты принадлежат конечному полю, из которого берутся координаты векторов.

Основной сложностью является построение таблиц умножения базисных векторов со структурными коэффициентами. На первом этапе строится таблица умножения базисных векторов и проверяется её ассоциативность. На втором этапе строится таблица умножения структурных коэффициентов и также проверяется её ассоциативность. В случае, когда обе таблицы оказались задающими ассоциативную операцию, таблица умножения векторов в кольце векторов считается заданной. Ассоциативность требуется, поскольку без неё невозможно использовать алгоритм быстрого возведения в степень, что в свою очередь негативно сказывается на производительности построенных на основе данной алгебраической структуры криптосхем.

Операция автоморфного отображения перестановочна с операцией возведения в степень в некоммутативном кольце векторов со специальной операцией умножения. Поэтому с помощью данной алгебраической структуры возможно построить, в частности, протокол открытого распределения ключей и протокол бесключевого шифрования [3]. В основу предлагаемого протокола положены следующие операции, которые в используемой последовательности задают взаимно коммутативные преобразования, выполняемые отправителем (Алиса) и получателем сообщения (Боб):

- операция автоморфного отображения в некоммутативной группе;
- операция умножения четырехмерных векторов;
- операция умножения вектора на скаляр;
- операция представления заданного вектора в виде произведения случайных векторов.

Заключение. Таким образом, показана принципиальная возможность использования некоммутативного кольца векторов со специальной операцией умножения и операцию автоморфного отображения некоммутативной группы для построения протоколов открытого согласования ключа и открытого шифрования. Одновременное нахождение элемента, с помощью которого выполняется автоморфное отображение и неизвестного показателя степени в явном виде не сводится к задаче дискретного логарифмирования, поэтому построенная алгебраическая структура может претендовать на роль основы для постквантовых протоколов.

СПИСОК ЛИТЕРАТУРЫ

1. Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer // SIAM Journal of Computing. 1997. Vol. 26. P. 1484–1509.
2. Молдовян Н.А. Алгоритмы аутентификации информации в АСУ на основе структур в конечных векторных пространствах // Автоматика и телемеханика. 2008. № 12. С. 163–177.
3. Молдовян Н.А., Абросимов И.К., Ковалева И.В. Постквантовый протокол бесключевого шифрования // Вопросы защиты информации. 2017. № 3 (118). С. 3–13.

УДК 004.451

ПРОГРАММНО-ТЕХНИЧЕСКИЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ЗАДАЧ ЭКСПЛУАТАЦИИ РБД

Нечитайленко Роман Александрович, Новопашин Владимир Сергеевич, Белько Роман Вячеславич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5,
email: rnet2005@ gmail.com; novopashin.vladimir@gmail.com; vvcehanovskiy@mail.ru

Аннотация: Предлагается предварительное исследование функционального назначения и предпочтений пользователей в работе РБД для обеспечения её информационной и программно-аппаратной безопасности. Рассматриваются два основных подхода для реализации РБД: программной поддержки работы с РБД и поддержка БД, распределенных аппаратно.

Ключевые слова: базы данных; распределенные базы данных; информационные технологии; информационная безопасность.

PROGRAM AND TECHNICAL ISSUES OF INFORMATION SECURITY FOR THE OPERATION PROBLEMS OF DDB

Nechitailenko Roman, Novopashin Vladimir, Belyko Roman

The St. Petersburg State Electrotechnical University "LETI",

email: rnet2005@ gmail.com; novopashin.vladimir@gmail.com; vncehanovskiy@mail.ru

Abstract: A preliminary study of functional and user preferences in the work of the RBD to ensure its information and software and hardware security. Discusses the two main approaches for the implementation of DDB: software support for DDB and DB support distributed hardware.

Keywords: *database; distributed databases; information technology; information security.*

Распределенная база данных, как система логически интегрированных и территориально распределенных баз данных (РБД), языковых, программных, технических и организационных средств, предназначена для создания, ведения и обработки информации [1]. Обеспечение информационной безопасности РБД необходимо обеспечить по всем элементам этой интегрированной системы. В качестве самостоятельного направления обеспечения безопасности можно рассматривать решение задач администраторами РБД и реализации режима "клиент-сервер", поддерживаемого предметно-ориентированным сервисным интерфейсом при решении задач обработки данных. Необходимо установить, как решаются программно-технические вопросы обеспечения информационной безопасности для задач эксплуатации РБД, подготавливается функциональный каталог задач проектирования и эксплуатации РБД. Задачами эксплуатации являются: увеличение доступности и производительности системы, что относится к основным принципам организации РБД. Необходимо определить подход к выбору структуры и архитектуры РБД [2], зная, какую задачу обработки данных будет решать некоторая информационная система (ИС). Устанавливается архитектура прикладной ИС и поддерживающей ее РБД. Реализуются два основных подхода для реализации РБД:

Первый подход. Программная поддержка работы с РБД, когда вся БД может быть физически разделена на несколько независимых частей или располагающихся на одном или нескольких серверах. При этом можно выделить архивную БД и БД, требуемую для текущей работы. ИС в таком случае должна автоматически определять, является ли текущая инсталляция распределенной, а также сама осуществлять обмен данными между серверами в режиме реального времени или же с помощью репликации. Для пользователя данной системы наличие РБД не заметно, так как не изменится ни производительность системы, ни её функциональные возможности, но на последующих стадиях доработки задания на курсовое проектирование найдет отражение в разработке интерфейсов и сервисов пользователей.

Второй подход. Поддержка БД, распределенных аппаратно. Рассматривается решение задачи обеспечения параметров доступности и производительности системы. Выбирается техническое решение, которое защитит позицию разработчика БД по размещению БД в структуре системы. Так, например, часть системы, наиболее требовательную к производительности, можно поместить на самые мощные серверы, а оставшуюся же часть поместить на менее производительные, тогда ресурсы основных серверов не будут расходоваться для мелких задач. При этом необходимо правильно сбалансировать нагрузку между серверами. Можно показать несколько схем подключения серверов, выбор между которыми обуславливается планируемой нагрузкой, а также имеющимися ресурсами. В случае, когда имеется один мощный сервер, а второй менее производительный, можно построить «псевдокластер». За счет репликации по расписанию между серверами будет происходить регулярное резервное копирование. При работе же с данным кластером пользователи будут обращаться к более мощному серверу, а если же он будет недоступен – к менее мощному. При этом есть вероятность снижения производительности системы, а также потери части данных, которая не была реплицирована на резервный сервер. Если же серверы одинаковы по мощности, то целесообразно объединить их в настоящий кластер. При использовании механизма балансировки нагрузки необходимо синхронизировать операции записи в базу данных между серверами, при отказе одного из серверов это будет незаметно, так как вся нагрузка перенесется на работающий сервер. Однако, в таком случае так же есть вероятность уменьшения производительности системы.

Серверы кластера могут располагаться в разных сегментах сети, если сеть сегментирована, размещение серверов в разных сегментах сети позволит уменьшить нагрузку на сеть. При высокой нагрузке ИС необходимо строить систему по высокопроизводительной схеме, когда часть системы, требующая больших вычислительных мощностей, располагается на самых мощных серверах, объединенных в первый кластер. Остальная же часть системы располагается на менее мощных серверах, объединенных во второй кластер, содержащий полную реплику всех данных первого. При работе с данной системой обращение идет к первому кластеру, к его наименее загруженному серверу, а при необходимости доступа к архивам – подключается второй кластер. Внутри кластера работает система синхронизации информации между серверами, и между кластерами происходит репликация по расписанию, составленному так, чтобы минимизировать затраты ресурсов первого кластера.

Можно обеспечить выбор режима информационной безопасности РБД под любое решение, показывающее механизмы модификации структуры под параметры доступности и производительности.

Рассмотрение информационной и программно-аппаратной безопасности РБД в контексте предварительной регламентации функциональных аспектов пользователей РБД и конкретной архитектуры информационной системы позволяет установить элементы структуры наиболее подверженные уязвимости и возможных угроз функционирования информационной системы. РБД и их информационного ресурса.

СПИСОК ЛИТЕРАТУРЫ

1. Советов Б.Я., Цехановский В.В., Чертовской В.Д. Базы данных: теория и практика. М.: Юрайт. 2013.-464с.
2. Советов Б.Я., Водяхо А.И., Дубенецкий В.А. Цехановский В.В. Архитектура информационных систем Учебник. М.: Издат. центр «Академия. 2012.-288с.

УДК 004.5

ИСПОЛЬЗОВАНИЕ АЛГОРИТМА ПОИСКА МИНИМАЛЬНОГО ОСТОВНОГО ДЕРЕВА ДЛЯ СРЕДСТВ ВИЗУАЛИЗАЦИИ ИЗОБРАЖЕНИЙ ЗАЩИЩЕННОЙ ОТКАЗОУСТОЙЧИВОЙ КОРПОРАТИВНОЙ ИНФРАСТРУКТУРЫ

Пелевин Максим Сергеевич

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5,
emails: maks.pelevin@gmail.com

Аннотация: Рассматривается технология обработки изображений для создания защищенной отказоустойчивой инфраструктуры. Технология распознавания и обработки изображений использует разработанный алгоритм поиска минимального остовного дерева в задаче сегментации по водоразделам.

Ключевые слова: визуализация изображений; алгоритм Крускала; система непересекающихся множеств; аутентификации пользователей.

USING THE ALGORITHM FIND A MINIMUM SPANNING TREE FOR VISUALIZATION THE IMAGES ARE PROTECTED FAULT-TOLERANT ENTERPRISE INFRASTRUCTURE

Pelevin Maksym

The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
emails: maks.pelevin@gmail.com

Abstract: Discusses the image processing technology to provide a secure resilient infrastructure. Recognition technology and image processing uses the algorithm of finding minimum spanning tree the problem of segmentation of watersheds.

Keywords: Imaging; Kruskal's algorithm; disjoint sets; user authentication.

С использованием средств визуализации изображений для аутентификации пользователей, встали новые задачи создания дополнительных средств обработки, хранения и пересылки изображений и видеоинформации в целом. Во многих корпоративных сетях используются технология распознавания изображений, в том числе, лиц и других биометрических показателей для установления форм доступа к ресурсам корпоративной сети, регистрации обращений к разделам информационных баз данных сети, ведению журналов регистрации обращений пользователя к внутренними и внешним информационным ресурсам. Применение технологий обработки изображений для создания защищенной отказоустойчивой инфраструктуры и включение современных программно-вычислительных и сервисных средств обработки изображений в компьютерное сопровождение корпоративной инфраструктуры, является актуальной современной технической и пользовательской задачей, широко востребованной в области разработок и применений на рынках труда и производства.

В современном мире всё больше систем, которые анализируют изменяющуюся обстановку посредством извлечения информации из графических изображений. Такие системы, например, могут автоматически сканировать лица людей для поиска соответствия их в базе подозрительных людей или людей, находящихся в розыске. Также современные системы умеют анализировать эмоциональное состояние человека, и по определённым маркерам выявлять тех, кто собирается совершить преступление. Такие системы нуждаются в алгоритмах, которые могут в короткое время получать различные сегменты изображения при различном уровне шума на изображении.

Для технологии распознавания и обработки изображений используется алгоритм поиска минимального остовного дерева в задаче сегментации по водоразделам. Изображение определяется как двумерная функция, где на осях — координаты в пространстве (конкретно, на плоскости), и

значение функции которой в любой точке, задаваемой парой координат, называется интенсивностью или уровнем серого изображения в этой точке.

Изображение может быть представлено как связанный полный ненаправленный взвешанный граф, где каждая точка является его вершиной. Для каждого ребра, соединяющего смежные точки изображения заранее можно вычислить её функция. Минимальное остовное дерево будет соединять все вершины таким образом, что сумма весов полученного графа будет наименьшим, чем сумма любого другого остовного дерева, построенного на этом графе. При этом, если убрать на таком дереве все рёбра, вес которых был бы больше заданного уровня, то для конкретного τ получится разбиение изображения на сегменты, аналогичному для решения задачи сегментации по водоразделам. При этом каждый подграф будет являться минимальным остовным деревом для своего сегмента.

Алгоритм Крускала (или Краскала) [1, 2, 3] является одним из алгоритмов поиска минимального остовного дерева. Алгоритм сводится к следующим шагам: сначала множество всех рёбер считается пустым. Далее из всех рёбер данного графа выбирается такое ребро, которое не вызовет в искомом графе появления циклов и при этом имеет минимальный вес. Алгоритм завершается в том случае, когда таких рёбер больше нет. Для работы алгоритма традиционно используют систему непересекающихся множеств (СНМ), поскольку решение задачи о том, будет ли создавать рассматриваемое ребро цикл в уже построенном дереве, легко решается стандартными операциями над СНМ. Для решения этой задачи достаточно найти корневой элемент для каждой из вершин в СНМ. Когда они ссылаются на один и тот же корневой элемент означает, что добавление ребра между этими вершинами приведёт к появлению цикла. Такое ребро исключается из рассмотрения. Оценкой работы алгоритма Крускала является линейно-логарифмическим в зависимости от размеров изображения.

Из-за того, что остовное дерево наращивается, начиная с наименьших весов, задача поиска минимального остовного дерева в алгоритме Крускала повторяет шаги алгоритма сегментации по водоразделам, но в отличие от неё, наращивание сегментов производится одновременно, когда обнаруживается новое ребро этого графа. Классическом вариант наращивает только один сегмент, после чего алгоритм переходит к поиску и наращиванию следующего.

В случае использования персистентной СНМ (ПСНМ) мы получаем возможность определять отдельные сегменты для фиксированного значения, где полученное значение будет соответствовать конкретному значению веса ребра. Если мы знаем порядковый номер веса в упорядоченном по возрастанию списке всех рёбер изображения, из ПСНМ мы получаем информацию о том, на какие именно сегменты было разбито изображение на этом шаге. При этом во всех сегментах не будет рёбер, вес которых бы превышал заданного τ

СПИСОК ЛИТЕРАТУРЫ

1. Белоусов А. И., Ткачев С. Б. Дискретная математика. — М. : МГТУ, 2006. — 744 с.
2. Алексеев В.Е., Таланов В.А. Графы и алгоритмы // Интуит.ру, 2006. Лекция: Жадные алгоритмы и матроиды. Теорема Радона-Эдмондса.
3. Joseph. B. Kruskal. On the Shortest Spanning Subtree of a Graph and the Traveling Salesman Problem. // Proc. AMS. 1956. Vol 7, No. 1. P. 48-50.

УДК 006.72

АЛГОРИТМ ВЫБОРА ОПТИМАЛЬНОГО ВАРИАНТА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Попова Елена Владимировна

Смольный институт РАО,

Россия, Санкт-Петербург, Полжостровский проспект, 59.

emails: serana5@inbox.ru

Аннотация: В статье рассмотрен алгоритм выбора системы защиты информации. Построение алгоритма основано на использовании модели повышения информационной безопасности по критерию конкурентоспособности предприятия.

Ключевые слова: система защиты информации, информационная безопасность, экспертные оценки.

ALGORITHM OF SELECTING THE OPTIMAL VARIANT OF THE INFORMATION SECURITY SYSTEM

Popova Elena

Smol'nyj Institut RAO,

Rossija, Sankt-Peterburg, Poljustrovskij prospekt, 59.

emails: serana5@inbox.ru

Abstract: The article considers the algorithm for selecting the information security system. To build an algorithm based on the use of models increase information security on the criterion of competitiveness of the enterprise.

Keywords: *information security system, information security, expert assessments.*

Введение. Необходимость усиления борьбы с информационной безопасностью вынуждают предприятия выбирать системы защиты информации (СЗИ), оптимально соответствующие сформированным моделям угроз [3], уязвимостей и располагаемым ресурсам предприятия.

Предложенная модель повышения информационной безопасности (ИБ) [2] по критерию конкурентоспособности предприятия объясняет нахождение экстремального значения целевой функции по нескольким критериям. На основе рассмотренной модели алгоритм выбора оптимального варианта СЗИ с использованием минимального значения коэффициента изменения конкурентоспособности составляет последовательность следующих действий:

1. Проектируются нескольких вариантов СЗИ для данного предприятия по схеме формирования СЗИ [2].

2. Подбираются эксперты, и формируется экспертная группа.

3. Вербальные экспертные оценки являются входными данными для нечёткой модели модифицированного метода рандомизированных сводных показателей (ММРСП).

4. Определяются опорные точки лингвистической переменной коэффициента изменения конкурентоспособности (пессимистичные верхние и нижние оценки, интервал наиболее ожидаемых значений).

5. Производится фаззификация [1] входных значений, формирование трапецеидальных функций принадлежности.

6. Формируется набор продукционных правил типа «ЕСЛИ...ТО», отражающих взаимосвязи входных и выходных значений. Выбирается оператор для конъюнктивного условия в продукционных правилах.

7. Производится нахождение функции принадлежности выходного значения по принципу обобщения для функции нескольких переменных.

8. Дефаззифицируется результирующая функция принадлежности на выходе нечёткой модели, и результаты дефаззификации поступают на вход чёткой модели ММРСП.

9. Решается многокритериальная оптимизационная задача на основе рандомизации вектора весовых коэффициентов и оценки сводных показателей.

10. Определяются теоретическое значение коэффициента изменения конкурентоспособности и оптимальный вариант СЗИ.

После выбора оптимального варианта СЗИ, производится его реализация, а затем сопровождение.

Заключение. Выбор оптимального варианта СЗИ является одной из самых актуальных проблем построения адекватных защитных мер для борьбы с современными вызовами нарастания активности киберпреступлений.

СПИСОК ЛИТЕРАТУРЫ

1. Заде Л. Понятие лингвистической переменной и его применение к принятию приближённых решений -Мж МИР, 1976-165с.
2. Попова Е. В. Метод выбора системы защиты информации с учётом критерия конкурентоспособности предприятия // Информационно-управляющие системы. – 2016. – № 6 (85). – С. 85-90.
3. Федеральная служба по техническому и экспертному контролю 15 февраля 2008 г. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. URL: <http://fstec.ru/component/attachments/download/289> (дата обращения 18.06.16).

УДК 004.056.53

ЭЛЕКТРОННЫЕ ПОДПИСИ СТРУКТУРИРОВАННЫХ ХРАНИЛИЩ ДАННЫХ

Романова Юлия Николаевна, Янюшкин Константин Александрович
Государственный университет морского и речного флота им. адм. С.О. Макарова,
Россия, г. Санкт-Петербург, ул. Двинская 5/7,
emails: romanovaiuli@gmail.com, kayahidden@gmail.com

Аннотация: В статье рассматривается задача формирования блоков данных для вычисления дайджеста структурированных хранилищ информации большого размера, а также размещения сформированных электронных подписей в этих хранилищах. Описаны свойства предложенного подхода, который позволяет хранить подписи в виде древовидной структуры (с учетом порядка их формирования), которая позволяет последующее добавление данных и электронных подписей в хранилище.

Ключевые слова: *электронная подпись; структурированное хранилище; сплошное файловое хранилище; crypto api; потоки данных; дайджест; хэширование данных.*

DIGITAL SIGNATURES OF STRUCTURED DATA STORAGE

Romanova Yuliya Nikolaevna, Yanyushkin Konstantin Aleksandrovich
Admiral Makarov State University of Maritime and Inland Shipping,
Russia, St. Petersburg, Dvinskaya str. 5/7,
emails: romanovaiuli@gmail.com, kayahidden@gmail.com

Abstract: This paper provides one of possible ways of forming data blob from big data storage with serial access for hashing function to form digital signature. Also, we describe the way of storing digital signatures of data parts inside of these storages, which allow to keep tree structure of signatures sequences and add subsequent data to storage.

Keywords: digital signature; structured storage; big data storage; crypto api; data stream; data hashing.

Введение. На современных предприятиях водного транспорта вся циркулирующая в них информация представлена в виде документов. Согласно российскому законодательству, электронные документы, при соблюдении определённых законодательных норм, могут использоваться как для сообщения юридических и физических лиц с государственными органами, так и между собой. Ведение архива последовательности обмена данными, подписанными электронными подписями в сложных конфигурациях согласования документов в современной бизнес-логике, является не очевидной задачей с ростом скорости обработки и числа обрабатываемых документов.

Архив может быть представлен как последовательный поток данных, который разворачивается в древовидную структуру, похожую на структуру каталогов современных файловых систем [1]. Структура хранилища с подписью имеет вид непрерывной битовой последовательности, хранящейся на физическом носителе. Логически, корневое хранилище состоит из суб-хранилищ, и потоков данных. Каждое суб-хранилище имеет имя и свойства, а также, в свою очередь, само является хранилищем, тем самым обеспечивая древовидную структуру данных. Поток имеет имя и свойства и хранит в себе последовательность неформатированных данных. Для создания электронной подписи текущего состояния хранилища необходимо рекурсивно обойти все его элементы, представив их свойства и их содержание в виде последовательности по заранее определённой схеме, которая будет использоваться при проверке [2], [3]. Для хранения контейнеров подписей в корневом хранилище создаётся суб-хранилище с зарезервированным именем, содержимое которого не является субъектом для формирования дайджеста данных. Это суб-хранилище содержит лишь потоки, содержащие закодированные в открытом формате контейнеры с электронными подписями. Процесс формирования подписи будет производиться с использованием сертификата, который содержит открытый ключ электронной подписи, а также сведения о владельце сертификата и удостоверяющем центре, который его изготовил. Помимо сформированной подписи в контейнер с подписью добавляются все сертификаты цепочки доверия, а также идентификаторы используемых алгоритмов проверки и формирования подписи. Такая структура устойчива к любым изменениям данных хранилища, в том смысле, что подпись, расположенная после последовательности данных, при изменении этих данных становится невалидной (как и при изменении самого контейнера подписи), при этом оставляя возможность добавлять данные расположенные после неё, оставляя их свободными к изменению до добавления последующей электронной подписи [4]-[6].

Заключение. Предложенная схема позволяет работать с последовательными хранилищами очень больших объёмов, содержащими древовидную структуру данных, которые могут быть подписаны последовательностью электронных подписей по мере заполнения.

СПИСОК ЛИТЕРАТУРЫ

1. Черняков А.В. Алгоритмы резервного копирования / Черняков А.В., Нырков А.П. // Материалы работы III научно-исследовательской конференции студентов и аспирантов факультета информационных технологий. «IT: ВЧЕРА, СЕГОДНЯ, ЗАВТРА – 2014» 19 декабря 2014 г. – СПб.: ГУМРФ имени адмирала С.О. Макарова, 2015. – С. 129–133.
2. Guntheroth K. Optimized C++: Proven Techniques for Heightened Performance [Книга]. - California (USA): O'Reilly Media Inc., 2016.
3. Summerfield M. Advanced Qt Programming: Creating Great Software with C++ and Qt 4 [Книга]. - London, England: Pearson Education (UK), 2016.
4. Сабанов А. Г. Скиба В. Ю., Некоторые аспекты защиты электронного документооборота [Журнал] // Проблемы информационной безопасности. Компьютерные системы. - 2012 г. №2 стр. 42-45.
5. Bukharmetov M.R. Robust Method for Protecting Electronic Document on Waterway Transport with Steganographic Means by Embedding Digital Watermarks into Images / M. R. Bukharmetov, A. P. Nyrkov, S. S. Sokolov, S. G. Chernyi, V. N. Kuznetsov, D. G. Mamunts // Proceedings of the 16-th Conference on Reliability and Statistics in Transportation and Communication, RelStat'2016, 19-22 October, Procedia Engineering 178, 2017. – С. 507 – 514. DOI: 10.1016/j.proeng.2017.01.097
6. Зима В.М. Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий [Книга]. - СПб. : БХВ-Петербург, 2003. - стр. 368. - ISBN: 5-94157-213-1.

УДК 0004.75

БЛОКЧЕЙН ДЛЯ ГЕОТЕГИРОВАНИЯ ПЕРИМЕТРА БЕЗОПАСНОСТИ

Рыжков Сергей Романович

Санкт-Петербургский институт информатики и автоматизации РАН,

Россия, Санкт-Петербург, 14 линия, 39

email: Ryzhkov@ias.spb.su

Аннотация: в статье рассмотрены возможности новой технологии блокчейн применительно к гарантированному хранению геометок с целью создания периметра безопасности

Ключевые слова: блокчейн; геометки; периметр

THE BLOCKCHAIN FOR SECURITY PERIMETER GEOTAGGING

Ryzhkov Sergey

The St. Petersburg Institute for Informatics and Automation of RAS,
Russia, St. Petersburg, 14-ya liniya V. O., 39
email: Ryzhkov@iias.spb.su

Abstract: The article presents how the blockchain technology can be used to create the guaranteed geotag storage to build a trusted security perimeter

Keywords: *blockchain; geotagging; perimeter*

Применение совокупности технологий геотегирования и блокчейн позволяет создать доверенный периметр, контролировать перемещаемые данные. «Геотегирование» представляет собой процесс определения, создания и инициализации набора объектов геолокации стационарного вычислительного устройства. Актуальным применением геотега является обеспечение соблюдения пограничного контроля на основе геотегов в концепции, называемой «геозаслон» [1]. Блокчейн можно представить, как информационную сеть нового поколения, которая базируется на уникальной единице хранения информации — транзакции. Уникальность технологии связана с тем, что эффект «сцепления» обуславливает зависимость каждого отдельного блока от всех блоков, обработанных перед ним, а не только от предыдущего блока, а распределённо хранимая база исключает возможность фальсификации. Блокчейн позволяет идентифицировать любые нуждающиеся в идентификации Сущности, т.е. данные геолокации стационарного вычислительного устройства (например, межсетевого экрана) хранящиеся в распределённой блокчейн базе можно считать верифицированными. Созданный за счёт геотегирования доверенный периметр возможно дополнить функцией контроля перемещения данных за счёт криптографического опечатывания данных (при выходе за пределы периметра геометок данные не читаемы).

Для РФ технология блокчейн конкурентно важна. Важно отметить уникальную возможность РФ для внедрения технологии блокчейн, она обусловлена следующими факторами:

1. Необходимость развития собственной независимой платёжной системы;
2. Наличие собственных, национальных криптографических алгоритмов (ГОСТ Р 34.11-2012(стрибог)) [2];
3. Контроль за лицензируемой деятельностью в области криптографии со стороны государственного регулятора;
4. Распределённая сеть аккредитованных удостоверяющих центров, которые могут выступать в роли гарантированных «майнеров» (поиск новых блоков, формирование хеш-последовательностей и майнинг-верификация блоков).

Всё вышеперечисленное может стать основой внедрения отечественной технологии блокчейн при условии сотрудничества между операторами, разработчиками и регуляторами.

Технология блокчейн, а точнее база транзакций содержащая данные геолокации стационарного вычислительного устройства может быть применена в системах подтверждения состояния рабочих станций, работающих в реальном времени, по начальному (проверенному или доверенному) состоянию системы строится ХЭШ, который сравнивается с ХЭШ нового состояния. В таких системах единожды проверив программно-аппаратное обеспечение в любой момент времени, можно убедиться, что в эталонное состояние не было внесено изменений [3]. Более того, построенный таким образом периметр позволяет картографировать исходное состояние объекта информатизации, чтобы затем иметь возможность контролировать перемещение данных мобильными пользователями. Для этого каждый мобильный пользователь, оснащается средствами глобального позиционирования и средствами криптографической защиты информации. С определённой периодичностью мобильное устройство передаёт данные о своём местонахождении на сервер доступа и получает авторизацию, право на работу с данными. В случае выхода за пределы периметра данные блокируются. Для усиления защиты данных они могут храниться благодаря высокой фрагментации множества географически распределённых репликаций, а также благодаря использованию особого метода кодирования в момент записи, что позволяет гарантированно восстановить данные при аппаратном сбое. Логика хранения реализуется шлюзами, осуществляющими фрагментацию, распределение по удалённым серверам хранения и выполнение обратной операции сборки данных в единое целое из фрагментов с коррекцией в случае обнаружения ошибок [4].

Через механизм аттестационного протокола геотегируемая информация (сформированная на этапе конфигурации сервера) сохраняется в виде зашифрованного хеш-значения в аппаратном криптографическом модуле BIOS (АМД3 – АППАРАТНЫЙ МОДУЛЬ ДОВЕРЕННОЙ ЗАГРУЗКИ). Для обеспечения ограничений геолокации перед развертыванием и миграцией рабочей нагрузки запускается мониторинг геолокации. АМД3 в защите периметра выполняет следующие функции:

1. подтверждение данных геолокации;
2. применение ограничений геолокации;
3. запуск мониторинга геолокации

и специфически служит для гарантированного доверенного хранения, мониторинга и аудита за счет использования содержащегося в аппаратной части криптопроцессора, обеспечивающего средства безопасного создания ключей шифрования (с той же степенью неповторяемости, что и генератор случайных чисел), а также средства ограничения использования ключей (как для подписи, так и для шифрования/дешифрования). Модуль АМДЗ также используется для подтверждения подлинности аппаратных средств за счет уникальности специфических устройств, что делает возможным однозначное установление подлинности доверенной платформы [3].

Сервер доступа и мобильные устройства, находящиеся внутри периметра, обмениваются сессионными ключами, позволяющими авторизовать устройство для доступа к данным. Сессионный ключ имеет дополнительный идентификатор периметра, в котором разрешено обрабатывать данные.

СПИСОК ЛИТЕРАТУРЫ

1. Воробьев В. И., Рыжков С. Р., Фаткиева Р. Р. Защита периметра облачных вычислений // Программные системы: теория и приложения. – 2015. – Т. 6. – №. 1-1. – С. 61-71.
2. <http://protect.gost.ru/document1.aspx?control=31&id=180209>
3. Руднев Д. О., Сычугов А. А. МЕТОД ПОВЫШЕНИЯ ДОВЕРИЯ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ // Известия Тульского государственного университета. Технические науки. – 2016. – №. 11-1.
4. Черняк Л. Хранилище данных на кодах Риди-Соломона // Открытые системы. СУБД. – 2012. – №. 2. – С. 52-52.

УДК 004.7.056.53

АУДИТ СЕТЕВОЙ БЕЗОПАСНОСТИ

Садикова Анастасия Александровна, Титова Юлия Алексеевна, Савков Сергей Витальевич
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, пр-кт Кронверкский, 49
emails: nastya.sadkoo@mail.ru, titova.yulishna@mail.ru, sergsavkov@gmail.com

Аннотация: Со временем сетевая инфраструктура усложняется, расширяются виды приложений и данных. Все эти изменения приводят к тому, что при осуществлении системы информационной безопасности, пользователь может не заметить некоторые уязвимости сети. В связи с этим необходимо проведение регулярного аудита безопасности. В данной статье обобщены виды аудита сетевой безопасности, рассмотрены методологии IAM и SAFETAG, а также особенности их проведения. Приведена краткая характеристика некоторых сканеров уязвимостей. Сделан вывод о том, что, хотя аудит безопасности и носит рекомендательный характер, он является необходимым для обеспечения целостности и конфиденциальности персональных данных людей, так или иначе связанных с организацией.

Ключевые слова: аудит, тест на проникновение, сканеры уязвимостей, методология аудита, SAFETAG, IAM, сетевая безопасность, международные стандарты безопасности.

NETWORK SECURITY AUDIT

Sadikova Anastasia, Titova Yulia, Savkov Sergei
Saint Petersburg National Research University of Information Technologies, Mechanics and Optics «ITMO»,
Russia, St. Petersburg, Kronverkskiy prospekt, 49
emails: nastya.sadkoo@mail.ru, titova.yulishna@mail.ru, sergsavkov@gmail.com

Abstract: Over time, the network infrastructure becomes more complex, the types of applications and data expand. All these changes lead to the fact that when implementing an information security system, a user may not notice some network vulnerabilities. In this regard, it is necessary to conduct a regular security audit. This article summarizes the types of network security audit, examines the methodologies of IAM and SAFETAG, as well as specifics of their conduct. A brief description of some vulnerability scanners is given. It is concluded that, although the security audit is advisory in nature, it is necessary to ensure the integrity and confidentiality of the personal data of people in one way or another related to the organization.

Keywords: audit, penetration testing, vulnerability scanners, audit methodology, SAFETAG, IAM, network security, international safety standards.

Введение. В современном мире сетевая безопасность имеет колоссальное значение. Под сетевой безопасностью понимают комплекс требований, которые предъявляются к инфраструктуре компьютерной сети, при выполнении которых обеспечивается защита сетевых ресурсов от несанкционированного доступа и эффективное функционирование сети в целом. Одной из задач организации является предоставление своим сотрудникам безопасного доступа к сетевым ресурсам в любое время. Для решения задачи безопасности сети на предприятии проводят аудит сетевой безопасности. В коммерческих организациях руководство озабочено обеспечением безопасности своих активов, поэтому понимает важность проведения аудита. В некоммерческих организациях (далее – НКО) аудиту уделяется намного меньше внимания. Такое пренебрежение чревато тем, что

персональные данные граждан, которые по ряду причин обратились в конкретную НКО, а также сотрудников, работающих в данной НКО, могут попасть в руки злоумышленников. Аудит безопасности информационных систем — это их проверка, тестирование, которое должно выявить потенциальные опасности и уязвимости в защите. При этом используется принцип сравнения результатов теста с неким идеалом, установленным целями аудита, а также личным опытом самого аудитора. При этом должно учитываться множество самых разнообразных факторов, в том числе и информация о компании: область её деятельности, размер фирмы и прочее [1]. Целями проведения аудита безопасности являются:

- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов информационной системы (далее — ИС);
- оценка текущего уровня защищенности ИС;
- локализация узких мест в системе защиты ИС;
- оценка соответствия ИС существующим стандартам в области информационной безопасности;
- выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.

Существует три вида аудита:

- Активный аудит;
- Экспертный аудит;
- Аудит на соответствие стандартам.

Экспертный аудит можно условно представить, как сравнение состояния информационной безопасности с «идеальным» описанием. Результаты экспертного аудита могут содержать разноплановые предложения по построению или модернизации системы обеспечения информационной безопасности.

Суть аудита на соответствие стандартам наиболее приближена к тем формулировкам и целям, которые существуют в финансовой сфере — при проведении данного вида аудита состояние информационной безопасности сравнивается с неким абстрактным описанием, приводимым в стандартах.

Заключение. Аудит как средство защиты информации носит сугубо рекомендательный характер, другими словами, эта процедура не привносит изменений в саму систему. Однако анализ полученных данных позволяет говорить о мерах защиты от несанкционированного доступа к конфиденциальным ресурсам. Сканеры безопасности охватывают довольно обширную сферу проблем, поэтому благодаря их использованию можно не только искать уязвимые программы в сети, но и изменять политику безопасности, реагируя на обнаруженные проблемы [2]. При планировании проверки состояния системы информационной безопасности важно не только точно выбрать вид аудита, исходя из потребностей и возможностей компании, но и не ошибиться с выбором исполнителя. Результаты любого вида аудита содержат рекомендации по модернизации системы обеспечения информационной безопасности. Если аудит проводит консалтинговая компания, которая кроме консалтинговой деятельности занимается еще и разработкой собственных систем защиты информации, она, по понятным причинам, заинтересована в том, чтобы результаты аудита рекомендовали организации использовать её продукты. Для того чтобы рекомендации на основе аудита были действительно объективными, необходимо, чтобы компания-аудитор была независима в выборе используемых систем защиты информации и имела большой опыт работы в области информационной безопасности [3].

СПИСОК ЛИТЕРАТУРЫ

1. Кравчук Д. И., Коркушко Д. А. Аудит безопасности корпоративных информационных систем // Молодой ученый. — 2015. — №10. — С. 697-700.
2. Обзор бесплатных инструментов для аудита web-ресурсов и не только. [Электронный ресурс]. — Режим доступа: <https://habrahabr.ru/post/125206/>, свободный. Яз. рус. (дата обращения 26.12.2016)
3. Аудит безопасности: когда и чем проводить? // CNews — Издание о высоких технологиях. [Электронный ресурс]. — Режим доступа: http://www.cnews.ru/articles/audit_bezopasnosti_kogda_i_chem_provodit_ свободный, Яз. рус. (дата обращения 26.12.2016)

УДК 004.056

СТЕГАНОГРАФИЯ КАК АЛЬТЕРНАТИВА КРИПТОГРАФИИ

Соколов Сергей Сергеевич, Ревера Галина
ГУМРФ имени адмирала С.О. Макарова
Россия, Санкт-Петербург, Двинская, 5/7
emails:sokolovss@gumrf.ru, reveragm@gumrf.ru

Аннотация: В статье рассматривается задача возможного сокрытия информации и ее дальнейшее нахождение. Рассмотрены различные утилиты для реализации данных задач.

Ключевые слова: *стеганография, стеганоанализ, сокрытие информации.*

STEGANOGRAPHY AS AN ALTERNATIVE TO CRYPTOGRAPHY

Sokolov Sergey Sergeevich, Revera Galina
GUMRF named after Admiral S.O. Makarova
Russia, St. Petersburg, Dvinskaya, 5/7
emails: sokolovss@gumrf.ru, reveragm@gumrf.ru

Abstract: The article deals with the problem of possible concealment of information and its continued presence. Reviewed various tools to implement these tasks.

Keywords: *Steganography, Steganalysis. hiding information.*

Стеганография — это междисциплинарная наука и искусство передавать сокрытые данные, внутри других, не сокрытых данных.

В цифровой стеганографии электронные коммуникации могут включать стеганографическое кодирование внутри транспортного слоя, например, файл документа, файл изображения, программу или протокол [1]. Файлы мультимедиа идеально подходят для стеганографической передачи из-за их большого размера. Например, отправитель может начать с безобидного файла изображения и настроить цвет каждого 100-го пикселя, чтобы соответствовать букве в алфавите, изменение настолько тонкое, что кто-то кто не специально ищет, вряд ли заметит его.

Преимущество стеганографии над криптографией состоит в том, что предполагаемое секретное сообщение не привлекает к себе внимание как объект изучения, в то время как криптография-это практика защиты содержимого одного сообщения, стеганография занимается, скрывая тот факт, что секретные сообщения, а также сокрытие содержания сообщения. Существуют различные методы сокрытия информации: в текстовых файлах, методы шифровки в аудио/видео файлах, а также, методы сокрытия информации в графических файлах [2]-[4].

В стеганографии можно выделить три уровня защиты:

1. Неизвестен факт обмена информацией;
2. Неизвестен ключ, с помощью которого сокрыта информация;
3. Неизвестен алгоритм шифрования.

Стеганографию используют на протяжении 2000 тысяч лет. Ее используют в военных, дипломатических, интеллектуальных и личных целях. С каждым годом появляется все больше и больше утилит для сокрытия информации. Например, Anubis позволяет скрыть текстовую информацию внутри картинки и аналогичная ей программа DeEgger Embedder, DeepSound, как видно из названия, скрывает секретные данные в аудиофайлы — wave и flac, Hallucinate (v. 1.2), Steganography Tools может скрыть информацию в графическом или звуковом файле и многие другие.

В вычислениях стеганографически закодированное обнаружение пакетов называется стеганолизом. Однако самый простой способ обнаружения измененных файлов - сравнить их с известными оригиналами. Например, для обнаружения информации, перемещаемой через графику на веб-сайте, аналитик может поддерживать известные чистые копии этих материалов и сравнивать их с текущим содержанием сайта. Различия, если предположить, что перевозчик один и тот же, составляют полезную нагрузку. В целом, использование сверхвысоких скоростей сжатия затрудняет стеганографию, но не делает ее невозможной. Ошибки сжатия обеспечивают укрытие данных, но высокое сжатие уменьшает объем данных, доступных для хранения полезной нагрузки, повышая плотность кодирования, что облегчает обнаружение (в крайних случаях, даже при случайном наблюдении).

Параллельно с быстрым развитием программ для сокрытия информации развиваются и программы для ее обнаружения в контейнерах (информация, в котором стеганографическим алгоритмом скрыто сообщение). Например, Stegdetect, которая очень эффективна против большинства стеганографических программ. Stegdetect сначала проверяет доступные хранилища: поля-комментарии и поля расширений различных форматов файлов, наличие искусственно созданных изображений, а также изображений с большим количеством участков однотипной заливки. Программа сравнивает частоту распределения цветов для возможного носителя скрытой информации и теоретически ожидаемую частоту распределения цветов для файла-носителя скрытой информации. Так же существует множество программ, которые работают с популярным алгоритмом стеганографии «Метод наименее значащих битов».

Данная область изучения является новой, но быстрой в развитии, потому что стеганография является надежным способом сокрытия информации на сегодняшний день. Да, у данного метода сокрытия информации есть и плюсы, и минусы, но даже это не мешает стеганографии набирать популярность в сферах, где необходимо защитить информацию [5].

СПИСОК ЛИТЕРАТУРЫ

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. — М.: Солон-Пресс, 20002 — 274 с.
2. Быков С.Ф. Алгоритм сжатия JPEG с позиций компьютерной стеганографии // Защита информации. Конфидент. 2000. № 3.

3. Bukharmetov M.R. Robust Method for Protecting Electronic Document on Waterway Transport with Steganographic Means by Embedding Digital Watermarks into Images / M. R. Bukharmetov, A. P. Nyrkov, S. S. Sokolov, S. G. Chernyi, V. N. Kuznetsov, D. G. Mamunts // Proceedings of the 16-th Conference on Reliability and Statistics in Transportation and Communication, RelStat'2016, 19-22 October, Procedia Engineering 178, 2017. – С. 507 – 514. DOI: 10.1016/j.proeng.2017.01.097
4. Бухарметов М.Р. О защите электронного документооборота на основе технологий скрытой связи / Бухарметов М.Р., Нырклов А.П. // Материалы работы IV научно-исследовательской конференции студентов и аспирантов Института водного транспорта. «IT: ВЧЕРА, СЕГОДНЯ, ЗАВТРА – 2014» 11 декабря 2015 г. – СПб.: ГУМРФ имени адмирала С.О. Макарова, 2016. – С. 56–59.
5. James C. Judge, —Steganography: Past, Present, Futurell GSEC Version 1.2f SANS Institute InfoSec Reading Room 2001.

УДК 004.8

КОМПЛЕКСНАЯ СИСТЕМА ИНЖЕНЕРНО ТЕХНИЧЕСКОЙ ЗАЩИТЫ КАБИНЕТА РУКОВОДИТЕЛЯ. ЭФФЕКТИВНОСТЬ РАБОТЫ ПРИБОРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ КОМПЛЕКСНОЙ СИСТЕМЫ ИНЖЕНЕРНО ТЕХНИЧЕСКОЙ ЗАЩИТЫ КАБИНЕТА РУКОВОДИТЕЛЯ

Фаязов Кобилджон Абдукаюмович

Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский проспект 49,
email: kobil93@mail.ru

Аннотация: В статье рассмотрены системы защиты информации, также эффективность используемых приборов, различные вопросы инженерно-технической защиты информации также предпринята попытка систематизировать большой объем часто противоречивых сведений по инженерно-технической защите информации.

Ключевые слова: *защита кабинета; руководитель; защита информации; средства защиты.*

INTEGRATED SYSTEM OF ENGINEERING AND TECHNICAL PROTECTION OF THE MANAGER'S OFFICE. THE EFFECTIVENESS OF THE WORK OF INFORMATION SECURITY DEVICES ON THE EXAMPLE OF AN INTEGRATED SYSTEM OF ENGINEERING AND TECHNICAL PROTECTION OF THE MANAGER'S OFFICE

Fayazov Kobiljon Abdukayumovich

Russia, St. Petersburg, University of ITMO, Kronverkskiy prospect 49;
email: kobil93@mail.ru

Abstract: The article considers information security systems, also the efficiency of the devices used, various issues of engineering and technical protection of information, an attempt is also made to systematize a large volume of often contradictory information on engineering and technical protection of information.

Keywords: *protection of the cabinet; leader; data protection; protection devices.*

Введение. Разработанная система рассмотрена в пределах одного помещения - кабинета руководителя предприятием. Изложены основные сведения, которые требуются для организации такой защиты. Среди них и теоретическая база, и практические решения информационной безопасности такие как: выявление каналов утечки информации и их защита, способы несанкционированного доступа и их предотвращение, модели угроз и приемы их реализации. Предложены средства защиты информации от прослушивания и скрытого видеонаблюдения.

Данная статья актуальна для любых организаций, имеющих конфиденциальную информацию, разработана с ориентацией на инженерно - техническую защиту информации в кабинете руководителя.

Достоинством работы является ее комплексность: решены все вопросы, которые возникают при разработке системы инженерно - технической защиты, предлагаемые решения по инженерно - технической защите кабинета руководителя могут быть использованы для любой организации, как в государственных, так и в частных.

Одно из средств которое использовалось это PTRD 018 (Portable tape recorder detector) - стационарная микропроцессорная система для охраны помещений от несанкционированного использования портативных звукозаписывающих устройств (ПЗУ) - диктофонов и им подобной аппаратуры.

PTRD 018 предназначен для обнаружения скрытой записи на ПЗУ переговоров, ведущихся в Вашем офисе. Используя систему Вы будете знать о наличии в офисе включенного диктофона, времени и месте его включения. Этот прибор достаточно эффективен, но также имеет в свою очередь минусы такие как: PTRD 018 снят с производства, учитывая это его трудно будет содержать в работоспособном режиме, и производить монтаж в случае поломки; еще один из недостатков - это то, что прибор направлен для обнаружения только ленточных диктофонов, а в наше время в большинстве случаев используют цифровые диктофоны.

Широко распространены способы съёма акустической информации, реализуемые с помощью внедрения в контролируемое помещение закладочных устройств: диктофонов, микрофонных устройств с передачей акустической информации по радиоканалу (радиомикрофонов) или по проводным линиям.

Для предотвращения утечки информации по данному каналу прибегаем в помощи активных систем зашумления, но сталкиваемся с печальной действительностью, очень много типов активных систем зашумления, не способных обеспечить комфортные условия работы в защищаемом помещении. Требуемый для надёжной маскировки речи уровень помехи оказывается настолько большим, что шум в помещении начинает превышать «комфортный» уровень, а в ряде случаев - и санитарные нормы по акустическому воздействию на человека.

Также в статье рассмотрена эффективность ряда приборов...

Заключение. Точно также, способы защиты информационных ресурсов должны представлять собой целостный комплекс защитных мероприятий, планирование которых рассмотрено в третьей главе. Разумеется, это не полный перечень, поскольку каждый руководитель решает какие методы и средства защиты необходимо использовать применительно к данному объекту, что зависит от функций, выполняемых объектом, а также от его экономических соображений. Таким образом, главной целью данного дипломного проекта была разработка комплексной системы защиты информации

СПИСОК ЛИТЕРАТУРЫ

1. Торокин А. А. Инженерно-техническая защита информации. — М.: Гелиос АРВ, 2005.
2. Хорев А. А. Способы и средства защиты информации. — М.: МО РФ, 1998. Волокитин А.В., Манюшкин А.П., Солдатенков А.В., Савченко С.А., Петров Ю.А. Информационная безопасность государственных организаций и коммерческих фирм. - Справочное пособие (под общей редакцией Реймана Л.Д.) М: НТЦ «ФИОРД-ИНФО», 2002г.-272с.



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

УДК 004.7

АНАЛИЗ ОСНОВНЫХ ВИДОВ ТРАФИКА В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ И ОЦЕНКА ЕГО ЧУВСТВИТЕЛЬНОСТИ К ПОКАЗАТЕЛЯМ КАЧЕСТВА ОБСЛУЖИВАНИЯ

Власова Дарья Николаевна, Баглай Валерия Витальевна, Апарина Елена Юрьевна
Военная академия связи им. Маршала Советского Союза С.М. Буденного,
Россия, Санкт-Петербург, пр. Тихорецкий 3.
emails: vlasowa.d@yandex.ru

Аннотация: Проведен анализ основных видов трафика в информационно – телекоммуникационных сетях. Дана оценка чувствительности трафика к показателям качества обслуживания.

Ключевые слова: трафик, качество обслуживания, потери, задержки.

ANALIS IS OF THE MAIN TYPES OF TRAFFIC IN INFORMATIONTELECOMMUNICATION NETWORKS AND TO EVALUATE IT IS SENSITIVITY TO THE QUALITY OF SERVICE INDICATORS

Vlasova Darya Nikolaevna, Baglay Valeria Vitalievna, Aparina Elena Yurievna
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny,
Russia, St. Petersburg, Tikhoretsky avenue 3,
emails: vlasowa.d@yandex.ru

Annotation: The analis is of the main types of traffic in information telecommunication networks. The evaluate it is sensitivity to the quality of service indicators.

Keywords: traffic, quality of service, losses, delays.

Введение. На сегодняшний день сети связи и системы телекоммуникации находятся в фазе активной модернизации и совершенствования. Связано это, в первую очередь, с расширением спектра услуг связи и увеличением количества пользователей. В связи с этим возникает необходимость обеспечения требуемого качества обслуживания потоков данных новых услуг связи на ряду с передачей служебного управляющего трафика. Этот факт требует особого внимания при исследовании и модернизации сетей связи, которые предназначены для решения задач в реальном времени. В предложенной работе представлен краткий обзор основных видов трафика, и оценка его чувствительности к различным показателям качества обслуживания

Анализ основных руководящих документов по связи показал, что на сегодняшний день пользователями наиболее востребованы следующие группы услуг:

- услуги пакетной телефонной связи (ПТС);
- услуги видеотелефонной связи (ВТС), видеоконференцсвязи (ВКС), потоковое видео;
- услуги обмена документированной информацией (это обмен электронной корреспонденцией, передача телеграфной и факсимильной информации), а также файловый обмен (картографической, фото информацией, базы данных);
- служебный управляющий трафик (данные систем реального времени, у которых сообщения содержат информацию небольшого объема критичную к задержкам (сигналы управления технологическими процессами, сенсорные сети и т.п.)).

В связи с этим весь трафик в сетях связи можно условно разделить на четыре категории:

- речевой трафик;
- трафик видеоданных (ВКС, потоковое видео);
- трафик данных (текстовое, фото, картографические данные и т.п.);
- служебный управляющий трафик;

Каждому типу трафика требуется свой, определенный уровень качества обслуживания.

Речевой трафик:

Речевой трафик чувствителен к временным параметрам, особенно при двунаправленной передаче. Приемная оконечная станция должна получать битовый поток с той же скоростью, с которой пользователь-отправитель посылает его в сеть. Время задержки передачи не должно превышать 25 мс (в соответствии с рекомендацией G.164). При большей задержке необходимо применение

эхоподавителей, что позволяет допускать $t_{\text{зад}} > 25$ мс, но не более 500 мс. При большем времени передачи интерактивность диалога становится затруднительной.

Избыточность человеческого голоса позволяет при передаче речи допускать незначительные ошибки в битовом потоке (10^{-7}) и вероятность потери пакета $P_{\text{пот}} = 10^{-3}$ и такую же величину засылки не по адресу.

Для передачи речи в цифровом виде требуется пропускная способность 64 Кбит/с. Различные методы уплотнения позволяют представить полный битовый поток 64 Кбит/с меньшим числом битов (до 10 - 20 Кбит/с) и использовать переменную скорость передачи.

Трафик видеоданных:

Для передачи видеопотока характерна постоянная скорость передачи, значение которой зависит от числа пикселей в кадре и количества информации для предоставления каждого пикселя (бит на пиксель) и варьируется от единиц до сотен Мбит/с.

Видеоинформация должна передаваться по сети и приниматься в конечной точке со скоростью, позволяющей воссоздать исходные кадры и воспроизводить их с постоянной скоростью, отсюда возникают требования к временным параметрам задержки: время задержки до 100-150 мс; отклонение времени задержки от среднего значения (джиттер) до 50 мс. Требования к передаче интерактивного видеопотока и потокового видео отличаются.

Для интерактивного трафика предъявляются следующие требования: потери должны быть не более 1%; время задержки должно быть не более 30мс; минимально гарантированная полоса пропускания должна быть равна размеру сессии видео конференции +20%.

Поток видеоданных обладает большой избыточностью, которую снижают с помощью различных методов уплотнения. В этом случае видеоинформация становится более чувствительной к ошибкам и потерям данных, так потери должны быть менее 2%, а так как качество передачи видеоинформации очень чувствительно ко времени передачи, механизмы выявления и коррекции ошибок не применяются. Видеосигнал лучше воспроизводить со всеми искажениями, чем создавать задержки, выявляя ошибки и выполняя повторную передачу.

Трафик данных:

Можно сказать, что трафик данного вида характеризуется большой чувствительностью к потерям, поскольку несет точную информацию – это сегменты баз данных, буквенно-цифровые материалы, а также различные виды программного обеспечения. Однако, приложения, осуществляющие передачу трафика данных, используют протокол транспортного уровня ТСР, который имеет механизмы восстановления потерянных и ошибочно принятых данных. Что полностью компенсирует чувствительность к потерям. Наиболее критичным для данного вида трафика является пропускная способность линий связи.

Трафик данных менее чувствителен и к задержкам, даже в тех случаях, когда передача данных должна осуществляться в реальном времени, однако рекомендуемая пропускная способность линий связи должна быть не ниже 1 Мбит/с.

Служебный управляющий трафик

Требования по обмену служебным управляющим трафиком (короткие сообщения - сообщения размером до 100 Кбайт, которые необходимо доставлять за требуемое время с заданной вероятностью), содержащими информацию реального времени, которая с течением времени быстро обесценивается. Временные ограничения составляют несколько секунд, при больших потерях статистические данные теряют адекватность.

Заключение. Проведенный краткий анализ в данной работе, показал, что каждый из видов трафика чувствителен к различным показателям качества обслуживания. Которые, кроме того являются противоречивыми. Так, например, борьба с потерями и ошибками может значительно сказаться на времени доставки, что может быть неприемлемо для служебного управляющего трафика. Это обуславливает необходимость наличия в сетях связи дополнительных механизмов, позволяющих обеспечить качество мультимедийного трафика, и выполнить требования к вероятностно – временным характеристикам служебного управляющего трафика

СПИСОК ЛИТЕРАТУРЫ

1. .В. Г. Олифер, Н. А. Олифер. 54 Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. 2006.

УДК 623.618

АНАЛИЗ ПРОБЛЕМ РАЗВИТИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Борисов Александр Иванович, Логинов Вячеслав Алексеевич, Пименов Алексей Сергеевич
Военная академия связи имени Маршала Советского Союза С.М. Будённого,
Россия, Санкт-Петербург, Тихорецкий проспект, 3,
email: B.A.I.58@yandex.ru

Аннотация: В статье рассмотрены проблемы создания автоматизированных систем специального назначения, показана необходимость комплексного подхода к развитию данной системы, обоснована важнейшая роль в этом процессе применяемой системы стандартов.

Ключевые слова: *автоматизированная система управления; средства автоматизации. информационное взаимодействие.*

ANALYSIS OF PROBLEMS OF DEVELOPMENT OF ASU OF A SPECIAL PURPOSE

Alexander Borisov, Vyacheslav Loginov, Aleksey Pimenov

Military academy of telecommunications named after Marshal of the Soviet Union S.M. Budyonny,
Russia, St. Petersburg, Tikhoretskiy Prospect, 3,
emails: B.A.I.58@yandex.ru

Abstract: In article problems of creation of automated systems of a special purpose are considered, need of an integrated approach to development of this system is shown, the major role in this process of the applied system of standards is justified.

Keywords: *automated control system, automation tools, information interaction*

Введение. Современный период развития общества характеризуется возросшей ролью управления. Использование достижения науки и техники, усложнение социальных процессов, рост объема обрабатываемой информации ужесточают требования к управлению. В современных системах управления в несколько раз увеличился общий объем циркулирующей информации, при этом время, отводимое на выработку решений по управлению, резко сократилось. Возникает противоречие в количестве обрабатываемой информации, ее анализа и уменьшении времени на принятия решения по управлению

В настоящее время успех в противостоянии сторон зависит не только от количества задействованных сил и средств, но и от оперативности и качества управления, в частности за счет использования средств автоматизации. Система управления, в которой информационный процесс реализуется с применением средств автоматизации, с целью повышения эффективности управления называется автоматизированной системой управления. Средства автоматизации, используемые в системах управления, могут быть как в стационарном, размещающие в специальных помещениях, так и в мобильном исполнении, монтируемые на специальной транспортной базе. Мобильные комплексы могут быть использованы как автономно, так и в качестве наращивания стационарной компоненты.

В различных структурах специального назначения, на сегодняшний день, используется достаточное большое количество средств автоматизации, но говорить о создании единой автоматизированной системы, удовлетворяющей потребностям органов управления для повышения оперативности управления и принимаемых решений можно лишь с натяжкой.

Это обусловлено такими факторами как большая разнородность средств автоматизации, с дублированием функциональных возможностей, использованием программного обеспечения различных производителей и др. Все это приводит к сложности организации взаимодействия, совместимости, избыточности обрабатываемой и хранимой информации, и, в конечном итоге, усложнения и увеличения цикла управления.

В настоящее время система управления специального назначения представляет собой иерархическую структуру осуществляющую на всех уровнях сбор информации ее обработку для принятия качественных решений. Разработка автоматизированных систем различного назначения, до недавнего времени, не была определена стандартами информационно-технического взаимодействия, что привело к появлению и применению множества уникальных протоколов информационно-технического сопряжения. Взаимодействие таких систем, при их совместном использовании при создании общего информационного пространства, приводило к снижению скорости обмена информацией, увеличение времени и стоимости разработок, привлечение значительного ресурса специалистов предприятий-разработчиков и т.д., что влекло за собой дополнительные сложности при модернизации автоматизированных систем, конфигурировании и применении.

Одним из аспектов в решении описанных проблем может явиться внедрение общих требования для разработки систем автоматизированного управления специального назначения таким, позволяющих сформировать единое информационное и технологическое пространство, обеспечить эксплуатацию и своевременную модернизацию. При этом единая технологическая основа должна обеспечивать уменьшение количества разрабатываемых протоколов информационно-технического сопряжения различными автоматизированными системами, что позволит сосредоточить основные усилия на развитии специального программного обеспечения.

Базовыми элементами для разработки автоматизированной системы должны стать единая операционная система, общее специальное программное обеспечение, объектная модель хранения данных, единая система управления базой данных, информационно-лингвистическое обеспечение, географическая информационная система. Кроме того, целесообразно разработать единые стандарты обмена информацией для обеспечения информационно-технического сопряжения

автоматизированных систем и комплексов различного назначения в автоматизированными системами управления различного уровня. Также необходимо обеспечить разработку базовых элементов, на которых будет строиться единая технологическая основа автоматизированной системы управления, разработать единый ряд технических средств, предназначенный для применения в автоматизированных системах управления различного назначения и уровней – как для мобильного, так и стационарных исполнения. Выполнение таких требований построенная автоматизированных систем позволит обеспечить управление силами и средствами на всех звеньях управления.

Заключение. Таким образом, рассмотренные проблемы оснащения средствами и комплексами автоматизации систем управления специального назначения, безусловно, относятся к разряду организационных и решение этих проблем позволит сконцентрировать усилия в научной и технической сфере на наиболее важных направлениях и тем самым повысить эффективность управления.

СПИСОК ЛИТЕРАТУРЫ

1. Цели и задачи создания инфокоммуникационной системы специального назначения // Легков К.Е., 2013
2. Новые информационные и сетевые технологии в системах управления военного назначения. Часть 1. Новые сетевые технологии в системах управления военного назначения. Учебник / под редакцией С.М. Одоевского. СПб.: Вас, 2010 – 432 с.
3. Новые информационные и сетевые технологии в системах управления военного назначения.
4. часть 2. Новые сетевые технологии в системах управления военного назначения. Учебник / под редакцией И.Б. Саенко. СПб.: Вас, 2010 – 520 с.

УДК 004.7.056.53

СХЕМА И ИНФРАСТРУКТУРА ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОСТИ КОММУНИКАЦИЙ В СЕТИ ИНТЕРНЕТ ОТ АТАКИ ТИПА «ЧЕЛОВЕК ПОСЕРЕДИНЕ», ОСНОВАННОЙ НА ИСПОЛЬЗОВАНИИ ОТОЗВАННЫХ СЕРТИФИКАТОВ

Бусыгин Алексей Геннадьевич, Коноплев Артем Станиславович, Зегжда Дмитрий Петрович
Санкт-Петербургский политехнический университет Петра Великого
Кафедра «Информационная безопасность компьютерных систем»
Россия, г. Санкт-Петербург, ул. Политехническая, 29,
emails: a.busygin@ibks.spbstu.ru, artem.konoplev@ibks.spbstu.ru, dmitry.zegzhda@ibks.spbstu.ru

Аннотация: Авторами рассмотрена архитектурная уязвимость сетевых приложений, реализующих протокол TLS к атаке типа «человек посередине», основанной на использовании отозванных сертификатов, и предложены схемы проверки статуса сертификатов и сетевая инфраструктура, позволяющие защититься от данной атаки в сети Интернет.

Ключевые слова: TLS; «человек посередине»; проверка статуса сертификатов

PROTOCOL AND INFRASTRUCTURE OF THE INTERNET COMMUNICATIONS PROTECTION AGAINST MAN-IN-THE-MIDDLE ATTACK BASED ON THE REVOKED CERTIFICATES

Alexey Busygin, Artem Konoplev, Dmitry Zegzhda
Peter the Great St.Petersburg Polytechnic University
Russia, St. Petersburg, Polytechnicheskaya, 29
emails: a.busygin@ibks.spbstu.ru, artem.konoplev@ibks.spbstu.ru, dmitry.zegzhda@ibks.spbstu.ru

Abstract: Authors present an architectural vulnerability of the TLS protocol implementing network applications to the man-in-the-middle attack, based on the revoked certificates, and propose certificate revocation checking protocols and network infrastructure, allowing to protect the Internet communications against this attack.

Keywords: TLS; man-in-the-middle; certificate revocation check

Введение. Современные веб-браузеры уязвимы к атаке типа «человек посередине», реализуемой с помощью отозванных сертификатов [1]. Атака основывается на том, что при установке TLS-соединений браузеры проверяют статус сертификата веб-сервера (отозван ли сертификат) не достаточно строго. Данная уязвимость является архитектурной, потому ей подвержено и другое программное обеспечение, использующее протокол TLS и реализующие эквивалентные политики проверки статуса сертификатов.

В теории стандартной процедуры отзыва сертификатов должно быть достаточно для защиты пользователей от атак данного типа, поскольку при установке TLS-соединения клиент должен проверить статус сертификата сервера и разорвать соединение, если сертификат сервера отозван. На практике TLS-клиенты либо вовсе не проверяют статус сертификата TLS-сервера, либо проверяют в режиме «soft fail», т.е. если информация о статусе сертификата не была получена (например, из-за того, что OCSP-сервер оказался недоступен), то сертификат считается действительным. Это означает, что если «человек посередине» имеет возможность блокировать попытки клиента получить информацию о статусе сертификата (например, блокировать OCSP-запросы), он сможет успешно

провести атаку, т.е. проверка статуса сертификата, как и процедура отзыва скомпрометированного сертификата, оказываются бессмысленными.

Проверка статуса сертификатов в режиме «hard fail» не выполняется по ряду причин, например: инфраструктура удостоверяющих центров (УЦ) становится единой точкой отказа, увеличение затрат на поддержку инфраструктуры УЦ, снижение надёжности TLS-соединений в зашумлённых сетях и др. Авторами предлагаются схемы проверки статуса сертификатов и инфраструктура, позволяющие нивелировать указанные выше недостатки. В облегчённой схеме проверки используются сертификаты с коротким сроком действия и агрегаторами CRL [4], обладающими унифицированным интерфейсом доступа. В схеме со строгой проверкой используются сертификаты с расширением, обязывающим применять прикрепленные OCSP-ответы для всей цепочки сертификатов [2] и защищать их от атаки повторного воспроизведения. Для устранения единой точки отказа и снижения нагрузки на УЦ в строгой схеме применяются несколько сертификатов, выпущенных независимыми УЦ, и защищённые механизмы возобновления TLS-соединений [3].

Закключение. Данные схемы проверки статуса сертификатов и сопутствующая сетевая инфраструктура (агрегаторы CRL, независимые УЦ и программное обеспечение, поддерживающее возобновление соединений), позволяют достичь компромисса между защищённостью и издержками безопасности и могут быть внедрены в сеть Интернет в будущем.

СПИСОК ЛИТЕРАТУРЫ

1. Langley A. Revocation doesn't work // ImperialViolet. 2011. URL: <https://www.imperialviolet.org/2011/03/18/revocation.html> (дата обращения: 20.09.2017).
2. Busygin A.G. Approaches to Protection of Applications Based on the TLS Protocol against Attacks Using Revoked Certificates / A.G. Busygin, A.S. Konoplev, M.O. Kalinin // Automatic Control and Computer Sciences. 2016. Vol. 50. No. 8. P. 743.
3. Salowey J. RFC 5077. Transport Layer Security Session Resumption without Server-Side State / Salowey J., Zhou H., Eronen P., Tschofenig H. // IETF Tools. 2008. URL: <https://tools.ietf.org/html/rfc5077> (дата обращения: 20.09.2017).

УДК 004.8

ПОДХОД К ПРОТИВОДЕЙСТВИЮ КОМПЬЮТЕРНЫМ АТАКАМ НА КРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННЫХ СЕГМЕНТАХ СЕТИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Васюков Дмитрий Юрьевич, Смыгин Александр Михайлович Митрофанов Михаил Валерьевич
Военная Академия связи
Россия, Санкт-Петербург, Тихорецкий проспект, 3
emails: cmiginsam1983@gmail.com

Аннотация: В докладе рассмотрены актуальные вопросы защиты информации от компьютерных атак пути решения вопросов безопасности информации на критически важных информационных сегментах сети специального назначения.

Ключевые слова: критически важные информационные сегменты, средства противодействия компьютерным атакам.

APPROACH TO COUNTERING COMPUTER ATTACKS ON CRITICAL INFORMATION SEGMENTS OF A SPECIAL PURPOSE NETWORK

Vasyukov Dmitry Yuryevich, Smygin Alexander Mikhailovich Mitrofanov Mikhail Valerievich
Military Academy of Communications
Russia, St. Petersburg, Tikhoretsky prospect, 3
emails: cmiginsam1983@gmail.com

Abstract: In report topical questions of protection of the information from computer attacks and ways of the decision of questions of safety of the information on critical information segments of a network of special appointments.

Keywords: critical information segments means of counteraction to computer attacks.

Введение. В соответствии с Доктриной информационной безопасности РФ, важнейшей составляющей технологии информационной безопасности являются средства противодействия компьютерным атакам на критически важные информационные сегменты.

Под критически важными сегментами понимаются такие подсистемы и объекты НИИ, поражение которых наносит существенный ущерб функционированию экономики, национальной безопасности и национальным интересам страны

К числу основных задач типовых критически важных информационных сегментов(КВИС) относятся:

- передача и прием исходных данных для проведения расчетов;
- сбор, хранение и доставка информации на пункте управления;
- доставка, сбор и выдача управляющей информации абонентам центров управления;
- обмен информацией между абонентами пунктов и центров управления;

- организация оперативного взаимодействия и управления между КВИС по каналам связи.

Топология, состав и функции КВИС формируются на основе унифицированных информационно-телекоммуникационных средств в соответствии с требованиями к объектам управления. Способы и протоколы информационного взаимодействия абонентов КВИС, для каждого конкретного объекта управления, реализуются в схеме организации связи с абонентами, объединяющими средства измерений, сбора, обработки и передачи информации. В каждом конкретном КВИС могут использоваться дополнительные коммутационные средства, учитывающие специфику технического и программного обеспечения.

В настоящее время, в условиях воздействий компьютерных атак эффективность функционирования КВИС, как главного системообразующего и управляющего компонента автоматизированных систем, во многом определяется устойчивостью функционирования КВИС сбора, обработки и передачи информации. С заменой устаревших вычислительных средств и систем связи в КВИС появилась принципиальная возможность осуществления компьютерных атак через уязвимые места в цифровом коммуникационном оборудовании и используемом программном обеспечении в режиме удаленного доступа через прозрачные сети (как для штатного оператора, так и нарушителя) на базе типовых протоколов передачи данных.

Последствием воздействия компьютерных атак могут стать блокирование управляющей информации и внедрение ложной информации, нарушение установленных регламентов сбора, обработки и передачи информации в комплексах управления, отказы и сбои в работе КВИС, а также компрометация получаемой потребителями информации.

Актуальность разработки предложения, которое позволит нейтрализовать атаки и сохранить при этом устойчивость функционирования КВИС в ходе выполнения ТЦУ, обусловлена следующими факторами:

- интенсивным развитием технологий и средств реализации компьютерных атак;
- опасностью потери устойчивости функционирования КВИС при воздействии компьютерных атак;
- вынужденной необходимостью внедрения в КВИС программно-аппаратных комплексов иностранного производства;
- невозможностью решения, проблемы в полной мере традиционными методами и средствами защиты информации, по отношению к которым совершенствуются в настоящее время средства реализации компьютерных атак;
- несовершенством методов и средств противостояния компьютерным атакам.

Разработка подхода противодействия компьютерным атакам на КВИС базируется на комплексном использовании положений теории защиты информации, устойчивости и надежности функционирования автоматизированных систем, моделирования сложных систем, автоматического управления, качества и достоверности информации, обнаружения компьютерных атак.

Результаты анализа современных подходов к защите информации, обеспечению надежности и устойчивости функционирования КВИС показывают, что в них не в полной мере решены следующие вопросы:

- не рассмотрены проблемы, связанные с разработкой методов и моделей противодействия компьютерным атакам на средства сбора, обработки и передачи информации КВИС, интеллектуальных средств контроля состояния информационно-вычислительного процесса и организацией активного противодействия компьютерным атакам;
- большинство известных методов и моделей обнаружения атак не учитывают взаимосвязанное решение вопросов противодействия компьютерным атакам и устойчивости функционирования КВИС при выполнении ТЦУ;
- практически отсутствуют комплексные методы, модели и алгоритмы, в которых, наряду с сигнатурным анализом атак и выявлением аномалий в КВИС, обнаружение атак осуществляется путем функционального анализа контролируемых параметров и идентификации состояния устойчивости функционирования КВИС;
- недостаточно проработаны методы и модели принятия решений, в том числе статистических, по обеспечению активного противодействия источникам атак.

Кроме того, используемые в настоящее время методы и модели противодействия компьютерным атакам на КВИС не разрешают ряд противоречий:

- между повышением оперативности и устойчивости системы управления, с одной стороны, и ухудшением процессов управления при воздействии компьютерных атак на КВИС, с другой;
- между уменьшением количества факторов уязвимостей КВИС, требующих устранения избыточных функций и параметров, с одной стороны, и усложнением процессов контроля информационно-вычислительного процесса в КВИС и обнаружения атак, с другой;
- между требованиями к своевременности технологического цикла управления, с одной стороны, и временем, необходимым для обнаружения и нейтрализации источника атаки, с другой.

Одним из возможных путей создания КВИС, защищенных от воздействия компьютерных атак, является интеграция информационных технологий КВИС с внедренными в ее структуру датчиками

СПКА (средства противодействия компьютерным атакам), с соблюдением обязательного взаимодействия средств администрирования с управляющими программами СПКА. При этом эффект состояния защищенности КВИС будет достигнут тогда, когда наряду с компонентами СПКА осуществляется комплексное использование организационно-технических мер, максимальное применение средств администрирования и мониторинга сети, используются антивирусные средства, сертифицированное программное обеспечение, компьютерное и коммутационное оборудование. Кроме того, необходимо составить перечень критических контролируемых параметров КВИС, определить их чувствительность к воздействию КА, экспериментально проверить согласованность работы компонентов КВИС, СПКА, средств защиты информации от несанкционированного доступа при выполнении реальных технологических циклов управления КА, и на основании изменений контролируемых параметров разработать (уточнить) технические решения.

Заключение. Это позволит решить вопрос обеспечения информационной безопасности и защиты информации на критически важных сегментах сети специального назначения.

СПИСОК ЛИТЕРАТУРЫ

1. «Методы и модели противодействия компьютерным атакам» С.М. Климов Москва 2008, 2. «Системный анализ в защите информации» учеб. Пособие для студентов вузов А.А. Шумский, А.А. Шелупанов.- М.: Гелиос АРВ, 2005,
3. Обеспечение защиты информации в локальных вычислительных сетях Бударин Э.А., Васюков Д.Ю., Дементьев В.Е., Колбасова Г.С., Краснов В.А., Лепешкин О.М., Лаута О.С., Митрофанов М.В., Худайназаров Ю.К. ВАС им. Маршала Советского Союза С.М. Буденного. Санкт-Петербург, 2013.
4. Исследование функциональной безопасности систем государственного управления Лепешкин О.М. Инфокоммуникационные технологии. 2007. Т. 5. № 3. С. 165-166.
5. Разработка подхода по оценке функциональной безопасности критической социотехнической системы Лепешкин О.М. Инфокоммуникационные технологии. 2008. Т. 6. № 3. С. 113-116.

УДК: 004.056.53

ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ ПЕРЕДАЧИ, ХРАНЕНИЯ И ОБРАБОТКИ ИНФОРМАЦИИ

Волостных Виктор Анатольевич, Рогов Руслан Александрович, Митрофанов Михаил Валерьевич

Военная Академия связи

Россия, Санкт-Петербург, Тихорецкий проспект, 3

email: rus6283@list.ru

Аннотация: В докладе рассмотрена необходимость проведения мероприятий защиты информации в системах передачи, хранения и обработки информации, а так же основные причины влекущие за собой утечку информации с данных систем.

Ключевые слова: информационная безопасность, системы передачи, хранения и обработки информации, информация конфиденциального характера, утечка информации.

PROTECTION OF INFORMATION IN THE SYSTEMS OF TRANSMISSION, STORAGE AND PROCESSING OF INFORMATION

Volostnykh Viktor, Rogov Ruslan, Mitrofanov Mikhail

Military Academy of communications

Russia, Saint-Petersburg, Tikhoretsky prospect, 3

email: rus6283@list.ru

Annotation: The report considers the need to carry out information protection measures in information transmission, storage and processing systems, as well as the main reasons leading to information leakage from these systems.

Keywords: information security, information transfer, storage and processing systems, confidential information, information leakage.

Введение. Появление новых информационных технологий и развитие мощных компьютерных систем передачи, хранения и обработки информации повысили требования к уровню защиты информации и вызвали необходимость, чтобы эффективность защиты информации росла вместе со сложностью архитектуры хранения данных. Таким образом, средства обеспечения информационной безопасности стали одной из обязательных характеристик данных систем. На сегодняшний день существует широкий круг систем передачи, хранения и обработки информации, где в процессе их проектирования фактор информационной безопасности, хранения конфиденциальной информации имеет особое значение [1,2].

Актуальность применения данных систем связана с значительно упрощившемся порядком работы, а так же с сокращением времени обмена документами между пользователями системы. В связи с использованием в вышеперечисленных системах большого количества информации содержащей сведения государственной тайны или информации конфиденциального характера, в значительной степени привлекли к себе внимания злоумышленников, которые всевозможными способами пытаются завладеть, изменить или удалить данную информацию из системы. Таким

образом, главной задачей защиты информации является изолирование нормально функционирующей информационной системы от несанкционированных управляющих воздействий и доступа посторонних лиц или программ к данным с целью хищения [3].

Рассматривая угрозы безопасности систем передачи, хранения и обработки информации, их следует разделить на преднамеренные и случайные.

Исходя из публикаций последних лет в данной области, можно сделать вывод, что как минимум 70% утечки информации связаны с случайными (непреднамеренными) угрозами. При этом 95% снижения эффективности защиты связано с самим пользователем. Простейшая не внимательность, безответственное отношение, а, зачастую, элементарное незнание использования систем передачи, хранения и обработки информации в комплексе.

Существует системный подход к организации защиты информации от несанкционированного доступа. К методам и средствам защиты информации относят организационные, технические и правовые [4,5].

При этом в данном подходе должным образом не уделяется внимание вопросам комплексной подготовки пользователей данной системы, проведение контрольных занятий, доведение статей, предусматривающих ответственность виновных в утрате или утечке какой-либо информации, что является весомым аргументом в системе защиты информации. Важно понимать, что основная утечка данных происходит не благодаря хитроумным способам, а из-за небрежности и невнимательности.

Закключение. Исходя из этого можно сделать вывод, что, уделяя больше внимания комплексной подготовке пользователей систем передачи, хранения и обработки информации, соблюдения новых стандартов ФСТЭК, психо-эмоционального подбора личного состава можно не только снизить количество утечек информации, но и повысить эффективность функционирования самой системы.

СПИСОК ЛИТЕРАТУРЫ

1. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. 3-е изд., стер. - М.: Академия, 2008. - 336 с.
2. Черней Г.Л., Охрименко С.А., Ляху Ф.С. Безопасность автоматизированных информационных систем. Ruxancia, 1996. - 225 с.
3. Галатенко, В.Л. Основы информационной безопасности.
4. Лепешкин О.М., Харечкин П.В. Функционально-ролевая модель управления доступом в социотехнических системах. Известия ЮФУ. Технические науки. 2009. № 11 (100). С. 52-57.
5. Бурлов В.Г., Лепешкин О.М. Методологический подход к оценке безопасности функционирования социальной и экономической системы управления региона. Проблемы экономики и управления в торговле и промышленности. 2013. № 2. С. 99-103.
6. Лепешкин О.М. Разработка подхода по оценке функциональной безопасности критической социотехнической системы. Инфокоммуникационные технологии. 2008. Т. 6. № 3. С. 113-116.

УДК 004.056.57

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

Дахнович Андрей Дмитриевич, Москвин Дмитрий Андреевич
Санкт-Петербургский политехнический университет Петра Великого,
Россия, Санкт-Петербург, ул. Политехническая, 29,
emails: andrei_dahnovich@mail.ru, moskvin@mail.ru

Аннотация: В статье рассматриваются понятия промышленного Интернета вещей и Индустрии 4.0, а также формируются требования к информационной безопасности, возникающие в сетях, построенных с применением данных технологий.

Ключевые слова: промышленный интернет вещей; индустрия 4.0; киберфизические системы.

ENSURING INFORMATION SECURITY IN INDUSTRIAL INTERNET OF THINGS NETWORKS

Dakhnovich Andrei, Dmitrii Moskvina
Peter the Great St.Petersburg Polytechnic University,
Russia, Saint-Petersburg, Polytechnic street, 29,
emails: andrei_dahnovich@mail.ru, moskvin@mail.ru

Abstract: The article deals with concepts of Industrial Internet of Things and Industry 4.0. Concerning these terms information security requirements for networks utilizing Internet of Things technologies are proposed.

Keywords: industrial internet of things; Industry 4.0; cyber-physical systems.

Введение. Четвертая промышленная революция, или Industry 4.0, мало-помалу начинает внедряться в производственные процессы предприятий. Впервые концепция Industry 4.0 была представлена на Ганноверской ярмарке в 2011 году, в следующем 2012 году рабочая группа

представила набор рекомендаций федеральным правительствам ФРГ в рамках «Стратегии в области высоких технологий 2020». В свою очередь в России была создана Национальная технологическая инициатива (НТИ), согласно которой страна должна выйти на мировые рынки высокотехнологичной продукции в 2020-2025 годах [1]. Весной 2014 года по инициативе таких компаний, как Intel, IBM, GE, Cisco и AT&T в США образовался консорциум под названием «Industrial Internet Consortium», в задачи которого входит устранение несовместимостей различных технологий, а также создание рекомендаций по безопасности промышленных систем, использующих «Интернет вещей» [2].

На данный момент системы используют различные наборы технологий, сетевые протоколы, архитектуры, стандарты и модели управления. Индустрия 4.0 призвана объединить различные технологии, применяемые в производственных сетях, в одну автономную, децентрализованную сеть: предприятия, цепочки поставок, клиенты – всё должно функционировать в одной кибер-физической среде, элементы которой должны работать автономно, запускать работу и обеспечивать контроль друг друга. Это позволит предприятиям увеличить скорость производства, доставку продукции, уменьшить издержки, а также увеличить качество обслуживания клиентом. Но в то же время обеспечение совместимости и интеграции разнородных систем является и главной проблемой. Поэтому понятие Индустрии 4.0 часто называют эквивалентом термина «Интернета вещей» (Internet of Things, IoT), но ориентированного на производство продукции и услуг – промышленный Интернет вещей (Industrial Internet of Things, IIoT) [2].

В связи с этим появляются новые угрозы информационной безопасности, которые влекут за собой новые риски. В большинстве работающих сегодня систем производственные процессы, а значит, и данные, изолированы друг от друга, что упрощает обеспечение их безопасности и уменьшает риски, связанные с компрометацией одного из компонентов. При интеграции систем друг с другом риски возрастают из-за того, что, получив несанкционированный доступ через одну из точек входа, злоумышленник может получить доступ ко всем процессам предприятия. Помимо этого, сети Индустрия 4.0 подразумевают использование различных IoT-устройств (например, сенсоров), к которым невозможно применить стандартное программное обеспечение защиты информации. И, наконец, подобные системы имеют подключение к глобальной сети Интернет, поскольку объединяют всех участников производственного процесса. Это упрощает их управление, но также делает более доступными для злоумышленников.

Промышленный Интернет вещей является проекцией технологий Интернета вещей на технологии автоматизированных систем управления техническими процессами (АСУ ТП). Каждая технология имеет свои требования к безопасности. Для Интернета вещей это: обеспечение приватности пользовательских данных; обеспечение безопасности киберфизических объектов; обеспечение сетевой безопасности, а также обеспечение безопасности облачного пространства вычислений. Для АСУ ТП требования к безопасности заключаются в контроле доступа (локальном и удаленном), обеспечение сетевой безопасности, а также контроль событий. Отсюда вытекают новые требования к безопасности предприятий, использующих технологии промышленного Интернета вещей, как слияние требований к вышеуказанным технологиям: обеспечение приватности данных предприятия, обеспечение киберфизической безопасности объектов, обеспечение контроля доступа между различными сегментами сети и между КФО, обеспечение безопасности взаимодействий по сети (как локальной, так и сети Интернет).

Закключение. Необходимо создать модель безопасности, отвечающую выявленным требованиям, при этом не снижающая эффективность и экономическую выгоду использования промышленного Интернета вещей в производстве. Обеспечение информационной безопасности в подобных сетях необходимо с самого начала стратегического процесса их внедрения.

СПИСОК ЛИТЕРАТУРЫ

1. NIST Current Standards Landscape for Smart Manufacturing Systems. 2016 [Электронный ресурс]. URL: <https://www.redhat.com/cms/managed-files/rh-industrial-internet-of-things-iiot-security-intelligent-gateway-whitepaper-f6951kc-201706-en.pdf> (Дата обращения: 30.08.2017).
2. Industrial Internet of Things Volume G4: Security Framework. 2016 [Электронный ресурс]. URL: http://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf (Дата обращения: 12.09.2017).

УДК 004.725.5 + 004.056.5

СПОСОБ ЗАЩИТЫ РЕСУРСОВ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ

Журавель Евгений Павлович

Санкт-Петербургский политехнический университет Петра Великого
Россия, Санкт-Петербург, ул. Политехническая, 29,

Аннотация: В статье сформулирован подход к защите ресурсов мультисервисной сети связи на основе комплексного анализа априорной и апостериорной информации состояния о ресурсах мультисервисной сети связи. Формирование адекватных мер защиты мультисервисной сети связи предлагается на уровнях её ресурсов и технологий и (или) сред передачи деструктивных воздействий.

Ключевые слова: мультисервисная сеть связи; сеть управления; сеть обеспечения функционирования; сеть сбора и анализа информации состояния.

THE WAY OF PROTECTION OF RESOURCES OF A MULTISERVICE COMMUNICATION NETWORK

Evgeny Zhuravel

Peter the Great St. Petersburg Polytechnic University
Russia, St. Petersburg, Politehnicheskaya Street, 29

Abstract: In article approach to resource protection of a multiservice communication network on the basis of the complex analysis of prior and posteriori information of a status on resources of a multiservice communication network is formulated. Formation of adequate measures of protection of a multiservice communication network is offered at the levels of its resources and technologies and (or) transmission mediums of destructive influences.

Keywords: multiservice communication network; control plane; operation provisioning plane; collecting and analysis of information state network.

Введение. Основными характеристиками единой сети электрической связи (ЕСЭС) Российской Федерации (РФ) являются целостность, устойчивость и безопасность её функционирования, соответственно, указанными характеристиками должны обладать и сети, её составляющие. Модели источников угроз (нарушителей), угроз, деструктивных воздействий, технологий и (или) сред передачи деструктивных воздействий, а также модели ресурсов мультисервисной сети связи (МССС) ЕСЭС РФ целесообразно рассмотреть в соответствии с [1] и, на основе результатов рассмотрения, в общем виде сформулировать подход к защите ресурсов МССС, заключающийся в комплексном анализе априорной и апостериорной информации состояния о ресурсах МССС и последующем формировании на его основе адекватных мер защиты МССС на уровнях её ресурсов и технологий и (или) сред передачи деструктивных воздействий.

Для построения модели защиты МССС целесообразно использование разработанной в 1990 г. Д. Ризоном из Манчестерского университета Великобритании модели определения и описания ситуаций, потенциально ведущих к наступлению некоторого не приемлемого события, которая получила название модели "швейцарского сыра". Применительно к обобщённой модели воздействий на ресурсы МССС должен быть источник угроз (нарушитель), который должен формировать угрозу, которая должна оказывать воздействие, способное быть переданным с использованием среды передачи и, в той или иной мере, соответствовать ресурсам МССС. При этом если какую-либо взаимосвязь обобщённой модели воздействий на ресурсы МССС удастся разорвать, то воздействия не произойдет.

В [2] рассмотрен один из вариантов реализации защиты МССС на уровнях её ресурсов и технологий и (или) сред передачи, под которым понимается статическое выделение в МССС сети обеспечения функционирования и сети, непосредственно реализующей контур управления.

Приняв предложенные в [1] и [2] модели воздействий и подход реализации защиты МССС за основу, рассмотрим следующий способ защиты ресурсов МССС на уровнях ресурсов и технологий и (или) сред передачи деструктивных воздействий дополнением, взаимным построением и определением функционального назначения составляющих её ресурсов, заключающийся в выделении в МССС следующих сетей:

- сеть обеспечения функционирования МССС реализует функции обеспечения синхронизации точного времени с использованием протокола NTP, которое используется в МССС с коммутацией пакетов вместо систем тактовой синхронизации синхронных сетей, функции именования сетевых элементов на основе единого указателя ресурсов URL с использованием системы доменных имён DNS, функции сетевой идентификации с использованием опций 43, 60 и 82 протокола DHCPv4, опций 16, 17 и 18 протокола DHCPv6 и (или) функции аутентификации, авторизации и учёта использования услуг с использованием протокола RADIUS, TACACS+, DIAMETER, LDAP, SCIM и др., при этом, функция сетевой идентификации и указанные выше протоколы могут быть объединены в иерархию с целью формирования услуги "Удостоверение как услуга" для пользователя и (или) программного обеспечения ресурсов МССС;

- сеть управления МССС предлагается использовать как основу для кроссплатформенной системы управления оборудованием МССС на основе принципов автоматизированного конфигурирования сетевых устройств с использованием протоколов безопасного сетевого соединения, таких как протоколы SOAP, CWMP, XML инкапсулированные в протокол HTTPS, TL1, SNMPv3 с расширением SNMP trap, протокол SSH версии 2 и др., а также для резервного копирования конфигураций сетевого оборудования с использованием протокола SFTP, метода put протокола FTP в реализации vsftpd, scp, методы put и post протокола HTTPS и др., что позволит автоматизировать отслеживание изменений в конфигурации сетевых устройств, например, с использованием систем контроля версий CVS, Subversion, Git, WebDAV и др.;

- к введенным в [2] сетям управления и сетям обеспечения функционирования в соответствии с выполняемыми ими функциями следует подсоединить сети доступа, сети агрегации, транспортные

сети и сети систем коммутации соответственно (последние – в случае, если эти сети принадлежат данной организации связи). Присоединение подразумевает двусторонний обмен информацией и, как следствие, в случае реализации проникновения в соответствующие ресурсы МССС, потенциальную возможность для нарушителя (источника угроз) осуществить подчистку (стирание, изменение, маскирование и др.) соответствующей информации о его действиях или другой информации. В связи с этим, целесообразно физически выделить еще одну выделенную сеть для сбора и анализа информации состояния ресурсов МССС и однонаправленно присоединить к ней сеть обеспечения функционирования с использованием, например, имеющихся программно-аппаратных решений шлюза односторонней передачи данных (ШОПД), которые позволяют осуществлять однонаправленную передачу информации на основе протоколов syslog, syslog-tls, UDP или других протоколов прикладного уровня ЭМВОС. Для контроля ресурсов, составляющих демилитаризованную сеть, ее также целесообразно однонаправленно присоединить к сети сбора и анализа информации через ШОПД и, по возможности, использовать для передачи данных протоколы syslog-tls и UDP. К сети сбора и анализа информации через ШОПД следует, по возможности, подключать и сети систем коммутации, которые имеют иного собственника и осуществляют предоставление услуг в рассматриваемой МССС.

Построение предлагаемых технологических сетей управления и обеспечения функционирования для экономии денежных средств целесообразно выполнить программно с использованием технического ресурса сети общего пользования средствами межсетевого экранирования и (или) виртуализации ТКО и общего программного обеспечения ЭВМ, то есть отделения одного вида трафика от другого с использованием реализаций, позволяющих тем или иным способом виртуализировать физический порт и (или) логический сетевой ip/rppr-интерфейс, например, с использованием стандарта 802.1q.

В сети сбора и анализа информации МССС целесообразно выполнение периодического и/или ретроспективного автоматизированного анализа собранной информации с использованием соответствующих методов представления и использования знаний, методов искусственного интеллекта, методов нечеткой логики или других методов и подходов, что позволит выявлять сложные распределенные сценарии атак на ресурсы МССС, состоящие из множества распределенных во времени действий, каждое из которых по отдельности не расценивается как потенциально опасное.

Достоинством предлагаемого способа защиты МССС является не возможность изменения информации нарушителем (источником угроз), который, получив доступ к некоторым ресурсам МССС, может остановить функционирование процесса передачи информации состояния. Для ослабления данного недостатка следует реализовать мониторинг периодичности поступающей информации от ресурсов МССС.

Заключение. Рассмотренный способ защиты ресурсов МССС может применяться на этапах планирования, построения и эксплуатации МССС и, наряду с комплексным применением других средств (например, антивирусных средств, средств контроля изменений, средств построения виртуальных частных сетей, реализаций TLS/SSL и др.), позволяет осуществить формирование защищенной структуры ресурсов МССС что, в совокупности, существенно снижает риски воздействий на ресурсы МССС, но не устраняет их полностью. Не смотря на явные и потенциальные возможности по выявлению, снижению и (или) ослаблению деструктивных воздействий с использованием формулируемого выше способа защиты МССС следует отметить, что угрозы безопасности МССС будут существовать до тех пор, пока существуют ресурсы МССС, требующие защиты, существуют пользователи и администраторы услуг и (или) ресурсов МССС, подчас являющиеся нарушителями (источниками угроз) безопасности или создающие предпосылки к нарушениям безопасности, существуют и развиваются МССС, используемые ими технологии и протоколы, а также существует окружающая среда, в которой находятся пользователи, администраторы и функционирует МССС. Представляется целесообразным как дальнейшее периодическое уточнение существующих, так и разработка новых моделей, методик, профилей, способов, систем и средств для формирования адекватных (достаточных) мер защиты МССС на уровнях её ресурсов и технологий и (или) сред передачи деструктивных воздействий, актуализация и применение которых в совокупности позволит достигать требуемого уровня функциональной, технической и технологической безопасности МССС.

СПИСОК ЛИТЕРАТУРЫ

1. Журавель Е.П., Журавель П.Н. Модели воздействий на ресурсы мультисервисной сети связи // Т-Comm: Телекоммуникации и транспорт. 2017. №4. С. 26 – 33.
2. Журавель Е.П., Шерстюк Ю.М. Информационная безопасность в расширенной схеме деятельности организации связи. // Проблемы информационной безопасности. Компьютерные системы. 2016. № 2. С. 29 - 36.

УДК 004.056.57

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ УПРАВЛЕНИЯ РОБОТИЗИРОВАННЫХ СИСТЕМ С ПРИМЕНЕНИЕМ НЕЙРОННЫХ СЕТЕЙ

Захаров Руслан Владимирович, Лаута Олег Сергеевич, Крибель Александр Михайлович,
Соловьев Дмитрий Владимирович
Военная академия связи имени Маршала Советского Союза С.М. Будённого,
Россия, Санкт-Петербург, Тихорецкий пр., 3,
email: vlasenko199@yandex.ru, asuetin5@yandex.ru

Аннотация: В статье представлен подход по обеспечению безопасности управления роботизированных систем на основе искусственного интеллекта с применением нейронных сетей.

Ключевые слова: *роботизированная система; искусственная нейронная сеть; метод преобразования.*

SAFETY OF MANAGEMENT OF ROBOTIC SYSTEMS ON THE BASIS OF ARTIFICIAL INTELLIGENCE WITH APPLICATION OF NEURAL NETWORKS

Ruslan Zakharov, Oleg Laut, Aleksandr Kribel, Dmitriy Soloviov
Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tihoreckii' av. 3,
email: vlasenko199@yandex.ru, asuetin5@yandex.ru

Abstract: Approach on safety of management of robotic systems on the basis of artificial intelligence with application of neural networks is presented in article.

Keywords: *robotic system; neural network; transformation method.*

На текущем этапе развития технологий робототехнические комплексы (РТК) выполняют широкий спектр задач в различных областях деятельности человека. Отдельную нишу занимают РТК, выполняющие задачи специального назначения: военные РТК, РТК, обеспечивающие ликвидацию последствий чрезвычайных происшествий и других задач, связанных с риском для жизни человека.

Одной из важнейших задач при построении РТК как специального назначения, так и некоторых других типов, является обеспечение управления комплексом. Под управлением РТК понимается решение комплекса задач, связанных с адаптацией робота к кругу решаемых им задач, программированием движений, синтезом системы управления и её программного обеспечения [1], [3].

Наибольший интерес для решения задач, связанных с риском для жизни человека, представляют интерактивные системы управления, так как при решении сложных задач пока что избежать необходимости участия оператора избежать не удастся. При этом, более перспективным методом интерактивного управления РТК является дистанционное беспроводное управление. Применение данного метода управления позволяет изолировать оператора от опасных для жизни факторов, а также обеспечить максимально мобильный процесс управления.

Важнейшим вопросом, при построении и использовании РТК специального назначения, а в особенности, РТК, применяемых силовыми структурами, является обеспечение защищённости канала управления комплексом. Получение злоумышленником передаваемых сведений, их подмена, искажение или подавление могут привести к различными негативным последствиям вплоть до гибели людей. Для обнаружения злоумышленника и противодействия ему предлагается использовать системы, контролирующие процесс обмена данными в процессе управления РТК и выполняющими обнаружение аномальной активности на основе анализа протоколов различных уровней.

Хорошо зарекомендовавшим себя подходом к решению подобных задач является использование искусственных нейронных сетей (ИНС). Процесс построения профиля нормального поведения в случае с нейронными сетями сводится к созданию обучающей выборки, состоящей из примеров, содержащих данные нормального обмена РТК с оператором, и дальнейшего обучения ИНС с использованием этих данных. Алгоритмы обучения, обычно, выбираются на основе выбранного типа ИНС. Параметры ИНС выбираются эмпирическим путём в зависимости от конкретной задачи.

В случае, когда профиль нормального поведения строится на основе данных протоколов передачи, в качестве характеристик используются поля заголовков пакетов, а также дополнительные данные, такие как, например, временная метка, если эти данные не предусмотрены протоколом, но

Результатом работы такой ИНС является формирование топологической структуры (карты) [2], которая классифицирует входные примеры на кластеры (группы схожих примеров) и визуально отображает многомерные входные данные на плоскости нейронов. Важным преимуществом данного подхода является то, что эта ИНС является самообучающейся, то есть для обучения ей не нужны наборы входных данных и соответствующих им «правильных» выходных данных.

Для идентификации аномальной активности по результатам работы оператору РТК следует дожидаться формирования устоявшейся структуры кластеров на выходе ИНС, а в процессе дальнейшего функционирования РТК наблюдать за изменением данной структуры. Наличие явных

изменений в ней будет свидетельствовать об аномальном поведении. Задача прогнозирования в контексте обнаружения аномалий управления РТК будет заключаться в определении возможной следующей команды на основе информации о предыдущих. Если полученная команда будет значительно отличаться от прогнозируемых, то можно сделать вывод об аномальном поведении.

СПИСОК ЛИТЕРАТУРЫ

1. Обеспечение живучести информационных систем (часть 3. Методы обеспечения и повышения живучести). Елисеев А.И., Долгов А.А., Хорохорин М.А., Лаута О.С., Набатов К.А. Вестник Воронежского института ФСИИ России. 2013. №1. С.91-94.
2. Применение метода топологического преобразования стохастических сетей для оценки эффективности средств защиты. Баранов В.В., Крибель А.М., Лаута О.С., Нечепуренко А.П. В сборнике: Актуальные проблемы обеспечения информационной безопасности. труды Межвузовской научно-практической конференции. 2017. С. 47-52.
3. Методика оценки защищенности информационно-телекоммуникационной сети в условиях информационного противодействия. Коцыняк М.А., Иванов Д.А., Лаута О.С., Нечепуренко А.П. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 83-89.

УДК 004.056

РОЛЕВАЯ МОДЕЛЬ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ ДЛЯ СЕТЕЙ ТРАНСПОРТНЫХ СРЕДСТВ

Калинин Максим Олегович, Резединова Евгения Юрьевна
Санкт-Петербургский политехнический университет Петра Великого
Россия, Санкт-Петербург, ул. Политехническая, 29,
emails: max@ibks.spbstu.ru, er@ibks.spbstu.ru

Аннотация: В статье рассмотрены особенности сетей транспортных средств и принципы ролевого управления доступом, адаптированные к особенностям VANET.

Ключевые слова: ролевая модель; управление доступом, сети транспортных средств.

ROLE-BASED ACCESS CONTROL FOR VEHICULAR NETWORKS

Kalinin Maxim, Evgenia Rezedinova
Peter the Great St. Petersburg Polytechnic University,
Russia, St. Petersburg, Polytechnicheskaya, 29
emails: max@ibks.spbstu.ru, er@ibks.spbstu.ru

Abstract: The paper discusses features of VANET and adapts the role-based access control principles to VANET environment.

Keywords: RBAC; access control; vehicular networks.

При финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП "Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы" (Соглашение №14.578.21.0224, от 03.10.2016, уникальный идентификатор Соглашения RFMEFI57816X0224).

Введение. Актуальной задачей является построение моделей контроля и управления доступа для сетей транспортных средств (VANET). Рассматриваемые сети обладают динамической топологией, им свойственны самоорганизация, одноранговость, постоянное и непрерывное изменение состояния всей сети [1]. Основополагающим здесь является развитие моделей, приближающихся к реальным ситуациям и учитывающих сложные межмашинные связи и динамику топологии.

Анализ исследований в названной сфере показывает, что ролевые модели контроля доступа успешно применяются в сложных динамических системах, например, в Интернете вещей [2]. Основными преимуществами использования ролевой модели контроля и управления доступом являются: адаптируемость к изменениям в процессе развития сложной динамической системы (возможность добавления новых сущностей), а также удобство представления и контроля сущностей (узлов, объектов и привилегий) [3].

С учетом существующих особенностей сетей транспортных средств могут быть выделены следующие принципы построения ролевой модели контроля доступа в сетях данного типа:

1. Принцип упрощенного администрирования: субъекты получают привилегии только через механизм ролей.

2. Принцип иерархии ролей: каждая роль наряду со своими собственными привилегиями может наследовать привилегии других ролей.

3. Принцип минимальных привилегий: субъекты получают минимальные привилегии, которых будет достаточно для успешного выполнения задачи поставленной перед субъектом.

4. Принцип разделения обязанностей: статический и динамический.

5. Принцип динамического переназначения ролей: возможность быстро переназначить роль в зависимости от внешних условий (ситуаций) в сети. Указанный принцип может быть реализован за счет применения атрибутов "геозона", "дата/время", "текущие сервисы" и т.п.

6. Принцип группового управления: возможно переназначение ролей группе узлов.

Заключение. Ролевая модель позволяет решить ряд проблем контроля и управления доступом в условиях большого числа динамически меняющихся групп пользователей. В части контроля и управления доступом в сетях транспортных средств ролевая модель может быть реализована в сети с изоляцией сетевого трафика.

СПИСОК ЛИТЕРАТУРЫ

1. Dr. Nirbhay Kumar Chaubey. 2016. Security Analysis of Vehicular Ad Hoc Networks (VANETs): A Comprehensive Study. International Journal of Security and Its Applications, 10 (5), 2016, 261-274.
2. Wenshuang Liang, Zhuorong Li, Hongyang Zhang, Shenling Wang, Rongfang Bie. 2015. Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends. International Journal of Distributed Sensor Networks, 11 (8), 2015.
3. Ravi Sandhu. 2016. Access Control Models for Cloud-Enabled Internet of Things: A Proposed Architecture and Research Agenda. <http://profsandhu.com/confnc/misconf/picsoc16-asma-slides.pdf>

УДК 621.391.28

СИСТЕМАТИЧЕСКАЯ ПРОЦЕДУРА ПРИМЕНЕНИЯ МЕТОДА ДВУХМОМЕНТНОЙ АППРОКСИМАЦИИ ДЛЯ ОПРЕДЕЛЕНИЯ ФУНКЦИИ РАСПРЕДЕЛЕНИЯ ВРЕМЕНИ РЕАЛИЗАЦИИ СТОХАСТИЧЕСКОЙ СЕТИ

Канаев Андрей Константинович, Карабанов Юрий Сергеевич, Привалов Андрей Андреевич
ФГБОУ ВО Петербургский государственный университет путей сообщения императора Александра I
Россия, Санкт-Петербург, Московский пр., 9
emails: kanaevak@mail.ru, karabanov1994@yandex.ru, aprivalov@inbox.ru

Аннотация: В статье рассматривается разработанная авторами процедура многократного применения метода двухмоментной аппроксимации при определении эквивалентной функции стохастической сети, что значительно упрощает задачу определения функции распределения времени реализации моделируемого процесса.

Ключевые слова: метод топологического преобразования стохастических сетей, уравнение Мейсона, эквивалентная функция, метод обращения, разложение Хевисайда, двух моментная аппроксимация, функция распределения, неполная гамма-функция.

TWO-MOMENT APPROXIMATION METHOD APPLICATION SYSTEMATIC PROCEDURE FOR THE FUNCTION DETERMINATION OF STOCHASTIC NETWORK TIME DISTRIBUTION IMPLEMENTATION

Kanaev Andrey., Karabanov Yuriy., Privalov Andrey
Emperor Alexander I Saint-Peterburg State Transport University
Russia, Saint-Petersburg, Moskovsky pr., 9
emails: kanaevak@mail.ru, karabanov1994@yandex.ru, aprivalov@inbox.ru

Abstract: In this article, we consider the developed by the authors procedure for the repeated application of the moment approximation spirit method in determining the stochastic network equivalent function, which greatly simplifies the task of determining the implementation time distribution function for the simulated process.

Keywords: the topological transformation of stochastic networks, Mason equation, Equivalent function, treatment method, Heaviside decomposition, two-moment approximation, Distribution function, Incomplete gamma function.

Введение. Современные системы поддержки принятия решений по управлению сложными организационно-техническими системами требуют включения в состав модуля информационно-расчетных задач таких расчетных моделей, которые позволяют получать достаточно точные результаты в масштабе времени, близком к реальному. При этом модели должны не только адекватно отображать функционирование системы в конкретных условиях, но и производить оценку качества (эффективности) по показателям, согласующимся с требованиями макросистемы.

Одним из методов моделирования, позволяющих разрабатывать модели, удовлетворяющие указанным выше требованиям, является метод топологического преобразования стохастических сетей (ТПСС) [1], известным также под названием GERT (Graphical Evaluation and Review Technique) [2,3].

Метод предполагает представление процесса функционирования системы в виде стохастической сети с последующим определением ее эквивалентной функции, математического ожидания и дисперсии времени успешной реализации моделируемого процесса, [4].

В работах [1,5,6] были описаны способы получения функции распределения времени успешной реализации и спектральных характеристик моделируемого процесса из эквивалентной функции путем использования методов двух- и четырех - моментной аппроксимации, а также метода обращения, основанного на использовании разложения Хевисайда. [7].

Однако увеличение размерности стохастической сети приводит к значительному усложнению эквивалентной функции, определяемой из уравнения Мейсона для замкнутых потоковых графов [2,3]

Понятно, что это приводит к увеличению громоздкости получаемых формульных соотношений, а зачастую и к невозможности использования метода обращения, что обусловлено сложностью точного определения большого числа полюсов эквивалентной функции. Кроме того, использование для определения функции распределения методов двух- и четырех- моментной аппроксимации при моделировании процессов функционирования систем в условиях антагонистических конфликтов может привести к недопустимо большой погрешности получаемых результатов моделирования [8].

В настоящей статье на примере модели процесса функционирования системы передачи информации в условиях конфликта с системой кибервоздействия нарушителя [8] предлагается систематическая процедура использования метода двухмоментной аппроксимации, значительно упрощающая получение функции распределения времени успешной реализации моделируемого процесса.

Постановка задачи. Пусть имеется система передачи информации (СПИ), под которой понимается совокупность технических средств, объединенных в единую технологическую цепочку, использующих общий физический принцип обработки и передачи сигналов, а также определенный порядок взаимодействия технических средств между собой, осуществляющая доставку потока данных пользователям. Указанная СПИ функционирует в условиях деструктивных кибервоздействий

нарушителя, который за случайное время $t_{рп}$ с функцией распределения $R(t)$ обнаруживает факт передачи информации и реализует воздействие, не позволяющее осуществлять доставку достоверных данных пользователям.

Если деструктивное воздействие нарушителя на СПИ отсутствует, то она функционирует в условиях постоянно действующих случайных воздействий и обеспечивает успешную доставку данных

за случайное время $t_{пс}$ с функцией распределения $B(t)$. В противном случае, в течение времени передачи данных нарушителем будет реализовано деструктивное кибервоздействие, которое обнаруживается анализатором качества функционирования или оператором, и, после восстановления работоспособности, СПИ переключается в такой режим работы, который обеспечивает доставку пользователям достоверных данных в новых условиях. При этом время обнаружения факта деструктивного воздействия нарушителя и смены режима работы $t_{в}$ является случайным с функцией распределения $D(t)$. В новом режиме работы СПИ обеспечивает успешную доставку данных за

случайное время $t_{нр}$ с функцией распределения $A(t)$.

Функции распределения времени оказания нарушителем деструктивного кибервоздействия, успешной доставки данных в различных условиях, а также обнаружения факта деструктивного воздействия и смены режима работы, определяются с использованием моделей, описанных в [9, 10, 11].

Требуется определить функцию распределения и среднее время успешной доставки данных в СПИ.

Решение. Порядок решения задачи соответствует предлагаемой авторами систематической процедуре, которая заключается в реализации следующей последовательности:

Шаг 1. Составление стохастической сети моделируемого процесса, в т.ч. и с использованием подхода, изложенного в [13];

Шаг 2. Укрупнение стохастической сети, таким образом, чтобы ветви соответствовали отдельным, самостоятельно реализуемым композиционным подпроцессам;

Шаг 3. Для ветвей, отображающих композиционные процессы, с использованием уравнения Мейсона для замкнутых графов определяются их (частные) эквивалентные функции;

Шаг 4. Из каждой частной эквивалентной функции определяются первый начальный и второй центральный моменты случайного времени их реализации;

Шаг 5. Определяются параметры формы и масштаба неполной гамма-функции по формулам (16...19);

Шаг 6. Составляется эквивалентная функция укрупненной стохастической сети, элементами которой являются изображения по Лапласу неполных гамма функций с параметрами, определенными на шаге 5;

Шаг 7. Для фрагментов эквивалентной функции, представляющих собой произведение изображений по Лапласу ставится в соответствие изображение неполной гамма-функции с математическим ожиданием, равным сумме математических ожиданий и дисперсией, равной сумме дисперсий, как это сделано при проведении преобразований в (20). Таким образом, получается выражение, представляющее алгебраическую сумму изображений неполных гамма-функций;

Шаг 8. Осуществление по членного перехода в пространство оригиналов и получение плотности распределения вероятностей времени реализации моделируемого процесса;

Шаг 9. Интегрирование полученного на шаге 8 результата с переменным верхним пределом и определение искомой функции распределения.

Завершение процедуры.

При расчетах предполагалось, что среднее время реализации частных процессов составляло: $T_b = 3,3$ мин., $T_a = 10$ мин., $T_d = 14$ мин., $T_r = 3$ мин. Дисперсия времени их реализации полагалась равной: $D_b = 11 \text{ мин}^2$, $D_a = 100 \text{ мин}^2$, $D_d = 196 \text{ мин}^2$, $D_r = 9 \text{ мин}^2$.

Анализ полученных результатов показывает, что систематическая процедура применения метода двухмоментной аппроксимации имеет погрешность при определении функции распределения времени свершения процесса, представленного в виде стохастической сети, не превышающую 2% относительно строго полученного результата. При этом аппроксимация реальной функции распределения по двум моментам случайного времени приводит к погрешности получаемых результатов до 30%.

Тем более, что используемая неполная гамма-функция содержится в библиотеке встроенных функций большинства известных математических пакетов прикладных программ. Это свидетельствует о целесообразности использования предложенной процедуры для упрощения задачи определения функции распределения с достаточной для инженерных расчетов точностью.

Заключение. Таким образом, в настоящей статье рассмотрено новое решение известной задачи, для которого авторами предложена систематическая процедура применения метода двух моментной аппроксимации при определении функции распределения времени реализации случайного процесса, представленного в виде стохастической сети. Использование в методе двух моментной аппроксимации неполной гамма-функции не является обязательным условием для реализации процедуры и закон распределения времени свершения композиционных ветвей в укрупненной стохастической сети может быть выбран любым другим. Порядок проведения преобразований при этом не изменяется.

Предложенная систематическая процедура позволяет получать результаты, имеющие погрешность, не превышающую 2 %, что является достаточным для большинства инженерных расчетов.

СПИСОК ЛИТЕРАТУРЫ

1. Привалов А.А. Метод топологического преобразования стохастических сетей и его использование для анализа систем связи ВМФ. // СПб, ВМА, 2000 г. – 166 с.
2. Pristker A.A.B., Happ W.W. GERT: Graphical Evaluation and Review Technique, Part I, Fundamentals. // The Journal of Industrial Engineering (May, 1966).
3. Pristker A.A.B., Whitehouse G.E. GERT: Graphical Evaluation and Review Technique, Part II. // The Journal of Industrial Engineering (June, 1966).
4. Филлипс Д., Гарсиа-Диас А. Методы анализа сетей: Пер. с англ. // Мир: 1984. – 496 с.
5. Привалов А.А., Симонов М.В. Метод поиска функций распределения времени доставки кадров данных в сетях передачи данных. // Техника средств связи. / Сборник научных статей НПК «Красная Заря». Серия: Техника проводной связи. Выпуск 4. – СПб: «Политехника», 1992 г. – С. 56-61.
6. Бекбаев Г.А., Вандич А.П., Привалов А.А., Привалов Ал.А., Ясинский С.А. Динамическая модель процесса функционирования телекоммуникационной сети ОАО «РЖД» в нестационарных условиях. // Информация и космос. 2015г., № 4. – С. 13-17.
7. Дёч Г. Руководство к практическому применению преобразований Лапласа: Пер. с нем. // М.: «Государственное издательство физико-математической литературы», 1960г. – 208 с.
8. Куделя В.Н., Привалов А.А., Петриева О.В., Чемиренко В.П. Методы математического моделирования систем и процессов связи. // По общ. ред. Чемиренко В.П. – СПб: Изд-во Политехн. ун-та, 2009 г. – 368с.
9. Вандич А.П., Кудряшов В.А., Привалов А.А. Моделирование процесса работы в ЕСМА. // Автоматика, связь, информатика. 2012г., № 6. – С. 24-26.
10. Вандич А.П., Евлевская Н.В., Привалов А.А., Привалов Ал.А. Комплексная модель воздействия злоумышленника на автоматизированные системы управления технологическими процессами. // «Актуальные проблемы инфотелекоммуникаций в науке и образовании». Сборник трудов II Международной научно-технической и научно-методической конференции. 2013. – С. 118-122.
11. Евлевская Н.В., Привалов А.А. Модель информационного воздействия на объекты телекоммуникационной сети. // Известия Петербургского университета путей сообщения. 2015. № 1 (42). – С. 72-77.
12. Мартин Дж. Системный анализ передачи данных. Том 2. // Пер. с англ. – М.: Мир, 1975г. – 434с.
13. Рытов М.Ю., Мегаев К.А. Алгоритм управления трафиком в среде корпоративного портала. // Вестник Брянского государственного технического университета. 2014. – № 1(41). – С. 87-93
14. Еременко, В.Т. Анализ моделей управления трафиком в сетях АСУП на основе технологии MPLS / В.Т. Еременко, С.В. Еременко, Д.В. Анисимов, С.А. Черепков, А.А. Лякишев // Информационные системы и технологии. –2013. – № 1. – С. 106-112.
15. Андрущенко В.А., Скалозуб В.В. Метод структурного преобразования стохастических сетей для ГЕРТ-моделирования технологических и экономических процессов/ Наука и прогресс транспорта. Вестник Днепропетровского университета железнодорожного транспорта им. акад. В. Лазаряна. – Д.: Изд-во ДНУЖТ, 2008. – С. 167-180

УДК 004.056.57

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА КАНАЛА УПРАВЛЕНИЯ РОБОТИЗИРОВАННЫХ СИСТЕМ

Коцыняк Михаил Антонович, Гудков Михаил Александрович, Сафонов Алексей Александрович,
Арутюнян Борис Артурович

Военная академия связи имени Маршала Советского Союза С.М. Будённого,
Россия, Санкт-Петербург, Тихорецкий пр.,3,
emails: vlasenko199@yandex.ru, asuetin5@yandex.ru

Аннотация: В статье рассмотрен способ защиты канала управления роботизированных систем на основе криптографических алгоритмов.

Ключевые слова: роботизированная система; канал управления; метод преобразования.

CRYPTOGRAPHIC PROTECTION OF A CONTROL PATH OF ROBOTIC SYSTEMS

Mikhail Kocinyak, Mikhail Gudkov, Alexey Safonov, Boris Arutunyan
Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tihoreckii' av. 3,
emails: vlasenko199@yandex.ru, asuetin5@yandex.ru

Abstract: In article, the way of protection of a control path of robotic systems on the basis of cryptographic algorithms is considered.

Keywords: robotic system; control path; transformation method.

Автоматизированные и роботизированные системы обладают неразрывной связью между входящими в них вычислительными и физическими элементами. Сегодня представители таких систем могут быть найдены в самых разнообразных областях - космос, автомобильные, химическая технология, гражданская инфраструктура, энергетика, здравоохранение, производство, транспорт, и потребительские устройства. Такой класс систем рассматривается как киберфизические системы [1].

С одной стороны, киберфизические системы за счет распределенной сети датчиков и блоков управления позволяют решить многие практические задачи, позволяющие сэкономить время и уменьшить человеческие потери, за счет выполнения опасных заданий роботизированными системами.

С другой стороны, за счет использования открытых радиоканалов и протоколов киберфизические системы подвержены воздействию компьютерных атак, которые в наилучшем случае могут привести к нарушению работоспособности сети, а в худшем к перехвату управления.

К наиболее распространенным компьютерным атакам на киберфизические системы относятся: активные и пассивные виды компьютерных атак [2].

Учитывая вышеизложенное, в настоящее время остро стоит вопрос о защите киберфизических систем и каналов управления ими. С этой целью предлагается использовать криптографические протоколы и алгоритмы [3].

Для реализации защиты канала управления киберфизической системы, рациональным является симметричный алгоритм AES, который отличается криптостойкостью и быстродействием.

В настоящее время криптография решает следующие основные задачи:

Обеспечение конфиденциальности сообщений – решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, не имеющих права к ней.

Обеспечение целостности данных –невозможность несанкционированного изменения информации.

Аутентификация – подтверждение подлинности сторон и самой информации в процессе обмена данными.

Невозможность отказа от авторства – предотвращение отказа от совершенных действий.

Эти задачи защиты данных реализованы в специальном аппаратном блоке, который называют криптографическим ускорителем (криптографическим блоком).

Для обеспечения криптографически стойкого протокола управления в разработанной роботизированной системе используется микроконтроллер с 32-разрядным ядром ARM Cortex-M4F с криптографическим ускорителем stm32f415rgt производства компании «STMicroelectronics». Для того, чтобы чип дешифровал принятые пакеты, в качестве алгоритма дешифрования используется AES с длиной ключа 128 бит.

В качестве алгоритма распределения ключей был рассмотрен и реализован алгоритм Диффи–Хеллмана, который позволяет двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания, но защищенный от подмены, канал связи.

Таким образом, в настоящей статье представлен пример создания роботизированного комплекса, как элемента КБС, с защищенной системой управления им на основе алгоритма шифрования AES, являющимся на сегодняшний момент наиболее криптостойким.

Кром того, для защиты от атаки «грубого перебора» криптографического ключав системе управления необходимо реализовывать алгоритм распределения ключей, позволяющий генерировать новый ключ, каждый раз перед выполнением команды.

СПИСОК ЛИТЕРАТУРЫ

1. Обеспечение живучести информационных систем (часть 3. Методы обеспечения и повышения живучести). Елисеев А.И., Долгов А.А., Хорохорин М.А., Лаута О.С., Набатов К.А. Вестник Воронежского института ФЦИН России. 2013. №1. С.91-94.
2. Методика оценки защищенности информационно-телекоммуникационной сети в условиях информационного противодействия. Коцыняк М.А., Иванов Д.А., Лаута О.С., Нечепуренко А.П. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно- технической конференции. В 3-х томах. 2017. С. 83-89.
3. Защита канала управления роботизированных систем. Баранов В.В., Гудков М.А., Крибель А.М., Лаута О.С., Нечепуренко А.П. В сборнике: Актуальные проблемы обеспечения информационной безопасности. труды Межвузовской научно-практической конференции. 2017. С. 32-37.
4. Информационной безопасности. труды Межвузовской научно-практической конференции. 2017. С. 47-52.

УДК 004.056.53

**МЕТОДИКА ОЦЕНКИ КОМПЛЕКСНОГО ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ НА ИТКС
СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ**

Коцыняк Михаил Антонович, Ястребов Владимир Васильевич, Клиншов Илья Андреевич,
Гулевич Антон Владимирович
Военная Академия связи,
Россия, Санкт-Петербург, Тихорецкий проспект, 3
emails: dmitry-chikov@rambler.ru

Аннотация: В докладе рассмотрена методика прогнозирования распределения КА с учетом места и роли элементов в ИТКС, определение очередности воздействия на элементы ИТКС и наиболее опасных КА, что в свою очередь, позволит формировать исходные данные для принятия мер защиты элементов и ИТКС в целом.

Ключевые слова: матрица, дифференцированный, субэлементы.

**ASSESSMENT METHODOLOGY OF INTEGRATED INFORMATION IMPACT OF INFORMATION AND
TELECOMMUNICATION SYSTEMS SPECIAL PURPOSE**

Kocinac Michael, Yastrebov Vladimir, Klinshov Ilya, Gulevich Anton
Military Academy of communications
Russia, Saint-Petersburg, Tikhoretsky prospect, 3
emails: dmitry-chikov@rambler.ru

Abstract: the article considers the methodology of forecasting the distribution of KA taking into account the place and role of elements in information and telecommunication systems, prioritizing the impact on the elements of ITKS and the most threat ON, which in turn, will generate baseline data for the adoption of measures of protection elements and of ITKS in General.

Keywords: matrix, different, sub.

Введение. Анализ построения современных ИТКС показывает, что их архитектурные решения в общем случае идентичны. Они представляют собой территориально распределённые системы, объединяющие в своем составе ЛВС и отдельные компьютеры, которые осуществляют обмен данными друг с другом и могут иметь общие ресурсы и единое управление. Увеличение объёмов хранимой и передаваемой информации, территориальная распределенность сетей связи приводит к наращиванию потенциальных возможностей для технической компьютерной разведки противника.

Основным воздействующим фактором на ИТКС являются компьютерные атаки (КА), являющиеся частью информационного воздействия. Очевидно, что в условиях информационного воздействия (ИВ) довольно затруднено выбрать средства и способы защиты ИТКС, так как ресурс ограничен. Одним из путей разрешения этого противоречия является дифференцированный подход к защите ИТКС и ее элементов, который заключается в выборе наиболее актуальных для сложившейся обстановки направлений защиты. Для обоснования направления защиты и ее элементов, асимметричных возможностям КА, необходимо разработать методику оценки воздействия КА на ИТКС и ее элементы.

Целью методики является прогнозирование распределения КА с учетом места и роли элементов в ИТКС, определение очередности воздействия на элементы ИТКС и наиболее опасных КА, что в свою очередь, позволит формировать данные для принятия мер защиты элементов и ИТКС.

В основу методики положено определение степени опасности КА, для чего необходимо рассмотреть физические основы отдельных КА, особенности их воздействия, характер проявления на элементах ИТКС. Методика предназначена для обоснования принятия решений по защите элементов ИТКС от КА должностными лицами на этапах формирования, развертывания и функционирования ИТКС.

Заключение. Результатом оценки ИВ на ИТКС является матрица сравнения критериев опасности КА на элементы ИТКС. Матрица сравнения критериев опасности КА, выражающий весовые значения критериев относительно общей цели (вскрытие ИТКС). Таким образом, используя метод анализа иерархий, представляется возможным определить вероятность воздействия на субэлементы ИТКС оцениваемыми КА. Полученные результаты могут быть уточнены на этапе детального планирования при аналитической защищенности ИТКС.

СПИСОК ЛИТЕРАТУРЫ

1. Коцыняк М.А., Иванов Д.А., Лаута О.С., Нечепуренко А.П. Методика оценки защищенности информационно-телекоммуникационной сети в условиях информационного противодействия. Радиолокация, навигация, связь. Международная научно-техническая конференция. В 3-х томах. 2017. С. 83-89
2. Лепешкин О.М., Харечкин П.В., Анализ Моделей Разграничения Доступа, Реализованных В Современных Социотехнических Системах. Инфокоммуникационные технологии. 2008. Т. 6. № 2. С. 91-93.
3. Антонюк Л.Я., Игнатов В.В. Эффективность радиосвязи и методы её оценки. – СПб.: ВАС, 1994. – 138 с.
4. Лепешкин О.М. Исследование функциональной Безопасности Систем Государственного Управления. Инфокоммуникационные технологии. 2007. Т. 5. № 3. С. 165-166.
5. Куприянов А.И., Шустов Л.Н. Радиоэлектронная борьба. Основы теории., 2011. – 789 с.

УДК 004.056.57

**МЕТОДИКА ПРОГНОЗИРОВАНИЯ ПРОТОКОЛЬНЫХ ВОЗДЕЙСТВИЙ НА
РОБОТИЗИРОВАННЫЕ СИСТЕМЫ**

Коцыняк Михаил Антонович, Дементьев Владислав Евгеньевич, Тесля Сергей Петрович,
Лаута Олег Сергеевич

Военная академия связи имени Маршала Советского Союза С.М. Будённого,
Россия, Санкт-Петербург, Тихорецкий пр., 3,
email: vlasenko199@yandex.ru, asuetin5@yandex.ru

Аннотация: В статье рассмотрен подход по прогнозированию протоколированных воздействий на роботизированные системы на основе метода двух функций.

Ключевые слова: роботизированная система; канал управления; метод преобразования.

TECHNIQUE OF FORECASTING OF LEGAL IMPACTS ON ROBOTIC SYSTEMS

Mikhail Kocinyak, Vladislav Dementiev, Sergei Teslya, Oleg Lauta

Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tihoreckii' av. 3,
email: vlasenko199@yandex.ru, asuetin5@yandex.ru

Abstract: In article approach on forecasting of the recorded impacts on robotic systemson the basis of a method of two functions is considered.

Keywords: robotic system; control path; transformation method.

Информация о сетевом трафике имеет статистический характер и представляет собой временные последовательности. Методы статистического анализа сетевого трафика широко освещены при их использовании в качестве инструментов прогнозирования загруженности каналов управления, определения потерь, качества управления и т.п. С точки зрения обеспечения сетевой безопасности, проводить анализ сетевого трафика крайне необходимо для решения задач сетевого администрирования, и мониторинга корректного функционирования роботизированных систем (РБС).

Как класс статистический анализ относится к поведенческим методам определения нарушений в каналах управления и основан на сопоставлении текущего состояния РБС с некими определенными заранее признаками, характеризующими штатное их функционирование. Методы статистического анализа имеют различные интерпретации, основанные на различных динамических характеристиках сетевого трафика [1], однако базовые принципы практически у всех идентичны. Неоспоримым преимуществом применения методов статистического анализа является возможность определения впервые реализовываемых методов негативного воздействия на объект атаки со стороны злоумышленника. Однако для его успешной реализации необходимо определить объект анализа, иметь определенные структурированные характеристики, образующие корректную конфигурацию, иметь критерии, по которым можно определить потенциальное протокольное воздействие (ПВ). Для уменьшения вероятности получения ошибочных результатов анализа, основного недостатка применения поведенческих методов выявления инцидентов информационной безопасности, при реализации комплексного подхода, положенного в основу разработки системы протокольной защиты каналов управления роботизированных систем (СПЗ КУ РБС) метод статистического анализа использовался совместно с методами нейросетевого и сигнатурного анализа [2].

Таким образом, основными решаемыми задачами являлись: определение анализируемых и контролируемых характеристик сетевого трафика – признаков ПВ, разработка методик оценки информативности и идентификации признаков ПВ, построение правил штатного функционирования (ПШФ) КУ РБС, разработка алгоритма прогнозирования, а также интеграция методов прогнозирования ПВ в разработанную СПЗ КУ РБС. Для идентификации ПВ необходимо сформировать их сигнатуры. Здесь учитываются как классические признаки ПВ, так и добавочные – фаза ПВ и тип угрозы. Для прогнозирования фиксируется объём данных, т.е. длина пакета.

Таким образом, имеем три признака: "пороговый на основе шаблона штатного функционирования сети (ШШФС)", "доверительного интервала", "доверительного интервала на основе ШШФС". Использование трех признаков сравнения характеристик позволяет с более высокой степенью вероятности выявить именно действия, направленные на нарушение безопасного сетевого взаимодействия. При статистическом анализе необходимо учитывать, что трафик РБС обладает свойством масштабной инвариантности – имеет особую фрактальную (самоподобную) структуру, сохраняющуюся на разных масштабах. В процессе передачи возникают большие всплески при относительно низком среднем уровне трафика, что важно учитывать при статистическом анализе [3].

Производя периодический или постоянный анализ состояния РБС, появляется возможность идентифицировать действия злоумышленников, направленные на подготовку к проведению атак: сканирование портов, службы, получение информации об используемом прикладном, системном программном обеспечении и системах защиты (на этапе рекогносцировки).

Описанные выше методы обнаружения попыток нарушения безопасности в КУ РБС основаны на том обстоятельстве, что в этом случае могут изменяться некоторые статистические характеристики потока пакетов. Сопоставляя результаты, можно сделать вывод, что диапазоны значений характеристик штатного функционирования КУ РБС, имеют относительное постоянство уровней значений математических ожиданий и дисперсий [4]. При возникновении нештатной ситуации аналогичные оценки по различным характеристикам изменяются значительно.

СПИСОК ЛИТЕРАТУРЫ

1. Защита канала управления роботизированных систем. Баранов В.В., Гудков М.А., Крибель А.М., Лаута О.С., Нечепуренко А.П. В сборнике: Актуальные проблемы обеспечения информационной безопасности. труды Межвузовской научно-практической конференции. 2017. С. 32-37.
2. Обеспечение живучести информационных систем (часть 3. Методы обеспечения и повышения живучести). Елисеев А.И., Долгов А.А., Хорохорин М.А., Лаута О.С., Набатов К.А. Вестник Воронежского института ФСИИ России. 2013. №1. С.91-94.
3. Методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного воздействия. Коцыняк М.А., Лаута О.С., Нечепуренко А.П., Штеренберг И.Г. Труды учебных заведений связи. 2016. Т. 2. № 4. С. 82-87.
4. Применение метода топологического преобразования стохастических сетей для оценки эффективности средств защиты. Баранов В.В., Крибель А.М., Лаута О.С., Нечепуренко А.П. В сборнике: Актуальные проблемы обеспечения информационной безопасности. труды Межвузовской научно-практической конференции. 2017. С. 47-52.

УДК 004.056.57

ВЕРОЯТНОСТНО-ВРЕМЕННЫЕ ХАРАКТЕРИСТИКИ АТАК НА РОБОТИЗИРОВАННЫЕ СИСТЕМЫ

Кузнецов Сергей Иванович, Иванов Денис Александрович, Власенко Максим Андреевич,
Латушко Николай Александрович

Военная академия связи имени Маршала Советского Союза С.М. Будённого,
Россия, Санкт-Петербург, Тихорецкий пр.,3,
email: vlasenko199@yandex.ru, asuetin5@yandex.ru

Аннотация: В статье рассматриваются атаки на роботизированные системы, а так же представлен подход к определению их вероятностно – временных характеристик.

Ключевые слова: *роботизированная система; таргетированная кибернетическая атака; метод преобразования.*

PROBABILISTIC AND TIME CHARACTERISTICS OF THE ATTACKS TO ROBOTIC SYSTEMS

Sergey Kuznetsov, Denis Ivanov, Maxim Vlasenko, Nikolay Latushko
Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tihoreckii' av. 3,
email: vlasenko199@yandex.ru, asuetin5@yandex.ru

Abstract: In article, the attacks to robotic systems are considered, and approach to definition of their probabilistic and time characteristics is also presented.

Keywords: *robotic system; targeted cybernetic attack; transformation method.*

XXI Век - век информационных технологий, в котором все очень быстро меняется. В настоящее время мир стоит на грани новой промышленной революции – четвертой или Индустрия 4. «Умные» фабрики, заводы-принтеры и интернет вещей уже заменяют человека в производстве.

Основные компоненты Индустрии 4.0: умные сенсоры, которые позволяют собирать данные в процессе производства; передача больших объемов данных людям, другим машинам и заводам; облачные сервисы, которые предоставляют данные из любого места; «умные станки», которые сами определяют свою производственную траектории, т.е. охватывают все сферы жизни человека.

Технологически это означает не только создание «единой сети станков и машин», но и самостоятельную и непрерывную оптимизацию их текущей работы, большую гибкость производств, персонализацию заказов и более тесную связь с потребителем.

В рамках проекта немецкого правительства Industry 4.0 по компьютеризации промышленности в 2006 году Хелен Джилл ввел понятие киберфизические системы, которые включают в себя:

- системы управления производством;
- беспилотные летательные аппараты и автомобили;
- системы военного назначения;
- роботизированные системы.

Особое внимание зарубежное руководство уделяет внимание роботизированным системам. В качестве основных каналов воздействия на них рассматривают следующие:

- воздействия на подсистемы управления;
- воздействие на человеко-машинный интерфейс;
- воздействия на протоколы взаимодействия;
- воздействия на устройства, входящие в роботизированные системы.

С целью воздействия на роботизированные системы злоумышленник перешел от массовых атак к таргетированным, или целевым. Целевая атака всегда строится под объект воздействия, являясь продуманной операцией. Отличием от других атак является: адресность; скрытность; продолжительность; использование разнородных инструментов и методов; изменчивость вектора атаки, ее инструментария по мере развития; наличие центра управления атакой; результативность.

Таргетированная кибернетическая атака (ТКА) [1] обладает вероятностно-временными характеристиками (ВВХ), определение их позволит оценить степень их опасности, выбрать и реализовать меры защиты. С этой целью предлагается использовать профильные модели ТКА и метод топологического преобразования стохастических сетей (ТПСС) [2].

Профильная модель – условное представление (последовательность действий или алгоритм) реального объекта, системы или процесса (компьютерных атак) в форме, которая создается для более глубокого изучения их функционирования.

Стохастическая сеть – совокупность взаимоувязанных узлов (вершин) и ветвей, соединение которых соответствует алгоритму функционирования исследуемой системы.

В методе ТПСС исследуется не система, а целевой процесс, который она реализует. Этот сложный процесс декомпозируется на элементарные, каждый из которых может характеризоваться функцией распределения времени его выполнения, плотностью вероятности, вероятностью или средним и дисперсией времени выполнения.

Сущность метода ТПСС состоит в представлении анализируемого процесса в виде стохастической сети, замене множества элементарных ветвей сети одной эквивалентной и последующим определением эквивалентной функции сети, начальных моментов и функции распределения случайного времени ее реализации, т.е. реализации анализируемого процесса.

Анализ вероятностно-временных характеристик ТКА позволит обосновать направления разработки системы защиты РТС, целью которой является предотвращение (затруднение) реализации ТКА.

СПИСОК ЛИТЕРАТУРЫ

1. Модель таргетированной кибернетической атаки. Коцыняк М.А., Иванов Д.А., Лаута О.С., Нечепуренко А.П. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIII Международной научно-технической конференции. В 3-х томах. 2017. С. 90-98.
2. Применение метода топологического преобразования стохастических сетей для оценки эффективности средств защиты. Баранов В.В., Крибель А.М., Лаута О.С., Нечепуренко А.П. В сборнике: Актуальные проблемы обеспечения и

УДК 004.056.53

ПОДХОД К ОЦЕНКЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ОТ ТЕХНИЧЕСКОЙ КОМПЬЮТЕРНОЙ РАЗВЕДКИ

Лаута Олег Сергеевич, Клиншов Илья Андреевич,
Ястребов Владимир Васильевич, Русаков Егор Владимирович,
Военная Академия связи,
Россия, Санкт-Петербург, Тихорецкий проспект, 3
email: laos-82@yandex.ru

Аннотация: В докладе представляется один из подходов к оценке защищенности информационно-телекоммуникационной сети специального назначения от технической компьютерной разведки на основе использования оригинальных моделей, учитывающих специфику системы защиты и сценарии действий нарушителей.

Ключевые слова: техническая компьютерная разведка, компьютерная атака, информационно-телекоммуникационная сеть.

THE APPROACH TO THE SECURITY ASSESSMENT OF INFORMATION-TELECOMMUNICATION NETWORKS OF SPECIAL PURPOSE FROM TECHNICAL COMPUTER INTELLIGENCE

Lauta Oleg, Klinshov Ilya, Yastrebov Vladimir, Rusakov Yegor
Military Academy of communications
Russia, Saint-Petersburg, Tikhoretsky prospect, 3
email: laos-82@yandex.ru

Abstract: Theses seem to be one of the approaches to the security assessment of information-telecommunication networks of special purpose from technical computer intelligence through the use of the original models, taking into account the specifics of the protection system and scripts of actions of violators.

Keywords: technical computer intelligence, computer attack, information-telecommunication network.

Введение. Техническая компьютерная разведка (далее - ТКР) – специально подготовленная, согласованная по цели, месту, времени и формам деятельность, направленная на извлечение и специальную обработку информации из информационно-телекоммуникационной сети специального назначения (ИТКС), а также особенностях их построения и функционирования.

В современных условиях ведение ТКР объективно обладает большим потенциалом по вскрытию функционирующей ИТКС и является предварительным этапом перед воздействием активных компьютерных атак (далее – КА).

В связи с этим возникает необходимость в оценке защищенности ИТКС в условиях КР и КА. Анализ показал, что в большинстве нормативно-правовых документов отсутствует требуемая методика, а в ГОСТе РВ 51987-2002 для оценки защищенности информационных и программных ресурсов рекомендуется разработать оригинальные модели, учитывающие специфику системы защиты и сценарии действий нарушителей.

Для определения оценки защищенности представляется объект ИТКС, основными элементами в котором являются маршрут, направления связи, которые характеризуются вероятностью защищенности.

В ходе анализа ИТКС исследован в обобщенном виде процесс функционирования ИТКС в условиях воздействия КА и были определены основные этапы.

Для осуществления передачи оперативной информации сначала операторы ИТКС входят в связь, на что затрачивается определенное время.

С некоторого времени система информационного воздействия реализует КА за среднее время, которую оператор ИТКС сможет обнаружить за время, определяемое временем реакции системы мониторинга ИТКС ОЗУ.

Обнаружив воздействие КА, оператор ИТКС будет принимать меры по восстановлению связи, в частности, переход на резервные маршруты и принятие других мер. Временные затраты при этом будут определяться оперативностью управления сетью, маршрутом, каналом, средством защиты.

После этого операторы ИТКС восстанавливают связь, на что затрачивается некоторое время, и передача оперативной информации возобновляется.

Среднее время, затрачиваемое на принятие мер защиты, вхождение в связь характеризует реакцию системы управления на воздействие КА, то есть вышеуказанные временные интервалы суммируются.

Среднее время от момента передачи полезной информации до момента воздействия КА назовем временем реакции комплекса технической компьютерной разведки. Реакция комплекса ТКР определяется временем доразведки, необходимым для обнаружения нового маршрута передачи оперативной информации после принятия мер защиты, и временем, необходимым КА для реализации повторного воздействия на идентифицированный маршрут передачи оперативной информации.

Среднее время реакции комплекса технической компьютерной разведки и воздействия КА характеризует среднее время воздействия противника на ИТКС КА.

Интервал времени, определяемый реакцией КА и затратами времени для реализации мер защиты ИТКС от КА, назовем циклом функционирования комплекса ТКР. В реальных условиях один цикл работы комплекса ТКР отличается по длительности от другого. Это обусловлено тем, что составляющие циклов – время доразведки, время подготовки комплекса ТКР к работе, принятие мер защиты маршрута от КА, время вхождения в связь и т.д. – имеют, в общем случае, различную длительность в каждом цикле. С учетом этого возможно определить вероятность защищенности ИТКС от КА как на одном маршруте, так и на маршруте передачи информации, состоящий из нескольких интервалов связи, организованных средствами связи различных родов (радио, радиорелейные, тропосферные, спутниковые и проводные).

Совокупность маршрутов образуют направление связи (НС). Исходя из этого возможно определить вероятность защищенности НС, которое может характеризоваться вероятностью сохранения на НС хотя бы одного маршрута.

Для оценки вероятности защищенности ИТКС необходимо определить вероятность защищенности маршрутов передачи оперативной информации, для чего необходимо определить вероятностно-временные характеристики КА, а также комплекса ТКР.

С этой целью предлагается использовать профильные модели КА (комплекса ТКР) и метод топологического преобразования стохастических сетей (ТПСС). Результаты расчетов представляются в виде зависимостей: а) зависимость интегральной функции распределения вероятностей от времени работы комплекса ТКР, б) зависимость среднего времени компьютерной разведки комплексом ТКР от вероятности вскрытия ИТКС.

Вышеуказанные результаты дают возможность определить вероятность решения разведывательной задачи комплексом ТКР за время не более заданного, а также среднее время ведения технической компьютерной разведки ИТКС комплексом ТКР. При анализе функции распределения вероятности можно видеть, что при вероятности обнаружения 0,9 и функции распределения вероятности 0,9 время ведения технической компьютерной разведки составляет 100 минут. Для сокращения этих показателей вероятностно-временная характеристика ТКР будет вестись непрерывно и зависит от параметров КА и комплекса ТКР.

Результаты расчета вероятности защищенности ИТКС представлены в виде зависимостей: а) зависимость вероятности защищенности маршрута от среднего времени реакции комплекса

технической компьютерной разведки, б) зависимость вероятности защищенности ИТКС от вероятности защищенности НС.

В качестве исходных данных использовались данные, а также значения, соответствующие действующим нормативно-правовым документам (нормативные требования оперативного управления элементами маршрутов и НС ИТКС).

Заключение. Анализ полученных результатов показал, что защищенность ИТКС в условиях КА зависит от времени ведения противником ТКР, являющей предварительным этапом при реализации активных компьютерных атак. Для выполнения общих тактико-технических требований системы специальной связи время ведения противником разведки должно быть не ниже 50 мин.

Однако, в интересах сокращения цикла управления противника ТКР будет вестись непрерывно, в этом случае среднее время будет определяться только подсистемой поиска комплекса ТКР.

Таким образом, полученные результаты позволяют обосновать требования к построению системы защиты в условиях КА и времени реакции системы защиты при ведении противником ТКР.

СПИСОК ЛИТЕРАТУРЫ

1. Исследование функциональной безопасности систем государственного управления. Лепешкин О.М. Инфокоммуникационные технологии. 2007. т. 5. № 3. с. 165-166.
2. Анализ моделей разграничения доступа, реализованных в современных социотехнических системах. Лепешкин О.М., Харечкин П.В. Инфокоммуникационные технологии. 2008. т. 6. № 2. с. 91-93.
3. Методологический подход к оценке безопасности функционирования социальной и экономической системы управления региона. Бурлов В.Г., Лепешкин О.М., Кириллова Т.В. Проблемы экономики и управления в торговле и промышленности. 2013. № 2. с. 99-103.
4. Обеспечение устойчивости информационно-телекоммуникационных сетей в условиях информационного противоборства. Лаута О.С., Коцыняк М.А., Коцыняк М.М., Васюков Д.Ю., Осадчий А.И., Дементьев В.Е. СПб.: ВАС, 2014 – 117 с.
5. Устойчивость информационно-телекоммуникационных сетей. Лаута О.С. Коцыняк М.А., Кулешов И.А. СПб.: Издательство Политехнического университета, 2013 – 93 с.

УДК 004.056.53

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ НА ОСНОВЕ ВЫБОРА ЗАЩИЩЕННЫХ ИНТЕРВАЛОВ СВЯЗИ ОТ РАДИОПОДАВЛЕНИЯ

Митрофанов Михаил Валерьевич., Ракицкий Станислав Николаевич, Чиков Дмитрий Викторович
Военная Академия связи

Россия, Санкт-Петербург, Тихорецкий проспект, 3
emails: dmitry-chikov@yandex.ru

Аннотация: В докладе рассмотрен подход повышения помехозащищенности систем управления и связи. Предлагается подход к обоснованию выбора, защищенного от радиоподавления интервала связи, на основе выбора защищенного интервала связи от радиоподавления.

Ключевые слова: помехозащищенность, радиоподавление.

SECURITY OF TELECOMMUNICATION NETWORKS BASED ON THE SELECTION OF PROTECTED INTERVALS WHEN JAMMING

Mitrofanov Michael, Rakitskiy Stanislav, Chikov Dmitry
Military Academy of communications

Russia, Saint-Petersburg, Tikhoretsky prospect, 3
emails: dmitry-chikov@yandex.ru

Abstract: the article considers the problem of increasing noise immunity of the systems of control and communication. The approach to substantiation of a choice that is protected from jamming interval when, based on the selection of protected interval communications from jamming.

Key words: noise immunity; radio countermeasure.

Введение. В связи с усложнившейся военно-политической обстановкой в мире, задача повышения помехозащищенности систем управления и связи является весьма острой и до сих пор не нашла своего решения в большинстве прикладных задач [1]. Решению этой задачи способствует комплексное использование различных методов и средств (сигналов сложной формы, оптимальных методов их обработки, фазированных антенных решеток, быстродействующей цифровой техники, современной технологии, организационных мер). Однако применение этих способов не обеспечивает выполнение требований по помехозащищенности при постановке противником заградительных помех [2].

Таким образом, возникло противоречие между развитием способов воздействия противника на радио электронные средства (РЭС) и устаревшими подходами к обеспечению и оценки помехозащищенности РЭС.

С целью устранения указанного противоречия предлагается подход к обоснованию выбора, защищенного от радиоподавления интервала связи [3].

Вероятность радиоподавления зависит от:

- вероятности частотно-временного контакта излучения преднамеренной помехи с приемником сигнала;
- вероятности принятия решения на подавление;
- вероятности доставки забрасываемых передатчиков помех (ЗПП) к объекту подавления.

Исходя из условий задачи, примем что вероятность радиоподавления и вероятность доставки ЗПП к объекту подавления равны единицы, задавшись допустимым значением вероятности принятия решения равным 0,15.

Значение вероятности частотно-временного контакта излучения преднамеренной помехи с приемником сигнала определяется по методике, изложенной в [4]. По графику (таблице) табулированной функции Лапласа для трассы радио подавления (РП) определяется допустимое значение аргумента U . С помощью U рассчитываем среднее превышение уровня сигнала над уровнем помех на входе приемника, при котором среднее превышение уровня сигнала над уровнем помех на входе приёмника равно сумме среднеквадратичного отклонения превышения уровня сигнала над уровнем помех и значения величины среднего превышения уровня сигнала над уровнем помех на входе приемника.

На реальных трассах РП величина значения среднего превышения уровня сигнала над уровнем помех на входе приемника определяется из соотношения уровня сигнала над уровнем помех на входе приемника [5].

Значение уровня сигнала и уровня помех на входе приемника определяется с помощью первого уравнения передачи, где суммарный множитель ослабления сигнала (помехи) на интервале связи, определяется протяженностью интервала связи и рабочей частотой. Приняв, что коэффициент полезного действия фидеров антенных устройств средств связи и станций РП равны между собой, входы передающих антенн и выходы передатчиков, а также выходы приемных антенн и входы приемников полностью согласованы по сопротивлению, и все антенны согласованы по поляризации, получим выражение, удобное для расчета дальности связи.

По графику нормального распределения функции Лапласа находим параметр распределения функции Лапласа. Анализ результатов, полученных с помощью приведенного подхода показывает, что протяжённость защищённого от радиоподавления интервала связи зависит от дальности, на которой ведётся подавление.

Заключение. Данный подход обеспечения безопасности телекоммуникационных сетей позволяет обосновать защищенный интервал связи от преднамеренных помех.

СПИСОК ЛИТЕРАТУРЫ

1. Лепешкин О.М. Исследование функциональной безопасности систем государственного управления. Инфокоммуникационные технологии. 2007. Т.5. №3. С.165-166.
2. Лепешкин О.М., Корсунский А.С. Оптимизация структуры комплекса информационно-технических средств в автоматизированных системах управления. Автоматизация процессов управления. 2011. №4. С.76-81.
3. Краснокутский А.В., Лепешкин О.М., Харечкин П.В. Анализ функциональной применимости ролевой модели разграничения доступа в системах управления. Инфокоммуникационные технологии. 2007. Т.5. №3. С.162-164.
4. Комарович В.Ф., Симонов М.В., Фролов В.Ю. Основы радиоэлектронной борьбы, радиоэлектронная защита и безопасность связи и АСУ. Инв. № 77420. – Л.: ВАС, 1989. – 346 с.
5. Антонюк Л.Я., Игнатов В.В. Эффективность радиосвязи и методы её оценки. – СПб.: ВАС, 1994. – 138 с.

УДК 621.391.28

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ РФ ОТ КИБЕРАТАК

Мошак Николай Николаевич, Евсейко Константин Владиславович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Россия, Санкт-Петербург, пр.Большевиков, 22
emails: nnmoshak49@mail.ru

Аннотация: В докладе рассматриваются современные проблемы информационной безопасности информационно-телекоммуникационной инфраструктуры РФ в условиях информационного противоборства в киберпространстве.

Ключевые слова: информационное противоборство, кибератака, модель угроз, политика информационной безопасности мониторинг информационной безопасности

PROBLEMS OF PROTECTION OF INFORMATION AND TELECOMMUNICATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION AGAINST CYBER ATTACKS

Moshak Nikolay Nikolaevich, Evseiko Konstantin Vladyslavovich
The Bonch-Bruевич Saint-Petersburg State University of Telecommunications,
Russia, St. Petersburg, Bolshhevikov pr.,22
emails: nnmoshak49@mail.ru, belosheeva.polin@mail.ru

Abstract: In the report modern problems of information security of information and telecommunication infrastructure of the Russian Federation in the conditions of information confrontation in a cyberspace are considered.

Keywords: *information confrontation, cyber attack, model of threats, politician of information security, monitoring of information security*

Введение. В настоящее время очевидным является тот факт, что информационное противоборство (ИП) в киберпространстве становится неотъемлемой частью внешней политики развитых государств. Причем, его масштабы в современных условиях растут непрерывно и уже требуют рассмотрения ИП как самостоятельной формы межгосударственного противостояния. В докладе рассматриваются основные угрозы в киберпространстве РФ на современном этапе развития информационного общества, а также причины выбора решений в области мониторинга ИБ на основе разрабатываемых российских специализированных систем.

Внедрение на современном этапе развития информационного общества технологий третьей платформы информатизации (ТПИ) одновременно с предоставлением многих недоступных ранее информационных услуг создает и угрозы нового типа. Это обстоятельство стало одной из основных предпосылок создания новой доктрины информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. №646. Анализ приведенного в новой доктрине информационной безопасности (ИБ) Российской Федерации перечня блоков угроз показывает, что эффективность защиты информационных интересов РФ напрямую зависит от внедрения технологий ТПИ, элементами которой являются [1]:

- облачные вычисления, безопасность которых связана с виртуализацией логически разделяемых вычислительных процессов и физических вычислительных ресурсов;

- интернет вещей, ставших частью киберпространства, безопасность которых связана с соединением физических вещей с цифровыми сенсорами, с объединением аналогового мира и его цифрового описания, что заставляет обеспечивать информационно-энергетическую, информационно-транспортную, информационно-производственную и, в целом, информационно-экономическую безопасность;

- большие данные, безопасность которых связана с возможностью путем их обработки, в том числе и с деструктивными целями, делать достаточно точные статистические оценки о состоянии дел во всех областях деятельности государств, а также силовых министерств и ведомств РФ;

- мобильный широкополосный доступ, безопасность которого связана с внедрением в мобильные устройства вредоносных программ как на этапе собственно изготовления устройства, так и в процессе эксплуатации, т. к. отсутствует граница сети, на которой можно было бы блокировать атаки;

- наложенные сервисы, безопасность которых связана, помимо традиционных угроз (Web-атаки, фишинг и др.), с появлением рисков и угроз при обезличивании пользователей в социальной сети и необходимо учитывать, что процессы и тематика общения в социальных сетях могут быть намеренно организованы противником, использующим средства социальной инженерии.

Рассмотренные проблемы безопасности в киберпространстве РФ ставят на повестку дня ускоренное внедрение технических и организационно-технических систем контроля и мониторинга ИБ киберпространства РФ, которые выступают в статусе вспомогательных («индикативно-сенсорных») по отношению к базовым системам защиты и являются одним из компонентов систем контроля защищенности информационных инфраструктур РФ. Указанные системы позволяют нейтрализовать потенциальные киберугрозы путем оперативного устранения уязвимостей информационно-телекоммуникационной инфраструктуры страны.

Заключение. Рассмотренные проблемы безопасности и новые типы угроз в киберпространстве РФ на современном этапе развития информационного общества должны быть учтены в типовых моделях нарушителей и угроз при построении политики ИБ информационно-телекоммуникационной инфраструктуры страны [2]. При этом выбор решений в области мониторинга ИБ должен базироваться на основе разрабатываемых российских специализированных систем в противовес решениям на базе стандартных продуктов ведущих иностранных производителей.

СПИСОК ЛИТЕРАТУРЫ

1. Колбанёв А.М., Колбанёв М.О., Цехановский В.В. Проектирование корпоративных информационных систем. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2016. - с.192
2. Мошак Н.Н., Яшин А.И., Иванов В.И. Модели нарушителя и угроз в автоматизированных информационных системах специального назначения на технологии «клиент-сервер». «Телекоммуникационные технологии». Вып. 2(142) – СПб.: ОАО «НИИ «Рубин», 2014, инв.№в-760с – с. 50-65.

УДК 621.391 (075.8)

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МОБИЛЬНЫХ УСТРОЙСТВАХ И ВОЗМОЖНЫЕ ПУТИ ИХ РЕШЕНИЯ

Неижмак Алексей Владимирович

Военная академия связи им. Маршала Советского Союза С.М. Буденного,
Россия, Санкт-Петербург, пр-т Тихорецкий, 3,
email: leshechka_87@mail.ru

Аннотация: В статье рассмотрены некоторые способы хищения персональных данных из мобильных устройств и несколько вариантов их предотвращения. Описаны наиболее распространенные причины хищений, виды информации, которая чаще всего подвержена атакам, а также неумышленные ошибки пользователей, приводящие к утечкам персональных данных.

Ключевые слова: *мобильные устройства, хищения персональных данных, кибератаки, маскировка, способы защиты устройств*

PROBLEMS OF INFORMATION SECURITY IN MOBILE DEVICES AND POSSIBLE WAYS OF THEIR SOLUTIONS

Alexey Neizhmak

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny,
Russia, St. Petersburg, Tikhoretsky avenue 3,
email: leshechka_87@mail.ru

Abstract: In the article some methods of stealing personal data from mobile devices and several variants of their prevention are considered. The most common causes of theft, types of information most often susceptible to attacks, as well as unintentional errors of users, leading to leaks of personal data are described.

Keywords: *mobile devices, theft of personal data, cyberattacks, disguise, ways to protect devices*

Мобильные устройства, под ними мы привыкли понимать телефоны и смартфоны, являются сегментом, которому уделяется особое внимание благодаря удобному и выгодному развитию всевозможных технологий и сервисов в данной отрасли. И чем большее развитие получает направление мобильных устройств, тем острее встаёт вопрос об обеспечении безопасности владельца устройства и его персональных данных.

Опасность хищения персональных данных возрастает пропорционально расширению функционала мобильных устройств, который напрямую связан с аппаратной и программной составляющей. Мобильное устройство способно выступать в качестве привычного каждому настольного компьютера. Если посмотреть на программную составляющую, то, для начала, стоит отметить популярные мобильные платформы – это Android, IOS, Windows. Для Android и IOS, можно выделить, огромное множество программных продуктов и всевозможных сервисов, которые могут удовлетворить практически все потребности требовательных пользователей. Развитие мобильных устройств в настоящее время находится на высоком уровне, следовательно, данному уровню должна соответствовать и защита [1].

Каждый пользователь мобильных устройств подвержен риску кибератак. Количество моделей многократно увеличивается, поэтому, как правило, поддержка ранних устройств и ранних версий операционных систем осуществляется недостаточно долго. С выходом свежих версий программного обеспечения мы получаем вместе с обновлённой операционной системой уязвимости и недоработки, которые разработчики стремятся исправить в обновлениях [2].

Часто пользователи страдают от приложей, которые лишены таких изобретательных методов, как описывалось ранее. Владелец современных гаджетов должны быть знакомы с онлайн-магазинами iTunes Store, Google Play, Windows Phone Store, в которых пользователи могут покупать различный контент, а также его распространять. У каждого есть возможность приобрести аккаунт разработчика, и продавать собственные программные продукты в этих магазинах, контент в которых подвергается проверкам. Если в магазине Apple проверки тщательные и строгие, в магазине Google – чуть проще. Возникают ситуации, когда в продажи просачиваются приложения с вредоносным кодом, который, к примеру, похищает логины и пароли, отправляя их третьим лицам. Во избежание неприятных ситуаций стоит пользоваться «софтом» известных разработчиков, которым вы доверяете (стоит помнить, что каждый желающий может приобрести аккаунт разработчика).

Но кража данных происходит не только преступными методами, случается, что пользователь наделяет разработчиков программного обеспечения правами на их использование. В онлайн-магазине перед загрузкой необходимого приложения всплывает окно с запросом разрешая на исполнение приложением ряда действий, принимая данное соглашение перед установкой пользователь может открыть доступ к своим персональным данным и не только своим [3].

Пересылка какой-либо информации происходит в ходе работы системных приложений и приложений известных разработчиков. Это позиционируется, как сбор данных для «удобства» работы

пользователя с устройством. Происходит следующее: программа запоминает поисковые запросы, ваши геоданные, статистику работы с приложениями и прочее – эта информация обрабатывается и на её основе, например, в качестве рекламы, предъявляется информация, которая скорее всего будет интересна или близка пользователю. Но это наталкивает на неприятные мысли и чувство вторжения в личную жизнь. Если взглянуть серьезнее на проблему сбора подобной статистики и обратиться к исследованиям, то получается, что подозрения оказываются не такими уж и беспочвенными [4].

Ещё одной причиной кражи персональных данных может служить потеря вашего мобильного устройства или возможность бесконтрольного доступа к нему. Например, если ваш смартфон остаётся на продолжительное время без присмотра, заинтересованное лицо получает шанс воспользоваться случаем и похитить личную информацию. Аналогична ситуация с потерей или хищением устройства. К счастью, современные гаджеты имеют средства защиты, которые могут свести на нет извлечение данных из устройства, имея к нему физический доступ, без вашего ведома. К ним можно отнести: пароль – простой и действенный способ защиты (эффективность которого зависит от сложности пароля), графический ключ – последовательное соединение опорных точек на экране (не является серьёзной преградой для наблюдательных людей), распознавание лица – использует фронтальную камеру (на качество работы влияет множество факторов), распознавание голоса – запись звукового файла и сравнение с оригиналом, являющимся ключом, дактилоскопический сканер – надёжный способ защиты устройства (количество оснащённых такой функцией устройств растёт), сканер радужной оболочки глаза – использует фронтальную камеру (впервые использовано на флагманах компании Microsoft в 2015 году) [6]. Такие инструменты защиты снижают риски хищения данных через физический доступ к устройству. Для подобных случаев утраты контроля над гаджетом существуют специальные функции – блокировка устройства через интернет, определения местонахождения, удаления данных с устройства. [5].

Таким образом, приобретая полезные сервисы и удобные функции, мы жертвуем безопасностью своих личных данных. Современному человеку очень сложно отказаться от использования мобильных устройств, так как это практически равносильно изоляции от информационного пространства, что не соответствует установившимся тенденциям и образу жизни общества. Каналы передачи данных обеспечивают нас возможностью доступа практически к любой информации, но нельзя забывать, что это средства двустороннего обмена данными, поэтому использовать их нужно, не пренебрегая правилами информационной безопасности [6].

СПИСОК ЛИТЕРАТУРЫ

1. Информационная безопасность: учеб. пособие / В.В. Гафнер. — Ростов н/Д : Феникс, 2010. — 324 с.
2. Чуднов А.М., Кирик Д.И., Курашев З.В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений / Чуднов А.М., Кирик Д.И., Курашев З.В. / Радиотехнические и телекоммуникационные системы. - 2017. - №2. - с.41-49
3. Брунилин А.А., Бирюков М.А., Саенко И.Б. Модель и метод использования онтологий для управления разграничением доступа в едином информационном пространстве // Математические методы в технике и технологиях – ММТТ. 2016. №6 (88). С. 122-124
4. Башкирцев А.С., Михайличенко Н.В., Ренсков А.А., Парашук И.Б. Совершенствование объема и номенклатуры множества контролируемых параметров, принадлежащих пространству управления информационными системами и сетями // Успехи современной науки 2017, №1, Т.4, С.46-52
5. Овсянников С.Н., Хмелевской В.П. Региональная информатика и информационная безопасность. Сборник трудов. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. 2016. С. 389-391
6. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. - 372 с.

УДК 004.056.57

МОДЕЛИ ИНТЕЛЛЕКТУАЛЬНЫХ ВОЗДЕЙСТВИЙ

Нечепуренко Александр Петрович, Суетин Артем Игоревич, Муртазин Ильдар Робертович,
Лаута Олег Сергеевич
Военная академия связи имени Маршала Советского Союза С.М. Будённого,
Россия, Санкт-Петербург, Тихорецкий пр., 3,
email: vlasenko199@yandex.ru, asuetin5@yandex.ru

Аннотация: В статье рассмотрены атаки на каналы управления роботизированных систем и представлен подход по определению вероятностно – временных характеристик.

Ключевые слова: роботизированная система; канал управления; метод преобразования.

MODELS OF INTELLECTUAL INFLUENCES

Aleksandr Nechepurenko, Artem Suetin, Ildar Murtazin, Oleg Laut
Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny
Russia, St. Petersburg, Tihoreckii' av. 3,
email: vlasenko199@yandex.ru, asuetin5@yandex.ru

Abstract: In article, the attacks to robotic systems are considered, and approach to definition of their probabilistic and time characteristics is also presented.

Keywords: *robotic system; control path; transformation method.*

Роботизированные системы (РТС) как объект управления представляет собой сложную систему, включающую в себя многозвенную механическую конструкцию с исполнительными пневмо-, гидро- или электроприводами, активно взаимодействующую с окружающей средой и характеризующуюся совокупностью параметров, изменяющихся во времени.

Вместе с тем, непосредственное внедрение РТС приводит к усилению опасности существующих и появлению новых атак противника на подлинность и доступность передаваемой информации, передаваемой по каналам управления (КУ) РТС.

Возможными результатами воздействия атак на РТС являются несанкционированный доступ, блокирование управляющей информации, внедрение ложной информации, нарушение установленных регламентов сбора, обработки и передачи информации, отказы и сбои в работе РТС, а также компрометация передаваемой или получаемой информации. Однако, анализ атак показывает, что наиболее опасными для РТС являются атаки, направленные на перехват канала управления, т.е. интеллектуальные воздействия [1].

Под интеллектуальными воздействиями в статье понимаются целенаправленные, согласованные по месту и времени воздействия, предназначенные для перехвата канала управления системой.

Учитывая вышеизложенное, необходимо разработать способы защиты КУ РТС от интеллектуальных воздействий. Для построения системы защиты предлагается первоначально построить модели интеллектуальных воздействий, определить их вероятностно-временные характеристики [2] и используя полученные, в качестве исходных данных, обосновать защиту КУ РТС.

Подход, рассматриваемый в настоящей статье, предполагает построение аналитических моделей интеллектуальных воздействий (ИВ). Результатом моделирования является функция распределения времени и среднее время реализации ИВ. Для построения аналитической модели ИВ применяется подход, основанный на преобразовании стохастических сетей. Этот подход отличается более высокой точностью и устойчивостью получаемых решений и хорошо зарекомендовал себя для моделирования многошаговых стохастических процессов различной природы.

Первым этапом при моделировании является построение эталонной модели [3]. Эталонная модель атаки – это последовательность (алгоритм) действий злоумышленника при реализации ИВ. В качестве примера построения эталонной модели атаки рассмотрена атака «Человек по середине».

Следующий этап - построение стохастической сети и нахождение эквивалентной функции [4], сохраняющей в своей структуре параметры распределения и логику взаимодействия элементарных случайных процессов. Эквивалентная функция позволяет определить первые моменты случайного времени выполнения целевого процесса.

Далее используя преобразование Лапласа и разложение Хевисайда, находятся расчетные выражения для определения функции распределения вероятности времени реализации ИВ «Человек по середине» и среднее время, затрачиваемое на реализацию ИВ «Человек по середине».

Результаты расчеты представляются в виде зависимостей интегральной функции распределения вероятности от времени реализации ИВ и зависимость среднего времени реализации ИВ от вероятности.

Таким образом, материал настоящей статьи предлагает новый подход к аналитическому моделированию атак, основанный на методе преобразования стохастических сетей. Сущность данного метода заключается в замене множества элементарных ветвей стохастической сети одной эквивалентной ветвью и последующим определением эквивалентной функции сети, а также начальных моментов и функции распределения случайного времени реализации атаки.

Проверка предложенного подхода была произведена для моделирования ИВ «Человек по середине», которые являются одними из наиболее распространенных и опасных для компьютерных сетей.

СПИСОК ЛИТЕРАТУРЫ

1. Защита канала управления роботизированных систем. Баранов В.В., Гудков М.А., Крибель А.М., Лаута О.С., Нечепуренко А.П. В сборнике: Актуальные проблемы обеспечения информационной безопасности. труды Межвузовской научно-практической конференции. 2017. С. 32-37.
2. Применение метода топологического преобразования стохастических сетей для оценки эффективности средств защиты. Баранов В.В., Крибель А.М., Лаута О.С., Нечепуренко А.П. В сборнике: Актуальные проблемы обеспечения информационной безопасности. труды Межвузовской научно-практической конференции. 2017. С. 47-52.
3. Обеспечение живучести информационных систем (часть 3. Методы обеспечения и повышения живучести). Елисеев А.И., Долгов А.А., Хорохорин М.А., Лаута О.С., Набатов К.А. Вестник Воронежского института ФСИН России. 2013. №1. С.91-94.
4. Методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного воздействия. Коцыняк М.А., Лаута О.С., Нечепуренко А.П., Штеренберг И.Г. Труды учебных заведений связи. 2016. Т. 2. № 4. С. 82-87.

УДК 681.518.5:004.052.32

КОНТРОЛЬ МНГОВЫХОДНЫХ ЛОГИЧЕСКИХ СХЕМ АВТОМАТИКИ НА ОСНОВЕ МЕТОДА ЛОГИЧЕСКОГО ДОПОЛНЕНИЯ ПО РАВНОВЕСНЫМ КОДАМ

Пивоваров Дмитрий Вячеславович, Ефанов Дмитрий Викторович,
Сапожников Валерий Владимирович, Сапожников Владимир Владимирович
Петербургский государственный университет путей сообщения Императора Александра I
Россия, Санкт-Петербург, Московский пр., 9,
emails: pivovarov.d.v.spb@gmail.com, TrES-4b@yandex.ru, at.pgups@gmail.com,
port.at.pgups@gmail.com

Аннотация: В статье рассмотрены способы организации систем функционального контроля логических комбинационных схем с шестью выходами по равновесным кодам «1 из 3», «1 из 4» и «2 из 4». Были проведены эксперименты с контрольными комбинационными схемами, результатами которых являются значения структурной избыточности для каждого из способов.

Ключевые слова: система диагностирования; логическое дополнение; равновесные коды; функциональное диагностирование; площадь системы диагностирования.

CONTROL OF MULTI-OUTPUT LOGIC AUTOMATIC SCHEMES BASED ON THE METHOD OF A BOOLEAN COMPLEMENT ON CONSTANT WEIGHTS CODES

Pivovarov Dmitry, Efanov Dmitry, Sapozhnikov Valery, Sapozhnikov Vladimir
The Emperor Alexander I St. Petersburg State Transport University,
Russia, St. Petersburg, Moscow ave., 9
emails: pivovarov.d.v.spb@gmail.com, TrES-4b@yandex.ru,
at.pgups@gmail.com, port.at.pgups@gmail.com

Abstract: The article considers ways to organization of current error detection system of logical combinational circuits with six outputs by the constant weights codes «1 of 3», «1 of 4» and «2 of 4». Experiments with control combination schemes were carried out, the results of which are the values of structural redundancy for each of the methods.

Keywords: diagnostic system; Boolean complement; constant weights codes; current error detection; structural redundancy of diagnostic system.

Введение. При проектировании информационных систем необходимо обеспечивать устойчивость этих систем к различным неисправностям, а также своевременно их идентифицировать. Для этого применяют различные средства диагностирования, в том числе, функциональный контроль. Системы функционального контроля позволяют обнаруживать отказы комбинационных схем прямо во время их работы, при этом, рабочие входные воздействия являются одновременно и тестовыми.

Существует множество способов организации систем функционального контроля, например, по кодам с суммированием [1]. В данном исследовании рассматривается метод логического дополнения по равновесным кодам «1 из 3», «1 из 4» и «2 из 4».

Особенности применения равновесных кодов «1 из 3», «1 из 4» и «2 из 4» изучены в [2 – 5], однако они рассматривались только для схем с тремя и четырьмя выходами. В данной статье рассматриваются варианты контроля схем с шестью выходами. В этом случае выходы схемы разбиваются на подгруппы по три или четыре выхода, при этом для некоторых схем выходы разбивались на пересекающиеся группы.

Для определения эффективности исследуемых кодов в задачах построения систем функционального контроля были проведены эксперименты на контрольных комбинационных схемах LGSynth'89 и MCNC Benchmarks alu2 и MCNC max512 и max1024 (они выбраны из всего многообразия контрольных комбинационных схем как шестивыходные схемы; для схем с большим количеством выходов результаты являются похожими). Для экспериментов использовалось специальное программное обеспечение, разработанное на кафедре «Автоматика и телемеханика на железных дорогах» ФГБОУ ВО ПГУПС, позволяющее получать описания компонентов систем функционального контроля в стандартном формате *.pla. Используя файлы-описания компонентов систем функционального контроля и интерпретатор SIS, были получены значения условных площадей, занимаемых системами функционального контроля, организованными по равновесным кодам «1 из 6», «1 из 3», «1 из 4» и «2 из 4», на кристалле. При построении систем функционального контроля по кодам «1 из 3», «1 из 4» и «2 из 4» производилось разбиение выходов на группы по 3 или 4 и каждая группа контролировалась отдельно. В случае кода «1 из 6» разбиения не производилось. Были определены показатели структурной избыточности и получено сравнение с дублированием.

В ходе эксперимента было установлено, что структуры, построенные по равновесному коду «2 из 4» имеют наименьшую избыточность в случае контрольных комбинационных схем max512 и max1024, а структуры, построенные по равновесному коду «1 из 6» имеют наименьшую избыточность в случае схемы alu2.

СПИСОК ЛИТЕРАТУРЫ

1. Сапожников В.В., Сапожников Вл.В., Ефанов Д.В. Применение кодов с суммированием при синтезе систем железнодорожной автоматики и телемеханики на программируемых логических интегральных схемах // Автоматика на транспорте. – 2015. – Том 1. – №1. – С. 84-107.
2. Сапожников В.В., Сапожников Вл.В., Дмитриев А.В., Морозов А.В., Гессель М. Организация функционального контроля комбинационных схем методом логического дополнения // Электронное моделирование. – 2002. – Том 24. – №6. – С. 52-66.
3. Сапожников В.В., Сапожников Вл.В., Ефанов Д.В., Пивоваров Д.В. Метод логического дополнения на основе равновесного кода «1 из 4» для построения полностью самопроверяемых структур систем функционального контроля // Электронное моделирование. – 2017. – Том 39. – №2. – С. 15-34.
4. Пивоваров Д.В. Особенности организации полностью самопроверяемых структур на основе равновесного кода «1 из 4» // Материалы Юбилейной XV Санкт-Петербургской международной конференции «Региональная информатика – 2016», Санкт-Петербург, 26-28 октября 2016 г., СПОИСУ, СПб, 2016. – С. 307-308. – ISBN 978-5-906841-68-1.
5. Пивоваров Д.В. Один способ построения полностью самопроверяемых структур систем функционального контроля на основе равновесного кода «1 из 4» // Информационные технологии на транспорте: сборник материалов секции «Информационные технологии на транспорте» Юбилейной XV Санкт-Петербургской международной конференции «Региональная информатика – 2016», Санкт-Петербург, 26-28 октября 2016 г.; под. ред. Вал. В. Сапожникова. – СПб: ФГБОУ ВО ПГУПС, 2016, с. 17-27. ISBN 978-5-7641-0951-0.

УДК 621.391

ПРОТИВОДЕЙСТВИЕ НЕСАНКЦИОНИРОВАННОМУ ДОСТУПУ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ НА ОБЪЕКТЫ УЧРЕЖДЕНИЙ

Остроумов Олег Александрович, Атигов Умар Умарович, Сотникова Дарья Ивановна
Военная академия связи им. Маршала Советского Союза С.М. Буденного,
Россия, Санкт-Петербург, пр-т Тихорецкий, 3,
emails: oleg-26stav@mail.ru

Аннотация: в докладе рассмотрена проблема обеспечения противодействия несанкционированному доступу на объекты учреждений с использованием беспилотных летательных аппаратов. Приведены способы противодействия такому проникновению.

Ключевые слова: беспилотные летательные аппараты, несанкционированный доступ, безопасность.

COUNTERMEASURES TO UNAPPROVED UNMANNED DRENES ACCSESS ON INSTITUTES

Oleg Ostroumov, Umar Atigov, Daria Sotnikova
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny,
Russia, St. Petersburg, Tikhoretsky avenue 3,
emails: oleg-26stav@mail.ru

Abstract: The problem of providing counter measures to unapproved access on institutes using unmanned drones is considered in the report. The methods of opposing to such penetration are presented.

Keywords: unmanned drones, unapproved access, security.

Ведение: в последние сорок лет человечество совершило огромный скачок в приобретении знаний. Количество информации о мире увеличилось в два раза по сравнению с предыдущим периодом существования человечества. Дальнейшее развитие техники и технологий будет осуществляться еще быстрее. При создании предприятий, научных центров, различных учреждений, расположенных на какой-то ограниченной территории всегда большое внимание, уделяется обеспечению безопасности, особенно в современном мире, где развитие технологий так стремительно и утечка информации о создании чего-то нового может привести к большим потерям (материальным, экономическим, людским и т.д.).

До недавнего времени больше внимания уделяли методам пресечения возможности физического проникновения на охраняемые объекты (пересечения периметра охраняемого объекта). Охрана внешнего периметра объекта как правила рассчитывается на обнаружение проникновения человека. Однако развитие технологий беспилотных летательных аппаратов (БПЛА) и робототехники привели к необходимости создания специализированных систем как обнаружения таких объектов, так и пресечения их деятельности по сбору информации и другому воздействию. Особенно актуальной данная проблема стоит для предприятий военно-промышленного комплекса, объектов силовых структур (МВД, ФСБ, ВС, СВР, ФСО), для которых утечка информации и перехват ее противником может привести к нарушению интересов не только предприятия, но страны в целом.

Об этой проблеме давно задумались в нашей стране. Например, в период проведения Олимпиады в городе Сочи и проведении спортивных мероприятий чемпионата мира по футболу большое внимание уделялось и уделяется вопросам безопасности. БПЛА могут использоваться для фото и видео разведки иностранными спецслужбами, террористами для выявления мест массового скопления людей, а также поиска уязвимостей в конструкциях и близлежащих объектах к таким

скоплениям. Кроме этого для переноса взрывчатых веществ при совершении терактов (хотя размер и масса переносимых предметов имеют ограничения, и как правило малый размер).

Существуют следующие способы нейтрализации БПЛА [1]:

- акустические;
- лазерные;
- микроволновые;
- противодроны;
- системы РЭБ;
- системы перехвата управления БПЛА;
- сети.

Для противодействия БПЛА, в составе которых присутствует гироскоп, который отвечает за устойчивость полета и пространственную ориентацию, используют явление резонанса. При резонансе он выходит из строя, что приведет к дезориентации в пространстве аппарата и аварии. Диапазон частот, на которых работают гироскопы, находится в диапазоне от нескольких кГц до нескольких десятков кГц. Однако этот метод воздействия не всегда эффективен. Если, кроме гироскопа используется магнитометр, отвечающий за горизонтальную ориентацию, воздействие на гироскоп может не привести к аварии БПЛА.

ВМФ США проводились испытания маломощной лазерной системы, которая позволяет обнаруживать, отслеживать и уничтожать движущиеся воздушные цели. Система разработана компанией Boeing и способна уничтожать приближающиеся к кораблю (объекту) БПЛА, артиллерийские снаряды и небольшие низколетящие самолеты. Лазер способен обнаруживать цели на расстоянии до 35 км, эффективная зона поражения радиусом до 1.6 км [2]. Время уничтожения объекта примерно 2 секунд. В отличие от лазерных противодронных систем, которые разрушают дрон механически, за счет его сильного дистанционного нагрева, микроволновые системы, дистанционно формирующие в электрических цепях наведенные токи, способны уничтожать целые группы дронов [3].

Для противодействия БПЛА, которые переносят опасные грузы и при падении могут нанести вред охраняемым объектам, а также при необходимости получения такого груза или информации дрона используют различные сети. Компания OpenWorks Engineering представила систему SkyWall 100 (200 и 300). Устройство представляет собой пушку, выстреливающей в сторону беспилотника сеть. Радиус эффективного действия устройства - более 100 метров [1].

Дроны-перехватчики могут быть как управляемыми оператором, так и автоматическими. При обнаружении объекта, нарушающего охранный периметр они реагируют на шум двигателя, или определяют нарушителя по имеющейся базе БПЛА. Дрон-перехватчик может быть оснащен сетью для обезвреживания дрона-нарушителя, как это было применено в Японии [1].

Системы радиоэлектронной борьбы (РЭБ) используются для забития помехами канала управления БПЛА. В дальнейшем оставшийся без управления БПЛА может быть уничтожен.

Вывод: таким образом, развитие современных технологий беспилотных летательных аппаратов открывают большие возможности перед злоумышленником сбора информации о закрытых объектах, доставке различных предметов (закладок, взрывчатки и др.), проведении различных диверсий. Поиск способов борьбы с БПЛА и совершенствование уже имеющихся является актуальным и требует изучения. Особенно большое внимание проблеме несанкционированного доступа на объекты уделяют силовые ведомства и оборонные предприятия.

СПИСОК ЛИТЕРАТУРЫ

1. Теодорович Н.Н., Строганова С.М., Абрамов П.С. Способы обнаружения и борьбы с малогабаритными беспилотными летательными аппаратами // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, №1 (2017).
2. US Marines Test Boeing Laser To Knock Down Drones, Enemy Artillery. [Электронный ресурс]: <http://www.ibtimes.com/us-marines-test-boeing-laser-knock-down-drones-enemy-artillery-2011610?ft=h6k97>
3. The Army's Real-Life "Phaser" Would Knock Out an Entire Drone Swarm With One Shot. [Электронный ресурс]: <http://www.popularmechanics.com/military/weapons/a23881/the-army-is-testing-a-real-life-phaser-weapon/>

УДК 004.49

ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ АКТИВНОГО ОБОРУДОВАНИЯ КОРПОРАТИВНЫХ СЕТЕЙ

Серёгин Сергей Сергеевич, Гвоздков Игорь Вячеславович
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М. А. Бонч-Бруевича
Россия, Санкт-Петербург, просп. Большевиков, 22к1
emails: serezh.seregin@gmail.com, gvozdkov@rambler.ru

Аннотация: В статье рассматривается задача обеспечения безопасности информационных систем. Это требует размещения средств защиты как можно ближе к источнику опасности. Такие устройства - активное сетевое оборудование, в котором средства защиты устройств реализованы и

правильно сконфигурированы, но также и безопасность сетевых ресурсов, которые они обеспечивают. Такими возможностями обладает оборудование фирмы Cisco.

Ключевые слова: информационная безопасность, угрозы безопасности, Cisco, средства и рекомендации по обеспечению безопасности

ENSURING INTEGRATED SAFETY OF ACTIVE EQUIPMENT OF CORPORATE NETWORKS

Seregin Sergey Sergeevich, Gvozdkov Igor Vyacheslavovich
St. Petersburg State University of Telecommunications. prof. M. A. Bonch-Bruevicha,
Russia, St. Petersburg, prosp. Bolshieviks, 22k1
emails: serezhha.seregin@gmail.com, gvozdkov@rambler.ru

Abstract: The article considers the problem of ensuring the security of information systems. This requires the deployment of protection tools as close as possible to the source of danger. Such devices are active network equipment in which the security features of the devices are implemented and properly configured, but also the security of the network resources that they provide. Such facilities are available from Cisco.

Keywords: information security, security threats, Cisco, security tools and recommendations

Информационная безопасность — это состояние защищенности информации, при котором осуществляется её конфиденциальность, доступность, и целостность. Так, угрозой безопасности являются любые действия, направленные на нарушение одного или нескольких этих критериев. Угрозы делятся на внутренние (атака непосредственно на устройство связи) и внешние (атака через внешнюю сеть или сеть Интернет). К внутренним угрозам относятся:

Включенные неиспользуемые порты. Это значит, что через порты, которые не используются активно устройством, можно получить доступ к конфигурации сетевого устройства.

Отсутствие защиты режима конфигурации, а именно отсутствие паролей (или других способов аутентификации) к ним, или их простота.

Отсутствие шифрования трафика. Перехват такого трафика приводит к получению аутентификационных данных и последующему доступу к конфигурации устройства.

К внешним устройствам относятся такие угрозы, как:

Distributed Denial of Service (DoS), или распределенный отказ в обслуживании — это атака, использующая несколько компьютеров для непрерывной передачи запросов на устройство (флуд), приводящая его к перегрузке (что означает потерю или затруднению доступа к такому устройству).

IP-спуфинг (Spoofing в переводе с английского — подмена) — Выдача постороннего пользователя в качестве санкционированного при помощи подмены IP-адреса, который используется во внутренней сети.

Большинство современных сетевых устройств имеет средства защиты от таких атак. К таким относятся устройства компании Cisco, такие, как маршрутизаторы и коммутаторы. Они работают на регулярно обновляющейся операционной системе Cisco IOS.

Защита от выше перечисленных атак обеспечивается на программном уровне. Устранение внутренних угроз производится при помощи следующих решений:

Отключить неиспользуемые порты. Эта практическая рекомендация предотвратит несанкционированный доступ через физически доступные порты.

Использовать надежные пароли и регулярно менять их. Надежным паролем считается длинный пароль (длиннее 12 символов) с заглавными, прописными символами, специальными символами, и цифрами. При этом пароль должен быть легко запоминаемым.

Использовать защищенное соединение. Рекомендуется для управления устройством заменить протокол telnet протоколом SSH (Secure SHell), так как telnet передает данные сплошным текстом, в то время, как SSH шифрует трафик при помощи ключа RSA, без которого расшифровка невозможна.

Устранение внешних угроз на устройствах Cisco производится при помощи следующих функций:

Контроль доступа. Правильная настройка списков контроля доступа (ACL — Access Control List) снизит эффективность IP-спуфинга и DDoS-атак и повысит производительность сети. На устройствах Cisco доступна установка как входящих (фильтрация входящего трафика), так и исходящих списков (ограничение сервисов внутри сети).

Устранение DDoS-атак производится при помощи аппаратных устройств, таких как Cisco Guard XT-5650, и сервисов, таких как CloudFlare, Akamai и RadWare. Эти сервисы перенаправляют весь трафик через свою глобальную сеть дата-центров и поглощают DDoS-трафик, пропуская только данные порта 80 (HTTP) и 443 (HTTPS).

Так же рекомендуется настроить ведение журналов. Это позволит системному администратору эффективно вести отладку и диагностику устройств, а также может послужить доказательством атаки.

В то время, как абсолютная защита от некоторых видов атак невозможна, большинство современных устройств способно снизить эффективность таких атак.

СПИСОК ЛИТЕРАТУРЫ

1. <https://pages.nist.gov/800-63-3/sp800-63b.html> Национальный институт стандартов и технологий. США. Руководство по цифровой идентификации.
2. Кокшенев В.В. Информационная безопасность корпоративных внутренних сетей. Томск, 2006, 64 с.
3. CCNA Routing and Switching Essentials. Cisco Networking Academy
4. Cisco Systems. Defeating DDoS Attacks.
5. <https://www.cloudflare.com/ddos/under-attack/>

УДК 004.056.53

**МЕТОДИКА ПРОЕКТИРОВАНИЯ СИСТЕМЫ РАЗГРАНИЧЕНИЯ ДОСТУПА
АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ**

Фиалкин Илья Александрович

Военная Академия связи

Россия, Санкт-Петербург, Тихорецкий проспект, 3

emails: ifialkin-81@mail.ru

Аннотация: В докладе рассмотрены актуальные вопросы защиты информации от несанкционированного доступа в автоматизированных информационных системах, формирования предложения по совершенствованию подсистемы управления доступом, как основы системы защиты информации. Предлагается методика проектирования системы разграничения на основе функционально-ролевой модели.

Ключевые слова: разграничение доступа; информационные ресурсы; защита информации; функционально-ролевая модель.

THE DESIGN METHOD OF SYSTEM ACCESS SECURITY AVTOMATIC INFORMATION SYSTEMS

Fialkin Ilya

Military Academy of communications

Russia, Saint-Petersburg, Tikhoretsky prospect, 3

emails: ifialkin-81@mail.ru

Abstract: The article deals with relevant questions of information protection from unauthorized access in automated information systems, the formation of proposals to improve the access management subsystem, as the basis for the information security system. A method of designing control system based on the functional-role models.

Keywords: access control; information resources; information security; functional-role model.

Введение. Базовым элементом современных систем защиты информации является система разграничения доступа к информационным ресурсам системы. В соответствии с требованиями приказов (стандартов) в области информационной безопасности система разграничения доступа должна строиться на основе формальных моделей разграничения доступа. Данные модели строго определяют свойства элементов системы, правила их взаимодействия и позволяют проводить математическое доказательство безопасности системы. Однако наличие формальной модели безопасности не является достаточным условием для построения гарантированно защищенной системы [1]. Необходимо обеспечить полное соответствие абстрактных сущностей и процессов модели реальным объектам и правилам функционирования системы.

Поэтому большую роль при построении систем защиты информации и разграничения доступа играют методики, позволяющие с высокой степенью адекватности интерпретировать формальную модель безопасности в реальной системе. Однако при разработке и применении подобных методик возникают сложности, связанные с особенностями современных информационных систем (ИС). К ним относятся разветвленная организационно-штатная структура, различные классы информационных ресурсов и процессов их обработки, специфика предметной области ИС и многое другое.

Из всего комплекса задач и элементов проектирования автоматизированных информационных систем (АИС), необходимых для создания системы разграничения доступа, выделим формирование структуры информационных ресурсов, разработку функционально-алгоритмической структуры, построение системы ролей и рабочих групп пользователей, что формирует исходные условия создания системы разграничения доступа согласно функционально-ролевой модели безопасности АИС. Решение данных задач должно быть основано на детальном анализе предметной области АИС, среди которых организационно-штатная структура, функциональная модель деятельности, модели процессов и потоков данных, формируемых в рамках проектирования АИС.

Таким образом, методика построения системы разграничения доступа должна содержать следующие этапы [2]:

- построение структуры информационных ресурсов системы;
- определение набора процессов и процедур для формирования функциональных модулей, т.е. построение функционально-алгоритмической структуры системы;

- создание ролей, групп на основе функциональных обязанностей персонала и организационно-штатной структуры;
- назначение итоговых (ролевых и индивидуальных) прав доступа.

После построения системы разграничения доступа необходимо провести оценку эффективности системы согласно критерию эффективности и на основе результатов оценки принять решение либо о достижении цели построения системы, либо о корректировке элементов системы.

Проектирование системы разграничения доступа – многокритериальная задача. В общем случае система критериев, используемых при планировании системы, имеет иерархическую структуру. Центральной проблемой разработки распределенных процедур решения сложных задач является нахождение такой декомпозиции распределения на подзадачи, а также выбор таких методов решения в каждом элементе созданной структуры, которые приводили бы к получению приемлемого по качеству решения всей задачи в целом за приемлемое время [3].

В основе декомпозиционного подхода лежит предположение о наличии общей глобальной модели информационной защиты, которая описывает основные свойства системы адекватно поставленным целям принятия решения. При наличии такой модели применение декомпозиционных методов позволяет резко сократить размерность решаемой задачи и свести ее к последовательному решению ряда задач намного меньшей размерности. Все модели, ограничения и критерии этих задач непосредственно вытекают только из специальным образом расчлененной глобальной целевой функции. При декомпозиционном подходе алгоритм взаимодействия между подсистемами (решаемыми задачами) [4] и характер потоков информации между вышестоящими и нижестоящими уровнями являются производными и определяются методом декомпозиции глобальной задачи.

Попытка непосредственного использования единого глобального критерия верхнего уровня с последующей его декомпозицией для подсистем всех уровней делает задачу оптимизации крайне сложной и игнорирует наличие собственных целевых функций у активных подсистем. Оптимальное решение многоуровневой иерархической системы обладает тем свойством, что каковы бы ни были состояние и решение вышестоящего уровня управления в момент t , последующие решения нижестоящих уровней должны быть оптимальными относительно этого решения.

Применение принципа оптимальности позволяет реализовать наиболее эффективный способ координации решений, принимаемых на отдельных уровнях иерархии. Этот принцип позволяет до минимума сократить обмен информацией между уровнями и обеспечить локальную обработку информации по подсистемам [5].

Поэтому необходимо проводить оценку выполнения поставленных требований на каждом этапе построения системы разграничения доступа, при этом критерии оптимальности каждого из этапов должны быть связаны с критерием оптимальности всей системы. В связи с этим расширим методику за счет добавления процедур оценки эффективности каждого из этапов и процедуры итоговой оценки эффективности системы в целом. При этом по итогам оценки эффективности этапа возможна корректировка полученных результатов в случае, если не были достигнуты требуемые характеристики. Особую роль в методике играет процедура итоговой оценки эффективности системы, результат которой определяет степень удовлетворения построенной системы основному критерию проектируемой системы разграничения доступа.

Заключение. На основе данного результата корректировке может быть подвергнута любая из подсистем, построенных на предыдущих этапах.

СПИСОК ЛИТЕРАТУРЫ

1. Будко Н.П., Будко П.А., Булгаков О.Ю., Васильев В.В., Давидчук В.В., Евграфов А.Е., Жук А.П., Карпов В.В., Князев В.В., Лепешкин О.М. и др. Интеллектуализация сложных систем язык схем радикалов в проблемных вопросах предпроектных исследований, оснащения, сопровождения систем и в экспериментальных задачах внедрения критических наукоемких технологий. - Информационно-измерительные и управляющие системы. 2009. Т. 7. № 3. С. 1-92. М.: Яхтсмен, 1996. - 192 с.
2. Краснотутский А.В., Лепешкин О.М., Харечкин П.В. Анализ функциональной применимости ролевой модели разграничения доступа в системах управления. Инфокоммуникационные технологии. 2007. Т. 5. № 3. С. 162-164.
4. Лепешкин О.М., Харечкин П.В. Функционально-ролевая модель управление доступом в социотехнических системах. Известия ЮФУ. Технические науки. 2009. № 11 (100). С. 52-57.
5. Лепешкин О.М. Методика реализации функционально-дискреционной модели на основе среды радикалов. Известия ЮФУ. Технические науки. 2009. № 11 (100). С. 21-26.
6. Лепешкин О.М., Харечкин П.В. Подходы к обеспечению функциональной применимости ролевой модели разграничение доступа в системе управления предприятия. Информационное противодействие угрозам терроризма. 2008. № 11. С. 57-66.

УДК621.391

АНСАМБЛИ ДИСКРЕТНЫХ ОРТОГОНАЛЬНЫХ СИГНАЛОВ СЛОЖНОЙ СТРУКТУРЫ

Сазонов Виктор Викторович, Беззубов Олег Владимирович, Мосягин Дмитрий Евгеньевич

Военная академия связи им. Маршала Советского Союза им. С.М. Буденного

Россия, Санкт-Петербург, Тихорецкий пр. 3

emails: vmktor-sazonov@yandex.ru, bov774@mail.ru, mitya.mosyagin@mail.ru

Аннотация: В статье рассмотрены ансамбли дискретных ортогональных сигналов с изменяющейся структурой, на основе свойств собственных векторов эрмитовых матриц.

Ключевые слова: дискретный сигнал, определяемый вектором в многомерном пространстве, амплитуды и фазы единичных элементов формируемых сигналов.

ANSAMBLER OF DISCRETE ORTHOGONAL SIGNALS OF COMPLEX STRUCTURE

Sazonov Viktor, Bezubov Oleg, Mosyagin Dmitry

Military Academy of Communications. Marshal of the Soviet Union. CM. Budyonny

Russia, St. Petersburg, Tikhoretsky Ave 3

emails: vmktor-sazonov@yandex.ru, bov774@mail.ru, mitya.mosyagin@mail.ru

Annotation: The article considers ensembles of discrete orthogonal signals with a variable structure, based on the properties of the eigenvectors of Hermitian matrices.

Keywords: a discrete signal determined by a vector in a multidimensional space, amplitudes and phases of unit elements of the generated signals.

Введение. Известно [1], что формирование ансамблей дискретных ортогональных сигналов (АДОС) удобно разделить на три основные направления:

Первое направление базируется на анализе свойств сигналов, для описания которых используется широкий класс известных в математике ортогональных полиномов Якоби, Гегенбауэра, Чебышева, Лагерра, Эрмита, дискретных ортогональных функций Уолша, Хаара, Радемахера, Виленкина-Крестенсона, Трофимова - Ласунского. Среди работ этого направления следует выделить публикации Л.Е. Варакина, А.Г.Леонтьева, М.К. Размахнина, В.П. Яковлева, Х. Хармута.

Второе направление связано с построением производных сигналов на базе перемножения специально подобранных производящих последовательностей на известные ортогональные функции и достаточно полно представлено работами Л.Е. Варакина, Н.Г. Дядюнова, Стиффлера.

Третье направление связано с векторным синтезом АДОС по совокупности требований к ним. Среди работ этого направления известны работы В.С. Попенко, А.П. Жука и других.

Анализ работ первого направления показывает, что оно ограничено и остается только на уровне рассматриваемых систем сигналов, а работы второго направления ограничиваются синтезом АДОС всего лишь по одной характеристике и не могут быть использованы для решения задачи формирования систем сигналов сложной структуры, по совокупности предъявляемых требований и ограничений.

В докладе рассматривается вопрос повышения структурной скрытности, посредством изменения структуры формируемых АДОС, развивая математический аппарат третьего направления, на основе использования свойств собственных векторов бидиагональных эрмитовых матриц (БЭМ) [2, 3]. Координаты собственных векторов БЭМ в общем случае являются комплексными числами, выполняющие условия ортогональности. Количество формируемых структур АДОС будет напрямую зависеть от значений числа состояний модулей и аргументов диагональных коэффициентов исходной БЭМ и её размерности. При росте размерности исходной БЭМ, количество возможных формируемых структур АДОС возрастает по экспоненциальному закону, при этом скорость возрастания напрямую зависит от числа возможных состояний диагональных коэффициентов, что в свою очередь, способствует увеличению структурной скрытности системы связи.

При этом возможны три варианта формирования структуры АДОС:

1. С различными амплитудными параметрами единичных элементов, при изменении модулей коэффициентов БЭМ;
2. С различными фазовыми параметрами единичных элементов, при изменении аргументов коэффициентов БЭМ;
3. С различными амплитудными и фазовыми параметрами единичных элементов, при изменении модулей и аргументов коэффициентов БЭМ.

Заключение. Подводя итог вышеизложенному, можно сказать что случайно сформированные АДОС для каждого этапа передачи информации, на основе изменения исходных коэффициентов БЭМ по одному из трёх вариантов, позволит решить задачу повышения структурной скрытности системы связи.

СПИСОК ЛИТЕРАТУРЫ

1. Помехозащищённость радиосистем со сложными сигналами // Г.И.Тузов, В.А. Сивов, В.И. Прытков, и др.; Под ред. Г.И.Тузова. –М.: Радио и связь, 1985. -264 с.
2. Пашинцев В. П., Малофеев О. П., Жук А. П. и др. Развитие теории синтеза и методов формирования ансамблей дискретных сигналов для перспективных систем радиосвязи различных диапазонов радиоволн. М.: Физматлит, 2010. 264 с.
3. Жук А.П., Галкин И.В., Сазонов В.В., Черняк З.В., Топкин Е.В. Оценка структурной скрытности сигналов в системе передачи информации с ортогональными последовательностями / Известия ЮФУ. Технические науки. 2007. № 4 (76). С. 167-171.

УДК 004.77

**ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ОБМЕНА ЭЛЕКТРОННОЙ
КОРРЕСПОНДЕНЦИИ ВЕДОМСТВЕННОГО НАЗНАЧЕНИЯ**

Сазонов Виктор Викторович, Салыхова Алия Маратовна
Военная академия связи им. Маршала Советского Союза им. С.М. Буденного
Россия, Санкт-Петербург, Тихорецкий пр. 3
emails: vmktor-sazonov@yandex.ru

Аннотация: В статье представлен анализ телекоммуникационных услуг основных на системах документального обмена, раскрыт программно-аппаратный комплекс системы обмена электронной почты.

Ключевые слова: комплекса средств телекоммуникаций, услуги связи, электронная почта

**FEATURES OF FUNCTIONING OF SYSTEMS OF EXCHANGE OF ELECTRONIC CORRESPONDENCE
VEDOMSTVENNAJA PURPOSE**

Sazonov Viktor, Salyahova Alia
Military Academy of Communications. Marshal of the Soviet Union. SM. Budyonny
Russia, St. Petersburg, Tikhoretsky Ave 3
emails: vmktor-sazonov@yandex.ru

Annotation: in the article the analysis of telecommunication services of the basic in systems of documentary exchange is presented, the software and hardware complex of the e-mail exchange system is disclosed.

Keyword: a set of telecommunications facilities, communication services, e-mail

Введение. Уникальной защищенной инфокоммуникационной структурой, предназначенной для объединения территориально разнесенных объектов и предоставления широкого перечня унифицированных услуг электронного информационного взаимодействия должностным лицам и приложениям автоматизированных систем, является система обмена электронной корреспонденцией (СОЭК) [1]. Особенностью СОЭК является построение сети на базе аналоговых и цифровых каналов и сетей связи различной ведомственной принадлежности. Развитие аппаратно-программного комплекса средств телекоммуникаций и услуг связи неразрывно связано с усложнением их структуры построения и алгоритмов передачи и обработки электронной корреспонденцией [2]. Существующие методы оценки качества передачи информации имеют следующие недостатки:

- проведение измерений, а также анализ их результатов занимают продолжительное время;
- необходимо привлекать опытных специалистов (администраторов и операторов);
- невозможность в большинстве случаев проведения экспериментов без нарушения режима эксплуатации СОЭК.

На основании вышеизложенного целью доклада является раскрытие логической архитектуры комплекса средств телекоммуникации СОЭК.

Для достижения поставленной цели в докладе поэтапно рассматриваются вопросы:

- обмена электронной корреспонденцией с использованием услуг традиционной почты;
- аппаратные и программные элементы СОЭК;
- передача сообщений в СОЭК;
- основные протоколы СОЭК

Представленный в докладе анализ функционирования комплекса средств телекоммуникации СОЭК имеет три отличительные особенности:

- проведён сравнительный анализ телекоммуникационных услуг основных систем документального обмена;
- проведен анализ функционирования комплекса средств телекоммуникации при обмене электронной корреспонденцией в СОЭК.

Заключение. Практическая значимость полученных результатов состоит в том, что они позволяют представить особенности функционирования комплекса средств телекоммуникации СОЭК, при обмене электронной почтой и получении исходных данных для построения модели её функционирования.

СПИСОК ЛИТЕРАТУРЫ

1. Система обмена электронной корреспонденцией ВС РФ: Учеб.-методич. пособие / Под ред. И. А. Молокович. – СПб.: ВАС, 2011. – 104 с.
2. Пакулин Н.В., Тугаенко А.Н. Тестирование протоколов электронной почты интернета с использованием моделей / Труды Института системного программирования РАН. 2011. Т. 20. С. 125-141

УДК 004.056.53

МОДЕЛЬ ДЛЯ ОПРЕДЕЛЕНИЯ СКРЫТНОСТИ СИСТЕМЫ СВЯЗИ

Худайназаров Юрий Кахрамонович, Маслов Олег Николаевич, Барауля Игорь Геннадьевич
Военная Академия связи
Россия, Санкт-Петербург, Тихорецкий проспект, 3
emails: nastia-petror@mail.ru

Аннотация: В докладе рассмотрен процесс обратного преобразование «эфирных образов» в реальные объекты, отображающие пространство этих сигналов в деятельность сил, а также модель для определения скрытности формируемой системы связи.

Ключевые слова: подсистема добывания; подсистемой обработки; радиосвязь; эфирный образ, информационная структура, процесс управления.

A MODEL FOR DETERMINATION OF SECRECY COMMUNICATION SYSTEM

Hudaynazarov Yuri, Maslov Oleg, Baraulya Igor
Military Academy of communications
Russia, Saint-Petersburg, Tikhoretsky prospect, 3
emails: nastia-petror@mail.ru

Abstract: The report describes the process of reverse transformation of the "essential image" in the real objects that show the space of these signals in the activity and also forces the model to determine generated stealth communication system.

Keywords: the extraction subsystem; a subsystem of processing; telecommunication; ethereal image, information structure, process management.

Введение. Современные операции отличаются высокой мобильностью. Высокая мобильность приводит к тому, что основным средством управления становятся различные виды радиосвязи. Высокая насыщенность радиоэлектронными средствами и необходимость их постоянной или периодической работы на излучение приводят к тому, что деятельность войск (сил) с их помощью отображается в пространство сигналов радиоэлектронных средств, формируя там «эфирные» объекты - образы реальных физических объектов и связей между ними, имеющих определенную степень сходства с реальными объектами и их взаимосвязями.

Принимая во внимание тот факт, что система связи является динамически изменяющимся объектом, подверженным различным и трудно прогнозируемым видам воздействий противника, в этих условиях актуальным становится вопрос моделирования поведения системы связи с учетом обеспечения ее скрытности [1].

Так, радиосвязь, обеспечивая управление силами, отображает в пространство сигналов радиосвязи структуру системы связи, процессы управления, отражающие деятельность сил. Таким образом, система связи является постоянным, непрерывным, глобальным источником информации о деятельности сил, перекрыть который можно, лишь прекратив связь, что ведет к потере управления. В свою очередь средства радиоэлектронной разведки (РЭР), наблюдая за пространством сигналов радиоэлектронных средств, производят обратное преобразование «эфирных образов» в реальные объекты, т.е. отображают пространство этих сигналов в деятельность сил [2].

Процесс обратного преобразования состоит из двух этапов, реализуемых соответственно двумя подсистемами радиоразведки - подсистемой добывания и подсистемой обработки. Эффективность подсистемы добывания характеризуется вероятностями обнаружения, распознавания (анализа), определения местоположения источника излучений (пеленгования), перехвата сообщения. Этими же вероятностями характеризуется скрытность объектов (источников сигналов).

Подсистема обработки на основе анализа данных, полученных подсистемой добывания, может дать с высокой вероятностью заключение о составе сил, их боевой организации, оперативном построении, о характере, порядке и последовательности выполняемых задач силами, т.е. о замысле применения сил. Таким образом, используя современные методы обработки, РЭР противника может проникать в планы и замыслы, не раскрывая содержания сообщений, передаваемых по каналам связи.

Например, экспертная система HANNIBAL - интерпретатор радиообмена - предназначена, по заявлению ее авторов, «для выдачи командиру на поле боя рекомендаций по оперативному построению и замыслу применения сил (войск) по результатам перехвата радиообмена». Показателем эффективности такой системы является вероятность правильного распознавания по работе связи к заданному времени замысла применения сил противника. Более поздней разработкой, построенной на принципах экспертных систем, стала ASAS - система автоматизированной обработки разведывательной информации от всех источников (all source automatic system), принятая на вооружение в странах НАТО в начале 90-х годов. Показателем эффективности такой системы реально может быть вероятность правильного распознавания замысла применения сил на основе информации от всех источников.

Для формализации деятельности сил разработан метод системного представления деятельности сил. Сущность его заключается в том, что для описания деятельности сил используют набор структур, отражающих основные аспекты деятельности сил, информационную структуру, отображающую каналы связи между пунктами и объектами управления.

Этот набор структур является необходимым и достаточным для того, чтобы однозначно представлять деятельность сил (задачи, замысел, решение, план). Так, боевая организация, количественный и качественный состав группировок сил задается составом и организационной структурой; оперативное построение и боевые порядки - пространственной структурой; задачи, порядок и последовательность их выполнения - временной структурой; организация управления, взаимодействия и связи- информационной структурой.

Все рассмотренные структуры при описании деятельности сил представляются детерминированными взвешенными графами и являются эталонами вариантов деятельности сил, замысла их применения, задач, решаемых силами. Накопление и систематизация таких эталонов являются основной задачей разведки противника в мирное время, поскольку в ходе боевой и оперативной подготовки отрабатывается то, что нужно на войне. Эти же структуры служат и для описания системных демаскирующих признаков при распознавании характера деятельности сил разведкой противника. Математически они также представляются взвешенными графами, только вероятностными. В качестве весов используются накопленные к заданному времени вероятности обнаружения, распознавания, пеленгования и перехвата излучений, зависящие от текущего времени, интенсивности излучений и характеристик подсистемы добывания по единичным излучениям [3], [4].

Вычисление накопленных вероятностей по указанным исходным данным соответствует процессу отображения деятельности сил в пространство сигналов радиосвязи к заданному моменту. Процесс обратного преобразования отображения пространства сигналов в предметную область, т.е. превращение «эфирных образов» и их связей в реальные взаимосвязанные объекты, описывается статистическим розыгрышем накопленных вероятностей, которые дают конкретные реализации структур, соответствующих своим или другим (ложным) структурам эталонов. Сравнение структур-реализаций со структурами эталонами осуществляется в виде операции распознавания изоморфности (изоморфного вложения) графов реализаций и графов эталонов. Решение о принадлежности варианта реализации к одному из вариантов эталона принимается по критерию минимума меры различия по совокупности структур.

Результатом моделирования является получение статистических оценок, т.е. отношения числа Mj/k принятых решения отнесения варианта реализации к i -му эталону (при фактическом исполнении варианта k) к общему числу реализации (N) и данному временному сечению (t). При $i=k$ это решение является показателем скрытности связи (точнее, ее нескрытности), а при $i \neq k$ - показателем эффективности оперативной радиомаскировки, т.е. вероятностью навязывания радиоразведке противника средствами связи i -го ложного варианта замысла при фактической реализации k -го варианта.

При моделировании в качестве основных видов разведок, действующих против элементов системы связи необходимо учитывать радиолокационную, инфракрасную, радиоразведку и техническую компьютерную разведку. В качестве прогнозируемых внешних деструктивных воздействий на систему связи в модели целесообразно учитывать огневое поражение и воздействия электромагнитной энергией высокого уровня и особенно дистанционные программные воздействия. В качестве наиболее актуального на сегодняшний день воздействия, как в угрожаемый период, так и военное время [5].

Закключение. Предложенная модель может использоваться в учебном процессе высших военных учебных заведениях, при исследовании вопросов организации связи в ходе проведения современных операций, а также различными должностными лицами органов военного управления на этапах планирования и функционирования системы связи.

СПИСОК ЛИТЕРАТУРЫ

1. Каневский З.М., Литвиненко В.П., Макаров Г.В. Теория скрытности. Часть 1, Основы теории скрытности: Учеб. пособие. Воронеж: Воронеж. гос. техн. ун-т, 2003. 92 с.
2. Литвиненко В.П. Основы теории скрытности: практикум: учеб. пособие / В.П. Литвиненко. Воронеж: ГОУВПО «Воронежский государственный технический университет», 2010. 106 с.
3. Лепешкин О.М. Исследование функциональной безопасности систем государственного управления. Инфокоммуникационные технологии. 2007. Т. 5. № 3. С. 165-166.
4. Лепешкин О.М., Корсунский А.С. Оптимизация структуры комплекса информационно-технических средств в автоматизированных системах управления. Автоматизация процессов управления. 2011. № 4. С. 76-81.
5. Лепешкин О.М., Харечкин П.В. Управление конфликтным процессом решения коллективной задачи социотехнической информационной системы в условиях ресурсной координации. Информационное противодействие угрозам терроризма. 2010. № 14. С. 162-166.

УДК 004.9

ВНЕДРЕНИЕ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В ДЕЯТЕЛЬНОСТЬ ПОЛИЦИИ

Шалагинова Ольга Борисовна
Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, ул. Летчика Пилютова, 1,
email: shalaginova1337@yandex.ru

Аннотация: В статье рассмотрены вопросы внедрения и эффективного использования в работе полиции телекоммуникационных систем. Перечислена система необходимых мероприятий для соответствующей деятельности. Предлагается создание цифровой видеотехники для системы МВД России и использование стандартов видеоданных для международного сотрудничества в рамках Интерпола.

Ключевые слова: *видеофиксация; видеосъёмка; видеотехника; видеобанки; видеотеки.*

IMPLEMENTATION OF TELECOMMUNICATION SYSTEMS IN THE WORK OF THE POLICE

Shalaginova Olga Borisovna
Saint-Petersburg University of MIA of Russia,
Russia, St.-Petersburg, street Pilot, Pilyutova, 1,
email: shalaginova1337@yandex.ru

Abstract: The article presents the issues of implementation and effective use in police telecommunication systems. The system lists the required activities for the respective activities. We propose the creation of digital video equipment for law enforcement agencies and the use of standards video for international cooperation in the framework of Interpol.

Keywords: *video recording; videography; video equipment; videobank; video library.*

Введение. В федеральном законе «О полиции» [1] подчёркивается необходимость внедрения и эффективного использования в работе подразделений и сотрудников полиции современных телекоммуникационных систем. Для обеспечения соответствующей деятельности требуется система организационно-управленческих, кадровых, финансовых и технических мероприятий [2].

Кадровое обеспечение внедрения телекоммуникационных систем в деятельность ОВД потребует расширения штата аттестованных инженерно-технических работников.

Финансовое обеспечение дальнейшего введения телекоммуникационных систем в деятельность полиции требует существенных инвестиций в масштабах всей страны. Техническое обеспечение включает в себя приобретение и использование разнообразных устройств цифрового видео [3].

Заключение. Предлагается создание научно-производственного центра видеотехники для системы МВД и использования её во всех регионах. Стандарты видеоданных позволят осуществлять международное сотрудничество подразделений полиции в рамках Интерпола по обмену значимой для раскрытия, расследования и профилактики транснациональных преступлений цифровой информацией.

СПИСОК ЛИТЕРАТУРЫ

1. ФЗ N 3 от 07.02.2011 «О полиции» с изменениями от 10.08.2017.
2. Молотков А. С. Проблематика развития и внедрения и внедрения современных информационных технологий в системе МВД России. // Мировой судья. -2012. - № 5. - С. 13 – 16.
3. Ржавский К. В. Информационная безопасность: практическая защита информационных технологий и телекоммуникационных систем: Учебное пособие. - Волгоград: Изд-во ВолГУ, 2012 — 120 с.

УДК 004.9

ПОДХОД К ЗАЩИТЕ ИНФОРМАЦИИ В СЕТЯХ С ВЫСОКИМ УРОВНЕМ КОНФИДЕНЦИАЛЬНОСТИ

Штаненко Василий Иванович, Барауля Игорь Геннадьевич, Маслов Олег Николаевич
Военная Академия связи
Россия, Санкт-Петербург, Тихорецкий проспект, 3
emails: shteff81@mail.ru

Аннотация: В докладе рассмотрен подход к защите информации в сетях с высоким уровнем конфиденциальности – создание замкнутой компьютерной системы (ЗКС) с применением «классических» программно-аппаратных средств, обеспечивающих высокую степень защиты информации на автоматизированных рабочих местах (АРМ) сетей с высоким классом защиты.

Ключевые слова: *автоматизированное рабочее место; модуль доверенной загрузки; несанкционированный доступ; средства разграничения доступа.*

THE DESIGN METHOD OF SYSTEM ACCESS SECURITY

Shtanenko Vasily, Baraulya Igor, Maslov Oleg
Military Academy of communications
Russia, Saint-Petersburg, Tikhoretsky prospect, 3
emails: shteff81@mail.ru

Abstract: In the report approach to information security on networks with the high level of confidentiality – creation of the closed computer system (CCS) using the "classical" software and hardware tools providing high degree of protection of information on the automated jobs (AJ) of networks with a high class of protection is considered.

Keywords: workstation; trusted boot module; unauthorized access; access control system.

Введение. Проблемы защиты информации от несанкционированного доступа при ее обработке и хранении на автоматизированных рабочих местах являются весьма актуальными в мире современных информационных технологий [1].

По сообщению аналитического центра Zecurion Analytics [2] по числу утечек (49 публичных инцидентов) Россия стоит на 4-м месте после США (абсолютный лидер, 72% от всех зарегистрированных 868 инцидентов в мире), Великобритании и Канады.

Статистика наличия умысла в несанкционированных действиях показывает тенденцию к увеличению целенаправленных атак (более 32 %), в том числе с участием сотрудников внутри организаций (учреждений, компаний), при этом случайные утечки за счет халатности сотрудников составили около 37%. Больше всего конфиденциальной информации (22%) утекает через интернет (веб-сервисы).

Одним из основных способов обеспечения защиты от несанкционированного доступа (НСД) к информации, обрабатываемой в информационно-вычислительных системах, является создание замкнутой компьютерной системы (ЗКС). Особенно это важно при использовании зарубежных вычислительных средств.

Для создания замкнутой среды разработан широкий ассортимент устройств, призванных ограничить потенциально злонамеренные возможности недоверенного компьютера [3]. Они обеспечивают строго регламентированный доступ к автоматизированным рабочим местам (АРМ) и регламентируют или полностью ограничивают доступ к транспортной среде.

Средства создания замкнутой среды можно разделить на две категории:

- защита от прямого доступа злоумышленника или недобросовестного сотрудника к АРМ: включение, загрузка операционной системы (ОС), вход в систему и получение доступа к ресурсам;
- защита каналов связи локальной вычислительной сети (ЛВС), т.е. защита АРМ от НСД по сети.

Создание замкнутой среды для АРМ с одним пользователем можно построить с помощью аппаратно-программных модулей доверенной загрузки (АПМДЗ), доверенных систем запуска компьютера (BIOS), средств виртуализации и средств защиты от атак из ЛВС. Для многопользовательского АРМ для создания ЗКС для каждого пользователя дополнительно применяется система (или средство) разграничения доступа (СРД) [4]. С целью предотвращения доступа к информации на жестком диске в случае разуклоптования АРМ или его кражи применяются шифраторы диска, обеспечивающие криптографическую защиту хранящейся на нем информации.

Применение «классических» программно-аппаратных средств обеспечит высокую степень защиты информации на АРМ.

Наиболее полно функции аппаратно-программного модуля доверенной загрузки [5] реализованы в АПМДЗ ведущих разработчиков: линейки изделий «КРИПТОН-ЗАМОК» ООО «Фирма АНКАД», средств защиты информации от НСД серии «Аккорд», АПМДЗ «Соболь» ООО «Код безопасности».

Использование системы разграничения доступа предоставит каждому пользователю доступ только к определенным программным и аппаратным ресурсам, а также к информации определенного уровня. Также позволит осуществить динамический и статический контроль за каждым пользователем по доступу к ресурсам АРМ [6].

Как правило, система разграничения доступа привязана к АПМДЗ. Большинство систем защиты от НСД в той или иной степени реализуют возможности СРД. Наиболее полно функции АПМДЗ и СРД реализованы в семействе изделий "КРИПТОН-ЗАМОК" (СРД "КРИПТОН-ЩИТ"), средствах защиты серии «Аккорд» и продукте "Secret Net" (ООО "Код безопасности").

Заключение. Данный подход позволит обеспечить защиту информации в сетях с высоким уровнем конфиденциальности и предотвратить несанкционированный доступ на эти объекты.

СПИСОК ЛИТЕРАТУРЫ

1. Лепешкин О.М. ИССЛЕДОВАНИЕ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СИСТЕМ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ. Инфокоммуникационные технологии. 2007. Т. 5. № 3. С. 165-166.
2. Утечки конфиденциальной информации в России и мире. Итоги 2016 года. Аналитический обзор Zecurion Analytics, www.zecurion.ru
3. Рябко С.Д. Угрозы недоверенного рабочего места пользователя и методы защиты от них. Информационная безопасность. ТСотм. Спецвыпуск. 2012 С.26-30.
4. Хорев П.Б. Анализ средств разграничения доступа к объектам в операционных системах Microsoft Windows Linux // Электронный журнал "Вычислительные сети. Теория и практика" 2009. №2 (15).
6. Лепешкин О.М., Харечкин П.В. Анализ моделей разграничения доступа, реализованных в современных социотехнических системах. Инфокоммуникационные технологии. 2008. Т. 6. № 2. С. 91-93.
7. Краснокутский А.В., Лепешкин О.М., Харечкин П.В. Анализ функциональной применимости ролевой модели разграничения доступа в системах управления. Инфокоммуникационные технологии. 2007. Т. 5. № 3. С. 162-164.



ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

УДК 004.04

ТЕХНОЛОГИИ БЕЗОПАСНОСТИ В БАНКОВСКОЙ СФЕРЕ ОТ КИБЕРАТАК

Абрамова Кристина Владимировна, Голубева Мария Геннадьевна
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Россия, Санкт-Петербург, ул. Двинская, д 5/7
email: Kris410@yandex.ru, mariiigolubeva@gmail.com

Аннотация: В статье рассмотрены проблемы кибератак, изложены актуальные проблемы компьютерных преступлений в банковской сфере и предложены пути их решения.

Ключевые слова: банковская сфера, информационная безопасность, компьютерные преступления, кибератака

TECHNOLOGIES OF SAFETY IN THE BANK SPHERE FROM CYBER ATTACKS

Abramova Kristina, Golubeva Maria
Admiral Makarov State University of maritime and inland shipping
Russia, St. Petersburg, Dvinskaya str. 5/7,
email: Kris410@yandex.ru, mariiigolubeva@gmail.com

Abstract: In article problems of cyber-attacks are considered, current problems of computer crimes in the bank sphere are stated and ways of their solution are proposed.

Keywords: bank sphere, information security, computer crimes, cyber attack

Введение. В настоящее время банки играют большую роль в экономической жизни общества. Сегодня, как никогда прежде, банковские карты и системы нуждаются в защите от киберугроз, которое способны повлиять на критические важные финансовые процессы, которые могут привести к большому ущербу.

Хакеры и киберпреступники применяют все более изощренные методы атак на автоматизированные банковские системы. Без соответствующих средств защиты и управления информационной безопасностью в банковской системе, все подвергается повышенному риску. В связи с проблемой рисков, большая часть нарушений связана с ошибками персонала, которые мало знакомы с аспектами компьютерной безопасности [3].

Безопасность информационных банковских систем содержит две составляющие: безопасность компьютера и безопасность сети. Безопасность компьютера рассматривается как автономная система, где обеспечивается средствами операционных систем и приложений и встроенными аппаратными средствами компьютера. Сетевая безопасность предполагает защиту данных в момент передачи по линиям связи и защиту от несанкционированного удаленного доступа в сеть [1].

Организуя меры обеспечения сетевой безопасности, банки строят защиту корпоративных информационных ресурсов от проникновения и кражи данных, постоянно контролируют все события в сетевой инфраструктуре, обнаруживая сбои в работе оборудования, анализируют их причины. Системы работают по принципу проактивной защиты – речь идет о том, что потенциальные конфликты и угрозы ликвидируются еще до их появления. Это обеспечивает постоянную доступность корпоративных сетей, сервисов и приложений, увеличивает скорость коммуникаций и выполнения задач, повышает мобильность сотрудников и служит эффективной защитой от большинства современных киберугроз [2].

Существуют некоторые базовые технологии для обеспечения безопасности сетей:

- антивирусы;
- межсетевые экраны (Firewall);
- виртуальные частные сети (VPN);
- системы обнаружения и предотвращения сетевых вторжений (IDS/IPS);
- системы противодействия DDoS-атакам;
- средства обнаружения сетевых аномалий;
- управление доступом в сети.

Современные антивирусные решения включают в себя не только сигнатурную защиту, но и более современные средства, такие как поведенческий анализ программ, экраны уровня приложений, контроль целостности критических для операционной системы данных и другие методы защиты рабочих мест и серверов. Корпоративная сеть должна быть защищена не только от вирусных, но и от целенаправленных сетевых атак. Для этого достаточно поставить систему блокировки неиспользуемых сетевых протоколов и сервисов, что и делает межсетевой экран [4].

Существуют два основных типа межсетевых экранов: межсетевые экраны прикладного уровня и межсетевые экраны с пакетной фильтрацией. В их основе лежат различные принципы работы, но при правильной настройке оба типа устройств обеспечивают правильное выполнение функций безопасности, заключающихся в блокировке запрещенного трафика. Кроме того, также есть межсетевые экраны нового поколения (Next-Generation Firewall, NGFW), которые наряду с традиционным функционалом Firewall могут выполнять и ряд других функций.

Система обнаружения вторжений (IDS – Intrusion Detection System) – это решение, обеспечивающее мониторинг событий, происходящих в информационной системе, и их анализ на наличие признаков вторжения в систему: нарушения конфиденциальности и целостности информации и других правил политики информационной безопасности. Система предотвращения вторжений (IPS – Intrusion Prevention System) – решение, которое обеспечивает блокировку выявленных вторжений [4].

Использование средств IDS/IPS позволяет финансово-кредитной организации достичь нескольких целей. Во-первых, обнаружить сетевую атаку и спрогнозировать возможные будущие атаки для предотвращения их дальнейшего развития. Во-вторых, выполнить документирование обнаруженных атак. В-третьих, обеспечить контроль качества администрирования сетей с точки зрения безопасности. Наконец, определить расположение источника атаки по отношению к атакуемой сети или узлу [5].

Закключение. Таким образом, можно сказать что проблемы в данной области обусловлены тем, что количество угроз растёт с каждым годом. Основной целью преступников является доступ к критически важным банковским системам. При этом атаки нацеливаются на конкретные банки с определенной спецификой.

Большинство из таких атак можно было бы предотвратить, применяя базовые принципы защиты информации. Среди главных принципов защиты являются:

- использование спам-фильтров в электронной почте,
- сегментирование корпоративной сети,
- проверка наличия сертификатов устанавливаемых программ,
- фильтрация подозрительных URL,
- использование патчей и обновлений безопасности для эксплуатируемого ПО,
- отслеживание запущенных процессов в корпоративной сети,
- повышение осведомленности персонала.

Наряду с этим важно осуществлять сканирование антивирусными решениями (обновление антивирусных баз), настройку поведенческого анализа в антивирусных решениях, использовать файрвол, межсетевые экраны. Конечно, работники компании не должны открывать ссылки в письмах, пришедших из непроверенных источников. Наконец, необходима организация обмена информацией об инцидентах между участниками информационного взаимодействия в рамках центров реагирования на компьютерные преступления.

СПИСОК ЛИТЕРАТУРЫ

1. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: федеральный закон РФ от 27 июля 2006 г. № 149-ФЗ (в ред. от 28.07.2012 г.) // ГАРАНТ: информационно-правовой портал. – URL: <http://base.garant.ru/12148555/>
2. Валерий Васильев Информационная безопасность в финансовой сфере-2013. / [Электронный ресурс]. URL: <http://www.pcweek.ru/security/article/detail.php?ID=156455>
3. Кибербезопасность: процессы важнее технологий. [Электронный ресурс]. URL: <http://nbj.ru/publs/banki-i-biznes/2017/08/27/kiberbezopasnost-protsessy-vazhnee-tekhnologii/index.html>
4. Технологии безопасности. [Электронный ресурс]. URL: <http://nbj.ru/publs/upgrade-modernizatsija-i-razvitie/2017/02/13/tekhnologii-bezopasnosti/index.html>
5. В.В. Бондарь. Киберпреступность – современное состояние и пути борьбы. // Юридические записки №2 – 2013. [Электронный ресурс]. URL: <http://cyberleninka.ru/article/n/kiberprestupnost-sovremennoe-sostoyanie-i-puti-borby>

УДК 53.087.92

ОБЛАСТИ ПРИМЕНЕНИЯ АРОМОСЕНСОРНЫХ СИСТЕМ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Афанасьев Дмитрий Сергеевич¹, Бардакова Елена Андреевна², Быстрыков Денис Сергеевич¹

¹Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
им. В.И. Ульянова (Ленина)

Россия, Санкт-Петербург, ул. Профессора Попова, 5,

²Санкт-Петербургский государственный экономический университет (СПбГЭУ)

Россия, Санкт-Петербург, ул. Садовая, 21

emails: dmitr-afanas@yandex.ru, bardakova.elena95@mail.ru, bystryakov.denis@gmail.com

Аннотация: В статье предлагается организовать мониторинг аромобезопасности пространства при помощи аромосенсорных систем и сетей терминалов запахов. Аромобезопасность – отсутствие в пределах жизненного пространства запахов (летучих веществ), которые указывали бы на возможность возникновения событий, несущих опасность для человека или группы людей. Показано, что подход позволяет создавать эффективные системы для обеспечения безопасности жизненного пространства, защиты от техногенных процессов и социальных взаимодействий, обусловленных терроризмом, алкоголизмом, наркоманией и др. факторами.

Ключевые слова: Аромобезопасность; датчики запахов; электронный нос; интернет вещей; сенсорные сети; обработка данных; облачные вычисления.

APPLICATIONS AROMOSENSOR SYSTEMS FOR SAFETY

Dmitry Afanasiev¹, Elena Bardakova², Denis Bystryakov¹

¹ The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,

² St. Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str. 21

emails: dmitr-afanas@yandex.ru, bardakova.elena95@mail.ru, bystryakov.denis@gmail.com

Abstract: The article is proposed to organize space aromosecurity monitoring by means of aromosensor systems and smell terminal networks. Aromosecurity stands for the absence of smells (volatile substances), indicating the likelihood of events that pose a threat to a person or a group of people within the vital space. It was demonstrated that the approach allows creating effective systems for ensuring vital space security, protection against man-caused processes and social interactions caused by terrorism, alcoholism, drug addiction and other factors.

Keywords: Aromosecurity, sensors of smells, electronic nose, Internet of things, sensor networks, data handling, cloud computing.

Введение. Практическим инструментом движения России к цифровой экономике является Национальная технологическая инициатива. НТИ – это долгосрочная комплексная программа по созданию условий для обеспечения лидерства российских компаний на новых высокотехнологичных рынках, которые будут определять структуру мировой экономики в ближайшие 15–20 лет.

Согласно одному из принципов, которые лежат в основе выбора рынков будущего – рынок должен представлять собой:

- сеть, которая содержит сенсорные поля, измеряющие физические характеристики жизненного пространства,
- логический уровень, на котором, при помощи телекоммуникационных технологий данные с сенсоров объединяются в облачных хранилищах,
- уровень сервиса, на котором при помощи специального программного обеспечения осуществляется обработка, анализ собранных данных и вырабатываются управляющие воздействия.

Одним из типов сенсоров такого рода могут служить сенсоры запахов. Они способны преобразовать в цифровой вид любые запахи, возникающие в пространстве. Характеристики сенсоров все время улучшаются так, что они становятся все дешевле, могут работать автономно продолжительное время и регистрировать концентрации в долях ppm. Контроль запахов позволяет осуществлять мониторинг аромобезопасности жизненного пространства.

Аромобезопасность – отсутствие в пределах жизненного пространства запахов (летучих веществ), которые указывали бы на возможность возникновения событий, несущих опасность для человека или группы людей.

Предлагается организовать мониторинг аромобезопасности пространства при помощи аромосенсорных систем и сетей терминалов запахов.

Заключение. В статье рассматриваются возможные области применения аромосенсорных систем [1], [2]. К числу таких областей относятся [3]:

- противодействие террору. К этой группе относятся сенсоры, способные регистрировать тротил, тринитрофенол, гексоген, октоген и другие вещества;
- контроль производственных процессов. К данной группе относятся сенсорные поля, регистрирующие аммиак, сернистый ангидрид, фосген, окись этилена, сероуглерод, бензол и др.;
- социальные взаимодействия. К этой группе относятся датчики регистрирующие запахи этанола, наркотических веществ;
- экологический мониторинг. К ней можно отнести сенсоры, регистрирующие параметры смога в больших городах, запахи, возникающие вследствие вредных выбросов на химических производствах и т.п.;
- контроль бытовых газов. К этой группе относится регистрация запаха метана, угарного газа, горючих веществ;

— контроль качества воздуха. В эту группу относится регистрация недопустимых концентраций углекислых газов в офисных, образовательных и др. помещениях.

СПИСОК ЛИТЕРАТУРЫ

1. Афанасьев Д. С., Быстряков Д. С., Колбанёв М. О. Принципы построения системы аромобезопасности // Информационные технологии и телекоммуникации. 2016. Том 4. № 4. С. 97–103.
2. Колбанёв М.О., Татарникова Т.М. Информационный объем базовых информационных процессов // Информационно-управляющие системы. – СПб.: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2014. С.42–47.
3. Афанасьев Д. С., Бардакова Е. А., Быстряков Д. С. Аналитический обзор датчиков летучих веществ для интернета вещей // Информационные технологии и телекоммуникации. 2016. Том 4. № 4. С. 1–12.

УДК 681.3

ОСОБЕННОСТИ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Володина Анастасия Андреевна, Левкин Игорь Михайлович
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский пр., 49,
email: nasti.vol@gmail.ru lev.kin@yandex.ru

Аннотация: В статье рассмотрены особенности использования методического аппарата адаптивного управления для построения системы защиты информации государственных информационных систем. Показаны варианты использования различных уровней адаптации для элементов иерархической системы защиты информации.

Ключевые слова: государственная информационная система, система защиты информации, уровни адаптации.

FEATURES OF CONSTRUCTION OF SYSTEMS OF INFORMATION SECURITY OF STATE INFORMATION SYSTEMS

Volodin Anastasiya Andreevna, Levkin Igor Mikhailovich
Saint-Petersburg National research University of information technologies, mechanics and optics,
Russia, Saint-Petersburg, Kronverkskiy prospect, 49,
email: nasti.vol@gmail.ru lev.kin@yandex.ru

Abstract: In the article the peculiarities of using the methods of adaptive control to build the system of information security of state information systems. Shows the use of different levels of adaptation to elements of a hierarchical system of information protection.

Keywords: public information system, information protection system, the levels of adaptation.

Введение. Процесс быстрого развития информационного общества поспособствовал широкому внедрению информационных систем на объектах микро (предприятия, организации, фирмы и т.п.), мезо (регионы, отрасли) и макроуровня (государства и их коалиции), что резко обострило проблему их информационной безопасности. В особенности это относится к большим информационным системам, обеспечивающим функционирование крупномасштабных объектов (объектов мезо и макроуровня). К таким информационным системам относятся, в частности, государственные информационные системы (ГИС). ГИС обладают свойствами сложных систем, которые необходимо учитывать при оценке безопасности их инфраструктуры: во-первых, при увеличении числа пользователей системы возрастает количество запросов и обращений, а вместе с этим увеличивается и нагрузка на подсистемы и соответственно на программно-аппаратное обеспечение; во-вторых, поскольку элементы ГИС разнесены на большое расстояние, повышается сложность их обслуживания; в-третьих, в ГИС содержится большее количество подсистем и уровень их значимости выше, а также большие ИС выполняют больше функций и задач, соответственно процессы обработки информации усложняются и требуют больших временных затрат; в-четвертых, обработка и хранение большого объема разноплановой информации приводит к увеличению количества информационных потоков.

В состав агрегированных подсистем ГИС должны входить распределенные подсистемы:

- аппаратного обеспечения (базы данных, серверы приложений, системы хранения данных);
- программного обеспечения (состав системы будет зависеть от реализуемых сервисов, а также от уровня их доступности);

- математического обеспечения (будет состоять из алгоритмического и программного обеспечения [1, 2]. Учитывая сложность информационной инфраструктуры и, принимая во внимание, что ГИС относятся к объектам, работающим в условиях высокой неопределенности внешних и внутренних информационных угроз, среды которых подвергаются интенсивным изменениям,

управление их системами защиты информации (СЗИ) целесообразно строить на принципах адаптации [3, 4].

— функционирования, рациональным решением по обеспечению состояния информационной безопасности, будет применение адаптивного метода.

В связи с тем, что рассматриваемая СЗИ ГИС является сложной иерархической системой на первом этапе целесообразно рассмотреть локальные задачи адаптации, охватывающие лишь отдельные аспекты функционирования СЗИ ГИС (например, систему защиты информации элементов ГИС различных уровней иерархии) и лишь потом сформировать из этих подсистем иерархическую систему адаптации, позволяющую оперативно приспосабливать всю СЗИ ГИС к новым состояниям среды. Справедливость этого подхода обусловлена тем, что рассматриваемые информационные угрозы являются универсальными для любых элементов ГИС, однако их набор является специфическим для каждого элемента. Подсистемы адаптации этих элементов могут соответствовать следующим уровням.

1. Аппаратурный уровень, предполагающий адаптацию установок, параметров и структуры технических средств СЗИ ГИС (например, параметров фильтров в каналах связи элементов информационной инфраструктуры, чувствительности средств наблюдения и т.д.). Критериями эффективности этого уровня обычно являются среднее время ликвидации информационной угрозы с вероятностью не ниже заданной; минимальный набор средств защиты информации, препятствующий реализации информационной угрозы и т.п.

2. Алгоритмический уровень адаптации СЗИ ГИС, предполагающий адаптацию алгоритмов ликвидации информационных угроз с целью учета специфики решаемых в системе задач (например, при адаптации алгоритмов оптимизации и т.д.). Критериями эффективности алгоритмического уровня адаптации СЗИ ГИС обычно являются среднее время решения задачи, точность этого решения, вероятность ошибки и т.д.

3. Программный уровень адаптации, предполагающий адаптацию при выборе программ работы аппаратно-программных средств СЗИ ГИС из альтернативного множества (например, при выборе антивирусных программ, программ разделенного доступа и т.п.). Программная адаптация СЗИ элементов ГИС связана с манипулированием отдельными программами защиты информации и выбором той, которая работает наилучшим образом в смысле заданного критерия. Алгоритмически программная адаптация реализуется в виде альтернативного варианта структурной адаптации

4. Системный уровень адаптации, предполагающий совершенствование функционирования системного обеспечения СЗИ ГИС (например, адаптация дисциплин ликвидации информационных угроз, распределения сил и средств защиты информации и т.д.). Эта адаптация затрачивает системное обеспечение СЗИ ГИС, для того чтобы повысить эффективность ее функционирования при различных условиях эксплуатации.

5. Сетевой уровень адаптации, предполагающий адаптацию процессов передачи информации о характере информационных угроз по СЗИ ГИС (например, при определении маршрута сообщения по элементам ГИС).

Формирование адаптивной иерархической СЗИ ГИС на заключительном этапе должно осуществляться методами стохастического программирования с учетом законов распределения продолжительности решения задач защиты информации в различных подсистемах адаптации различных уровней иерархии.

Заключение. Использование методического аппарата адаптивного управления сложными информационными системами позволяет, с одной стороны рационально распределить силы и средства защиты информации по элементам СЗИ ГИС в зависимости от статистических параметров их проявляемости, с другой стороны, своевременно реагировать на появление новых информационных угроз.

СПИСОК ЛИТЕРАТУРЫ

1. Информационные системы в государственном управлении [Электронный ресурс]. - Режим доступа: file:///C:/Users/HP%20ProBook/Downloads/informatsionnye-sistemy-v-gosudarstvennom-upravlenii.pdf (дата обращения 26.08.2017).
2. Создание систем защиты информации государственных информационных систем [Электронный ресурс]. - Режим доступа: http://www.dialognauka.ru/solutions/security_gosinfosystem/ (дата обращения 26.08.2017).
3. Растринин Л.А. Адаптация сложных систем. — Рига: Зинатне, 1981.
4. Володина А.А., Левкин И.М. Оценка эффективности процесса отражения информационных угроз в больших информационных системах// Приборостроение, № 5, 2016, с. 335-341.

УДК 681.3

ОБ АЛГОРИТМЕ ОБРАБОТКИ СИТУАЦИОННЫХ МОДЕЛЕЙ

Головкин Юрий Борисович

Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, 21,
email: comparif@rambler.ru

Аннотация: В статье рассмотрены вопросы разработки алгоритмов обработки ситуационных моделей управления.

Ключевые слова: алгоритм, модель, система, управление.

ABOUT ALGORITHM PROCESSING SITUATION MODELS

Golovkin Yuri

The St. Petersburg State Economic University,
Russia, St. Petersburg, Sadovaya str. 21,
email: comparif@rambler.ru

Abstract: The article presents design algorithm processing situation models control.

Keywords: algorithm, model, system, control.

Введение. Разработка моделей и программных средств, повышающих качество формирования управляющих воздействий для обеспечения эффективного автоматизированного управления сложными объектами, является важной и актуальной задачей. К процессу и результату проектирования предъявляются многие требования, основными из которых являются качество и сроки разработки.

Сложные объекты управления характеризуются многоуровневой структурой, большим количеством взаимодействующих и взаимосвязанных элементов, разнообразием режимов функционирования. Особенностью многих объектов является дискретный характер управления. Процесс управления объектами подобного класса можно представить в виде последовательной смены ситуаций, требующих вполне конкретных управляющих действий. При организации автоматизированного управления такими системами целесообразно и эффективно использовать ситуационный подход. Под ситуацией понимается состояние процесса управления, характеризующееся определенными параметрами функционирования объекта управления и определяющее необходимые управляющие действия.

Модель управления сложными объектами, в том числе и техническими, можно представить в виде ориентированного графа. Вершины графа соответствуют ситуациям процесса управления, а дуги задают возможные переходы ситуаций. Дугам ставятся в соответствие предикаты, контролирующие условия перехода ситуаций. Кроме того, дуги помечаются символами, которые определяют управляющие действия. Также дугам могут быть присвоены приоритеты. При этом значения приоритетов для всех дуг, исходящих из одной вершины, должны быть различны. Одна из вершин модели выбирается в качестве первой и соответствует начальной ситуации. Для адекватного описания процесса управления ситуационная модель может иметь многоуровневую структуру, при которой любой вершине (ситуации) ставится в соответствие некоторая внутренняя модель [1-2].

Рассматривается алгоритм обработки ситуационной модели. Обработка начинается с начальной вершины ориентированного графа. Далее производится проверка значений предикатов исходящих дуг. Если предикат истинен, то производится переход к обработке следующей вершины. Если же предикат ложен, то происходит проверка на активность других исходящих дуг данной вершины графа. Аналогичным образом производится обработка всех уровней модели. Таким образом, на каждом такте работы формируются выходные управляющие действия и корректируется текущая ситуация процесса управления.

Обсуждаются вопросы программной реализации разработанного алгоритма и моделирования процесса управления в интегрированной среде программирования. Процесс разработки программного обеспечения включает в себя два этапа: создание пользовательского интерфейса и написание программного кода, который придает элементам интерфейса определенную функциональность. Пользовательский интерфейс создается с использованием визуальных компонентов, каждый из которых характеризуется своими свойствами и методами их обработки.

При разработке программного обеспечения использовался метод нисходящего проектирования. Программное обеспечение имеет многоуровневую модульную структуру. Между модулями устанавливается взаимодействие по информации и управлению. Модули верхнего уровня выполняют более общие функции и вызывают модули нижних уровней, в которых детализируется решение задачи. Модули контроля обеспечивают проверку логических условий перехода ситуаций. Программа определяет текущее состояние процесса управления по ситуационной модели и запускает соответствующие процедуры, которые задают необходимые управляющие действия.

Закключение. Таким образом, использование ситуационных моделей и эффективных алгоритмов их обработки приводит к увеличению надежности формирования управляющих действий и повышает качество автоматизированного управления сложными объектами в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Головкин Ю.Б., Ярцев Р.А., Газетдинова С.Г., Арсланова А.Р., Давлетова Г.Б. Динамическая модель дискретных процессов с учетом предыстории // Региональная информатика и информационная безопасность. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. – 2015. С 178-180.
2. Головкин Ю.Б., Гусаренко А.С. Моделирование производственных систем в GPSS // Управление в сложных системах. Межвузовский научный сборник. Уфимский государственный авиационный технический университет. Уфа, 2011. С.136-149.

УДК 004.75

АЛГОРИТМ РАЗМЕЩЕНИЯ СЕНСОРОВ СИСТЕМЫ ИНТЕРНЕТА ВЕЩЕЙ

Дзюбенко Иван Николаевич

Санкт-Петербургский государственный университет аэрокосмического приборостроения
Россия, Санкт-Петербург, ул. Большая Морская, 67,
email: azruhal@gmail.com

Аннотация: Предлагается генетический алгоритм размещения сенсорных устройств в одноранговой беспроводной сети Интернета вещей.

Ключевые слова: Интернет вещей, беспроводная сенсорная сеть, задача размещения, генетический алгоритм.

ALGORITHM OF IOT SYSTEM SENSORS PLACEMENT

Ivan Dzubenko

Saint-Petersburg State University of Aerospace Instrumentation
Russia, St. Petersburg, Bolshaya Morskaya str. 67
email: azruhal@gmail.com

Abstract: A genetic algorithm for locating sensory devices in a peer-to-peer wireless Internet of things.

Keywords: Internet of things, wireless sensor network, allocation problem, genetic algorithm.

В работе предложен генетический алгоритм (ГА) размещения сенсорных узлов (СУ) с целью максимального покрытия территории, на которой функционирует система Интернета вещей [1-5]. Суть ГА состоит в следующем: территория размещения делится на отдельные фрагменты, каждый из которых может быть свободным участком или участком с препятствиями, например, зданием, деревьями и т.д. или на участке уже расположено СУ с неким радиусом действия R . Территория представлена как матрица A , в которой свободный участок обозначен нулем, препятствие - единицей, а СУ цифрами $2...N+1$, где N – количество различных СУ. Матрица A разбивается на два множества: множество B , представляющее собой позиции размещения СУ и вспомогательное множество C , позволяющее восстановить из B оригинальную матрицу. Кодирование индекса СУ составляет $N_b = \lceil \log_2 N \rceil$ бит.

В терминах ГА хромосома представляет собой набор из индексов СУ в битовом коде. Фитнесс функция есть суммарная площадь покрытия. Рекомбинирование в ГА реализовано стандартными методами: одноточечное скрещивание с вероятностью $p_{cr} \geq 0,5$ между случайно попарно взятыми прошедшими отбор хромосомами и мутация с вероятностью $p_{mt} = 0,1$ для одного из генов хромосомы.

Оценка фитнес функции совершается следующим образом. Для решения, записанного в i -й хромосоме составляется двумерный булевский массив покрытия X , размерности матрица A . Далее происходит обход по СУ, при котором для каждого СУ определяются четыре границы в разные стороны на плоскости в зависимости от R . Таким образом, по полученным границам совершается обход квадратной области. Далее проверяется, удовлетворяет ли ячейка условию при помощи простого уравнения окружности $(x-a)^2 + (y-b)^2 \leq R^2$, где a, b – координаты СУ; x, y – координаты ячейки обходимой области. Если ячейка удовлетворяет условию, то в X с аналогичным индексом записывается true. Таким образом, создаются «круги покрытия» вокруг СУ.

Условие выхода из ГА выполняется при достижении одного из двух ограничений:

1) выполнено максимальное число итераций и оптимальным решением размещения будет считаться хромосома с максимальным значением фитнес функции.

2) полное покрытие выполнено и найденное решение невозможно улучшить.

При приложении такой постановки задачи к трехмерному пространству размерность множеств B и C не изменится.

Предложенный ГА размещения СУ реализован на языке C++, где класс Grid описывает территорию с препятствиями и некий начальный вариант расстановки СУ, класс ГА осуществляет работу алгоритма.

На вход ГА подаются следующие параметры: Grid, набор СУ, включающий их номера и количество; таблица соответствий СУ и R в виде $\text{map} < \text{int}, \text{int} >$; размер популяции; p_{cr} , p_{mt} , максимальное число итераций работы ГА.

Для визуализации результата реализован графический интерфейс на базе открытой библиотеки wxWidgets. В окне интерфейса появляется карта рассматриваемой территории и отмечаются радиусы действия всех СУ, что позволяет визуально оценить качество решения.

Проведенные эксперименты для различных вариантов территорий с препятствиями и разного количества разнородных СУ показали результат размещения близкий к 100%, худшим решением для 100 различных экспериментов является 97,4% покрытия рассматриваемой территории.

СПИСОК ЛИТЕРАТУРЫ

1. Татарникова Т.М. Елизаров М.А. Модель оценки временных характеристик при взаимодействии в сети интернета вещей // Информационно-управляющие системы. – 2017. № 2 (87). – С. 44-50.
2. Воробьев А.И. Татарникова Т.М. Применение генетического алгоритма для решения задачи обеспечения отказоустойчивости вычислительного кластера// Информационные технологии и системы: управление, экономика, транспорт, право. – 2011. № 1. – С. 3-11.
3. Кутузов О.И., Татарникова Т.М. Подход к оптимизации структуры межсетевого устройства с привлечением генетических алгоритмов//Известия СПбГЭТУ ЛЭТИ. 2006. № 11. С. 61-67.
4. Татарникова Т.М. Структурный синтез центра сопряжения корпоративных сетей// Информационно-управляющие системы. – 2015. №3. –С. 92-98.
5. Татарникова Т.М. Аналитико-статистическая модель оценки живучести сетей с топологией mesh// Информационно-управляющие системы. – 2017. № 1 (86). – С. 17-22.

УДК 004.056

SOC КАК ИНСТРУМЕНТ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ

Демидова Наталья Дмитриевна, Колоколов Даниил Сергеевич
Санкт-Петербургский государственный технологический институт (технический университет),
Россия, Санкт-Петербург, Московский проспект, 26,
Санкт-Петербургский государственный университет,
Россия, Санкт-Петербург, Университетская наб., 7/9,
email: dmdv.natalie@gmail.com, kolokolov.d@gmail.com

Аннотация: Рассматривается SOC, как эффективный инструмент управления информационной безопасностью предприятия наравне с управлением рисками, контролем утечек информации и управлением доступом. Поступающая информация анализируется на основании существующей базы инцидентов, которая нарабатывается на основе опыта полученных в рамках внедрения и реализации проектов по разворачиванию центров реагирования на инциденты ИБ у заказчиков. На первый план здесь выходят проактивность, актуальность решения, оперативность и быстрая перестройка под изменяющиеся реалии.

Ключевые слова: *Безопасность, Security Operation Center*

SOC AS INSTRUMENT OF MANAGEMENT OF INFORMATION SECURITY OF THE ENTERPRISE

Natalia Demidova, Daniil Kolokolov
St. Petersburg State Technological Institute (Technical University),
Russia, Saint-Petersburg, Moskovsky prospect, house 26,
St. Petersburg State Institute,
Russia, St. Petersburg, Universitetskaya Embankment, 7/9
email: dmdv.natalie@gmail.com, kolokolov.d@gmail.com

Abstract: SOC as the effective instrument of information security management of the enterprise on an equal basis with risk management, monitoring of information leakages and access control is considered. The arriving information is analyzed based on the existing basis of incidents which is acquired on the basis of experience received within implementation and projects implementation on deployment of centers of response to IB incidents at customers. Into the forefront there are a pro-activity, relevance of the decision, efficiency and fast reorganization under the changing realities here.

Keywords: *Security, Security Operation Center*

Security Operations Center, (SOC) следует рассматривать в качестве современного инструмента эффективного управления информационной безопасностью (ИБ) предприятия наравне с управлением рисками, контролем утечек информации и управлением доступом. Инфраструктура банков, организаций, коммерческих и промышленных предприятий непрерывно усложняется, что связано, в первую очередь, с развитием технологий и увеличением разновидностей электронных устройств, хранящих и передающих информацию. Естественно, такая тенденция формирует повышенную потребность бизнеса в автоматизации и защите своих информационных и других активов [1].

Традиционный подход к контролю потенциально опасных событий в виде нескольких независимых средств защиты информации с самостоятельными консолями, которые, как правило, контролируются разными людьми, становится чрезмерно ресурсоемким и неэффективным, в результате чего адекватная и своевременная реакция на них становится все более трудозатратной. Сложность обеспечения соответствующей реакции на потенциально опасные события неизбежно приводит к снижению эффективности системы ИБ организации. Решением такой задачи является создание центра мониторинга и реагирования, который строится на регламентах, процессах, квалифицированных кадрах и грамотном техническом решении.

Однако, как показывает практика, создание собственного ситуационного центра ИБ не всегда возможно. Большие капитальные затраты на закупку и внедрение средств автоматизации, а также

необходимость содержания и поддержания квалификации персонала, обслуживающего ситуационный центр (группа мониторинга, аналитики ИБ, администраторы) – вот лишь часть подводных камней, с которыми сталкиваются организации, желающие развернуть у себя ситуационный центр ИБ.

Комплексное организационно-техническое решение, позволяет:

- автоматизировано выявлять события, представляющие потенциальную угрозу для организации, ее информационных систем или информационных активов (инциденты ИБ);
- обеспечить длительное хранение всего объема собранных событий и зафиксированных инцидентов ИБ для возможности проведения постинцидентного расследования;
- реализовать процесс обработки выявленных инцидентов, который бы позволил в гарантированное время (зависящее от уровня критичности инцидента) оповещать ответственные подразделения организации о том, что произошло, и рекомендовать необходимые меры для предотвращения воздействия инцидента информационной безопасности на бизнес.

Вся информация консолидируется аналитиками на основании существующей базы инцидентов, которая нарабатывается на основе опыта полученных в рамках внедрения и реализации проектов по разворачиванию центров реагирования на инциденты ИБ у заказчиков. База инцидентов пополняется постоянно на основании новых угроз и актуализации способов выявления известных.

В случае появления или выявления новых угроз осуществляется информирование и доработка решения. На первый план здесь выходят проактивность, актуальность решения, оперативность и быстрая перестройка под изменяющиеся реалии.

В докладе обсуждаются проблемы выявления инцидентов информационной безопасности, наиболее часто интересующих заказчиков:

- DDoS-атаки;
- компрометация административных учетных записей;
- компрометация учетных записей внешних сервисов;
- атаки на веб-приложения;
- сетевые атаки;
- вирусное заражение;
- выявления сбора информации о системах;
- нелегитимное использование привилегированных учетных записей;
- утечки конфиденциальной информации;
- нарушения правил удаленного доступа;
- нарушения правил доступа в сеть Интернет;
- несанкционированные изменения в ИТ-инфраструктуре, (например, вследствие деятельности подрядчиков).

СПИСОК ЛИТЕРАТУРЫ

1. Хаханов В. И. Инфраструктура диагностического обслуживания SOC. Вестник томского государственного университета., 2008, 75-80 с.

УДК 004.75

ИМИТАЦИОННАЯ МОДЕЛЬ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ В СЕТИ ИНТЕРНЕТА ВЕЩЕЙ

Елизаров Максим Андреевич

Санкт-Петербургский государственный экономический университет

Россия, Санкт-Петербург, ул Садовая, д 21,

emails: elizarovmaks@gmail.com **Аннотация:** Предлагается модель взаимодействия в сетях Интернета вещей, реализованная в системе имитационного моделирования AnyLogic. Модель учитывает фундаментальные характеристики сетей Интернета вещей.

Ключевые слова: агентное моделирование, Интернет вещей, информационное взаимодействие, сенсорные устройства, динамика изменения состояния Интернета вещей.

IMITATION MODEL OF INFORMATIONAL INTERACTION IN THE IOT NETWORK

Elizarov Maksim

Saint-Petersburg State University of Economics

Russia, St. Petersburg, Sadovaya str, 21,

emails: elizarovmaks@gmail.com

Abstract: A model of interaction in IoT networks, implemented in the AnyLogic simulation system, is proposed. The model takes into account the fundamental characteristics of IoT networks.

Keywords: agent simulation, Internet of things, information interaction, sensory devices, dynamics of IoT state change.

Специфика информационного взаимодействия в сетях Интернета вещей (Internet of Things, IoT) определяется фундаментальными характеристиками IoT [1]. В соответствии с рекомендациями Международного Союза Электросвязи (МСЭ-Т) к их числу относятся: *связность* – возможность любой вещи быть связанной с глобальной инфокоммуникационной структурой [2]; *обеспечение вещей услугами* – предоставление сетевых услуг без ограничений; *гетерогенность* – возможность устройствам IoT быть построенными на различных аппаратных, программных платформах и сетях; *динамические изменения* – изменения статуса вещей во времени, их числа, местоположения, скорости и т.п.; *огромное число вещей* – десятки триллионов вещей и триллионные сети соответственно.

Предложена имитационная модель информационного взаимодействия в сети Интернета вещей, основанная на мультиагентной парадигме, которая реализована в системе имитационного моделирования AnyLogic. Модель функционирует следующим образом: стохастическим образом заданные запросы поступают от агентов сети [3]. Если агент проходит валидацию и сертифицирован на прием/передачу информации и передает запрос впервые с момента обнаружения в сети, то он добавляется в «карту» сети, для идентификации его в пространстве [4]. После обработки и сохранения информации в памяти, происходит отправка управляющей команды от сервера агенту, на которую агент должен отправить нотификацию о получении [5]. В процессе прохождения всех этапов схемы могут возникнуть следующие ситуации:

Запрос агента на передачу данных отклонен в силу возникновения коллизий источников данных или маршрут для передачи еще не построен [6].

Многократное добавление одного и того же агента в карту. Проблема решается путем удаления объекта из карты, если по истечении заданного времени от него не поступает ответ.

«Зацикливание» – отправка одной и той же команды агенту после отключения/подключения. Если агент не может выполнить переданную команду (выражается в отсутствии данных, которые ожидается получить в ответ), то система будет предлагать выполнить эту команду снова до тех пор, пока она не будет выполнена, либо по истечении определенного количества попыток, информация о которых хранится в памяти. Запрос успешно проходит – информационное взаимодействие состоялось.

Предполагается, что мобильный объект имеет возможность перемещаться свободно, или следуя определенному алгоритму [7-9]. В процессе своего перемещения он может покидать и входить в зону покрытия сети, в зависимости от стандарта и используемого частотного диапазона радиус покрытия может различаться (IEEE 802.11). Таким образом, первые два блока схемы описывают движение и подключение агента к сети, после которого становится возможным обмен информацией с другими агентами и участниками сети. Подключившись, агент начинает передавать и получать сообщения. Следует отметить, что валидация агента (разрешение на прием-передачу) производится на уровне всей системы. При отсутствии ответа на сообщение, агент считается отключенным от сети. Помимо вероятности отключения агента от сети, существует также возможность возникновения коллизии между несколькими объектами, которые пытаются одновременно передать информацию.

СПИСОК ЛИТЕРАТУРЫ

1. Kellmerit Daniel. The Silent Intelligence: The Internet of Things. Publisher: DND Ventures LLC, 2013. – 454 p.
2. Татарникова Т.М. Аналитико-статистическая модель оценки живучести сетей с топологией mesh// Информационно-управляющие системы. – 2017. № 1 (86). – С. 17-22.
3. Кутозов О.И. Татарникова Т.М. Из практики применения метода Монте-Карло//Заводская лаборатория. Диагностика материалов. – 2017. Т. 83. № 3. – С. 65-70.
4. Татарникова Т.М., Елизаров М.А. Процедура разрешения коллизий в RFID-системе// Известия высших учебных заведений. Приборостроение. – 2017. Т. 60. № 2. – С. 150-157.
5. Богатырев В. А. Богатырев А. В., Богатырев С. В. Оценка надежности выполнения кластерами запросов реального времени//Известия вузов. Приборостроение. – 2014. Т. 57. № 4. – С. 46-48.
6. Татарникова Т. М., Елизаров М.А. Имитационная модель виртуального канала// Научно-технический вестник информационных технологий, механики и оптики. – 2016. Т.16. № 6. – С. 1120-1127.
7. Татарникова Т.М. Елизаров М.А. Модель оценки временных характеристик при взаимодействии в сети интернета вещей// Информационно-управляющие системы. – 2017. № 2 (87). – С. 44-50.
8. Кутозов О.И. Татарникова Т.М. Моделирование систем и сетей телекоммуникаций. – СПб: РГГМУ, 2012. –134 с.
9. Кутозов О.И., Татарникова Т.М. Инфокоммуникационные сети. Моделирование и оценка вероятностно-временных характеристик.– СПб.: ГУАП, 2015. – 382 с.

УДК 004.7

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ В ОБЛАЧНЫХ СЕРВИСАХ

Емельянов Александр Александрович

Санкт-Петербургский государственный экономический университет

Россия, Санкт-Петербург, ул. Садовая, 21

emails: S1_Alex2000@mail.ru

Аннотация: приводится обзор существующих облачных сервисов и анализ проблем информационной безопасности, возникающих при их эксплуатации

Ключевые слова: облачные сервисы, безопасность, обслуживание

SECURITY IN CLOUD SERVICES

Emelyanov Alexandr

Saint-Petersburg state university of economics
Russia, Saint-Petersburg, Sadovaya street, h.21
emails: S1_Alex2000@mail.ru

Abstract: provides an overview of existing cloud services and an analysis of information security problems arising during their operation.

Keywords: *cloud services, security, maintenance.*

Введение. Внедрение новых информационных технологий в экономическую сферу позволяет существенно улучшать схемы реализации бизнес-процессов предприятий. Одним из актуальных направлений являются облачные сервисы. Их применение предоставляет более удобные, быстрые и надёжные модели управления данными, что, в свою очередь, уменьшает затраты на формирование, обслуживание и поддержку программно-аппаратного комплекса компаний.

Важнейшими характеристиками, определяющими возможность использования сервисов обработки и хранения данных, являются надёжность [1], [2], скорость реакции, безопасность, кроссплатформенность и удобство эксплуатации.

Все облачные технологии можно разделить на несколько категорий, или моделей обслуживания:

- SaaS, или Software as a Service. Данный подход реализует доступ к программному обеспечению в облачной инфраструктуре. Использование этой модели позволяет поместить существенную часть ПО вне предприятия, тем самым снижая расходы на закупку аппаратного обеспечения, поддерживающего функционирование серверной части различных АИС. Также упрощается централизованный доступ [3] и взаимодействие пользователей, находящихся в различных местах.

- PaaS, или Platform-as-a-Service. В рамках данной модели используется не только готовое ПО, но и разрабатываемое сотрудниками предприятия.

- IaaS, или Infrastructure-as-a-Service. Допускается использование как прикладного, так и системного ПО, включая различные ОС, сетевые сервисы, системы хранения данных и т.д.

В рамках подхода к развёртыванию облачных сервисов можно выделить четыре основных модели:

- Публичное облако. Используется большим числом клиентов (как частных лиц, так и компаний), находится в собственности какой-либо из организаций – научной, коммерческой или правительственной. Применяются общедоступные центры обработки данных.

- Общественное облако. Подобная инфраструктура предназначена для совместного использования несколькими организациями с общими направлениями деятельности. Обычно находится в собственности одной из организаций либо осуществляется распределение задач между двумя предприятиями и более.

- Частное облако. Данная модель предназначена для эксплуатации в рамках одной организации. Решаются задачи, реализуемых в процессе деятельности конкретного предприятия.

Большинство компаний (особенно в сферах малого и среднего бизнеса) заинтересованы в снижении капитальных и операционных расходов на АПК. При переходе на облачные технологии выделяют следующие преимущества:

- уменьшение затрат на обслуживание внутрикорпоративных ЦОДов. Делегирование задач контроля функционирования систем обработки данных провайдеру облачных услуг позволяет сократить штат системных техников и администраторов;

- отказ от покупки серверного оборудования, а также его регулярного обновления, высвобождает существенные финансовые ресурсы, аналогично ситуация обстоит с лицензионным программным обеспечением;

- облачные сервисы характеризуются высокой степенью доступности.

На текущий момент существенная часть решаемых задач с применением ИТ в рамках большинства предприятий может быть реализована с помощью описанных выше моделей обслуживания [4], [5].

Вне зависимости от модели обслуживания и развёртывания, каждый из облачных сервисов реализуется в виде ЦОДа либо системы ЦОДов, представляющих из себя совокупность программно-аппаратных (серверных) решений, объединённых в единую инфраструктуру [6]. Существует большое количество различных внешних угроз, способных нарушить штатное функционирование всего комплекса. Это и сетевые атаки, и уязвимости операционных систем, и вредоносное ПО. Кроме того, существуют внутренние угрозы безопасности: выход из строя дисковых массивов, некорректный контроль среды, ошибки в балансировке нагрузки между отдельными вычислительными модулями/кластерами, нерациональное делегирование полномочий и распределение прав доступа.

Возникновение идеи виртуализации, как и её последующее воплощение, стало причиной переноса операционных систем и прикладного ПО на ВМ. Преимущества данного подхода самоочевидны: это и экономия аппаратных ресурсов (в рамках одной физической вычислительной системы располагается множество виртуальных), и упрощение управления (отсутствует

необходимость подключения к нескольким компьютерам), и повышение надёжности работы всего комплекса в целом (меньшее количество аппаратных реализаций снижает вероятность физического повреждения компонент). Однако обеспечение безопасности подобных систем требует специализированных подходов. Средства защиты, применяемые в рамках классических вычислительных сред, требуют их адаптации для использования в условиях виртуализации.

Для контроля состояния облачной среды требуется разработка модели управления рисками. Реализация аппаратной безопасности требует жесткого контроля доступа к вычислительным модулям (серверным устройствам). Данный аспект является весьма существенным из-за того, что в рамках внутренних ЦОДов доступ специалистов управления к серверам легко контролировать, в то время как при реализации облачного доступа большинство пользователей и администраторов работают с системами удалённо. В результате, одним из важнейших условий стабильности работы среды является разграничение прав и обеспечение прозрачности (незаметности применения средств контроля/защиты для внешних подключений).

Не менее важным аспектом представляется решение задачи избыточного копирования информации, динамического перераспределения вычислительных ресурсов с сохранением работоспособности - как отдельных виртуальных систем, так и всего комплекса в целом.

Среды виртуализации облачных сервисов используют то же системное и прикладное программное обеспечение, что и локальные системы. Соответственно, они имеют внутренние уязвимости, с помощью которых возможно инжектирование вредоносного ПО либо получение несанкционированного доступа к данным с последующим копированием/внесением деструктивных изменений. Система предотвращения вторжений позволяет снизить риск подобных событий. Для этого она должна быть сконфигурирована таким образом, чтобы обнаруживать вредоносную активность для каждой из эксплуатируемых в облачной среде ВМ.

Сетевая безопасность также является весьма существенным фактором. Классическое представление периметра сети, разделяющего внутренние и внешние сегменты, в облачных решениях размывается. В результате инфицирование либо несанкционированный доступ к одной из виртуальных машин может повлечь за собой повреждение других ВМ. Защита от данной угрозы может быть реализована установкой и конфигурированием межсетевого экрана, использующего систему фильтров, разграничивающих внутренние виртуальные вычислительные машины от взаимного влияния. Рационально использование модели разбиения на подсети с различными уровнями доверия и правами передачи межсетевых данных.

СПИСОК ЛИТЕРАТУРЫ

1. Богатырев В.А. Богатырев А.В. Модель резервированного обслуживания запросов реального времени в компьютерном кластере // Информационные технологии 2016. N5, Т 22. С. 348—355
2. Богатырев А.В., Богатырев В.А. Надёжность функционирования кластерных систем реального времени с фрагментацией и резервированным обслуживанием запросов // Информационные технологии - 2016. - Т. 22. - № 6. - С. 409-416
3. Верзун Н. А. Основы моделирования информационных систем множественного доступа : учеб. пособие / Н. А.Верзун, М. О. Колбанёв, И. Л. Коршунов, С. Ю. Микадзе. – СПб.: Изд-во СПбГЭУ. – 2015. – 138 с.
4. Татарникова Т.М. Защищенные корпоративные сети. Раздел: "Задачи по защите информации" / Т. М. Татарникова. – СПб: РГГМУ, 2012. – 113 с.
5. Емельянов А.А. Опыт реализации политики информационной безопасности на предприятии малого бизнеса в целях обеспечения информационно-экономической безопасности/А.А. Емельянов, И.Л. Коршунов//В сборнике «Информационная безопасность регионов России (ИБРР-2015). Материалы конференции. – 2015. – С. 213-214.
6. Татарникова Т.М. Технологии долговременного хранения данных/ Т.М. Татарникова, Е.Д. Пойманова //В сборнике: Наука и образование в XXI веке сборник научных трудов по материалам Международной научно-практической конференции: в 34 частях. – 2013. – С. 136-138.

УДК 004.7

МЕХАНИЗМЫ ПОВЫШЕНИЯ УРОВНЯ БЕЗОПАСНОСТИ ПРИ ПЕРЕДАЧЕ СЕТЕВЫХ ДАННЫХ

Емельянов Александр Александрович

Санкт-Петербургский государственный экономический университет,
информационных систем и технологий.

Россия, Санкт-Петербург, ул. Садовая, 21

emails: S1_Alex2000@mail.ru

Аннотация: Рассматриваются варианты потоковой криптографической защиты информации в сетевой инфраструктуре.

Ключевые слова: сетевые данные, защита, криптография.

SECURITY IN NETWORKS

Emelyanov Alexandr

Saint-Petersburg state university of economics,
191023, Russia, Saint-Petersburg, Sadovaya street, h.21
e-mails: S1_Alex2000@mail.ru

Abstract: Review of methods cryptographic protection in networks.

Keywords: network data, security, cryptography.

Введение. Применение сетей с механизмом пакетной передачи данных для реализации широкого класса задач – как для организаций, так и для частных лиц, в настоящее время является стандартом де-факто. Развитие инфокоммуникационных сервисов, воплощенных в проводных и беспроводных решениях, локальных и глобальных вычислительных сетях, позволяет использовать большое количество технологий, которые без данного подхода были бы труднореализуемы. Компьютерные сети интегрированы в процессы информационных взаимодействий настолько глубоко, что без них затруднительно представить существование любой современной области деятельности человека. Данное направление является одной из динамически развивающихся сфер внедрения научно-практических разработок [1], [2]. Однако, как и любая иная ИТ-область, сетевая передача данных несёт с собой множество угроз [3], [4]. Наиболее важной из них является перехват передаваемых данных, что может повлечь за собой финансовые, репутационные и иные потери.

Программно-аппаратные решения обеспечения безопасности передачи данных. С целью сведения к минимуму вероятности возникновения данного вида угроз применяются различные программно-аппаратные решения. Это VPN-туннелирование, внутренние протоколы передачи данных с потоковой шифрацией на основе технологии IPsec и т.д. Но большинство среднестатистических пользователей слабо представляют себе информационные угрозы и не обладают знаниями и умениями, необходимыми для применения вышеописанных механизмов, что зачастую приводит к ситуациям непреднамеренных утечек конфиденциальной информации. Одним из наиболее подверженных данной угрозе сервисов является интернет-серфинг, то есть работа с веб-контентом с применением различных программ-браузеров (Internet Explorer, Google Chrome, Mozilla Firefox и т.д.).

Для того, чтобы существенно повысить защищенность данного вида деятельности пользователей, можно применить многослойную поточную криптографическую защиту, реализуемую «прозрачно», то есть без каких-либо специализированных действий со стороны пользователя. Идея данной технологии базируется на принципе смешанных соединений Чаума: имеется многосвязный анизотропный граф, в узлах которого находятся прокси-серверы. В задачу последних входит передача пакетов данных с предварительной шифрацией уже имеющейся информации. При старте передачи выбирается произвольное число промежуточных узлов на основе генерации псевдослучайных последовательностей. Далее для каждого узла формируется индивидуальное сообщение, закрываемое симметричным ключом. Сам ключ генерируется с использованием открытого ключа каждого из промежуточных серверов. Так как маршрут выбирается произвольно, то весьма затруднительно осуществить точный перехват, и даже в случае успеха данного действия информация будет бессмысленна, так как она зашифрована несколькими последовательными «слоями». Каждый из промежуточных прокси-серверов (маршрутизаторов) работает лишь с одним слоем шифрования для того, чтобы извлечь трассировочные инструкции и перенаправить сообщение к другому серверу. Соответственно, промежуточные серверы не владеют информацией как о содержании сообщения, так и об изначальном источнике и конечной точке передачи [5,6].

В результате классический вариант сетевой атаки MITM (перехват/сниффинг через промежуточные узлы) становится неэффективным [7]. Кроме этого, возможно применение технологии, реализованной в проекте I2P: внутри многослойно зашифрованного сообщения производится инкапсуляция множества иных сформированных сообщений (транзитных), а также инструкций для их доставки. Кому принадлежит конкретное сообщение – знает только тот, кто создал всю структуру, и никто иной узнать эту информацию не может. Если один маршрутизатор согласовывает с другим участие в общем туннеле, то запрос помещается в пакет, зашифрованный открытым алгоритмом (в проекте I2P используется схема Эль-Гамала с 2048-битным ключом) и передаёт его через созданный туннель. При отправке пользователем сообщения в конечную точку, маршрутизатор отправителя закрывает данные сообщения вместе с другими в общий пакет, шифруя его открытым алгоритмом, и передает его через соответствующие туннели. Инструкции, присоединённые к каждому пакету внутри зашифрованного слоя, включают возможность запросить, чтобы сообщение было отправлено к конкретному маршрутизатору или туннелю. Инструкции содержат поля, с помощью которых промежуточный узел запрашивает задержку в определённый промежуток времени или согласует условия получения.

Описанный подход применим, когда требуется отправить зашифрованное сообщение через промежуточные узлы, у которых не должно быть доступа к этой информации.

Плюсом этого вида защиты является то, что для конечного пользователя взаимодействие с сетью Интернет будет осуществляться по классической схеме, то есть с использованием обычного браузера, в котором установлено соответствующее расширение/плагин. При этом все передаваемые и принимаемые данные будут надёжно защищены, что позволит повысить безопасность как с точки зрения частного лица, так и в рамках организации.

СПИСОК ЛИТЕРАТУРЫ

1. Коршунов И.Л. Состояние и концепция развития информационных технологий в сфере сервиса. Известия высших учебных заведений. Приборостроение. 2014. Т. 57. № 9. С. 7-10.
2. Кутузов О.И. Инфокоммуникационные сети. Моделирование и оценка вероятностно-временных характеристик. – СПб.: ГУАП, 2015. – 382 с.
3. Верзун Н. А. Аспекты безопасности информационно-экономической деятельности / Н. А. Верзун, М. О. Колбанев, Т. М. Татарникова // Технологии информационно-экономической безопасности: сб. статей сотр. каф. ИС и Т. – СПб.: Изд-во СПбГЭУ, 2016. – С.52–56.
4. Левкин И.М. Информационно-экономическая безопасность как специфический элемент экономической безопасности// Технологии информационно-экономической безопасности: сборник статей. – СПб.: Изд-во СПбГЭУ, 2016, с. 79-89.
5. Паршутин С.А, Богатырев В.А. Модели многопутевой отказоустойчивой маршрутизации при распределении запросов через сеть // Вестник компьютерных и информационных технологий -2015. - № 12. - С. 23-28
6. Коломойцев В.С., Богатырев В.А. Оценка эффективности и обоснование выбора структурной организации системы многоуровневого защищенного доступа к ресурсам внешней сети // Информация и космос -2015. - № 3. - С. 71-79
7. Левкин И.М. Модель обработки документальных источников деловой разведки// Известия вузов. Приборостроение. Выпуск № 9 / том 57 / 2014.

УДК 004.9

НЕКОТОРЫЕ АСПЕКТЫ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ КРИПТОВАЛЮТ

Кадырова Асия

Санкт-Петербургский государственный экономический университет, студент

191023, Россия, Санкт-Петербург, ул. Садовая, 21

emails: Asyi21071997@mail.ru

Аннотация: рассматриваются некоторые виды угроз и пути защиты от них при использовании криптовалют.

Ключевые слова: криптовалюта, защита.

SOME ASPECTS OF SECURITY AT USING CRYPTOCURRENCY

Kadyrova Assiya

Saint-Petersburg state university of economics, student

191023, Russia, Saint-Petersburg, Sadovaya street, h.21

emails: Asyi21071997@mail.ru

Abstract: review of some threats and ways to protect them while using cryptocurrency.

Keywords: cryptocurrency, security.

Введение. Криптовалюта является на данный момент активно развивающимся и исследуемым направлением в мире IT. Модель её реализации базируется на пиринговой распределенной сети, использующей криптографические средства в целях обеспечения безопасности. Суть концепции сводится к исключению доверенных центров: участники сети совершают сделки без посредников. Технология блокчейн применяется для регистрации всех операций с криптовалютой [1]. Представляет собой цепь связанных между собой блоков (несколько объединенных транзакций) с временной меткой. Результат достигается с помощью специальных вычислений (майнинга), за которые выплачивается вознаграждение. С целью получения прибыли злоумышленники через уязвимости ПК или установку вредоносного ПО используют вычислительные мощности компьютеров пользователей без согласия и вовлекают их в процесс майнинга. Этот тип программного обеспечения часто распространяется через спам-сообщения в социальных сетях; также существуют средства, использующие браузеры для несанкционированного доступа к ПК и запуска процесса майнинга. На сегодняшний день выявлены зараженные сети с тысячами компьютеров, использующихся для вышеописанной цели. Для повышения уровня безопасности рационально применение антивирусных программ, модулей для блокировки контента (AdBlock), отключение JavaScript в браузерах [2].

Пользователи, осуществляющие финансовые транзакции с применением криптовалют, подвергаются опасности деанонимизации через контакты с централизованными системами. Возможность выявить владельца возникает при покупке расчетных единиц (например, биткойнов) с помощью банковской карты по cookie-файлам или IP-адресам, то есть по вторичным данным.

Специальные протоколы не могут обеспечить полную защиту персональной информации. Наиболее уязвимым ресурсом являются онлайн-кошельки. При их использовании передаются данные и средства конкретной компании, что не соответствует концепции безопасности, регламентируемой в модели анонимных финансовых транзакций. Особенно остро данный вопрос стоит для предприятий, так как финансовая и организационная информация может оказаться у конкурентов.

Возможным выходом из ситуации является использование виртуальных машин и взаимодействие с внешними сетями передачи данных только через сконфигурированную систему TOR [3]. Существенно затруднят отслеживание связей отправителя и получателя специальные ресурсы-

миксеры, представляющие собой сервисы, анонимизирующие транзакции - но и они тоже имеют ряд недостатков, так как личная информация остается на промежуточных серверах.

Рассмотренные меры по защите позволят избежать многих угроз при использовании криптовалют. В данном обзоре не рассматриваются все вопросы безопасности, затрагиваются лишь наиболее распространенные.

СПИСОК ЛИТЕРАТУРЫ

1. Бескид П.П., Татарникова Т.М. О НЕКОТОРЫХ ПОДХОДАХ К РЕШЕНИЮ ПРОБЛЕМЫ АВТОРСКОГО ПРАВА В СЕТИ ИНТЕРНЕТ // Ученые записки Российского государственного гидрометеорологического университета. 2010. № 15. С. 199-210.
2. Татарникова Т.М. ЗАДАЧА СИНТЕЗА КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ГИС // Ученые записки Российского государственного гидрометеорологического университета. 2013. № 30. С. 204-211.
3. Емельянов А.А. Практическая реализация внутрикорпоративных политик безопасности на примере малого предприятия. // Региональная информатика и информационная безопасность: сб. трудов – СПб.: Изд-во Санкт-Петербургского общества информатики, вычислительной техники, систем связи и управления, 2015. С. 253-255

УДК 004.7.056.53

ОЦЕНКА И ПРОГНОЗИРОВАНИЕ РИСКОВ ДЛЯ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Капанов Алексей Александрович, Мещеряков Евгений Евгеньевич, Косолапов Владимир Викторович,
Астахова Татьяна Николаевна

Нижегородский государственный инженерно-экономический университет,
Россия, Нижегородская обл., г. Княгинино, ул. Октябрьская, 22а.

emails: alesnim@gmail.com, leonline5@mail.ru, vladimir.kosolapov@mail.ru, ctn_af@mail.ru

Аннотация: В статье рассмотрены ключевые проблемы обеспечения безопасности информационных систем на базе предприятия за счет применения методик оценки и прогнозирования возможных рисков воздействия внешних хакерских атак.

Ключевые слова: информационная система; риск; прогнозирование; оценка.

ESTIMATION AND FORECASTING OF RISKS FOR INFORMATION SECURITY SYSTEMS

Alexey Kapanov, Evgeny Meshcheryakov, Vladimir Kosolapov, Tatyana Astakhova
Nizhny Novgorod State University of Engineering and Economics,
Russia, Knyaginino, Oktyabrskaya Str., 22a.

emails: alesnim@gmail.com, leonline5@mail.ru, vladimir.kosolapov@mail.ru, ctn_af@mail.ru

Abstract: Key problems of ensuring the security of information systems on the basis of the enterprise due to application of techniques for assessing and predicting the possible risks of external hacker attacks are considered in the article.

Keywords: information system; risk; forecasting; assessment.

Введение. Развитие информационных технологий, средств и систем, их активное внедрение в жизнь общества ставит проблему обеспечения безопасности объектов информационно-телекоммуникационной инфраструктуры в разряд первоочередных.

Основной задачей системы обеспечения информационной безопасности является обеспечение функционирования объекта, исключая или предотвращая нарушения безопасности объекта, недопущение хищения материальных или денежных средств при помощи информационной системы, предотвращение противоправных деяний и обеспечение деятельности всех объектов, зависящих от информационной системы.

Важнейшей задачей для создания и проектирования систем информационной безопасности является задача прогнозирования рисков [1]. Основу риска образуют возможные уязвимости и угрозы для организации, поэтому выявление потенциальных или реально существующих рисков нарушения конфиденциальности и целостности информации, распространения вредоносного программного обеспечения и финансового мошенничества, классификация угроз информационной безопасности является первостепенной задачей информационной безопасности.

Оценку риска нужно проводить постоянно, проводя их переоценку. Для облегчения процессов дальнейшей переоценки рекомендуется встраивать оценку рисков в жизненный цикл информационной системы (далее – ИС) [2].

На примере нашего университета проведем оценку рисков информационной безопасности (ИБ) для данных используемых в процессе обучения студентов. В настоящий момент используются различные бумажные варианты прогнозирования и оценки угроз и рисков, в достоинство которых входит гибкость и адаптивность. Так же существуют программные комплексы, позволяющие проводить анализ рисков, но их функционал предполагает использование в достаточно крупных фирмах с уровнем ИБ выше среднего. Поэтому будет проведен теоретический анализ угроз ИБ без использования специального программного обеспечения [3].

Для оценки рисков выделим основные этапы жизненного цикла информационной системы:

- инициация, согласно различным процессам организации;
- установка;
- эксплуатация;
- выведение из эксплуатации.

Под ИС университета «НГИЭУ» понимается совокупность баз данных, программ обработки документации, физические машины и локальная сеть университета. Для такой обобщенной системы так же справедливы правила управления риском.

Обобщенный алгоритм управления риском для ИС:

1. Выявление потенциальных угроз. В данном случае сосредоточимся на риске утечки информации, взломе и выведение ИС из рабочего состояния.
2. Анализ потенциальных угроз. Размер статьи не позволяет приводить полный анализ угроз.
3. Создание системы безопасности. В качестве контрмер предполагаются стандартные действия по настройке и обновлению антивирусных программ и повышение компьютерной грамотности пользователей.
4. Обнаружение реальных угроз. Примером реальной угрозы рассмотрим выход из строя ПК в одной из лабораторий университета после заражения вирусом. В результате ПК вышел из строя и заразил сегмент сети крипто-вирусом.
5. Сдерживание реальных угроз. Были проведены мероприятия по сдерживанию вируса внутри сегмента сети при помощи изоляции сегмента на время проведения работ.
6. Ликвидация последствий угроз. Проведена проверка системы на наличие сигнатуры вируса на каждом ПК в сегменте и его удаление, а также мероприятия по предотвращению проникновения такого типа вирусов вновь в локальную сеть.

Все пункты алгоритма выполняются циклически на протяжении всего жизненного цикла ИС. С каждым циклом производится модификация системы ИБ для защиты от актуальных угроз.

Все этапы выполняются последовательно, позволяя охватить наиболее полно все виды угроз и степень их опасности для ИС. Используя различные методики оценки рисков, как одного из наиболее важных этапов, возможно радикально снизить уровень опасности угроз для ИС.

Заключение. Поскольку полное устранение рисков не представляется возможным, существуют методики уменьшения последствий атаки. В ходе устранения последствий и модификации системы безопасности ИС следует руководствоваться целесообразностью и достаточностью в ходе применения регуляторов безопасности.

Анализ рисков для ИС является важным элементом стратегии обеспечения устойчивого и бесперебойного функционирования системы.

СПИСОК ЛИТЕРАТУРЫ

1. Костогрызов Андрей Иванович, Лазарев Виктор Михайлович, Любимов Алексей Евгеньевич Прогнозирование рисков для обеспечения эффективности систем информационной безопасности в их жизненном цикле // Правовая информатика. 2013. №4. С.4-16
2. Риски информационной безопасности веб-приложений // habrahabr URL: <https://habrahabr.ru/company/pentestit/blog/279219/> (дата обращения: 05.09.17).
3. Оценка рисков ИБ, разработка моделей угроз // УЦСБ URL: <http://www.ussc.ru/catalog/id/39> (дата обращения: 05.09.17).. Ендовицкий Д.А., Бабушкин В.А., Батурина Н.А. Анализ инвестиционной привлекательности организации: научное издание / под ред. Д.А. Ендовицкого. – М.: КНОРУС, 2010, 376 с.

УДК 001.103.2

МЕТАДАННЫЕ В СИСТЕМАХ ДОЛГОВРЕМЕННОГО ХРАНЕНИЯ

Колбанёв Михаил Олегович¹, Пойманова Екатерина Дмитриевна², Татарникова Татьяна Михайловна¹

¹Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5,

²Санкт-Петербург, Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, 21,
emails: mokolbanev@mail.ru, e.d.poymanova@gmail.com, tm-tatarn@yandex.ru

Аннотация: Рассматривается процесс сохранения данных, стандарт описания метаданных Дублинское ядро, виды и примеры метаданных формируемых в ходе процесса сохранения, приводится классификация метаданных.

Ключевые слова: *долговременное хранение данных, процесс сохранения, метаданные.*

METADATA IN THE LONG-TERM STORAGE SYSTEMS

Kolbanev Mikhail¹, Poimanova Ekaterina², Tatarnikova Tatiana¹

¹The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,

²The St. Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str. 21,
emails: mokolbanev@mail.ru, e.d.poymanova@gmail.com, tm-tatarn@yandex.ru

Abstract: The report considers the process of data storage, metadata description standard Dublin Core, types and examples of metadata generated during the process of data storage and metadata classification.

Keywords: long-term data storage, the process of data storage, metadata.

Введение. Известно, что количество информации в мире растет высокими темпами, при этом подавляющая ее часть хранится в электронном виде. Этому способствует развитие инфокоммуникационных технологий, рост активности пользователей, принятие некоторых законодательных актов. Современные технологии позволяют сохранять цифровые данные на длительное время – до сотен и даже тысяч лет, а производители некоторых носителей говорят и о миллионах лет. Принципиальным отличием цифровых данных от аналоговых является невозможность их восприятия человеком без определенного преобразования. Также существенным отличием цифровых данных является необходимость хранения и обработки метаданных, содержащих информацию о формате, объеме и других характеристиках данных, записанных на цифровой носитель. Роль метаданных очень важна – помимо данных, необходимых для поиска информации, они позволяют осуществить преобразование цифровых данных в аналоговый вид, который человек может воспринимать органами чувств (зрением, слухом, осязанием), то есть происходит процесс преобразования данных в информацию. [1], [2], [3]

Метаданные можно разделить на два больших класса: организационные и специализированные.

Организационные метаданные – это информация о расположении данных в пространстве, времени, привязанность к пользователю, местоположение на носителе (координаты пространства внутри носителя) и позволяющая одним пользователям сохранить информацию, а другим найти ее и воспользоваться ею, даже если временной интервал между сохранением и необходимостью доступа к такой информации составляет несколько поколений. Организационные метаданные формируются в процессе сохранения информации, причем происходит процесс, аналогичный инкапсуляции – данные «обрастают» дополнительной информацией. [4], [5]

Специализированные метаданные – метаданные, с которыми работает файловая система, например, адрес сектора на магнитном диске.

Одним из стандартов метаданных является стандарт описания метаданных сетевых ресурсов Дублинское ядро (Dublin Core). Стандарт описывает два уровня элементов: простые и компетентные и содержит ряд уточнений, необходимых для обнаружения ресурсов. Подобный стандарт может применяться и в системах долговременного хранения данных, главной особенностью которых является обеспечение доступа к информации через 10, 50, 100 и более лет после сохранения. [4], [5]

В докладе рассматривается:

- процесс сохранения и его этапы;
- стандарт описания метаданных сетевых ресурсов Дублинское ядро (Dublin Core);
- примеры метаданных, формируемых в процессе сохранения

Предлагается классификация формируемых метаданных.

Заключение. Метаданные являются средством для преобразования цифровых данных в вид, понятный для человека. Они должны быть организованы таким образом, чтобы обеспечить возможность поиска и преобразования данных даже если между сохранением информации и необходимостью доступа к ней проходят десятки и сотни лет.

СПИСОК ЛИТЕРАТУРЫ

1. Кожанов Ю. Ф., Колбанёв М. О. Технология инфокоммуникации. – Курск: Науком, 2011. – 260 с.
2. Верзун Н. А., Касаткин В. В., Колбанёв М. О. Цифровые технологии: инфокоммуникации и экономика / Сборник: Информационные технологии цифровой экономики: сб. статей. – СПб.: Изд-во СПбГЭУ, 2017. – С.29–34.
3. Пойманова Е.Д. Современные технологии сохранения информации. – Информационная безопасность регионов России (ИБРР-2013). VIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23-25 октября 2013 г.: Материалы конференции / СПОИСУ. – СПб., 2013. – С.190-191
4. Татарникова Т.М., Пойманова Е.Д. Технологии долговременного хранения данных. – Наука и образование в XXI веке: сборник научных трудов по материалам Международной научно-практической конференции 30 сентября 2013 г.: в 34 частях. Часть 31: Мин-во обр. и науки РФ. Тамбов: Изд-во ТРОО «Бизнес-Наука-Общество», 2013. – С.136-137.
5. Пойманова Е.Д. Организация метаданных для безопасной системы длительного хранения. Информационная безопасность регионов России (ИБРР-2013). IX Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30 октября 2015 г.: Материалы конференции / СПОИСУ. – СПб., 2015. – С.224

УДК 004.056.5

ПОДУРОВЕНЬ БЕЗОПАСНОСТИ АРХИТЕКТУРНОЙ МОДЕЛИ СОХРАНЕНИЯ ДАННЫХ

Колбанёв Михаил Олегович¹, Ипатов Олег Сергеевич², Пойманова Екатерина Дмитриевна¹

¹ Санкт-Петербург, Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, 21,

² Санкт-Петербургский политехнический университет Петра Великого,
Россия, Санкт-Петербург, ул. Политехническая, 29,

emails: mokolbanev@mail.ru, ipatov_os@spbstu.ru, e.d.poymanova@gmail.com

Аннотация: Рассматриваются функции подуровня безопасности архитектурной модели процесса сохранения.

Ключевые слова: процесс сохранения, эталонная модель, архитектурная модель, интеллектуальные ресурсы, аутентификация, разграничение доступа.

SECURITY SUBLEVEL OF ARCHITECTURAL MODEL OF DATA STORAGE

Kolbanev Mikhail¹, Ipatov Oleg², Poimanova Ekaterina¹

¹ The St. Petersburg State University of Economics,

Russia, St. Petersburg, Sadovaya str. 21,

² Saint Petersburg Polytechnic University Peter the Great, Russia, St. Petersburg, Polytechnicheskaya str.29
emails: mokolbanev@mail.ru, ipatov_os@spbstu.ru, e.d.poymanova@gmail.com

Abstract: The dependences of the energy and time characteristics of the process of data storage are considered.

Keywords: data storage process, reference model, architectural model, intellectual resources, authentication, access control.

Введение. Для описания информационных процессов требуются архитектурные модели, устанавливающие взаимосвязь между компонентами рассматриваемого процесса. Наиболее известной эталонной моделью является модель OSI (Open Systems Interconnections), подробно описывающая семь уровней и стеки протоколов информационного процесса распространения данных. Французской ассоциацией пользователей UNIX (AFUU) совместно с Французской ассоциацией стандартизации (AFNOR) была разработана Модель интерактивного взаимодействия компонентов MIC (Model for Interactions between Components), объединяющая различные подходы к классификации компонентов среды. Модель MIC отчасти описывает и процесс сохранения информации, однако не учитывает ряд его особенностей, в том числе касающихся вопросов организации безопасности хранения. [1], [2], [3]

Процесс сохранения – это процесс обеспечения целостности и безопасности переноса данных во времени и доведение их до получателя в виде, позволяющем получателю преобразовать эти данные в информацию (сведения). Для реализации этого процесса необходимы затраты ресурсов:

- интеллектуальных, поддерживающих процессы мышления (модели информационного взаимодействия, которое в ходе предметной деятельности людей происходит в предметных областях и требует автоматизации);

- информационных, поддерживающих информационные процессы (любые алгоритмы и данные, созданные людьми, доступные в информационном пространстве и используемые для решения практических задач информационного взаимодействия в информационных областях);

- физических, поддерживающих физические процессы (совокупность физических объектов, позволяющая реализовывать информационное взаимодействие в физическом пространстве). [2]

Предлагается архитектурная модель, разработанная с учетом требуемых ресурсов и организационных, технических и технологических особенностей процесса сохранения. Модель содержит три уровня, связанные с требуемыми для информационного процесса сохранения ресурсами (интеллектуальный, информационный и физический). Каждый уровень разделен на подуровни, реализующие этапы процесса сохранения.

Рассматривается подуровень безопасности интеллектуального уровня данной модели. Рассматриваются процессы аутентификации и разграничения доступа в системах длительного хранения данных.

Заключение. Рассматриваемая архитектурная модель учитывает ряд особенностей процесса сохранения. Подуровень безопасности интеллектуального уровня модели учитывает данные особенности при организации хранения данных и разграничения прав доступа.

СПИСОК ЛИТЕРАТУРЫ

1. Пойманова Е.Д. Современные технологии сохранения информации. – Информационная безопасность регионов России (ИБРР-2013). VIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23-25 октября 2013 г.: Материалы конференции / СПОИСУ. – СПб., 2013. – С.190-191
2. Колбанёв М.О. Информационный объем базовых информационных процессов / Колбанёв М.О., Татарникова Т.М. // Информационно-управляющие системы. 2014. №4. С. 42-47.
3. Советов Б.Я., Колбанёв М.О., Татарникова Т.М. Технологии инфокоммуникации и их роль в обеспечении информационной безопасности//Геополитика и безопасность.– 2014.– №1(25).– С. 69-77.

УДК 004.056.2

ЭНЕРГЕТИЧЕСКИЕ АСПЕКТЫ БЕЗОПАСНОСТИ ДОЛГОВРЕМЕННОГО ХРАНЕНИЯ ДАННЫХКолбанёв Михаил Олегович¹, Касаткин Виктор Викторович², Пойманова Екатерина Дмитриевна¹¹ Санкт-Петербург, Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, 21,² Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия, 39,
emails: mokolbanev@mail.ru, v.v.kasatkin@iiias.spb.su, e.d.poymanova@gmail.com

Аннотация: Рассматриваются зависимости энергетических и временных характеристик процесса сохранения данных.

Ключевые слова: *долговременное хранение данных, процесс сохранения, энергия, энергетические характеристики, временные характеристики.*

ENERGY ASPECTS OF LONG-TERM DATA STORAGE SECURITYKolbanev Mikhail¹, Kasatkin Viktor², Poimanova Ekaterina¹¹ The St. Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya str. 21,² St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,
Russia, St. Petersburg, 14 Line, 39
emails: mokolbanev@mail.ru, v.v.kasatkin@iiias.spb.su, e.d.poymanova@gmail.com

Abstract: The dependences of the energy and time characteristics of the process of data storage are considered.

Keywords: *long-term data storage, the process of data storage, energy, energy characteristics, time characteristics.*

Введение. Необходимость долговременного хранения данных обусловлена различными причинами. На первом месте стоят требования законов Российской Федерации, в которых жестко закреплены сроки хранения документации в различных сферах деятельности. Далее идут социальные и политические причины: это и сохранение фонда знаний для передачи будущим поколениям, что в условиях террористической угрозы становится все более актуальным, и сохранение информации о достижениях в науке, а также сохранение корпоративной и личной информации пользователей. [1], [2]

Информационная безопасность, в том числе, предполагает обеспечение целостности данных, что для систем долговременного хранения является одной из важнейших задач. Процесс сохранения данных - это процесс обеспечения целостности и безопасности переноса данных во времени и доведение их до получателя в виде, позволяющем получателю преобразовать эти данные в информацию (сведения), а главной характеристикой процесса сохранения является время хранения данных на носителе [3], [4], [5]

На физическом уровне целостность данных обеспечивается устойчивостью минимальной единицы хранения (МЕХ) носителя. МЕХ – это физическая система, которая может находиться в одном или нескольких устойчивых состояниях, в зависимости от количества устойчивых состояний МЕХ может содержать разное количество бит данных. Каждая минимальная единица хранения имеет свой размер и способна оставаться в устойчивом состоянии определенное время. Свойства МЕХ задают следующие параметры физических ресурсов процесса сохранения:

- гарантированное время сохранения – время, в течение которого данные гарантированно сохраняются на носителе, физически эта характеристика зависит от времени, в течение которого минимальная единица хранения способна оставаться в устойчивом состоянии;
- плотность записи – количество бит данных, сохраненных на одной единице площади (объема) носителя, данная характеристика зависит от физического размера минимальной единицы хранения;
- энергопотребление при сохранении – это энергия, затрачиваемая на создание энергетического барьера, отделяющего одну минимальную единицу хранения от другой. [5], [6]

В докладе приводятся результаты расчетов зависимостей энергетических и временных характеристик процесса сохранения данных.

Закключение: расчеты показывают, что при увеличении энергии, затрачиваемой на создание энергетического барьера увеличивается время, в течение которого минимальная единица хранения способна оставаться в устойчивом состоянии, в то же время при увеличении «времени устойчивого состояния» уменьшается удельная энергия, затрачиваемая на сохранение одного бита данных. [6], [7], [8].

СПИСОК ЛИТЕРАТУРЫ

1. Пойманова Е.Д. Современные технологии сохранения информации. – Информационная безопасность регионов России (ИБРР-2013). VIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23-25 октября 2013 г.: Материалы конференции / СПОИСУ. – СПб., 2013. – С.190-191

2. Татарникова Т.М., Пойманова Е.Д. Технологии долговременного хранения данных. – Наука и образование в XXI веке: сборник научных трудов по материалам Международной научно-практической конференции 30 сентября 2013 г.: в 34 частях. Часть 31: Мин-во обр. и науки РФ. Тамбов: Изд-во ТРОО «Бизнес-Наука-Общество», 2013. – С.136-137.
3. Колбанёв М.О. Физические ресурсы информационного процесса сохранения данных / Колбанёв М.О., Пойманова Е.Д., Татарникова Т.М. // Известия высших учебных заведений. Приборостроение. 2014. Т. 57. № 9. С. 38-42.
4. Колбанёв М.О., Татарникова Т.М. Физические ресурсы информационных процессов и технологий // Научно-технический вестник информационных технологий, механики и оптики. Том 14, № 6. 2014, С. 113-123.
5. Колбанёв М.О. Физические ресурсы информационных систем хранения данных. / Колбанёв М.О., Пойманова Е.Д., Татарникова Т.М. // Материалы IX Санкт-Петербургской межрегиональной конференции "Информационная безопасность регионов России (ИБРР-2015)" С. 216-217.
6. Колбанёв М.О. Физические ресурсы информационных процессов и технологий / Колбанёв М.О., Татарникова Т.М. // Научно-технический вестник информационных технологий, механики и оптики Scientific and Technical Journal of Information Technologies, Mechanics and Optics 2014, № 6 (94) С. 113-122.
7. Е.З. Мейлихов. Максимальная плотность магнитной записи и распределение переключающих полей / Е.З. Мейлихов, Р.М. Фарзетдинова. // Физика твердого тела, 2014, том 56, вып. 12 С. 2326-2334.
8. Верзун Н.А. Энергетические характеристики процесса долговременного хранения данных / Верзун Н.А., Колбанёв М.О., Пойманова Е.Д. // Известия высших учебных заведений. Приборостроение. 2017. Т. 60. № 2. С. 158-164.

УДК 004

ОБ УЧАСТИИ ЭКОНОМИЧЕСКОГО УНИВЕРСИТЕТА В ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ДЛЯ ЦЕНТРОВ КОМПЕТЕНЦИЙ РЕГИОНОВ

Коршунов Игорь Львович, Левкин Игорь Михайлович, Микадзе Сергей Юрьевич
Санкт-Петербургский государственный экономический университет
Россия, Санкт-Петербург, ул.Садовая 21,
email: it107@mail.ru

Аннотация: Рассматривается возможность участия экономического университета в подготовке кадров для центров компетенции регионов и решении ряда научных задач их функционирования.

Ключевые слова: информационные технологии; инфокоммуникационная сеть; центр компетенции; подготовка IT-специалистов.

ABOUT THE PARTICIPATION OF THE ECONOMIC UNIVERSITY IN THE TRAINING OF SPECIALISTS FOR THE CENTERS OF THE COMPETITIONS OF THE REGIONS

Korshunov Igor, Levkin Igor, Mikadze Sergey
Saint-Petersburg State University of Economics
21, Sadovaya street, 191023 St. Petersburg Russian Federation,
email: it107@mail.ru

Abstract: The possibility of participation of an economic university in the training of personnel for the competence centers of the regions and the solution of a number of scientific problems of their functioning is considered.

Keywords: information technologies, infocommunication network, competence center, training of IT specialists.

Актуальная проблема – повышение эффективности государственного управления. Одним из направлений ее решения является создание системы распределенных ситуационных центров, центров компетенций регионов.

Для региональных центров компетенций нужны кадры и методики прогнозирования и стратегического планирования управления государственными программами и проектами. Для решения этих задач целесообразно использовать потенциал высших учебных заведений и, в частности, Санкт-Петербургского государственного экономического университета. Наличие в университете факультета экономики и факультета информатики и прикладной математики позволяет создать межфакультетский учебный ситуационный центр, в рамках которого можно решать ряд учебных и научных задач, стоящих перед центрами компетенций регионов. Основной целью этого центра может стать оценка текущей конкурентной обстановки в регионе в сфере информационных систем и технологий и прогнозирование ее развития в интересах бизнеса. Основными задачами центра могут быть:

- добывание (сбор) и обработка информации о хозяйствующих субъектах;
- оценка конкурентоспособности, сильных и слабых сторон отечественных и зарубежных информационных продуктов и услуг по запросу органов управления;
- моделирование и вскрытие конкурентных угроз предприятиям бизнеса;
- создание информационной базы по существующим и перспективным разработкам в сфере информационных систем и технологий, ведущим специалистам и системам их подготовки в регионе, России и за рубежом для нужд предприятий бизнеса;
- определение востребованности разрабатываемых информационных продуктов и услуг в различных сферах социально-экономической деятельности по запросам предприятий.

Решение указанных задач потребует привлечения профессорско-преподавательского состава университета, специалистов научно-исследовательских организаций и промышленных предприятий, специализирующихся в сфере разработки и применения инфокоммуникационных технологий. Предполагается привлечь к работе центра, в первую очередь, студентов направлений «Информационные системы и технологии» и «Бизнес-информатика». Включение в рабочий учебный план занятий, проводимых в учебном центре, позволит обеспечить формирование профессиональных компетенций, необходимых выпускникам направленности «Информационные технологии в деловой разведке» (для направления «Информационные системы и технологии») и «Деловая аналитика» (для направления «Бизнес-информатика»). В результате выпускники указанных направлений будут подготовлены к работе в центрах компетенций регионов.

В свою очередь, научный потенциал профессорско-преподавательского состава университета [1-3], а также базовых кафедр (в Санкт-Петербургском институте информатики и автоматизации Российской академии наук, в группе компаний «Омега» и др.) позволяет решать научные задачи по совершенствованию информационного обеспечения работы региональных органов государственной власти на основе центров компетенции, разработке моделей для прогнозирования и стратегического планирования для использования в центрах компетенции регионов и др.

Создание межфакультетского ситуационного учебного центра позволит университету внести свой вклад в становление и развитие региональных центров компетенции в виде подготовки специалистов для работы в центрах, а также научно-методического обеспечения их функционирования. Кроме того, проведение занятий со студентами в учебном центре повысит уровень практической подготовки выпускников.

СПИСОК ЛИТЕРАТУРЫ

1. Bogatyrev V. A. Functional Reliability of a Real-Time Redundant Computational Process in Cluster Architecture Systems / V. A. Bogatyrev, A. V. Bogatyrev // Automatic Control and Computer Sciences. – 2015, Vol. 49, No. 1. – pp. 46-56.
2. Советов Б. Я. Диалектика информационных процессов и технологий / Б. Я. Советов, М. О. Колбанёв, Т. М. Татарникова // Информация и Космос. 2014 г. – № 3. – С.98–106.
3. Соколов Р. В. Проектирование информационных систем / Р. В. Соколов. – СПб.: СПбГИЭУ, 2012. – 336 с.

УДК 004.7

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРИ ПЕРЕНОСЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ ПРЕДПРИЯТИЯ В ОБЛАЧНУЮ СТРУКТУРУ

Кузнецова Маргарита Александровна

Санкт-Петербургский государственный экономический университет, студентка кафедры
информационных систем и технологий.

191023, Россия, Санкт-Петербург, ул. Садовая, 21

emails: Kuznetsovamargarita2131@gmail.com

Аннотация: Рассматриваются аспект миграции ресурсов предприятия в облачную структуру и их защита.

Ключевые слова: облачные технологии, защита.

SECURITY OF THE ENTERPRISE IN CLOUD SYSTEM

Kuznetsova Margarita

Saint-Petersburg state university of economics, student.

191023, Russia, Saint-Petersburg, Sadovaya street, h.21

emails: Kuznetsovamargarita2131@gmail.com

Abstract: Review of security on migrating company resources to the cloud.

Keywords: cloud, protection.

Введение. В процессе бизнес-деятельности предприятие использует разные технологии, от выбора которых зависит достижение той или иной цели. В частности, применение инструментария ИТ влечёт за собой риски, связанные с безопасностью, которые есть как в традиционных решениях, так и в облачных [1].

В разрезе облачных технологий риски связаны по большей части с несанкционированным доступом к платформе провайдера облачных услуг. Опираясь на этот факт, разрабатываются модели угроз и комплекс мер, ведущий к снижению вероятности их появления [2]. Для этого проводятся переговоры между руководителем организации и специалистами поставщика услуг.

От чего будет зависеть безопасность при переносе ресурсов предприятия в облако?

Немаловажную роль играет выбор провайдера облачных технологий. Преимуществом является наличие надежных резервных каналов, четко обозначенный пакет услуг, способность облачной инфраструктуры к быстрой масштабируемости, удобный для пользователей интерфейс, который сократит временные затраты на адаптацию.

На протяжении всего периода сотрудничества с провайдером следует подсчитывать ресурсы, тщательно изучать соглашение о предоставляемых компании услугах, планировать периоды пиковой нагрузки.

Следует представлять, что уровень безопасности формируют оба субъекта, вступающие в сотрудничество. Если это SaaS – максимальный контроль сосредоточен у провайдера, IaaS – контроль за безопасностью находится у клиента.

Продукты на рынке информационной безопасности можно разделить по бизнес-целям: продукты по защите виртуальной инфраструктуры, продукты по защите пользовательских данных для конкретных облачных инфраструктур-провайдеров, универсальные продукты по защите пользовательских данных [3].

Опираясь на вышесказанное, можно выделить 4 стратегии, которые обеспечивают безопасность бизнес-решениям различного масштаба и требований к конфиденциальности: "минимум ошибок", "минимальные усилия", "точечное внимание", "многослойная оборона".

Каждая из стратегий имеет свои преимущества и недостатки, которые необходимо учитывать при выборе способов переноса ресурсов предприятия в облачную инфраструктуру.

СПИСОК ЛИТЕРАТУРЫ

1. Татарникова Т.М. ЗАЩИЩЕННЫЕ КОРПОРАТИВНЫЕ СЕТИ. РАЗДЕЛ: "ЗАДАЧИ ПО ЗАЩИТЕ ИНФОРМАЦИИ" СПб: РГГМУ, 113 с.
2. Татарникова Т.М., Яготинцева Н.В. ЗАДАЧА СИНТЕЗА СИСТЕМЫ ЗАЩИТЫ КОРПОРАТИВНОЙ ИНФОРМАЦИИ: ПОСТАНОВКА И ЭТАПЫ РЕШЕНИЯ. В сборнике: Наука и образование в XXI веке сборник научных трудов по материалам Международной научно-практической конференции: в 34 частях. 2013. С. 135-136.
3. Емельянов А.А. Оценка затрат на системы информационно-экономической безопасности / А.А.Емельянов, И.Л.Коршунов // Технологии информационно-экономической безопасности: сб. статей сотр. каф. ИС и Т. – СПб.: Изд-во СПбГЭУ, 2016. – С.63–69.

УДК 004.056.5

ОСНОВНЫЕ ВИДЫ НАРУШИТЕЛЕЙ, СПОСОБНЫЕ ВЕСТИ КОНКУРЕНТНУЮ РАЗВЕДКУ ИЛИ ОКАЗАТЬ ВОЗДЕЙСТВИЯ НА ИНФОРМАЦИЮ

Кулишкин Виталий Александрович, Чуйков Игорь Олегович

Петербургский государственный университет путей сообщения Императора Александра I,
Россия, Санкт-Петербург, пр-кт. Московский, 9,
emails: vkulishkin@mail.ru, Igor1990rus46@ya.ru

Аннотация: В статье рассмотрены понятия конкурентной разведки и интеллектуальной собственности. Приводится перечень нарушителей, которые способны вести конкурентную разведку либо оказывать воздействие на информацию. Приводится графическая шкала вероятностей реализации атаки или нарушений свойств информации для каждого нарушителя.

Ключевые слова: конкурентная разведка; интеллектуальная собственность; нарушители безопасности информации.

THE MAIN TYPES OF INTRUDERS WHO ARE ABLE TO CARRY OUT COMPETITIVE INTELLIGENCE AND HAVE IMPACTS ON THE INFORMATION

Kulishkin Vitaliy, Chuikov Igor

Emperor Alexander I st. Petersburg state transport university
Russia, St. Petersburg, Moskovsky Str. 9,
emails: vkulishkin@mail.ru, Igor1990rus46@ya.ru

Abstract: The definitions of competitive intelligence and intellectual property are considered in the article. The list of the main types of Intruders who are able to carry out competitive intelligence and have impacts on the information is given. A graphical scale of probabilities for the implementation attack or impacts on the information properties for each intruders is given.

Keywords: competitive intelligence; intellectual property; intruders of information security.

Введение. Глобальная информатизация общества вкупе с повсеместным подключением устройств к сети открывают новые угрозы и вызовы для всех секторов промышленности. Жесткая конкурентная борьба за право быть лидером своего сегмента ведется всеми игроками рынка. На заре возникновения делового бизнеса несанкционированный сбор информации стал ничем иным, как первыми шагами промышленного шпионажа, послужившими появлению конкурентной разведки.

Конкурентная разведка (КР) – это сбор и обработка данных из разных источников, для выработки управленческих решений с целью повышения конкурентоспособности коммерческих организаций, проводимые в рамках закона и с соблюдением этических норм, а также структурными подразделениями. Вне зависимости от целей КР и действий нарушителей, объектом атак всегда будет информация, будь она открытая или закрытая. Пожалуй, основным видом информации, на которую постоянно направлена КР, является интеллектуальная собственность.

Основными источниками угроз для любой информации являются действия человека. В таблице 1 представлены основные виды нарушителей, которые способны вести КР, осуществлять методы несанкционированного получения информации, вступать в сговор друг с другом или по вине которых может произойти утечка информации.

Для понимания степени опасности перечисленных нарушителей, на рисунке 1 приводится графическая шкала с вероятностями успешной реализации атаки или оказания воздействия на свойства информации. Эти показатели вероятностей устанавливаются экспертным методом на основе возможностей, навыков и потенциала нарушителей и являются базовыми. Результатом такого метода является «чистый» показатель воздействия на информацию, определяемый организацией, который необходимо понижать применением мер защиты информации.

Заключение: Рассмотрены группы нарушителей, которые способны вести конкурентную разведку и оказать воздействия на информацию.

СПИСОК ЛИТЕРАТУРЫ

1. Гражданский кодекс Российской Федерации [Электронный ресурс]: Федеральный закон от 30.11.94 № 51 (ред. от 28.03.17) - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_5142.
2. О некоторых вопросах, возникших в связи с введением в действие части четвертой Гражданского кодекса Российской Федерации [Электронный ресурс]: Постановление Пленума Верховного Суда РФ от 26.03.2009 № 5, Пленума ВАС РФ от 26.03.2009 № 29 - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_86879/
3. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством РФ требований к защите персональных данных для каждого из уровней защищенности от 18.08.2014 №33620 [Электронный ресурс]: приказ ФСБ России от 10.07.2014 № 378 – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_167862/
4. Методика определения угроз безопасности информации в информационных системах [Электронный ресурс]: проект методического документа ФСТЭК России от апреля 2015 г. – Режим доступа: <http://fstec.ru/component/attachments/download/812>
5. Конкурентная разведка [Электронный ресурс] – Режим доступа: <https://ru.wikipedia.org/>

УДК 621.396.

ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКИЕ УГРОЗЫ В ЦИФРОВОЙ ЭКОНОМИКЕ

Левкин Игорь Михайлович, Левкина Светлана Вячеславовна
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский пр., 49,
ООО «Витамед» (Санкт-Петербург),
Россия, Санкт-Петербург, Ул. Льва Толстого, 5А,
email: vitamed2010@yandex.ru, lev.kin@yandex.ru

Аннотация: В статье отмечен рост значимости информационно-экономических угроз в цифровой экономике, приведены их особенности и проблемы, которые возникнут при реализации этих угроз в условиях роста цифровизации общества.

Ключевые слова: цифровизация, информационно-экономические угрозы, особенности реализации.

INFORMATION AND ECONOMIC THREATS IN THE DIGITAL ECONOMY

Levkin Igor Mikhailovich, Levkin Svetlana Vyacheslavovna
Saint-Petersburg National research University of information technologies, mechanics and optics,
Russia, Saint-Petersburg, Kronverkskiy prospect, 49,
ООО "Vitamed" (St.-Petersburg),
Russia, Saint-Petersburg, Ul. Lva Tolstogo, 5A,
email: vitamed2010@yandex.ru, lev.kin@yandex.ru

Abstract: the article noted the growing importance of information and economic threats in the digital economy, given their characteristics and the problems that arise when these threats in terms of growth of digitalization of society.

Keywords: digitalization, information and economic threats, especially the implementation.

Введение. Стремительная цифровизация информационного пространства привела к появлению нового уклада хозяйственной деятельности – цифровой экономике, ключевым фактором производства в которой являются данные в цифровой форме, способствующие формированию информационного пространства с учетом потребностей граждан и общества в получении качественных и достоверных сведений, развитию информационной инфраструктуры Российской Федерации, созданию и применению российских информационно-телекоммуникационных технологий, а также формированию новой технологической основы для социальной и экономической сферы [1]. Это изменило

конфигурацию угроз экономической деятельности, сместив акценты в сторону возрастания значимости угроз информационно-экономического характера.

Сущность информационно-экономических угроз заключается в использовании информации циркулирующей или создаваемой на объекте микро (личность, хозяйствующий субъект), мезо (регион, отрасль, социальная группа) и макро (страна, группа стран) уровня или вокруг него для нанесения экономического ущерба этому объекту [2].

К числу типовых информационно-экономических угроз обычно относят: хищение информационных продуктов как экономической субстанции, добывание информации для формирования и реализации экономических угроз, модификации информации, вывод из строя элементов информационной инфраструктуры, ограничение доступа к информационным ресурсам и технологиям, информационно-психологическое воздействие на руководящий состав и коллектив хозяйствующего субъекта. Важными особенностями этих угроз в условиях цифровой экономики являются: приобретение отдельными информационно-экономическими угрозами глобального характера, например, в середине мая 2017 года по всему миру прошла волна заражений шифровальщиком WannaCry. Вирус заражал компьютеры, не установившие обновление операционной системы Windows. В ходе хакерской атаки WannaCry поразило до 300 000 компьютеров более чем в 70 странах мира и зашифровало информацию на них, сделав ее недоступной для использования [3]; появление новых форм информационно-экономического воздействия на большие информационные системы, в частности на государственные информационные системы (ГИС). Так как эти системы являются сложными по структуре, пространственно-распределенными и содержат различные виды информации (текстовую, иконо-графическую, табличную и т.п.) для нанесения им существенного экономического ущерба, потребуются согласованные во времени и пространстве действия по формированию и реализации информационных угроз в отношении как отдельных элементов информационной инфраструктуры ГИС, так и в отношении всей ГИС целиком; повышение напряженности конкурентной обстановки в информационной сфере, рост частоты использования методов недобросовестной конкуренции (например, американские власти в июле 2017 года предписали государственным департаментам и агентствам в течение трех месяцев удалить с компьютеров и серверов программное обеспечение «Лаборатории Касперского» [4]); рост числа «несистемных» информационно-экономических угроз, связанных с желанием отдельных хорошо подготовленных в информационном отношении индивидуумов потренироваться в вопросах создания вредоносных компьютерных программ, несанкционированного доступа к информационным ресурсам случайно выбранных хозяйствующих субъектов, воздействия на эмоционально-психологическое состояние отдельных социальных групп населения (например, школьников) и т.п.; стремительный рост информационного шума, способного, с одной стороны, существенно осложнить выбор оптимальных для потребителя информационных продуктов и услуг, с другой стороны, широко внедрить неэффективные (не достаточно убедительные) информационные технологии (например, неоднозначно воспринимаемую криптовалюту); другие.

Реализация большинства из информационно-экономических угроз в условиях дальнейшей цифровизации общества способна привести к серьезным проблемам, связанным с уменьшением доверия граждан к цифровой среде; наращиванием возможностей внешнего информационно-технического воздействия на информационную инфраструктуру хозяйствующих субъектов; ростом масштабов компьютерной преступности, в том числе международной; отставанием от ведущих иностранных государств в развитии конкурентоспособных информационных технологий; зависимостью социально-экономического развития от экспортной политики иностранных государств; утечкой умов из информационной сферы и других.

Закключение. Учет рассмотренных особенностей информационно-экономических угроз цифровой экономике потребует разработки и внедрения новых подходов к организации защиты информации в хозяйствующих субъектах всех масштабов, особенно мезо и макроуровня.

СПИСОК ЛИТЕРАТУРЫ

1. Программа "цифровая экономика Российской Федерации" [Электронный ресурс]. - Режим доступа: <http://legalacts.ru/doc/rasporjazhenie-pravitelstva-rf-ot-28072017-n-1632-r-ob-utverzhdenii/> (дата обращения 26.08.2017).
2. Технологические аспекты информационно-экономической безопасности / В.В. Касаткин, А.М. Колбанёв, И.Л. Коршунов, И.М. Левкин, С.Ю. Микадзе. – СПб.: Изд-во СПбГЭУ, 2016. – 193 с.
3. Новый компьютерный вирус поразило информационные системы тысяч компаний по всему миру [Электронный ресурс]. - Режим доступа: <http://www.banki.ru/news/bankpress/?id=9834619> (дата обращения 20.09.2017).
4. США против Касперского: госучреждениям дали три месяца на удаление ПО российской компании [Электронный ресурс]. - Режим доступа: <http://www.forbes.ru/tehnologii/350221-ssha-protiv-kasperskogo-gosuchrezhdeniyam-dali-tri-mesyaca-na-udalenie-po> (дата обращения 20.09.2017).

УДК 004.415.2:33(075.8)

**ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ ПРОЕКТИРОВАНИЯ
ИНФОРМАЦИОННЫХ СИСТЕМ**

Лобанов Вячеслав Игоревич, Соколов Роман Владимирович
Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, 21
emails: imlobanov@yandex.ru, rsok7@rambler.ru

Аннотация: В статье рассмотрены стохастическая модель формирования и планирования выполнения портфеля проектов, идентифицированы возможные риски и предложены методы повышения информационно-экономической безопасности.

Ключевые слова: *стохастическое моделирование; факторы риска; проектирование информационных систем; повышение информационно-экономической безопасности.*

INFORMATION AND ECONOMIC SECURITY OF INFORMATION SYSTEMS DESIGN

Lobanov Viacheslav, Sokolov Roman
The St. Petersburg State University of Economics,
Russia, St. Petersburg, Sadovaya st., 21
emails: imlobanov@yandex.ru, rsok7@rambler.ru

Abstract: The article provides a stochastic model for the formation and planning of the portfolio of projects, identifies possible risks and suggests methods to improve information and economic security.

Keywords: *stochastic modeling; risk factors; design of information systems; increase of information and economic security.*

Введение. Оценка информационно-экономической безопасности проектной деятельности предприятий информатизации может быть сделана на основе модели формирования и планирования выполнения портфеля проектов информационных систем.

Исходя из ранее представленной детерминированной модели планирования [1] можно построить стохастическую модель, характеризующейся следующей структурой. В качестве целевой функции используется максимизация вероятности превышения чистой приведенной совокупной стоимости работ, входящих в портфель по отношению к заданной величине. В качестве ограничений модели используются:

- вероятности соблюдения заданного уровня сальдо накопленных денежных средств по подпериодам планирования;
- вероятности соблюдения балансировки по ресурсным ограничениям;
- вероятности соблюдения регламентированных сроков окончания проектов.

В модели используются двоичные переменные, характеризующие подпериоды начала выполнения работы по каждому проекту.

Типы рисков:

- отклонение планируемого общего финансового результата в меньшую сторону;
- потеря эффективности отдельно взятого бизнес-процесса, соответствующего заказанному проекту;
- потеря требуемой абсолютной ликвидности предприятия информатизации, т.е. сокращение сальдо накопленных денежных средств на расчетном счете ниже заданного значения;
- превышение суммарной допустимой трудоемкости по видам работ при выполнении комплекса бизнес-процессов в планируемом периоде;
- нарушение договорных сроков выполнения бизнес-процессов, соответствующих заказанным проектам.

Заключение. Для повышения информационно-экономической безопасности проектирования информационных систем рекомендуется:

- совершенствование нормативной базы. Увеличение стоимости выполнения комплекса работ;
 - совершенствование нормативной базы. Сбор статистики, характеризующей нарушения показателей выполнения плана;
 - совершенствование нормативной базы. Увеличение стоимости выполнения комплекса работ.
- Утверждение графика платежей заказчика, использование предоплаты;
- совершенствование нормативной базы. Увеличение по сравнению с расчетными сроков выполнения бизнес-процессов, соответствующих заказам клиентов.

СПИСОК ЛИТЕРАТУРЫ

1. Соколов Р.В., Лобанов В.И. Планирование портфеля заказов предприятия информатизации на основе процессного подхода. Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Экономические науки №3 (221), 2015.

УДК 004.056

ТРЕБОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАЗРАБОТКЕ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

Маслов Никита Сергеевич, Астахова Татьяна Николаевна
Нижегородский государственный инженерно-экономический университет,
Россия, Княгинино, ул. Октябрьская, 22а
emails: j-knaginino@yandex.ru, ctn_af@mail.ru

Аннотация: В статье сформулированы требования информационной безопасности, которые необходимо использовать в рамках выполнения выпускной квалификационной работы. Представлен обзор существующих уровней безопасности, а также варианты оценки информационной безопасности.

Ключевые слова: *информационная безопасность; требования информационной безопасности; выпускная квалификационная работа; стандарты информационной безопасности.*

INFORMATION SAFETY REQUIREMENTS FOR THE DEVELOPMENT OF GRADUATION WORK

Maslov Nikita, Astakhova Tatyana
Nizhniy Novgorod State University of Engineering and Economic,
Russia, Knyaginino, Oktyabrskaya str. 22 a,
emails: j-knaginino@yandex.ru, ctn_af@mail.ru

Abstract: The information security requirements that must be used in the implementation of the final graduation work are presented in the article. An overview of existing security levels is presented, as well as options for assessing information security.

Keywords: *information security; requirements of informational security; graduation work; information security standard.*

Введение. Каждый год студенты многих технических вузов, проходящих подготовку по направлениям укрупненной группы 09.00.00, создают информационные системы (ИС) в рамках выпускной квалификационной работы (ВКР) [1], [2]. Чем сложнее задача автоматизации и чем важнее предметная область, в которой используются разработанные программные продукты, тем острее встает вопрос обеспечения безопасности информационной системы. Поэтому, реализация информационной безопасности системы – это необходимость, которую необходимо осуществить и описать в одной из глав ВКР.

Под безопасностью ИС будем понимать такое состояние информационной системы, при котором [3, с. 1]:

- ИС способна работать безотказно, сопротивляться условиям разрушающего характера как внешних, так и внутренних информационных угроз. Примером таких угроз служат попытки вмешательства в процесс функционирования системы и не важно, будет эта попытка случайна или преднамеренна. Возможны попытки кражи или получения информации без соответствующего разрешения, возможность физического воздействия на ее элементы [3, с. 1];

- ИС, содержащая в себе аппаратно-программное обеспечение надлежащего уровня, должна обеспечивать обработку информации разного уровня секретности различными пользователями или группами пользователей, которые имеют соответствующие права доступа, не нарушающие целостности и конфиденциальности данных и информации. А её работа не создаёт угроз для элементов самой системы и внешней среды [3, с. 2];

Чтобы сформировать и достигнуть необходимого уровня безопасности, необходимо выдвинуть ряд основных требований к разрабатываемому программному продукту, которые студент должен выполнить:

- изучить стандарты информационной безопасности, направленные на защиту ИС;
- определить объект защиты, и установить категорию защиты;
- описать процесс обеспечения информационной безопасности ИС, учитывая:
- программно-технический уровень, описывающий механизмы безопасности, которые необходимы для эффективной работоспособности ИС. Главными механизмами являются процедуры идентификации и аутентификации. Так же не стоит забывать о таких механизмах как протоколирование и аудит, криптография, управление доступом, уровень доступности;
- процедурный уровень – меры безопасности, нацеленные на защиту ИС от воздействия "человеческого фактора". Чтобы сформировать этот уровень используют меры: управление персоналом, физическая защита, поддержание работоспособности, реагирование на нарушения режима безопасности, планирование восстановительных работ;
- административный уровень – это разработанная стратегия руководства организации, обеспечивающая защиту информации. Чаще всего это действия, направленные на организацию и контроль работы по обеспечению информационной безопасности.

- реализовать информационную безопасность в своей ИС, основываясь на требованиях, сформулированных в предыдущих пунктах;

- произвести тестирование и отладку ИС. Для этого нужно использовать два вида тестирования:
- функциональное, при таком виде тестирования, программный код закрыт, проверяется только соответствие действий функций ИС с ее спецификацией;
- структурное, при котором происходит проверка логики программы, и ее код открыт.
- произвести оценку безопасности разработанной ИС. Для этого необходимо определить, по каким критериям будет происходить оценка информационной безопасности. Для этого можно использовать один из вариантов оценки:
- оценка по экономическим показателям, характеризуется соотношением затрат на информационную безопасность и результатами, полученными в итоге;
- оценка по эталону – сравнительный анализ деятельности организации по обеспечению информационной безопасности с выбранным эталоном;
- риск-ориентированная оценка – способность организации достигать своих целей за счет эффективного управления рисками информационной безопасности. Для этого организация анализирует свои риски и сопоставляет риски с принимаемыми мерами по их обработке;
- сформировать главу ВКР, в которой будут изложены и представлены полученные результаты, способ реализации информационной безопасности организации и системы на всех уровнях.

Заключение. В рамках данной работы были сформулированы требования, которые необходимо учитывать при разработке ВКР. Студенту следует изучить стандарты информационной безопасности, определить объект защиты. А также установить категории защищаемой информации. Также необходимо описать процесс обеспечения информационной безопасности ИС, которая имеет несколько уровней. Произвести тестирование и отладку ИС и оценить информационную безопасность разработанной системы.

СПИСОК ЛИТЕРАТУРЫ

1. Необходимость обеспечения информационной безопасности ИС и ИТ // docplayer URL: <http://docplayer.ru/43933419-Neobhodimost-obespecheniya-informacionnoy-bezopasnosti-is-i-it.html> (дата обращения: 18.09.2017).
2. Внуков, А. А. Защита информации: учебное пособие для бакалавриата и магистратуры / А. А. Внуков. – 2-е изд., испр. и доп. – М.: Издательство Юрайт, 2017. – 261 с.
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забаурин. – М.: Издательство Юрайт, 2017. – 312 с.

УДК 004.5, 338.14

ИРРАЦИОНАЛЬНОЕ ВЛИЯНИЕ ИНФОРМАЦИОННЫХ ПОТОКОВ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ В ЦИФРОВОЙ ЭКОНОМИКЕ

Минаков Владимир Федорович, Лобанов Олег Сергеевич, Сотавов Абакар Капланович
Санкт-Петербургский государственный экономический университет, Россия, Санкт-Петербург,
Садовая ул., 21,
emails: m-m-m-m-m@mail.ru, sotavov@gmail.com, thelobanoff@gmail.com

Аннотация. Рассмотрены новые виды угроз и опасностей цифровой экономики, связанные с влиянием информационных потоков в современных инфокоммуникационных системах на поведение стейкхолдеров. Показано влияние таких угроз на деятельность кредитных организаций.

Ключевые слова. Цифровая экономика; информация; информационное воздействие; угрозы; поведение.

IRRATIONAL INFLUENCE OF INFORMATION FLOWS ON THE ECONOMIC SAFETY IN DIGITAL ECONOMY

Minakov Vladimir, Lobanov Oleg, Sotavov Abakar
Saint-Petersburg State University of Economics, Russia, St. Petersburg, Sadovaya str., 21,
emails: m-m-m-m-m@mail.ru, sotavov@gmail.com, thelobanoff@gmail.com

Abstract. Digital economy connected to influence of information flows in the modern infocommunication systems on behavior of stakeholders are considered. Influence of such threats on activities of credit institutions is shown.

Keywords: digital economy; information; information influence; threats; behavior.

Введение. Современная инфраструктура экономики создала условия для реализации бизнес-процессов с широкой поддержкой информационными потоками на базе информационно-телекоммуникационных систем и технологий, средств автоматизации. Одновременно с тем, инфраструктура информационного общества позволяет каждому члену общества открыто излагать свое мнение, а широким слоям населения, иметь доступ к ней [1]. На этой основе формируется отношение граждан к явлениям и социально-экономическим процессам, а соответственно, их поведение на рынках в качестве стейкхолдеров.

Рациональное и иррациональное информационное влияние. Для экономических процессов общественное мнение важно в части формирования лояльности и приверженности клиентов компаний.

Рассмотрим влияние информационных потоков в цифровой инфраструктуре на настроения клиентов, и под их воздействием – на экономическую безопасность банков.

Для банковской сферы деятельности критически важное значение имеет доверие клиентов. Традиционно оно базировалось на количественных показателях деятельности кредитных организаций: ликвидности, собственном капитале, заемном капитале, объеме привлеченных средств, наличии и размерах «плохих» активов, учете сумм и сроков невозврата выданных кредитов. Однако, несмотря на высокие показатели кредитных организаций первой и второй десятки в рейтингах РФ, в 2017 г. ряд из них начали испытывать трудности, а затем – стремительный отток привлеченных финансовых ресурсов. К настоящему времени это привело к санации. Очевидно, что более существенное влияние оказали не традиционные факторы банковской деятельности, а новые факторы, пришедшие вместе с цифровой экономикой и ее инструментальными средствами [2]. Это факторы информационного влияния на экономическую безопасность.

Исследуя указанное явление, важно отметить, что в 2013 году Нобелевская премия по экономике была присуждена за эмпирический анализ цен активов (ученым: Фаме, Шиллеру, Хансену). Классическая часть анализа (теория эффективных рынков) описывает цены активов как зависящие исключительно от исчерпывающей информации, доступной все участникам рынка, которая обеспечивает сбалансированные уровни цен на основе интересов стейкхолдеров. Дополнения к теории, основанные на эмпирических данных XXI века, позволили открыть феномен «надувания» пузырей цен активов, в первую очередь, на рынках акций.

На наш взгляд, можно констатировать факт информационного влияния на иррациональное поведение участников рынка. Очевидно, что такое поведение противоречит экономическим интересам. И действительно, сдувание многочисленных «пузырей», особенно на рынке акций доткомов (когда в 2000 году индекс NASDAQ, достигший порога 5132 п., за одни торги испытал падение более чем в полтора раза), привело к беспрецедентным убыткам компаний, а стоимость высокотехнологичных компаний упала на пять триллионов долларов США).

Аналогично в банковском секторе РФ сложилась ситуация с иррациональным информационным влиянием мнения одного из аналитиков о появлении проблем в крупных банках (Югра, Открытие, Бинбанк). В результате такого влияния и произошло снижение доверия клиентов к кредитным организациям, отток денежных средств и переход через пороговые значения показателей экономической безопасности (капитализации), что и стало для Банка России основанием для их санации.

Если учесть, что за последние три года лицензии отозваны у 279 банков, в результате чего агентством по страхованию вкладов (АСВ) затрачено свыше одного триллиона рублей на выплаты вкладчикам банков. Это повлияло на экономическую безопасность самой государственной корпорации АСВ. Она вынуждена прибегнуть к займам для обеспечения экономической устойчивости. Это привело к снижению эффективности собственной деятельности. Отсюда можно сделать вывод, что в цифровой экономике, одним из признаков которой как раз и является перевод информации (данных, сведений) в категорию ключевого фактора экономической деятельности, становится критически важным переход к управлению информационными потоками [3] так, чтобы обеспечить блокирование ее деструктивного влияния на поведение участников бизнес-процессов. На практике так поступил банк «Тинькофф Кредитные Системы». Такое управление позволит исключить иррациональные и неэффективные по экономическим показателям решения и действия стейкхолдеров. Действительно, перевод деструктивного информационного потока в правовое поле и открытое информационное пространство привело к повышению котировок его акций менее, чем за два месяца почти в полтора раза.

Заключение. Таким образом, анализ фактов информационного воздействия на поведение клиентов кредитных организаций, а также фактов образования «пузырей» цен активов на мировых рынках позволяют установить, что информационно-экономическая безопасность в банковской системе существенно зависит от информационных потоков. Наряду с позитивным, например, маркетинговым влиянием, возрастает число прецедентов деструктивного воздействия. Степень такого влияния составляет триллионы рублей на Российском рынке и триллионы долларов США на мировых рынках. Следовательно, особую актуальность приобретает управление потоками информации, формирующей гуманитарные императивы субъектов экономики, предопределяющие их поведение в цифровой экономике. В таком управлении решающую роль играет программное обеспечение идентификации и локализации влияния потоков ложной и деструктивной информации.

СПИСОК ЛИТЕРАТУРЫ

1. Майданович О.В., Охтилев М.Ю., Куссуль Н.Н., Соколов Б.В., Цивирко Е.Г., Юсупов Р.М. Междисциплинарный подход к оцениванию и анализу эффективности информационных технологий и систем // Известия высших учебных заведений. Приборостроение. – 2010. – Т. 53. – № 11. – С. 7-16.
2. Осипов В.Ю., Воробьев В.И., Левоневский Д.К. Проблемы защиты от ложной информации в компьютерных сетях // Труды СПИИРАН. – 2017. – № 4 (53). – С. 97-117.
3. Юсупов Р.М., Соколов Б.В. Методологические и методические основы оценивания и анализа влияния информационных технологий на эффективность систем управления / В книге: Перспективные направления развития отечественных информационных технологий материалы II межрегиональной научно-практической конференции. – Севастополь, Севастопольский государственный университет. – 2016. – С. 10-14.

УДК 004.056

СТРАТЕГИЯ РАЗВИТИЯ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

Михайлов Николай Семёнович

АО «Равенство»

Россия, Санкт-Петербург, ул. Промышленная, д. 19

email:nickmick@mail.ru

Аннотация: Рассмотрены проблемы создания стратегии развития промышленного предприятия

Ключевые слова: стратегия развития предприятия; промышленное предприятие.

STRATEGY OF DEVELOPMENT OF INDUSTRIAL ENTERPRISE

Mikhailov Nikolay

JSC "Equality"

Russia, St. Petersburg, st. Promyshlennaya, house 19

email:nickmick@mail.ru

Abstract: The problems of creating a strategy for the development of an industrial enterprise

Keywords: development strategy of enterprise; industrial enterprise

Процесс формирования стратегии развития предприятия - это модель управленческих воздействий, состоящая из структурно-взаимосвязанных процедур выполняющих отдельные функции стратегического менеджмента с целью создания стратегии развития предприятия.

Программа инновационного развития (ПИР) промышленного предприятия формирует на долгосрочную перспективу (до 2025 года) и среднесрочный (3 года) период комплекса мероприятий, направленных на достижение цели: разработку и внедрение новых технологий и инновационных продуктов и услуг, соответствующих мировому уровню, что позволит обеспечить лидирующие позиции на рынке России.

Проведение инновационных мероприятий направлено на обеспечение выполнения основных показателей эффективности за счет:

- Уменьшения себестоимости выпускаемой продукции за счет внедрения новых или усовершенствованных технологий создания и производства техники вследствие технического перевооружения производства.

- Повышения производительности труда за счет внедрения новых и усовершенствованных технологий проектирования и изготовления опытных и серийных образцов оборудования, автоматизации рабочих мест, повышения кадрового потенциала.

- Экономии энергетических ресурсов в процессе производства за счет использования современного оборудования.

- Повышение экологической безопасности при производстве готовой продукции.

В стратегии развития предприятия существуют и слабые стороны, которые нуждаются в корректировке для успешного достижения поставленных предприятием целей:

- 1) увеличение выручки за счет снижения затрат на производство продукции;
- 2) повышение производительности труда за счет оплаты труда на основе KPI (ключевых показателей эффективности);
- 3) сокращение малоэффективного персонала;
- 4) техническое перевооружение;
- 5) оптимизация бизнес-процессов.

СПИСОК ЛИТЕРАТУРЫ

1. Чечин О.П. Механизм формирования стратегии развития промышленного предприятия / О.П. Чечин // Вестник Самарского гос. техн. ун-та. Сер.: Экон. науки. – 2014. – № 1 (11). – С. 46-49.
2. Царикаев А.Ю. Процесс формирования стратегии развития промышленных предприятий // Бизнес в законе. Экономико-юридический журнал. Издательский дом Юр-ВАК, 2011

УДК 004.056

МОТИВАЦИЯ ПЕРСОНАЛА НА ОСНОВЕ KPI

Михайлова Анна Сергеевна

Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова

Россия, Санкт-Петербург, ул. 1-я Красноармейская, д. 1

email:aretta@mail.ru

Аннотация: Рассмотрена проблема создания системы мотивации персонала на предприятии

Ключевые слова: система мотивации персонала, KPI.

KPI-BASED MOTIVATION OF PERSONNEL

Mikhailova Anna

Baltic State Technical University "VOENMEKh" them. D.F. Ustinov

Russia, St. Petersburg, st. 1-ya Krasnoarmeyskaya, 1

email: aretta@mail.ru

Abstract: The problem of creating a system of staff motivation in an enterprise**Keywords:** system of personnel motivation, KPI

Мотивация труда – мотивация работающего человека или группы лиц, направленная на повышение эффективности работы организации путем соотнесения внешних и внутренних мотивирующих факторов. KPI – метод оценки на основе использования количественных показателей несбалансированной, выполнение бизнес-процессов и сравнения результатов их стратегических, тактических и оперативных целей должны получить значение отклонения (разница) между целевой и фактической производительности.

Главным преимуществом систем KPI является то, что процесс принятия решений сводится к анализу данных, которые доступны в любое время и представлены в заранее утвержденном формате.

Ключевые показатели эффективности в производстве рассчитываются, исходя из следующих показателей:

- среднедневной расход сырья;
- объем незавершенного производства и запасов;
- производительность труда рабочих;
- прочие производственные расходы;
- ремонт оборудования;
- хранение готовой продукции.

Рассмотрим аргументы в пользу применения системы KPI в мотивации персонала:

1) 100%-ная ориентация на результат – сотрудник получает вознаграждение за достижение результата и за выполнение работ, которые должны привести к результату;

2) управляемость – позволяет корректировать направленные усилия сотрудников без серьезной модификации самой системы при изменении ситуации на рынке;

3) справедливость – достойная оценка вклада сотрудника в общий успех компании и справедливое распределение рисков (между сотрудником и компанией) в случае неуспеха;

4) понятность – сотрудник понимает, за что компания готова его вознаграждать; компания понимает, за какие результаты и сколько она готова заплатить;

5) неизменность – любой сотрудник выстраивает свою работу в соответствии с системой мотивации. Если в определенный момент система меняется, то часть усилий сотрудника уходит впустую.

Системы ключевых показателей эффективности позволяет дифференцировать вознаграждение – связь между результатом и вознаграждением, размер которого должен быть совместим со значением цели в организации.

СПИСОК ЛИТЕРАТУРЫ

1. Овсяк Н. В. Мотивация персонала: сущность и современные проблемы // БИ . 2014. №2. URL: <http://cyberleninka.ru/article/n/motivatsiya-personala-suschnost-i-sovremennye-problemy>.
2. Ключков А.К. KPI и мотивация персонала. Полный сборник практических инструментов.- Эксмо, 2010.-103с.

УДК 004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЦИФРОВОЙ ЭКОНОМИКЕРоманова Анна Александровна¹, Астахова Татьяна Николаевна¹, Колбанев Михаил Олегович²¹Нижегородский государственный инженерно-экономический университет,
Россия, Княгинино, ул Октябрьская, д 22а²Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, 21.

emails: anya-romanova-07@yandex.ru, ctn_af@mail.ru, mokolbanev@mail.ru

Аннотация: Рассмотрены проблемы защиты информации в современном мире. Представлены особенности обеспечения информационной безопасности в цифровой экономике.

Ключевые слова: информационная безопасность; информационные технологии; информационные угрозы; конкурентоспособность; цифровая экономика.

INFORMATION SECURITY IN THE DIGITAL ECONOMYRomanova Anna¹, Astakhova Tatyana¹, Kolbanev Mikhail²¹Nizhny Novgorod State University of Engineering and Economics,
Russia, Knyaginino, Oktyabrskaya str., 22a²St. Petersburg State Economic University, Russia, St. Petersburg, Sadovaya str., 21.
emails: anya-romanova-07@yandex.ru, ctn_af@mail.ru, mokolbanev@mail.ru

Abstract: The problems of information protection in the modern world are considered. Features of information security in the digital economy are presented.

Keywords: *information security; information threats; information technology; competitiveness; digital economy.*

Введение. В настоящее время происходит цифровая революция впоследствии производственного скачка информационных и коммуникационных технологий. Цифровая экономика стремительно вытесняет старый уклад во всех сферах деятельности современного общества. Трансформируется частная жизнь и рабочие места, появляются новые профессии и инструменты взаимодействия.

Отличие цифровой экономики от обычной состоит в том, как информация могла быть представлена, храниться и передаваться. В предыдущей экономике информация была аналоговой или физической, передача которой осуществлялась только посредством фактического перемещения людей или, непосредственно, используя материальный носитель информации. Также и с хранением информации – всегда необходим физический объект (материальный носитель).

Цифровая экономика – это «деятельность, в которой ключевыми факторами производства являются данные, представленные в цифровом виде, а их обработка и использование в больших объемах, в том числе непосредственно в момент их образования, позволяет по сравнению с традиционными формами хозяйствования существенно повысить эффективность, качество и производительность в различных видах производства, технологий, оборудования, при хранении, продаже, доставке и потреблении товаров и услуг» [1].

Цифровая экономика представлена следующими уровнями, которые в своем тесном взаимодействии влияют на жизнь граждан и общества в целом [1]:

- рынки и сферы деятельности, где выполняются взаимодействие конкретных субъектов (поставщиков и потребителей товаров, работ и услуг);
- платформы и технологии, где формируются компетенции для развития рынков и отраслей экономики (сфер деятельности);
- среда, которая создает условия для развития платформ и технологий, эффективного взаимодействия субъектов рынков и отраслей экономики (сфер деятельности) и охватывает нормативное регулирование, информационную инфраструктуру, кадры и информационную безопасность.

Благодаря цифровой экономике повышается эффективность всех отраслей за счет использования информационных технологий; качественно и количественно увеличиваются возможности совершения практически всех операций через компьютер, среди которых предоставление (получение) различных услуг и выполнение транзакций. Однако, помимо ряда преимуществ, цифровая экономика несет и определенные риски. Жизненно важные интересы субъектов (государства, юридических и физических лиц), участвующих в процессах автоматизированного взаимодействия, как правило, заключаются в том, чтобы определенная часть информации, касающаяся их экономических, политических и других сторон деятельности, конфиденциальные коммерческие и персональные данные были бы постоянно легко доступны и в то же время надежно защищены от неправомерного использования. Искажение или фальсификация, уничтожение или разглашение определенной части информации, равно как и дезорганизация процессов её обработки и передачи, наносят серьезный материальный и моральный урон. Таким образом, крайне остро встает вопрос обеспечения информационной и экономической безопасности государства и бизнеса, защиты персональных данных и неприкосновенности частной жизни российских граждан в цифровом пространстве.

Применение технологий цифровой экономики, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы.

Складывается устойчивое мнение, что сеть Интернет формируется как свободное информационное, правовое, финансовое, социально-культурное пространство, свободное от государственного регулирования и контроля. Самыми распространёнными для населения являются простые и быстрые способы и формы обмена информацией, включая установление договорных отношений в сфере электронной торговли, покупки ценных бумаг, учета и отчетности за доходами и движением капитала [2].

Состояние информационной безопасности в экономической сфере характеризуется недостаточным развитием конкурентоспособных информационных технологий, которые можно было использовать для производства продукции и оказания услуг. Высокая зависимость отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обуславливает соотношение социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран [3].

Существующее в настоящее время разделение ресурсов между странами, которые необходимы для обеспечения безопасного и устойчивого функционирования сети «Интернет», не позволяет

реализовать совместное справедливое, основанное на принципах доверия управление ими. Отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий, затрудняет формирование системы международной информационной безопасности, направленной на достижение стратегической стабильности и равноправного стратегического партнерства [3].

Основными аспектами обеспечения информационной безопасности в цифровой экономике являются [4]:

- инновационное развитие отрасли информационных технологий и электронной промышленности, увеличение продукции данной отрасли в валовом внутреннем продукте, в структуре экспорта страны;

- устранение зависимости отечественной промышленности от зарубежных информационных технологий и средств; гарантия информационной безопасности за счет создания, развития и внедрения отечественных разработок, а также производства продукции и оказания услуг на их основе;

- повышение конкурентоспособности российских компаний, осуществляющих деятельность в отрасли информационных технологий и электронной промышленности, разработку, производство и эксплуатацию средств обеспечения информационной безопасности, оказывающих услуги в области обеспечения информационной безопасности, в том числе за счет создания благоприятных условий для осуществления деятельности на территории Российской Федерации;

- развитие отечественной конкурентоспособной электронной компонентной базы и технологий производства электронных компонентов, обеспечение потребности внутреннего рынка в такой продукции и выхода этой продукции на мировой рынок.

Заключение. Обеспечение информационной безопасности в современном мире, во всех сферах деятельности человека, является актуальной, и весьма трудозатратной и трудоемкой проблемой, решение которых зависит не только от разработки конкурентоспособного отечественного программного обеспечения, в представлении усовершенствованных услуг, но и в повышении качества предоставляемых на данный момент.

СПИСОК ЛИТЕРАТУРЫ

1. Паньшин Б. Цифровая экономика: особенности и тенденции развития / Б. Паньшин // Наука и инновации. 2016. Т. 3. № 157. С. 17-20.
2. Верзун Н. А. Аспекты безопасности информационно-экономической деятельности / Н. А. Верзун, М. О. Колбанев, Т. М. Татарникова // Технологии информационно-экономической безопасности: сб. статей сотр. каф. ИС и Т. - СПб.: Изд-во СПбГЭУ, 2016. - С.52-56
3. Petrova G.V. Legal security issues in the formation of a "digital economy" and a single "digital space industry" eaeu / G. V. Petrova // Международное сотрудничество евразийских государств: политика, экономика, право. 2017. Т. 1. № 10. С. 37-46.
4. Доктрина информационной безопасности Российской Федерации [Текст]: Президент РФ В. В. Путин от 5 декабря 2016 г.
5. Колбанев М. О., ИНФОРМАТИЗАЦИЯ И ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ /М. О. Колбанев, И. Л. Коршунов, И. М. Левкин // В сборнике: Россия и Санкт-Петербург: экономика и образование в XXI веке научная сессия профессорско-преподавательского состава, научных сотрудников и аспирантов по итогам НИР за 2015 год: сборник лучших докладов. 2016. С. 159-163.

УДК 004.72

МЕТОДЫ МОДЕЛИРОВАНИЯ САМОПОДОБНОГО ТРАФИКА

Татарникова Татьяна Михайловна¹, Яковлев Сергей Алексеевич²

¹Санкт-Петербургский государственный университет аэрокосмического приборостроения
Россия, Санкт-Петербург, ул. Большая Морская, 67,

² Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5,
emails: tm-tatarn@yandex.ru, sayakovlev@list.ru

Аннотация: Обсуждаются вопросы моделирования трафика, адекватно отображающего реальную нагрузку в сети, а также существующие подходы к имитационному моделированию самоподобного сетевого трафика.

Ключевые слова: сетевой трафик, фрактальные свойства трафика методы моделирования самоподобного трафика.

METHODS OF SIMULATION OF THE SELF-SIMULATED TRAFFIC

Tatiana Tatarnikova, Yakovlev Sergey

¹Saint-Petersburg State University of Aerospace Instrumentation
Russia, St. Petersburg, Bolshaya Morskaya str. 67

²The St. Petersburg State Electrotechnical University «LETI»,
Russia, St. Petersburg, Professor Popov str., 5,
emails: tm-tatarn@yandex.ru, sayakovlev@list.ru

Abstract: Discusses the issues of modeling traffic that adequately reflects the real load on the network, as well as existing approaches to simulating simulated self-similar network traffic.

Keywords: *network traffic, fractal properties of traffic, methods for modeling self-similar traffic.*

Развитие инфокоммуникационных сетей, появление новых сетевых технологий и приложений типа видео по требованию возобновили интерес к изучению трафика сетей, генерируемого реальными службами и приложениями [1], [2].

Исследования показывают, что отличительной особенностью нагрузки быстродействующих компьютерных сетей является ее пачечный характер, причем пачки (скупенности) появляются в разных масштабах времени. Пачечный трафик может быть описан статистически с использованием понятия фракталов [3], [4].

Методы моделирования сетевого трафика, концептуально можно разделить на два класса аналитические и имитационные. Возможны также комбинированные модели, сочетающие в себе аналитическую и алгоритмическую части [5].

На сегодняшний день разработано множество моделей, предназначенных для имитации фрактального трафика. Анализ доступных публикаций по моделированию самоподобного трафика позволяет выделить следующие модели.

Фрактальное броуновское движение (Fractional Brown Motion – FBM). В основе модели FBM лежит случайный процесс движения некоторой гипотетической частицы, которая совершает хаотическое перемещение в пространстве.

Фрактальный гауссовский шум (Fractional Gaussian Noise – FGN). FGN – стационарный в широком смысле стохастический процесс с определенными параметрами и автокорреляционной функцией заданного вида. По сравнению с обычным гауссовым шумом, FGN имеет дополнительный параметр Херста, который количественно определяет степень фрактального масштабирования.

Хаотические отображения (Chaotic Map – CMAP). Такие модели являются достаточно распространенными и концептуально простыми, они используют меньшее число параметров, чем FGN и FBM, и их выбор имеет более наглядную трактовку.

В основе лежит логистическое уравнение

Модели на основе техники «динамического моделирования Маркова» (Dynamic Markov Modelling – DMM). Эти модели представляют собой автоматы с конечным числом состояний, изображаемые орграфами или диаграммами состояний модели. В процессе обучения модели, при получении очередного символа входного потока, происходит переход модели в следующее состояние и модификация частотных счетчиков, соответствующих вероятностям переходов. Выходом модели является набор вероятностей появления символов.

Модели с использованием нечеткой логики. Построение нечетких моделей, как правило, основано на настройке функций принадлежности по параметрам нечетких множеств, используемых в правилах, весов правил и на настройке операций. Задание уровней пачечности может быть представлено в виде ступенчатой функции полезности.

Нейросетевые модели, которые позволяют решить задачу аппроксимации функций нескольких переменных по обучающей выборке путем погружения временного ряда в многомерное пространство.

Авторегрессионные модели (Autoregressive Models – AR) широко применяются для моделирования и предсказания благодаря свойству длительной памяти самоподобных процессов. В этих моделях текущее значение генерируемой величины рассчитывается как взвешенная сумма N предыдущих отсчетов плюс случайная переменная. Суть всех этих моделей в общем виде может быть представлена таким образом «завтра будет также, как в среднем за прошедшее время».

ON/OFF-модели. В этих моделях трафик рассматривается как комбинация источников, которые его генерируют. Каждый источник имеет следующую структуру. Некоторый период времени они могут генерировать пакеты информации (так называемые ON-периоды), при этом внутри одного периода пакеты приходят с одинаковыми интервалами между ними. После ON-периода следует OFF-период, когда источник не генерирует пакеты. Размер ON- и OFF-периодов является случайной величиной, которая должна иметь конечное математическое ожидание и бесконечную дисперсию [6], [7].

Адекватность описания реального трафика достигается путем усложнения моделей, объединения нескольких моделей, введения дополнительных параметров. Естественно для более сложных моделей требуются большие вычислительные возможности или большее время для генерирования реализаций трафика. В работе предлагаются различные генераторы сетевого трафика с пачечной характеристикой, которые можно обучать и адаптировать под разные сетевые процессы.

СПИСОК ЛИТЕРАТУРЫ

1. Богатырев В.А. Имитационная модель поддержки проектирования инфокоммуникационных резервированных систем // Научно-технический вестник информационных технологий, механики и оптики. / В.А. Богатырев, Н.С. Кармановский, Н.А. Попцова, С.А. Паршутина, С.В. Богатырев. – 2016. Т. 16. № 5(105). – С. 831-838.
2. Кутузов О.И., Татарникова Т.М. Инфокоммуникационные сети. Моделирование и оценка вероятностно-временных характеристик. – СПб.: ГУАП, 2015. – 382 с.

3. Шелухин О. И., Осин А. В., Смольский С. М. Самоподобие и фракталы. Телекоммуникационные приложения. – М.: Физматлит, 2008. – 368 с.
4. Кутузов О.И., Татарникова Т.М. К оцениванию и сопоставлению очередей классических и фрактальных систем массового обслуживания//Информационно-управляющие системы. 2016. Т. 81. № 2. С. 48-55.
5. Пуха Г.П. Концепция моделирования систем радиосвязи. В сборнике: Технологии информационного общества/ Г.П. Пуха, Р.В. Драчев// X Международная отраслевая научно-техническая конференция: сборник трудов. – 2016. – С. 386-387.
6. Tatarnikova T. Evaluation and Comparison of Classical and Fractal Queuing Systems/ T. Tatarnikova, O. Kutuzov //XV International Symposium "Problems of Redundancy in Information and Control Systems", September 26-29, 2016. St. Petersburg, Russia.
7. Татарникова Т. М. Имитационная модель виртуального канала / Т.М. Татарникова, М.А. Елизаров // Научно-технический вестник информационных технологий, механики и оптики. 2016. Т.16. № 6. С. 1120-1127.

УДК 004.9

ЗАЩИЩЕННАЯ СИСТЕМА УДАЛЕННОГО МОНИТОРИНГА ПАЦИЕНТОВ

Татарникова Анна Александровна

Санкт-Петербургский государственный университет аэрокосмического приборостроения
Россия, Санкт-Петербург, ул. Большая Морская, 67,
email: a.a.tatarnikova@mail.ru

Аннотация: предлагается решение защищенной системы удаленного мониторинга пациентов с заболеванием опорно-двигательного аппарата, рассматриваются аппаратно-программные модули системы и интерфейсы.

Ключевые слова: электронное здравоохранение, мобильное устройство, удаленный мониторинг пациентов, защищенная информационная система.

PROTECTED SYSTEM OF REMOTE PATIENTS MONITORING

Anna Tatarnikova

Saint-Petersburg State University of Aerospace Instrumentation
Russia, St. Petersburg, Bolshaya Morskaya str. 67
email: a.a.tatarnikova@mail.ru

Abstract: a solution of a protected system for remote monitoring of patients with locomotor system diseases is considered, hardware-software modules of the system and interfaces are considered.

Keywords: e-health, mobile device, remote patient monitoring, secure information system.

В здравоохранении первостепенную важность для большинства людей имеет легкий доступ к медицинским услугам, а также возможность самостоятельно следить за своим здоровьем. Из-за этого медицинские учреждения во всем мире постепенно переходят к ориентированной на пациента инструментальной модели здравоохранения. Такой переход осуществляется и в нашей стране и связан с электронным здравоохранением (общепринятый термин –eHealth). Во многих медицинских учреждениях есть услуга дистанционной записи к врачу и электронные медицинские карты, а в некоторых уже введены такие услуги и технологии как виртуальное здравоохранение (телемедицина) и Интернет медицинских устройств (Internet of Health Things, IoHT) [1]. Также относительно недавно появилась новое направление электронного здравоохранения – мобильное здравоохранение (mHealth).

В работе предлагается решение защищенной системы удаленного мониторинга пациентов с заболеванием опорно-двигательного аппарата (ОДА).

Система состоит из следующих основных программно-аппаратных модулей.

- мобильное устройство со встроенными акселерометрами, которое можно закрепить на теле пациента, например, с помощью чехла для телефона, который можно прикрепить к ремню;
- приложение на мобильном устройстве пациента, которое получает данные с акселерометров и отправляет результаты обработки данных на компьютер медицинского учреждения;
- компьютер, к которому имеет доступ лечащий врач; компьютер подключен к сети Интернет и расположен в медицинском учреждении или в любом другом месте, доступном лечащему врачу.
- приложение на компьютере, которое принимает данные от приложения с мобильного устройства, обрабатывает полученные данные и выдает информацию о состоянии пациента лечащему врачу.

Так как в предлагаемой информационной системе подразумевается передача медицинских данных через сеть Интернет и хранение персональных данных, то необходимо реализовать защищенную передачу и хранение этих данных с помощью сертифицированных средств защиты информации, соответствующих требованиям законодательства Российской Федерации [2-5].

В работе обсуждаются особенности разработанного программного обеспечения для мобильных устройств, которыми будут пользоваться пациенты, и программное обеспечение для серверной части системы, вопросы защиты информации и технологии обеспечения информационной безопасности при работе подобной информационной системы.

СПИСОК ЛИТЕРАТУРЫ

1. Коршунов И. Л. Состояние и концепция развития информационных технологий в сфере сервиса// Известия вузов. Приборостроение. – 2014. Т. 57. № 9. – С. 7-10.
2. Левкин И. М. Модель обработки документальных источников информации деловой разведки / И. М. Левкин//Изв. вузов. Приборостроение. – 2014. Т. 57. № 9. – С. 23–26.
3. Татарникова Т.М. Защищенные корпоративные сети. Раздел: "Задачи по защите информации" / Т. М. Татарникова. – СПб: РГГМУ, 2012. –113 с.
4. Соколов Р. В. Проектирование информационных систем. – СПб.: СПбГИЭУ, 2012. – 336 с.
5. Коломойцев В.С., Богатырев В.А. Оценка эффективности и обоснование выбора структурной организации системы многоуровневого защищенного доступа к ресурсам внешней сети // Информация и космос. – 2015. № 3. – С. 71-79.

УДК 004.72

МЕТОДИКА ПРОЕКТИРОВАНИЯ ИНФРАСТРУКТУРЫ ГИС ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЯ ПРИ УПРАВЛЕНИИ КОРАБЛЕМ

Яготинцева Наталья Владимировна

Российский государственный гидрометеорологический университет,
Россия, Санкт-Петербург, Малоохтинский пр., 98,email: solnishko234@yandex.ru **Аннотация:** Предлагается методика проектирования структурно-функциональной модели ГИС, предназначенная для решения задачи формирования инфраструктуры ГИС поддержки принятия решения при управлении морским судном.**Ключевые слова:** управление морским судном, ГИС корабля, архитектура ГИС, локальная вычислительная сеть, технология коммутации сегментов сети, методика проектирования.**THE METHOD OF DESIGNING GIS INFRASTRUCTURE SUPPORTING DECISION-MAKING AT THE MANAGEMENT OF SHIPS**

Natalia Yagotinceva

Russian State Hydrometeorological University,
Russia, St. Petersburg, Malookhtinsky prospect, 98,

email: solnishko234@yandex.ru

Abstract: The article deals with the methodology of designing a structured and functional GIS model designed to solve the problem of forming a GIS infrastructure for decision support in the control of a ship.**Keywords:** ship's GIS control, GIS architecture, local area network, technology of switching network segments, design methodology.

Методика проектирования ГИС корабля включает в себя алгоритм решения, обеспечивающий формирование инфраструктуры ГИС и дальнейшее приближение архитектуры ГИС к заданному набору свойств [1-3].

ГИС корабля, представляет собой трехслойную структуру: информационное обеспечение, программное обеспечение и аппаратное обеспечение. Транспортной основой ГИС является локальная вычислительная сеть с коммутацией сегментов [4], технология построения которой позволяет одновременно передавать данные между всеми взаимодействующими парами «Клиент-Сервер» [5].

Модель ГИС представлена количественно как функция множества параметров, которые задаются как технические требования на функциональные модули ГИС, множества стоимостных характеристик функциональных модулей ГИС и множества пространственных параметров (форм-факторов) функциональных модулей ГИС.

Выбор облика ГИС решается как целочисленная задача условной многопараметрической оптимизации с ограничениями второго рода по стоимости, производительности и ограничений на площади, выделяемые под проект ГИС [6-10].

Предложенная методика проектирования структурно-функциональной модели ГИС предназначена для решения задачи формирования инфраструктуры ГИС поддержки принятия решения при управлении морским судном. В рамках верификации методики разработана экспертная система по выбору облика ГИС морского судна [11], которая позволяет в диалоговом режиме формировать списочный состав функциональных модулей и оборудования необходимого при проектировании.

СПИСОК ЛИТЕРАТУРЫ

1. Татарникова Т.М., Яготинцева Н.В. Характеристика проблемы интеграции образцов радиоэлектронного вооружения корабля//Ученые записки РГГМУ. 2012. №25. С. 156-162.
2. Татарникова Т.М., Яготинцева Н.В. Новый подход к организации информационной инфраструктуры корабля//67-я научно-техническая конференция, посвященная дню радио: Сб. науч. тр. СПб. 2012. С. 24-25.
3. Татарникова Т.М., Яготинцева Н.В. Интеграция образцов радиоэлектронного вооружения на основе информационной транспортной сети корабля// Региональная информатика и информационная безопасность сборник трудов. Сб. науч. тр. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. 2015. С. 148-151.
4. Татарникова Т.М. Структурный синтез центра сопряжения корпоративных сетей//Информационно-управляющие системы. 2015. № 3 (76). С. 92-98.

5. Яготинцева Н.В. Модель информационной транспортной сети корабля// Региональная информатика и информационная безопасность сборник трудов: Сб. науч. тр. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. 2016. С. 415-418.
6. Татарникова Т.М., Яготинцева Н.В. Модель оценки характеристик локальной вычислительной сети корабля //Материалы международной конференции «Теоретические и прикладные проблемы науки и образования в 21-м веке», часть 5, Тамбов. С. 143-144.
7. Богатырев В.А., Богатырев А.В. Функциональная надежность систем реального времени//Научно-технический вестник информационных технологий, механики и оптики. 2013. № 4. С. 150-151
8. Татарникова Т.М., Яготинцева Н.В. Оценка функциональной надежности корабельной сети передачи данных// Известия высших учебных заведений. Приборостроение. 2014. Т. 57. № 9. С. 62-66.
9. Татарникова Т.М., Яготинцева Н.В. Вероятностная модель установления соединения в инфокоммуникационной сети// Известия высших учебных заведений. Приборостроение. 2017. Т. 60. № 2. С. 157-166.
10. Татарникова Т.М., Яготинцева Н.В. Предоставление услуг передачи данных на корабле // Инновационные технологии в сервисе: Сб. науч. тр. IV Международной научно-практической конференции. Под ред. А. Е. Карлика. 2015. С. 321-322.
11. Татарникова Т.М., Яготинцева Н.В. Принципы организации экспертной системы выбора структуры локальной сети корабля// Современное общество, образование и наука сборник научных трудов по материалам: Сб. науч. тр. Международной научно-практической конференции: в 16 частях. 2015. С. 142-144.



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ИМПОРТОЗАМЕЩЕНИЕ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

УДК 37.014.7

МОДЕЛИ СОТРУДНИЧЕСТВА ВУЗОВ И ИТ-КОМПАНИЙ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ В УСЛОВИЯХ ИМПОРТОЗАМЕЩЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Абрамян Геннадий Владимирович

Российский государственный педагогический университет им. А. И. Герцена, Россия,
Санкт-Петербург, набережная реки Мойки, 48; Финансовый университет при Правительстве РФ,
Россия, Санкт-Петербург, ул. Съезжинская, 15-17
email: abrgv@rambler.ru

Аннотация: В статье рассматриваются нормативные, исследовательские, ресурсно-технологические, маркетинговые, корпоративные и образно-кодовые модели обеспечения информационной безопасности регионов России на основе сотрудничества вузов и ИТ-компаний в условиях импортозамещения программного обеспечения.

Ключевые слова: информационная безопасность, модели, взаимодействие вузов, импортозамещение, исследования, ИТ-технологии, сотрудничество, подготовка, программное обеспечение, процессы, сервисы, совместная деятельность

MODELS OF COOPERATION OF HIGH SCHOOLS AND IT COMPANIES IN THE FIELD OF SECURING INFORMATION SECURITY OF THE REGIONS OF RUSSIA IN THE CONDITIONS OF IMPORT REPLACEMENT OF THE SOFTWARE

Abrahamyan Gennady

Russian Federation, Saint-Petersburg, The Herzen State Pedagogical University of Russia, Embankment of
the Moika River, 48; Financial University under the Government of the Russian Federation, Saint-Petersburg,
Sjezhinskaya str. 15-17
email: abrgv@rambler.ru

Abstract: The article discusses the methodology of the analysis, classification and taxonomy of learning objectives Informatics and information technologies in conditions of internationalization of education, polarization of economic markets, regional and global labour migration.

Keywords: learning objectives, taxonomy, teaching model, learning standards, domains, internationalization of education, polarization of economic markets, global labour migration

Введение. В условиях экономического и политического кризиса в этих странах развитие научно-исследовательских, учебно-образовательных и промышленно-производственных (НИУОиПП) технологий, сервисов и процессов (ТСиП) ИТ-сотрудничества и моделей обеспечения информационной безопасности (ИТСиМОИБ) в России и странах ближнего зарубежья (РиСБЗ) нуждается в новых формах, качественной переоценке, оптимизации и перепрофилирования существующей деятельности и имеющихся ИТ-ресурсов.

Для обеспечения ИТСиМОИБ в области импортозамещения ПО в статье предлагается развивать НИУОиПП ТСиП ОИБ в РиСБЗ. Нормативно-правовое ИТСиМОИБ НИУОиПП ТСиП в РиСБЗ на основе ГСиИИ основано на наличии, разработке, внедрении и развитии монопольных ТСиП, используемых в конкретных НИУОиПП учреждениях/организациях РиСБЗ инновационной нормативной и законодательной базы функционирования, управления и организации различных видов совместной деятельности на основе доступа и использования инфотелекоммуникационных ресурсов НИУОиПП. При этом монопольные преимущества НИУОиПП определяются уникальным нормативно-правовым статусом НИУОиПП МОИБ в инфотелекоммуникационной сети (ИС) муниципальных связей, ее международным и/или российским рейтингом НИУОиПП. Инновационно-исследовательское ИТСиМОИБ НИУОиПП ТСиП в РиСБЗ на основе ГСиИИ основана на наличии, разработке, внедрении и развитии монопольных инновационных научных концепций, методологий, патентов, изобретений, сервисов, услуг и управления в области ИБ, которые позволяют повысить инновационный потенциал взаимодействия субъектов ИС - качество и количество совместных исследований, программ

подготовки и переподготовки, полезность различных видов совместной НИУОиПП ИТСиМОИБ деятельности при сохранении уровня финансирования и стоимости затрат на основные виды деятельности.

Ресурсно-технологическое ИТСиМОИБ НИУОиПП ТСиП в РИСБЗ на основе ГСиИИ предполагает наличие, разработку, внедрению и развитию монопольных инновационных сегментов ИС - ресурсов, средств, методик и технологий эффективной деятельности сотрудников и органов управления ОИБ НИУОиПП ТСиП с использованием эффективных принципов методов научной организации труда, призванных повысить заинтересованность разрабатывать и внедрять новые методики и технологии работы, повышающие эффективность НИУОиПП по реализации основной деятельности при условии обеспечения федеральных (муниципальных, региональных) показателей и нормативов по количеству и качеству научных исследований, образовательных программ, увеличению перечня и объемов услуг при минимизации затрат на основную деятельность.

Конкурентно-маркетинговое ИТСиМОИБ НИУОиПП ТСиП в РИСБЗ на основе ГСиИИ реализуется на:

- 1) непрерывном поддержании и развитии инновационной уникальности функционирования и управления уже существующих НИУОиПП ТСиП ИТСиМОИБ на муниципальном уровне РИСБЗ,

- 2) базе и при условии эффективно работающих 1, 2, 3 моделей ИТС и МОИБ НИУОиПП и достаточного объема материально-технических, трудовых и производственных ресурсов и средств ИС поддержки ТСиП НИУОиПП ИТСиМОИБ деятельности в РИСБЗ для работы в условиях непрерывного развития и жесткой муниципальной или региональной конкуренции с аналогичными НИУОиПП ИТСиМОИБ.

Бренд-корпоративное ИТСиМОИБ НИУОиПП политики ТСиП в РИСБЗ на основе ГСиИИ основано на:

- 1) непрерывном поддержании и развитии инновационной уникальности функционирования и управления уже существующих НИУОиПП ТСиП ИТСиМОИБ на муниципальном и частично региональном уровнях РИСБЗ,

- 2) на наличии, разработке, внедрении и развитии ИС поддержки тактических и стратегических политик-технологий бренд-уникальности результатов, процессов и технологий НИУОиПП ИТСиМОИБ деятельности на частично региональном и частично федеральном уровнях.

Образно-кодовое информационное ИТСиМОИБ глобальной НИУОиПП политики ТСиП в РИСБЗ на основе ГСиИИ основано на

- 1) непрерывном поддержании и развитии инновационной уникальности функционирования и управления уже существующих НИУОиПП ТСиП ИТСиМОИБ на муниципальном, региональном и частично федеральном уровнях РИСБЗ,

- 2) развитию тактических и стратегических политик-технологий бренд-уникальности результатов ТСиП ИТСиМОИБ НИУОиПП на федеральном и частично международном уровнях,

- 3) наличии, разработке, внедрении и развитии образ-кодов НИУОиПП ТСиП.

Виртуально-сетевое информационно-персонифицированное ИТСиМОИБ глобальной НИУОиПП политики ТСиП в РИСБЗ на основе ГСиИИ основано на

- 1) непрерывном поддержании и развитии инновационной уникальности функционирования и управления уже существующих НИУОиПП ТСиП на муниципальном, региональном, федеральном и частично на международном уровнях,

- 2) развитию тактических и стратегических политик-технологий бренд-уникальности результатов ТСиП ИТСиМОИБ НИУОиПП на международном уровне,

- 3) наличии, разработке, внедрении и развитии образ-кодов ИТСиМОИБ НИУОиПП ТСиП заинтересованности РИСБЗ в создании результатов инновационного ИТСиМОИБ НИУОиПП ТСиП политик сотрудничества со стороны потребителей, инвесторов и общества на муниципальном, региональном, федеральном и частично международных уровнях (модель реализуется на базе эффективно работающих материально-технических, трудовых, методических ресурсов и информационных средств ИС, налаженного НИУОиПП виртуально- сетевого информационно-персонифицированного ТСиП социально-культурного процесса и деятельности в условиях информационного общества и технотронной цивилизации, в которых структура деятельности всех ИТ-субъектов инновационной НИУОиПП среды ИТСиМОИБ ориентирована преимущественно на персонифицированные глобальные и облачно-сетевые формы взаимодействия друг с другом, определяемые индивидуальными и безопасными правами доступа к необходимым ТСиП работы.

Заключение. Рассмотренные модели могут быть использованы в качестве основы построения перспективных моделей ИТСиМОИБ [6] эффективных российских ИТ -компаний, –вузов, –научных комплексов, –центров (РИТ-КВНКЦ), [2] ведущих ИТ-специалистов РФ в условиях импортозамещения ПО [1] на основе:

- 1) разработки, внедрения, развития и использования (РВРиИ) безопасных российских ИТ - алгоритмов, –программ, –сервисов, –процессов, –патентов и –изобретений (РИТ-АПСППИИ) ОИБ,

- 2) подготовки, повышения квалификации и переподготовки (ППКиП) ИТ-специалистов в области ИТСиМОИБ, [5] [9] [10]

3) использования опыта ведущих мировых и РИТ-КВНКЦ [3] [4] с целью монопольной или коллективной разработки эффективного и безопасного российского ПО:

1. Нормативно-правовая модель ИТСИМОИБ РИТ-КВНКЦ основана на наличии монопольного или коллективного авторского права РВРИИ РИТ-АПСППИИ поддержки основной деятельности, в том числе ППКиП в области безопасности ИТ [11].

2. Инновационно-исследовательская модель ИТСИМОИБ РИТ-КВНКЦ основана на совместных исследованиях в области РВРИИ РИТ-АПСППИИ, которые повышают инновационный потенциал и взаимодействие субъектов РИТ-КВНКЦ, качество и количество совместных исследований, программ ППКиП в области безопасности ИТ, при сохранении уровня финансирования и стоимости затрат.

3. Ресурсно-технологическая модель ИТСИМОИБ основана на РВРИИ монопольных или коллективных инновационных сегментах (ИТ -ресурсов, -средств, -методик, -технологий) эффективной деятельности и взаимодействия РИТ-КВНКЦ ИТСИМОИБ в том числе с органами управления на основе принципов и методов научной организации труда, призванных повысить заинтересованность РВРИИ новых РИТ-АПСППИИ, повышающих эффективность ППКиП в области безопасности ИТ.

4. Конкурентно-маркетинговая региональная модель ИТСИМОИБ РИТ-КВНКЦ реализуется на 1) основе и при условии эффективно работающих 1, 2, 3 моделей РВРИИ РИТ-КВНКЦ ИТСИМОИБ, 2) непрерывном РВРИИ и переносе существующей инновационной уникальности функционирования и управления РИТ-АПСППИИ ИТСИМОИБ на региональные уровни РИТ-КВНКЦ РФ в области ИТ-ППКиП.

5. Бренд-корпоративная модель региональной политики ИТСИМОИБ РВРИИ РИТ-АПСППИИ РИТ-КВНКЦ основана на:

1) непрерывном поддержании и развитии инновационной уникальности функционирования и управления (НПиРИУФиУ) существующих РИТ-АПСППИИ на региональном и частично федеральном уровнях ИТ-ППКиП,

2) на наличии, РВРИИ РИТ-АПСППИИ ИТСИМОИБ поддержки тактических и стратегических политик-технологий бренд-уникальности ИТ-ППКиП в РИТ-КВНКЦ ИТСИМОИБ на региональном и частично федеральном уровнях.

6. Образно-кодовая информационная модель федеральной ИТСИМОИБ политики РВРИИ РИТ-АПСППИИ основана на

1) НПиРИУФиУ уже существующих РИТ-АПСППИИ ИТСИМОИБ в вузе на региональном, федеральном и частично международном уровнях ИТ-ППКиП,

2) развитии тактических и стратегических политик-технологий бренд-уникальности результатов РИТ-АПСППИИ ИТСИМОИБ на федеральном и частично международном уровнях ИТ-ППКиП,

3) наличии, разработке, внедрении и развитии образ-кодов РИТ-АПСППИИ ИТСИМОИБ.

7. Виртуально-сетевая информационно-персонифицированная модель глобальной политики РВРИИ РИТ-АПСППИИ ИТСИМОИБ основана на

1) НПиРИУФиУ уже существующих в РИТ-КВНКЦ ИТСИМОИБ [7] [8] РИТ-АПСППИИ и ИТСИМОИБ на региональном, федеральном и международном уровне,

2) развитии тактических и стратегических политик-технологий бренд-уникальности результатов РИТ-АПСППИИ ИТСИМОИБ и деятельности в области ИБ РИТ-КВНКЦ на международном уровне,

3) наличии, разработке, внедрении и развитии образ-кодов заинтересованности ИТ-субъектов в создании АПСППИИ РИТ-КВНКЦ в области ИТСИМОИБ со стороны ИТ-потребителей, инвесторов ИТ-ППКиП на международном уровне.

СПИСОК ЛИТЕРАТУРЫ

1. Абрамян Г.В. Инфотелекоммуникационные проблемы, риски и угрозы высокотехнологичных зон, научных парков и инкубаторов в науке и образовании стран БРИКС. / Г.В. Абрамян // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 томах. Санкт-Петербург, 2015. С. 663-667
2. Абрамян Г.В. К вопросу о научно-методических аспектах, подходах и возможностях информационного моделирования элементов инновационного развития университетских комплексов на современном этапе. / Г.В. Абрамян // Формирование университетских комплексов - путь стратегического инновационного развития образовательных учреждений сборник научных трудов. Федеральное агентство по образованию, Санкт-Петербургский государственный университет сервиса и экономики. Санкт-Петербург, 2008. С. 19-23
3. Абрамян Г.В. Модели научного сотрудничества и профессионального образования в информационной среде стран Азиатско-Тихоокеанского экономического сотрудничества (АТЭС). / Г.В. Абрамян // Информационно-телекоммуникационные системы и технологии» (ИТСИТ-2014) Материалы Всероссийской научно-практической конференции. Кемерово, 2014. С. 7-8.
4. Абрамян Г.В. Модели развития научно-исследовательских, учебно-образовательных и промышленно-производственных технологий, сервисов и процессов в России и странах ближнего зарубежья на основе глобализации сотрудничества и интеграции инфотелекоммуникаций. / Г.В. Абрамян // Актуальные проблемы инфотелекоммуникаций в науке и образовании IV Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 томах. Санкт-Петербург, 2015. С. 668-673
5. Абрамян Г.В. Профессиональная подготовка, становление и адаптация специалиста-информатика в условиях экономического кризиса. / Г.В. Абрамян // Математика, информатика, естествознание и проблемы устойчивого развития сборник научных трудов 28-й международной конференции "Школьная информатика и проблемы устойчивого развития". Комитет по образованию Санкт-Петербурга и Ленинградской области, Академия информатизации образования, Санкт-Петербургский государственный университет, РГПУ им. А. И. Герцена, СПб ГУАП. 2009. С. 23-28.
6. Абрамян Г.В. Система международного научного сотрудничества и модели глобализации профессионального образования и науки в информационной среде стран БРИКС. / Г.В. Абрамян // Региональная информатика "РИ-2014" материалы XIV Санкт-

- Петербургской международной конференции. 2014. С. 290-291.
7. Абрамян Г.В. Телекоммуникационные модели образования и научной деятельности как облачные сервисы SAAS/SOD взаимодействия в вузе. / Г.В. Абрамян // Перспективы развития науки и образования Сборник научных трудов по материалам Международной научно-практической конференции 29 ноября 2013 г. В 7 частях. ООО «АР-Консалт». Москва, 2013. С. 100-101.
 8. Абрамян Г.В., Катасонова Г.Р. Переходные и стационарные алгоритмы обеспечения континуальной квазиустойчивости системы непрерывного образования в условиях бинарно-открытого информационного пространства и связей на основе механизмов откатов. / Г.В. Абрамян, Г.Р. Катасонова // Фундаментальные исследования. 2015. № 2-26. С. 5884-5890.
 9. Абрамян Г.В., Катасонова Г.Р. Таксономия, классификация и методология анализа целей обучения информатике и информационным технологиям в условиях глобализации образования. / Г.В. Абрамян, Г.Р. Катасонова // Фундаментальные исследования. 2014. № 8-7. С. 1647-1652
 10. Абрамян Г.В., Марон А.Е. Стратегия и технология развития систем опережающего образования в современных условиях. / Г.В. Абрамян, А.Е. Марон // Содержание и технологии образования взрослых: проблема опережающего обучения сборник научных трудов. Гос. науч. учреждение "Ин-т образования взрослых Российской акад. образования "; под ред. А. Е. Марона. Санкт-Петербург, 2007. С. 12-13.
 11. Фокин Р.Р., Абрамян Г.В. Мета модель обучения информационным технологиям в высшей школе. / Г.В. Абрамян, Р.Р. Фокин // Санкт-Петербургский государственный университет сервиса и экономики. Санкт-Петербург, 2011

УДК 519.81

ПАРАМЕТРИЧЕСКИЙ СИНТЕЗ СИСТЕМЫ РАДИОМОНИТОРИНГА НА ОСНОВЕ ФОРМАЛЬНОГО ПОДХОДА

Гудков Алексей Александрович, Малышев Сергей Романович
Военная академия связи им. С.М. Буденного,
Россия, Санкт-Петербург, Тихорецкий пр-т, 3,
emails: gudkov_aa@rambler.ru, malishevsv56@ya.ru

Аннотация: В статье рассматривается оптимизационная задача параметрического синтеза системы радиомониторинга и радиотехнического контроля на основе формального подхода, задаются этапы построения данной системы, определяются показатели эффективности, включая требования к уровню эффективности и критерии ее оценки. Проводится сравнение метода отсечения (Гомори) и предлагаемого модифицированного метода неявного перебора при решении задач структурного и параметрического синтеза при заданных условиях и ограничениях.

Ключевые слова: параметрический синтез; оптимизация; система радиомониторинга.

PARAMETRIC SYNTHESIS OF THE RADIOMONITORING SYSTEM BASED ON THE FORMAL APPROACH

Alexey Gudkov, Sergey Malishev
Military Academy of Signal Communication named after S.M. Budyonny,
Russia, St. Petersburg, Tichorezki prospect, 3,
emails: gudkov_aa@rambler.ru, malishevsv56@ya.ru

Abstract: The optimization task of the parametric synthesis of the radio monitoring system and radio technical control based on the formal approach is considered in the article, stages of the system construction are specified, efficiency indicators are determined, including requirements to the level of efficiency and criteria for its evaluation. A comparison is made between the cutting-plane method (Gomori's method) and the proposed modified method of implicit search in solving problems of structural and parametric synthesis under given conditions and constraints.

Keywords: parametric synthesis; optimization; radiomonitoring system.

Введение. На разрабатываемую систему управления радиомониторингом может быть возложено решение комплекса задач. Все решаемые ею задачи, как правило, делятся на 4 блока. Первый комплекс, задачи класса «А» - управление подсистемами мониторинга. Второй комплекс, задачи класса «В» - оперативное слежение за обстановкой в регионах, блоках, странах, за состоянием и деятельностью объектов мониторинга. Третий комплекс, задачи класса «С» - информационно-расчетное обеспечение. Четвертый комплекс, задачи класса «D» - информационно-техническое сопряжение автоматизированных комплексов и средств мониторинга с автоматизированной системой.

В рамках общей постановки оптимизационной задачи процесс синтеза системы отдельного центра радиомониторинга и радиотехнического контроля (СОЦРМ), как сложной военно-технической системы, может быть осуществлен в два этапа.

На первом этапе задаются:

- показатели результатов – вектор показателей частных (единичных) результатов;
- требования к результатам – вектор предельно допустимых значений;
- критерий для оценки качества результатов – 2n-местный неопределенный предикат.

На втором этапе определяются:

- показатель эффективности – вероятность выполнения целевой задачи, стоящей перед СОЦРМ [1];

- требования к уровню эффективности – минимально допустимое (требуемое) значение вероятности выполнения задачи мониторинга;
- критерий для оценки эффективности – одноместный предикат.

Показатель эффективности функционирования СОЦРМ является комплексным показателем качества, а критерий для оценки качества результатов работы системы указывает на цель ее функционирования и требуемую степень достижения этой цели.

В качестве наиболее информативного комплексного показателя эффективности функционирования СОЦРМ целесообразно выбрать вероятность выполнения задачи (достижения цели функционирования). Это справедливо при любом характере результатов функционирования СОЦРМ (случайном или детерминированном) и требований к ним. Если некоторые (или все) компоненты векторов неслучайны и определены заданными значениями, то в выражениях для интегрального закона распределения случайного вектора и функции распределения случайного вектора они будут фигурировать как константы.

Другим аспектом получения оптимального решения будет выбор условий и ограничений, влияющих на полученный результат исследований в соответствии с обоснованной параметрической пригодностью.

Математическая модель задачи определения оптимального состава СОЦРМ состоит из:

- целевой функции, значение которой минимизируется;
- условий и ограничений.

Исходя из сказанного, математическая постановка задачи структурного и параметрического синтеза имеет детерминированный характер, полностью определяемой структурой СОЦРМ [2].

Данная задача относится к задачам большой размерности, принадлежащих к классу NP-полных [3]. Все задачи из этого класса эквивалентны по вычислительной сложности в том смысле, что если одна из них имеет эффективное (с полиномиально ограниченным временем) решение, то все они имеют эффективное решение.

Одним из способов получения решения для подобного класса задач является применение метода так называемого децентрализованного управления, предложенного для задач линейного программирования блочного типа (метод декомпозиции Данцига-Вульфа), с дальнейшим выходом на целочисленную постановку задачи [4].

Конечное или счетное множество допустимых альтернатив во многом определяется значениями параметров, которые характеризуют качественный и количественный состав СОЦРМ.

При решении задачи синтеза основным параметром является стоимость СОЦРМ, т. е. в качестве целевой функции будет выступать общая стоимость системы, включающая стоимостные характеристики энергозатрат, стоимость-площадные характеристики и стоимость-эргатические характеристики. Очевидно, что, с учетом вышеизложенного, целевая функция должна минимизироваться с учетом условий и ограничений на функционирование СОЦРМ.

Исследования показали, что для каждой из выделенных подсистем с помощью разработанных математических подмоделей необходимо рассчитать оптимальный состав технических средств и программных продуктов.

При решении задач структурного и параметрического синтеза при заданных условиях и ограничениях традиционным путем, получение решения происходит с использованием методов динамического, линейного и целочисленного линейного программирования. Известные подходы в силу большой размерности задачи имеют ряд недостатков, к которым относятся низкое быстродействие алгоритмов и значительные затраты памяти ЭВМ, что затрудняет получение высокоэффективного программного продукта.

Новым методом может быть модифицированный метод неявного перебора, который после соответствующей настройки на конкретную технологию решения задач синтеза дает положительный эффект. Применение этого метода в сравнении с методом отсечения (Гомори), основанного на симплекс-методе (решении задачи линейного программирования) дает более эффективное решение, так как:

- не требуется предварительного решения задачи линейного программирования (вычисления ограничиваются операциями сложения или вычитания);
- исключается необходимость масштабирования (алгоритм, построенный на базе метода неявного перебора, в соответствии с заложенной в него методологией, обладает сходимостью в пределах заданных условий и ограничений, что важно для получения оперативных методик при планировании функционирования СОЦРМ);
- дает большую точность решения (относится к методам абсолютной оптимизации).

При конкретной реализации предложенного метода неявного перебора для подзадач структурного и параметрического синтеза СОЦРМ можно учесть индивидуальные особенности аппаратно-программных средств путем введения дополнительных ограничений технологического типа в целях сокращения размерности задачи (сокращение количества переборов возможных альтернатив).

Закключение. Анализ времени, затрачиваемого на решение оптимизационной задачи, показал, что использование известных методик, которые базируются на применении методов динамического и дискретного программирования, не дают выигрыша во времени получения решения по сравнению с

применением метода неявного (частичного) перебора. Алгоритм решения подзадач структурного и параметрического синтеза СОЦРМ носит универсальный характер и может быть использован для других систем передачи данных, в том числе и для оценки возможностей аналогичных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Абчук В. А., Матвейчук Е. Т., Томашевский Л. П. Справочник по исследованию операций. – М.: МО СССР, 1979, – 736 с.
2. Морозов Л. М., Петухов Г. Б., Сидоров В. Н. Методологические основы теории эффективности. Учебное пособие. – Л.: МО СССР, 1979. – 236 с.
3. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. – М.: Мир, 1979. – 536 с.
4. Вагнер Г. Основы исследования операций. Т. 2. – М.: Мир, 1973. – 490 с.

УДК 004.42

ПОРТИРОВАНИЕ ОПЕРАЦИОННОЙ СИСТЕМЫ РЕАЛЬНОГО ВРЕМЕНИ «FREERTOS» НА АППАРАТНЫЕ МОДУЛИ, ПОСТРОЕННЫЕ НА БАЗЕ ПРОЦЕССОРОВ РОССИЙСКОЙ КОМПАНИИ «ЭЛВИС»

Гук Игорь Иосифович, Павлов Федор Андреевич
Акционерное общество «Научно-производственное объединение «Импульс»,
Россия, Санкт-Петербург, ул. Киришская, д.2,
emails: Gook_igor@mail.ru, pavlfyodor@yandex.ru

Аннотация: В статье рассмотрен алгоритм портирования операционной системы реального времени FreeRTOS на процессоры российской компании «Элвис».

Ключевые слова: операционная система реального времени, FreeRTOS, портирование на российскую элементную базу, процессоры компании «Элвис», Мультикор.

THE PORTING OF THE OPERATING SYSTEM REAL-TIME «FREERTOS» IN THE HARDWARE MODULES, ARE BUILT ON THE BASIS OF PROCESSORS OF THE RUSSIAN COMPANY "ELVIS"

Guk Igor, Pavlov Fedor
Joint stock company "Scientific-production Association "Impulse"
Russia, Saint-Petersburg, Kirishskaya str., 2,
emails: Gook_igor@mail.ru, pavlfyodor@yandex.ru

Abstract: In the article the algorithm of porting the operating system real time "FreeRTOS" on processors of the Russian company "Elvis".

Key words: operating system real-time, FreeRTOS, porting, the Russian element base, the processors of the company "Elvis", multicor.

Уровень развития вычислительной техники не стоит на месте. Вычислительный ресурс современных процессоров позволяет просчитывать за ограниченное время несколько десятков, и даже сотен, задач. В этих условиях требуется решить проблему распределения ресурса процессора таким образом, чтобы все задачи были решены в полном объёме и за минимальное время. В критический инфраструктурах, таких, например, как системы управления и контроля, обеспечивающих безопасность какой-либо производственной деятельности, требуется ещё и поддержание жёстких временных рамок для времени реакции на внешние воздействия. Все эти задачи решает операционная система (ОС) реального времени. Таких систем разработано достаточное количество. Проблема заключается в том, что в силу малой мировой распространённости российский электронных компонентов, производители таких ОС не занимаются портирование своего продукта на российские процессоры, либо делают это платно.

В связи с этим были решены следующие задачи:

1. Выбор российской элементной базы для реализации поставленных задач.
2. Выбор ОС реального времени с открытым кодом и хорошей информационной поддержкой.
3. Разработка алгоритма портирование выбранной ОС на аппаратные модули, построенные на российской элементной базе.
4. Разработка драйверов для ОС под периферию аппаратных модулей.
5. Оптимизация кода.
6. Построение программно аппаратных систем на базе выбранной ОС и аппаратных модулей.

СПИСОК ЛИТЕРАТУРЫ

1. Припутин В.С., Жанкевич А.О. Исследование эффекта масштабируемости в беспроводных ad-hoc сетях // Телекоммуникации и транспорт. 2010, № 11. С. 23-25.

УДК 510.6

**СЕЛЕКТИРОВАНИЕ В ИЕРАРХИЧЕСКИХ СИСТЕМАХ ОБЪЕКТОВ НАБЛЮДЕНИЯ И
УСТАНОВЛЕНИЕ ИХ ПРИНАДЛЕЖНОСТИ С ПРИМЕНЕНИЕМ АЛГОРИТМА ОЦЕНКИ
ХАРАКТЕРИСТИК ВЗАИМОСВЯЗАННОСТИ**

Кузьмин Виталий Владимирович, Удальцов Николай Петрович
Военная академия связи имени С.М. Буденного,
Россия, Санкт-Петербург, Тихорецкий проспект, 3,
emails: vitalij.kuzmin.1987@mail.ru, n-p-ud@mail.ru

Аннотация: В статье рассматривается возможность применения алгоритма, позволяющего определять структурное построение организации в пространстве, проводить отбор и принадлежность ее объектов к уровням управления в иерархических системах. При моделировании структуры организации в пространстве использование алгоритма оценки характеристик взаимосвязанности позволяет принимать альтернативные решения при построении ее структуры.

Ключевые слова: алгоритм; структура; организация; объект.

**SELECTION IN THE HIERARCHICAL SYSTEMS OF SUBJECTS TO OBSERVATION AND
ESTABLISHMENT OF THEIR ACCESSORY WITH APPLICATION OF THE ALGORITHM OF
ASSESSMENT OF CHARACTERISTICS OF COHERENCE**

Kuzmin Vitaly, Udaltsov Nikolai
Military academy of communication of Marshall of the Soviet Union S. M. Budyonny,
Russia, St. Petersburg, Tikhoretsky Avenue str., 3,
emails: vitalij.kuzmin.1987@mail.ru, n-p-ud@mail.ru

Abstract: In article the possibility of application of the algorithm allowing to define structural creation of the organization in space, to make selection and belonging of her objects to levels of management in hierarchical systems is considered. When modeling structure of the organization in space use of an algorithm of assessment of characteristics of coherence allows to make alternative decisions at creation of its structure.

Keywords: algorithm; structure; organization; object.

Введение. Системы связи являются составной частью управления эвентуальной организацией, режимы их работы отражают состояние и деятельность объектов наблюдения (ОН), входящих в ее структуру. Основную часть времени функционирование средств связи подчинено состояниям деятельности многих организаций, их распределение в пространстве отражает плотность построения системы управления организации. На основании вышеизложенного формируется вывод о том, что плотность размещения средств связи в пространстве адекватно отображает структуру построения конкретных организаций в иерархических системах. В системном представлении организации важное место занимает их структурное описание. Структурное описание системы включает данные о количестве элементов системы и данные их взаимосвязей [1]. При описании организации выделяются два уровня: уровень, включающий совокупность объектов с определенной степенью детализации и взаимных связей между ними по всему пространству; уровень объектов, входящих в групповые объекты более высокой детализации и состоящих из нескольких элементов, сами объекты в этом случае рассматриваются как системы определенного уровня.

В интересах моделирования деятельности объектов необходимо учитывать факторы, влияющие на их размещение: объект, занимает определенный район, обеспечивающий ему выполнение поставленной задачи; объект стремится к сохранению коммуникабельности, т.е. способности управлять подчиненными элементами и быть управляемым, что естественно выражается в сохранении определенных взаимных удалений между объектами.

Рассмотрение особенностей в размещении объектов на основе расширения понятия взаимосвязанности до межсистемного уровня и взаимодействия с внешней средой позволит выявлять закономерности во взаимном размещении объектов в более широком аспекте.

В размещении ОН проявляются определенные закономерности, отражающие основные требования, предъявляемые к их функционированию. Это выражается в том, что в интересах обеспечения требований по живучести, скрытности, управлению ОН и их элементы размещаются на максимальном удалении друг от друга, а для обеспечения оперативности и непрерывности управления, расстояние между ОН и их элементами должно быть по возможности сокращено. При размещении ОН возникает необходимость в решении этого противоречия, тем самым предлагается использовать эти особенности для оценки вариантов экспозиции ОН.

Анализ вариантов построения организаций различных уровней управления, рекомендуемых руководящими документами, наставлениями и создаваемых в ходе проведения учений, а также при ведении реальных действий, подтверждает наличие определённых закономерностей во взаимном расположении ОН.

В общем случае взаимосвязанность в размещении объектов эвентуальной организации можно определить, как величину, характеризующую возможность того, что в определённом районе сбора информации (РСИ) i -го ОН будет размещён j -ый ОН или же исключено его размещение.

В зависимости от выбранных размеров β -го РСИ взаимосвязанность районов размещения i -го и j -го объектов может быть охарактеризована следующим образом:

размещение i -го объекта в определённом районе предполагает обязательное размещение в пределах β -го РСИ j -го объекта $P_{\beta i}(O_j/O_i) = 1$, $d_{ij} \leq R_{\beta i}$; размещение i -го объекта исключает возможность размещения в пределах β -го РСИ j -го объекта $P_{\beta i}(O_j/O_i) = 0$, $d_{ij} > R_{\beta i}$; в β -ом РСИ i -го объекта размещение j -го объекта носит вероятностный характер $0 < P_{\beta i}(O_j/O_i) < 1$.

Системы отсчёта могут касаться пространственных характеристик различного типа: расстояний, направлений, взаимного расположения объектов в пространстве. Пространственная логика описывает соотношения в статической пространственной ситуации или в ситуации, где отдельные объекты могут перемещаться.

С практической точки зрения наиболее удобно разнос объектов оценивать путём непосредственного определения возможных расстояний между ними - R_{ij} . Значение величины R_{ij} определяется многими факторами, в том числе и случайного характера, и поэтому может быть описано нормальным усечённым законом распределения [2].

Кроме расстояния между объектами информативными признаками может выступать взаимная ориентация их относительно друг друга. На вербальном уровне это может быть представлено следующим образом: j -ый объект может быть размещён относительно i -го объекта произвольным образом, в направлении север (юг, запад, восток). Характеристики ориентации размещения объектов указывают возможное направление размещения j -го объекта относительно i -го объекта и наоборот. Размещение объектов друг относительно друга можно представить значениями азимутов с i -го объекта на j -ый объект. В этом случае ориентация размещения объектов может быть описана равномерным или нормальным законами распределения, Θ_{ij} - значения азимутов.

В целом взаимосвязанность размещения объектов можно определить двумерной функцией плотности вероятности, отражающей зависимость размещения, исходя из их удалённости друг от друга и взаимной ориентации. Потому как случайные величины R и Θ независимы, то их совместная плотность распределения будет определяться как произведение соответствующих функций распределения.

Вышеуказанные характеристики взаимосвязанности получены при условии, что динамика действий позволяет объектам, находится в пределах некоторых РСИ, размеры и взаимное расположение которых учитывались при расчётах.

Заключение. Знание характеристик взаимосвязанности размещения объектов позволит получить специальную информацию об объекте на основе данных о других объектах, что особенно важно в условиях ограниченных возможностей по установлению непосредственного разведывательного контакта с некоторыми объектами эвентуального противника.

СПИСОК ЛИТЕРАТУРЫ

1. Денисов А.А., Колесников Д.Н. Теория больших систем управления. – Л.: Энергоиздат, 1982. – 216 с.
2. Вадзинский Р.Н. Справочник по вероятностным распределениям. – СПб.: Наука, 2001. – 287 с..

УДК 004.94

АНАЛИЗ ТРЕБОВАНИЙ К СИСТЕМЕ УПРАВЛЕНИЯ ИБ ДЛЯ КРИТИЧНЫХ ОБЪЕКТОВ

Лившиц Илья Иосифович¹, Маликов Владимир Викторович²

¹ Санкт-Петербургский национальный исследовательский университет,
Российская Федерация, 197101, Санкт-Петербург, Кронверкский пр., 49

² УО "Центр повышения квалификации руководящих работников и специалистов" Департамента
охраны МВД Республики Беларусь,
223030 Минский р-н, Горанский с/с, р-н д. Горани,
emails: Livshitz.il@yandex.ru, malvvv104@mail.ru

Аннотация: В статье рассматриваются аспекты создания современных систем управления, в частности, обеспечения заданных режимов функционирования и параметров контроля объекта. Для решения данной задачи применяются различные методики, которые подразумевают получение оценки безопасности для критичных объектов. Однако в настоящее время не создано единого подхода к расчету безопасности для информационных систем, что не позволяет в должной мере реализовать безопасное управление сложными промышленными объектами. В данном исследовании предпринята попытка анализа систем управления для сложных промышленных объектов с позиции определения безопасности такой системы.

Ключевые слова: система управления, интегрированная система менеджмента; информационная система; информационная безопасность; аудит.

THE DEVELOPMENT OF IT-SECURITY MANAGEMENT SYSTEM FOR CRITICAL industrial OBJECT

Livshitz Ilya ¹, Malikov Vladimir ²

¹ University of Information Technologies, Mechanics and Optics
Kronverkskiy prospekt, 49, St. Petersburg, 197101, Russia

² "Center of improvement of professional skill of executives and specialists" of the Interior Ministry
Department of the Republic of Belarus
Gorany, Goransky distr., Minsk, 223030, Belarus
emails: Livshitz.il@yandex.ru, malvvv104@mail.ru

Abstract: Creation the modern management systems it is important to provide specific modes of operation and parameters of control object. For this task apply a variety of techniques which involves the estimate of the Information systems. However, currently there is no common approach to the calculation of IT-Security for the Information systems, that is not taken into account in modern control systems of complex industrial facilities. This study attempts to analyze the control systems for complex industrial facilities from the position of determining the security assessment of such a system.

Keywords: Management system, Integrated management system; Information system; Information security; Audit.

Введение. При создании современных систем управления (СУ) представляется важным обеспечение не только заданных технологических режимов и параметров контроля объектов (в данном случае информационных систем — ИС), но и достижение определенной цели устойчивого безопасного функционирования ИС в составе сложного промышленного объекта (СлПО). Применительно к специфике объекта — ИС особое значение приобретает не только обеспечение устойчивости, но и в целом проблема обеспечения информационной безопасности (ИБ).

В настоящее время для решения данной комплексной задачи применяются различные методики, часть из которых подразумевает учет различных компонент — внутренних и внешних подсистем и мониторинг ИС: работы Агуреева [1-5] и работы зарубежных ученых [6-8]. В современных риск-ориентированных стандартах введен специальный термин, описывающий влияние внутренних и внешних подсистем — «контекст» [9-12]. В известных работах поддерживается тезис, что «мониторинг (энтропии) в информационной системе целесообразен для поддержания устойчивой работы» [9-21]. В данной работе авторы расширяют классический термин ИБ [9], в том числе и на свойство обеспечения устойчивости СлПО. Также в ряде изданий отмечается, что это свойство в ИС имеет физический смысл и может быть рассчитана и измерена косвенными методами» [14, 15, 21]. Далее под открытой системой понимается СУ для СлПО, в состав которой входят ИС, для которых необходимо обеспечение ИБ, в том числе — обеспечение функциональной устойчивости (в терминах [14]). Однако в ряде публикаций отмечается, что в ИС диссипация (рассеяние информации) в «чистом виде» не существует [19-21]. Этот факт может означать, что в настоящее время «чистые» ИС (и конкретно — ИС в составе СУ для СлПО) не рассматриваются с должным вниманием к протекающим процессам, в том числе — с точки зрения обеспечения безопасности. Соответственно, для СУ и систем обеспечения ИБ в их составе, не предложено описание потоков энергии и уравнения полной энергии, в том числе с учетом диссипативного характера.

Современный этап развития теории управления и, соответственно, синтез СУ, включает в себя не только моделирование физических аспектов функционирования систем обеспечения ИБ (насколько это необходимо для создания адекватной модели), но и учет аспектов экономических факторов. Вторая (экономическая) часть СУ необходима для учета внешних аспектов любой открытой системы (в терминах стандартов [9-12]) и разнородной структуры требований. Влияние указанных аспектов позволяет осуществить учет как внешних аспектов открытой системы, так и разнородной структуры требований безопасности [9-11]. Построение обобщенной модели СУ начинается с формирования начальных условий, определяющих состояния объекта управления в моменты времени ($t_1, \dots, t_k$). Для подсистемы управления ИБ важно, чтобы выбор шага (дискретности) был четко увязан с известным множеством ограничений, связанных с особенностями функционирования СлПО. Например, на объектах электроэнергетики рекомендуется формировать несколько представлений энергетического состояния СУ и далее контролировать их расхождения в зависимости от воздействий. В частности, различные состояния функциональной безопасности возможно отследить, начиная от начального состояния СУ — Z_1 , и далее под воздействием условий к состоянию ΔZ_1 . Состояния СУ предлагается обозначать как Z_1, Z_2, Z_k . В рассматриваемой системе каждый компонент под воздействием особых условий меняет свое состояние: $Z_1 \rightarrow Z_2$.

Заключение. На основании учета компонент различной природы предложен подход к формированию оценки в СУ для СлПО для обеспечения функциональной безопасности, как расширение классического базового понятия «информационная безопасность». Показана возможность

рассмотрения современных СУ для СлПО с целью достижения устойчивого функционирования и обеспечения требуемого уровня ИБ.

СПИСОК ЛИТЕРАТУРЫ

1. Агуреев И.Е., Денисов М.В. Математическое описание динамики пассажирских транспортных систем // Мир транспорта и технологических машин. 2011. Вып. 1. С. 15-22.
2. Агуреев И.Е., Тропина В.М. Динамика логистической системы в транспортных цепях поставок // ИзвестияТулГУ. Технические науки. 2011. Вып. 4. С. 158-167.
3. Агуреев И.Е., Атлас Е.Е., Пастухова Н.С. Хаотическая динамика в математических моделях транспортных систем // Известия ТулГУ. Технические науки. 2012. № 3. С. 372-389.
4. Агуреев И.Е., Богма А.Е., Пышный В.А. Динамическая модель транспортной макросистемы // ИзвестияТулГУ. Технические науки. 2013. Вып. 6. Ч. 2. С. 139-145.
5. Агуреев И.Е., Гладышев А.В. Динамика производства и спроса в диссипативной модели логистической системы // ИзвестияТулГУ. Технические науки. 2013. Вып. 6. Ч. 2. С. 152-160.
6. Baumgarte J. Stabilization of constraints and integrals of motion in dynamical systems // Comp. Math. Appl. Mech. Eng. 1972. No. 1. P. 1-16.
7. Ascher U.M., Hongsheng Chin, Petzold L.R., Reich S. Stabilization of constrained Mechanical systems with DAEs and invariant manifolds // J. Mechanics of Structures and Machines. 1995. Vol. 23. P. 135-158.
8. Amirouche F. Fundamentals of Multibody Dynamics. Theory and Applications. Birkhauser, Springer, 2005. 684 p.
9. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements, International Organization for Standardization. 2013. 23 p.
10. ISO 19011:2011. Guidelines for auditing management systems;
11. ISO 55001:2014 Asset management – Management systems – Requirements // International Organization for Standardization, 2014. – 14 pages.
12. PAS-99:2012 «Specification of common management system requirements as a framework for integration»
13. Хайтун С.Д. Трактровка энтропии как меры беспорядка и ее негативное воздействие на современную научную картину мира // Вопросы философии. 2013. Вып. 2. С. 62.
14. Шеннон К. Работы по теории информации. – М.: Изд-во иностранной литературы. 1966. 88 с.
15. Лившиц И.И. Практические применимые методы оценки систем менеджмента информационной безопасности // Менеджмент качества. 2013. Вып. 1. С. 22-34.
16. Лившиц И.И. Подходы к применению модели интегрированной системы менеджмента для проведения аудитов сложных промышленных объектов – аэропортовых комплексов // Труды СПИИРАН. 2014. Вып. 6. С. 72-94.
17. Лившиц И.И. Методика выполнения комплексных аудитов промышленных объектов для обеспечения эффективного внедрения систем энергоменеджмента // Энергобезопасность и энергосбережение. 2015. Вып. 3. С. 10-15.
18. Лившиц И.И. Формирование концепции мгновенных аудитов информационной безопасности // Труды СПИИРАН. 2015. Вып. 6. С. 272 – 300.
19. Андрианова Е.Г., Мельников С.В., Раев В.К. Диссипация и энтропия в физических и информационных системах. Фундаментальные исследования. 2015. Вып. 8. С. 233 – 238
20. Кудж С.А., Цветков В.Я. Особенности развития направлений информатики // Перспективы науки и образования. 2013. Вып. 6. С. 11.
21. Маркин А.А., Мельников С.В. Философский и естественнонаучный аспекты понятия информационной энтропии // Труды российской научной конференции «Инновационные стратегии развития науки, техники и общества», Минобрнауки РФ, МГТУ МИРЭА. М., 2014. С. 98–102.

УДК 004.94

АНАЛИЗ ТРЕБОВАНИЙ К ОЦЕНКЕ ДОВЕРИЯ КРИТИЧНЫХ ОБЪЕКТОВ НА БАЗЕ СОВРЕМЕННЫХ СТАНДАРТОВ ISO

Лившиц Илья Иосифович¹, Малиов Владимир Викторович²

¹ Санкт-Петербургский национальный исследовательский университет
Российская Федерация, 197101, Санкт-Петербург, Кронверкский пр., 49

² УО "Центр повышения квалификации руководящих работников и специалистов" Департамента
охраны МВД Республики Беларусь,
223030 Минский р-н, Горанский с/с, р-н д. Горани,
emails: Livshitz.il@yandex.ru, malvvv104@mail.ru

Аннотация: В статье рассматриваются результаты революции в области ИТ, произошедшей в конце XIX века, среди которых отмечен следующий: вопросы информационной безопасности (ИБ) практически полностью утратили самостоятельность и стали органичной и неотъемлемой частью ИТ. Соответственно, возросла значимость корректного определения сущностей, подлежащих защите, и именуемых активами в нотации стандарта ISO 27001. В работе рассмотрены несколько примеров несуществующих (или мнимых) активов, для которых применяется термин – «токсичный актив». Выявление таких активов очень важно для формирования требований к оценке доверия критичных объектов на базе современных стандартов ISO. Отмечается необходимость создания в России национальной, сбалансированной и самодостаточной индустрии ИТ, которая от базиса до самого верхнего слоя надстройки будет «пронизана» функциями безопасности.

Ключевые слова: система управления, система менеджмента информационной безопасности; активы; аудит.

THE ANALYSIS OF REQUIREMENTS FOR ASSESSMENT OF CRITICAL OBJECTS BASED ON MODERN ISO STANDARDS

Livshitz Ilya ¹, Malikov Vladimir ²

¹ University of Information Technologies, Mechanics and Optics
Kronverkskiy prospekt, 49, St. Petersburg, 197101, Russia

² "Center of improvement of professional skill of executives and specialists" of the Interior Ministry
Department of the Republic of Belarus
Gorany, Goransky distr., Minsk, 223030, Belarus
emails: Livshitz.il@yandex.ru, malvvv104@mail.ru

Abstract: The IT revolution, which had been in the XIX century, had a very interesting consequence. During this revolution the IT-security almost completely lost its independence and become an organic and integral part of IT. Respectively, increased the importance of correct determination of entities to be protected and referred to as assets in the notation of ISO 27001. The paper considers several examples of non-existent (or imaginary) assets, which introduced the term "toxic asset". It is noted that it is necessary to create in Russia a national full-length, balanced and self-sustaining IT industry, which from the basis to the top layer of the add-in should be "riddled" with security features.

Keywords: *Management system, IT-Security management system; Asset; Audit.*

Введение. Статья появилась под впечатлением от документа Организации по безопасности и сотрудничеству в Европе (ОБСЕ) «Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства» (далее – Руководство) [1]. Одна деталь Руководства заставила задуматься о целесообразности дополнения широко используемого в мире информационных технологий (далее – ИТ) понятия актива, еще одной характеристикой – токсичностью. Заметим, что мир финансов, в свое время утративший видение меры и получавший проблемы нестабильных инвестиций, ввел общее понятие «токсичного» актива. Токсичность актива, безусловно, величина относительная, т.е. со временем может изменяться (интересующихся точными примерами классификации и базовыми процессами управления активами просят ознакомиться со стандартами ISO серии 27000 или их аналогами ГОСТ Р ИСО) [2 – 5].

Революция в области ИТ, произошедшая в конце XIX века за рубежом, имела одно весьма интересное следствие. В ходе революции вопросы информационной безопасности (далее – ИБ) практически полностью утратили самостоятельность и стали органичной и неотъемлемой частью ИТ [6 – 8]. Данный тезис подтверждается многими фактами из зарубежной практики: это и структура организаций, их процессы, и практика взаимодействий организаций [9, 10]. Поскольку сегодня общее понятие «ИТ» органично включают в себя вопросы ИБ, то далее уместно говорить предметно не только о токсичности активов, но и о влиянии токсичных активов на ИБ.

Документы 90-х годов представляют несколько утратившими актуальность. ИТ являются чрезвычайно динамичным направлением, в котором все меняется быстро и непрерывно. Соответственно, самые актуальные документы – это документация производителей на компоненты систем обработки информации (далее – СОИ). За ними стараются «успеть» международные стандарты и нормативные документы государств, имеющих под своей юрисдикцией развитую индустрию ИТ. В последнее время наблюдается переход к сертификации средств защиты в соответствии с ГОСТ 15408 [11 – 13]. ГОСТ 15408 абсолютно адекватный документ, являющийся переводом международных стандартов ISO/IEC серии 15408. В реальной СОИ вероятность преодоления защиты не равна нулю, и для того чтобы связать вероятность такого события с последующим ущербом давно используют понятия рисков ИБ (например, ранее Guide 73, позже ISO 27005). В мире для организаций уже созданы реестры рисков общепринятых «отраслевых» форматов (Basel, SOLAS-74, ISO 31000, IATA).

Необходимо безусловно обеспечить единообразие и прозрачность процедур оценки соответствия требованиям ИБ, для чего необходимо внести изменения в нормативно-правовые акты по техническому регулированию. В целях обеспечения процедур оценки соответствия, предлагается признать целесообразным использование для данных целей установленных как ГОСТ Р актуальных международных документов:

ГОСТ Р ИСО/МЭК серии 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»;

ГОСТ Р ИСО/МЭК серии 27000 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности».

Использование вышеперечисленных документов обеспечит единство шкал и методов оценки соответствия с зарубежными центрами компетенций в области ИТ, что позволит объективно, в сопоставимых измеряемых величинах, оценивать степень соответствия российских ИТ мировому уровню (кстати, это уже делают в «Лаборатории Касперского» в AV-TEST).

Заключение. Навык распознавания токсичных активов в области ИТ и очистки от них может существенно улучшить показатели устойчивости организации в России. Необходимо признать

неизбежность того, что вопросы ИБ должны практически полностью утратить иллюзорную самостоятельность и стать неотъемлемой частью ИТ. Предлагается пересмотреть практикуемое в раздельное «выращивание» ИБ и ИТ и обеспечить формирования требований к оценке доверия критичных объектов на базе современных стандартов ИСО.

СПИСОК ЛИТЕРАТУРЫ

1. Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства (<http://www.osce.org/ru/atu/110472?download=true>)
2. ISO/IEC 27000:2014. Information technology — Security techniques — Information security management systems — Overview and vocabulary, International Organization for Standardization, 2014. — 31 pages.
3. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements, International Organization for Standardization, 2013. — 23 pages.
4. ISO/IEC 27004:2009. Information technology — Security techniques — Information security management — Measurement, International Organization for Standardization, 2009. — 55 pages.
5. ISO/IEC 27005:2011. Information technology — Security techniques — Information security risk management, International Organization for Standardization, 2011. — 68 pages.
6. Лившиц И.И. Практическая оценка результативности СМИБ в соответствии с требованиями различных систем стандартизации: ИСО 27001 и СТО Газпром / Лившиц И.И., Полещук А.В. // Труды СПИИРАН. — 2015. — № 3. — С. 33 — 44.
7. Лившиц И.И. Подходы к решению проблемы учета потерь в интегрированных системах менеджмента // Информатизация и Связь. — 2013, № 1. — С. 57 — 62.
8. Лившиц И.И. Подходы к применению модели интегрированной системы менеджмента для проведения аудитов сложных промышленных объектов — аэропортовых комплексов // Труды СПИИРАН. — 2014, № 6. — С. 72 — 94.
9. Шишкин В.М., Юсупов Р.М. Доктрина информационной безопасности Российской Федерации — опыт количественного моделирования // Труды СПИИРАН. Вып. 1, т. 1. - СПб: СПИИРАН, 2002.
10. Юсупов Р. М., Шишкин В. М. О некоторых противоречиях в решении проблем информационной безопасности // Труды СПИИРАН. Вып. 6. — СПб.: Наука, 2008. С. 39–59.
11. ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель». 2012.
12. ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности». 2013
13. ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности». 2013

УДК 004.94

АНАЛИЗ ВЛИЯНИЯ РИСК-ОРИЕНТИРОВАННЫХ СТАНДАРТОВ НА ОБЕСПЕЧЕНИЕ ИБ ОБЪЕКТОВ КРИТИЧНОЙ ИНФРАСТРУКТУРЫ

Лившиц Илья Иосифович¹, Маликов Владимир Викторович²

¹ Санкт-Петербургский национальный исследовательский университет,
Российская Федерация, 197101, Санкт-Петербург, Кронверкский пр., 49

² УО "Центр повышения квалификации руководящих работников и специалистов" Департамента
охраны МВД Республики Беларусь,
223030 Минский р-н, Горанский с/с, р-н д. Горани,
emails: Livshitz.il@yandex.ru, malvvv104@mail.ru

Аннотация: В статье рассмотрена проблема оценки влияния современных риск-ориентированных стандартов для обеспечения безопасности и защищенности критичных и сложных промышленных объектов (СлПО). Основное внимание уделено обеспечению цикла PDCA для процессов обеспечения безопасности СлПО, в том числе – информационной безопасности (ИБ). Приведены практические примеры формирования унифицированной системы оценки безопасности СлПО для топливно-энергетического комплекса (ТЭК) на основании приказов ФСТЭК и современных стандартов ISO.

Ключевые слова: информационная безопасность, стандарт, система менеджмента информационной безопасности; сложный промышленный объект; активы.

ANALYSIS OF THE IMPACT OF RISK-BASED STANDARDS FOR IT-SECURITY provision for an CRITICAL INFRASTRUCTURE OBJECTS

Livshitz Ilya ¹, Malikov Vladimir ²

¹ University of Information Technologies, Mechanics and Optics
Kronverkskiy prospekt, 49, St. Petersburg, 197101, Russia

² "Center of improvement of professional skill of executives and specialists" of the Interior Ministry
Department of the Republic of Belarus
Gorany, Goransky distr., Minsk, 223030, Belarus
emails: Livshitz.il@yandex.ru, malvvv104@mail.ru

Abstract: This issue discusses the problem of assessing the impact of modern risk-oriented standards to ensure the safety and security of Complex Industrial Facilities (CIF). The main attention is paid to ensure the PDCA-cycle for general security processes of CIF, including IT-security. The practical examples of the

formation of a unified system of safety CIF assessment for the fuel and energy objects on the basis both Russian FSTEC and modern ISO standards.

Keywords: *IT-Security, Standard, IT-Security management system; Complex Industrial Facilities Asset.*

Введение. В настоящее время проблема формирования требований для обеспечения безопасности СлПО ТЭК является актуальной для специалистов в области обеспечения ИБ. Для лиц, принимающих решения (ЛПР) важно унифицировать совокупность требований, принятых на законодательном уровне: Федеральные законы, приказы ФСТЭК и дополнительно применять современные стандарты ISO, прежде всего ISO серии 27001 и «целевой» стандарт для энергетики ISO 50001, которые совместно формируют методологическую основу обеспечения ИБ для СлПО ТЭК.

Отметим, что в классическом труде Н. Винера по теории кибернетики отмечается: «Для получения приемлемых результатов в приемлемое время необходимо довести до максимума скорость элементарных процессов и добиться, чтобы течение этих процессов не прерывалось существенно более медленными шагами». Для выполнения требований нормативных документов и стандартов ISO предлагается далее применять обобщенный термин СлПО, под которым будем понимать «технический объект, несанкционированное изменение штатного режима функционирования которого, связанное с нарушением свойств ИБ, может привести к угрозе техногенных катастроф с необратимыми последствиями».

В любой системе менеджмента одним из важнейших вопросов является вопрос корректного выявления перечня активов (в нотации ISO 27000 – “asset”), для которых требуют обеспечить защиту от актов незаконного вмешательства. Для ТЭК проблему выявления и защиты критически важных промышленных объектов возможно сопоставить с общей проблемой выявления и защиты ценных для бизнеса активов СлПО в СМИБ и/или ИСМ. В стандартах ISO изложена четкая логика данного процесса – выделенная совокупность ценных (критичных) активов, намеченных ЛПР к защите в составе СМИБ объектов ТЭК, требует определенных ресурсов (временных, технических, персонал) для оценки уязвимостей, анализа соответствующих угроз, формирования файла рисков и плана обработки рисков. Однако на объектах ТЭК требуется принятие решений в режиме, близком к режиму реального времени. Пример явно завышенного времени выполнения процесса показан в работе Л. Кини и Х. Райфа, когда ЛПР для обдумывания различных альтернатив может потребоваться неделя.

На основании сформированного перечня активов, подлежащих защите, на следующем шаге определяется перечень уязвимостей и угроз, для противодействия применяются определенные меры (средства) обеспечения ИБ (в нотации ISO 27000 – “control”). Конечной целью применения мер (средств) обеспечения ИБ является снижение потенциального ущерба (потерь) в отношении выбранных активов СлПО ТЭК до приемлемой меры (уровня риска), установленной ЛПР. Для формирования перечня угроз рекомендуется использовать совместно Приложение «В» стандарта ISO 27005 и Приказ ФСТЭК № 31. В качестве возможных критериев, используемых для определения ценности актива, могут быть выбраны: исходная (балансовая) стоимость, стоимость замены (воссоздания) актива в случае реализации неблагоприятного сценария акта незаконного вмешательства (события риска ИБ), или дополнительная ценность (например, ценность репутации и политических рисков).

В ст. 9 Приказа ФСТЭК № 31 определено, что паспорт, признанный по результатам актуализации подлежащим замене и утратившим силу, хранится в порядке, установленном субъектом ТЭК, в течение 25 лет. Это требование также соответствует требованиям, соответственно, п. 9.3 в ISO 27001 и п. 4.7 в ISO 50001 по анализу со стороны руководства (“Management Review”). В тоже время в постановлениях Правительства не отражены в явном виде требования к обеспечению полного цикла управления рисками для организаций ТЭК. Также не предусмотрена оценка остаточного риска (“Residual risk”), которая позволяет дополнительно оценить уровень оценки защищенности активов СлПО ТЭК после применения выбранных мер (средств) обеспечения ИБ и определенного перечня рисков. Это обстоятельство может быть компенсировано как применением стандартов ISO, например, серии 27001, где требование менеджмента рисков установлено в явном виде, так и созданием ИСМ – с теми же требованиями и/или дополнительным внедрением «целевого стандарта» ISO серии 31000.

Требования по выполнению проверок (аудитов) активов СлПО ТЭК установлены, соответственно, в п. 9.2 в ISO 27001 и п. 4.6.3 ISO 50001. Наиболее важные проверки на объектах ТЭК установлены Приказом ФСТЭК № 31 и, дополнительно ISO 27001. Отметим, что в Приказе ФСТЭК № 31 многократно отмечается важная роль ISO 27001 (даны прямые ссылки, соответственно, на п.п. 13.4 и 15.2). Предложенный методический подход позволяет «мягко» преобразовать существующую систему к требованиям СМИБ и обеспечить результативное проведение различных аудитов и мониторинга состояния СлПО, находящегося под воздействием угроз нарушения ИБ. Методика основана на преобразовании базовой системы и учете требований по идентификации всех групп активов в соответствии с требованиями к СМИБ на базе стандартов ISO серии 27001 и серии 27005. Учет активов в соответствии с требованиями стандарта ISO серии 27001 позволит привнести в СМИБ управляемость по единым целям, измеримых в терминах бизнеса, что позволит выполнять в

дальнейшем интеграцию с другими системами менеджмента. Соответственно, для СМИБ могут быть применены соответствующие количественные метрики как доказательства «полезности» для бизнеса.

Заключение. Процесс формирования требований к защищенности СлПО ТЭК рекомендуется реализовать на базе системы современных нормативных документов (ФСТЭК) и стандартов ISO серии 27001 и ISO серии 50001. Предлагаемый подход позволит обеспечить необходимый уровень обеспечения безопасности СлПО, в том числе уровень ИБ, адекватный современным требованиям к оценке угроз, анализу уязвимостей и менеджмента рисков на объектах ТЭК.

СПИСОК ЛИТЕРАТУРЫ

1. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements, International Organization for Standardization, 2013. – 23 pages.
2. ISO/IEC 27004:2009. Information technology – Security techniques – Information security management – Measurement, International Organization for Standardization, 2009. – 55 pages.
3. ISO/IEC 27005:2011. Information technology – Security techniques – Information security risk management, International Organization for Standardization, 2011. – 68 pages.
4. Лившиц И.И. Практическая оценка результативности СМИБ в соответствии с требованиями различных систем стандартизации: ИСО 27001 и СТО Газпром / Лившиц И.И., Полещук А.В. // Труды СПИИРАН. – 2015. – № 3. – С. 33 – 44.

УДК 004.72

ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ, ИХ РАЗВИТИЕ

Михайленко Евгений Иванович

Акционерное общество «Научно-производственное объединение «Импульс»,
Россия, Санкт-Петербург, ул. Киришская, 2,
emails: eimihailenko@yandex.ru

Аннотация: В статье рассмотрены телекоммуникационные технологии в критических инфраструктурах и их развитие.

Ключевые слова: телекоммуникационные технологии; программно-определяемые сети - SDN.

TELECOMMUNICATION TECHNOLOGIES IN CRITICAL INFRASTRUCTURES, THEIR DEVELOPMENT

Mihailenko Evgeny

Joint-stock company "Research-and-production union "Impuls",
Russia, St. Petersburg, Kirichskay str. 2,
emails: eimihailenko@yandex.ru

Abstract: The article presents telecommunication technology in critical infrastructures and their development.

Keywords: telecommunication technology; *Software Defined Networking* — SDN.

Введение. Системы критических инфраструктур, в соответствии с предъявляемыми к ним требованиями, должны осуществлять безопасный информационный обмен с использованием ресурсов телекоммуникационных сетей связи. Телекоммуникационные сети связи общего пользования является составной частью единого информационного пространства общей автоматизированной системы управления и базируется на элементах специальных систем связи, а также на транспортных ресурсах, арендованных у операторов связи единой системы электросвязи (ЕСЭ) России.

В настоящее время актуальными направлениями развития телекоммуникационных сетей связи являются:

- цифровизация транспортной сети связи и сетей доступа, создание интегрированной цифровой транспортной сети на основе волоконно-оптических SDH/WDM/DWDM и VSAT-технологий;
- расширение номенклатуры предоставляемых услуг и повышение их качества;
- интеграция служб и услуг на основе создания широкополосных сетей связи с интеграцией служб с применением технологий MPLS;
- создание интеллектуальных сетей и сетей связи следующего поколения (NGN).

В целом данные направления развития свидетельствуют о поэтапном переходе от построения узкоспециализированных выделенных сетей связи к цифровым перспективным сетям связи (ПСС) с пакетной коммутацией. В общем случае построение ПСС за счёт унификации сетевых решений обеспечивает:

- предоставление и интеграцию широкого спектра услуг с требуемым качеством обслуживания;
- гибкость и адаптацию к изменению уровня требований пользователей к объёму, скорости и качеству доставки информации, а также к появлению требований на предоставление новых видов услуг;
- минимизацию затрат на развитие и эксплуатацию сети.

Вместе с тем построение ПСС требует новых подходов к вопросам обеспечения качества обслуживания при совместной передаче трафика различных служб, особенно в условиях ограниченных сетевых ресурсов и обеспечения безопасности информации.

АСУ территориально распределенными объектами имеют ряд общих особенностей, которые позволяют выделить для исследования объект – АСУ критических инфраструктур (АСУ КИ), и на его базе провести обоснованный анализ и синтез ее телекоммуникационной сети. Как правило, в АСУ КИ значительная часть элементов управления (ЭУ) являются подвижными объектами (ПО). Необходимость обеспечения высокой динамики управления различными ПО в современных изменяющихся условиях требует совершенствования как АСУ КИ в целом, так и ее сети связи, являющейся технической основой управления.

Актуальным и приоритетным направлением развития элементов АСУ КИ становится всесторонняя интеграция и повышение уровня взаимодействия на основе создаваемого единого информационно-разведывательного пространства (ЕИРП) и единого информационно-управляющего пространства (ЕИУП) элементов управления за счет реализации сетеориентированного подхода и интеграции оружия и его носителей, систем управления, связи и навигации, средств разведки и обеспечения на любом театре военных действий. Системообразующим элементом сетеориентированного подхода являются телекоммуникационные сети (ТКС).

Однако сегодня имеется ряд проблемных вопросов в направлении создания ТКС и систем, действующих на принципах сетецентрического управления (СЦУ). Это, прежде всего, реализация сильносвязного пространства с многочисленными взаимоувязанными средствами сете- и каналообразования, выстроенного по принципам их иерархий с сильно развитыми вертикальными и горизонтальными межвидовыми связями ЕИРП КИ.

Для реализации принципов СЦУ необходима широкополосная высокоскоростная транспортная сеть, при этом широкополосная связность пространства должна доходить до мобильного высокоскоростного объекта. Главным принципом этой структуры становится обеспечение постоянной связи между любыми потребителями, в любое время, в любом месте, в любой обстановке.

При этом современные инфокоммуникационные технологии работают на фундаменте, заложенном полвека назад. Перспективная телекоммуникационная среда должна строиться как сеть с коммутацией пакетов на базе перспективного стека протоколов, используя технологию, получившую название программно-определяемых сетей и виртуализации сетевых функций (SDN и NFV). В общем случае SDN/NFV – это сеть передачи данных, в которой уровень управления отделен от сетевых устройств передачи данных и реализуется программно на базе стандартных аппаратных платформ. Появление данной технологии обязано всевозрастающей производительности процессоров общего назначения, достигшей при решении специфических сетевых задач аналогичных показателей специализированных вычислителей на фоне более высокой стоимости последних. Это заставило радикально пересмотреть основные подходы к дизайну аппаратных платформ и перейти от традиционной практики создания дорогостоящего «специализированного монолитного комплекса», в котором отдельные компоненты глубоко интегрированы между собой, к разработке модульных платформ с относительно независимыми компонентами. В новой модели основной функционал и добавленную стоимость телекоммуникационного оборудования будет определять программное обеспечение, что в значительной степени снижает барьеры выхода на этот рынок для российских компаний и во многом уравнивает их возможности в борьбе с зарубежными конкурентами. При этом важным направлением является импортозамещение. Импортозамещение—это совокупность мер, имеющих своей целью создание, всестороннее обеспечение продвижения востребованных на рынке конкурентоспособных по цене и качеству и диверсифицированных с точки зрения разработки и производства образцов техники. Под диверсифицированным в данном случае понимается технологический процесс разработки и производства оборудования на основе кооперационных связей, в том числе международных, гарантирующий необходимый уровень его защищенности от рисков информационной безопасности и технологической независимости от зарубежных поставщиков.

СПИСОК ЛИТЕРАТУРЫ

1. Давыдов А.Е. Перспективные направления развития радиоэлектронной отрасли в области телекоммуникационного оборудования // Сборник «Связь в Вооружённых Силах Российской Федерации»
2. RFC 7426: SDN: Layers and Architecture Terminology, January 2015.

УДК 004.75

ПРОТОКОЛ МАРШРУТИЗАЦИИ В БЕСПРОВОДНОЙ СЕТИ

Молокович Игорь Аркадьевич

Акционерное общество «Научно-производственное объединение «Импульс»,
Россия, Санкт-Петербург, ул. Киришская, 2,
emails: molokovich@mail.ru

Аннотация: В статье рассмотрен гибридный протокол маршрутизации в беспроводной сети, имеющей стационарную и подвижные компоненты.

Ключевые слова: гибридный протокол маршрутизации; беспроводная сеть.

PROTOCOL ROUTING IN WIRELESS NETWORK

Molokovich Igor

Joint-stock company "Research-and-production union "Impuls",
Russia, St. Petersburg, Kirichskay str. 2,
emails: molokovich@mail.ru

Abstract: The article presents hybrid protocol routing in *wireless network*, having stationary and mobile component.

Keywords: *hybrid protocol routing; wireless network.*

Введение. В беспроводных сетях могут быть мобильны не только рабочие станции, но и сами маршрутизаторы. В таком случае узел состоит из маршрутизатора и хоста одновременно, они даже могут быть совмещены в пределах одного устройства. Кроме того, топология таких сетей постоянно меняется, а с ней меняется и предпочтительность (и даже реализуемость) путей.

Такие сети являются подклассом беспроводных сетей, это так называемые сети MANET (Mobile Ad Hoc NETworks) – сети без предварительной инфраструктуры, с изменяющейся из-за подвижности узлов топологией [1], [2]. Каждый узел в мобильной ad hoc сети работает одновременно подобно конечной системе и маршрутизатору.

Особенности беспроводных сетей приводят к тому, что протоколы и технические решения, используемые в классических проводных сетях, например, централизованная маршрутизация с иерархией заранее назначенных маршрутизаторов, в мобильных сетях без предварительной инфраструктуры, с изменяющейся из-за подвижности узлов топологией оказываются неэффективными и не обеспечивают нужную производительность.

Одной из ключевых задач в многошаговых беспроводных сетях является задача поиска маршрута между двумя станциями (задача маршрутизации). Протоколы маршрутизации, работая на сетевом уровне, не взаимодействуют с канальным уровнем. Таким образом, им недоступна информация о вероятности искажения пакетов помехами и коллизиями, о свойствах сигнально-кодированных конструкций, о методе доступа к каналу и параметрах механизма повтора непринятых пакетов. Следовательно, эти протоколы не могут определить вероятность успешной передачи пакета по соединению, а также пропускную способность соединения, а маршруты, найденные с их помощью, обладают малой пропускной способностью и часто пропадают. Кроме того, протоколы маршрутизации зачастую не учитывают особенности беспроводной среды.

В многошаговой беспроводной сети возможны явления, которые не наблюдаются в одношаговых сетях, например, эффект скрытых станций. Наличие скрытых станций приводит к существенному снижению скорости передачи в сети, а в некоторых случаях – к блокировке соединений между станциями, что может приводить к нарушению связности сети.

Для повышения эффективности протоколов маршрутизации в беспроводных сетях их необходимо снабдить информацией о канальном уровне, например, о качестве соединений с помощью метрики маршрутизации. Другой подход заключается в решении задачи маршрутизации на канальном уровне.

При разработке большинства алгоритмов оптимизации основное внимание уделялось вопросам взаимодействия распределенных узлов для формирования маршрута, при этом использовались простейшие критерии оценки оптимальности полученного маршрута. В большинстве протоколов таким критерием является длина маршрута, т.е. число узлов, задействованных при передаче информации. В отдельных случаях также учитывалась максимальная пропускная способность связей между двумя узлами. В идеальном случае оценка оптимальности на основе данных параметров позволяет выбрать наилучший маршрут, однако не учитывает ряд параметров, которые присутствуют в сетях при практическом применении. Для беспроводных сетей такими параметрами могут быть учет уровня сигнала для канала между двумя узлами и параметры текущей загрузки отдельных фрагментов маршрута.

В настоящее время существует два основных подхода к построению алгоритмов и протоколов маршрутизации для динамических сетей [3].

Первый из них является превентивным, т.к. алгоритмы данного типа поддерживают маршруты ко всем узлам сети, используя периодический обмен служебными сообщениями. Как следствие, увеличение скорости изменения топологии приводит к соответствующему росту служебного трафика, что, в свою очередь, влечет неоправданный расход процессорного времени, энергоресурса, пропускной способности. Альтернативный подход заключается в организации маршрутов «по требованию», когда по ним действительно нужно передавать данные. В этом случае нет необходимости поддерживать в рабочем состоянии все возможные маршруты, однако в определенных ситуациях затраты на поиск пути становятся сопоставимыми с объемом передаваемой информации, а возникающие задержки – неприемлемо высокими.

По принципу поиска маршрута выделяют три класса протоколов: проактивные, реактивные и комбинированные [2], [4].

И проактивные, и реактивные протоколы маршрутизации имеют свои преимущества и недостатки, которые делают их пригодными для определенных условий функционирования сети. Так как протоколы проактивной маршрутизации обрабатывают информацию так, что она сразу же доступна, задержка перед отправкой пакета является минимальной. Напротив, протоколам реактивной маршрутизации необходимо сначала определить маршрут, что может привести к значительной задержке, если информация не доступна в кэше.

Кроме того, реактивная процедура поиска маршрута требует значительного контроля трафика из-за лавинного распространения служебных пакетов. Это вместе с большой задержкой определения маршрута может сделать реактивную маршрутизацию менее пригодной для трафика, критичного к времени.

Тем не менее, объем трафика может быть уменьшен за счет использования схемы обслуживания маршрута. Чисто активные схемы используют большую часть пропускной способности для поддержания актуальности маршрутной информации. Вследствие быстрой мобильности узлов обновления маршрутов могут быть более частыми, чем запросы маршрутизации, и большая часть информации о маршрутизации никогда не используется. Некоторая часть из дефицитной пропускной способности, таким образом, тратится впустую.

Лучшим решением было бы использовать различные протоколы маршрутизации для различных частей сети. Реактивный протокол можно использовать для контроля динамического изменения топологии и подвижности узлов. Активный протокол лучше подошел бы для статических узлов, чтобы обеспечить быструю доступность маршрутов.

Заключение. Предлагается гибридный протокол маршрутизации в беспроводной сети, использующий реактивный протокол маршрутизации для контроля динамического изменения топологии и подвижности узлов и активный протокол маршрутизации для статических узлов, обеспечивающий быструю доступность маршрутов.

СПИСОК ЛИТЕРАТУРЫ

2. Метелев А.П., Чистяков А.В., Жолобов А.Н. Протоколы маршрутизации в беспроводных самоорганизующихся сетях // Вестник Нижегородского университета им. Н.И. Лобачевского. 2013, № 3 (1). С. 75-78.
3. Орлов В.Г., Фадеев А.Н. Протоколы маршрутизации в мобильных AD-HOC-сетях // Материалы Международной научно-технической конференции. 2012. С. 208 – 212.
4. Припутин В.С., Жанкевич А.О. Исследование эффекта масштабируемости в беспроводных ad-hoc сетях // Телекоммуникации и транспорт. 2010, № 11. С. 23-25.
5. Маркин В.Г., Рыжкова А.Г. Протоколы маршрутизации в мобильных самоорганизующихся сетях // Теория и техника радиосвязи. 2013, № 4. С. 48-56.

УДК 004.75

АЛГОРИТМ УПРАВЛЕНИЯ РЕЖИМАМИ ОБМЕНА ДАННЫМИ В САМООРГАНИЗУЮЩЕЙСЯ СЕТИ ДЕКАМЕТРОВОЙ РАДИОСВЯЗИ

Путилин Алексей Николаевич

Акционерное общество «Научно-производственное объединение «Импульс»,
Россия, Санкт-Петербург, ул. Киришская, 2,
email: a.n.putilin@yandex.ru.ru

Аннотация: В статье рассмотрен алгоритм управления режимами обмена данными в самоорганизующейся сети декаметровой радиосвязи.

Ключевые слова: алгоритм управления, сеть декаметровой радиосвязи.

DATA EXCHANGE PROCEDURE CONTROL ALGORITHM INTO SELF-ORGANIZING HF RADIO NET

Putilin Aleksey

Joint-stock company "Research-and-production union "Impuls",
Russia, St. Petersburg, Kirichskay str. 2,
email: a.n.putilin@yandex.ru.ru

Abstract: The article presents data exchange procedure control algorithm into self-organizing HF radio net.

Keywords: control algorithm, HF radio net.

Рассматриваются способы построения сети декаметровой радиосвязи, основанной на принципах:

- полной децентрализации алгоритмов управления,
- работы на едином пакете частот,
- возможности ретрансляции чужих пакетов данными станциями сети.

Сеть создаётся для функционирования в условиях преднамеренного подавления. Все станции используют режим псевдослучайного переключения рабочих частот (ППРЧ). Предполагается оснащение станций сети многоканальными приёмниками. Приёмники постоянно отслеживают

состояния различных направлений связи по результатам попыток информационного обмена как собственных, так и чужих. По данным наблюдениям динамически станциями радиосвязи вычисляются априорные вероятности успешной передачи пакетов данных в различных направлениях для различных режимов передачи и приёма пакетов данных.

Под режимом передачи пакета данных станцией радиосвязи понимается выбор управляемых параметров работы радиостанции в зависимости от

- адресов вызывающего и отвечающего абонентов,
- текущего состояния матрицы априорных вероятностей успешной передачи пакетов,
- ограничений по выбору управляемых параметров радиостанции, обусловленных составом каналаобразующего оборудования на каждой конкретной станции.

Управляемые параметры радиостанции определяют порядок использования всех видов ресурса используемого ею для организации информационного обмена:

- пространственного (направление приёмной и передающей характеристик направленности),
- энергетического (мощность передаваемого сигнала),
- частотного (пакет одновременно используемых в направлении связи частот и их номиналы),
- временного (сигнально-кодовая конструкция и способ повышения достоверности).

При необходимости передачи пакетов данных станция выбирает режим передачи для каждого пакета отдельно, с использованием процедуры рандомизации выбора режима. Веса рандомизации определяются текущим состоянием матрицы априорных вероятностей успешной передачи.

Ожидаемые эффекты от использования данного протокола:

- приближение производительности рассматриваемой сети к границе потенциально достижимой производительности в условиях преднамеренного подавления,
- существенное снижение средней мощности радиостанций сети за счёт использования маршрутизации пакетов данных,
- возможность вторичного использования одних и тех же частот на пространственно разнесённых участках радиосети,
- существенное увеличение производительности рассматриваемой сети по сравнению с радиосетью, построенной на прямых связях,
- увеличение структурной надёжности сети радиосвязи,
- увеличение защищённости станций рассматриваемой сети от обнаружения.

Основные задачи дальнейшего исследования:

- моделирование функционирования радиостанции рассматриваемой сети,
- моделирование функционирования рассматриваемой сети в условиях преднамеренного подавления,
- сравнительная оценка границ производительности сетей с различными алгоритмами управления в рассматриваемых условиях,
- оценка устойчивости и сходимости предлагаемых алгоритмов управления,
- выработка предложений по их реализации.

СПИСОК ЛИТЕРАТУРЫ

1. Путилин А.Н. Радиосистемы с множественным доступом. - СПб.: ВАС, 1998, 148 с.
2. Путилин А.Н. Модель взаимодействия линии радиосвязи и станции радиоэлектронного подавления // Труды юбилейной XIII Санкт-Петербургской международной конференции «Региональная информатика (РИ-2012)», СПОИСУ. – СПб, 2013, стр. 196-207.
3. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетевых войнах начала XXI века. – СПб, 2017, 546 с.

УДК 004.9

МЕТОД МОДЕРНИЗАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ ЭКОЛОГИЧЕСКОГО МОНИТОРИНГА

Рябовая Валентина Олеговна

Севастопольский государственный университет «СевГУ»,
Россия, Севастополь, ул. Университетская, 33,
email: valentina_rb@mail.ru

Аннотация: В статье рассматривается метод модернизации систем экологического мониторинга на основе двух подходов, учитывающих требования, возникшие в процессе функционирования системы. Для оценки и отбора вариантов ИСЭМ применяется критериальный подход.

Ключевые слова: информационная система, модернизация, мониторинг, критериальный подход

MODERNIZATION METHOD INFORMATION SYSTEMS OF ENVIRONMENTAL MONITORING

Ryabovaya Valentina

The Sevastopol State University "SevGU",
Russia, Sevastopol, University st.,33
email: valentina_rb@mail.ru

Abstract: The article considers the method of modernization of environmental monitoring systems based on two approaches that take into account the requirements that arose in the process of the system functioning. A criterial approach is used to evaluate and select ISEM options.

Keywords: information system, modernization, monitoring, criterial approach.

Введение. Мониторинг и прогноз состояния экологической обстановки в Крымском регионе были и остаются важными научно-практическими задачами. Существующие для их решения информационные системы экологического мониторинга (ИСЭМ) требуют постоянного совершенствования (модернизации).

Основными причинами, требующими модернизации ИСЭМ, являются: моральное устаревание информационной системы (информационных технологий, пользовательских и программных интерфейсов, используемых в составе ИС); физическое устаревание информационной системы (износ её аппаратных компонентов); причины организационного характера (связанные с окружением ИС, бизнес-процессами предприятия, пользователями системы, реализующими новые требования к ИС). Одной из основных проблем модернизации ИСЭМ является то, что она определена на концептуальном уровне и не зависит от какой-то одной программной технологии. При возникновении новых требований к данным мониторинга и к работе самой системы возможны проблемы структурного характера. Реализация некоторого требования, с ограничением по времени, может привести к преобразованию структуры системы с последующей её модернизацией.

Для решения этой задачи и выбора единственного варианта решения применяются два основных подхода [1]. Сущность первого – исключить из анализа заведомо неприемлемые варианты решений, тем самым сузив множество возможных альтернативных решений, второго – использовать приемы и способы приведения многоцелевой задачи к типовой задаче с одним критерием. Функционирование ИСЭМ осуществляется с учетом реализации двух видов требований: к данным (точность, качество) и к самой системе (функции и ресурсы). Это связано с модернизацией двух типов: по структуре и по функциям системы. Для оценки и отбора вариантов ИСЭМ применяется критериальный подход. Критериями, участвующими в отборе, являются: достоверность информации, своевременность реализации требований к системе и к данным мониторинга, надежность ИСЭМ. В представленной многокритериальной задаче, для аналитической оценки эффективности иерархических структур, применяется метод вложенных скалярных сверток [2].

Заключение. Преимущество представленного метода, по сравнению с существующими – более полный учет данных, минимизация функциональной избыточности элементов системы в составе одного решения по мере наращивания задач.

СПИСОК ЛИТЕРАТУРЫ

1. Доронина Ю.В. Рябовая В.О. Метод структурно-функционального синтеза в задачах реструктуризации систем экологического мониторинга // Международный научно-технический журнал «Проблемы управления и информатики». 2013. № 6. С. 79-89.
2. Воронин А.Н. Вложенные скалярные свертки векторного критерия // Проблемы управления и информатики. – 2003. – № 5. – С. 10-21.

УДК 004.75

ПРОГРАММНАЯ МОДЕЛЬ ЦИФРОВОЙ СИСТЕМЫ СВЯЗИ В КВ ДИАПАЗОНЕ С ПСЕВДОСЛУЧАЙНОЙ ПЕРЕСТРОЙКОЙ РАБОЧЕЙ ЧАСТОТЫ

Шаптала Василий Сергеевич, Секунов Николай Юрьевич
АО «Научно-производственное объединение «Импульс»,
Россия, Санкт-Петербург, ул. Киришская, д.2,
emails: nsekunov@yandex.ru, vasily.shaptala@gmail.com

Аннотация: В статье описана программная модель цифровой системы связи.

Ключевые слова: программная модель; ППРЧ.

SOFTWARE MODEL OF DIGITAL COMMUNICATION IN SHORT WAVES RANGE WITH FREQUENCY-HOPPING SPREAD SPECTRUM

Shaptala Vasily
Joint-stock company "Research-and-production union "Impuls",
Russia, St. Petersburg, Kirichskay str. 2,
emails: nsekunov@yandex.ru, vasily.shaptala@gmail.com

Abstract: This article presents a software model of digital communication.

Keywords: software model; FHSS.

При методе ППРЧ расширение спектра сигнала осуществляется скачкообразным изменением рабочей (несущей) частоты в пределах выделенного для работы системы связи набора частот, что позволяет эффективно противостоять как искусственным, так и естественным помехам. Исследуемая

система связи характеризуется высокой вычислительной сложностью, поэтому при ее реализации на отечественной элементной базе, и, особенно, на процессорах, предназначенных для работы в условиях внешних мешающих факторов, требуется алгоритмическая оптимизация.

Программная модель позволяет провести алгоритмическую оптимизацию, а кроссплатформенный код, полученный в результате моделирования, может быть с минимальными затратами перенесен на целевую платформу. Дополнительно программная модель существенно упрощает реализацию и проверку межсетевого взаимодействия абонентов, алгоритмов адаптации и повышения достоверности передаваемой информации, а используемая в составе модели многоканальная модель КВ канала, выполненная в соответствии с рекомендацией ITU-R F1487, позволяет оценить работу системы без дорогостоящих трассовых испытаний.

Реализованная модель системы связи использует трехуровневую архитектуру:

- интерфейс пользователя;
- динамическая библиотека;
- статические библиотеки кроссплатформенного кода модели канала и цифровой системы связи;
- и работает под управлением операционной системы Windows.

СПИСОК ЛИТЕРАТУРЫ

1. Припутин В.С., Жанкевич А.О. Исследование эффекта масштабируемости в беспроводных ad-hoc сетях // Телекоммуникации и транспорт. 2010, № 11. С. 23-25.



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТРАНСПОРТНЫХ СИСТЕМ

УДК 004.7

ТЕХНОЛОГИЙ СЕТЕЙ НОВОГО ПОКОЛЕНИЯ (NGN) И ИХ ПРИМЕНЕНИЕ НА ВОДНОМ ТРАНСПОРТЕ

Алексеев Андрей Дмитриевич, Ерисова Анастасия Дмитриевна, Малов Сергей Сергеевич
Петербургский государственный университет морского и речного флота имени адмирала С.О.
Макарова, Россия, Санкт-Петербург, ул. Двинская, 5/7
emails: xoytlo@ya.ru, andalexs@ya.ru, malov_sergey@mail.ru

Аннотация: В статье рассмотрены сети нового поколения (NGN) и возможность их реализации на водном транспорте.

Ключевые слова: *сети нового поколения (NGN); водный транспорт.*

NEXT GENERATION NETWORK TECHNOLOGIES AND THEIR APPLICATION FOR THE WATER TRANSPORT

Andrey Alexeev, Anastasiya Erisova, Malov Sergey
Admiral Makarov State University of Maritime and Inland Shipping Russia, Saint-Petersburg, Dvinskaya st.,
5/7
emails: xoytlo@ya.ru, andalexs@ya.ru, malov_sergey@mail.ru

Abstract: The article presents Next Generation Network (NGN) and application of it for the water transport.

Keywords: *Next Generation Network (NGN); water transport.*

Введение. Водный транспорт, как и многие другие виды транспорта, использует множество различных средств передачи данных. Например, одними из самых распространенных на водном транспорте видов передачи данных являются такие как сети: передачи данных и телематических служб, управления движением судов, аудио-видео и диспетчерской связи. Также огромную роль в навигации и связи морского судна с сушей играет радиосвязь. Эти и многие другие средства обмена информации значительно упрощают жизнь людям, но для того чтобы ими управлять, усовершенствовать и делать их безопаснее необходимо создавать отдельные системы, и данные действия необходимо повторять для каждого вида связи. Чтобы уйти от этого и создать единую систему управления, которая должна упростить обеспечение безопасности и управление всеми видами связи, были выполнены разработки нового вида сетей. О сетях нового поколения (NGN) начинали говорить ещё в 2004 году и прогнозы были обнадеживающими, но все новости о внедрении или попытка внедрения NGN в России заканчиваются 2008 годом. В настоящее время технологии сетей нового поколения активно развиваются за рубежом. NGN подразумевает объединение систем сотовой связи (GSM, GPRS, UMTS и др.), систем связи беспроводного доступа Wi-Fi (IEEE 802.11), систем кабельного телевидения, телефонии, спутниковых и других информационных систем. Рассмотрим возможности применения технологий сетей нового поколения (NGN) на водном транспорте. Состав задач, решаемых сетями нового поколения (NGN) заключается в следующем:

Централизация управления всеми видами информационно-коммуникационных сетей, то есть создание возможности управления сетями управления движения судов, навигации, сетями диспетчерской связи и другими из единого центра координации действий;

Повышение защищенности сетей от различного рода информационных атак по средствам создания общего для всех сетей, но при этом разделенного сетевого шлюза и многочисленных, но независимых друг от друга сетевых экранов;

Создание обширной информационной структуры, охватывающей всю область применения, а не отдельные её разделы.

На сегодняшний день развитие инфокоммуникационных услуг в большей своей степени ограничено рамками Интернета, который реализуется через традиционные сети. Но даже сейчас Интернет все еще не в состоянии предоставлять услуги, отвечающие требованиям, предъявляемым современным обществом. Требуется решить ряд задач, связанных с эффективным управлением информационными ресурсами, с увеличением функциональности сетей. Это говорит о том, что

необходимость в развитии современных сетей и протоколов построения сетей существует и возрастает.

Протокол IP и технология MPLS - это интернет технологии на которых основывается NGN. Сегодня существует несколько подходов к построению сетей IP-телефонии: H.323, SIP и MGCP.

Построение сети. Для создания сети нового поколения нужно иметь следующие ресурсы:

Протоколы и транспортные каналы связи, которые бы обеспечивали поддержку и доставку информации любого формата;

Оборудование необходимое для поддержки и доступа к NGN как с суши, так и с воды;

Устройства, которые обеспечивали бы связь всех подсистем, входящих в водный транспорт. [1]

Структура сети NGN. Перейдем к структуре сети нового поколения, для более полного понимания того, как же построить мультизадачную сеть.

Принцип построения и работы NGN отличается от работающих на данный момент моделей сетей. Руководящей идеей сетей нового поколения является сближение существующих сетей и технологий, таких как IP или мобильные сети. Это процесс слияния всевозможных технологий и услуг связи для того, чтобы сделать работу имеющегося оборудования более обширной и многофункциональной.

Наиболее подходящей, для начала реализации NGN, на данный момент технологией является TCP/IP, из которого можно взять за основу протокол IP.

Протокол IP удовлетворяет требованию к скорости передачи данных и благодаря технологии VoIP отвечает требованию к передаче информации, чувствительной к задержке по времени, то есть аудио и видео связь в настоящем времени. Но данный протокол не гарантирует качественную доставку информации. Исходя из вышеперечисленного, наиболее развитым можно считать многопротокольную технологию MPLS, которая использует коммутацию с помощью меток. [2,3]

Для управления сетями доступа была создана система управления функциями сетей доступа, которая предназначена для решения следующих задач:

- обеспечение технической эксплуатации и технического обслуживания;
- управление сетью и конфигурирование;
- координация с системой управления транспортной сетью;
- обнаружение и индикация неисправностей;
- сбор и обработка статистических данных;
- управление ресурсами и безопасностью.

Перечисленные технологии обеспечивают доступ к ресурсам сети и передачу данных разного вида, но не обеспечивают требуемого качества доставки информации, так как не устанавливают соединений для доставки данных, чувствительных к задержке и потерям.

Наиболее подходящими решениями здесь можно считать протоколы сигнализации и стандартизованные протоколы и интерфейсы:

RSVP (Reservation Protocol) – протокол резервирования ресурсов;

Q.931 (протокол сетевого уровня абонентской цифровой системы сигнализации);

V5.2 (интерфейс N-ISDN, позволяющий предоставить пользователям удаленный фиксированный и мобильный доступ к ресурсам). [4]

Эффекты, которые можно ожидать при внедрении решений сетей NGN на водном транспорте:

- повышение безопасности сети водного транспорта в целом и отдельных услуг;
- повышение конкурентоспособности сети водного транспорта;
- повышение эффективности использования сети на большом количестве станций как клиентских, так и серверных;
- повышение готовности сети к мгновенному ответу на запросы различного характера.

Заключение. Проанализировав информацию о способе построения и плюсах данной системы, а так же столкнувшись с проблемами перехода к NGN, а именно: отсутствие достаточного количества инвестиций; отсутствие единой политики перехода к NGN; единого мнения по поводу путей и темпов построения NGN; отсутствие или незаконченность стандартов, описывающих все аспекты NGN; отсутствие полной линейки оборудования для NGN; несовместимость оборудования разных изготовителей (риски по поводу масштабируемости и сохранения инвестиций). Можно прийти к выводу, что в будущем данная технология может стать уникальной и получить распространения за счет преимуществ, рассмотренных выше, но в настоящее время из-за нехватки специализированного оборудования, квалифицированных кадров и отсутствия доработанной системы стандартов ее применение стоит под вопросом, т.к. ее реализация требует больших материальных затрат.

СПИСОК ЛИТЕРАТУРЫ

1. Jingming Li Salina, Pascal Salina. Next Generation Networks: Perspectives and Potentials - 2007.
2. Битнер В. И., Михайлова Ц. Ц. Сети нового поколения – NGN. Учебное пособие для вузов. –М.: Горячая линия – Телеком, 2011.
3. Kevin Foster, Office of the Group CTO, British Telecommunications plc (BT), UKITU-T / ATIS Workshop «Next Generation Technology and Standardization»
4. Онлайн библиотека [Электронный ресурс]: Электрон. журн. -<http://www.tinlib.ru/> - [Россия] 2017г

УДК 658

ИСПОЛЬЗОВАНИЕ ЦВЕТНЫХ СЕТЕЙ ПЕТРИ ПРИ МОДЕЛИРОВАНИИ ПОДСИСТЕМ ПРЕДПРИЯТИЯ

Барашков Александр Валерьевич, Петровский Дмитрий Валерьевич
Высшая школа экономики
Россия, г. Санкт-Петербург, Кантемировская ул., 3, корп.1.
email: abarashkov@hse.ru, dpetrovskij@hse.ru.

Аннотация: В данной статье рассматривается применение цветных сетей Петри для анализа двухкомпонентной системы внутри предприятия логистической системы. Анализировалось совместное поведение следующих подсистем предприятия: системы электронного документооборота и товародвижения. Создана модель, основанная на цветных сетях Петри, проведена симуляция поведения данной системы с заданными параметрами. Получены численные показатели работы данной системы, могущие служить для её оптимизации.

Ключевые слова: информационная безопасность, логистические системы, бизнес-процессы, сети Петри, моделирование.

USING OF COLOURED PETRI NETS AT THE MODELING OF THE ENTERPRISE SUBSYSTEMS

Barashkov Alexander, Petrovskii Dmitrii
Higher School of Economics
Russia, Saint Petersburg, Kantemirovskaya st 3, b 1.
email: abarashkov@hse.ru, dpetrovskij@hse.ru.

Abstract: This article considers the application of coloured Petri nets for the analysis of a two-component system within a logistics enterprise. The joint behaviour of the following subsystems of the enterprise was analysed: the EDI system and goods circulation. A model based on coloured Petri nets was created, a simulation of the behaviour of this system with given parameters was carried out. Numerical performance indicators of this system are obtained, which can serve to optimize it.

Keywords: information security, logistics systems, business processes, Petri nets, modelling.

Введение. В современной экономике всё больше становится очевидной необходимость применения электронных информационных систем и систем документооборота в деятельности компаний, в особенности в логистических системах компаний, где количество документов может достигать наибольшего количества по отношению к остальным видам деятельности компании. Однако, применение информационных систем может приводить к возникновению рисков, связанных с надёжностью их работы, что приводит к необходимости исследования данного вопроса.

Одним из наиболее актуальных подходов к данному вопросу является моделирование и анализ модели различных систем компании в связке с информационной системой их обслуживающей. Логистическая система в связке с информационной системой представляет из себя динамическую дискретную систему, что приводит к тому, что одним из актуальных методов моделирования таких систем является применение цветных сетей Петри.

Аппарат сетей Петри зарекомендовал себя в широком спектре областей исследований и практики как удобный способ моделирования работы систем, изучение данных моделей в аналитическом виде и дальнейшей оптимизации работы системы, если это возможно в данной области.

Цель данной работы – показать возможности применения цветных сетей Петри при моделировании взаимодействия информационной системы предприятия с остальными подсистемами компании. Эта цель достигается построением наглядной модели транспортной системы и информационной системы, обслуживающей деятельность по транспортировке.

Представлены основные показатели модели, выявлены свойства этой логистической системы. Проведён тест функционирования работы системы при заданных параметрах её работы, а также при заданных параметрах возможных сбоев при передаче информации, необходимой для дальнейшего продвижения товаров в системе.

В итоге, можно увидеть, что при достаточной оптимизации логистических операций, невысокая надёжность работы информационной системы может сильно повлиять на работу логистической системы, что приводит к необходимости либо повышения надёжности информационной системы, либо подстройки функционирования логистической системы к имеющейся надёжности процессов по передаче информации.

Таким образом можно увидеть пример применения аппарата цветных сетей Петри для моделирования работы логистической системы при том с описанием свойств такого рода систем и учётом особенностей протекания параллельных процессов в системе. Цветные сети Петри имеют высокий потенциал в применении при анализе и оптимизации функционирования компаний как экономических систем, так как их аппарат позволяет моделировать различные подсистемы внутри

компании, следовательно, применение сетей Петри с целью анализа существующих компаний или цепей поставок позволяет существенно оптимизировать ключевые параметры их функционирования.

Немаловажным фактором является то, что цветные сети Петри применимы на всех этапах оптимизации логистических систем, начиная от дизайна логистической системы и, включая моделирования существующих цепей поставок.

Но, с другой стороны, использование ЦСП сопряжено с рядом трудностей, связанных с вычислительной сложностью при симуляции созданных моделей, а также с невозможностью анализа данных сетей в аналитическом виде. Данные трудности могут оказывать серьезное влияние на принятие решения об их использовании, однако, аппарат сетей Петри продолжает развиваться и по сей день, что приводит к созданию методов и способов, нивелирующих негативные последствия от вышеописанных трудностей,

Так, был разработан целый комплекс методов, упрощающих работу с сетями Петри. Во-первых, были созданы методы редукции цветных сетей Петри, которые исключают из сети бесконечные циклы, группируют ряд узлов, объединяя их в один и так-далее, данные методы позволяют существенно упростить сложность вычислений, что делает более доступной симуляцию сложных сетей [1]. Во-вторых, благодаря доказанному изоморфизму ЦСП по отношению к СП [2] были разработаны методы сведения цветных сетей к монохромным за конечное число шагов. Это позволило производить анализ сложных цветных сетей также эффективно, как и в случае с монохромными. Кроме этого, разрабатывается ряд алгоритмов численного анализа ЦСП по средствам симуляции [3], их увеличенная точность позволяет без ущерба для производительности операций осуществлять их анализ также эффективно, как и при их аналитическом анализе.

Закключение. Таким образом, применение ЦСП для анализа сложных систем несет большое количество преимуществ. Во-первых, становится возможным создавать модели, наиболее полно отражающие моделируемый объект. Во-вторых, анализ ЦСП может проводится сразу рядом способов, варьирующимися в зависимости от целей исследования, что повышает их универсальность.

СПИСОК ЛИТЕРАТУРЫ:

1. Viswanadham, N., & Raghavan, N. R. S. (2000). Performance analysis and design of supply chains: a Petri net approach. Journal of the Operational Research Society, 51(10), 1158–1169. <https://doi.org/10.1057/palgrave.jors.2600063>
2. Wells, L. (2002). Performance Analysis using Coloured Petri Nets, 1–164. Retrieved from papers3://publication/uuid/AB064166-C22F-4118-8679-18D93D5A9F66
3. Evangelista, S., Haddad, S., & Pradat-Peyre, J. F. (2005). Syntactical colored petri nets reductions. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 3707 LNCS, 202–216. https://doi.org/10.1007/11562948_17

УДК 004.94

МОДЕЛЬ ТРАНСПОРТНОГО ПОТОКА

Бариков Леонид Николаевич, Галанина Валентина Александровна
Санкт-Петербургский университет Аэрокосмического приборостроения,
Россия, Санкт-Петербург, ул. Б.Морская, д. 67
emails: lnbarikov@gmail.com, va_gal@rambler.ru

Аннотация: В статье рассмотрены вопросы компьютерного моделирования транспортной системы. Предлагается модель транспортного потока, в которой моделирование производится на микроуровне, то есть моделируется поведение отдельных транспортных средств в потоке с учетом их характеристик. Такой подход позволяет моделировать дорожную ситуацию наиболее приближенно к действительности и, кроме того, исследовать влияние различных внешних факторов на безопасность движения.

Ключевые слова: моделирование; транспортный поток; безопасность движения; модель микроуровня

MODEL OF TRAFFIC FLOW

Barikov Leonid, Galanina Valentina
Saint-Petersburg state University of Aerospace instrumentation,
Russia, Saint-Petersburg, Bolshaya Morskaya str. 67
emails: lnbarikov@gmail.com, va_gal@rambler.ru

Abstract: the article considers the issues of computer modeling of the transport system. A model of traffic flow in which the modeling is performed at micro level is suggested, what means that the behavior of individual vehicles in the flow based on their characteristics is simulated. This approach allows modeling the traffic situation as closely as possible to reality and, in addition, to investigate the influence of various external factors on traffic safety.

Key words: modeling; traffic flow; traffic safety; micro level model

Рассматривается модель транспортного потока, ориентированная в основном на учёт поведения автомобилей в узловых точках дорожной сети (на перекрёстках).

В качестве варианта выбора модели транспортного потока с точки зрения уровня детализации реализована модель микроуровня. Такая модель позволяет учитывать реальные характеристики отдельных автомобилей (в частности, динамические) и рассматривать каждое транспортное средство не как составляющую потока транспортных средств (на уровне макромоделей), а как отдельный элемент дорожной ситуации. Разработанная модель позволяет выявить конкретные механизмы возникновения пробок на дорогах с учётом поведения автомобилей между узловыми точками, а также исследовать влияние таких угроз безопасности движения как: несанкционированный доступ к периферийному оборудованию (светофоры, датчики, экраны отображения) системы управления движением; несанкционированный доступ к данным с целью их искажения или подмены.

Учитываются варианты движения транспортных средств без смены полосы движения, со сменой полосы движения, наличие регулируемых перекрёстков с конкретными схемами переключения светофоров, а также нерегулируемых перекрёстков равнозначных и неравнозначных дорог.

Описывается программное обеспечение модели транспортного потока, в состав которого входит база данных, программный интерфейс управления моделированием и графический интерфейс пользователя.

Основная задача разработанного пользовательского интерфейса заключается в обеспечении управления системой моделирования транспортного потока и доступа к полученным результатам моделирования. Интерфейс реализует логику управления процессом моделирования. Интерфейс реализован как web-приложение и фактически является сервером удалённых процедур формирования исходных данных для моделирования конкретной транспортной ситуации и получения сведений о результатах моделирования.

Для разработки был использован локальный сервер Denwer, при запуске которого был создан виртуальный диск для хранения файлов проектов моделей.

В качестве СУБД использована MySQL версия 5.5.25 с панелью администрирования phpAdmin версии 3.5.1. Для доступа к базе данных использовано расширение MySQLi (MySQL Improved).

СПИСОК ЛИТЕРАТУРЫ

1. Б.Я. Советов, В.В. Цехановский. Информационные технологии: теоретические основы. Учебное пособие. СПб: Лань, 2017 г. 444 с.

УДК 519.876.5:519.6:004.357

СКРЫТАЯ ПЕРЕДАЧА ДАННЫХ ЧЕРЕЗ ВОЗДУШНЫЙ АУДИОКАНАЛ С ПОМОЩЬЮ АУДИОСИГНАЛОВ, ПОДВЕРГНУТЫХ ЦИФРОВОМУ МАРКИРОВАНИЮ

Гофман Максим Викторович, Корниенко Анатолий Адамович, Кустов Владимир Николаевич,
Мирончиков Евгений Тимофеевич, Никитин Александр Борисович
Петербургский государственный университет путей сообщения Императора Александра I,
Россия, Санкт-Петербург, Московский пр., 9

Аннотация: В этой работе развивается методика цифрового маркирования аудиосигналов, ориентированная на передачу данных через воздушный аудиоканал. Внедряемый цифровой маркер занимает весь слышимый частотный диапазон. Цифровой маркер кодирует один бит информации. Решение о значении переданного бита выносится на основании знака центрального значения взаимно-корреляционной функции. Предлагаются две методики построения цифрового маркера. Обе специально ориентированы на частотные свойства обычных аудиосигналов. Невысокая вычислительная сложность предлагаемого метода маркирования позволяет использовать его для беспроводного обмена информацией между обычными смартфонами. Методика позволяет выполнять цифровое маркирование как речевых, так и музыкальных аудиосигналов без появления каких-либо заметно слышимых артефактов. Информация внедряется в виде маркера в частотную область аудиосигнала путём амплитудной модуляции его частотных составляющих. Эта работа снабжена результатами имитационного моделирования и натурных экспериментов, подтверждающих применимость методики для скрытой передачи данных через воздушный аудиоканал.

Ключевые слова: цифровой маркер, аудиосигнал, скрытая передача данных, воздушный аудиоканал, акустическая связь, стегоаудиосигнал

COVERT AIR AUDIO DATA TRANSMISSION VIA DIGITAL WATERMARKED AUDIO SIGNALS

Gofman Maksim, Kornienko Anatolij, Kustov Vladimir, Mironchikov Evgenij, Nikitin Aleksandr
Emperor Alexander I St. Petersburg State Transport University, Russian Federation,
Saint Petersburg, 9 Moskovsky pr.

Abstract: The article presents a digital audio watermarking method for air audio data transmission. The digital watermark occupies whole frequency range of audio signal. The digital watermark encodes one bit of

information. A decision about transmitted bit is based on a sign of center value of mutual correlation function. Two methods to design the digital audio watermark is presented. Low complexity of presented methods of digital audio watermarking makes them useful for smartphones. The method can be used in digital audio watermarking of both speech and music. An information is embedded via the digital watermark in frequency domain of host audio via amplitude modulation of frequency constituents. The paper includes results of simulation modeling and natural experiments.

Keywords: *digital watermark, audio signal, covert data transmission, air audio channel, acoustic telecommunication, steganography audio signal*

Введение. Процедура цифрового маркирования аудиосигналов лежит во основе системы скрытой передачи данных с помощью таких сигналов. Она включает в себя три этапа: этап построения маркера, этап внедрения маркера в аудиосигнал и этап выделения маркера из маркированного аудиосигнала. Цифровое маркирование аудиосигнала предполагает создание из информации такого маркера и его внедрение в аудиосигнал таким образом, что становится возможным его выделить даже при условии, что маркированный аудиосигнал или стегоаудиосигнал подвергнется преднамеренной или ненамеренной атаке, то-есть процедура цифрового маркирования должна быть робастной к некоторого рода воздействиям.

Частым приложением процедуры цифрового маркирования является защита авторских прав при распространении аудио, видео и изображений в цифровых форматах. В этих случаях внедряемый сигнал либо сообщает получателю какие-то авторские данные или лицензионные ограничения, либо предотвращает или запрещает неавторизованное копирование. Например, внедряемый сигнал может представлять собой «отпечаток пальца», который уникальным образом идентифицирует первоначального покупателя защищённой авторскими правами работы. Если незаконные копии этой работы были сделаны, то все эти копии будут содержать в себе такой отпечаток пальца, идентифицируя владельца исходного цифрового объекта. Другой пример приложения – внедряемый сигнал может либо разрешать, либо запрещать копирование некоторому копирующему устройству, которое проверяет внедряемый сигнал перед выполнением процедуры дубликации. Или иначе, согласованный с неким стандартом проигрыватель может проверить наличие маркера перед тем как решать проигрывать ли диск или нет.

Акустическая связь в основном разрабатывается для подводной связи в сенсорных сетях для осуществления мониторинга водных экосистем и состояния нефтяных вышек. Схему цифровой модуляции, которую используют для связи с помощью электромагнитных волн, например, фазовую или частотную манипуляцию, можно применить для акустической связи, чтобы выполнить модуляцию звуковых сигналов. Подводная акустическая связь требует приёмопередатчики, способные работать в водной среде, что зачастую означает использование специальных динамиков и микрофонов, то-есть гидрофонов.

С другой стороны, воздушная акустическая связь доставляет информацию с помощью воздушных звуковых волн. В зависимости от рабочей частотной полосы воздушная акустическая связь может использоваться, как обычный смартфон, который способен проигрывать/записывать аудио (до 22 кГц), так и ультразвуковой приёмопередатчик (свыше 22 кГц). Поэтому любое устройство, оснащённое аудио интерфейсом может быть использовано как устройство аудиосвязи. Таким образом появляется альтернативный интерфейс беспроводной связи между смарт-устройствами, помимо имеющихся Wi-Fi и Bluetooth, которые часто выключены, для экономии батареи и/или предотвращения нежелательных подключений. Воздушная акустическая связь в диапазоне до 22 кГц исследуется в работах [1-4].

В этой работе развивается подход, описанный в статье [5], использующий тоекратное кодирование передаваемых информационных битов перед передачей через воздушный аудиоканал. Предложенный в работе [5] подход показал свою устойчивость к искажающим влияниям воздушного аудиоканала. Однако, он требовал использования двух различных последовательностей для кодирования значений бита информации. Особенностью развиваемого подхода является кодирование битов в знаке корреляционной функции, что уменьшает требуемое количество последовательностей до одной, и тем самым увеличивает потенциально возможную скорость передачи информации. Процедура передачи состоит из трёх этапов. Первый этап состоит в получении кодового слова, соответствующего передаваемому биту – построение маркера. Второй – во внедрении этого кодового слова в аудиосигнал, в результате чего получается стегоаудиосигнал – маркированный аудиосигнал. А третий этап состоит в восстановлении переданного бита из стегоаудиосигнала, полученного после передачи через воздушный аудиоканал.

Заключение. В этой работе сформулированы свойства, которыми следует наделить скрываемую последовательность, чтобы повысить её робастность к искажающим влияниям воздушного аудиоканала, когда используется предлагаемый метод цифрового маркирования. Предложены способы построения последовательностей, обладающих подходящими свойствами. Способ детектирования наличия скрытого сигнала (цифрового маркера), предложенный в работе, является слепым, так как не требует знания приёмником скрывающего сигнала. Простота предлагаемого в этой работе метода скрытой передачи данных позволяет применять его в режиме реального времени без необходимости требовать от передатчика и приёмника значительной вычислительной мощности.

СПИСОК ЛИТЕРАТУРЫ

1. Lee H., Kim T. H., Choi J. W., Choi S. Chirp signal-based aerial acoustic communication for smart devices // IEEE Conference on Computer Communications (INFOCOM). – 2015. – pp. 2407-2415.
2. Nandakumar R., Chintalapudi K. K., Padmanabhan V., Venkatesan R. Dhvani: secure peer-to-peer acoustic NFC // ACM SIGCOMM Computer Communication Review. – 2013. Vol. 43. – № 4. – pp. 63–74.
4. Wang Q., Ren K., Zhou M., Lei T., Koutsonikolas D., Su L. Messages behind the sound: real-time hidden acoustic signal capture with smartphones // Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking. – ACM, 2016. – pp. 29-41.
5. Hanspach M., Goetz M. On covert acoustical mesh networks in air // Journal of Communications. – 2013. – Vol. 8. – № 11. – pp. 758 – 767
6. Гофман М.В. Методика скрытой передачи данных при связи через воздушный аудиоканал // Труды СПИИРАН. – 2017. – Вып. 51. – С. 97-122.

УДК 551.501.815.003.121

**МЕТОД ВОССТАНОВЛЕНИЯ ПРОФИЛЯ ВЕТРА ПО ОЦЕНКАМ ШИРИНЫ СПЕКТРА
РАДИОЛОКАЦИОННОГО СИГНАЛА**

Денисенков Дмитрий Анатольевич, Жуков Владимир Юрьевич, Щукин Георгий Георгиевич
Военно-космическая академия имени А.Ф.Можайского.
Россия, Санкт-Петербург, ул. Красного курсанта, 16.
emails: dimasden@yandex.ru, vuzhukov2002@list.ru, ggshchukin@mail.ru

Аннотация: В статье описывается разработанный авторами метод обнаружения и определения параметров сдвига ветра когерентным метеорологическим радиолокатором. Требуемая для этого информация извлекается из формируемых в штатном режиме работы карт пространственного распределения измеряемых параметров и не требует внесения каких-либо изменений в конструкцию радиолокатора или характеристики проводимых им обзоров.

Ключевые слова: *сдвиг ветра; ширина спектра сигнала; метеорологическая радиолокация.*

**METHOD OF RESTORING THE WIND PROFILE DUE TO SPECTER WIDTH ESTIMATION OF THE
RADAR SIGNAL**

Denisenkov Dmitriy, Zhukov Vladimir, Shukin Georgiy
Military Space Academy of A. Mozhaitskiy.
Russia, Saint- Petersburg, Krasniy kursant street, 16
emails: dimasden@yandex.ru, vuzhukov2002@list.ru, ggshchukin@mail.ru

Abstract: the authors describe their method of the wind shift detection and parameters identification by coherent meteorological radar. This method allow to get the information using created in regular mode maps of the measured parameters spatial spreading and do not require to make changes in the radar construction or in scan algorithms.

Keywords: *wind shift, width of signal spectrum, meteorological radiolocation*

Введение. Информация о вертикальном профиле ветра необходима для обеспечения безопасности летательных аппаратов. Для его оперативного определения в аэропортах и на космодромах устанавливают специальные устройства – профилометры. Как правило, их устанавливают парами, способными заменять друг друга в различных метеорологических условиях [1]. Наиболее распространено сочетание лидарного и радарного профилометров. Первый работает в условиях «чистой» атмосферы, второй – при наличии частиц (в основном, гидрометеоров) способных создавать достаточной величины отражения. Одновременно рядом, как правило, находится метеорологический радиолокатор, которому можно было бы передать функции радарного профилометра и тем сэкономить значительные средства. Однако характеристики такого радиолокатора определяются из условия выполнения им своих задач и не соответствуют требованиям, предъявляемым к профилометрам.

Основная часть. Авторами разработан метод, позволяющий извлекать информацию о вертикальном профиле ветра из данных, получаемых радиолокатором в штатном режиме работы, и не требующем внесения каких-либо изменений в конструкцию или характеристики обзоров. Исходным материалом при этом служат карты ширины спектра радиальных скоростей частиц. Появление в окружающем пространстве изменений скорости или направления ветра с высотой приводит к характерным пространственным распределениям данного параметра.

Для исследования последних была разработана модель получения радиолокатором упомянутых карт [2]. При этом окружающее пространство представлялось в виде трех слоев, характеризующихся различными параметрами: отражаемостью, вектором средней скорости и шириной спектра скоростей частиц, составляющих данный слой. В верхнем и нижнем слоях все параметры считались постоянными, в среднем же скорость и/или направление ветра изменялось с высотой по линейному закону.

Численное решение модели позволило выявить три основных варианта пространственного распределения ширины спектра сигнала, соответствующих трем возможным соотношениям линейных размеров элемента разрешения радиолокатора и толщины среднего слоя. В соответствии с тем, сколько слоев одновременно попадает внутрь элемента разрешения, они были названы трех-, двух- и однослойными.

Первый из них является основным, т.к. всегда может быть достигнут путем уменьшения угла места антенны и увеличением дальности наблюдения, и несет информацию о суммарном изменении ветра, вызванном его сдвигом по величине и по направлению. Характеризуется появлением областей аномально больших (от 6 м/с и более) значений ширины спектра, имеющих вид симметрично расположенных относительно радиолокатора двух дуг окружности.

Двухслойный вариант порождает появление на карте аномально больших значений ширины спектра в виде двух симметричных спиралей. Величина области их существования по координате азимута не превышает, как правило, 30 градусов. Между ними могут образовываться спирали малых (не более 1 м/с) значений параметра.

Для однослойной модели характерно появление на карте двух симметричных спиралей малых значений ширины спектра, существующих иногда на участках более 180 градусов по азимуту. Аномально широких спектров в данном случае не возникает.

Для получения практически значимых зависимостей величины изменения ветра с высотой и параметров пространственного распределения ширины спектра скоростей модель решалась аналитически [3]. Было показано, что при трехслойном варианте возможно определение абсолютной величины изменения вектора скорости частиц в среднем слое по всей его толщине. Для этого достаточно найти максимальное достигнутое значение параметра в области образовавшихся их аномально больших значений, а также средние значения ширины спектра в нижнем и верхнем слоях на дальности нахождения максимального значения. Толщина слоя считается равной линейному размеру элемента разрешения на дальности, предшествующей появлению аномально больших значений параметра.

Полученных оценок вполне достаточно для решения задачи обнаружения опасного сдвига ветра, являющейся важной при обеспечении полетов авиации. Если же необходимо разделить вклады, вносимые в общее изменение скорости частиц сдвигом ветра по величине и по направлению, надо добиться появления на карте ситуации, соответствующей двух- или однослойному варианту. Достичь этого можно простым поднятием антенны.

Полученные аналитические соотношения позволяют по скорости «завития» образующихся при этом спиралей рассчитать скорость изменения с высотой направления ветра. При этом предпочтителен именно однослойный вариант, при котором вращение спирали происходит с той же быстротой, что и вращение вектора скорости. В двухслойном же варианте спираль «завивается» примерно в четыре раза медленнее ветра.

Закключение. Таким образом, доказана возможность восстановления профиля ветра по данным обзоров метеорологического радиолокатора, работающего в штатном режиме. Правильность теоретических расчетов подтверждается рядом проведенных натурных экспериментов, давших положительный результат [4].

Особая ценность полученных результатов состоит в том, что на их основе может быть построен метод восстановления профиля ветра по данным некогерентного радиолокатора, что будет объектом следующих исследований авторов.

СПИСОК ЛИТЕРАТУРЫ

1. Жуков В.Ю., Шукин Г.Г. Современные проблемы метеорологической радиолокации. // Радиотехника и электроника, 2016, т.61, № 10, с. 927–939.
2. Денисенков Д.А., Жуков В.Ю. О влиянии сдвига ветра на пространственное распределение ширины спектра радиолокационного сигнала. // Радиотехнические и телекоммуникационные системы, 2016, №1, с. 5–14.
3. Д.А.Денисенков, В.Ю.Жуков. Обнаружение сдвига ветра на основе анализа карт ширины спектра сигнала, принимаемого метеорологическим радиолокатором. // Вестник Российского нового университета., 2015, вып.2, с. 10-13.
4. Денисенков Д.А., Жуков В.Ю., Сивак О.А., Шукин Г.Г. Исследование эффективности метода обнаружения сдвига ветра по оценкам ширины спектра радиолокационного сигнала. // Ученые записки РГМУ, 2016, № 42, с. 109–116.

УДК.629.5.06

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ ПОДСИСТЕМ СИСТЕМЫ ДИНАМИЧЕСКОГО ПОЗИЦИОНИРОВАНИЯ СУДНА ПОСРЕДСТВОМ АЛГОРИТМА ОПТИМАЛЬНОГО РАСПРЕДЕЛЕНИЯ УПОРОВ ДВИЖИТЕЛЬНО-РУЛЕВОГО КОМПЛЕКСА

Зайцев Алексей Николаевич¹, Азаров Михаил Михайлович²

¹ Государственный университет морского и речного флота имени адмирала С.О. Макарова
Россия, Санкт-Петербург, ул. Двинская, 5/7

² АО «Концерн «НПО «Аврора»
Россия, Санкт-Петербург, ул. Карбышева, 15
email: zalexnic@gmail.com

Аннотация: Рассмотрен эффективный способ повышения безопасности выполнения судном работ в режиме динамического позиционирования в условиях единичного отказа, а также комбинации единичного и второстепенных отказов, обусловленных как отказом приборов подсистем системы динамического позиционирования (СДП), так и отказом межсистемных информационных каналов или снижением качества обмена информацией.

Ключевые слова: система динамического позиционирования, отказ, алгоритм оптимального распределения, защита от перегрузки.

OPTIMAL THRUST ALLOCATION ALGORITHM FOR PROVIDING OF SAFETY DATA INTERACTION BETWEEN SUBSYSTEMS OF DYNAMICAL POSITIONING SYSTEM

Zaitsev Aleksey¹, Azarov Michael²

¹ Federal state educational Institution of higher education «Admiral Makarov State University of Maritime And Inland»

Russia, St. Petersburg, 5/7, Dvinskaya str.

² Aurora JSC,

Russia, St. Petersburg, 15, Karbysheva str.

email: zalexnic@gmail.com

Abstract. The article presents an effective way to provide more safe vessels operation in DP mode with single failure or sequence of failures in DP system caused by failures of subsystems set, data channels or decreased data signal quality.

Keywords: dynamical positioning system, failure, optimal thrust allocation algorithm, overload defence.

Введение. Производство работ судном в режиме динамического позиционирования (ДП) связано с повышенными рисками и последствиями при потере заданного местоположения. В зависимости от вида и сложности производимых работ к СДП предъявляются требования к оснащенности оборудованием и его надежности, установленные в классификациях различных Сертификационных обществ. В результате исследований отказов в СДП [4] установлен факт, что повышение класса СДП (по классификации ИМО [1, 2] с 2 до 3-го) не уменьшает вероятность отказа в ней. Множество факторов оказывают влияние на безопасность проведения работ в режиме ДП. Основными из них являются: надежность оборудования, входящего в состав подсистем СДП, уровень подготовки экипажа, качество планирования работ. Надежность оборудования традиционно обеспечивается за счет автоматизации и резервирования, а также разработкой соответствующих нормативных документов, устанавливающих требования к СДП и ее компонентам. Подготовка экипажа и качество планирования работ относятся к человеческому фактору и обеспечиваются соответствующими обучением и опытом персонала.

Анализ причин и последствий отказов в СДП. Причины потери заданного местоположения могут быть различны, а тяжесть последствий зависит от типа судна и вида производимых работ [3, 4, 5, 6]. Отказ в электроэнергетической системе (ЭЭС), например, отказ дизель-генератора (ДГ), может привести к перегрузке работающих ДГ при резерве мощности, недостаточном для обеспечения питанием судовых потребителей, главным образом движительно-рулевого комплекса (ДРК). Восстановление резерва мощности производится за счет подключения резервного ДГ. Однако, на его запуск и ввод в работу требуется время. Нельзя также исключать не включение в работу на сеть резервного ДГ. В таком случае время обеспечения достаточного резерва мощности увеличивается непредсказуемо. Перегрузка электростанции может привести к полному обесточиванию судна, потере заданного местоположения и управляемости. При отказе одного или нескольких технических средств (ТС) ДРК судно может потерять управляемость, что приведет к нарушению технологии производства работ. Динамическое перераспределение упоров ТС ДРК для компенсации дефицита упора, отказавшего ТС может привести к перегрузке оставшихся в работе ТС. Нередко [4] единичный отказ, определяемый как первичный, приводит к возникновению других отказов – второстепенных, которые также могут быть обусловлены человеческим фактором в том числе действиями экипажа по восстановлению работоспособности СДП.

Система управления ДП (СУ ДП) является *компонентом (подсистемой) системы ДП* и выполняет функции информационной интеграции *компонентов системы ДП*, вычислительные функции для расчета требуемых параметров ТС ДРК, функции взаимодействия с оператором. Таким образом, качество информации, поступающей в СУ ДП от сопрягаемых систем непосредственно оказывает влияние на качество управления судном. Отказ линии связи или недостоверность (низкое качество сигнала, обусловленное помехами) информации может привести к отказу в *компоненте* системы ДП, а также последующей серии отказов в других подсистемах, например, в ситуации, когда оператор ДП принимает неадекватные решения, вследствие некорректности (ложности) сигналов аварийно-предупредительной сигнализации (АПС), отображаемой на мониторах пультов управления СУ ДП.

Описание алгоритма. Рациональным решением проблемы сохранения заданного местоположения судна в условиях единичного отказа в СДП является использование функциональных возможностей СУ ДП в части информационного взаимодействия подсистем и внедрение в СУ ДП

алгоритма минимизации и оптимального распределения мощностей, потребляемых ТС ДРК. Задачей алгоритма является обеспечение минимального потребления мощности ДРК в условиях действия внешних воздействий (ветра, течения, волнения), а также наличия ограничений на процессы управления: отсутствия резерва мощности, отказами отдельных ТС ДРК, ДГ или их информационных каналов. Реконфигурация и изменение структуры распределения упоров должна выполняться автоматически, в том числе по аварийно-предупредительным сигналам от сопрягаемых с СУ ДП систем. При этом, должны быть обеспечены наименьшие отклонения от точки позиционирования, от заданного курса, потребление мощности ДРК в пределах доступной мощности ЭЭС. Таким образом, параллельно решается задача дополнительной защиты ЭЭС судна от перегрузки [7].

Структурно алгоритм минимизации и оптимального распределения мощностей, потребляемых ТС ДРК, представляет собой задачу математического программирования. Целевой функцией задачи является общая потребляемая ДРК мощность в виде квадратичной функции. Функции-ограничения представляют собой системы линейных (в ряде случаев линеаризованных) уравнений, выражающих: задание параметров работы ТС от регулятора СУ ДП, ограничение максимально возможных упоров ТС ДРК, ограничение мощности, потребляемой ТС ДРК, исходя из имеющегося резерва по мощности. Функции-ограничения на задание параметров работы ТС от регуляторов СУ ДП определяются системой линейных уравнений, связывающих заданные силы продольного и бокового движения и заданный момент с продольными и боковыми составляющими сил ТС ДРК. Функции-ограничения максимально возможных упоров ТС ДРК вводятся вследствие теоретической возможности превышения значением заданного регулятором СУ ДП упора максимально допустимого значения упора ТС ДРК. Функция-ограничение мощности, потребляемой ТС ДРК (определяемая располагаемым резервом мощности), вводится для защиты ЭЭС судна от перегрузки. Таким образом, решением оптимизационной задачи является нахождение минимума целевой функции при наличии указанных ограничений.

Функционирование алгоритма минимизации и оптимального распределения мощностей, потребляемых ТС ДРК, ограничивается временем, необходимым для запуска резервного оборудования и приведения СДП в состояние готовности обеспечения технологии проводимых работ.

СПИСОК ЛИТЕРАТУРЫ

1. IMO MSC/Circ. 645. International Maritime Organization. Guidelines For vessels with dynamic positioning systems, June 1994 – 17 стр.
2. IMO SSE2/13. Amendments to the guidelines for vessels with dynamic positioning (dp) systems (MSC/Circ.645), December 2014 – 25 стр.
3. IMCA M103 Rev. 3. Guidelines for The Design and Operation of Dynamically Positioned Vessels, February 2017 – 129 стр.
4. Фишер П. Анализ отказов систем динамического позиционирования [Электронный ресурс] / П. Фишер // Нефтегазовые технологии: научно-технический журнал. – 2006 – №8 – С. 30-33. – Режим доступа: <http://> (Дата обращения: 21.09.17)
5. Torstein I, Tor Johansen, Dynamic consequence analysis of marine electric power plant in dynamic positioning, AMOSNTNU, 2016.
6. Kristian S. Hauff. Analysis of Loss of Position Incidents for Dynamically Operated Vessels. Norwegian University of Science and Technology (NTNU), 2014
7. Азаров М.М. Постановка задачи минимизации и распределения потребляемых мощностей технических средств движительно-рулевого комплекса судна в системе динамического позиционирования / М.М. Азаров, А.Н. Зайцев // Системы управления и обработки информации: научн.-техн. сб./ АО «Концерн «НПО «Аврора», СПб. Вып. 4(35).

УДК 004.056

ОСОБЕННОСТИ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ УПРАВЛЕНИЯ ЕДИНЫМ ПАРКОВОЧНЫМ ПРОСТРАНСТВОМ

Зайцев Святослав Игоревич, Ильченко Лидия Михайловна

¹ Государственный университет морского и речного флота имени адмирала С.О. Макарова
Российская Федерация, 198035, г. Санкт-Петербург, ул. Двинская, 5/7

² Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики
Российская Федерация, 197101, Санкт-Петербург, Кронверкский пр., 49
email: Sunilink@yandex.ru, Lidiya9510@yandex.ru

Аннотация: В данной работе рассматриваются особенности построения системы защиты информации в автоматизированных системах управления единым парковочным пространством.

Ключевые слова: информационная безопасность, интеллектуальная дорожно-транспортная система, угрозы безопасности, средства защиты информации, автоматизированная система управления единым парковочным пространством.

PARTICULAR QUALITIES OF CONSTRUCTION OF INFORMATION PROTECTION SYSTEM IN INTELLECTUAL THE CONTROL SYSTEM OF THE UNIFIED PARKING SPACE

Zaytsev Svyatoslav, Ilchenko Lydia

¹ Admiral Makarov State University of Maritime and Inland Shipping
198035, Russia, St.Petersburg, Dvinskayast., 5/7

²Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics
197101, Russia, St. Petersburg, 49 Kronverksky Pr.
email: Sunilink@yandex.ru, Lidiya9510@yandex.ru

Abstract: in this paper we consider the construction of a system for protecting information in the intellectual the control system of the unified parking space.

Keywords: *information security, intellectual road and transport system, security threats, data protection facilities, intellectual the control system of the unified parking space.*

Введение. Автоматизированная система управления (далее – АСУ) единым парковочным пространством создана для предоставления в режиме реального времени всей необходимой информации о количестве и координатах свободных парковочных мест участникам дорожного движения, как водителям, так и операторам, позволяя производить оплату, бронирование стоянок, а также регистрацию времени стоянок на парковочных пространствах. Располагая этой информацией, можно осуществлять контроль парковок путем сопоставления числа занятых мест с количеством поступивших платежей, осуществленных через терминалы оплаты.

Мониторинг в режиме реального времени необходим на крупных транспортных узлах, где число автомобилей часто превышает пропускную способность дорог [6].

АСУ единым парковочным пространством предусматривает различные сервисы для оплаты парковочных мест: через sms-сообщения, через парковочный терминал, с помощью специальных мобильных приложений, а также с использованием сети Интернет – порталы [5].

АСУ единым парковочным пространством является полноценной информационно-коммуникационной технологической платформой с программным интерфейсом для осуществления взаимодействия с другими уровнями интеллектуальной дорожно-транспортной системы.

Ведущими функциями АСУ единым парковочным пространством являются:

Мониторинг занятых и свободных парковочных мест [2], [4].

Осуществление взаимодействия со службами экстренного реагирования.

Осуществление взаимодействия с обслуживающими организациями.

Обработка статистических данных, а также их предоставление сторонним системам.

Предоставление заинтересованным пользователям информации о наличии свободных парковочных мест, а также об изменениях тарифов в режиме реального времени.

Предоставление пользователям сервисов оплаты [3].

Системно-техническая характеристика АСУ единым парковочным пространством состоит из:

1. СУБД – физический сервер.
2. WEB-сервер взаимодействия – виртуальный сервер.
3. WEB-сервер взаимодействия мобильных приложений – виртуальный сервер.
4. VOIP-шлюз – виртуальный сервер.
5. Шлюз взаимодействия через SMS – виртуальный сервер.
6. Система биллинга – физический сервер.
7. АРМ администратора – персональный компьютер [1].

Определение класса защищенности АСУ единым парковочным пространством производится в соответствии с приказом ФСТЭК России от 14.03.2014 г. № 31, напрямую зависит от уровня значимости данных (УЗ), циркулирующих в АСУ.

Степень возможного ущерба для каждого из критериев:

- целостность – низкая степень ущерба;
- доступность – низкая степень ущерба;
- конфиденциальность – низкая степень ущерба.

Исходя из вышесказанного можно сделать вывод о том, что для АСУ единым парковочным пространством характерен третий уровень значимости (УЗ-3), а также третий класс защищенности (КЗ).

Для рассматриваемой системы класс защищенности определяется в соответствии с приказом ФСТЭК России от 14 марта 2014 г. № 31, и напрямую зависит от уровня значимости обрабатываемых данных, который прямо пропорционален возможному ущербу для каждого из свойств безопасности информации (целостности, доступности, конфиденциальности).

Степень возможного ущерба для АСУ наземного городского пассажирского транспорта: для целостности, доступности и конфиденциальности – низкая.

Исходя из вышеуказанных данных уровень значимости системы соответствует третьему (УЗ-3), а класс защищенности, в соответствии с таблицей в п.3 Приложения № 1 приказа ФСТЭК России от 14 марта 2014 г. № 31, соответствует третьему классу (КЗ).

Обеспечение защиты информации в АСУ наземного городского пассажирского транспорта достигается за счет комплексного подхода к организации системы защиты данных. Базовый набор мер представлен в приложении № 2 приказа ФСТЭК России от 14 марта 2014 г. № 31. Адаптивный набор мер формируется в результате оценки угроз информационной безопасности на базе составленной модели угроз. [8]

Как минимум, меры защиты должны обеспечивать минимизацию, либо полную ликвидацию угроз безопасности информации, источником которых является нарушитель с низким потенциалом.

В системе защиты должны быть реализованы следующие группы мер:

- идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ);
- управление доступом субъектов доступа к объектам доступа (УПД);
- ограничение программной среды (ОПС);
- защита машинных носителей информации (ЗНИ);
- регистрация событий безопасности (РСБ);
- антивирусная защита (АВЗ);
- обнаружение (предотвращение) вторжений (СОВ);
- контроль (анализ) защищенности информации (АНЗ);
- целостность автоматизированной системы управления и информации (ОЦЛ);
- доступность технических средств и информации (ОДТ);
- защита среды виртуализации (ЗСВ);
- защита технических средств и оборудования (ЗТС);
- защита автоматизированной системы и ее компонентов (ЗИС);
- безопасная разработка прикладного и специального программного обеспечения (ОБР);
- управление обновлениями программного обеспечения (ОПО);
- планирование мероприятий по обеспечению защиты информации (ПЛН);
- обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС);
- информирование и обучение персонала (ИПО);
- анализ угроз безопасности информации и рисков от их реализации (УБИ);
- выявление инцидентов и реагирование на них (управление инцидентами) (ИНЦ);
- управление конфигурацией автоматизированной системы управления и ее системы защиты (УКФ).

Исходя из анализа Реестра сертифицированных ФСТЭК России средств защиты информации и практики их применения, можно составить перечень необходимых и достаточных средств защиты:

- СЗИ от несанкционированного доступа (СЗИ от НСД) применимы для следующих групп мер: ИАФ, УПД, ОПС, РСБ, АНЗ, ОЦЛ, ЗИС, ОПО, ИНЦ;
- средств индивидуального межсетевое экранирования (МЭ) применимы для следующих групп мер: ИАФ, УПД, ОПС, РСБ, ЗСВ, ОЦЛ, ИНЦ;
- средств обнаружения вторжений применимы для следующих групп мер: УПД, РСБ, СОВ, АНЗ, ЗИС, ИНЦ;
- средств резервирования применимы для следующих групп мер: ОЦЛ, ОДТ, ЗИС, ДНС;
- средств антивирусной защиты информации (АВЗ) применимы для следующих групп мер: РСБ, АВЗ, ОЦЛ, ЗИС, ОПО, ИНЦ.

А также средства криптографической защиты информации (СКЗИ), сертифицированные Федеральной службой безопасности РФ (ФСБ России) применимы для следующих групп мер: РСБ, ОЦЛ, ЗИС, ИНЦ.

Кроме этого, необходимо применять ряд организационных мер.

Третий класс защищенности предъявляет следующие требования:

- средства вычислительной техники не ниже 5 класса;
- СЗИ не ниже 6 класса [7].

Заключение. Несмотря на аналогичность используемого программно-аппаратного комплекса в системах такого типа, при проектировании системы защиты информации необходим индивидуальный подход, основанный на комплексном анализе обрабатываемых данных, условиях обработки и актуальных угрозах в каждой отдельно взятой системе.

СПИСОК ЛИТЕРАТУРЫ

1. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. – М.: Горячая линия – Телеком, 2014. – 594 с.
2. Жанказиев, С.В. Интеллектуальные транспортные системы: учеб. пособие / – М.: МАДИ, 2016. – 120 с.
3. Ивченко Б.П., Мартыщенко Л.А., Монастырский М.Л. Теоретические основы информационно-статистического анализа сложных систем. – СПб.: Лань, 1997. – 320 с.
4. Коноплянко, В.И. Организация и безопасность дорожного движения / В.И. Коноплянко. – М.: Транспорт, 1991. – 183 с.
5. Косолапов, А.В. Повышение эффективности информационного обеспечения участников дорожного движения в городах: дис. канд. техн. наук. – М., 1992.
6. Опыт создания и эксплуатации интеллектуальных транспортных систем: Информационный сборник / Федеральное дорожное агентство Министерства транспорта Российской Федерации. – М.: ООО «Принт Форс Пабблишинг», 2009. – 287 с.
7. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». – 42 с.
8. Руководящий документ «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры», от 18 мая 2007 года, ФСТЭК России.

УДК 004.89 : 656.078

ЗАЩИТА КОРПОРАТИВНОЙ ИНФОРМАЦИИ В ТРАНСПОРТНО-ЛОГИСТИЧЕСКИХ СЕТЯХИскандеров Юрий Марсович¹, Паутов Михаил Дмитриевич²¹Санкт-Петербургский институт информатики и автоматизации РАН,
Россия, Санкт-Петербург, 14 линия, 39,²ООО "Инновационный центр транспортных исследований",
Россия, Санкт-Петербург, ул. КИМа, 4,
emails: iskanderov_y_m@mail.ru, mdpautov@mail.ru

Аннотация: В докладе изложены возможности использования методов защиты корпоративной информации в транспортно-логистических сетях.

Ключевые слова: корпоративная информация; защита информации; транспортно-логистические сети.

THE PROTECTION OF CORPORATE INFORMATION IN THE TRANSPORT AND LOGISTICS NETWORKSIskanderov Yuriy¹, Pautov Mikhail²¹ The St. Petersburg Institute for Informatics and Automation of RAS,
Russia, St. Petersburg, 14-th Line, 39,² LLC «Innovative Center of Transport Researches»,
Russia, St. Petersburg, KIMa Street 4,
emails: iskanderov_y_m@mail.ru, mdpautov@mail.ru

Abstract: The article presents possibilities of using methods of protecting corporate information in transport and logistics networks.

Keywords: corporate information; protection of information; transport and logistics networks.

Введение. С целью эффективного функционирования транспортно-логистических сетей применяются современные информационные технологии, позволяющие обеспечить удобство взаимодействия между сотрудниками компаний, а также с внешними контрагентами. В этих сетях генерируются и циркулируют значительные потоки информации, в том числе и конфиденциальная информация, представляющая коммерческую тайну. Для защиты подобной рода информации необходимо иметь адекватную систему информационной безопасности [1,2].

Известно, что корпоративные сети подобных организаций построены с использованием оборудования нескольких поколений и от разных производителей, кроме того, информационные ресурсы отличаются разнородностью, они состоят из различных баз данных и знаний, следствием такого положения является их высокая уязвимость. Наиболее серьезную опасность для ИТ-инфраструктуры в настоящее время представляют вирусы (троянское ПО, черви), шпионское и рекламное программное обеспечение, спам и фишинг-атаки типа «отказ в обслуживании», подмена главной страницы интернет-ресурса и социальный инжиниринг. Причем источником угроз могут быть и внешние пользователи, и сотрудники компании, как умышленно, так и ненамеренно. Реализация вредоносных алгоритмов может привести как к сбоям системы и утраты ее работоспособности, так и к утере, подмене или утечке информации. Все это чревато огромными не только временными и финансовыми потерями, но и утратой репутации для компании. Таким образом, главными задачами любой системы информационной безопасности являются: обеспечение доступности данных для авторизованных пользователей — возможности оперативного получения информационных услуг; гарантия целостности информации — ее актуальности и защищенности от несанкционированного изменения или уничтожения; обеспечение конфиденциальности сведений. Для решения обозначенных целей применяются такие методы защиты информации, как регистрация и протоколирование, идентификация и аутентификация, управление доступом, создание межсетевых экранов и криптография [3].

Заключение. В представленном докладе рассматриваются актуальные проблемы использования методов защиты корпоративной информации в транспортно-логистических сетях, даются практические рекомендации с учетом особенностей их применения.

СПИСОК ЛИТЕРАТУРЫ

1. Искандеров Ю.М., Дорошенко В.И. Организация транспортно-технологических процессов на основе интегрированных информационных систем. Сборник статей Международной научно-практической конференции "Новая экономика и основные направления ее формирования". СПб., ФГАОУ ВО "Санкт-Петербургский политехнический университет Петра Великого", ISBN: 978-5-7422-5215-3, 2016г., с.53-62.
2. Искандеров Ю.М. Построение моделей интегрированной информационной системы транспортной логистики на основе мультиагентных технологий. Сборник статей Международной научно-практической конференции "Новая экономика и основные направления ее формирования". СПб., ФГАОУ ВО "Санкт-Петербургский политехнический университет Петра Великого", ISBN: 978-5-7422-5215-3, 2016г., с.62-69.
3. Зима В., Молдовян А., Молдовян Н. Безопасность глобальных сетевых технологий. Серия "Мастер". - СПб.: БХВ-Петербург, 2001. - 320 с.: ил.

УДК 004.89 : 656.078

**ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЦЕССА ПЕРЕВОЗКИ
НЕГАБАРИТНЫХ ГРУЗОВ**

Искандеров Юрий Марсович¹, Чумак Александр Сергеевич²
¹Санкт-Петербургский институт информатики и автоматизации РАН,
Россия, Санкт-Петербург, 14 линия, 39,
²ООО «НеваСпецТяж»,
Россия, Санкт-Петербург, Московское шоссе, 25, корп.1,
emails: iskanderov_y_m@mail.ru, chumak@nst-spb.ru

Аннотация: В докладе рассмотрены проблемы создания и функционирования информационной системы процесса перевозки негабаритных грузов и обеспечения ее информационной безопасности.

Ключевые слова: *информационная система; информационная безопасность; негабаритный груз; перевозка.*

THE PROVISION OF INFORMATION SECURITY OF OVERSIZE CARGO TRANSPORTATION

Iskanderov Yuriy¹, Chumak Alexander²
¹ The St. Petersburg Institute for Informatics and Automation of RAS,
Russia, St. Petersburg, 14-th Line, 39,
² LLC «NevaSpecTyag»,
Russia, St. Petersburg, Moscow highway, 25, building 1,
emails: iskanderov_y_m@mail.ru, chumak@nst-spb.ru

Abstract: The article presents problems of creation and operation of the information system for the transportation of oversized cargo and ensuring its information security.

Keywords: *information system; information security; oversized cargo; transportation.*

Введение. Перевозка негабаритных грузов - наиболее сложный вид перевозки, требующий специальной, технически оснащенной техники, наличия необходимых разрешений, предварительных согласований, при необходимости сопровождения и конвоя, специально обученных водителей, а также целого ряда других условий, соблюдение которых требует правила перевозки негабаритных и сверхтяжелых грузов.

В соответствии с Приказом Минтранса России [1], в тех случаях, когда ширина транспортного средства превышает пять метров или длина транспортного средства превышает 35 метров, или когда на двухполосных дорогах при движении крупногабаритного транспортного средства ширина проезжей части для встречного движения составляет менее трех метров необходима разработка проекта организации дорожного движения по маршруту.

Указанный проект должен содержать следующие сведения:

- схема и описание маршрута движения;
- характеристики и параметры транспортных средств, участвующих в движении;
- схема(ы) размещения и крепления груза;
- график движения по маршруту с учетом интенсивности дорожного движения;
- схемы организации движения и прикрытия на участках, имеющих ограниченную видимость, и места, указанные в графе "Особые условия" специального разрешения, утвержденного приказом Минтранса России [2], с указанием расположения автомобилей прикрытия, схемы изменения организации дорожного движения;
- порядок проезда наиболее сложных участков маршрута (поворотов, перекрестков, железнодорожных переездов, сужений проезжей части, участков с выездом на полосу встречного направления движения и с ограниченной видимостью) с нанесенной на схему траекторией движения;
- места осуществления контрольных промеров габаритов искусственных сооружений и коммуникаций в процессе перевозки;
- информация о необходимости полного или частичного перекрытия движения на участках дороги;
- места остановок и стоянок для отдыха и пропуска попутных (встречных) транспортных средств.

Изложенные в проекте сведения должны подтверждаться фотоматериалами, отражающими реальное состояние объектов дорожной инфраструктуры.

Очевидно, что в настоящее время без эффективной информационной системы успешно выполнить подобную разработку не представляется возможным [3]. Информационная система дает возможность осуществлять планирование, управление и контроль всего процесса перевозки негабаритных грузов в режиме реального времени. Сведения, которые будут сформированы и использованы в проекте, а также информационный обмен в ходе перевозки представляют

значительный интерес для злоумышленников. Поэтому, учет аспектов обеспечения информационной безопасности является актуальным и важным.

Заключение. В докладе рассмотрены проблемы создания и функционирования информационной системы процесса перевозки негабаритных грузов и обеспечения ее информационной безопасности [4].

СПИСОК ЛИТЕРАТУРЫ

1. Приказ Министерства транспорта Российской Федерации от 15 января 2014 г. N 7 "Об утверждении Правил обеспечения безопасности перевозок пассажиров и грузов автомобильным транспортом и городским наземным электрическим транспортом и Перечня мероприятий по подготовке работников юридических лиц и индивидуальных предпринимателей, осуществляющих перевозки автомобильным транспортом и городским наземным электрическим транспортом, к безопасной работе и транспортных средств к безопасной эксплуатации"
2. Приказ Министерства транспорта Российской Федерации от 24 июля 2012 г. N 258 "Об утверждении Порядка выдачи специального разрешения на движение по автомобильным дорогам транспортного средства, осуществляющего перевозки тяжеловесных и (или) крупногабаритных грузов".
3. Искандеров Ю.М., Дорошенко В.И. Организация транспортно-технологических процессов на основе интегрированных информационных систем. Сборник статей Международной научно-практической конференции "Новая экономика и основные направления ее формирования". СПб., ФГАОУ ВО "Санкт-Петербургский политехнический университет Петра Великого", ISBN: 978-5-7422-5215-3, 2016г., с.53-62.
4. Искандеров Ю.М. Построение моделей интегрированной информационной системы транспортной логистики на основе мультиагентных технологий. Сборник статей Международной научно-практической конференции "Новая экономика и основные направления ее формирования". СПб., ФГАОУ ВО "Санкт-Петербургский политехнический университет Петра Великого", ISBN: 978-5-7422-5215-3, 2016г., с.62-69.

УДК 004.89 : 656.078

ФОРМИРОВАНИЕ БЕЗОПАСНОЙ БАЗЫ ЗНАНИЙ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ПРОЕКТИРОВАНИЯ АСУ НА ТРАСПОРТЕ

Искандеров Юрий Марсович¹, Ершов Александр Александрович²
¹Санкт-Петербургский институт информатики и автоматизации РАН,
Россия, Санкт-Петербург, 14 линия, 39,
²СП ЗАО "ИВС",
Россия, Санкт-Петербург, ул. Железноводская, 11А,
emails: iskanderov_y_m@mail.ru, ershets@mail.ru

Аннотация: В докладе изложено применение базовой технологии для формирования безопасной базы знаний интеллектуальной системы проектирования АСУ на транспорте.

Ключевые слова: база знаний; интеллектуальная система; безопасность; транспортная система.

THE FORMATION OF THE SAFE KNOWLEDGE BASE OF THE INTELLIGENT SYSTEM OF DESIGNING ACS ON TRANSPORT

Iskanderov Yury¹, Ershov Alexander²
¹ The St. Petersburg Institute for Informatics and Automation of RAS,
Russia, St. Petersburg, 14-th Line, 39,
² Closed Joint-Stock Company «IVS»,
Russia, St. Petersburg, Zheleznovodskaya Street 11A,
emails: iskanderov_y_m@mail.ru, ershets@mail.ru

Abstract: The article presents application of the basic technology for the formation of the safe knowledge base for an intelligent system for designing automated control systems in transport.

Keywords: knowledge base; intellectual system; safety; transport system.

Введение. База знаний интеллектуальной системы (БЗ ИС) является основным, ключевым элементом любой интеллектуальной системы. От высокого качества построения базы знаний зависит эффективность функционирования интеллектуальной системы в целом [1,2].

БЗ ИС для разработки АСУ на транспорте должна включать в себя:

- Знания о транспортной инфраструктуре, т.е. о совокупности всех путей сообщения и предприятий транспорта, как выполняющих перевозки, так и обеспечивающих их выполнение и обслуживание;
- Знания о транспортных средствах, т.е. средствах для перевозки материальных объектов (людей и грузов);
- Знания о методах и средствах управления, обеспечивающих достижение целевой функции транспортной системы.

Одним из основных требуемых свойств транспортных систем является безопасность их функционирования, соответственно это внешнее требование вполне определенным образом отражается во внутренних требованиях при формировании указанной базы знаний. Исходя из этого,

знания, используемые в базе должны быть адекватными, полными, достоверными, непротиворечивыми и защищенными.

Поскольку формирование БЗ ИС для разработки АСУ на транспорте представляет собой сложный итерационный процесс, необходимо использовать базовую технологию ее создания [1]. Применение базовой технологии позволяет обеспечить такое качество, которое в максимально степени удовлетворяет предъявляемым требованиям при проектировании АСУ на транспорте [2].

Заключение. В представленном докладе рассмотрены особенности использования базовой технологии для формирования безопасной базы знаний интеллектуальной системы проектирования АСУ на транспорте и даны рекомендации по ее практическому внедрению.

СПИСОК ЛИТЕРАТУРЫ

1. Искандеров Ю.М. Технология создания базы знаний для автоматизированной системы управления корпоративной сетью связи морского порта : диссертация ... доктора технических наук : 05.12.13. - Санкт-Петербург, 2005. - 243 с. : ил.
2. Ершов А.А. Модель и методы интеллектуализации разработки АСУ для сложных производственно-технических систем: диссертация ... кандидата технических наук: 05.13.01. – Санкт-Петербург, 2013. – 148 с.; ил.

УДК 004.056

МЕТОД ЗАЩИТЫ ОТ УГРОЗ ДОСТУПНОСТИ УЗЛОВ МЕЖМАШИННЫХ СЕТЕЙ ПУТЕМ ДИНАМИЧЕСКОЙ МАРШРУТИЗАЦИИ СЕТЕВЫХ ПОТОКОВ С ПОМОЩЬЮ МУРАВЬИНОГО АЛГОРИТМА

Калинин Максим Олегович

Санкт-Петербургский политехнический университет Петра Великого,
Россия, Санкт-Петербург, ул. Политехническая, д. 29,
emails: max@ibks.spbstu.ru

Аннотация: В статье рассмотрен метод проактивной маршрутизации в одноранговых межмашинных сетях (MANET/VANET) на базе муравьиного алгоритма. Метод обеспечивает защиту от киберугроз доступности узлов в крупных транспортных и мобильных компьютерных сетях.

Ключевые слова: доступность, искусственный интеллект, маршрутизация, муравьиный алгоритм, роевой алгоритм, MANET, VANET.

THE METHOD OF PROTECTION OF M2M NETWORKS AGAINST UNAVAILABILITY THREATS BY DYNAMIC ROUTING WITH ANT ALGORITHM

Kalinin Maxim

Peter the Great St. Petersburg Polytechnic University,
Russia, St. Petersburg, Polytechnicheskaya street, 29,
emails: max@ibks.spbstu.ru

Abstract: The paper reviews the method of proactive routing in MANET/VANET networks using ant algorithm as a kind of artificial swarm algorithms. This method protects m2m networks against cyber threats targeted at transport and moving networks availability.

Keywords: availability, artificial intelligence, муравьиный алгоритм, роевой алгоритм, MANET, VANET.

Введение. Масштабное распространение устройств, поддерживающих межмашинное взаимодействие, а также технологий (machine-to-machine) M2M в мобильных сетях MANET и сетях транспортных средств VANET, привело к тому, что классические способы построения компьютерных сетей стали малоэффективными ввиду огромного числа узлов, которые постоянно меняют свое местоположение. В таких сетях применяются технологии организации прямого взаимодействия между устройствами и алгоритмы одноранговой маршрутизации, в которых устройства одновременно выполняют функции клиента и маршрутизатора. В докладе показаны проблемы безопасности, возникающие при маршрутизации в таких сетях, а также методы, основанные на применении методов искусственного роевого интеллекта, позволяющие устранить данные проблемы.

Маршрутизация в одноранговых сетях основана на метриках соединений, что приводит к тому, что, имитируя лучшую метрику, узел-нарушитель может переориентировать сетевые потоки. Существует два подхода к реализации маршрутизации в одноранговой сети – проактивный и реактивный. При проактивном подходе все устройства сети знают всю топологию сети и могут построить путь до любого другого узла. Такой подход неэффективен для крупных сетей. При реактивном подходе маршрут строится перед отправкой данных, и в большой одноранговой сети данный процесс может занять продолжительное время. Таким образом, обеспечение безопасности динамической одноранговой сети является вычислительно сложной задачей.

Для реализации возможности применять средства защиты в такой сети необходимо большую сеть разбить на несколько подсетей, и на устройствах, соединяющих разные подсети, организовать фильтрацию трафика. Для разбиения на подсети предлагается использовать муравьиный алгоритм:

весь распространяемый по сети трафик помечается феромоном, при проходе через любое устройство феромон откладывается на нем. Устройства, преодолевшие определенный уровень феромона, становятся кандидатами на то, чтобы стать граничными узлами. Для этого они должны поддерживать фильтрацию трафика и пройти регистрацию в центре безопасности. Общение между устройствами из разных областей возможно только через граничные узлы. Подход позволяет создать фильтрацию трафика между различными сегментами, но если устройства взаимодействуют в рамках одного сегмента, то трафик не фильтруется. Для фильтрации внутри сегмента необходимо выбрать внутренний узел фильтрации. Выбор такого устройства происходит аналогично выбору граничного узла. Если ни одно из устройств не подходит по критериям выбора, то внутренним устройством фильтрации назначается граничный узел (рисунок). При построении маршрута от узла-источника до узла назначения в рамках одной области, накладывается ограничение, что трафик должен пройти через узел фильтрации трафика, а такое ограничение реализуется как при использовании проактивного, так и при использовании реактивного подхода к маршрутизации.

Заключение. Предложенный метод позволяет строить большие одноранговые M2M-сети с фильтрацией трафика и поддержкой функций контроля доступа. Описанный подход позволяет локализовать воздействия атак типа "черная дыра" и "воронка" в рамках одной подсети, атаки типа "червоточина" становится нереализуемой.

Проект выполнен при финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы» (Соглашение №14.578.21.0224, уникальный идентификатор Соглашения RFMEFI57816X0224).

СПИСОК ЛИТЕРАТУРЫ

1. Minin, A., Kalinin, M. Information security in computer networks with dynamic topology. Proceedings of the 8th International Conference on Security of Information and Networks, ACM New York, NY, USA, 2015, pp. 127-130.

УДК 004.056

КИБЕРБЕЗОПАСНОСТЬ, КАК НЕОТЪЕМЛЕМАЯ ЧАСТЬ СИСТЕМЫ БЕЗОПАСНОСТИ СУДНА

Кардакова Мария Владимировна

Государственный университет морского и речного флота имени адмирала С.О. Макарова,

Россия, Санкт-Петербург, г. Санкт-Петербург, ул. Двинская, 5/7

emails: m.v.kardakova@ya.ru

Аннотация: В статье рассмотрены вопросы кибербезопасности судна, определены наиболее уязвимы системы для кибератак, и даны рекомендации по снижению риска кибератак.

Ключевые слова: безопасность; кибербезопасность; система безопасности; система защиты; угроза; киберугроза; кибератака; шпионаж; уязвимость.

CYBERSECURITY, AS AN INTEGRAL PART OF THE SECURITY SYSTEM OF THE SHIP

Kardakova Mariia

Admiral Makarov State University of Maritime and Inland Shipping,

Russia, Saint-Petersburg, Dvinskaya st., 5/7,

emails: m.v.kardakova@ya.ru

Abstract: The article presents the issues of cyber security of the vessel, the most vulnerable systems to cyber-attacks, and recommendations to reduce the risk of cyber-attacks.

Keywords: security; cybersecurity; security system; threat; the cyber threat; cyber-attacks; espionage; vulnerability.

Введение. Современные суда оснащены системами автоматизации и удаленного мониторинга, через данные системы можно получить несанкционированный доступ к основным компонентам управления. Например, взломав систему навигации можно изменить маршрут судна, что может привести к убыткам или конфликтным ситуациям. Поэтому все больше внимания уделяется системам защиты и способам устранения вреда от кибератак.

Кибератаки могут быть целенаправленные, их жертвами становятся заранее определенные компании, и нецеленаправленные, они ориентированы на уязвимые места в системах всех компаний [1].

Социальная инженерия, «фишинг», «водопой», программы-вымогатели, сканирование, развертывание бот-сетей, разрушение системы являются наиболее распространенными видами кибератак.

Наиболее уязвимыми для кибератак могут быть следующие системы:

- любое сетевое программное обеспечение;
- любые коммуникационные системы;

- системы контроля доступа;
- системы управления грузом;
- системы управления движением, оборудованием;
- системы учёта и обслуживания пассажиров;
- цифровые навигационные системы, имеющие связь с сетями и серверами на суше;

Кроме риска утечки важной информации, актуальными являются риски изменения курса судов и кражи активов. Таким образом, все компьютерные системы на борту судна должны быть защищены в любой момент времени, а также должна предусматриваться защита для офисов систем, которые расположены на берегу.

Что бы система защиты не была бесполезна, нужно установить порядок использования и функционирования систем судна. Так же необходимо настроить контроль доступа ко всем системам и сетям. Необходимо обучать экипаж судна и обслуживающий персонал общими правилами защиты от кибератак. Важным элементом любой защиты является система резервного копирования, которая может обеспечить быстрое восстановление работы или спасет от потери важных документов. Программное обеспечение необходимо вовремя обновлять и обслуживать, это поможет избежать некоторых сбоев и ошибок в его работе. Так же необходимо установить антивирусное и антишпионское программное обеспечение, и своевременно обновлять их базы. Соблюдение этих простых рекомендаций повысит эффективность любых систем безопасности.

Заключение. Любое судно подвержено такой угрозе, как кибератака. Поэтому необходимо развернуть систему безопасности и от данных угроз. Важным элементом такой системы является подготовка членов экипажа и обслуживающего персонала в области информационной безопасности, которая даст им необходимые знания о принципах работы систем защиты, о способах и методах реагирования на кибератаки, и о возможных киберугрозах. Необходимо проводить мониторинг систем безопасности, следить за новыми продуктами защиты и анализировать угрозы безопасности. Своевременная оценка рисков поможет избежать появления окна опасности, и необходима при активном развитии технологий шпионажа и кибератак.

СПИСОК ЛИТЕРАТУРЫ

1. The Guidelines on Cyber Security Onboard Ships Version 2.0– Produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI. 04.07.2017 – 47 с.

УДК 004.056

МОДЕЛИРОВАНИЕ И ИССЛЕДОВАНИЕ СВОЙСТВ БЕЗОПАСНОСТИ ПЕРЕМЕЩАЮЩИХСЯ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ VANET/MANET С ИСПОЛЬЗОВАНИЕМ ВИРТУАЛЬНОЙ СРЕДЫ СУПЕРКОМПЬЮТЕРА

Крундышев Василий Михайлович, Калинин Максим Олегович, Зегжда Дмитрий Петрович
Санкт-Петербургский политехнический университет Петра Великого,
Россия, Санкт-Петербург, ул. Политехническая, 29,
emails: vaskrund@mail.ru, max@ibks.spbstu.ru

Аннотация: В статье рассмотрен подход к построению защищенных транспортных сетей типа VANET/FANET с использованием технологии программно-конфигурируемых сетей, приведены результаты экспериментов по исследованию эффективности предлагаемого подхода, полученные с помощью суперкомпьютерного имитационного моделирования в крупномасштабной виртуальной киберсреде.

Ключевые слова: безопасность; динамическая топология; моделирование; программно-конфигурируемая сеть; суперкомпьютер; централизация; MANET; SDN; VANET.

MODELING AND INVESTIGATION OF SECURITY FEATURES OF MOVING SOFTWARE-DEFINED VANET/MANET NETWORKS IN SUPERCOMPUTER-BASED VIRTUAL ENVIRONMENT

Krundyshov Vasiliy, Kalinin Maxim, Zegzhda Dmitry
Peter the Great St. Petersburg Polytechnic University,
Russia, St. Petersburg, Polytechnicheskaya street, 29,
emails: vaskrund@mail.ru, max@ibks.spbstu.ru

Abstract: The paper reviews the new approach to the construction of the protected vehicular and mobile networks of VANET/MANET types using the technology of software-defined networks. The results of modeling and experiments on the evaluation of the effectiveness of the proposed approach obtained with the help of supercomputer-based virtual cluster are presented.

Keywords: *security; dynamic topology; modeling; software-defined network; supercomputer; centralization; MANET; SDN; VANET.*

Проект выполнен при финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы» (Соглашение №14.578.21.0224, уникальный идентификатор Соглашения RFMEFI57816X0224).

Введение. В последнее десятилетие большое внимание уделяется созданию мобильных сетей, которые не имеют фиксированной инфраструктуры – самоорганизующиеся беспроводные одноранговые компьютерные сети с динамической топологией (например, VANET – сеть между автомобилями, MANET – сеть между мобильными устройствами). Класс межмашинных (m2m) сетей обладает свойствами самоорганизации, имеет одноранговую архитектуру, поддерживает множественные связи между узлами, обеспечивает динамическое управление маршрутизацией на каждом узле, что обеспечивает ее преимущества перед традиционными сетями, а именно:

- неограниченная размерность,
- возможность многопоточной передачи данных на большие расстояния;
- устойчивость к пространственным изменениям в сетевой топологии;
- динамическая реконфигурация сети в условиях помех и отказов узлов.

Поддержание целостной киберсреды между транспортными средствами и понимание транспорта как киберфизической системы определяет новое представление о нем, как об интегральном объекте, агрегирующем механизм перемещения в пространстве и информационную составляющую, обеспечивающую устойчивое выполнение целевой функции в условиях внешних воздействий [1]. Максимальная децентрализация, самоорганизация и перемещение узлов определяет появление новых проблем для современных сетей VANET/MANET:

- проблема обеспечения помехоустойчивости сети;
- проблема обеспечения безопасности информации в сети;
- проблема доступности узлов (интегральной пропускной способности сети и защищенной маршрутизации).

Для решения проблем традиционных VANET/MANET-сетей предложено использовать технологию программно-конфигурируемых сетей – SDN (software-defined network). Адаптируемость и управляемость SDN делает такой подход привлекательным для реализации требований по построению эффективной и безопасной сети. Применение принципов SDN обеспечивает программируемость и универсальность управления сетью, которых не хватает в современных транспортных сетях [2]. Технология SDN позволяет добиться упрощения управления сетью, внедрить новые интеллектуальные V2V и V2I услуги, основанные на знании состояния сети, и внедрить механизмы безопасности на уровне сети в целом.

Возможны три сетевые архитектуры внедрения механизмов безопасности на основе технологии SDN в сети VANET/MANET:

- архитектура с центральным звеном управления – серверами, решающими задачи безопасности.
- архитектура с частичной децентрализацией.
- иерархическая архитектура.

Для сравнения спроектированных архитектур сетей SDN-VANET/MANET относительно традиционной одноранговой транспортной сети выполнено экспериментальное исследование. Для проведения экспериментов использованы симуляторы сети NS-3 [3] и SUMO [4], эмулятор SDN – Mininet-WiFi[5], а также было проведено глобальное моделирование с использованием вычислительных ресурсов суперкомпьютерного центра.

Установлено и экспериментально показано, что причинами проблем, связанными с безопасностью VANET/MANET, являются:

- отсутствие средств защиты узлов от злоумышленников, невозможность реализации политики безопасности ввиду децентрализации VANET/MANET -сети и отсутствия традиционных механизмов безопасности, работающих с динамической топологией;
- возможность прослушивания каналов и подмены сообщений по причине общей доступностью среды передачи;
- невозможность применения классической системы обеспечения безопасности из-за особенностей архитектуры сетей VANET/MANET;
- необходимость использования сложных алгоритмов маршрутизации, учитывающих вероятность появления некорректной информации от скомпрометированных узлов в результате изменения топологии сети.

Самоорганизующиеся сети уязвимы как к классическим типам атак, присущим большинству беспроводных сетей, так и имеют свои особенные уязвимости. Атаки в сетях VANET/MANET можно разделить на пассивные и активные. При пассивных атаках злоумышленник обычно скрыт, он подсоединяется к линиям связи для сбора определенных данных. Пассивные атаки могут быть разбиты

на два класса: перехват (сниффинг) и анализ трафика. При активных атаках злоумышленник оказывает прямое влияние на работу систем. Активные атаки могут быть классифицированы на следующие группы: физические; фальсификация (спуфинг), повтор и изменение сообщений; отказ в обслуживании. Активные атаки эксплуатируют особенности динамической маршрутизации в сети данного типа: например, атаки типа «черная дыра», «серая дыра», перенаправление трафика, man-in-the-middle и пр.

Все предложенные архитектуры превосходят по эффективности классическую архитектуру VANET/MANET. В отличие от традиционных VANET/MANET-сетей предложенный программно-конфигурируемый подход позволяет имплементировать политику безопасности в сети, увеличить пропускную способность сети, улучшить мобилизационные способности сети, автоматизировать управление, сократить время реакции системы на внешние воздействия, что направлено на обеспечение целостности, доступности и конфиденциальности ресурсов.

Заключение. Разработанные архитектуры VANET/MANET с использованием централизованного SDN-подхода превосходят по показателям классические VANET-сети. В крупномасштабных транспортных сетях наиболее эффективны архитектуры с несколькими контроллерами: архитектура с частичной децентрализацией и иерархическая архитектура.

На основе проведенных экспериментов можно сделать вывод, что применение технологии SDN позволяет решить существующие проблемы VANET-сетей.

Результаты работы получены с использованием вычислительных ресурсов суперкомпьютерного центра Санкт-Петербургского политехнического университета Петра Великого – СКЦ «Политехнический» (<http://www.spbstu.ru>).

СПИСОК ЛИТЕРАТУРЫ

1. Minin, A., Kalinin, M. Information security in computer networks with dynamic topology. Proceedings of the 8th International Conference on Security of Information and Networks, ACM New York, NY, USA, 2015, pp. 127-130.
2. Ku I., Lu Y., Cerqueira E., Gerla M. Towards Software-Defined VANET: Architectures and Services. Med-Hoc-Net 2014, Piran Slovenia, June, 2014.
3. NS-3, <http://www.nsnam.org/>
4. Simulation of Urban Mobility (SUMO), <http://sumo-sim.org/>
5. Mininet-WiFi, <https://github.com/intrig-unicamp/mininet-wifi>

УДК 004.056

СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ В СЕТЯХ ТРАНСПОРТНЫХ СРЕДСТВ НА БАЗЕ ТЕХНОЛОГИИ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ

Крундышев Василий Михайлович, Калинин Максим Олегович
Санкт-Петербургский политехнический университет Петра Великого,
Россия, Санкт-Петербург, ул. Политехническая, 29,
emails: vaskrund@mail.ru, max@ibks.spbstu.ru

Аннотация: В статье рассмотрен подход к построению системы контроля и управления безопасностью в перемещающихся компьютерных сетях современных беспилотных и связанных транспортных средств с использованием технологии программно-конфигурируемых сетей (ПКС). Представлены основные архитектурные элементы программно-конфигурируемых сетей транспортных средств, выделены возможные режимы работы транспортной ПКС-сети.

Ключевые слова: архитектура; безопасность; программно-конфигурируемая сеть; режим работы; сети транспортных средств, SDN, VANET

SECURITY CONTROL AND MANAGEMENT SYSTEM IN INTER-CAR NETWORKS WITH TECHNOLOGY OF SOFTWARE-DEFINED NETWORKS

Krundyshchev Vasiliy, Kalinin Maxim
Peter the Great St. Petersburg Polytechnic University,
Russia, St. Petersburg, Polytechnicheskaya street, 29,
emails: vaskrund@mail.ru, max@ibks.spbstu.ru

Abstract: The paper reviews the approach to building a cybersecurity control and management system in vehicular networks using the technology of software-defined networks. The main elements in the network architectures based on the SDN technology are described, as well as the possible modes of operations in the SDN-VANET.

Keywords: VANET architecture; security; mode of operation; software-defined network; vehicular network SDN, VANET.

Введение. Сети транспортных средств (VANET) – беспроводные децентрализованные самоорганизующиеся сети, состоящие из перемещающихся транспортных средств и инфраструктурных сетевых узлов. Задачей, которая ставится при создании транспортных сетей VANET, является создание сетевого интерфейса в автомобиле, который позволил бы поддерживать

четыре группы соединений: автомобиль — автомобиль (V2V), автомобиль — инфраструктурная сеть (V2I), автомобиль — жилье (V2H), инфраструктурная сеть — жилье (I2H). Внедрение беспроводных самоорганизующихся сетей VANET предназначено для повышения эффективности и безопасности дорожного движения. Основные цели использования VANET можно разделить на три группы [1]:

- помощь водителю (навигация, предотвращение столкновений и смена полос движения);
- информирование (об ограничении скорости или зоне ремонтных работ);
- предупреждение (послеаварийные, о препятствиях или состоянии дорог).

Архитектура сети VANET предполагает взаимодействие автомобиля, как с другими автомобилями, так и с придорожной сетью. Для сетей транспортных средств характерна максимальная децентрализация и топология с высокой степенью динамики, что сопряжено с рядом проблем, в том числе с проблемами обеспечения защиты передаваемых данных, общей пропускной способностью сетей, эффективной и безопасной маршрутизацией [2]. Кроме того, с целью решения указанных проблем предложено применить технологию программно-конфигурируемых сетей (ПКС, software defined networks, SDN) [3].

Основные архитектурные элементы в сетях транспортных средств, построенной на базе технологии ПКС:

- программно-конфигурируемый контроллер: логический центральный интеллект ПКС, управляющий поведением сети. Контроллер обеспечивает управление потоками данных и сегментацию сети транспортных средств, установку и реализацию правил контроля доступа, мониторинг состояния устройств, трафика и сетевой статистики;
- облачная суперкомпьютерная система: осуществляет различные ресурсозатратные вычисления и использует хранящиеся в базе данных знания для осуществления вычислений;
- база данных: связана с облачной суперкомпьютерной системой, хранит данные об автомобилях и их владельцах, постоянно обновляется.
- узлы ПКС – коммутаторы ПКС и мобильные устройства: находятся под управлением контроллера ПКС, осуществляют передачу сетевых пакетов и их обработку в соответствии с правилами, заданными контроллером ПКС.

Разработано три архитектуры внедрения механизмов безопасности в сети VANET на основе технологии SDN:

- архитектура с центральным звеном управления и выделенными серверами, решающими задачи безопасности,
- архитектура с частичной децентрализацией,
- иерархическая архитектура.

Данные архитектуры превосходят по эффективности традиционную одноранговую архитектуру VANET. Эффективность архитектур зависит от условий и сценария, при которых они используются. Однако с учетом плотности населения и количества транспортных средств в мегаполисах показано, что наиболее целесообразно использовать иерархическую архитектуру благодаря наличию центрального контроллера, который обеспечивает распределение зон влияния контроллеров и предоставляет возможность установления общей политики безопасности.

Программно-конфигурируемая сеть VANET может работать с учетом различной степени вовлеченности контроллера ПКС в процесс управления:

- централизованный режим – контроллер (кластер контроллеров) ПКС контролирует все потоки данных, передавая на узлы-маршрутизаторы правила обработки трафика;
- распределенный режим – контроллер ПКС отсутствует, режим представляет оригинальную самоорганизующуюся сеть транспортных средств;
- гибридный режим – контроллер (кластер контроллеров) ПКС осуществляет гибкий контроль в любом сегменте сети (например, контроллер ПКС рассылает правила политики, которые определяют поведение узлов сети транспортных средств в целом, а узлы ПКС используют локальный интеллект для пересылки пакетов и обработки на уровне потоков).

Заключение. В отделенной плоскости управления использование технологии ПКС обеспечивает гибкость и программируемость сети, что позволяет системе адаптироваться к изменяющимся условиям и требованиям. Эта особенность позволяет узлам программно-конфигурируемой сети транспортных средств принимать более обоснованные решения на основе комбинированной информации из различных источников. Кроме того, динамичность и гибкость позволяют реагировать на внезапные события, например, при чрезвычайных ситуациях и изменяющихся требованиях. Применение технологии программно-конфигурируемых сетей при построении систем управления кибербезопасностью для крупномасштабных перемещающихся сетей позволяет достичь следующих преимуществ по сравнению с традиционными подходами:

- мониторинг ситуации во всей сети. Контроллер ПКС может назначать потоки по определенным каналам или удалять их в зависимости от изменяющихся внешних условий и требований приложений, в т.ч. требований и правил политик кибербезопасности;
- динамическое разделение и группирование информационных потоков. Контроллер ПКС устанавливает правила потоков данных, чтобы эти данные достигали всех необходимых узлов. Таким

образом, передача данных напоминает широковещательную рассылку, осуществляемую контроллером в отношении групп транспортных средств (например, транспортным средствам подписчиков информационных сервисов, транспортным средствам специальных служб полиции, медицинской помощи и т.п.);

– применение эластичных сетевых сервисов. Виртуализация сетей призвана обеспечить абстрактные логические сети на общих физических сетевых ресурсах.

Проект выполнен при финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы» (Соглашение №14.578.21.0224, уникальный идентификатор Соглашения RFMEFI57816X0224).

СПИСОК ЛИТЕРАТУРЫ

1. Glass, S., Portmann, V., Muthukkumarasamy, V. Securing Route and Path Integrity In Multihop Wireless Networks. // Security of Self-Organizing Networks. MANET, WSN, WMN, VANET. CRC Press, 2011, P.595.
2. Vinh, Hoa La, Cavall A. Security attacks and solutions in vehicular ad hoc networks: a survey. // International Journal on AdHoc Networking Systems (IJANS), Vol. 4, No. 2, April 2014 – pp. 1-20.
3. Kalinin, M., Zegzhda, P., Zegzhda, D., Vasiliev, Y., Belenko V. Software Defined Security for Vehicular Ad Hoc Networks // Proc. of 7th International Conference on Information and Communication Technology Convergence (ICTC2016), Jeju Island, Korea (Oct. 19-21, 2016). – pp. 533-537.

УДК 004.77

МЕТОДЫ РЕИНЖИНИРИНГА САЙТОВ В ЗАДАЧЕ ОПТИМИЗАЦИИ ИТ-АРХИТЕКТУРЫ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ ОРГАНИЗАЦИИ

Москалева Валерия Дмитриевна, Кривцов Александр Николаевич
Санкт-Петербургский государственный университет,
Россия, Санкт-Петербург, Университетская наб., 7/9,
emails: a_kriv@mail.ru, lera.mosk@gmail.com

Аннотация: В статье представлены результаты применения методов реинжиниринга сайта для решения задачи оптимизации ИТ-архитектуры научно-исследовательской компании ООО «Инновационный центр транспортных исследований».

Ключевые слова: веб-сайт; реинжиниринг сайта; ИТ-архитектура; научно-исследовательская организация

METHODS OF REENGINEERING WEBSITES IN THE PROBLEM OF OPTIMIZATION OF THE IT-ARCHITECTURE OF THE SCIENTIFIC RESEARCH ORGANIZATION

Moskaleva Valeriia, Krivtsov Alexander
Saint-Petersburg State University,
Russia, Saint-Petersburg, Universitetskaya emb., 7/9,
emails: a_kriv@mail.ru, lera.mosk@gmail.com

Abstract: The article presents the results of applying the methods of site reengineering to solve the problem of optimizing the IT architecture of a research company.

Keywords: website; site reengineering; IT-architecture; research organization

Введение. Понятие «архитектура» исторически ассоциируется у людей со строительством зданий и сооружений. Говоря об архитектуре предприятия, подразумевают совокупность множества различных составных частей, одной из которых является ИТ-архитектура предприятия. Архитектура информационных технологий, в свою очередь, включает в себя различные инструменты для обеспечения управления потоками данных внутри компании. Одним из таких инструментов является информационный портал. Одним из элементов большого информационного портала является веб-сайт, выполняющий роль представительства компании в сети Интернет. Таким образом, реинжиниринг веб-сайта является одним из элементов оптимизации архитектуры организации.

Неотъемлемой частью реинжиниринга сайта является его грамотный и качественно проведенный аудит. Применение методов технического, текстового, поискового, маркетингового и юзабилити аудита [1] было рассмотрено на примере анализа сайта ООО «Инновационный центр транспортных исследований» и выявлены основные проблемы и узкие места в его организации. ООО «Инновационный центр транспортных исследований» – это малое инновационное предприятие, созданное в Санкт-Петербургском государственном университете в 2011 году. Каждый из данных пяти аудита сайта затрагивает проверку множества параметров: удобство навигационной структуры, информативность контента, видимость по ключевым фразам семантического ядра и т.д.

Сайт данной компании представляет собой её визитную карточку и предназначен для расширения клиентской базы, предоставления пользователям информации о деятельности компании и осуществлении обратной связи.

Следует отметить важность наличия веб-ресурса у научно-исследовательской организации: на сегодняшний день сайт является не только площадкой для размещения материалов по популяризации своих научных открытий, исследований, достижений и привлечения новых кадров через глобальную сеть Интернет. Кроме этого, сайт принимает активное участие в формировании единого информационного пространства, которое объединяет ученых с разных уголков мира и способствует распространению и развитию научных знаний [2]. Веб-ресурс во многом определяет имидж научно-исследовательской компании.

В связи с расширением базы проведенных научных исследований в сфере транспорта и увеличением количества успешно реализованных проектов руководителем ООО «Инновационный центр транспортных исследований» была поставлена задача проведения реинжиниринга сайта с учетом дальнейших международных перспектив расширения деятельности организации. Еще одна важная задача, в решении которой участвует сайт, это поиск источников финансирования. Также в связи с получением патента под проект для Министерства образования и науки Российской Федерации у исследовательского центра появилась необходимость в привлечении научных кадров и разработчиков.

Был проведен подробный аудит сайта научно-исследовательской организации ООО «Инновационный центр транспортных исследований», сформированы рекомендации по реинжинирингу и развитию сайта и выделены ключевые критерии оптимальности сайта заданной структуры. На основе сформированных рекомендаций было сформировано техническое задание в соответствии с ГОСТ 34.602-89, в результате которого был спроектирован и разработан новый сайт.

Для проведения сравнительного анализа старого и нового сайтов и выбора оптимального на основании экспертных оценок [3] воспользуемся методом анализа иерархий [4].

Верхний уровень иерархии – цель: выбрать оптимальный сайт.

Средний уровень иерархии (ключевые критерии оптимальности сайта):

- информативность, полезность, уникальность контента,
- удобство и понятность навигационной структуры,
- видимость сайта в различных поисковых системах, оптимизированность в соответствии с семантическим ядром,

– наличие технических ошибок,

– удобство восприятия текстовых, графических и мультимедийных элементов, представленных на сайте,

- наличие необходимых контактных данных,
- адаптивность и кроссбраузерность сайта,
- корректность работы форм обратной связи и отправки сообщений.

Нижний уровень иерархии:

- старый сайт (URL: <http://innocentr.ru/>)
- новый сайт (URL: <http://transport-research.org/>).

В результате проведенного с помощью программы MPriority (URL: <http://www.tomakechoice.com/mpriority.html>) анализа был получен вектор с показателем 0,64 для нового сайта и 0,36 для старого сайта. Сравнительный анализ старого и нового сайтов на основе экспертных оценок выявил явное преимущество нового сайта по большинству выделенных ключевых критериев оптимальности.

Закключение. Таким образом, был получен один из возможных подходов к решению задачи реинжиниринга сайтов типа интернет-представительство как одной из подзадач оптимизации ИТ-архитектуры научно-исследовательской организации.

СПИСОК ЛИТЕРАТУРЫ

1. Кривцов, А. Н. Реинжиниринг сайтов: классификация, виды и основные этапы анализа / А. Н. Кривцов, В. Д. Москалева // Развитие технических наук в современном мире: сборник научных трудов по итогам международной научно-практической конференции (11 декабря 2016 г., Воронеж). / Инновационный центр развития образования и науки; ред. Э. К. Аракелян [и др.]. – Инновационный центр развития образования и науки, 2016. № 3. – 128 с. – С. 115-119.
2. Москалева, В. Д. Выбор оптимальной структуры интернет-представительства инновационной исследовательской компании на основе анализа существующих структур сайтов / В. Д. Москалева // Интеллектуальные информационные технологии, энергетика и экономика: сборник трудов XIV международной научно-технической конференции студентов и аспирантов в 3 т. (22-23 июня 2017 г., Смоленск). / Филиал ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске. – ООО «Принт-Экспресс», 2017. – Т. 1. – 244 с. – С. 36-40.
3. Кривцов, А. Н. Применение метода анализа иерархий в задаче выбора системы обеспечения сервиса программно-технического уровня информационной безопасности / А. Н. Кривцов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V-я Международная научно-техническая и научно-методическая конференция: сб. научных статей в 2 т. / ред. С.В. Бачевский, сост. А.Г. Владыко, Е.А. Аникевич, Л.М. Минаков. – СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. Проф. М.А. Бонч-Бруевича, 2016. – Т. 2. – С. 121-127.
4. Саати Т. Принятие решений. Метод анализа иерархий. – М.: Радио и связь, 1993. – 320 с.

УДК 629.75.33 + 533.6.013.622

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПОЛЕТОВ БЕСПИЛОТНЫХ ВОЗДУШНЫХ СУДОВ

Рубцов Евгений Андреевич

Санкт-Петербургский государственный университет гражданской авиации,
Россия, Санкт-Петербург, ул. Пилотов, 38,
email: rubtsov.spb.guga@rambler.ru

Аннотация: В статье рассмотрены основные проблемы обеспечения безопасности полетов беспилотных воздушных судов. Наиболее важными являются проблемы организации каналов связи и управления, обеспечения требуемых характеристик навигации и наблюдения, а также проблемы идентификации беспилотных воздушных судов.

Ключевые слова: беспилотное воздушное судно; безопасность полетов; связь, навигация, наблюдение; идентификация.

PROBLEMS OF FLIGHT SAFETY OF UNMANNED AIRCRAFT

Rubtsov Evgeny

Saint-Petersburg state University of civil aviation,
Russia, St. Petersburg, Pilotov str. 38,
email: rubtsov.spb.guga@rambler.ru

Abstract: The article considers the main problems of flight safety of unmanned aircraft. The most important problems include organization of communication and control channels, support of required navigation and surveillance performance and the problems of unmanned aircraft identification.

Keywords: unmanned aircraft; flight safety; communication, navigation, surveillance; identification.

Введение. Беспилотные авиационные системы (БАС) представляют одну из самых молодых и быстроразвивающихся отраслей, которая имеет ряд особенностей. В настоящее время полеты беспилотных воздушных судов (БВС) разрешены только в закрытом (сегрегированном) воздушном пространстве. Для малых аппаратов это не является серьезной проблемой, однако в ближайшей перспективе ожидается широкое применение тяжелых БВС, которые способны будут выполнять сложные и разнообразные задачи, включающие перевозку грузов и пассажиров. Такие беспилотные воздушные суда можно применять для перевозки грузов как внутри города, так и за его пределами, в том числе медицинских и опасных грузов, а также использовать в качестве аэротакси [1, 2].

Для взлета и посадки тяжелым БВС потребуются взлетно-посадочные полосы с искусственным покрытием. Сами полеты будут осуществляться в общем воздушном пространстве с пилотируемыми ВС. Это потребует решения ряда проблем, связанных с интеграцией пилотируемой и беспилотной авиации, целью статьи является рассмотрение наиболее важных из них.

Основные проблемы обеспечения безопасности полетов БВС

Среди основных проблем интеграции пилотируемой и беспилотной авиации выделим проблемы радиотехнического обеспечения полетов БАС, а именно: организацию каналов связи и управления, обеспечение требуемых характеристик навигации и наблюдения, а также проблемы идентификации беспилотных воздушных судов.

Обеспечение требуемых характеристик связи (RCP) для беспилотных авиационных систем сопряжено с рядом трудностей из-за специфики построения самой системы. В пилотируемой авиации радиообмен осуществляется между диспетчером и экипажем, находящимся на борту ВС, в связи с этим применение находят низкоскоростные каналы связи (например, скорость канала VDL-2 составляет 31,5 кбит/с) [3]. В беспилотных авиационных системах внешний пилот получает всю информацию о состоянии БВС, его координатах, а также информацию от различного рода полезной нагрузки посредством передачи данных, поэтому потребные скорости канала в БАС могут иметь значение от сотен кбит/с до единиц и десятков Мбит/с. В связи с этим средства связи беспилотных авиационных систем должны обладать лучшими характеристиками, чем применяемые в настоящее время в пилотируемой авиации.

Для навигации БВС в настоящее время применяются глобальные навигационные спутниковые системы (ГНСС). Поскольку инерциальные навигационные системы, применяемые в БАС обладают низкой точностью и служат для ориентации аппарата на начальном этапе полета, приемник ГНСС является единственным навигационным средством беспилотного воздушного судна. Отказ приемника приводит к потере точности навигации, в связи с этим можно сделать вывод о необходимости разработки резервной навигационной системы БВС. Эта система при соблюдении всех требований по точности и надежности работы должна иметь малый вес. Отсюда следует, что применение существующих систем VOR/DME в малых БВС технически невозможно. Кроме того, азимутально-дальномерные системы имеют довольно малую по размеру рабочую область и не в состоянии обеспечить требования перспективных навигационных спецификаций RNP2 и A-RNP [4].

Малые размеры БВС затрудняют их наблюдение с помощью первичных радиолокаторов. Применение вторичной радиолокации также затруднено из-за сравнительно большой массы бортового ответчика. Таким образом, наблюдать малые и средние БВС возможно только с помощью автоматического зависимого наблюдения (АЗН), что повышает требования к надежности канала передачи данных о местоположении аппарата. В то же время, отказ приемника ГНСС приведет к тому, что беспилотное воздушное судно не только лишится средств навигации, но и пропадет с экрана диспетчерского пульта [3].

Важной проблемой для БАС является присутствующая в настоящее время обезличенность БВС. В настоящее время не разработано единой системы по идентификации аппаратов или присвоению им позывных. При возникновении опасных ситуаций или предпосылок к опасным ситуациям, связанным с БВС, владелец имеет шанс уйти от ответственности по причине практической недоказуемости того, что аппарат принадлежит именно ему.

Варианты решения проблем обеспечения безопасности полетов БВС

Для обеспечения требуемых характеристик связи, особенно требуемой скорости передачи данных, потребуется внедрение новых средств, отличных от применяемых в пилотируемой авиации. Возможным решением может стать применение средств мобильной связи в качестве резервного, а при достижении требуемых показателей – основного средства. При обеспечении требуемых характеристик надежности и безопасности передачи информации возможно применение средств мобильной связи для организации канала между внешним пилотом и диспетчером. Для уменьшения массы БВС возможно построение системы, предусматривающей информационный обмен только между экипажем пилотируемого ВС и внешним пилотом.

Для определения местоположения БВС необходимо помимо ГНСС применять резервную систему. В качестве такой системы целесообразно рассмотреть средства мобильной связи, в частности их возможности позиционирования абонента. При наличии достаточного количества станций, точность позиционирования может быть достаточной для выполнения полета по требуемой траектории в случае отказа или ухудшения сигнала ГНСС. Кроме того, в пределах рабочих областей радиолокационных систем возможно обеспечить передачу радиолокационной информации по линии передачи данных, т.е. обеспечение технологии TIS [5].

Обнаружение БВС с помощью первичных радиолокаторов возможно обеспечить с помощью линз Люнеберга или другого эффективного отражателя. Разработка малогабаритного ответчика вторичной радиолокации возможно решит проблему для средних и больших БВС, однако основным средством наблюдения будет АЗН. Отсюда следует необходимость обеспечения надежного канала передачи координатной информации, либо совокупности взаимно-резервируемых каналов: ОБЧ диапазона (VDL), спутникового, а также применение средств мобильной связи.

Проблема идентификации БВС может быть решена путем установки приемо-передающего модуля с SIM-картой оператора мобильной связи. Это решит задачу идентификации самого аппарата, а также позволит составить базу данных пользователей БАС.

Таким образом, применение средств мобильной связи способно решить проблему идентификации БВС, проблему организации высокоскоростных каналов передачи данных (в том числе для реализации АЗН), а также проблему навигации при отсутствии ГНСС. Решение поставленных проблем должно иметь комплексный характер и может быть выражено в создании комплексных систем безопасности [6].

СПИСОК ЛИТЕРАТУРЫ

1. Беспилотные авиационные системы. Учебное пособие / С.А. Кудряков, В.Р. Ткачев, Г.В. Трубников, В.И. Кисличенко // СПб.: Свое издательство. – 2015. – 121 с.
2. Рубцов Е.А., Котов С.А., Рустамов Ю.М. Анализ возможностей беспилотного летательного аппарата Dominator для решения задач гражданской авиации России // Материалы международной научно-практической конференции «Транспорт России: проблемы и перспективы - 2016». – 2016. – С. 303-307.
3. Радиотехническое обеспечение полетов воздушных судов и авиационная электросвязь. Учебное пособие / С.А. Кудряков, В.К. Кульчицкий, Н.В. Поваренкин, В.В. Пономарев, Е.А. Рубцов, Е.В. Соболев, Б.А. Сушкевич // СПб.: Свое издательство. – 2016. – 287 с.
4. Аль-Рубой М.Х., Рубцов Е.А. Обзор методик расчета рабочей области азимутально-дальномерных радиотехнических систем // Естественные и технические науки. – 2014. – № 8 (76). – С. 137-144.
5. Рубцов Е.А., Соболев Е.В., Аль Рубой М. Комплексная обработка данных о местоположении воздушных судов, полученных от радиолокатора и системы ближней навигации // Материалы юбилейной международной научно-практической конференции «Транспорт России: проблемы и перспективы - 2015». – 2015. – С. 91–95.
6. Опыт создания комплексных систем безопасности на объектах транспортной инфраструктуры / С.А. Беляев, Ю.Б. Остапченко, С.А. Кудряков, Е.Н. Шаповалов, М.Г. Павловский // Актуальные проблемы защиты и безопасности. Комплексная безопасность на транспорте. Труды XIX Всероссийской научно-практической конференции. Том 6. – 2016. – С. 52-57.

УДК 656.02

**АЛГОРИТМЫ РЕШЕНИЯ ЗАДАЧ МАРШРУТИЗАЦИИ КАК ОПРЕДЕЛЯЮЩАЯ ЗАДАЧА
ОНЛАЙН-РИТЕЙЛА**

Котляр Софья Денисовна, Кривцов Александр Николаевич
Санкт-Петербургский государственный университет,
Россия, Санкт-Петербург, ул. Чайковского 62,
emails: kotlyar.sofya@gmail.com, a_kriv@mail.ru

Аннотация: В статье рассмотрены подходы к решению задач маршрутизации с ограничением по времени, как определяющей задачи торговли в условиях растущего рынка онлайн-ритейла.

Ключевые слова: задача маршрутизации; временные окна; эвристические методы

VEHICLE ROUTING FOR E-FULFILLMENT

Kotliar Sofia, Krivtsov Aleksandr
The St. Petersburg State University,
Russia, St. Petersburg, Chaykovskogo str. 62,
emails: kotlyar.sofya@gmail.com, a_kriv@mail.ru

Abstract: The article presents construction heuristic to solve the multi-vehicle routing problem with time windows as the defining problem in the growing market of online retail.

Keywords: vehicle routing problem; time windows; construction heuristic

Введение. Определяющей задачей торговли, является выбор временного окна доставки заказа клиенту, а также время начала сборки заказов, так как минимизация времени нахождения собранного заказа позволяет сокращать издержки на аренду складов и тем самым дает возможность расширить ассортиментный ряд при равной площади склада, удовлетворив при этом потребности клиента. Класс задач, занимающихся поиском оптимальных маршрутов транспортных средств, называют задачами маршрутизации транспортных средств (The vehicle routing problems - VRP).

Обычно задача маршрутизации выведена в отдельную функцию системы управления и планирования транспортом (TMS). Однако для многих компаний решение TMS-систем является дорогостоящим продуктом и обладает избыточным функционалом, а задача сводится к грамотному распределению заказов между курьерскими компаниями по рейсам. Поэтому уже сейчас многие разработчики складских систем управления (WMS) задаются вопросом, как предложить компаниям единую систему для полноценной организации доставок и контроля перемещения товара от распределительного центра до конкретного клиента с возможностью автоматически строить маршрутизацию всех заказов и определять приоритеты для своевременной сборки заказов. Таким образом, с одной стороны, сейчас на рынке существуют всевозможные системы для автоматизации всех бизнес-процессов предприятий, однако, на уровне предприятий онлайн-ритейла, где наибольшую роль играет автоматизация и контроль распределительного центра и WMS-системы неизбежно, содержание и обслуживание двух отдельных систем, WMS и TMS, оказывается дорогостоящим и в случаях малого и среднего бизнеса зачастую функционал TMS системы оказывается избыточным, поэтому возникает вопрос автоматизации процесса маршрутизации в рамках единой системы, а именно WMS-системы.

В статье рассмотрены алгоритмы решения задачи транспортной маршрутизации с временными окнами для совершенствования функционала маршрутизации WMS-системы.

Впервые математическая постановка базовой задачи была сформулирована Г. Данцигом и Дж. Рамсером более 50 лет назад и связана с составлением оптимального набора маршрутов для автопарка транспортных средств с целью обслужить заданное множество клиентов. Проблема VRPTW является NP-трудной задачей. И, хотя существуют некоторые точные алгоритмы, которые используют методы математического программирования для нахождения оптимального решения VRPTW, эти алгоритмы обычно позволяют решить обсуждаемую проблему только для случаев, в которых используется до 100 клиентов в течение соответствующего периода времени. Следовательно, многие исследования сосредоточены на разработке соответствующей эвристики для решения VRPTW, именно поэтому основное внимание в литературе и исследованиях уделяется эвристическим алгоритмам.

Заключение. Эвристические подходы являются мощной альтернативой точным методам решения VRPTW, поскольку они способны довольно быстро по сравнению с точными методами разрабатывать решения соответствующего качества, и могут быть применены в качестве основы модулей маршрутизации логистических систем.

СПИСОК ЛИТЕРАТУРЫ

1. В. И. Сергеев, М. Н. Григорьев, С. А. Уваров. Логистика: информационные системы и технологии: Учебно-практическое пособие - М.: Издательство Альфа-Пресс, 2009. – 608 с. – ISBN: 978-5-9428-332-2;
2. Д. А. Иванов. Информационные системы и технологии в логистике. Интегрированные системы управления предприятием: Учебное пособие - СПб.: Изд-во Политехн. ун-та, 2005. – 94 с.
3. Barnhart C., Laporte G. (Eds.), (2007). Handbook in OR & MS, Vol. 14, 367–428.

4. Lao, H.C., Liang, Z., 2002. Pickup and delivery with time windows: Algorithms and test case generation. International Journal on Artificial Intelligence Tools (Architectures, Languages, Algorithms) 11 (3), 455–472.
5. Li, H., Lim, A., 2001. A metaheuristic for the pickup and delivery problem with time windows. In: Proceedings 13th IEEE ICTAI 2001, Los Alamitos, CA, pp.160-167.
6. Nanny, W.P., Barnes, J.W., 2000. Solving the pickup and delivery problem with time windows using reactive tabu search. Transportation Research B 34 (2), 107–121.

УДК 004.588

ФОРМИРОВАНИЕ ЭЛЕКТРОННОЙ ОБРАЗОВАТЕЛЬНОЙ ТРАЕКТОРИИ ПРИ ОБУЧЕНИИ КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Митрофанова Анастасия Витальевна, Соколов Сергей Сергеевич, Новоселов Роман Юрьевич
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Государственный университет морского и речного флота имени адмирала С.О. Макарова»
Россия, Санкт-Петербург, ул. Двинская, 5/7

Emails: mitrofanovaav@gumrf.ru, sokolovss@gumrf.ru, rnovoselov93@gmail.com

Аннотация: Построение индивидуальной образовательной траектории для обучающихся (вариационное обучение) становится трендом современного образования. Появляется необходимость в методах автоматизированной поддержки обучающегося при построении траектории обучения. Теоретические аспекты обоснования образовательной траектории уже существуют, тогда становится необходимым разбивать свое практическое применение в процессе обучения. В статье рассматривается технология формирования вариационного обучения при использовании системы электронного обучения.

Ключевые слова: *Индивидуальная образовательная траектория, вариационное обучение, электронное обучение, Data Mining, персонализация.*

FORMATION OF ELECTRONIC EDUCATIONAL TRAJECTORY AT TRAINING OF STAFF IN THE FIELD OF SECURITY OF INFORMATION SECURITY

Anastasya Mitrofanova, Sergey Sokolov, Roman Novoselov

Federal State Educational Institution of Higher Education "Admiral Makarov State University of Maritime and Inland Shipping"

198035, Russia, Saint-Petersburg, Dvinskaya str., 5/7

mails: mitrofanovaav@gumrf.ru, sokolovss@gumrf.ru, rnovoselov93@gmail.com

Abstract: Nowadays, students have the opportunity to self-realization and build an individual educational trajectory, as well as provides methods of automated support for the learner in choosing it. Thus, there is an individual educational trajectory (variational learning). Theoretical aspects of the justification of the educational trajectory already exist, then it becomes necessary to develop its practical application in the learning process. The article considers the technology of formation of the electronic educational trajectory is considered when the e-learning system is used.

Keywords: *Electronic individual educational trajectory, Data Mining, personalization, e-learning system, adaptive learning*

Эффективное развитие образования направлено на обеспечение доступности качественного процесса обучения, отвечающего требованиям современного инновационного развития страны. В связи с этим появляются новые формы и способы обучения. Образовательный процесс приобретает личностный характер, у обучающихся в области информационной безопасности появляется возможность самореализации и построения индивидуальной образовательной траектории (вариативного обучения).

Если уже существуют теоретические аспекты обоснования образовательной траектории, то возникает необходимость разработки ее практического применения в процессе обучения.

Рассмотрим технологию формирования электронной образовательной траектории при использовании системы электронного обучения. Данная технология может быть применена при обучении кадров в области обеспечения информационной безопасности, когда электронное обучение и дистанционные образовательные технологии используются в дополнение к традиционному процессу образования, так и при применении дистанционного обучения в чистом виде.

Методология формирования образовательной траектории обучающегося должна строиться вокруг двух основных понятий: механизма планирования образовательной траектории и модели оценки результатов обучающегося.

При разработке системы построения индивидуальной образовательной траектории рекомендуется использовать следующие технологии:

Data Mining - интеллектуальный анализ данных объединяет строго формализованные методы и методы неформального анализа, то есть количественный и качественный анализ данных. Знания, добываемые методами Data mining, представляются в виде моделей. Основные свойства и

характеристики методов Data Mining: точность, масштабируемость, интерпретируемость, проверяемость, трудоемкость, гибкость, быстрота и популярность.

Персонализации - представляет собой отражение интересов пользователя электронного курса, подстраивание обучающего курса под пользователя.

Моделирование алгоритмов поведения пользователей и персонализация играют ключевую роль в адаптации обучающего курса к специфическим характеристикам пользователей. В данном случае очень важно определить эффективные и точные методы извлечения информации о пользовательских предпочтениях и интересах для использования их в дальнейшем в процессе адаптации всего массива информации.

Адаптивное обучение должно реагировать в реальном времени на результаты отдельного обучающегося и его действия в системе. Этот подход увеличивает вероятность того, что будущий специалист в области информационной безопасности получит правильный образовательный контент в нужный момент и достигнет поставленных перед собой целей.

СПИСОК ЛИТЕРАТУРЫ

1. Обзор методов Data Mining [электронный ресурс] - <http://intellect-tver.ru/?p=165>
2. Технология персонализации как метод повышения информационной доступности государственных услуг / Симагина О.В., Цукар С.С. 2016. № 1. с. 160–171 ежеквартальный научно-образовательный журнал.
3. Лексин Василий Алексеевич. Технология персонализации на основе выявления тематических профилей пользователей и ресурсов Интернет. [электронный ресурс] - <http://www.machinelearning.ru/wiki/images/c/c2/Lexin07master.pdf>
4. Адаптивное обучение, или несколько слов о Knewton [электронный ресурс] <https://habrahabr.ru/company/npl/blog/244539/>
5. Чичиленко Е. Концептуальная модель индивидуального подхода к преподавателям и студентам при организации и планировании учебного процесса в вузе // Интернет-ресурс «Хабрхабр» URL: <https://habrahabr.ru/post/195840/> (дата обращения: 20.06.2016).
6. Соколов С. С. Электронная информационно-образовательная среда современно университетского комплекса / С. С. Соколов, Н. М. Ковальногова // Морское образование: традиции, реалии и перспективы: материалы науч.-практич. конф. — СПб.: Изд-во ГУМРФ им. адм. С. О. Макарова, 2015. — Т. 1. — С. 157–163.
7. Нырк А.П., Соколов С.С., Белоусов А.С., Ковальногова Н.М., Мальцев В.А. Обеспечение безопасного функционирования мультисервисной сети транспортной отрасли // Доклады ТУСУР. 2014. №2 (32).
8. Kovalnogova N.M. Model of user identification of electronic informational-educational environment / N. M. Kovalnogova, S. S. Sokolov, A. P. Nyrvov // IOP Conf. Series: Materials Science and Engineering 124 (2016) 012066, 2016. doi:10.1088/1757-899X/124/1/012066
9. Kovalnogova N. Process model development of educational programs using e-learning and distance learning technologies / N. Kovalnogova, S. Sokolov, A. Nyrvov // Proceedings of the 2016 IEEE North West Russia Section Young Researchers in Electrical and Electronic Engineering Conference (2016 ElConRusNW) 2-3 Feb. 2016 St. Petersburg, 2016. — Pp. 817 - 819 doi:10.1109/ElConRusNW.2016.7448310

УДК 004.056

СПОСОБЫ ОПТИМИЗАЦИИ БАЗ ДАННЫХ В ВЫСОКОНАГРУЖЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ НА ТРАНСПОРТЕ

Новоселов Роман Юрьевич, Соколов Сергей Сергеевич, Митрофанова Анастасия Витальевна
ГУМРФ им. С. О. Макарова

Россия, Санкт-Петербург, ул. Двинская, 5/7

emails: rnovoselov93@gmail.com, sokolovss@gumrf.ru, mitrofanovaav@gumrf.ru

Аннотация: В статье рассматривается проблемы производительности баз данных при высоких нагрузках, а также основные способы оптимизации производительности в высоконагруженных информационных системах на транспорте.

Ключевые слова: базы данных; высокие нагрузки; оптимизация; производительность.

METHODS DATABASES OPTIMIZATION IN HIGHLOAD INFORMATION SYSTEMS ON TRANSPORT

Roman Novoselov, Sergey Sokolov, Anastasya Mitrofanova

Admiral Makarov State University of Maritime and Inland Shipping

198035, Russia, Saint-Petersburg, Dvinskaya str., 5/7

emails: rnovoselov93@gmail.com, sokolovss@gumrf.ru, mitrofanovaav@gumrf.ru

Abstract: The article deals with the problem of performance of databases on highload highload, and common methods of performance optimization in highload information systems on transport.

Keywords: databases; highload; optimization; performance.

Введение. В современном мире количество информации неуклонно растет. Существует проблема, которая называется “информационный взрыв” - постоянное увеличение скорости и объемов публикаций (объема информации) в масштабах планеты. Совершенно очевидно, что проблема работы с информацией стоит довольно остро, особенно в рамках одной информационной системы и простые решения тут не подходят. Необходимы способы, которые помогут решить проблему. В данной статье будет дано определение высоконагруженной информационной системе, а также будут рассмотрены основные способы оптимизации нагрузки.

Высоконагруженная ВС — это распределенная ВС, к которой при проектировании и разработке применяются соответствующие техники не только распределенных систем, а также другие, например,

определенные шаблоны при проектировании базы данных, алгоритмика и др. Данное определение основано на определении распределенной вычислительной системы, которое дал Эндрю Таненбаум в своем фундаментальном труде «Распределенные системы. Принципы и парадигмы».

Понятие высоконагруженной информационной системы неразрывно связано с понятием больших данных:

Большие данные (англ. big data) — серия подходов, инструментов и методов обработки структурированных и неструктурированных данных огромных объемов и значительного многообразия для получения воспринимаемых человеком результатов, эффективных в условиях непрерывного прироста, распределения по многочисленным узлам вычислительной сети, сформировавшихся в конце 2000-х годов, альтернативных традиционным системам управления базами данных и решениям класса Business Intelligence.

Примеры задач, в которых используется big data:

- Логи поведения пользователей в интернете.
- GPS-сигналы от автомобилей для транспортной компании.
- Данные, снимаемые с датчиков в большом адронном коллайдере.
- Оцифрованные книги в Российской Государственной Библиотеке.
- Информация о транзакциях всех клиентов банка.
- Информация о всех покупках в крупной ритейл сети и т.д.

Способы оптимизации. Масштабирование баз данных — это одна из самых сложных задач во время роста ИС. Существует очень много практик — денормализация, репликация, шардинг и многие другие. Рассмотрим основные:

Денормализация данных. Существует так называемая нормальная форма хранения данных, которая предполагает избегания дублирования данных. Ключевых правила два:

Атомарность означает, что все сущности хранятся в неделимом виде. Например, если мы храним адрес, то он скорее всего будет поделен на название города, страны и улицу. Все они должны быть представлены отдельными таблицами. Название города будет атомарным, т.к. дальше делиться не будет.

Уникальность требует, чтобы каждая сущность была определена только один раз. Например, название города с идентификатором 1 должно присутствовать только в таблице cities.

Денормализация — это постепенный процесс избавления от правил нормализации там, где это необходимо. Обычно это случаи, в которых есть частые повторные запросы к логически связанным данным [3]. Простым примером является хранение названия города вместе с данными пользователя. Если денормализовать эти данные, то можно будет получить название города одним SQL запросом, а не двумя.

Репликация данных — одна из техник масштабирования баз данных. Состоит эта техника в том, что данные с одного сервера базы данных постоянно копируются (реплицируются) на один или несколько других (называемые репликами). Для приложения появляется возможность использовать не один сервер для обработки всех запросов, а несколько. Таким образом появляется возможность распределить нагрузку с одного сервера на несколько.

Существует два основных подхода при работе с репликацией данных:

1. Репликация Master-Slave;
2. Репликация Master-Master [4].

Шардинг — это принцип масштабирования базы данных, когда данные разделяются по разным серверам. В нашем распоряжении есть два подхода:

Вертикальный шардинг — это простое распределение таблиц по серверам. Например, вы помещаете таблицу users на одном сервере, а таблицу orders на другом. В этом случае, группы таблиц, по которым выполняются JOIN, должны находиться на одном сервере.

Горизонтальный шардинг - разделение очень больших таблиц, которые перестают помещаться на одном сервере, на разные сервера. Это сильно усложняет логику приложения, однако на данный момент не существует лучших механизмов масштабирования [5].

Заключение. Исследование показывает, что наиболее простым и наименее мощным способом оптимизации нагрузки является денормализация данных. Однако, такое решение конечно - невозможно денормализовать данные бесконечно. Репликация и шардинг являются более востребованными способами оптимизации, к тому же могут применяться вместе. В случае разработки архитектуры действительно нагруженной информационной системы необходимо использовать реплики и шарды.

СПИСОК ЛИТЕРАТУРЫ

1. Таненбаум Э. Распределенные системы. Принципы и парадигмы. - СПб: Питер, 2003.
2. Новоселов Р.Ю., Соколов С.С. Тестирование и анализ скорости двух популярных реляционных баз данных при различных нагрузках // Материалы работы науч.-исслед. конф. студентов и аспирантов ф-та информационных технологий. «IT: ВЧЕРА, СЕГОДНЯ, ЗАВТРА — 2016» 11 декабря 2015 г./ Спб.: Изд-во ГУМРФ им. Адмирала С. О. Макарова, 2016
3. Денормализация данных [Электронный ресурс] // Оптимизация и масштабирование Web приложений. URL: <https://ruhighload.com/post/%D0%94%D0%B5%D0%BD%D0%BE%D1%80%D0%BC%D0%B0%D0%BB%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F+%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85> (дата обращения: 19.09.2017)
4. Репликация данных [Электронный ресурс] // Оптимизация и масштабирование Web приложений. URL: <https://ruhighload.com/post/%D0%A0%D0%B5%D0%BF%D0%BB%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F+%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85> (дата обращения: 19.09.2017)

5. 5 стратегий работы с высокими нагрузками в MySQL [Электронный ресурс] // Оптимизация и масштабирование Web приложений. URL: <https://ruhighload.com/post/4+%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D0%B8%D0%B8+%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D1%8B+%D1%81+%D0%B2%D1%8B%D1%81%D0%BE%D0%BA%D0%B8%D0%BC%D0%B8+%D0%BD%D0%B0%D0%B3%D1%80%D1%83%D0%B7%D0%BA%D0%B0%D0%BC%D0%B8+%D0%B2+MySQL> (дата обращения: 19.09.2017)

УДК 004.056

УЯЗВИМОСТИ VOIP

Полугина Юлия Константиновна
ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова»,
Россия, Санкт-Петербург, ул. Двинская, 5/7,
email: u13-@mail.ru

Аннотация: В статье рассматриваются основные способы взлома и хищения трафика в телефонных сетях нового поколения – VOIP сетях. Выявлены наиболее критичные уязвимости данной технологии передачи голосовых данных и предложены методы исключения несанкционированных действий путем построения правильной архитектуры сети и соблюдением рекомендуемых мер и политик безопасности.

Ключевые слова: VOIP; безопасность; перехват трафика; firewall; телефония.

VULNERABILITY VOIP

Polugina Julia
“Admiral Makarov SUMIS”,
Russia, St. Petersburg, Dvinskaya str, 5/7
email: u13-@mail.ru

Abstract: The article considers the main ways of hacking and stealing traffic in next-generation telephone networks - VOIP networks. The most critical vulnerabilities of this technology for voice data transmission are identified and methods for eliminating unauthorized actions are proposed by building the correct network architecture and observing the recommended security measures and policies.

Keywords: VOIP; security; interception of traffic; firewall; telephony.

VOIP как технология пакетной передачи данных все чаще используется в современном обществе, все большие объемы данных, в том числе конфиденциальных, передаются по IP сетям. Такое распространение неизбежно ведет к появлению тех, кто хочет завладеть информацией – как самым ценным ресурсом в настоящее время.

Первым возможным вариантом взлома является «прослушивание» устройств и автоподбор учетных данных к ним. Практически любой тип устройства можно отыскать в сети автоматизированным способом, т.к. оно отвечает на ряд типичных для данного вида устройств запросов. Так и VOIP оборудования постоянно находится в режиме «прослушивания» VOIP сигналов. После обнаружения необходимого устройства начинается подбор логина и пароля устройства. Такой метод возможен, если клиентские устройства и шлюзы выведены непосредственно в сеть Интернет, без использования шлюзов, firewall и транков.

Использование такой функции телефонии как DISA - функция, позволяющая после набора основного номера телефона указать дополнительный номер абонента во внутренней сети в тональном режиме. Служит для организации работы автоматического секретаря. В данном случае злоумышленник может для выясненного по DISA внутреннего номера подобрать в автоматическом режиме пароль и получить авторизацию на чужой АТС.

Инъекция компрометирующих данных в общий трафик является проблемой не только VOIP трафика, а всего IP трафика. Поскольку VOIP – также пакетная передача данных, значит, в общий поток данных со взломанной АТС можно добавить сторонние данные-команды для попытки получения доступа к другой АТС.

Из-за схожести технологий, VOIP АТС можно вывести из строя с помощью DoS атаки, как и любой другой сервис. Это самый простой, эффективный и самый убыточный для атакуемой компании способ вывода из строя телефонии. Данный способ атаки достаточно легко осуществить, если IP АТС подключена к оператору связи через Интернет и не защищена промежуточными устройствами. АТС напрямую получает огромное количество запросов, которые просто не в состоянии обработать, и телефония оказывается парализована.

Тот факт, что общение абонентов может происходить через сеть Интернет, дает возможность мошенникам перехватить сеанс, перехватить данные от клиента к его АТС, подменив часть/полностью данные и получить недостающие данные от клиента, не подозревающего о вводе пароля, например, на сторонней АТС. Или же просканировать используемые по-умолчанию порты 5060, 9000-9049 для передачи данных. На эти порты в первую очередь будут проводиться атаки. Помимо этого, не

некорректно настроенная АТС может иметь «открытые» порты, через которые можно получить к ней доступ (22-ssh, например).

Заключение. В век высоких технологий самой ценной валютой становится информация, получить которую можно все большим числом способов. Защита информации, передаваемой от VOIP АТС – является комплексной задачей, включающей все аспекты организации защиты объектов информатизации – от ограничения физического доступа и защиты firewall-ом, до соблюдения внутренних политик безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Баталова Н. Безопасность VoIP у операторов связи: "классика" IP-сетей и новые задачи // Connect! Мир связи. – 2011. – № 6.
2. Вихров Н.М., Нырков А.П., Шнуренко А.А., Соколов С.С., Некрасова А.А., Полугина Ю.К. Современные методы оптимизации передачи данных в информационно-вычислительных сетях на транспорте // Морской вестник. – 2017. - №1. – С. 95-98.
3. Куриленко Е. Гибридные IP-АТС Yeastar MyPBX U-серии // Технологии и средства связи. – 2013. – № 2. – С. 22–23.
4. Нырков А.П. Обеспечение необходимого режима информационной защищенности активов мультисервисной сети транспортной отрасли / А.П. Нырков, С.С. Соколов, Е.А. Мустакаева, В.А. Мальцев // Проблемы информационной безопасности. Компьютерные системы. –2014. – № 1. – С. 47-51.
5. Нырков А.П., Соколов С.С., Башмаков А.В. Методика проектирования безопасных информационных систем на транспорте // Проблемы информационной безопасности. Компьютерные системы. – 2010. –№ 3. – С. 58–61.
6. Сети ЭВМ: протоколы стандарты, интерфейсы. Ю. Блэк; перев. с англ. - М.: Мир, 1990.
7. Ушанев К.В., Макаренко С.И. Преобразование структуры трафика с учетом требований по качеству его обслуживания // Радиотехнические и телекоммуникационные системы. 2015. № 2 (18). С. 74-84.
8. Hedrick C.L. Routing Information Protocol. RFC 1058, 1988.
9. H. Takagi. Explicit delay distribution in first-come first-served M/M/m/K and M/M/m/K/n queue and a mixed loss-delay system // in Proceedings of Asia-Pacific Symposium on Queueing Theory and Its Applications to Telecommunication Networks, Seoul, Korea, 2006.

УДК 004.056

БЕЗОПАСНАЯ VOIP АТС

Полугина Юлия Константиновна
ГУМРФ имени адмирала С.О. Макарова
Россия, Санкт-Петербург, ул. Двинская, 5/7,
email: u13-@mail.ru

Аннотация: В статье рассматриваются основные способы взлома и хищения трафика в телефонных сетях нового поколения – VOIP сетях. Выявлены наиболее критичные уязвимости данной технологии передачи голосовых данных и предложены методы исключения несанкционированных действий путем построения правильной архитектуры сети и соблюдением рекомендуемых мер и политик безопасности.

Ключевые слова: VOIP; безопасность; перехват трафика firewall; телефония.

SAFE VOIP ATX

Polugina Julia
Admiral Makarov SUMIS
Russia, St. Petersburg, Dvinskaya str, 5/7
email: u13-@mail.ru

Abstract: The article considers the main ways of hacking and stealing traffic in next-generation telephone networks - VOIP networks. The most critical vulnerabilities of this technology for voice data transmission are identified and methods for eliminating unauthorized actions are proposed by building the correct network architecture and observing the recommended security measures and policies.

Keywords: VOIP; security; interception of traffic; firewall; telephony.

Новые технологии, привлекательные и многофункциональные пакеты услуг, низкие расходы на связь побуждают пользователей отказаться от традиционных телефонных услуг в пользу канала передачи голоса по IP. Все больше компаний внедряют VoIP. Но поскольку это система основана на передаче данных через Интернет, она сильно подвержена таким уязвимостям, о которых пользователи обычных телефонных сетей даже не задумываются. К ней, как к технологии передачи разного рода информации, в том числе о конфиденциальной, должны применяться повышенные меры безопасности.

Так запрос выделенной голосовой VLAN – виртуальной сети для подключения VOIP-транка к оборудованию провайдера, вместо подключения к провайдеру через Интернет значительно усложнит задачу взлома мошенниками.

Не лишним будет защитить VOIP оборудование путем «закрытия» его firewall-ом. Этот метод позволяет избежать DoS атак непосредственно на АТС. Существует специализированное оборудование, которое способно обрабатывать большое число запросов, распределять трафик, блокировать атаки. Такое оборудование должно быть у любой компании, обеспеченной защитой своей сети, не только защитой своей телефонии. Если необходимо осуществлять звонки за firewall – через

общедоступную сеть, не лишним будет использовать шифрование. Но надо помнить, что шифрование добавляет «вес» передаваемому трафику, нагружает сеть передачи данных.

Немаловажным фактором является возможность физического доступа к оборудованию, как на территории компании, так и в дата-центрах. Помимо физического необходимо ограничивать и удаленный доступ к оборудованию путем блокировки не используемых портов и установки определенных правил доступа, использования нестандартных портов для управления. Так самое простое правило для доступа к АТС лишь с определенных IP адресов убережет от потенциального взлома.

Защита клиентского оборудования – немаловажный пункт. Конечные пользователи пользуются физическими телефонами или программным обеспечением, оба варианта подключаются к АТС по логину/паролю и могут быть уязвимы. Обновление ПО машины, где установлен VOIP-клиент и защита надежными паролями физических устройств просто необходимы.

Самый простой с точки зрения реализации способ обеспечения безопасности, но порой и очень эффективный – простое соблюдение политик безопасности. Введение обязательных требований к сложности логина/пароля, ограничение на звонки группам пользователей, логирование работы системы – все эти меры помогут внутри компании настроить правила и политики пользования АТС, которые могут предотвратить несанкционированные действия извне.

Закключение. В век высоких технологий самой ценной валютой становится информация, получить которую можно все большим числом способов. Защита информации, передаваемой от VOIP АТС – является комплексной задачей, включающей все аспекты организации защиты объектов информатизации – от ограничения физического доступа и защиты firewall-ом, до соблюдения внутренних политик безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Баталова Н. Безопасность VoIP у операторов связи: "классика" IP-сетей и новые задачи // Connect! Мир связи. – 2011. – № 6.
2. Вихров Н.М., Нырков А.П., Шнуренко А.А., Соколов С.С., Некрасова А.А., Полугина Ю.К. Современные методы оптимизации передачи данных в информационно-вычислительных сетях на транспорте // Морской вестник. – 2017. - №1. – С. 95-98.
3. Куриленко Е. Гибридные IP-АТС Yeastar MyPBX U-серии // Технологии и средства связи. – 2013. – № 2. – С. 22–23.
4. Нырков А.П. Обеспечение необходимого режима информационной защищенности активов мультисервисной сети транспортной отрасли / А.П. Нырков, С.С. Соколов, Е.А. Мустакаева, В.А. Мальцев // Проблемы информационной безопасности. Компьютерные системы. – 2014. – № 1. – С. 47-51.
5. Нырков А.П., Соколов С.С., Башмаков А.В. Методика проектирования безопасных информационных систем на транспорте // Проблемы информационной безопасности. Компьютерные системы. – 2010. – № 3. – С. 58–61.
6. Сети ЭВМ: протоколы стандарты, интерфейсы. Ю. Блэк; перев. с англ. - М.: Мир, 1990.
7. Ушанев К.В., Макаренко С.И. Преобразование структуры трафика с учетом требований по качеству его обслуживания // Радиотехнические и телекоммуникационные системы. 2015. № 2 (18). С. 74-84.
8. Hedrick C.L. Routing Information Protocol. RFC 1058, 1988.
9. H. Takagi. Explicit delay distribution in first-come first-served M/M/m/K and M/M/m/K/n queue and a mixed loss-delay system // in Proceedings of Asia-Pacific Symposium on Queueing Theory and Its Applications to Telecommunication Networks, Seoul, Korea, 2006.

УДК 62; 004; 519.2

ПРИМЕНЕНИЕ МЕТОДОВ СТАТИСТИЧЕСКОГО АНАЛИЗА ДЛЯ ИДЕНТИФИКАЦИЙ ВЕРСИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ УДАЛЕННЫХ АВТОНОМНЫХ ОБЪЕКТОВ ТРАНСПОРТНЫХ СИСТЕМ

Салахутдинова Ксения Иркиновна, Лебедев Илья Сергеевич
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский проспект, 49
emails: kainagr@mail.ru, lebedev@cit.ifmo.ru

Аннотация: В статье рассмотрены общие тенденции к становлению автономных транспортных систем. Приводится актуальность обеспечения информационной безопасности в отношении элементов таких систем, а также предлагается подход к обеспечению безопасности используемого программного обеспечения.

Ключевые слова: транспортные системы; идентификация программ; статистические методы.

THE APPLICATION OF STATISTICAL ANALYSIS METHODS FOR IDENTIFYING VERSIONS OF REMOTE AUTONOMOUS TRANSPORTATION SYSTEM OBJECTS

Salakhutdinova Kseniya, Lebedev Ilya
ITMO University, Russia, St. Petersburg, Kronverkskiy pr., 49
emails: kainagr@mail.ru, lebedev@cit.ifmo.ru

Abstract: The article presents the general trends towards the formation of autonomous transportation systems. The relevance of information security in respect of such system elements is given and an approach to secure of used software is proposed.

Keywords: *transportation system; program identification; statistical methods.*

В настоящее время во многих странах происходят кардинальные изменения в сфере организации транспортного процесса и процесса управления транспортными средствами. Причиной этому является необходимость в решении таких вопросов как обеспечение безопасности дорожного движения, а также повышение эффективности транспортной логистики [1].

Уже сейчас и в обозримом будущем движение в этой области будет происходить в сторону развития интеллектуальных транспортных систем (ИТС), которые не только будут представлять собой систему помощи водителю, но смогут и вовсе исключить его из процесса дорожного движения.

Таким образом, наблюдается становление автономных транспортных систем, например, в ряде населенных пунктов Японии действуют автономные автобусы-шаттлы, нацеленные на предоставление пожилым жителям регионов более простого доступа к медицинским, торговым и банковским услугам. Россия также заинтересована в этом процессе, Владимир Путин поручил правительству России подготовить предложения по созданию российской сервисной информационно-телематической платформы, которая в перспективе должна стать специализированной инфосредой для движения беспилотного транспорта.

Интеллектуальная транспортная система состоит из множеств компонентов, которые можно объединить в несколько классов:

- Системы и датчики внутри контролируемых транспортных средств.
- Системы позиционирования GPS и ГЛОНАСС.
- Инфраструктура дороги.
- Центры мониторинга и анализа за движением.

Возлагаемые функции на транспортное средство уже сегодня приводят к гигабайтам кода, отвечающего за логику управления и анализ телеметрии от различных датчиков [2]. Такая сложная система нуждается в защите от несанкционированного вмешательства по отношению к каждому элементу ИТС.

Подход к обеспечению безопасности, предлагаемый авторами, заключается в идентификации программ удаленных автономных транспортных систем, т.е. обеспечение контроля установленного программного обеспечения (ПО). Под идентификацией стоит понимать процесс отождествления некоторой идентифицируемой программы с уже известной. Данный подход позволяет рассматривать два варианта контроля установки программ на объекте:

- Запрещено устанавливать какое-либо ПО, кроме разрешенного.
- Разрешено устанавливать какое-либо ПО, кроме запрещенного.

Рассмотрим сам процесс идентификации. Идентифицируемая программа рассматривается как совокупность частот встречаемости того или иного признака (в качестве такового рассматривались значения побайтового или ассемблерного кода программ) и после некоторых преобразований формируется ее сигнатура. В дальнейшем сигнатура идентифицируемой программы поочередно сравнивается с другими сигнатурами известных программ, которые хранятся в архиве сигнатур. Очевидно, что построение архива сигнатур происходит заранее и требует более сложного подхода.

Известно, что программы не создаются раз и навсегда, с течением времени в них вносят изменения и выпускают их новые версии. Предлагаемый метод по построению сигнатуры программы для архива, заключается в создании такой структуры, которая учитывала бы изменения различных версий, а также подходила для идентификации новой версии программы, не задействованной ранее в формировании архивной сигнатуры.

Сравнение идентифицируемой сигнатуры и сигнатуры из архива, с целью идентификации изучаемой программы, происходит с помощью методов статистического анализа, таких как: критерий однородности хи-квадрат и критерий Колмогорова. Первый критерий позволяет проверить гипотезу о том, что две выборки (сигнатуры) принадлежат одной и той же генеральной совокупности или их генеральные совокупности – одинаковы. Второй критерий позволяет проверить гипотезу о том, что рассматриваемая выборка (идентифицируемая сигнатура) распределена по заданному закону распределения [3].

Таким образом, архив сигнатур может выступать в роли белого или черного списков ПО. Очевидно, что, выступая в роли белого списка, представленный подход по идентификации программ не защитит систему от вредоносного кода, внедренного в устанавливаемую программу из белого списка. В тоже время, выступая в роли черного списка, представленный подход по идентификации программ в состоянии защитить систему от нежелательной программы, даже если в нее были внесены некоторые изменения.

СПИСОК ЛИТЕРАТУРЫ

1. Жанказиев С. В., Воробьев А. И., Морозов Д. Ю. Тенденции развития автономных интеллектуальных транспортных систем в России // Транспорт российской федерации. 2016. №5(66). С. 26-28.
2. Positive Technologies. Умный транспорт: Новые вызовы информационной безопасности // Хабрахабр, Блог компании Positive Technologies. 2016. [Электронный ресурс]. URL: <https://habrahabr.ru/company/pt/blog/302194/> (дата обращения: 17.09.2017).
3. Фадеева Л.Н., Лебедев А.В. Теория вероятностей и математическая статистика: учеб. пособие. – М.: Рид Групп, 2011 – 496 с.



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

УДК 629.12.001.2

ЭКСПЕРИМЕНТАЛЬНАЯ ОТРАБОТКА ТЕХНОЛОГИИ ОТМУ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ ПРОГРАММОЙ РАЗВИТИЯ ОМТИ

Александров Владимир Леонидович¹, Алексеев Анатолий Владимирович¹,
Поляничко Виктор Викторович², Ходан Сергей Владимирович³

¹Санкт-Петербургский государственный морской технический университет,
Россия, Санкт-Петербург, ул. Лоцманская, 3,

²ООО «Центр Научных Исследований и Разработок «Кристалл»,
Россия, Санкт-Петербург, Набережная Петроградская, 34, литер «Б»

³АО «Адмиралтейские верфи»,

Россия, Санкт-Петербург, наб.р. Фонтанки, 203,

emails: fckps@rambler.ru, 17151@bk.ru, info@ashipyards.com, centercrystal@mail.ru.

Аннотация: По результатам опытной эксплуатации программно-аппаратного комплекса «СОТМУ-ТЦ» в Техническом центре АО «Адмиралтейские верфи» выполнен анализ отработки в защищенном исполнении технологии организационно-технического мониторинга, прогнозирования и управления жизненным циклом современных систем морской техники и морской инфраструктуры на основе реализованной технологии СПРУ в варианте СОТМУ. Систематизированы предложения по широкомасштабному внедрению новой технологии и повышению качества организационно-технического мониторинга и управления жизненным циклом сложных человеко-машинных систем объектов морской техники и инфраструктуры, инвариантной к их специфическим свойствам.

Ключевые слова: объекты морской техники; качество управления; организационно-технический мониторинг; управление жизненным циклом.

DEVELOPMENT TEST OF TECHNOLOGY OF OTMA IN A SECURE EXECUTION PROGRAM FOR THE DEVELOPMENT OF OMTI

Vladimir Aleksandrov¹, Anatoly Aleksee¹, Viktor Polyanychko², Sergei Khodan³

¹Saint-Petersburg state marine technical University,
Russia, Saint-Petersburg, street Pilot, 3,

²Center of Scientific Research and Development "Crystal",
Russia, Saint-Petersburg, Petrograd Embankment., 34, liter "B"

³JSC "Admiralty shipyards",

Russia, Saint-Petersburg, Fontanka emb., 203,

emails: fckps@rambler.ru, 17151@bk.ru, info@ashipyards.com, centercrystal@mail.ru

Abstract: According to the results of trial operation of hardware and software complex "SOTA-TTS" in the Technical centre of JSC "Admiralteiskie Verfi" the analysis of mining in protected execution technology organizational and technical monitoring, forecasting and lifecycle management of modern systems for marine engineering and marine infrastructure on the basis of the implemented technology SPRU in the embodiment of SOTMU. Systematic proposals for large-scale introduction of new technology and improve the quality of organizational and technical monitoring and lifecycle management of complex man-machine systems marine facilities and infrastructure, invariant to their specific properties.

Keywords: the marine facilities, quality control, organizational and technical monitoring and lifecycle management.

Одной из основных критических проблем развития объектов морской техники (ОМТ) и объектов морской инфраструктуры (ОМТИ), характерных не только для кораблестроения, судостроения, но и для управления эргатическими (человеко-машинными) системами в целом, является системная проблема контроля качества и информационной защищенности управления ОМТИ в целом (СПККУ). Доказательством этому служит особое внимание, которое уделяется в последнее десятилетие

развитию в целом систем управления (менеджмента) качеством (СМК) организаций и предприятий при выпуске продукции любого вида и предоставлении различных услуг.

Обусловлено это характерным для настоящего времени интенсивным технологическим развитием общества, включая развитие информационных технологий и их защищенности [1, 2]. Еще более значимой СПККУ ОМТИ является при рассмотрении вопросов управления структурой и качеством жизненного цикла (ЖЦ) продукции и услуг. Причем, с учетом метрологически обеспеченной точности на всех этапах (стадиях), включая концептуальное и исследовательское проектирование, разработку рабочей и конструкторской документации, создание и все виды испытаний опытных образцов, головных проектов, а также освоения и эксплуатации ОМТ, его модернизацию [3, 4].

Контрольными точками реализации и оценки качества частных и групповых процедур управления и, соответственно, эффективности решения своих функциональных задач являются конкретные критерии качества решения частных, групповых и системной задачи с показателями качества и эффективности успешности их реализации. Например, по показателю доли (в %) решения на установленный срок каждой решаемой задачи. На качественном уровне этот алгоритм используется практически всегда, но контрольной точкой являются оценки только на конечную дату.

Это по существу не позволяет в реальном масштабе времени на количественном уровне контролировать решение каждой из задач с оценкой достаточности этого на конечную дату, что порождает соответствующих риск управления, возможности нештатных обстоятельств и т.п.

Системным решением данной проблемы следует считать введение в процесс управления процедуры непрерывного автоматизированного наблюдения (мониторинга), прогнозирования и управления развитием обстановки [1 - 4]. Именно такой подход используется в разработанной в 2012-2016 г.г. специализированной технологии системной поддержки принятия управленческих решений и управления (технологии СПРУ) [4]. В адаптированном виде она была в 2016-2017 г.г. реализована применительно к решению ежедневных, недельных, месячных, квартальных и годовых задач организационно-технического мониторинга управления в рамках сформулированной СПККУ [1] на одном из объектов АО «Адмиралтейские верфи», а именно - в его Техническом центре (ТЦ).

По результатам опытной эксплуатации установленного в ТЦ программно-аппаратного комплекса «СОТМУ-ТЦ», реализованного на основе технологии СПРУ в варианте СОТМУ, выполнен анализ отработки в защищенном исполнении технологии организационно-технического мониторинга, прогнозирования и управления. Реализация СОТМУ подтвердила заявленные возможности, удобство эксплуатации с ежедневными временными затратами порядка 15 минут на каждом рабочем месте и высокую результативность с возможностью: упреждения угроз невыполнения заданных требований по каждой из производственных задач; контроля достигаемого ежедневно уровня качества; упреждения потери управления каждым структурным подразделением и ТЦ в целом и других.

Систематизированы предложения по широкомасштабному внедрению инвариантной к специфическим свойствам объектов управления технологии СПРУ-СОТМУ в обеспечение контроля и повышения качества, организационно-технического мониторинга и управления жизненным циклом сложных человеко-машинных систем объектов морской техники и инфраструктуры, включая:

- целесообразность и практическую возможность расширения СОТМУ, в первую очередь, на ключевые структурные подразделения типа Инженерный центр, а также всего предприятия в целом;
- перспективность реализованного технологического решения по обеспечению системного контроля качества, его прогнозированию и информационной поддержке и организационно-техническому управлению жизненным циклом продукции и услуг организаций и предприятий;
- целесообразность и практическую возможность с учетом накопленного опыта внедрения предложенной отечественной технологии и средств её реализации на других предприятиях отечественного судостроения и кораблестроения, включая подготовку кадров [4], ввиду инвариантности к специфике решаемых задач СПККУ и предложенного её технологического решения;
- целесообразность отнесения данной технологии и средств её реализации к типовому проектному решению для задач автоматизированного управления сложными, в том числе критическими человеко-машинными комплексами и системами для объектов типа ОМТИ, ситуационных центров, центров управления комплексной безопасностью, включая центры управления информационной безопасностью, центры сетецентрического противоборства [5].

СПИСОК ЛИТЕРАТУРЫ

1. Александров В.Л., Алексеев А.В., Поляничко В.В., Ходан С.В. Проблема организационно-технического мониторинга, прогнозирования и управления жизненным циклом / Четвертая международная научно-практическая конференция «Имитационное и комплексное моделирование морской техники и морских транспортных систем» (ИКМ МТМТС-2017). Труды конференции – СПб.: АО «ЦТСС», 2017, с. 11 – 15.
2. Информационные технологии в системе управления силами ВМФ (теория и практика, состояние и перспективы развития). – СПб.: «Эльмор», 2005. – 832 с.
3. Алексеев А.В. Вербальная модель процессов стратегического развития объектов морской техники и инфраструктуры / Корабельная энергетика: из прошлого в будущее: материалы Всероссийского межотраслевого научно-технического форума. – СПб.: Изд-во СПбГМТУ, 2017, с. 324 – 329.
4. Алексеев А.В. Принципы и технология квалитетической оценки уровня подготовки командира корабля и специалистов по борьбе за живучесть оружия и технических средств / X Научно-практическая конференция «Актуальные проблемы

профессиональной подготовки командиров кораблей и специалистов ВМФ». ВУНЦ ВМФ «ВМА»: ВИДПО, 30 мая 2017 года – СПб.: ВИДПО ВУНЦ ВМФ «ВМА», 2017, с.5-12.

5. Алексеев А.В. Проблема мониторинга информационной безопасности при информационном противоборстве и пути её решения / Материалы 9-й конференции «Информационные технологии в управлении» (ИТУ-2016). – СПб.: АО «Концерн «ЦНИИ «Электрон», 2016, с. 641-650.

УДК 629.12

АДАПТИВНЫЙ АЛГОРИТМ ПРОГНОЗИРОВАНИЯ РАЗВИТИЯ IS-ОБСТАНОВКИ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И ИНФРАСТРУКТУРЫ

Алексеев Анатолий Владимирович, Мусатенко Роман Иванович, Киселев Валерий Михайлович
НП «Институт автоматизации процессов борьбы за живучесть корабля, судна»
198262, Санкт-Петербург, Ленинский проспект, 101, пом. 162.
email: iapbgks@bk.ru

Аннотация: Рассмотрена проблема обеспечения комплексной безопасности на объектах морской техники и инфраструктуры, прогнозирования и контроля обстановки по информационной безопасности (IS). Представлен один из перспективных вариантов технологии прогнозирования IS-обстановки по данным мониторинга состояния информационной защищенности ресурсов на основе адаптивного алгоритма регрессионного анализа. Приведены результаты численного эксперимента и устойчивости функционирования алгоритма при его программной реализации в составе программного комплекса «СПРУ-ИС.01». Реализация адаптивного алгоритма прогнозирования развития данных мониторинга обеспечивает минимальную погрешность регрессионного анализа данных за счет управления выбором типа альтернативной модели регрессии по критерию минимума погрешности.

Ключевые слова: объекты морской техники и инфраструктуры; мониторинг обстановки; технологии прогнозирования; адаптивный алгоритм; IS-обстановка.

ADAPTIVE PREDICTION ALGORITHM DEVELOPMENT IS-ENVIRONMENT, MARINE FACILITIES AND INFRASTRUCTURE

Anatoly Alekseev, Roman Musatenko, Valery Kiselyov
NP "Institute of automation of processes of struggle for survivability of the ship, ship"
Russia, St. Petersburg, Leninsky Prospekt, 101, of. 162.
email:iapbgks@bk.ru

Abstract: The problem of integrated security at marine facilities and infrastructure, forecasting and control environment for information security (IS). Represented one of the most promising options for technology forecasting IS-of the situation according to the monitoring the condition of information security resources based on the adaptive algorithm and regression analysis. The results of numerical experiment and stability of the algorithm with its implementation in the structure of a program complex "SPRU-IS.01". Implementation of the adaptive prediction algorithm development, data monitoring provides the minimum error of the regression analysis of the data by management type selection alternative regression model with the criterion of minimum error.

Keywords: the marine facilities and infrastructure; monitoring of the environment; technology forecasting; adaptive algorithm; IS-furnished.

Введение. Среди проблем развития риск-ориентированных технологий систем автоматизации управления объектами морской техники и морской инфраструктуры (ОМТИ) особое место занимают технологии и системы информационно-аналитической и интеллектуальной поддержки принятия решений (ИСППР) в составе автоматизированных систем в защищенном исполнении (АСЗИ).

Научно-методические и технологические аспекты формирования такой поддержки для повышения качества управления и, прежде всего, в условиях обеспечения комплексной безопасности эксплуатации, локализации аварийных ситуаций и аварий, борьбы за их живучесть являются востребованными, как никогда ранее. В том числе с учетом интенсивного развития информационных технологий и появления критической уязвимости объектов информатизации – необходимости обеспечения их информационной безопасности (ИБ), эффективной защиты информационных ресурсов (ИР) [1, 2].

Создание в этих условиях эффективных ИСППР с учетом тенденции наращивания сложности объектов информатизации, мониторинг защищенности ИР, прогнозирование и контроль обстановки в информационной сфере (ИСППР-ИС) имеет особое значение для обеспечения комплексной безопасности и минимизации эксплуатационных рисков объектов информатизации различного рода.

Тем не менее, эта задача наряду со своей новизной представляется весьма сложной системно и сегодня практически не решается. Попытки же решить данную проблему только за счет потенциала администраторов ИБ (офицеров ИБ) весьма ограничены в связи с высокой динамикой и масштабами проявления современных атак на защищаемые информационные ресурсы (ИР). В этих условиях факты

выявления информационных вторжений на 90-е сутки становятся в ряде случаев характерными и исключающими активные действия по защите ИР.

Предлагаемое технологическое решение по построению и функционированию ИСППР-ИС позволяет обеспечить наряду с оценкой комплексных показателей качества информационной безопасности (IS) по критерию агрегированных показателей качества (АПК), мониторингу получаемых оценок АПК, но и прогнозирование развития IS-обстановки по этим данным.

Для этого предложен, обоснован и реализован специализированный адаптивный алгоритм прогнозирования развития обстановки на основе управляемого выбора по критерию минимума погрешности прогнозирования из числа параллельных альтернативных алгоритмов регрессионного анализа данных мониторинга по каждому из каналов контроля частных, групповых, модельных и АПК.

В этом контексте с учетом опыта активного развития в последние годы технологии и систем поддержки принятия решений и управления (СПРУ) применительно к ОМТИ [3 - 5] признано целесообразным в качестве главного критерия безопасности использовать АПК IS-обстановки. Он оценивается в % и характеризует состояние безопасности ИР в информационной сфере, определяемое защищенностью жизненно-важных ИР в АСЗИ объекта информатизации от внутренних (инсайдеры) и внешних (нарушителей регламентов ИБ) угроз, при котором поддерживается заданное значение АПК ИБ и соответствующих свойств.

Анализ практик решения данной проблемы в смежных областях [5, 6] показал, что, комплексный мониторинг частных (ЧПК), групповых (ГПК), модельных показателей качества (МПК), а также определяемого через них АПК (сводного, интегрального, системного) [3], их использование в процессе информационно-аналитической и интеллектуальной поддержки принятия проектных и управленческих решений (ПУР) позволяет на качественно новом уровне не только оценивать обстановку в информационной сфере, но и эффективно прогнозировать её развитие с упреждением от (5...15) минут, включая обнаружение, идентификацию и классификацию информационных инцидентов (ИИ, «аварийных ситуаций» в информационной сфере). Более того, выбирать наиболее предпочтительные варианты системных ПУР, корректировать действия лиц, обосновывающих (ЛОР), принимающих (ЛПР) ответственные ПУР, а также лиц, исполняющих эти решения (ЛИР). То есть, в целом эффективнее и результативнее управлять ИИ с их локализацией и упреждением.

К главным конкурентным преимуществам представляемого технологического решения прогнозирования развития обстановки в информационной сфере могут быть отнесены: минимизация избыточности представления данных операторам с использованием 2-х битового цветового кодирования возможных состояний обстановки по каждому из ЧПК, ГПК и АПК; максимизация охвата функций операторов контурами автоматической обработки данных и поддержки принятия решений; прогнозирование развития обстановки с упреждением до (10...15) циклов принятия решений; представление проектов управленческих решений в текстовой форме с возможностью звуковой трансляции на посты управления; масштабируемость разработанных технологических решений с возможностью инвариантной адаптации к условиям ИСППР-ИС АСЗИ.

Заключение. В современных условиях интенсивного развития информационных технологий и актуализации задач совершенствования средств и систем ведения противоборства в информационной сфере, непрерывного обновления (модернизации) используемых средств обеспечения защищенности информационных ресурсов одним из приоритетных направлений технологического развития следует считать создание интеллектуальных систем поддержки принятия решений для обеспечения превосходства в информационной сфере на основе технологий и средств прогнозирования развития обстановки, интегрированных в существующие АСЗИ по всем контурам управления, обеспечения их конкурентной способности и перспективности развития.

Эффективное и конкурентно способное построение и использование ИСППР-ИС позволит наряду с повышением оперативности, достоверности, устойчивости, скрытности и непрерывности управления за счет реализации возможностей информационно-аналитической и интеллектуальной поддержки принятия решений ЛОР, ЛПР и ЛИР минимизировать негативное влияние субъективных факторов операторов, что сегодня является одной из наиболее актуальных задач развития. В условиях существенного возрастания функциональности и сложности систем реализация представленных возможностей квалитетической оценки, мониторинга и прогнозирования развития обстановки является одним из новых источников риск-ориентированного технологического развития, обнаружения, идентификации и классификации информационных инцидентов, их упреждения и эффективной нейтрализации, что приобретает особое значение и важность.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А.В., Смольников А.В., Ушакова Н.П., Сус Г.Н. Программный комплекс Макетного действующего образца Системы информационной поддержки судоводителей при обеспечении безопасности эксплуатации в части грузовых операций, локализации аварийных ситуаций, аварий и борьбы за живучесть морских объектов повышенного риска (ПК МДО СИП ЛА-ГО оз) – Свидетельство о государственной регистрации программ для ЭВМ. Реестр программ Федеральной службы по интеллектуальной собственности № 2014614620, 29.04.2014 (заявка № 2014611813, 05.03.2014).
2. Алексеев А.В. Вербальная модель процессов стратегического развития объектов морской техники и инфраструктуры / Корабельная энергетика: из прошлого в будущее: материалы Всероссийского межотраслевого научно-технического форума. – СПб.: Изд-во СПбГМТУ, 2017. С. 324 – 329.

3. Алексеев А.В., Мусатенко Р.И., Каганский М.А. Оценка конкурентной способности риск-ориентированных технологий обеспечения безопасности объектов морской техники / XX Всероссийская научно-практическая конференция «Актуальные проблемы защиты и безопасности», Санкт-Петербург, 05 апреля 2017 года. – СПб.: ГПУ, 2017.
4. Алексеев А.В., Согонов С.А., Пшеничная К.В., Максимова М.А., Прокофьева О.Е. Обеспечение безопасности автоматизированных информационных систем объектов морской техники / Методы и средства обеспечения безопасности информации: Материалы 26-й научно-практической конференции 26-29 июля 2017 г. СПб: Изд-во Потитехн. ун-та, 2017. С. 49 – 50.

УДК 629.12.001.2

ПРОБЛЕМА КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ОМТИ И ЕЁ РАЗРЕШЕНИЕ НА ОСНОВЕ ОПТИМАЛЬНЫХ ИНТЕГРАЦИОННЫХ РЕШЕНИЙ

Алексеев Анатолий Владимирович

Санкт-Петербургский государственный морской технический университет,
Россия, Санкт-Петербург, ул. Лоцманская, 3,
emails: iapbgks@bk.ru

Аннотация: Рассмотрена проблема критичности неравнопрочной архитектуры сложных систем обеспечения комплексной безопасности на примере объектов морской техники и инфраструктуры и концепция её разрешения на основе синтеза оптимальных структур с элементами квазиравной корневой чувствительности. Приведены примеры и квалиметрические оценки комплексной безопасности типовых ОМТИ, реализующие концепцию оптимальных интеграционных решений по построению и эксплуатации автоматизированных систем в защищенном исполнении.

Ключевые слова: интеграционное решение; комплексная безопасность; системные показатели качества; оптимизация; корневая чувствительность.

THE PROBLEM OF INTEGRATED SECURITY, OMTI AND ITS RESOLUTION BASED ON THE OPTIMAL INTEGRATION SOLUTIONS

Anatoly Alekseev

State Marine Technical University of St. Petersburg,
Russia, Saint-Petersburg, Lotsmanskaya Str. 3,
emails: iapbgks@bk.ru

Abstract: The problem of unequal sensitivity of complex systems architecture integrated security on the example of marine facilities and infrastructure and the concept of permission-based synthesis of optimal structures with elements vazirani root sensitivity. Examples of qualitative assessments and comprehensive security model FRTTO implementing the concept of optimal integration solutions for the construction and operation of the automated systems in the protected execution.

Keywords: integration solution; integrated security; system quality indices; optimization; root sensitivity.

Введение. Среди проблем повышения качества и эффективности современных систем автоматизации и обеспечения комплексной безопасности объектов морской техники и инфраструктуры (ОМТИ) все большее значение приобретают системные аспекты комплексирования и интеграции средств и систем. Среди них традиционно сложными, но не менее актуальными остаются задачи измерения, мониторинга и контроля качества и эффективности ОМТИ по критерию комплексной безопасности (КБ) с учетом таких критических факторов, как структурная (УС) и функциональная устойчивость (УФ), информационная безопасность (ИБ), информационная устойчивость (УИ) и живучесть (УЖ), робастность и других [1].

При этом, результаты исследовательского проектирования КБ, анализа и синтеза оптимальных вариантов построения и функционирования ОМТИ (кораблей, судов, включая критические атомные, а также подводных трубопроводов, морских платформ, портов, судостроительных предприятий и организаций и т.п.) и их основных элементов (корабельных и судовых технических систем, включая информационно-коммуникационные системы, а также навигационного, портового оборудования и т.п.) показывают, что одним из принципиальных направлений обеспечения их комплексной безопасности эксплуатации, локализации (минимизации возможности) возникновения аварийных ситуаций и аварий (ЛА), техногенных и экологических происшествий и катастроф следует считать проектное обоснование и применение равнопрочных (квазиравных) по системным (агрегированным) показателям качества (АПК) и эффективности элементов в составе обеспечивающих систем и ОМТИ в целом, а также архитектур (структур) их объединения (интеграции).

Именно концепция синтеза равнопрочных элементов и структур систем (КРС) за счет внутренних эмерджентных, синергетических свойств систем типа ОМТИ позволяет минимизировать число уязвимостей и угроз КБ, а, следовательно, обеспечить максимизацию УС, УФ, ИБ, УИ, УЖ.

В этом контексте представляется целесообразным использовать следующую методику оптимизации интеграционных решений:

1. В рамках анализа качества и эффективности ОМТИ при обязательном условии использования полномасштабных моделей квалиметрического оценивания (количественного измерения проектного качества и меры его обеспечения при эксплуатации) выбрать, либо разработать программный комплекс (ПК) оценки агрегированного показателя качества по критерию КБ на основе полимодельной свертки УС, УФ, ИБ, УИ, УЖ и т.п. с использованием соответствующих индексов критериальной значимости, при экспертной оценке которых будут учтены квалификация и опыт экспертов, а также специфика функционирования ОМТИ и адекватность используемой модели. Например, этим условиям вполне соответствует ПК «АСОР» разработки СПбГМТУ (2008 г.).

2. На основе вариантного сравнительного анализа определить (вычислить) матрицу индексов корневой чувствительности с соответствующими оценками их надежности.

3. Решить задачу вариантного синтеза и оптимизации структуры (архитектуры) анализируемой системы (ОМТИ) с обоснованным выбором её элементов, удовлетворяющих критерию оптимизации, позволяющего максимизировать системный показатель качества ОМТИ по критерию КБ.

Практика реализации приведенной методики оптимизации интеграционных решений показывает, что, действительно, обоснование выбора элементов системы является весьма критическим проектным процессом. Для минимизации проектных рисков рекомендуется при наличии аппарата оценки и контроля качества (типа ПК «АСОР») расширять ряд альтернативных вариантов при условии контроля адекватности (соответствия) используемых при оценках их параметров и характеристик. Последнее условие обеспечивается, как правило, наличием у выбираемых элементов ОМТИ сертификатов соответствия, а также, что более предпочтительно, сертификатов качества, подтверждающих достигнутые показатели не только соответствия, но и уровня качества [2].

Кроме того, рекомендуется критически подходить при оптимизации интеграционных решений к вопросу минимизации структурной и функциональной избыточности [3]. Последнее в целом ряде случаев удастся достигнуть за счет оптимального распределения функций внутри системы и соответствующего исключения функционального дублирования при выборе элементов системы. Эта тенденция проявляется часто, например, при анализе функций средств обеспечения ИБ.

Среди других перспективных путей решения КРС, проблемы оптимизации интеграционных решений, подтверждаемых практикой проведенных исследований и исследовательского проектирования могут быть названы: мониторинг динамики варьирования АПК по критерию КБ; формирование матрицы и базы данных динамических образов для типовых аварийных ситуаций и ЛА; прогнозирование развития КБ по системным, а также групповым и частным показателям качества; факторный анализ динамики АПК по критерию КБ с целью прогнозирования их поведения, мониторинг и контроль с учетом баз данных по самым «проблемным» факторам – человеческим.

Опыт исследований по КРС показывает, что вариантный анализ проектных интеграционных, системных, архитектурных, алгоритмических и технических решений и, безусловно, их оптимизация достаточно доступны при реализации на основе современных возможностей вычислительной техники и информационных технологий в целом, а также с учетом использования научно-технических результатов по квалиметрическому обоснованию ранжирования качества средств и систем обеспечения сегментов и КБ в целом, разработанной методологии обоснования оптимальных путей наращивания конкурентной способности и оптимальных путей перспективного развития ОМТИ.

В этих условиях, по нашему мнению, при реализации КРС именно переход к парадигме оптимизации интеграционных решений с парадигмой непрерывного оценивания, мониторинга и контроля системных показателей качества и эффективности [4] позволят обеспечить существенный скачок уровня проектного и эксплуатационного качества и комплексной безопасности современных автоматизированных систем ОМТИ в защищенном исполнении, безопасности их эксплуатации, минимизации рисков возникновения аварийных ситуаций и аварий, техногенных катастроф, обеспечения безопасности персонала при эксплуатации ОМТИ.

Заключение. Приобретающую все большую актуальность проблему обеспечения комплексной безопасности ОМТИ целесообразно решать, как показывают результаты и опыт проведенных исследований и многочисленных вариантов исследовательского проектирования, на основе оптимизации принимаемых проектных и управленческих решений, реализуя концепцию равнопрочных структур (КРС). Решений, принимаемых должностными лицами, в процессе интеграции сертифицированных технических решений, а также аттестованных организационных и технологических решений по критерию максимизации полимодельного агрегированного показателя комплексной безопасности современных сложных систем типа ОМТИ.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А.В. Технологические аспекты автоматизации процессов борьбы за живучесть корабля, судна / Актуальные проблемы морской энергетики: материалы второй Всероссийской межотраслевой научно-технической конференции. – СПб.: СПбГМТУ, 2013, с. 16 – 20.
2. Алексеев А.В., Антипов В.В., Бобрович В.Ю., Смольников А.В. Концепция и технология ранговой партнерской сертификации объектов морской техники и инфраструктуры / Материалы конференции «Информационные технологии в управлении» (ИТУ-2014). ГНЦ РФ ОАО «Концерн «ЦНИИ «Электрон». Спб., 7-9.10.2014 – СПб.: ОАО «Концерн «ЦНИИ «Электрон», 2014, с. 29-34.

3. Алексеев А.В. Технологии минимизации избыточности при мониторинге и управлении информационной безопасностью критических объектов / Информационная безопасность регионов России (ИБРР-2015). IX Санкт-Петербургская межрегиональная конференция. Санкт-Петербург: Материалы конференции / СПОИСУ. – СПб., 2015. с. 227-228.
4. Алексеев А.В. Проблема мониторинга информационной безопасности при информационном противоборстве и пути её решения / Там же, с. 641-650.

УДК 629.12

**ПРОБЛЕМА СИСТЕМАТИЗАЦИИ ЛУЧШИХ ПРАКТИК И ФОРМИРОВАНИЯ ТРЕБОВАНИЙ
К РАЗВИТИЮ СИСТЕМ АВТОМАТИЗАЦИИ И УПРАВЛЕНИЯ ЖИЗНЕННЫМ ЦИКЛОМ ОМТИ
В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ**

Алексеев Анатолий Владимирович, Тычинин Игорь Юрьевич, Мусатенко Роман Иванович
Институт автоматизации процессов борьбы за живучесть корабля, судна,
Россия, Санкт-Петербург, Ленинский пр., 101, оф. 162,
emails: iapbgks@bk.ru

Аннотация: Рассмотрены специфика и концепция решения проблемы систематизации лучших практик, а также формирования требований к развитию автоматизированных систем в защищенном исполнении с учетом всего жизненного цикла объектов морской техники и морской инфраструктуры. Это позволяет обоснованно решать системную задачу развития конкурентно способных технологий и образцов морской техники, включая требования по обеспечению их информационной защищенности, на основе методов квалиметрической оценки ОМТИ и их ранжирования.

Ключевые слова: лучшие практики; защищенное исполнение; жизненный цикл; конкурентная способность; системная оптимизация.

**THE PROBLEM OF SYSTEMATIZATION OF BEST PRACTICES AND BUILDING REQUIREMENTS FOR
DEVELOPMENT OF SYSTEMS OF AUTOMATION AND LIFECYCLE MANAGEMENT OMTI IN A
SECURE EXECUTION**

Anatoly Alekseev, Igor Tychinin, Roman Musatenko
Institute of automation of processes of struggle for survivability of the ship, vessel,
Russia, Saint-Petersburg, Leninsky prospect, d. 101, of. 162,
emails: iapbgks@bk.ru

Abstract: The specifics and the concept of the solution of a problem of systematization of best practices and building requirements for the development of automated systems in the protected execution taking into account the entire life cycle of the marine facilities and marine infrastructure. This allows to reasonably address the systemic problem of development of competitive technologies and samples of marine engineering, including requirements to ensure their information security, based on the methods of qualimetric assessment of OMTI and their ranking.

Keywords: best practices; secure execution; life cycle; competitive ability; system optimization.

Введение. Среди перспективных направлений развития автоматизированных систем управления (АСУ) объектов морской техники и инфраструктуры (ОМТИ) в условиях активного внедрения новых информационных технологий, включая технологии информационной безопасности (ИБ), все большее внимание уделяется системным требованиям обеспечения конкурентной способности разрабатываемых и создаваемых АСУ в защищенном исполнении (АСЗИ) с учетом всех стадий их жизненного цикла (ЖЦ). Причем, одним из традиционных резервов на этом направлении по-прежнему остаётся вариантное сравнение разрабатываемых средств с наиболее эффективными сравнительными свойствами и характеристиками АСЗИ [1, 2, 3].

Вместе с тем, в последние десятилетия этому препятствует целый ряд обстоятельств, включая: расширение спектра разрабатываемых аналогов каждого из типов и классов АСЗИ; существенное снижение возможностей получения конкретных (предметных) данных по описанию альтернативных вариантов АСЗИ, а также их качества и достоверности; существенное возрастание рекламной информации с «традиционными» для маркетинговых данных «неточностями» и завышением данных о качестве изделий; ограниченные возможности использования для обоснования технологических преимуществ разрабатываемых средств данных о сертификации и, в первую очередь, о сертификационных испытаниях в связи ограничением доступа к ним из соображений «охраны корпоративной тайны». Все это, вместе взятое, существенно сдерживает и снижает возможности наращивания конкурентных преимуществ разрабатываемых АСЗИ, а тем более, темпы их развития.

Более того, решением актуальной проблемы систематизации лучших практик, как правило, без выработки требований (как минимум, без публикации этих данных) к развитию АСУ, а, тем более, АСЗИ стали заниматься отдельные коммерческие структуры по заказам заинтересованных компаний с соответствующими договорными обязательствами и формированием «авторитетных» мнений.

Для решения проблемы систематизации и анализа лучших практик с соответствующим обоснованием требований по направлениям технологического развития АСЗИ, по нашему мнению,

должны быть признаны научной общественностью и специалистами, а также соответствующим руководством следующие основные направления обобщения лучших практик:

На стадии концептуального и исследовательского проектирования (завершается, как правило, формированием технического задания) – сбор данных по построению, функционированию и использованию, а также развитию эффективных вариантов средств и систем автоматизации и управления жизненным циклом морской техники различных классов и видов в защищенном исполнении. Их сравнительного квалиметрического (преимущественно) анализа и ранжирования по критерию достигаемого уровня проектного качества и прогнозируемого значения эффективности использования с максимальным учетом реальных факторов эксплуатации, включая требования ИБ.

На стадии конструкторского проектирования – сравнительный анализ качества проектных решений по критериям их технологической и эксплуатационной доступности, информационной защищенности каждого элемента и ОМТИ в целом, эргономичности, удобства и практичности, серийной повторяемости, экономичности на всех этапах жизненного цикла ОМТИ [3, 4, 5].

На стадии освоения и опытной эксплуатации – верификация ранее сформированных данных и обоснование требований по дальнейшему развитию. Завершение тем самым создания квалиметрически обоснованной базы данных и знаний (БДЗ) по систематизации лучших практик и формированию требований к развитию систем автоматизации и управления ЖЦ ОМТИ в целом.

Ценность сформированной БДЗ состоит в аккумулированной и непрерывно актуализируемой системе данных для практической реализации при обосновании путей развития, а также наиболее эффективных способов практического использования АСЗИ на каждом из этапов жизненного цикла.

Обоснованность предлагаемого авторами пути решения поставленной проблемы систематизации лучших практик и формирования требований к развитию АСЗИ и управления их жизненным циклом определяется качеством модели сравнительного анализа свойств и характеристик АСЗИ, а также достоверностью используемых данных. Для этого, по нашему мнению, наиболее предпочтительным следует считать использование данных, верифицируемых партнерскими экспертными объединениями в отличие от варианта с отдельными компаниями, выполняющими договорные работы, а потом активно публикующими предоставленные заказчикам результаты. Альтернативная практика, например, накоплена и активно развивается Центром ранговой партнерской сертификации Некоммерческого партнерства «Институт автоматизации процессов борьбы за живучесть корабля, судна» [4]. Причем, даже для таких новых задач, как партнерская и публичная экспертная комплексная оценка качества докладов, выносимых авторами на конференции.

Заключение. Решение проблемы систематизации лучших практик и формирования требований к развитию систем автоматизации и управления жизненным циклом ОМТИ в защищенном исполнении, по нашему мнению, лежит исключительно на пути обязательного использования и открытой публикации результатов количественного сравнения, а также системного анализа их свойств и характеристик. Более того, лучших вариантов построения и практического использования на всех этапах жизненного цикла АСЗИ, формирования партнерских экспертных советов для объективного квалиметрического сравнения лучших практик и их открытой публикации.

Это позволяет обоснованно решать системную задачу развития конкурентно способных технологий и образцов морской техники, включая требования по обеспечению их информационной защищенности, на основе методов квалиметрической оценки ОМТИ и их ранжирования.

СПИСОК ЛИТЕРАТУРЫ

1. Волков В.И., Тычинин И.Ю., Алексеев А.В. Системные аспекты управления развитием современных критических объектов морской техники и морской инфраструктуры / XIV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2014)»: Материалы конференции. \ СПОИСУ. – СПб, 2014, с. 447 – 448.
2. Волков В.И., Тычинин И.Ю., Алексеев А.В. Анализ системных аспектов управления развитием критических объектов морской техники и морской инфраструктуры /Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 1 / СПОИСУ. – СПб., 2015, с. 520 – 526.
3. Алексеев А.В., Мусатенко Р.И. Технология оценки качества и конкурентной способности при ранговой партнерской сертификации объектов морской техники и морской инфраструктуры /Актуальные проблемы морской энергетики: Материалы третьей Всероссийской межотраслевой научно-технической конференции. – СПб.: Изд-во СПбГМТУ, 2014, с. 72-75.
4. Бобрович В.Ю., Антипов В.В., Смольников А.В., Алексеев А.В., Мусатенко Р.И. Опыт организации ранговой партнерской сертификации качества объектов морской техники /Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 1 / СПОИСУ. – СПб., 2015, с.511 - 517.
5. Алексеев А.В. Концептуальные аспекты управления развитием критических объектов морской техники и морской инфраструктуры /Морские интеллектуальные технологии, 2015, № 2 (28), т. 1, с. 47 - 57.

УДК 629.12.001.2

**КОНЦЕПЦИЯ ПОЛИГОНА СЕТЕВОЙ МЕЖОБЪЕКТОВОЙ ОТРАБОТКИ ТЕХНОЛОГИЙ
УПРАВЛЕНИЯ И ОБЕСПЕЧЕНИЯ ПРЕВОСХОДСТВА В ИНФОСФЕРЕ**

Алексеев Анатолий Владимирович¹, Барабаш Павел Александрович²,
Жигadlo Валентин Эдуардович³, Зикратов Игорь Алексеевич⁴, Нышков Анатолий Павлович⁵

¹ Санкт-Петербургский государственный морской технический университет,
Россия, Санкт-Петербург, ул. Лоцманская, 3,

² Смольный институт Российской академии образования
Россия, Санкт-Петербург, Полюстровский проспект, 59,

³ Санкт-Петербургский филиал ФГУП ЦНИИС – ЛО ЦНИИС,
Россия, Санкт-Петербург, ул. Варшавская, 11,

⁴ Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
Россия, Санкт-Петербург, пр. Большевиков 22,

⁵ Государственный университет морского и речного флота имени адмирала С.О. Макарова,
Россия, Санкт-Петербург, Двинская ул., 5/7,

emails: iapbgks@bk.ru, : info@loniis.ru, apnyrkow@mail.ru, zikratov.ia@spbggu.ru. nyrkowap@gumrf.ru,
barabash_p@yahoo.com.

Аннотация: Предложена и обоснована Концепция Полигона сетевой межобъектовой отработки технологий управления и обеспечения превосходства в инфосфере. Её реализация, по мнению авторов, позволит достигнуть качественно новых результатов на основе виртуальной партнерской консолидации распределенных интеллектуальных и информационных ресурсов в интересах реализации синергетического эффекта консолидации участвующих в отработке на площадке Полигона технологий каждой компании, организации, предприятия, вуза и, как следствие, повышения потенциала, качества и защищенности их информационных ресурсов.

Ключевые слова: *превосходство в инфосфере; информационное противоборство; полигон; консолидация ресурсов; синергетический эффект.*

**THE CONCEPT OF INTER-OBJECT POLYGON NETWORK TECHNOLOGY MANAGEMENT AND
SUPPORT EXCELLENCE IN THE INFOSPHERE**

Anatoly Alekseev¹, Paul Barabash², Valentine Zhigadlo³, Igor Zikratov⁴, Anatoly Dives⁵

¹ Saint-Petersburg state marine technical University,
Russia, Saint-Petersburg, street Pilot, 3,

² The Smolny Institute of RAO,

Russia, Saint-Petersburg, street Pilot, 3,

³ The St. Petersburg branch of the FSUE ZNIIS – LO ZNIIS,
Russia, Saint-Petersburg, street Warsaw, d. 11,

⁴ Saint-Petersburg state University of telecommunications
them. Professor M. A. Bonch-Bruevich,

Russia, Saint-Petersburg, Bolshevikov d. 22,

⁵ State University of Maritime and Inland Shipping
them. Admiral Makarov,

Russia, Saint-Petersburg, Dvinskaya str., 5/7,

emails: iapbgks@bk.ru, info@loniis.ru, apnyrkow@mail.ru, zikratov.ia@spbggu.ru. nyrkowap@gumrf.ru,
barabash_p@yahoo.com.

Abstract: Proposed and substantiated the Concept of inter-object Polygon network technology management and support excellence in the InfoSphere. Its implementation, according to the authors, will allow to reach qualitatively new results based on the virtual affiliate consolidation of distributed information and intellectual resources to implement sinergeticheskogo effect of consolidation of participating in training on-site Landfill technologies of each company, organization, enterprise, institution and, as a consequence, improve the capacity, quality and security of their information resources.

Keywords: *superiority in the InfoSphere; information warfare; landfill; consolidation of resources; sinergeticheskyy effect.*

Актуальность поиска новых концептуальных подходов к развитию и освоению современных технологий обеспечения информационной безопасности (ИБ), информационного противодействия (ИПД) и информационного противоборства (ИП) в целом обусловлена целым рядом критических факторов [1 - 5], среди которых могут быть названы:

– критический рост сложности создаваемых информационных средств и систем (ИС), а также алгоритмов их функционирования;

– критический характер негативного влияния субъективных свойств обслуживающего персонала, породивший специфическую и трудно разрешимую проблему «человеческого фактора» (ЧФ), приводящую к дополнительному росту самой проблемы сложности ИС;

– существенное наращивание требований к качеству управления современными сложными информационно-коммуникационными и информационно-управляющими системами;

– необходимость совершенствования процессов управления информационным взаимодействием в организациях и в обществе в целом, в том числе в интересах изыскания коллективных (корпоративных, групповых) ресурсов обеспечения ИБ, ИПД и ИП в целом и, в первую очередь, в части создания и непрерывного совершенствования высокотехнологичных решений;

– необходимость консолидации научных и технологических потенциалов партнеров по моделированию сложных процессов межсистемного и внутрисистемного взаимодействия, что в ряде случаев даже для компаний с высокотехнологическими возможностями принципиально недостижимо;

– необходимость опережающего технологического развития ведущих компаний, организаций и предприятий в интересах минимизации информационных рисков и ресурсных затрат на основе использования синергетических и эмерджентных возможностей структурно-сложных систем;

– ключевой характер современных систем обеспечения комплексной безопасности производственных комплексов и систем, социальных информационных сетей и систем в сочетании с ограниченными возможностями использования только «оборонительных» технологий ИБ, необходимость их комплексного использования в сочетании с новыми технологиями активного ИПД («наступательными» технологиями) и технологиями сетецентрического ИП в целом.

Сетевые и организационно-технические ресурсы даже специализирующихся компаний для комплексного решения задач ИБ, ИПД и ИП в целом при названной постановке проблемы, как показывает анализ, сегодня уже далеко недостаточны. Прежде всего, для отработки, освоения и внедрения новых информационно-технологических решений ИП, в том числе по причине различия, многообразия и динамического развития соответствующих научно-методических школ в данной новой предметной области с явно выраженным междисциплинарным характером [3 - 7].

Более того, это сопровождается разобщенностью даже имеемых ресурсов и, даже, отставанием в развитии от международных (мировых) лидеров в области защиты данных, информационных сетей и жизненно важных интересов, как следует из «Доктрины информационной безопасности Российской Федерации» (ст. 20), утвержденной Президентом РФ 5 декабря 2016 г.

В этих условиях авторы считают возможным достигнуть качественно новых результатов на основе парадигмы виртуальной партнерской консолидации распределенных информационных ресурсов и реализации предлагаемой «Концепции Полигона сетевой межобъектовой отработки технологий управления и обеспечения превосходства в инфосфере (ПСОИП)». В её основу положен комплекс следующих взаимосвязанных ключевых принципов:

– целевая ориентация партнерской консолидации информационных ресурсов на совершенствование уровня подготовки и переподготовки персонала в интересах обеспечения превосходства в информационной сфере;

– технологическое освоение новых решений путем сетевой межобъектовой отработки технологий управления ИБ, ИПД и ИП в целом;

– приоритет формирования устойчивых систематических знаний и владения практическими навыками по обеспечению конкурентно способного уровня качества автоматизированных систем в защищенном исполнении (АСЗИ) и перспективных организационных мероприятий своевременного освоения и эффективного использования комплекса технологий информационного противоборства.

В развитие сформированного концептуального подхода предлагается создание Некоммерческого партнерского совета (НПС), например, в рамках СПОИСУ, исключительно для решения координационных задач планирования, реализации и публикации партнерских решений.

Основными решаемыми задачами Полигона, по нашему мнению, могут быть:

– теоретическое обобщение и моделирование процессов ИП, их анализ, синтез и оптимизация с привлечением к решению этих задач ведущих ученых и специалистов в области ИБ и ИПД;

– теоретическое обоснование практик создания, построения, освоения, эксплуатации и утилизации АСЗИ, технологий автоматизации процессов безопасной эксплуатации, локализации информационных инцидентов на объектах общего и специального назначения;

– освоение перспективных технологий ИП, обобщение и ранжирование лучших практик на основе систематизации данных и квалитетического оценивания технологий ИБ, ИПД и комплексного ИП в целом в интересах ускоренного практического освоения и внедрения лучших проектных и управленческих решений в организациях и на предприятиях с учетом всех публикуемых данных;

– развитие и совершенствование практических навыков ИБ, ИПД и комплексного ИП студентов, магистрантов, аспирантов и преподавателей на основе проведения межвузовских сетевых тренингов практикующими специалистами смежных специализаций (администраторы ИБ, программисты, системные администраторы, специалисты по комплексной защите информации и т. п.);

- привлечение перспективных студентов к выполнению научных исследований на основе, например, грантов Некоммерческого партнерского совета, данных, получаемых при отработке технологий на Полигоне (трафики, новые сервисы и ПО, обнаружение новых векторов атак и т.п.);

- создание межведомственной (межобъектовой, виртуальной) технологической базы для сетевого взаимодействия и мониторинга состояния защищенности выделенных ресурсов, сегментов Интернета, а также моделирования и межобъектовой тренажерной отработки технологий и задач ИП (сетевое взаимодействие, включая имитационное моделирование задач сетевых информационных инцидентов, атак, сражений, хаккинга и т.п.).

- формирование при координирующей функции НПС межведомственного (межобъектового, в том числе межвузовского) научно-технического сообщества специалистов по ИБ, привлечения их для экспертизы и разработки сложных, наукоемких и ресурсоемких совместных инновационных проектов;

- разработка учебно-методических комплексов по современным технологиям ИП с формированием, ведением и актуализацией баз данных и знаний по технологиям ИБ, ИПД и комплексному ИП, а также лучшим практикам преподавания дисциплин по этим дисциплинам.

Создание Полигона позволит, по мнению авторов, обеспечить в перспективе:

- организационно-техническое, научно-техническое и информационно-прозрачное пространство для межобъектового (межведомственного, межвузовского) взаимодействия при решении ресурсоемких и наукоемких современных проблем ИБ, ИПД и ИП в целом;

- регулярное проведение соревнований по ИП, например, в формате соревнований CTF, с целью повышения уровня квалификации участников взаимодействия, формирования Санкт-Петербургской, региональной команды для участия в CTF-соревнованиях мирового уровня;

- создание Полигона моделирования информационного общества Санкт-Петербурга для практической отработки навыков информационных технологий в защищенном исполнении.

Выступая с данным предложением, авторы выражают надежду на понимание и возможность практической консолидации усилий ведущих ученых и специалистов в области методов, технологий и средств создания высокотехнологичных решений, эффективного информационного взаимодействия и превосходства в информационной сфере. Тем самым, формирования плодотворного сотрудничества и создания Партнерского центра компетенций в области ИП уже в ближайшее время.

Реализация предлагаемой Концепции Полигона сетевой межобъектовой отработки технологий управления и обеспечения превосходства в инфосфере позволит достигнуть качественно новых результатов на основе виртуальной партнерской консолидации распределенных интеллектуальных и информационных ресурсов в интересах реализации синергетического эффекта консолидации участвующих в отработке на площадке Полигона технологий каждой компании, организации, предприятия, вуза. Одновременно, как следствие, повышения потенциала и качества и защищенности информационных ресурсов каждой из принявшей участие компании, организации, предприятия, вуза на площадках Полигона сетевой межобъектовой отработки технологий и Партнерского центра компетенций.

СПИСОК ЛИТЕРАТУРЫ

1. Барабаш П.А., Воробьев С.П., Курносое В.И., Советов Б.Я. Инфокоммуникационные технологии в Глобальной информационной инфраструктуре – Санкт-Петербург: Наука, 2008, 552 с.
2. Согонов С.А., Алексеев А.В., Тюрин И.С., Разживин И.С., Жуланова Д.Н., Филиппова А.С., Шитикова К.А., Кальбфляйш В.А. Предложение по созданию полигона сетевого межвузовского взаимодействия и моделирования процессов информационного взаимодействия / Региональная информатика «РИ-2016»: Материалы конференции. \ СПОИСУ. – СПб, 2016, С. 458 – 459.
3. Жигадло В.Э. Особенности реализации инфраструктурных проектов в условиях импортозамещения // Региональная информатика (РИ-2016): Материалы конференции. \ СПИСУ/ - СПб, 2016, с. 27.
4. Ныркеев А.П., Ныркеев А.А., Соколов С.С., Шнуренко А.А. Обеспечение безопасности объектов информатизации транспортной отрасли / под ред. А. П. Ныркова. – СПб.: Изд-во Политехн. ун-та, 2015. – 544 с. – ISBN 978-5-7422-4841-5.
5. Зикратов И.А., Шаго Ф.Н. Оптимизация мероприятий аудита системы менеджмента информационной безопасности. Информатика и космос. 2014. № 2. С. 59-65.
6. Ныркеев А.П., Соколов С.С., Белоусов А.С., Ковальногова Н.М., Мальцев В.А. Обеспечение безопасного функционирования мультисервисной сети транспортной отрасли // Доклады Томского государственного университета систем управления и радиоэлектроники. – № 2(32), 2014. – С. 143 – 149.
7. Алексеев А.В., Воробьев В.И. Информационное взаимодействие: 20 лет концептуального и технологического развития // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 1 / СПОИСУ. – СПб., 2015, с. 153 - 159.

УДК 629.12

СИСТЕМА БОРЬБЫ ЗА ИНФОРМАЦИОННУЮ ЖИВУЧЕСТЬ СУДНА ПО ТРЕБОВАНИЯМ НБЖС

Алексеев Анатолий Владимирович, Петров Александр Акимович
Санкт-Петербургский государственный морской технический университет,
Россия, Санкт-Петербург, ул. Лощманская, 3,
АО «Центральный научно-исследовательский и проектно-конструкторский
институт морского флота»,
Россия, Санкт-Петербург, Кавалергардская улица, 6, лит. А
emails: iapbgks@bk.ru, alexander.petrov@cniimf.ru

Аннотация: Выполнен системный анализ специфических аспектов обеспечения информационной безопасности судов и в контексте требований Наставления по борьбе за живучесть судна. Показана актуальность решения организационно-технической и научной задачи формирования новой парадигмы и разработки технологий борьбы за информационную живучесть судов в различных условиях их эксплуатации в обеспечение одного из критических сегментов их Системы управления безопасностью.

Ключевые слова: система управления безопасностью судна, борьба за живучесть судна; информационная живучесть судна, информационная устойчивость.

CONTROL SYSTEM FOR INFORMATION SURVIVABILITY OF A VESSEL ACCORDING TO THE REQUIREMENTS NBIS

Anatoly Alekseev, Alexander Petrov
Saint-Petersburg state marine technical University,
Russia, Saint-Petersburg, street Pilot, 3,
JSC "Central research and design Institute of Maritime fleet",
Russia, Saint-Petersburg, Kavalergardskaya ulitsa, 6, lit. And
emails: iapbgks@bk.ru, alexander.petrov@cniimf.ru

Abstract: Systematic analysis of the specific aspects of ensuring information security of the courts and in the context of the requirements of the manual on struggle for survivability of a vessel the urgency of addressing the new organizational-technical and scientific problems of formation of new paradigms and technology development of the struggle for information survivability of ships in various conditions of their operation in one of the most critical segments of their safety management System.

Keywords: the safety management system of the ship, the struggle for survivability of a vessel; information damage, information stability.

Одним из важнейших направлений на пути технологического развития судовых систем продолжает оставаться автоматизация управления, включая поддержку принятия решений капитаном судна, вахтенным помощником и другими лицами. Принимающими, как проектные (по обоснованию решений), так и управленческие решения (ПУР) при обеспечении безопасной эксплуатации (ОБЭ), локализации аварийных ситуаций и аварий (ЛА), а также борьбы за живучесть судна (ЖС).

Причем, одной из проблемных задач сегодня встала необходимость создания устойчивых к различным факторам информационных и информационно-аналитических подсистем управления, исключающих как традиционные ошибки управления, так и возможные угрозы несанкционированного доступа, нарушения целостности используемых информационных ресурсов, их модификацию, а также нарушения конфиденциальности данных, включая персональные данные членов экипажа.

При этом, с учетом морской специфики встает вопрос не только об обеспечении требований по информационной безопасности (ИБ) объектов морской техники (ОМТ), но и по гарантированной защите от любых информационных инцидентов. Более того, по эффективной борьбе за информационную живучесть судна в целом (ИЖС). Понятие ИЖС включает в себя способность обеспечивать постоянную готовность к действиям по прямому назначению, способность сохранять и восстанавливать свои свойства при информационных инцидентах, а также готовность противостоять последствиям информационных инцидентов, воздействию атак. Сохранять и восстанавливать при этом в достаточной мере управляемость судна и обеспечивать безопасность находящихся на борту судна пассажиров и экипажа, сохранность грузов и судового имущества [1].

Под борьбой за ИЖС понимаются своевременные энергичные, инициативные и квалифицированные действия его экипажа по обеспечению конфиденциальности, доступности, целостности информационных ресурсов судна, предупреждению возникновения и неуправляемого развития информационных инцидентов, а также по поддержанию в постоянной готовности к действию информационно-коммуникационных (ИКС) и информационно-управляющих средств судна (ИУС) [2].

Борьба за ИЖС, по нашему мнению, должна быть обязанностью всех членов экипажа, регламентироваться Уставом службы на судах, Наставлением по борьбе за живучесть судов (НБЖС, ЦНИИМФ, 2004) и документами по Системе управления безопасностью (СУБ) судна, требованиями Международного кодекса по управлению безопасностью (МКУБ).

Отработка организации борьбы за ИЖС должна быть составной частью повседневной службы на судне и направлена на рациональное распределение членов экипажа в интересах эффективного использования стационарных и мобильных ИКС и ИУС при информационных инцидентах, воздействии атак и вторжений как в портах, включая иностранные, так и на переходе морем.

В контексте требований НБЖС [1] ИЖС, как подсистема (сегмент) живучести технических средств (ЖТС) и СУБ судна в сочетании с подготовленностью экипажа к борьбе за ЖС, вопросами гарантированного обеспечения ЖС в целом должна представлять собой систему комплексной борьбы за ИЖС (СБИЖ) в составе судовой интегрированной автоматизированной информационной системы в защищенном исполнении (АСЗИ). Основными элементами СБИЖ АСЗИ судна должны быть:

Мероприятия по подготовке и допуску экипажа к использованию ИКС и ИУС судна.

Инвентаризация, контроль качества, защищенности информационных ресурсов судна (ИРС).

Комплекс организационно-технических мероприятий (КОТМ) по обеспечению ИБ и ИЖС на основе реализации комплекса мероприятий, регламентированных организационно-распорядительной (ОРД) и нормативно-методической документацией (НМД).

КОТМ по управлению проектным качеством и эффективностью (мерой практической реализации проектного качества) подсистемы ИЖС, включая мероприятия по внутреннему аудиту, аттестации, сертификации, лицензированию, аккредитации, корректирующим действиям и т.д.

Подсистема мониторинга и управления ИБ и ИЖС в составе СУБ (ПМУБ).

Подсистема разграничения доступа к ИРС (ПРД).

Подсистема аудита (контроля и анализа) защищенности ИРС (ПАЗ).

Подсистема обнаружения и защиты от вторжений в ИРС (ПЗВ).

Подсистема криптографической защиты ИРС (ПКЗИ).

Подсистема защиты от вредоносных (вирусов, спама, фишинга и т.п.) кодов (ПЗВК).

Подсистема контроля целостности ИРС (ПКЦ).

При этом типовыми уязвимостями (существующими дефектами построения судовой АСЗИ в части ИЖС) и соответствующими угрозами (потенциальными событиями по реализации уязвимостей и нарушению) ИЖС могут быть:

- негативное влияние субъективных свойств членов экипажа («человеческий фактор»), обусловленные недостаточной подготовкой (знаниями, навыками, способностями, опытом) и соответствующими ошибками эксплуатации, ограниченной мотивируемостью (безинициативность, безответственность) и нелояльностью (злоупотреблением должностным положением) члена экипажа;
- санкционированные программно-аппаратные процессы (удаление данных, использование не по прямому назначению, отказ в работе, включая типа «зависания» программного обеспечения и т.п.);
- несанкционированные программно-аппаратные процессы (заражение вредоносными кодами с деструктивными функциями, использование несертифицированные и нелицензированные средств);
- методы промышленного шпионажа, включая использование средств разведки, шантаж и т.п.;
- разнообразные информационно-аналитические методы и многие другие.

Для эффективного предотвращения названных возможностей и нейтрализации соответствующих рисков ИЖС требуют своего специального концептуального и исследовательского обоснования и проектирования архитектура, функционал и алгоритмы СБИЖ АСЗИ судна.

Таким образом, системный анализ различных аспектов обеспечения ИБ судов в контексте требований НБЖС показывает актуальность решения новой организационно-технической и научной задачи формирования парадигмы и разработки технологий борьбы за информационную живучесть судов в различных условиях их эксплуатации, что позволит обеспечить устойчивость одного из критических сегментов Системы управления безопасностью судна.

СПИСОК ЛИТЕРАТУРЫ

1. Наставление по борьбе за живучесть судов (РД 31.60.14-81) (НБЖС с Приложениями и Дополнениями) = Manual on Emergency Plans in Ships: - СПб.: ЗАО «ЦНИИМФ», 2004. – 384 с.
2. Алексеев А.В. Концептуальные аспекты управления развитием критических объектов морской техники и морской инфраструктуры / Морские интеллектуальные технологии, 2015, № 2 (28), т. 1, с. 47 - 57.

УДК 629.12

ВОПРОСЫ ИБ В ТРЕТЬЕЙ РЕДАКЦИИ МОНОГРАФИИ «АВТОМАТИЗАЦИЯ ПРОЦЕССОВ БОРЬБЫ ЗА ЖИВУЧЕСТЬ КОРАБЛЯ, СУДНА»: ПРЕЗЕНТАЦИЯ ИЗДАНИЯ

Алексеев Анатолий Владимирович, Поленин Владимир Иванович, Москаленко Василий, Александрович, Мусатенко Роман Иванович
Институт автоматизации процессов борьбы за живучесть корабля, судна,
Россия, Санкт-Петербург, ул. Ленинский пр., 101, оф. 162
emails: iapbgks@bk.ru

Аннотация: Представлены материалы и результаты подготовки третьей редакции открытой коллективной монографии «Автоматизация процессов борьбы за живучесть корабля, судна». Показано особое значение систематизации научных, практических данных и лучших практик в таких больших предметных областях знаний, как объекты морской техники и инфраструктуры, в том числе широкого спектра вопросов обеспечения информационной безопасности на кораблях и судах, при обеспечении безопасности службы их экипажей.

Ключевые слова: борьба за информационную живучесть; систематизация данных и знаний; информационная прозрачность безопасности; добросовестная конкуренция.

THE ISSUES OF INFORMATION SECURITY THIRD EDITION OF THE MONOGRAPH "AUTOMATION OF PROCESSES THE STRUGGLE FOR THE SURVIVAL OF THE SHIP, THE SHIP": A PRESENTATION OF THE PUBLICATION

Anatoly Alekseev, Vladimir Polenin, Vasily Moskalenko, Roman Musatenko
Institute of automation of processes of struggle for survivability of the ship, vessel
Russia, Saint-Petersburg, street Leninsky prospect, d. 101, of. 162
emails: iapbgks@bk.ru

Abstract: The submissions and results of the preparation of the third edition of an open monograph "automation of processes of struggle for survivability of the ship, ship". Shows the importance of systematization of scientific and practical data and best practices in such large subject areas of knowledge, as the marine facilities and infrastructure, including a wide range of issues of information security on ships and vessels, while ensuring the security of their crews.

Keywords: *the struggle for information survivability; systematization of data and knowledge; information security transparency; fair competition.*

Проблематика информационной безопасности (ИБ) с каждым годом приобретает все более острое и востребованное значение. Спектр исследуемых и публикуемых вопросов непрерывно расширяется и охватывает все более новые области. И это вполне естественно, чему главной причиной - интенсивное развитие информационных технологий, специфика информации как уникальной категории и предмета научного познания, а также широчайший спектр проявления возможностей информации в управлении как технологическими процессами, так и обществом в целом., включая новые аспекты (типа сетецентрического противоборства), ранее даже не ощутимые. Так, совершенно по-новому сегодня приходится рассматривать проблему взаимодействия «человек-машина» с таким масштабным проблемным проявлением, как «человеческий фактор» (ЧФ).

В этой связи особое значение приобретает вопрос систематизации данных и знаний в конкретных крупных прикладных областях, среди которых известное место отведено автоматизации процессов обеспечения комплексной безопасности объектов морской техники и морской инфраструктуры (ОМТИ). Проблему систематизации данных и знаний в интересах обеспечения безопасной эксплуатации ОМТИ на новую высоту поднимают: специфика эксплуатации корабельных и судовых технических систем в сложнейших морских и океанских условиях; особенности самой морской службы; повышенные риск и требования к персоналу; жесткие требования регламентов и стандартов, причем разных стран в связи с широким перечнем портов захода, а также необходимость сертификации технических средств и услуг по этим требованиям; комплексное использование оборудования; реализация новых возможностей информационных технологий и соответствующих угроз ИБ, интеллектуализация процессов управления в сочетании с критическими возможностями влияния ЧФ. В этом контексте подготовка и представление третьей редакции открытой коллективной монографии «Автоматизация процессов борьбы за живучесть корабля, судна» (АП БЖКС) [1] (презентация первой редакции состоялась в 2015 г.) в обеспечение комплекса работ по созданию систем автоматизации управления кораблями, подводными лодками ВМФ и судами Морского флота стало достойным ответом времени.

Подготовка третьей редакции монографии с учетом накопленного опыта позволила в широком авторском кругу специалистов обсудить целый ряд накопившихся проблем. Системное осмысление не только открывшихся новых технологических возможностей, но и взвешенная оценка возможностей и роли главного элемента системы автоматизации – операторов в лице командиров кораблей и подводных лодок, капитанов судов и других морских специалистов позволили авторам выйти на важные практические выводы и рекомендации. Более того, в результате проведенных четырех специализированных конференций по проблеме АП БЖКС, специализированного цикла научно-практических семинаров, мастер-классов и круглых столов по обобщению лучших практик в этой сложной и широко проблемной области был накоплен весьма значительный объем научных и практических данных и знаний в части:

- теоретического обоснования, обобщения, анализа, синтеза и оптимизации процессов АП БЖКС, практики создания, построения, освоения, эксплуатации и утилизации средств и технологий АП обеспечения безопасной эксплуатации (ОБЭ), локализации аварийных ситуаций и аварий (ЛА), борьбы за живучесть (БЖ) корабля, судна;

- научно-технического обоснования развития средств, систем и технологий АП БЖКС по её основным подсистемам (сегментам, кластерам) БЖКС в части обеспечения непотопляемости, взрывопожаро- и радиационной безопасности; живучести технических средств и оружия, защищенности экипажа судов и управляемости (качества) системы автоматизированного управления;

- обобщения и ранжирования лучших практик обеспечения БЖКС на основе систематизации данных и квалиметрического оценивания технологий БЖКС, оценки их конкурентной способности в интересах ускоренного практического освоения (инновационного обеспечения) лучших проектных и управленческих решений в части опубликованных данных в России и за рубежом в форме изобретений,

полезных моделей, книг, статей, докладов, отчетов о НИОКР и т.п., а также последующей их квалиметрической ранговой сертификации и аттестации;

– выявления и научного обоснования качественно новых и конкурентно способных технологий и технических решений по обеспечению комплексной безопасности ОМТИ, включая сегмент ИБ.

При этом авторы обрели определенный опыт преодоления таких проблем, как:

– необходимость использования данных, содержащих корпоративную, а в ряде случаев и государственную тайну, что принципиально ограничивает издательские возможности;

– научно-методическое несовершенство сравнения многочисленных моделей с учетом многочисленных трудно согласовываемых факторов при публичном обсуждении, решение проблемы создания и использования единого методического аппарата;

– критическое влияние ЧФ при принятии решения о введении регламента оценки конкурентной способности (КС) как в отдельной компании, организации, так в ведомстве, партнерстве в целом;

– как следствие, недостаточная востребованность разработки инвариантного к специфике широкого спектра разрабатываемой продукции и предоставляемых услуг научно-методического аппарата оценки КС современных сложных объектов типа ОМТИ и другие.

Сегодня авторский коллектив монографии представляет третью редакцию своего труда, новыми страницами которого стали:

– ряд системно связующих материалов монографии, подготовленных одним из ведущих специалистов в области автоматизации корабельных и судовых процессов д.т.н. Дыментом А.В.;

– дополнительные количественные и практические результаты, в том числе материалы по широкому внедрению технологии на основе метода обобщенного логико-вероятностного метода;

– новое видение комплексного обеспечения ИБ корабля, судна на всех этапах жизненного цикла с определением комплекса задач непрерывной борьбы за информационную живучесть ОМТИ;

– создание и развитие технологии организационно-технического мониторинга и управления кораблем, судном на основе информационно-аналитических и интеллектуальных технологий поддержки принятия проектных и управленческих решений.

Тем самым, по мнению авторского коллектива монографии «АП БЖКС» создается возможность введения регламента оценки КС по единой методике для сопоставления качества продукции и услуг в дополнение к системе сертификации соответствия как в отдельной компании, организации, так в отрасли в целом. Это позволит создать реальные условия обеспечения открытой добросовестной конкуренции, создания конкурентноспособной продукции и услуг, что в конечном итоге непременно приведет к повышению качества службы экипажей безопасности ОМТИ в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А.В., Ушакова Н.П., Поленин В.И., Соловьев С.Н., Москаленко В.А. Россия, Санкт-Петербург, ИАП БЖКС. Автоматизация процессов борьбы за живучесть корабля судна: результаты подготовки коллективной монографии / Информационная безопасность регионов России (ИБРР-2015). IX Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30 октября 2015 г.: Материалы конференции / СПОИСУ. – СПб., 2015, с. 253-254.
2. Бобрович В.Ю., Алексеев А.В., Антипов В.В., Смольников А.В. Системный анализ конкурентной способности и перспективности развития объектов морской инфраструктуры / Четвертая международная научно-практическая конференция «Имитационное и комплексное моделирование морской техники и морских транспортных систем (ИКМ МТМТС-2017). Труды конференции. – СПб., АО «ЦТСС», 2017, с. 31 – 35.

УДК 629.12.001.2

ПРОБЛЕМЫ СОЗДАНИЯ ИТ УПРАВЛЕНИЯ БОРЬБОЙ ЗА ЖИВУЧЕСТЬ ОМТ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ И ПЕРСПЕКТИВНЫЕ ПУТИ ИХ РЕШЕНИЯ

Алексеев Анатолий Владимирович¹, Соловьев Сергей Николаевич², Бороненков Иван Михайлович³, Туркин Игорь Иванович¹, Москаленко Василий Александрович², Мусатенко Роман Иванович²

¹ Санкт-Петербургский государственный морской технический университет, Россия, Санкт-Петербург, ул. Лоцманская, 3,

² Военный учебно-научный центр ВМФ «Военно-морская академия им. Н.Г. Кузнецова», Россия, Санкт-Петербург, Ушаковская набережная, 17/1

³ АО «Концерн «Научно-производственное объединение «Аврора», Россия, Санкт-Петербург, ул. Карбышева, 15,

emails: otd614@avromail.ru, solserjnic@rambler.ru, vasmoskalenko@mail.ru, rus-euro-roman@yandex.ru, 17151@bk.ru, iitg@ya.ru.

Аннотация: Рассмотрены специфика проблем создания корабельных и судовых автоматизированных комплексов. Систематизированы научно-технические и организационные перспективные пути решения проблем создания информационно-аналитических и интеллектуальных технологий автоматизации процессов борьбы за живучесть корабля, судна в информационно защищенном исполнении в обеспечение их конкурентной способности и перспективности развития.

Ключевые слова: интеграция; интеллектуальные технологии; автоматизация процессов; борьба за живучесть корабля, судна; оптимизация системных решений.

THE PROBLEM OF CREATING AN IT MANAGEMENT STRUGGLE FOR SURVIVABILITY OF OMT IN A SECURE EXECUTION AND PROMISING WAYS OF THEIR SOLUTION

Anatoly Alekseev¹, Sergei Solovyov², Ivan Boronenkov³, Igor Turkin¹, Vasily Moskalenko², Roman Musatenko²

¹ Saint-Petersburg state marine technical University,
Russia, Saint-Petersburg, street Pilot, 3,

² Military educational scientific center of Navy "Naval Academy. N. G. Kuznetsova",
Russia, Saint-Petersburg, Ushakovskaya embankment, 17/1,

³ JSC "Concern "research-and-production Association "Aurora",
Russia, Saint-Petersburg, Karbysheva str., 15,

emails: otd614@avromail.ru, solserjnic@rambler.ru, vasmoskalenko@mail.ru, rus-euro-roman@yandex.ru, 17151@bk.ru, iitg@ya.ru.

Abstract: Discusses the specific problems of the ship and ship systems. Systematized scientific-technical and organizational perspective ways of decision of problems of creation of information-analytical and intelligent technologies of automation of processes of struggle for survivability of the ship, ship information and secure execution in ensuring their competitiveness and development prospects.

Keywords: *integration; intelligent technologies; automation processes; the struggle for the survival of the ship, vessel; optimization of system solutions.*

Среди приоритетных и ключевых проблем создания информационных технологий (ИТ) управления борьбой за живучесть объектов морской техники (ОМТ) по-прежнему определяющее место занимают ИТ автоматизации процессов борьбы за живучесть корабля, судна (ТАП БЖКС). В сочетании с ИТ математического моделирования и ИТ исследования сложных управляющих систем и процессов ТАП БЖКС традиционно являются базовыми для построения большинства современных автоматизированных корабельных комплексов и систем.

Перспективы развития ТАП БЖКС обеспечиваются сегодня комплексом актуальных научных исследований и исследовательского проектирования в областях:

- развития методологических и методических основ системного (комплексного, гибридного) моделирования на основе междисциплинарных исследований и интеграции неоибернетики и общей теории систем, включая актуальные сегодня подсистемы информационной безопасности; комплексной автоматизации и интеллектуализации методов и инструментальных средств системного моделирования сложных объектов и процессов в реальном масштабе времени и в защищенном исполнении;

- разработки комбинированных методов, алгоритмов и методик системного моделирования и прогнозирования сложных объектов и процессов в кризисных (аварийных, нештатных, катастрофических) ситуациях, включая информационные инциденты различных видов от ошибок операторов в связи с недостаточным уровнем их подготовки (знаний, умений, владения навыками, опыта), недостаточной ответственности (халатности в исполнении регламентов, отсутствия творческой активности, разумной инициативы) до злоупотребления должностными полномочиями (нелояльности, немотивированности, меркантильности, коррумпированности и т.п.).

Уже сегодня результаты развития ТАП БЖКС все больше проявляются в разработках и повсеместном внедрении интегрированных самоорганизующихся (распределенных, полимодельных, робототехнических) комплексов. А также используемых в них комбинированных методов, алгоритмов, методик, соответствующих когнитивных технологий автоматизации моделирования сложных процессов и систем в динамических средах, в том числе повышенной агрессивности.

Специфика, критичность морской среды, техногенной среды ОМТ, особенности взаимодействия и противоборства в этих средах требуют соответствующего профессионального научно-технического анализа, синтеза, оптимизации как отдельных технических, так и системных решений в целом. Причем, критичность безошибочности, рациональности и оптимальности системных проектных решений является в условиях резкого наращивания сложности ОМТ проблемой первой значимости.

Особым ресурсом в этой связи является интеграция профессиональных знаний специалистов всех уровней от высшей школы до разработчиков современных корабельных и судовых систем автоматизации. В систематизированном виде приоритетными направлениями развития ТАП БЖКС, по нашему мнению, сегодня являются:

- интеллектуализация каналов контроля технического состояния ОМТ, число которых сегодня превышает 2000 и требует практически полного покрытия контурами автоматического управления; информационно-аналитическая и интеллектуальная поддержка решений лиц, принимающих решения (ЛПР), их обосновывающих (ЛОП) и исполняющих (ЛИР), прежде всего, с целью алгоритмической нейтрализации негативного влияния их субъективных («человеческих») факторов. В этой связи особую значимость и перспективность приобретает создание автоматизированных средств и систем в информационно защищенном исполнении (АСЗИ);

- оптимизация процессов и технологий мониторинга, прогнозирования и управления, включая минимизацию избыточности интерфейсных (экранных) форм, максимизацию охвата решаемых задач контурами автоматического управления в информационно защищенном исполнении; системная эргономическая оптимизация комплексных технологических решений с целью минимизации психофизиологической нагрузки на ЛПР, ЛОР и ЛИР на всех этапах службы экипажа, включая стрессовые перегрузки в процессе локализации аварийных ситуаций, аварий (ЛА) и БЖКС;

- мониторинг и прогнозирование системных (сводных, агрегированных) показателей качества функционирования систем диагностики и управления ОМТ с целью гарантированного решения АСЗИ задач обеспечения безопасной эксплуатации (ОБЭ) технических средств, их систем и оружия (ТССО);

- тренажерная обработка и совершенствование алгоритмов оптимизации принятия решений в АСЗИ, регламентов обслуживания и использования ТССО как при ОБЭ, ЛА, так и при БЖКС; внедрение в АСЗИ подсистем объективной оценки компетенций и адекватности персонала на всех стадиях их подготовки, переподготовки, а также непосредственно при эксплуатации АСЗИ;

- совершенствование средств и методов верификации внедряемых в АСЗИ программных комплексов на всех стадиях их жизненного цикла, создания и эксплуатации ТССО;

- оптимизация концептуальных решений и комплекса требований к ОМТ, средств и методов их полимодельной верификации и валидации, а также технологий их реализации в АСЗИ;

- концептуальное и проектное обоснование и аттестация конкурентной способности ТАП БЖКС и перспектив их развития с использованием современных методов квалиметрического обеспечения. Среди организационно-технических задач и направлений развития ИТ ОМТ и, в первую очередь, ТАП БЖКС наиболее актуальными, по мнению авторов, следует считать: проведение межведомственных конференций, семинаров, мастер-классов, тренингов, вебинаров, круглых столов по систематизации и популяризации лучших практик и ТАП БЖКС;

- проведение партнерской (добровольной, открытой) ранговой (по достигаемому уровню качества в дополнение к подтверждению соответствия заданным требованиям) сертификации средств и систем ОМТ в обеспечение их конкурентной способности и перспективности развития, проведение открытых конкурсов на лучшее технологическое решение, патент, доклад, публикацию и ведение открытых баз данных по ним, включая результаты квалиметрических оценок качества и конкурентной способности по национальному и мировому уровням;

- участие некоммерческих партнерств, экспертных советов и сообществ в независимой экспертизе и информационно-аналитической поддержке принятия решений организациями, центрами экстренной дистанционной поддержки и реагирования, ситуационными центрами и т.п.;

- издание открытых монографий по лучшим практикам внедрения ИТ ОМТ, ТАП БЖКС; консолидацию усилий научных школ отрасли на главных направлениях развития перспективных ИТ ОМТ и ключевых ТАП БЖКС.

В качестве средств реализации указанных задач целесообразно, по нашему мнению, рекомендовать следующие приоритетные научные направления исследований:

- дальнейшее совершенствование понятийного аппарата ИТ ОМТ и развитие единой методологии системной и технологической оптимизации проектных решений, в том числе по ТАП ОБЭ, ЛА и БЖКС;

- реализацию методов визуализации, мониторинга, контроля и прогнозирования состояния средств и систем ОМТ на основе интегрированных АСЗИ;

- дальнейшее развитие и разработку методов и технологий создания комплексных баз данных и знаний, в том числе по лучшим практикам АП БЖКС.

Тем самым, систематизация данных по проблеме создания ИТ управления БЖКС в защищенном исполнении позволяет определить перспективные пути решения этой актуальной проблемы, что обеспечит ускорение развития и формирование условий для создания конкурентно способных образцов отечественной морской техники и технологий.

СПИСОК ЛИТЕРАТУРЫ

1. Соколов И.А. Основные методологические подходы к созданию автоматизированных систем управления, создаваемых для обороны страны и обеспечения безопасности государства / Оружие наследников Победы. – М.: Издательский дом «Оружие и технологии», 2015, с. 96 – 107.
2. Алексеев А.В. Концептуальные аспекты управления развитием критических объектов морской техники и морской инфраструктуры / Морские интеллектуальные технологии, 2015, № 2 (28), т. 1, с. 47 - 57.
3. Гаврилов А.Ф., Дымент А.Б., Киваев Н.М., Масленников Ю.А. Системы поддержки принятия решений в ИСБУ ПЛ – составная часть искусственного интеллекта систем управления // Системы управления и обработки информации: научно-техн. сб. /ОАО «Концерн «НПО «Аврора», СПб., 2015. Вып. 31, с. 12 – 17.

УДК 681.5.03

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПРОБЛЕМЫ СИСТЕМЫ УПРАВЛЕНИЯ КАЧЕСТВОМ ПРАКТИЧЕСКОЙ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ОБЪЕКТОВ ВМФАлексеева Елена Кирилловна¹, Алексеев Сергей Алексеевич², Парфенов Николай Петрович²¹Государственный университет морского и речного флота имени адмирала С.О. Макарова
198035, г. Санкт-Петербург, ул. Двинская, 5/7.²Санкт-Петербургский университет МВД России,
198206, Санкт-Петербург, ул. Летчика Пилютова, 1,
emails: 5347@bk.ru, ksgati@yandex.ru, parfenov-nikolai@mail.ru

Аннотация: Рассматривается направление повышения эффективности управления качеством практической подготовки специалистов объектов ВМФ за счет создания и внедрения различного рода защищенных автоматизированных систем с учетом пяти их особенностей: человеко-машинный характер, непрерывность экспертизы на всех стадиях разработки и внедрения, разработка и внедрение по частям, адаптированность к конкретным техническим условиям и сложности оценки экономических показателей.

Ключевые слова: практическая подготовка, информационная безопасность, качество, управление, экспертные системы.

INFORMATION SECURITY AND PROBLEMS OF QUALITY MANAGEMENT SYSTEM PRACTICAL TRAINING FACILITIES OF THE NAVYElena Alekseeva¹, Alekseev, Sergei², Parfyonov, Nikolai²¹State University of sea and river fleet named after Admiral S. O. Makarov
198035, Saint-Petersburg, Dvinskaya str., 5/7.²Saint-Petersburg University of MIA of Russia,
198206, Saint-Petersburg, Ietchika Pilyutova St., 1,
emails: 5347@bk.ru, ksgati@yandex.ru, parfenov-nikolai@mail.ru

Abstract: The article discusses the way to increase the effectiveness of the quality management practical training facilities of the Navy at the expense of creation and introduction of various kinds of secure automated systems, taking into account five of their features: four-lobeco-machine character, continuity of expertise at all stages of development and implementation, design and implementation in parts, adapted to specific customer specifications and the complexity of economic performance.

Keywords: practical training, information security, quality management, expert systems.

Введение. Объективно существует противоречие между сложностью задач по управлению качеством практических занятий (ПЗ) и неразвитостью имеющихся у руководителей ПЗ методов и средств в принятии решений. Преодолению этого противоречия способствует применение защищенных средств автоматизации на всех уровнях управления качеством ПЗ. Использование ЭВМ, автоматизированных систем управления (АСУ), автоматизированных систем поддержки принятия решения (АС ППР), экспертных систем (ЭС) может создать принципиально новую ситуацию в предметной области управления качеством ПЗ. При этом должны будут использоваться человеко-машинные технологии управления, современные информационные технологии, включающие методы и процедуры сбора, накопления, передачи, хранения и выдачи информации пользователям в удобном для них виде, приемы работы с техническими устройствами и ПЭВМ.

Структура вычислительной системы может быть определена, как система, реализующая защищенную технологию с использованием элементов искусственного интеллекта (ИИ) при решении задач управления качеством ПЗ с помощью человеко-машинной системы типа «руководитель ПЗ – СУК ПЗ». Такая вычислительная система может служить основой для создания автоматизированной системы управления качеством ПЗ (СУК ПЗ), построенной по методологии экспертных систем (ЭС). С функциональной точки зрения, здесь под ЭС понимается вычислительная система, которая использует знания специалистов (экспертов) о конкретной узкоспециализированной предметной области, и которая в пределах этой области способна вырабатывать рекомендации (решения) на уровне с экспертом-профессионалом. Структура ЭС должна содержать пять основных компонент: интерфейс с пользователем (руководителем ПЗ), подсистему логического вывода, БЗ и БД, составляющие ядро ЭС, подсистему приобретения знаний, подсистему отображения и объяснения результатов выработанных рекомендаций (решений). Кроме того, в состав структуры ЭС могут входить две дополнительные компоненты – подсистемы обучения и самообучения. Применительно к проблеме автоматизации управления качеством ПЗ экспертная система должна решать следующие задачи [1]:

– прогнозировать вероятные последствия изменения качества ПЗ, вызванные неадекватными действиями специалиста в составе ПЗ в моделируемых ситуациях управления техническими средствами (ТС);

- планировать последовательность действий специалиста в составе ПЗ по отработке его умений и навыков в ходе функционирования ПЗ;
- сравнивать результаты, показанные специалистом в составе ПЗ, с заданными на это мероприятие руководителем;
- вырабатывать рекомендации (решения) по управлению качеством ПЗ для руководителя;
- выявлять причины ошибок, возникающих в ходе управления качеством ПЗ;
- диагностировать состояние личности специалиста в составе ПЗ в ходе реализации мероприятия ПЗ и вырабатывать рекомендации по ее коррекции.

Для успешного решения названных задач, в первую очередь, должна быть сформирована адекватная предметной области управления качеством ПЗ база знаний. При этом должны рассматриваться следующие уровни знаний [1]:

- общенаучные, содержащие информацию о качестве объектов, процессов, явлений и законах, методах и средствах управления качеством,
- общеинженерные, содержащие информацию об основных видах, типах и образцах ТС, которыми будет управлять специалист в составе ПЗ, и способах управления ими,
- специальные, содержащие информацию об управлении качеством ПЗ по управлению образцами ТС определенного типа,
- конкретно-специальные, содержащие информацию об управлении качеством ПЗ по управлению конкретным образцом ТС.

Следует подчеркнуть, что безопасность ЭС определяется тем, что она манипулирует не конкретными уровнями знаний, а их моделями, т.е. для представления знаний экспертов в БЗ необходимо реализовать, как процесс моделирования знаний. Наиболее распространенными видами моделей представления знаний являются: логические, продукционные и семантические, сравнительные характеристики назначения которых известны для каждой предметной области управления качеством ПЗ.

Входящая в структуру ЭС подсистема объяснения должна уметь разъяснять руководителю ПЗ различные аспекты управления ее качеством, отвечая на вопросы типа «как», «почему» и «какие». Формы ответов могут быть в виде: 1) текста на редуцированном естественном языке, сопровождаемого схемами и рисунками, 2) обратного развертывания дерева целей (трассы логического вывода) с указанием подцелей, 3) вызова работающего правила или правил, связанных с данной подцелью, 4) поиска в БЗ и предъявления правил, являющихся ответом на вопрос.

Подсистема приобретения знаний реализует процесс передачи опыта по решению задач управления качеством ПЗ от источника знаний (эксперты, специальная литература, личный опыт руководителя ПЗ) в БЗ.

Работа подсистемы логического вывода основана на использовании одного из класса моделей представления знаний: логических, семантических, продукционных. На вход данной подсистемы поступает запрос руководителя ПЗ в виде актуальной задачи управления качеством ПЗ. В свою очередь подсистема логического вывода, используя информацию из БЗ, генерирует рекомендации по решению задачи. Поскольку основу БЗ составляют факты (фактуальные знания) и правила (процедурные знания), то в подсистеме логического вывода формируется некоторая стратегия (последовательная, параллельная, прямая, обратная, с возможностью возврата, безвозвратная) выбора соответствующего правила из БЗ, тесно связанная с моделью представления знаний и характером решаемой задачи управления качеством ПЗ [2].

Выводы. При проектировании, внедрении и эксплуатации автоматизированной СУК ПЗ следует учитывать пять ее особенностей: человеко-машинный характер, непрерывность экспертизы на всех стадиях разработки и внедрения, разработка и внедрение по частям, адаптированность к конкретному ТС и сложности оценки экономических показателей. Основой для создания автоматизированной СУК ПЗ может служить ЭС. В состав ЭС должны входить: интеллектуальный (дружественный) интерфейс, подсистема логического вывода (решения задачи управления качеством ПЗ), БЗ и БД, подсистема объяснения и отображения руководителю ПЗ хода решения задачи и подсистема приобретения знаний, с которой работают эксперты. Кроме того, в состав ЭС могут входить подсистемы обучения и самообучения решению задач в предметной области управления качеством ПЗ.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев С.А., Гончар А.А., Стахно Р.Е. Направления интеллектуализации системы управления качеством тренажерной подготовки специалистов органов внутренних дел. / Научный журнал. № 6 (19) Москва. изд. «Проблемы науки». 2017. С.15-18.
2. Парфенов Н.П., Стахно Р.Е. Ужесточение требований к обработке персональных данных - основа повышения безопасности государства / Наука, техника и образование. №5 (35). Том 2. Изд-во «Проблемы науки», г. Иваново. 2017. С.13-15.

УДК 681.5.03

БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ПРОГНОЗЕ И ДИАГНОСТИКЕ КАЧЕСТВА ПРАКТИЧЕСКОЙ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ОБЪЕКТОВ ВМФАлексеева Елена Кирилловна¹, Алексеев Сергей Алексеевич², Парфенов Николай Петрович²¹Государственный университет морского и речного флота имени адмирала С.О. Макарова
198035, г. Санкт-Петербург, ул. Двинская, 5/7.²Санкт-Петербургский университет МВД России,
198206, Санкт-Петербург, ул. Летчика Пилютова, 1,
emails: 5347@bk.ru, ksgati@yandex.ru, parfenov-nikolai@mail.ru

Аннотация: Определены перечень задач безопасной квалиметрии практической подготовки и номенклатура методов педагогической диагностики, которые могут быть использованы при диагностике качества практической подготовки. Рассмотрена методика развертывания функции измерения качества практической подготовки с учетом безопасности персональных данных в виде обобщенной схемы процесса выработки числовых значений показателей качества объектов системы практической подготовки специалистов объектов ВМФ.

Ключевые слова: практическая подготовка, информационная безопасность, качество, управление, экспертные системы.

THE SECURITY OF PERSONAL DATA IN THE PROGNOSIS AND DIAGNOSIS OF THE QUALITY OF PRACTICAL TRAINING FACILITIES OF THE NAVYElena Alekseeva¹, Alekseev, Sergei², Parfyonov, Nikolai²¹State University of sea and river fleet named after Admiral S. O. Makarov
198035, Saint-Petersburg, Dvinskaya str., 5/7.²Saint-Petersburg University of MIA of Russia,
198206, Saint-Petersburg, Ietchika Pilyutova St., 1,
emails: 5347@bk.ru, ksgati@yandex.ru, parfenov-nikolai@mail.ru

Abstract: The article defines the list of tasks safe qualimetry practical training and the range of methods of pedagogical diagnostics, which can be used for diagnostics of the quality of practical training. The method of deployment of the measurement quality of practical training with regard to the security of personal data in the form of generalized scheme of the process of developing numeric values of indicators of quality of objects of the system of practical training.

Keywords: practical training, information security, quality management, expert systems.

Введение. Качество практических занятий (ПЗ) специалистов ВМФ можно рассматривать в двух аспектах:

- 1) с позиции объектных (объекты, методы, условия, средства ПЗ и т.д.) составляющих,
- 2) с позиции субъектных (требования к показателям качества структуры и функционирования элементов системы ПЗ и анализ определяющих их факторов) составляющих.

Методы моделирования управления качеством ПЗ специалистов ВМФ обеспечивают выделение системы единичных показателей качества с учетом безопасности персональных данных, определяющих эффективность для организационной и дидактической подсистем системы управления качеством практических занятий (СУК ПЗ) в целом. Построение моделей организационных и дидактических подсистем является исходным этапом для синтеза СУК ПЗ будущих специалистов ВМФ. Следует отметить, что построение названных моделей является необходимым, но недостаточным условием выработки функций управления качеством ПЗ.

Определяющим при принятии и реализации управленческих решений руководителем ПЗ является информация о числовых значениях показателей качества с учетом безопасности персональных данных и степени их влияния на интегральное качество ПЗ специалистов ВМФ. Исходя из сказанного можно определить следующие этапы процесса управления качеством ПЗ специалистов ВМФ:

- 1) разработка методов и инструментария для получения числовых значений показателей качества ПЗ с учетом безопасности персональных данных;
- 2) проведение процедур изменения числовых значений показателей качества ПЗ с учетом безопасности персональных данных; проведение агрегирования единичных показателей качества ПЗ в групповые и последних в интегральный;
- 3) вычисление числового значения интегрального показателя качества ПЗ с учетом безопасности персональных данных;
- 4) сравнение полученного значения интегрального показателя с критериальным (эталонным, заданным) значением;

5) принятие руководителем ПЗ решения о необходимости управляющего воздействия на некоторый элемент системы ПЗ с целью изменения его качественных характеристик для устранения рассогласования с критериальным значением показателя;

6) определение вида и содержания управляющего воздействия на обучающегося (обучающихся) руководителем ПЗ (сравнение конкурирующих вариантов и выбор наилучшего);

7) реализация принятого решения с помощью СУК ПЗ.

Следует подчеркнуть, что необходимость принятия и реализации с помощью СУК ПЗ управляющего воздействия возникает еще в одном случае, когда руководитель ПЗ на основании анализа качества хода ПЗ прогнозирует (диагностирует) возможность возникновения нежелательного отклонения. Такой вид управления качеством ПЗ может быть отнесен к классу опережающего управления.

Поскольку успешность профессиональной деятельности специалиста ВМФ является основным показателем эффективности ПЗ и образовательного процесса в целом, то возникает необходимость прогнозировать степень этой успешности. В зависимости от величины успешности выделяют диахронный и синхронный прогнозы. Последний вид прогноза – это диагностика. Следовательно, различие между задачами прогноза и диагностики успешности деятельности специалиста ВМФ, прошедшего ПЗ в учебном заведении ВМФ и в реальных условиях профессиональной деятельности по управлению техникой и объектами ВМФ с точки зрения выбора функции оценки практически отсутствует, а заключается только в величине успешности. Отличие же прогностических и диагностических постановок задач заключается в концептуальной основе, в целевых установках их решения. В конечном итоге, всякая диагностика процесса ПЗ осуществляется, по существу, в целях прогноза. Можно говорить, что в общем виде решение прогностических задач в системе ПЗ может включать решение одной или более диагностических задач. Прогностическим задачам соответствует успешность профессиональной деятельности специалиста ВМФ и может оцениваться на основе синтезированного экспертами решающего правила, использующего опыт зависимости успешности профессиональной деятельности выпускников от характеристик процессов ПЗ, похожих на оцениваемый.

Измерение качества объектов системы ПЗ предусматривает процедуру, при которой показатель качества объекта системы ПЗ сравнивается с некоторым эталоном и получает числовое значение в определенном масштабе или шкале. Для того, чтобы определить правила, в соответствии с которыми приписываются числа качественным признакам (свойствам) объектов системы ПЗ с учетом безопасности персональных данных необходимо определить их структуру и процесс функционирования, т.е. построить модели управления качеством. Формулировка цели данного процесса должна отражать целевую функцию выработки числовых значений показателей в управлении качеством процесса ПЗ. Цель определяет объект измерения, субъект измерения, отношение объекта и субъекта измерения. С использованием результатов классификации должны быть определены (выбраны) методы декомпозиции качества (совокупности свойств) объектов процесса ПЗ и СУК ПЗ. Применение этих методов должно обеспечить выделение групповых, а затем единичных свойств, которыми обладают реальные объекты процесса ПЗ и СУК ПЗ. По определенной номенклатуре единичных, групповых и интегральных свойств объектов процесса ПЗ и СУК ПЗ необходимо, во-первых, осуществить выбор методов для формирования номенклатуры показателей качества, покрывающих названные свойства. Во-вторых, сформировать номенклатуру эталонов, удовлетворяющих требованиям надежности (определять только признаки свойств, планируемых к измерению, не смешивая их с другими), устойчивости (повторные измерения должны давать те же результаты, что и предыдущие), точности (хорошая различимость степени выраженности признака измеряемого свойства). В-третьих, должно быть выполнено приведение показателей и эталонов к стандартному типу (нормирование). В-четвертых, должен быть осуществлен выбор типов шкал измерений с учетом особенностей каждого оцениваемого свойства.

Выбор методов и средств измерения играет важную роль, когда речь идет об оценке и управлении качеством такого сложного объекта как качество системы ПЗ (процесса ПЗ и СУК ПЗ). При этом следует учитывать тот факт, что полная формализация показателей качества и процесса ПЗ вряд ли возможна из-за того, что в системе ПЗ есть две компоненты, реализующие интеллектуальную образовательную деятельность – это руководитель ПЗ и обучающиеся. Методы и средства измерений при управлении качеством ПЗ должны быть гомоморфными объекту измерений, т.е. определенным отношениям свойств в измеряемом объекте должны соответствовать такие же отношения свойств измерительного эталона.

Вывод. Необходимость процедур агрегирования («свертки») частных (единичных и групповых) показателей в некоторые обобщенные (интегральные) показатели качества процесса ПЗ и СУК ПЗ обусловлена: с одной стороны, невозможностью получения оценок обобщенных показателей со сложной структурой непосредственным путем, а только путем оценок составляющих их частных показателей, с другой стороны, - различным весом отдельных показателей в общей структуре оценки качества практической подготовки.

СПИСОК ЛИТЕРАТУРЫ:

1. Алексеев С.А., Гончар А.А., Стахно Р.Е. Основы квалиметрии, автоматизации и интеллектуализации систем организационного управления практической подготовкой в вузах МВД. / Наука, техника и образование. № 5 (35) Москва. изд. «Проблемы науки». 2017. С. 29-32.
2. Парфенов Н.П., Стахно Р.Е. Вопросы правового регулирования обработки и защиты персональных данных. / Проблемы современной науки и образования № 19 (101). Москва. изд. «Проблемы науки». 2017. С. 29-32.

УДК 004.01

К ВОПРОСУ ПОДГОТОВКИ СИЛ ОБЕСПЕЧЕНИЯ ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ

Алимов Олег Михайлович

Государственный университет морского и речного флота им. адм. С.О. Макарова

Россия, г. Санкт-Петербург, ул. Двинская 5/7,

emails: alimovom@gumrf.ru

Аннотация: В статье рассматривается процедура подготовки сил обеспечения транспортной безопасности. Даны определения основных принципов обеспечения транспортной безопасности. Приводятся ссылки на нормативные документы, регламентирующие подготовку сил транспортной безопасности. Описаны основные проблемы при подготовке специалистов транспортной безопасности.

Ключевые слова: подготовка кадров; транспортная безопасность; информационная безопасность; морской транспорт; транспортная инфраструктура; силы безопасности.

QUESTIONS OF TRAINING TRANSPORT SECURITIES

Alimov Oleg Mihailovich

Admiral Makarov State University of Maritime and Inland Shipping,

Russia, St. Petersburg, Dvinskaya str. 5/7,

emails: alimovom@gumrf.ru

Abstract: The article deals with the procedure for training the forces for ensuring transport security. The main principles of transport security are defined. Reference is made to the regulatory documents regulating the training of transport security forces. The main problems in the training of transport safety specialists are described.

Keywords: personnel training; transport security; information security; sea transport; transport infrastructure; security forces.

Введение. В Российской Федерации уделяется достаточное внимание разработке и актуализации национального законодательства в области транспортной безопасности. В системе нормативных правовых актов, регламентирующих вопросы обеспечения транспортной безопасности, главенствующую роль играет Транспортная Стратегия Российской Федерации на период до 2030 года [1], одной из целей которой является повышение уровня безопасности транспортной системы страны. Важным элементом реализации Стратегии применительно к обеспечению комплексного подхода к безопасности является формирование и имплементация системы нормативно-правовых актов, принятых во исполнение Федерального закона от 09 февраля 2007 года № 16-ФЗ «О транспортной безопасности» [2]. В соответствии с указанными документами транспортная безопасность в Российской Федерации обеспечивается посредством реализации определяемой государством системы правовых, экономических, организационных и иных мер в сфере транспортного комплекса, соответствующих угрозам совершения актов незаконного вмешательства.

Основными принципами обеспечения транспортной безопасности являются: законность; соблюдение баланса интересов личности, общества и государства; взаимная ответственность личности, общества и государства в области обеспечения транспортной безопасности; непрерывность; интеграция в международные системы безопасности; взаимодействие субъектов транспортной инфраструктуры, органов государственной власти и органов местного самоуправления.

Подготовка сил обеспечения транспортной безопасности регламентирована частью 1 статьи 12.1 ФЗ-16 «О транспортной безопасности» и статьей 85.1 Федерального закона от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации» [3]. В развитие требований указанных Федеральных законов Министерством транспорта Российской Федерации изданы приказы:

– № 212 от 31 июля 2014 года «Об утверждении порядка подготовки сил обеспечения транспортной безопасности»;

– № 231 от 21 августа 2014 года «Об утверждении требований к знаниям, умениям, навыкам сил обеспечения транспортной безопасности, личностным (психологическим) качествам, уровню физической подготовки отдельных категорий сил обеспечения транспортной безопасности, включая особенности проверки соответствия знаний, умений, навыков сил обеспечения транспортной безопасности, личностных (психологических) качеств, уровня физической подготовки отдельных

категорий сил обеспечения транспортной безопасности применительно к отдельным видам транспорта»;

– № 243 от 08 сентября 2014 года «Об утверждении типовых дополнительных профессиональных программ в области подготовки сил обеспечения транспортной безопасности».

На основе типовых программ, утвержденных приказом Минтранса России от 08 сентября 2014 года № 243, в подведомственных образовательных учреждениях проводится обучение на курсах повышения квалификации сил обеспечения транспортной безопасности по программам:

1. Повышение квалификации работников, назначенных в качестве лиц, ответственных за обеспечение транспортной безопасности в субъекте транспортной инфраструктуры;

2. Повышение квалификации работников, назначенных в качестве лиц, ответственных за обеспечение транспортной безопасности на объекте транспортной инфраструктуры;

3. Повышение квалификации работников, назначенных в качестве лиц, ответственных за обеспечение транспортной безопасности на транспортном средстве;

4. Повышение квалификации работников субъекта транспортной инфраструктуры, подразделения транспортной безопасности, руководящих выполнением работ, непосредственно связанных с обеспечением транспортной безопасности объекта транспортной инфраструктуры и (или) транспортного средства;

5. Повышение квалификации работников, осуществляющих досмотр, дополнительный досмотр, повторный досмотр в целях обеспечения транспортной безопасности;

6. Повышение квалификации работников, осуществляющих наблюдение и (или) собеседование в целях обеспечения транспортной безопасности;

7. Повышение квалификации работников, управляющих техническими средствами обеспечения транспортной безопасности;

8. Повышение квалификации иных работников субъекта транспортной инфраструктуры, подразделения транспортной безопасности, выполняющих работы, непосредственно связанные с обеспечением транспортной безопасности объекта транспортной инфраструктуры и или транспортного средства.

Подготовка сил обеспечения транспортной безопасности состоит из теоретической, тренажерной и практической подготовки и направлена на приобретение знаний, умений, навыков, установленных требованиями законодательства Российской Федерации. Среди обязательных изучаемых разделов есть те, в которых слушатели знакомятся с современными методами и средствами обеспечения информационной безопасности на транспорте.

Возможными формами обучения являются очная (с отрывом от производства), или смешанная (с использованием дистанционных образовательных технологий электронного обучения и проведением в очной форме практических занятий иных, чем тестирование, и итоговой аттестации). Обучение исключительно с применением электронного обучения и дистанционных образовательных технологий не допускается.

Закключение. За последние годы в транспортных процессах произошли принципиальные изменения, в основном связанные с информационным обеспечением судов для более эффективного управления их движением [4], [5]. Стремительное развитие информационных технологий, внедрение автоматизированных систем управления транспортными процессами, а также различного рода информационных систем являются объективными факторами повышения безопасности транспорта. Процесс подготовки и переподготовки кадров, обеспечивающих безопасность на транспорте, также подвержен этим тенденциям. В ГУМРФ имени адмирала С.О. Макарова в соответствии с нормативно-правовой базой и с целью повышения качества образовательного процесса была создана электронная информационно-образовательная среда, обеспечивающая применение электронного обучения и дистанционных образовательных технологий, в том числе и для переподготовки кадров морского и речного флота [6].

СПИСОК ЛИТЕРАТУРЫ

1. Распоряжение Правительства Российской Федерации от 22 ноября 2008 года № 1734-р «Об утверждении Транспортная стратегия российской федерации на период до 2030 года». <http://docs.cntd.ru/document/902132678>.
2. Федеральный закон «О транспортной безопасности» от 09.02.2007 N 16-ФЗ (последняя редакция). http://www.consultant.ru/document/cons_doc_LAW_66069/.
3. Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 N 273-ФЗ (последняя редакция). http://www.consultant.ru/document/cons_doc_LAW_140174/.
4. Нырков А.П. Автоматизированное управление транспортными системами / А. П. Нырков, С. С. Соколов, А. А. Шнуренко // СПб.: ГУМРФ имени адмирала С.О. Макарова, 2013. – 325 с.
5. Нырков А.П., Нырков А.А., Соколов С.С., Шнуренко А.А. Обеспечение безопасности объектов информатизации транспортной отрасли / под ред. А. П. Ныркова. – СПб.: Изд-во Политехн. ун-та, 2015. – 544 с.
6. Kovalnogova, N. Applying E-learning and Distance Learning Technologies in Modern University Complex / N. Kovalnogova, S. Sokolov, A. Nyrkov, S. Chernyi // Asian Journal of Applied Sciences, Volume 3, Issue 6, 2015. – Pp. 790-793.

УДК 629.12

**РЕГРЕССИОННЫЙ АНАЛИЗ ДИНАМИКИ 10 ЛЕТ ХАКЕРСКИХ АТАК И
ИНФОРМАЦИОННЫХ ИНЦИДЕНТОВ**

Анциферов Александр Владимирович

Санкт-Петербургский государственный морской технический университет,
Россия, Санкт-Петербург, ул. Лоцманская, 3,
emails: ava1996@yandex.ru

Аннотация: Рассмотрена проблема систематизации и анализа динамики 10 лет хакерских атак и информационных инцидентов, наиболее распространенные виды хакерских атак. Приведены примеры и сравнительные оценки комплексной защиты типовых ОМТИ. Сформулированы 5 предложений по организационно-технической защите населения от информационного «разбоя».

Ключевые слова: комплексная безопасность; хакер; взлом; защита; уязвимость.

**REGRESSION ANALYSIS OF THE DYNAMICS OF 10 YEARS OF HACKING AND
INFORMATION INCIDENTS**

Antsiferov Alexander

State Marine Technical University of St. Petersburg,
Russia, Saint-Petersburg, Lotsmanskaya Str. 3,
emails: ava1996@yandex.ru

Abstract: The problem of systematization and analysis of the dynamics of 10 years of hacker attacks and information incidents, the most common types of hacker attacks. The examples and comparative assessment of integrated protection of the model of OMTI. Formulated 5 proposals for organizational and technical protection of the population from the information of "robbery".

Keywords: comprehensive security; hacker; hacking; security; vulnerability.

Введение. Среди проблем повышения качества и эффективности современных систем автоматизации и обеспечения комплексной безопасности в том числе объектов морской техники и инфраструктуры (ОМТИ) определенное значение имеет проблемный вопрос систематизации и анализа динамики, например, за 10 лет хакерских атак и информационных инцидентов, а также рассмотрения технологий наиболее распространенных видов хакерских атак и защиты от них [1 - 4].

«Наск» — по-английски когда-то обозначало массу понятий с общим значением «что-то резко обрывать». Были еще и другие варианты. Позже термин «hacking» стал толковаться как компьютерное хулиганство [1].

«Хакер» — это взломщик информационных ресурсов разного вида, включая сайты и сервера. Человек, использующий свое мастерство для разных, иногда неблагоприятных целей. Сейчас это для одних — индустрия, а для других — стиль жизни. Вторые предпочитают называть себя не «хакерами», а «хэкерами». Это - целое международное сообщество. Они взламывают сети из «спортивного» интереса и, уходя, зачастую «латают дыры» [1, 2].

«Чистые» хакеры не только не причиняют вреда, но и приносят пользу, указывая на слабые места в системе защиты информационных систем. И часто делают это бескорыстно. Иной раз и по просьбе самого владельца сети, желающего узнать эти самые «слабые» места.

В истории Интернета самые известные хакерские атаки постоянно публикуются в сетях, но, как и в айсберге, большая часть событий и технологий остаются невидимыми.

Кевин Митник [2], наверное, самый известный в мире американский хакер. Во многом - благодаря склонности к эксцентричному поведению, которого от него и ожидала праздная публика.

Во время своего ареста в 1995 году Митник безапелляционно заявил, что ему достаточно посвистеть в трубку уличного телефона-автомата, чтобы (!) развязать ядерную войну.

Будучи студентом, с компьютера TRS-80 Митник проник в глобальную сеть ARPANet, предшественницу Internet, и через компьютер Лос-Анджелесского университета «добрался» до серверов Министерства обороны США. Взлом был зафиксирован. Юного киберпреступника довольно быстро нашли. В итоге он отбыл полгода в исправительном центре для молодежи. Любопытный факт: он проделал это на компьютере с частотой процессора меньше 2 МГц.

Американец Джонатан Джеймс — первый несовершеннолетний хакер, осужденный в США за киберпреступления. Как утверждало обвинение, в 15-летнем возрасте в 1999 году он взломал компьютерную систему собственной школы, сеть телекоммуникационной компании Bell South, а затем проник на сервер Министерства обороны США [3].

Здесь он перехватил более трех тысяч электронных писем сотрудников госучреждений, взломал сервер НАСА и похитил программное обеспечение, предназначенное для управления системами жизнеобеспечения на Международной космической станции.

Кевин Поулсен - еще один бывший хакер, сменивший род занятий, как и Митник, на более безопасный [4]. В восьмидесятых годах Поулсен специализировался на взломе телефонных линий и с легкостью манипулировал номерами и каналами разных операторов.

Впервые Поулсен стал известен под псевдонимом Dark Dante в 1993 году после взлома системы управления телефонными линиями Лос-Анджелесской радиостанции KIIS-FM.

В результате искусной блокировки линий он стал победителем нескольких конкурсов и как 102-й дозвонившийся «выиграл» автомобиль Porsche 944 S2.

Выводы.

С учетом данных регрессионного анализа по динамике информационных инцидентов только за 10 последних лет хакерских атак и других информационных инцидентов можно утверждать:

1. Актуальность систематизации данных по информационным инцидентам возрастает как в связи с ростом их числа, так и с еще более заметным возрастанием сложности информационных инцидентов, их «изоэдренности» и масштабом роста наносимого при этом ущерба.

2. При этом анализе с учетом специфики процессов не должно допускаться дилетантства, так как возникающие при этом «страшилки» только поднимают интерес, особенно, у молодежи к «романтике удивлять мир». Это неизбежно приводит к росту «армии экспериментаторов», для нейтрализации которой может просто не хватать ресурсов.

3. Поэтому заслуживает внимание такое направление информационно-психологического противоборства информационно-зловредным действиям «любителей» как профессиональная (без паники и пустых слов) оценка инцидентов и популяризация «информационной гигиены населения».

4. В сочетании с активной правоприменительной практикой и должным реагированием правоохранительных структур на каждый информационный инцидент это позволит по существу управлять далеко не простыми, но социально опасными угрозами и ситуациями.

5. Прежде всего, информационно защищать общественность (прежде всего, самые мало защищенные слои населения – пенсионеров, граждан с гуманитарным образованием и объективно далеких от «технологий защиты») от массовых «тараканьих бегов» по «открытым пространствам».

В том числе от «информационного разбоя» в форме массовых социоинженерных взломов личных счетов граждан, телефонных «блокировок» счетов руками их владельцев и т.п., на которые сегодня полиция практически не реагирует, хотя имеет для этого все необходимые ресурсы. Но в силу своих специфических свойств «оборотней» эту информацию, получая от пострадавших граждан «из рук не выпускают» и, имеются основания утверждать, «активно используют». Благо спрос на «безответную» защиту возрастает лавинообразно. Может, это тоже «бизнес»?

СПИСОК ЛИТЕРАТУРЫ

1. <https://ria.ru/spravka/20130808/955191308.htm>.
2. <http://m.diletant.media/articles/26011961>

УДК 658.58

ВОЗМОЖНОСТИ ДИСТАНЦИОННОЙ ДИАГНОСТИКИ НА СУДАХ

Баркова Наталия Александровна¹, Барков Алексей Васильевич², Грищенко Дмитрий Вячеславович², Федорищев Владимир Валерьевич²

¹ Санкт-Петербургский государственный морской технический университет,
Россия, Санкт-Петербург, ул. Лотманская, 3,

² Ассоциация ВАСТ,
Россия, Санкт-Петербург, пр. Стачек, 140,
e-mails: barkova@vast.su, barkov@vast.su, gri_dmi@mail.ru, vvf@vast.su,

Аннотация: В докладе рассмотрены вопросы комплексного диагностирования судовых машин и оборудования во время длительного плавания с привлечением удаленных специалистов береговых служб диагностики и на основе технических средств отечественного производства. Изложены вопросы оптимизации номенклатуры контролируемых процессов и разделения средств диагностики на стационарные, мобильные и переносные.

Ключевые слова: прогноз; судовое оборудование; средства диагностики; вибрация, ток.

POSSIBILITIES OF REMOTE DIAGNOSTICS ON BOARD A SHIP

Nataliya Barkova¹, Alexey Barkov², Dmitry Grishchenko², Vladimir Fedorishchev²

¹ St. Petersburg State Marine Technical University,
Russia, St. Petersburg, ulica Lotsmanskaya 3,

² Association VAST
Russia, St. Petersburg, prospect Stachek 140
e-mails: barkova@vast.su, barkov@vast.su, gri_dmi@mail.ru, vvf@vast.su

Abstract: The report considers the issues of complex diagnostics of shipboard machinery and equipment during long sea voyages with the involvement of remote experts onshore services for diagnosis and on the basis of means of domestic production. The paper describes the optimization of the nomenclature of controlled processes and the division of diagnostic tools in stationary, mobile and portable systems.

Keywords: *prognosis; on board ship equipment; diagnostic means; vibration, current.*

На многих предприятиях промышленности и на транспорте все большее внимание уделяется дистанционной диагностике работающего оборудования, позволяющей контролировать и прогнозировать его состояние удаленно, в том числе без участия собственных специалистов. Задачи диагностики ответственного оборудования принято делить на две части. Первая – защитный мониторинг состояния, выполняемый в автоматическом режиме непосредственно на объекте для быстрого устранения причины ухудшения состояния или своевременного вывода оборудования из эксплуатации. Вторая – глубокая диагностика для подготовки к обслуживанию или ремонту, не требующая оперативного решения. Решаются эти задачи путем использования в составе ответственного оборудования стационарных систем защитного мониторинга, параллельно собирающих первичные данные для последующей глубокой диагностики. Менее ответственное оборудование обычно комплектуется только простейшими средствами аварийной защиты.

Большая длительность плавания судна, неполное резервирование его оборудования и отсутствие на борту специалистов по диагностике и ремонту требует расширенных подходов к обеспечению безаварийной работы. Во-первых, нужно обеспечивать дистанционное диагностирование ответственного и нерезервируемого оборудования с глубиной, достаточной для минимизации непрогнозируемых отказов во время плавания. А для этого следует оснащать его датчиками контролируемых процессов и средствами сбора информации. Во-вторых, необходимо организовывать береговые службы дистанционной диагностики судового оборудования.

В настоящее время Ассоциация ВАСТ разрабатывает, совершенствует и производит три типа технических средств и информационных систем мониторинга состояния и диагностики энергетических установок с паровыми и газовыми турбинами, а также различных агрегатов с электроприводом, для использования на разных предприятиях промышленности, городского хозяйства и транспорта. К ним относятся стационарные системы мониторинга и диагностики, мобильные системы мониторинга и средства сбора диагностической информации («черные ящики» со сбором информации «по событиям»). Все они рассчитаны на диагностику объектов по их вибрации, току и температуре, работают как в автоматическом режиме, так и в режиме удаленного управления, и могут быть адаптированы к судовым машинам и оборудованию. Особое внимание уделяется вопросам первичной диагностики объектов после изготовления, на испытательных стендах заводов – изготовителей. В частности, одна из систем устанавливается на объединении Звезда для первичной диагностики выпускаемых редукторов.

Нерешенные проблемы сохраняются в глубокой в том числе и дистанционной диагностике ДВС, которыми оснащены большинство судов. Проблемы в том, что диагностика ДВС проводится преимущественно по параметрам рабочих процессов, изменения которых при зарождающихся дефектах обычно не выходят за зоны допустимых отклонений. Но многие разработчики средств диагностики продолжают поиск методов диагностики ДВС по более чувствительным к зарождающимся дефектам вторичным процессам с учетом постоянно растущих возможностей современных средств их измерения и анализа.

СПИСОК ЛИТЕРАТУРЫ

1. Неразрушающий контроль: Справочник: В 7 т. Под общей редакцией В.В. Клюева. Т. 7: В 2 кн. Кн. 2: Балицкий Ф.Я., Барков А.В., Баркова Н.А. и др. Вибродиагностика, - М.: Машиностроение, 2005, 829 с.
2. Баркова Н.А., Грищенко Д.В. Направления развития информационно-измерительных технологий диагностики роторного оборудования // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 1 – СПб: СПОИСУ, 2015, С. 503-507
3. Барков А.В., Баркова Н.А., Грищенко Д.В., Федорищев В.В. Система мониторинга вибрации с оперативной идентификацией обнаруживаемых изменений // Защита от повышенного шума и вибрации. Сборник докладов всероссийской научно-практической конференции с международным участием – СПб.: БГТУ «Военмех», 2013, С. 272-278.
4. Грищенко Д.В. Система непрерывного мониторинга состояния и оперативной диагностики судового роторного оборудования // Вестник Астраханского государственного технического университета. Серия: Морская техника и технология – СПб.: ФГБОУ ВО «АГТУ», 2016, № 4. С. 54-62.
5. Грищенко Д.В. Автоматическая обработка узкополосных спектров вибрации судовых машин в целях выделения диагностически значимых компонент // Морские интеллектуальные технологии – СПб.: НИЦ «МОРИНТЕХ», 2016. Т. 2. № 4 (34). С. 8-13.

УДК 629.12

**АНАЛИЗ УЯЗВИМОСТЕЙ СЕРВИСОВ АВТОРИЗАЦИИ И ВОЗМОЖНОСТИ ИХ
СОВЕРШЕНСТВОВАНИЯ**

Бирюкова Александра Валерьевна
Санкт-Петербургский государственный морской технический университет,
Россия, Санкт-Петербург, ул. Лоцманская, 3,
emails: biryukova.aleksasha@mail.ru

Аннотация: Проведен анализ уязвимостей различных сервисов авторизации и возможности их совершенствования в настоящее время.

Ключевые слова: мониторинг, пользователь, система программное обеспечение, тестирование.

**ANALYSIS OF VULNERABILITY OF SERVICES AUTHORIZATION AND POSSIBILITIES
OF THEIR IMPROVEMENT**

Aleksandra Biryukova
State Marine Technical University of St. Petersburg,
Russia, Saint-Petersburg, Lotsmanskaya Str. 3,
emails: biryukova.aleksasha@mail.ru

Abstract: The analysis of vulnerabilities of various authorization services and the possibility of their improvement at the present time has been carried out.

Keywords: monitoring; user; system software; testing.

В настоящее время большое внимание уделяется мониторингу парольной защиты информационных ресурсов, а именно - мониторингу парольной защиты и контролю надежности пользовательских паролей.

Мониторинг попыток несанкционированного доступа, предупреждение и своевременное выявление попыток несанкционированного доступа осуществляется с использованием средств операционной системы, специальных программных средств.

Мониторинг производительности автоматизированных систем производится по обращениям пользователей в ходе обслуживания систем и при проведении профилактических работ.

Системный аудит производится администратором информационной безопасности ежеквартально и в особых ситуациях. Он включает проведение обзоров безопасности с занесением записей в Журнал обзоров безопасности, тестирование системы, контроль внесения изменений в системное программное обеспечение.

Журналы обзоров безопасности должны включать несколько важных пошаговых функций.

Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в систему с помощью автоматического инструментария или вручную.

Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы.

Внесение изменений в системное программное обеспечение осуществляется с условием обязательного документирования изменений в соответствующем журнале; уведомлением каждого сотрудника, которого касается изменение; рассмотрением претензий в случае, если внесение изменений повлекло причинение вреда; разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

Выводы:

Технологии сервисов авторизации сегодня весьма совершенны и непрерывно развиваются, что позволяет утверждать о возможности эффективной защиты данных на их основе.

Анализ уязвимостей сервисов авторизации показал необходимость и возможность их совершенствования в направлении упрощения интерфейсов, сокращении времени процедур, в том числе при использовании многограновой авторизации.

СПИСОК ЛИТЕРАТУРЫ

1. <https://ria.ru/spravka/20130808/955191308.htm>.
2. <http://m.diletant.media/articles/26011961>

УДК 629.12.001.2

АНАЛИЗ МОДЕЛЕЙ ОЦЕНКИ КОНКУРЕНТНОЙ СПОСОБНОСТИ ОМТИ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Бобрович Владимир Юрьевич, Алексеев Анатолий Владимирович, Антипов Василий Васильевич,
Смольников Александр Васильевич

Институт автоматизации процессов борьбы за живучесть корабля, судна,
Россия, Санкт-Петербург, ул. Ленинский пр., 101, оф. 162
emails: iapbgks@bk.ru

Аннотация: Рассмотрены проблемы и специфика количественной оценки конкурентной способности объектов морской техники и инфраструктуры, а также перспективные модели оценивания. Показано, что обеспечение защищенности данных на основе эффективных организационно-технических решений в развитие ранее разработанного Обобщенного метода квалиметрического анализа развития (ОМКАР) с учетом проведенного анализа моделей и многовариантных количественных оценок позволяет решить проблему обеспечения защиты корпоративной тайны. Тем самым, создается возможность введения регламента оценки КС по единой методике для сопоставления качества продукции и услуг в дополнение к системе сертификации соответствия как в отдельной компании, организации, так и в ведомстве. Это позволит создать условия обеспечения открытой добросовестной конкуренции, создания конкурентноспособной продукции и услуг, а тем самым – повышения качества жизни и безопасности граждан и общества.

Ключевые слова: системный анализ; конкурентная способность; модель; защищенное исполнение; информационная прозрачность; добросовестная конкуренция.

ANALYSIS OF MODELS ASSESSING THE COMPETITIVE ABILITY OF OMTI IN A SECURE EXECUTION

Vladimir Bobrovych, Anatoly Alekseev, Vasily Antipov, Alexander Smolnikov
Institute of automation of processes of struggle for survivability of the ship, vessel
Russia, Saint-Petersburg, street Leninsky prospect, d. 101, of. 162
emails: iapbgks@bk.ru

Abstract: The problems and specificity of a quantitative estimation of competitiveness of marine facilities and infrastructure, as well as promising models of evaluation. It is shown that the security of the data on the basis of effective organizational and technical solutions to the development of previously developed Generalized method of qualitative analysis of development (OMKAR) subject of the analysis models and multivariate quantitative estimates allows to solve the problem of ensuring the protection of corporate secrets. Thus is created the possibility of introducing regulation of evaluation of the COP uniform methodology for comparing the quality of products and services in addition to the certification system of conformity or private companies, organizations and the Agency. This will allow to create conditions ensuring open fair competition, creation of competitive products and services and thereby enhancing quality of life and security of citizens and society.

Keywords: system analysis; competitiveness; model; secure execution; transparency; fair competition.

Количественная оценка конкурентной способности (КС) современных объектов морской техники и инфраструктуры (ОМТИ) в условиях рыночной экономики, реальной конкуренции предприятий и организаций имеет особое значение, как для разработчиков, изготовителей, вендеров, конкурентов, так и для заказчиков. Причем, чем прозрачнее методология оценки конкурентной способности продукции и предоставляемых услуг, тем прозрачнее и добросовестнее будут процессы конкуренции. Тем меньший риск будет иметь заказчик, а также непосредственно – потребители продукции и услуг, что, естественно, является наиболее значимым. Именно в этих условиях более доступным будет выход на международный рынок, стабильнее национальные позиции в целом.

Среди главных проблем на этом пути, состояние которого весьма далеко от совершенства и является, как известно, даже одним из факторов коррупции, могут быть названы:

- необходимость использования данных, содержащих корпоративную, а в ряде случаев и государственную тайну, что принципиально ограничивает возможность «открытых» данных;
- научно-методическое несовершенство используемых моделей оценки КС в части многочисленных факторов, трудных для согласования при публичном обсуждении, а также необходимости использования в качестве единого аппарата оценивания КС ОМТИ;
- критическое влияние негативных субъективных свойств («человеческого фактора») при принятии решения о введении регламента оценки КС, как в отдельной компании, организации, так в ведомстве и в государстве в целом;
- как следствие, недостаточная востребованность разработки инвариантного к специфике широкого спектра разрабатываемой продукции и предоставляемых услуг научно-методического аппарата оценки КС современных сложных объектов типа ОМТИ и другие.

Именно в связи с особой значимостью оценок КС, критичностью их влияния на основные процессы управления ОМТИ проблема разработки моделей оценки КС, а, тем более, в защищенном исполнении остается далеко не решенной, но по-прежнему актуальной.

Вместе с тем, именно анализ КС на основе исследования её факторов и свойств позволяет обоснованно выходить на формирование концепций и программ перспективного развития ОМТИ.

Существует множество методик оценки КС продукции и предприятий и, даже, преподаются учебные дисциплины типа «Управление конкурентоспособностью» по направлению «Менеджмент» [1-3]. Вместе с тем, как показал анализ известных моделей оценки КС, их спектр далеко не разнообразен и насчитывает порядка 3-5 различных подходов, а уровень учета факторов влияния определяется порядка 12-15 критериями.

К числу наиболее совершенных, по мнению авторов, могут быть отнесены методические подходы и соответствующие средства автоматизации оценивания КС разнородных объектов анализа семейства SWOT-анализа, включая методы STEP-, PEST-анализа [3], а также в их развитие - Обобщенный метод квалиметрического анализа развития (ОМКАР) [4] с соответствующими вариантами реализации этого метода [5].

В развитие ОМКАР с целью обеспечения защищенности используемых данных авторы предлагают использовать следующие основные процедуры оценивания КС ОМТИ:

- переход от ввода абсолютных значений показателей качества продукции и услуг к их относительным значениям в виде коэффициентов конкурентного превосходства, что в определенной мере позволяет обеспечить защищенность данных, содержащих корпоративную тайну;

- экспертное оценивание анонимных данных по продукции и услугам с целью минимизации влияния субъективных негативных свойств экспертов;

- представление объектов конкурентного анализа не от их поставщика, а от имени соответствующих некоммерческих партнерств с соответствующими сертификатами не только соответствия, но и сертификатами качества с количественными оценками [6], определяемыми по согласованным партнерами методикам оценки КС без публикации самих данных.

С учетом, тем не менее, компромиссного характера приведенных выше методических рекомендаций принципиальное и перспективное решение проблемы доверительной оценки КС продукции и услуг лежит в поле максимального обеспечения прозрачности методического аппарата и используемых данных на основе принципа «Сильные компании прозрачности не боятся». При этом, предварительными шагами на этом пути вполне может быть использование приведенных выше «компромиссных процедур» обеспечения защищенности используемых данных. Следует отдельно отметить, что принцип «максимальной прозрачности» обеспечения защищенности корпоративных данных соответствует одному из 6 принципов «Доктрины информационной безопасности РФ».

Таким образом, обеспечение защищенности данных на основе эффективных организационно-технических решений в развитие ранее разработанного ОМКАР с учетом проведенного анализа моделей оценки КС ОМТИ и многовариантных расчетов позволяет решить проблему защиты корпоративной тайны. Тем самым, создается возможность введения регламента оценки КС по единой методике для сопоставления качества продукции и услуг в дополнение к системе сертификации соответствия как в отдельной компании, организации, так в ведомстве в целом. Это позволит создать реальные условия обеспечения открытой добросовестной конкуренции, а тем самым - создания конкурентоспособной продукции и услуг, что в конечном итоге непременно приведет к повышению качества жизни и безопасности граждан и общества в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Маркетинг по нотам. Практический курс на российских примерах - М.: Маркет ДС Корпорейшн, 2010. - 758с.
2. Печенкин А. В. Оценка конкурентоспособности товаров и товаропроизводителей - М.: МГЭИ, 2012. - 123с.
3. Лазаренко А. А. Методы оценки конкурентоспособности // Молодой ученый. – 2014, №1. – С. 374-377.
4. Алексеев А.В., Удодова Е.Н. Квалиметрический swot-анализ и его применение в задачах управления развитием критических морских объектов // Морские интеллектуальные технологии, 2016, № 1 (31), т. 1, с. 38 – 48.
5. Алексеев А.В., Антипов В.В., Бобрович В.Ю., Евсеев С.М. Реализация обобщенного метода квалиметрического анализа факторов развития и технология обеспечения управления развитием критических морских объектов // Морские интеллектуальные технологии, 2016, № 1 (31), т. 1, с. 27 - 36.
6. Смольников А.В., Алексеев А.В., Антипов В.В., Бобрович В.Ю. Ранговая сертификация современных эрготехнических систем, как реальный способ повышения конкурентоспособности объектов морской техники и морской инфраструктуры – Морской Вестник, 2013, № 1 (10), с. 55 - 59.

УДК 004.9

СОВРЕМЕННЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДАННЫХ КЛИНИЧЕСКИХ ИССЛЕДОВАНИЙ ЛЕКАРСТВЕННЫХ ПРЕПАРАТОВ

Галимов Тимур, Сухов Родион, Шавинская Сания
Санкт-Петербургский государственный морской технический университет «СпбГМТУ»,
Россия, Санкт-Петербург, ул. Лоцманская, 3,
emails: RS-Anti@yandex.ru

Аннотация: В статье рассматриваются основные требования к электронным системам, обрабатывающим данные о клинических и постклинических исследованиях. Выведен рекомендуемый набор действий для обеспечения надежности, безопасности и достоверности данных.

Ключевые слова: фармаконадзор; валидация; архитектура приложения; интерфейс приложения; тестирование.

MODERN APPROACH TO ENSURING INFORMATION SECURITY OF DATA OF CLINICAL TRIALS OF MEDICINAL DRUGS

Timur Galimov, Rodion Sukhov, Sania Shavinskaya
St. Petersburg State Marine Technical University "SPbGMTU"
Russia, St. Petersburg, st. Lotsmanskaya, 3,
emails: RS-Anti@yandex.ru

Abstract: The article considers the main requirements for electronic systems processing data on clinical and post-clinical studies. A recommended set of actions for ensuring the reliability, security and authenticity of the data is derived.

Keywords: *pharmacovigilance; validation; architecture of application; interface of application; testing.*

Введение. Высокие технологии все больше внедряются в нашу повседневную и профессиональную деятельность. Сейчас мы практически не представляем сферу деятельности человека, в которой бы не применялись высокие технологии. Неудивительно, что при современных темпах развития технологий появляются новые требования к программному обеспечению.

Интересными примерами таких предписаний являются негласные требования к искусственному интеллекту, которые в большей степени направлены в этическую сферу вопроса. В тех сферах деятельности человека, где возможна угроза жизни или здоровью, правила к разработке программного обеспечения должны иметь строгие и нормированные требования.

Одной из таких сфер являются клинические исследования препаратов. Как таковые, клинические исследования проводились и в девятнадцатом и начале двадцатого веков, но их целью было разоблачение шарлатанов, и они не имели ни четких описаний, ни каких либо обязательных условий. Впервые о необходимости клинических исследований задумались в США из-за наплыва огромного числа ложных препаратов, это привело к тому, что в 1912 году в конгрессе Соединенных Штатов было принято решение запретить рекламу лекарств с недоказанными лекарственными свойствами. Именно это послужило стимулом к широкому применению клинических исследований. И способствовало развитию таких исследований, а следственно и повышению эффективности препаратов.

Однако история показала, что одной эффективности для лекарственного средства недостаточно. И после ужасных событий, как талидомидовый бум в США, когда при использовании снотворного препарата талидомида у беременных, его тератогенное действие было выявлено через 6 лет применения, в результате чего родилось от 8000 до 12000 детей с отклонениями, было обязательным условием доказательства безопасности препарата. Все это стало предпосылками для возникновения системы контроля безопасности лекарственных средств. И естественно то, что с развитием программного обеспечения для данной системы был разработан ряд программных продуктов, облегчающих и систематизирующих деятельность исследователей.

Основными задачами программного обеспечения, работающего в данной сфере, которая получила название фармаконадзор, является учет, сбор и отслеживание информации о всевозможных нежелательных реакциях, возникших у пациентов во время клинического исследования. И естественно, что программные продукты должны обеспечивать надежность, безопасность и достоверность данных. Соответствующий раздел есть в стандарте под названием Надлежащая Клиническая Практика (Good Clinical Practice) и в 2016 году 1 апреля в Российской Федерации был выпущен приказ «Об утверждении правил надлежащей клинической практики». Где в разделе III «Организация, осуществляющая проведение клинического исследования» имеется ряд требований к электронным системам, которые обрабатывают данные о клиническом исследовании.

Обеспечение валидации данных.

Это обеспечивается путем проведения ряда сложных действий на протяжении жизненного цикла всей системы, в следующих операциях.

1 Создания архитектуры базы, данных. На этом этапе разработчик архитектор, продумывает структуру базы, правила ее взаимодействия с интерфейсом. Наиболее рациональным является использование реляционной базы данных, с использованием процедур и отображений данных;

2 Создание интерфейса приложения. На этой стадии программист, разрабатывает фронт-энд, и обеспечивает прописанные архитектором связи с базой данных;

3 Тестирование работы приложения. Процесс тестирования начинается с проверки структуры базы данных, их работоспособности и скорости работы. Далее тестируется интерфейс и связи с базой, по GCP рекомендуется прибегать к юнит тестированию и интеграционному тестированию, первое обеспечивает надежную работу отдельных модулей, второе их взаимосвязь. Чаще всего следующими

этапами тестирования являются системное и нагрузочное, проверяющие приложение со стороны конечного пользователя, и работу приложения в различных критических ситуациях. Примерами таких ситуаций являются: высокая загруженность базы данных, либо перегрузка информационного канала или низкая скорость интернета и т.п.

Обеспечения правильности формата электронных подач.

Это требование обеспечивает учет нежелательных явлений, в системах контроля. Но чтобы их загружать, необходимо, соответствовать принятому xml формату.

Обеспечение учета изменений данных в системе.

Для выполнения этого, следует использовать систему учета изменений, отражающую, кем, когда и что было изменено. Программно реализовать такое возможно с помощью логирования данных в системных таблицах. Во многих системах управления базами данных есть инструмент, позволяющий совершать данное действие, через триггеры таблиц, выполняющиеся после действий с данными.

Обеспечения защиты данных.

Чтобы выполнить данное требование, необходимо обеспечить систему защиты, предотвращающую несанкционированный доступ к данным. Такая система должна не только не допускать к данным людей, не являющихся пользователями, но и организовывать разграничение прав пользователей на доступ и совершения различных действий внутри самой системы.

Обеспечение заслепления данных.

Это необычное предписание вытекает из специфики клинических исследований. Существуют различные типы «слепых» исследований: Простое слепое – когда пациент не знает о получаемом лечении; Двойное слепое – когда, ни исследователь, ни пациент не знает какое лечение, получает больной; Тройное слепое – крайне редкое исследование, в котором любой представитель не в курсе как подобраны группы. Все это обеспечивает надежную маскировку лекарственного средства, позволяющую исключить влияние заинтересованных лиц на итоге исследований. С программной стороны это выполняется путем использования кодов вместо наименований лекарств и сокрытия, какой-либо значимой информации о препарате и результатах его применения.

Заключение. В итоге, выполнение всех этих требований обеспечивает создание надежного и достаточно безопасного приложения, для использования его в столь специфичном и требовательном к безопасности разделе высоких технологий, как клинические исследования.

СПИСОК ЛИТЕРАТУРЫ

1. Атаманенко И. А., Румянцев О. А., Кравчук Ж. П., Кривичкая Н. Г., Патофизиология внутриутробного периода развития / И. А. Атаманенко. М.: 2012, 20 с.
2. Приказ «Об утверждении правил надлежащей клинической практики», раздел III: «Организация, осуществляющая проведение клинического исследования», 2016.

УДК 629.12

АРХИТЕКТУРА, СОСТАВ И ТРЕБОВАНИЯ К СИСТЕМЕ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ ОМТИ

Доминова Татьяна

Санкт-Петербургский государственный морской технический университет,
Россия, Санкт-Петербург, ул. Лоцманская, 3,
email: tatifox@outlook.com

Аннотация: Рассмотрены наиболее распространенные виды архитектур, состав и требования к системе комплексной защиты информации ОМТИ и универсальное программное обеспечение по защите информации.

Ключевые слова: защита, требования к системе комплексной защиты информации безопасность, архитектура систем комплексной защиты информации.

ARCHITECTURE, COMPOSITION AND REQUIREMENTS FOR THE INTEGRATED INFORMATION SECURITY SYSTEM OF THE OMTI

Dominova Tatyana

State Marine Ttechnical University of St. Petersburg,
Russia, Saint-Petersburg, Lotsmanskaya Str. 3,
email: tatifox@outlook.com

Abstract: The article considers the most common types of architectures, composition and requirements for the comprehensive information protection system of OMTI.

Keywords: security, requirements to the complex information security system, security, the architecture of integrated information security systems.

Введение. Рассмотрен вопрос поиска путей обеспечения защиты информации для ОМТИ на основе разработки типовых проектных решений, а также возможности разработки универсального программного обеспечения по защите информации.

Проблемы защиты информации и создания необходимых средств для ее безопасности, конфиденциальности, целостности, обработки, хранения и распространения в защищенном исполнении существуют столько же лет, сколько существует и само понятие «информация». С ростом роли информации в обществе, в деятельности организаций, предприятий и отдельных лиц растет, и стремление их конкурентов получить эту информацию и использовать ее в своих целях. При этом меняется характер средств несанкционированного получения и способов использования информации: от примитивного «подглядывания» к современным средствам и методам ведения «информационных войн». Понятно, что соответственно должны эволюционировать как виды средств и методов защиты, так и требования к их функциональным возможностям и характеристикам.

Комплексной системой технической защиты информации принято называть совокупность организационно-правовых и инженерных мероприятий, а также программно-аппаратурных средств, которые обеспечивают защиту информации в автоматических и автоматизированных системах (АС). Эта задача решается как техническими, так и программными средствами базового и прикладного программного обеспечения, а также с использованием специально разрабатываемых программных и аппаратурных средств [1, 2].

Информационная безопасность обеспечивается использованием технических средств:

- построения модели защищенной системы;
- управления доступом к ресурсам АС;
- обеспечения целостности и конфиденциальности;
- обеспечения наблюдаемости;
- защиты от воздействий вирусов и иных воздействий, вызывающих любую несанкционированную модификацию информации;
- защиты информации при передаче информации.

Заключение. Можно утверждать, что единого «рецепта», обеспечивающего 100% гарантии сохранности данных и надёжной работы сети, не существует. Однако, создание комплексной, продуманной концепции безопасности, учитывающей специфику задач конкретной организации, может свести риск потери ценной информации к минимуму, для чего необходимо сочетать использование типовых (хорошо отработанных, безошибочных, малозатратных, в определенной мере универсальных, не требующих специальных испытаний) проектных решений и хорошо отработанной методикой их максимальной адаптации к специфике защищаемых информационных ресурсов (самых данных, их носителей, средств обработки и защиты). Для этого, как минимум, должен быть разработан специализированный интерактивный комплекс (экспертная система) адаптации типового проектного решения к условиям типовых ОМТИ и соответствующих рекомендаций.

СПИСОК ЛИТЕРАТУРЫ

1. <http://www.bezpeka.com/ru/lib/spec/law/architecture-tech-protection-information.html>.
3. Семкин С.Н., Беляков Э.В., Гребенев С.В., Козачок В.И. «Основы организационного обеспечения информационной безопасности объектов информатизации» 2005 г.

УДК 683.3.06

ВЕРБАЛЬНАЯ СТРУКТУРНО-ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ АДАПТАЦИИ ТЕХНОЛОГИИ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ И УПРАВЛЕНИЯ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ ДЛЯ РЕШЕНИЯ КРИТИЧЕСКИ ВАЖНЫХ ЗАДАЧ ВМФ

Каганский Михаил Александрович

Военный учебно-научный центр Военно-Морского Флота «Военно-морская академия им. Н.Г. Кузнецова», Россия, Санкт-Петербург, Ушаковская набережная, 17/1

email: gans1to@mail.ru

Аннотация: В статье рассмотрена вербальная структурно-функциональная модель адаптации технологии информационно-аналитической и интеллектуальной системы поддержки принятия решений и управления класса «СПРУ» для решения критически важных задач ВМФ, ее сравнительные свойства и специфические особенности.

Ключевые слова: система информационно-аналитической и интеллектуальной поддержки принятия решений и управления (СПРУ); технология; структурно-функциональная модель; процесс принятия решений.

VERBAL STRUCTURAL-FUNCTIONAL MODEL OF ADAPTATION SYSTEM TECHNOLOGY DECISION SUPPORT AND MANAGEMENT IN THE PROTECTED EXECUTION FOR MISSION-CRITICAL NAVY

Kagansky Mikhail

Military Educational-and-Research Centre Naval Academy named after «Admiral of the Fleet of the Soviet Union N.G. Kuznetsov», Russia, Saint-Petersburg, Ushakovskaya embankment 17/1,
email: gans1to@mail.ru

Abstract: The article considers the verbal structural-functional model of adaptation technologies of information-analytical and intelligent decision support system and control class "SPRU" for mission-critical Navy, its comparative properties and specific features.

Keywords: *information-analytical and intellectual decision support system and control (IDSSC); technology; structural-functional model; decision-making process.*

Введение. В современных условиях развития информационных компьютерных технологий, связанных, в первую очередь, с формированием и поддержкой принятия обоснованных решений, возникает необходимость уделять большее внимание методологическим и организационным вопросам создания качественных систем интеллектуальной поддержки принятия решений (СППР).

Развитие информационных технологий в интересах СППР и, как следствие, внедрение разработанных технологий поддержки принятия решений имеет большое значение в увеличении эффективности управления силами и средствами ВМФ и использования ресурсов.

Характерной особенностью решаемых сегодня задач является их многокритериальность, поэтому лицам, принимающим решения (ЛПР), приходится оценивать множество факторов и вариантов развития ситуаций, характеризующих варианты решений в ограниченный период времени. Формализация процессов принятия решений, их оценка и согласование являются чрезвычайно сложной задачей. Увеличение объема информации, поступающей в органы управления и непосредственно к руководителям, усложнение решаемых задач, необходимость учета большого числа взаимосвязанных факторов в быстро меняющейся обстановке требуют использования вычислительной техники в процессе принятия решений [1].

Для качественного решения возложенных на ВМФ критически важных задач предлагается адаптировать положительно зарекомендовавшую себя технологию обобщенного метода квалиметрического анализа факторов развития (ОМКАР) [2] в составе программных комплексов систем информационно-аналитической и интеллектуальной поддержки принятия решений и управления (СПРУ) [3].

Одним из этапов адаптации перечисленных решений является разработка вербальной структурно-функциональной модели, которая может быть реализована в качестве СППР на основе использования технологии СПРУ для решения одного из сегментов критически важных задач, стоящих перед ВМФ. Под критически важными задачами ВМФ будем понимать задачи, требующие обязательной реализации, от качества которой существенно зависит результативность всего комплекса задач ВМФ, определенных соответствующими руководящими документами, что обуславливает необходимость принятия оперативного (своевременного), обоснованного и оптимального (наиболее эффективного, предпочтительного) решения соответствующим должностным лицом, в том числе с использованием СППР.

Вариант разрабатываемой модели в обобщенном виде должен учитывать необходимость решения широкого круга разнородных задач. В основу предлагаемой модели положен типовой алгоритм принятия решений, для удобства анализа и большей наглядности выполненный в виде диаграммы IDEF0. Применяемый при этом метод структурно-функционального анализа позволяет учитывать все значимые факторы, влияющие на процесс принятия решений. Предлагаемая модель состоит из следующих необходимых элементов СППР: базы данных; базы знаний; должностные лица и их роли; подсистемы интеллектуального анализа; интерфейс, модули оценивания результатов решений и прогнозирования, географическая информационная система; экспертная подсистема и др. Ключевым элементом такой организации СППР является ее инвариантность к специфике решаемых задач.

При непосредственной реализации варианта модели для определенного центра управления, пункта управления и др. производится анализ его структуры и задач и строится частная модель, которая является совокупностью необходимых элементов из обобщенной модели СППР. Реализация данного подхода позволит при помощи квалиметрических методов оценить и оптимизировать качество и эффективность принимаемых решений и применяемых сил ВМФ, а также качество и эффективность предлагаемой модели.

Кроме того, применение данной технологии позволит решать на более качественном уровне следующие проблемные вопросы:

- мониторинг качества решения функциональных задач, определенных руководящими документами, для различных уровней управления по частным (ЧПК), групповым (ГПК) и сводному (агрегированному) показателю качества (СПК) в реальном масштабе времени с заданным циклом принятия решений по четырем основным уровням качества;

- прогнозирование качества решения задач по выбранным показателям на основе, как реализовано в СПРУ, метода адаптивного регрессионного анализа;

- информационно-аналитическая и интеллектуальная поддержка принятия решений;
- формирование и актуализация Баз данных (БД) и Баз знаний (БЗ) на основе требований руководящих документов, учета в процессе использования опыта должностных лиц ВМФ, результатов уже решенных задач с помощью СПРУ при минимизации избыточности исходных и выходных данных, включая минимально избыточную визуализацию данных;
- упреждающее управление критически важными задачами и структурами ВМФ;
- оперативное и непрерывное управление с использованием объективных и субъективных (с персонализацией ответственности за достоверность добываемой и используемой информации, а также за качество принимаемых управленческих решений, качество их реализации) источников данных;
- формирование и использование проектов оптимальных управленческих решений (в том числе непосредственно во время работы) с регистрацией событий по принятию решений и их доведению до соответствующих должностных лиц (ДЛ), а также получению докладов по их исполнению;
- формирование, актуализация, визуализация структуры и состояния решаемых задач органа военного управления в интересах ВМФ;
- минимизация избыточности информации на всех этапах её жизненного цикла;
- реализация проблемно-ориентированного подхода при решении задач с возможностью формирования новых вариантов решений ДЛ;
- совершенствование применяемых методов и технологий для последовательного наращивания качества СППР;
- квалиметрический анализ и оптимизация управленческих решений и разработанных структур с реализацией полимодельного подхода, учитывающего основные методы агрегирования векторных показателей (аддитивный, мультипликативный, гармонический).

Заключение. Отличительной особенностью существующих в настоящее время систем поддержки принятия решений является их ориентация на узкий круг решаемых задач, что создает значительные трудности для лиц, принимающих решения и лиц, обосновывающих и обеспечивающих реализацию решения.

Повышение качества и эффективности СППР ВМФ сегодня невозможно без моделирования, которое становится наиболее эффективным и минимально ресурсоемким средством нахождения путей и выработки оптимального решения проблем, характерных для сложных организационных систем, которыми являются системы поддержки принятия решений.

Очевидно, что применение ситуационных моделей в управлении способствует повышению эффективности принимаемых решений, сокращению времени принятия решений, повышению качества принимаемых решений, более рациональному использованию данных и знаний.

Разработанная модель и ее реализация с применением технологии СПРУ, по мнению автора, позволит выйти на новый качественный уровень в применении современных интеллектуальных технологий поддержки принятия решений на различных уровнях управления с целью выработки и выбора наиболее обоснованных решений для широкого спектра задач и возможностью минимизации негативного влияния «человеческого фактора».

СПИСОК ЛИТЕРАТУРЫ

1. Аксенов, К.А. Моделирование и принятие решений в организационно-технических системах: учебное пособие. В 2 ч. Ч. 1 / К.А. Аксенов, Н.В. Гончарова. – Екатеринбург : Изд-во Урал. Ун-та, 2015. – 104 с.
2. Алексеев, А.В. Реализация обобщенного метода квалиметрического анализа факторов развития и технология обеспечения управления развитием критических морских объектов / Алексеев А.В., Антипов В.В., Бобрович В.Ю., Евсеенко С.М. // Морские интеллектуальные технологии. – С-Пб. – 2016. – № 1(31) – С. 27-37 – Библиогр.: с. 36.
3. Alexeev A.V., Ravin A.A., Sogonov S.A., Khrutsky O.V. Optimization of the processes of management of quality and competitiveness of objects of marine technique and infrastructure / St-Petersburg State Marine Technical University Science & Technology Society Shipbuilders of the Russian federation Naoe2016 International Conference on Naval Architecture and Ocean Engineering 6-8 June, 2016, St-Petersburg, Russia. Programme, s. 14 - 22.
4. Алексеев, А.В. Концептуальные аспекты управления развитием критических объектов морской техники и морской инфраструктуры / А.В. Алексеев // Морские интеллектуальные технологии. – С-Пб. – 2015. – № 2 (28) – С. 47-57 – Библиогр.: с. 57.

УДК 681.3.00

ПРЕДЛОЖЕНИЯ В ОБОБЩЕННУЮ МОДЕЛЬ ИНТЕГРИРОВАННОЙ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ВМФ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Каганский Михаил Александрович

Военный учебно-научный центр Военно-Морского Флота «Военно-морская академия им. Н.Г. Кузнецова», Россия, Санкт-Петербург, Ушаковская набережная, 17/1

email: gans1to@mail.ru

Аннотация: В статье рассмотрен и обоснован комплекс основных предложений в обобщенную модель поддержки принятия решений ВМФ, а также сформулирован ряд аспектов по её реализации.

Ключевые слова: система поддержки принятия решений (СППР); поддержка принятия решений (ППР); системный анализ; структурно-функциональное моделирование; база данных; база знаний.

PROPOSALS IN A GENERALIZED MODEL OF THE INTEGRATED SYSTEM THE DECISION SUPPORT OF THE NAVY IN A SECURE EXECUTION

Kagansky Mikhail

Military Educational-and-Research Centre Naval Academy named after «Admiral of the Fleet of the Soviet Union N.G. Kuznetsov», Russia, Saint-Petersburg, Ushakovskaya embankment 17/1,
email: gans1to@mail.ru

Abstract: The article describes and justifies a set of basic sentences in a generalized model of decision support of the Navy, and formulated a number of aspects of its implementation.

Keywords: decision support system (DSS); decision support (DS); system analysis; structural-functional modeling; data base; knowledge base.

Введение. В настоящее время системы поддержки принятия решений проектируются и создаются во всех сферах деятельности человека, они позволяют принимать более взвешенные решения и выводят процесс принятия решений на более качественный уровень. Совершенствование и реализация современных интеллектуальных информационных технологий и методологической базы в сфере поддержки принятия решений показывают необходимость применения наиболее эффективных разработок в ВМФ.

В целом специалистами ВМФ уделяется определенное внимание системам поддержки принятия решений (СППР) как самостоятельному классу систем или подсистем. Однако, по-прежнему не решен ряд важных вопросов их взаимосвязи и взаимодействия, в первую очередь, по организационной и правовой составляющей, а также по многим другим направлениям: методологическое, методическое, технологическое, эргономическое, техническое, стандартизации, унификации и сертификации и др.

Но, тем не менее, для форсированного наращивания научного задела в данном перспективном направлении уже сейчас требуется активнее и взвешеннее использовать апробированные разработки и лучшие технологические решения.

Учитывая особенности формирования и развития единого информационного пространства ВМФ, на начальном этапе необходимо создание обобщенной модели интегрированной СППР в виде модульной системы, в структуре которой объединяются как уже существующие, так и вновь создаваемые задачи и модели ППР, а так же системы или подсистемы ППР (реализованные в виде специального программного обеспечения).

В рамках настоящего исследования разработаны модель и предложения по ее реализации, базирующиеся на методологии структурного системного анализа [3], в основе которого лежит структурно-функциональное моделирование. Этот метод позволяет описать работу сложной системы, «не теряя» точности и её полноты.

Учитывая то, что компьютерная поддержка принятия решений необходима на всех этапах процесса принятия решений, в основе предлагаемой модели лежит процесс (процедура) принятия решений в обобщенном виде, который содержит основные этапы принятия решений. При решении частных (специфических) задач он может модифицироваться (адаптироваться), путем исключения или добавления определенных этапов.

Предложения в обобщенную модель процесса принятия решений представлены в виде диаграммы IDEF0 [3] и реализованы в программном средстве AllFusion Process Modeler (BPwin). Разработанная модель является базовой структурой, вокруг которой должна строиться интегрированная СППР. Выбор инструмента моделирования обусловлен его эффективностью и функциональностью при моделировании мероприятий, процедур, операций, действий, процессов, повторяющихся регулярно и ведущих к определенным результатам. Обеспечивает логическую строгость, необходимую для достижения корректных и согласованных результатов.

Процесс компьютерной поддержки принятия решений, заложенный в предлагаемую модель, содержит следующие основные этапы принятия решений: оценка обстановки, выработка замысла, генерация возможных альтернатив, оценка альтернатив по установленным критериям, согласование решений, моделирование и прогнозирование, выбор наилучшего решения. Каждый из этапов в свою очередь разделяется на подэтапы, с учетом вводимых для модели ограничений в соответствии с [1].

В тоже время, следует отметить, что информационной основой спроектированной модели, как и СППР, является совокупность соответствующих баз данных и баз знаний, объединенных в интеллектуальную СППР: база данных критериев; база моделей, методов и алгоритмов; база способов визуализации данных (представлений); «внешние» базы данных; база знаний решенных задач; база знаний СППР; база данных; базы данных функциональных подсистем.

Ключевым является совместное использование четырех основных видов СППР (интеллектуального анализа данных, информационно-справочной, оперативно-аналитической и экспертной) в качестве подсистем на том или ином этапе принятия решений, как по отдельности, так и

вместе, в зависимости от специфики решаемых задач. В процессе принятия решений на каждом из подэтапов работает та подсистема, которая наиболее эффективно решает поставленную задачу или подзадачу. Первые три подсистемы различаются по степени интеллектуальности. Экспертная подсистема выделена отдельно из-за своей высокой значимости при решении задач ВМФ.

В подсистеме интеллектуального анализа данных применяются различные методы и алгоритмы интеллектуального анализа (нейронные сети, генетические алгоритмы, нечеткая логика и др.) позволяющие выявлять скрытые тенденции, взаимосвязи и закономерности, учет влияния которых повысит качество принимаемых решений.

В информационно-справочной подсистеме осуществляется поиск требуемых данных в БД и БЗ, как правило, при помощи заранее определенных запросов.

В оперативно-аналитической подсистеме производится группирование и обобщение данных в виде необходимом должностному лицу. В отличие от предыдущей подсистемы заранее необходимые запросы не известны.

В экспертной подсистеме закладывается опыт и знания признанных специалистов (экспертов) в определенных областях в виде формализованных знаний.

Основные преимущества рассматриваемой модели, заключаются в том, что реализованная с ее помощью СППР позволит:

- не перестраивать уже существующие системы и реализованные в них задачи ППР;
- настраивать СППР под решение определенного круга регламентированных задач в соответствующем структурном подразделении;
- применять современные средства визуализации данных с различной степенью детализации результатов работы СППР и форм их представления;
- реализовать идею многовариантных расчетов с применением различных методов (моделей) для оптимизации решаемых задач, с варьируемыми при этом наборами и значениями переменных, параметров и критериев;
- обеспечить возможность настройки СППР в соответствии с потребностями пользователя и уровнем его квалификации;
- расширить возможности СППР путем добавления новых методов, методик, моделей (полимоделный подход), а также наличием средств гибкого конфигурирования СППР.
- провести квалиметрический анализ и оптимизацию структуры, применяемых задач, методов и информационных технологий в решении задач ППР;
- оценить результаты принятых решений с внесением изменений (если необходимо) в процесс принятия решения;
- прогнозировать развитие ситуаций на основе накопленных знаний;

Заключение. Создаваемая обобщенная модель интегрированной СППР ВМФ позволит максимально эффективно использовать уже реализованные задачи ППР в различных АСУ ВМФ, а также накопленные знания для выработки наиболее качественных и эффективных решений на всех уровнях управления по горизонтали и вертикали. Создание системы поддержки принятия решений, объединяющей все подзадачи ППР в единую систему, позволит систематизировать, классифицировать и проанализировать весь спектр задач, методов и моделей поддержки принятия решений для выбора наиболее эффективных в определенных условиях.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 50.1.028–2001. Информационные технологии поддержки жизненного цикла продукции. Методология функционального моделирования. – Введ. 2001–02–07. – М.: Изд-во стандартов, 2001. – 49 с.: ил.
2. Симанков, В. С. Методологические аспекты построения систем поддержки принятия решений / В. С. Симанков, С. Н. Владимиров, А. О. Денисенко, А. Н. Черкасов // Вестн. ДГТУ. – 2008. – № 3(38) – С. 258–268. – Библиогр.: с. 267
4. Качала, В.В. Общая теория систем и системный анализ. Учебник для вузов. / В.В. Качала. – М.: Горячая линия – Телеком, 2017. – 432 с.: ил.
5. Трахтенгерц, Э. А. Компьютерные методы поддержки принятия решений в нефтегазовой промышленности / Э.А. Трахтенгерц, Ю.П. Степин, А.Ф. Андреев. – М.: Синтез, 2005. – 592 с.: ил.

УДК 78.25.01.51

ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНОГО КОМПЬЮТЕРНОГО АНАЛИТИЧЕСКОГО ТРЕНАЖЕРА (СКАТ) «БАРС» ДЛЯ ОТРАБОТКИ ПРАКТИЧЕСКИХ НАВЫКОВ ПО ОБЕСПЕЧЕНИЮ ЯДЕРНОЙ И РАДИАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ЭКСПЛУАТАЦИИ ЯЭУ ЭКИПАЖАМИ КОРАБЛЕЙ И ПОДВОДНЫХ ЛОДОВ

Каленихин Владимир Альбертович, Леберянский Александр Павлович,
Салащенко Александр Иванович,
ВУНЦ ВМФ Военно-Морская Академия
Россия, Санкт-Петербург, Малоохтинский пр. 80/2

Аннотация: Рассмотрены основные этапы и возможности использования СКАТ «Барс» для полного и точного контроля уровня подготовленности слушателей

Ключевые слова: Специальный компьютерный аналитический тренажер «Барс»; ядерная безопасность; радиационная безопасность; ядерная энергетическая установка; главная энергетическая установка.

USE OF A SPECIAL COMPUTER ANALYTICAL SIMULATOR (SCAS) "BARS" FOR PRACTICAL SKILLS TO ENSURE NUCLEAR AND RADIATION SAFETY DURING OPERATION OF NUCLEAR POWER PLANT BY CREWS OF SHIPS AND SUMARINES

Vladimir Kalenikhin, Alexandr Leberyanskiy, Alexandr Salazhenk
Military Institute of additional professional education, Military Training and Research
Centre of the Navy "Naval Academy",
80/2, Malookhtinsky av., Saint-Petersburg, Russia.

Abstract: The article describes the main stages and the possibilities of using special computer analytical simulator (SCAS) "BARS" for complete and accurate control of the level of preparedness of students.

Keywords: special computer analytical simulator "BARS"; nuclear safety; radiation safety; nuclear power plant; main power plant.

Использование специального компьютерного аналитического тренажера (СКАТ) «Барс» для теоретической подготовки, отработки навыков использования технических средств ЯЭУ ВМФ у слушателей повышает интенсивность учебных занятий, наглядность и доступность обучения. Широкий спектр возможностей СКАТ «Барс» позволяет выстроить поэтапный процесс обучения, где каждый следующий этап будет органично продолжать и дополнять предшествующий. При этом на каждом рубеже предусматривается контроль знаний и навыков обучающихся в зависимости от их категории и уровня подготовленности.

СКАТ «Барс» предназначен для:

- подготовки личного состава по различным категориям офицерского состава атомных подводных лодок: вахтенных офицеров, вахтенных инженер–механиков, вахтенных операторов пульта управления главной энергетической установки (ГЭУ), вахтенных машинистов-трюмных дивизиона движения, как индивидуально, так и в составе смен и групп;
- восстановления (периодически и после перерыва в работе) знаний и навыков личного состава по управлению ГЭУ в нормальных и аварийных режимах работы, как последовательно, так и с любого этапа режима работы в зависимости от уровня подготовленности обучающихся;
- повышения профессиональных навыков личного состава при работе в режиме «тренажер» по управлению работой ядерной энергетической установки (ЯЭУ) от её ввода в действие и работе в нормальном режиме до работы в условиях аварийных ситуаций с поэтапным усложнением обстановки, имитация которой на действующей установке невозможна, но важна с точки зрения безопасности ГЭУ;
- работы в режиме теоретической подготовки в форме группового занятия под руководством преподавателя (на начальной стадии подготовки);
- работы в режиме как тестового контроля уровня теоретической подготовленности личного состава по категориям, так и в форме индивидуального и группового контроля теоретических знаний на макетах и схемах.

Тренажер может использоваться для анализа аварийных ситуаций с отказами элементов и оборудования ГЭУ, имевших место в ВМФ РФ, для анализа и выработки решений по локализации и ликвидации последствий аварий. Использование тренажера возможно, как в условиях учебного центра ВМФ на соединениях, так и в учреждениях высшего и дополнительного профессионального образования.

СКАТ «Барс» обеспечивает в следующих режимах выполнение задач:

- режим автономной тренировки оператора ГЭУ с возможностью решения задач с вводными заданиями ситуаций, в том числе и аварийных;
- режим проверки знаний при совместной работе оператора с инструктором как индивидуально, так и в составе групп;
- повышение уровня профессиональных знаний обучающихся различных категорий персонала (вахтенных офицеров, вахтенных инженер - механиков, командиров групп дистанционного управления, машинистов - трюмных дивизиона движения) по устройству и эксплуатации установки;
- приобретение навыков по управлению ГЭУ как в нормальных режимах, так и при возникновении аварийных ситуаций;

Программное обеспечение тренажера реализует комплексную математическую модель ГЭУ, имитирующую работу установки на всех режимах, предусмотренных инструкцией по управлению и эксплуатации ГЭУ и руководством по боевому использованию технических средств (РБИТС). А также обеспечивает отображение на экране дисплея: графиков изменения в реальном масштабе времени выбранных пользователем параметров ГЭУ; динамики изменения состояния ГЭУ на мнемосхеме ЦПУ, как в целом, так и фрагментарно, с цифровой индикацией изменения параметров в точках штатных замеров; табло предупредительной и аварийной сигнализации.

Работа преподавательского состава по информатизации образовательного процесса должна быть ориентирована на: создание благоприятных условий для индивидуализации и интенсификации образовательного процесса; обеспечение непрерывного контроля результатов познавательной деятельности слушателей и своевременного принятия мер по устранению выявленных недостатков; формирование у обучающихся твердых навыков применения компьютерной техники; развитие мотивации обучающихся к использованию современных информационных технологий в практической деятельности на флоте при решении профессиональных задач.

При проведении учебных занятий с использованием технологии СКАТ «Барс» возможны следующие формы:

- использование инструментальных программных средств при демонстрации учебных материалов (графиков, видеовставок, презентационных роликов и других документальных средств информационного обеспечения в электронном виде);
- использование систем специального программного обеспечения в виде методик решения информационно-расчетных, расчетных и аналитических задач;
- применение автоматизированных систем обучения.

Проведению занятий с применением тренажера «Барс» предшествует предварительная и непосредственная подготовка. Основным документом преподавателя, определяющим методику и порядок подготовки и проведения занятий с использованием тренажера, является методическая разработка. Она содержит необходимую информацию методического и технического характера. Содержание разработки - сценарий проведения занятия.

Методика подготовки и проведения занятий, подготовка технических средств обучения, требования к слушателям и техническому персоналу тренажера по подготовке, порядку применения технических и программных средств обучения, виды и формы контроля полноты отработки учебных вопросов и качества подготовки слушателей - все это отражено в методической разработке.

В ходе непосредственной подготовки преподаватель выдает задание слушателям (за 3-5 суток) и организует подготовку слушателей, инженерно-технического персонала, места проведения занятия в соответствии с методикой и с учетом специфики занятия.

Непосредственно перед занятием преподаватель проводит консультации с инженерно-техническим персоналом тренажера. В ходе занятия преподаватель управляет познавательным процессом, усложняет обстановку и активизирует слушателей, оказывая им необходимую помощь.

В ходе проведения занятий в режиме тренажера по каждому элементу происходит диалог «человек-машина», в котором операторские действия слушателей вызывают ту или иную ответную реакцию тренажера, которая служит основанием для оценки качества приобретенных умений. Кроме того, программный потенциал тренажера позволяет оценить и обратную реакцию слушателя на задаваемые условия технической или аварийной обстановки. Результаты оценивания формируют основу итоговых оценок, умений и навыков по заданной дисциплине.

Использование специального компьютерного аналитического тренажера (СКАТ) «Барс» при теоретической подготовке, формировании навыков использования технических средств ЯЭУ ВМФ у обучающихся, повышает интенсивность учебных занятий, наглядность и доступность обучения.

СПИСОК ЛИТЕРАТУРЫ.

1. Гусев Л.Б., Баленко Ю.К. Основы ядерной физики и теории ядерных реакторов: Учебное пособие – Санкт-Петербург ВМИИ 2004г. – 550 с.
2. Салашенко А.И. Методика проведения занятий на специальном компьютерном тренажере, 2011г. – 123 с.

УДК 656.611

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МОРСКОМ СЕКТОРЕ ЕВРОПЕЙСКОГО СОЮЗА

Колесникова Марина Львовна
Институт Европы РАН
Россия, г. Москва, Моховая ул., 11, стр. 3В
email: kml2007@mail.ru

Аннотация: Анализируется опыт Европейского союза по обеспечению информационной безопасности в морском секторе. Данный опыт может быть использован для разработки подходов к управлению указанной сферой в Российской Федерации.

Ключевые слова: информационная безопасность, морская деятельность, Европейский союз.

INFORMATION SECURITY IN THE MARITIME SECTOR OF THE EUROPEAN UNION

Kolesnikova Marina
Russia, Moscow, Mokhovaya Street 11, building 3B
email: kml2007@mail.ru

Abstract: The experience of the European Union to provide an information security in the maritime domain is analyzed. It could be base for advanced approaches to control the maritime domain in the Russian Federation.

Keywords: *information security, maritime activities, the European Union.*

Введение. Широкое распространение информационно-коммуникационных технологий (ИКТ) во всех областях деятельности повышает актуальность мер, направленных на обеспечение безопасности Российской Федерации в информационной сфере, в том числе по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления [1].

Развитие функциональных видов морской деятельности Российской Федерации связано с расширением применения и возрастанием сложности информационной инфраструктуры, которая используется для решения множества первостепенных и вспомогательных задач [2]. Учитывая то обстоятельство, что большая часть морских хозяйственных операций проходит в условиях постоянного воздействия агрессивной внешней среды, наличия высокой степени экологических рисков и повышенной вероятности значительного материального ущерба, обеспечение информационной безопасности является обязательным условием для эффективного осуществления морской деятельности.

Как особый вид вызовов и угроз для морской промышленности и судоходства оценивается растущий уровень кибератак [3]. Расширение автоматизации морской деятельности, использование электронной навигации, автоматических идентификационных систем (АИС), других ИКТ, а также перспективы перехода на беспилотное управление судами и средствами судоходства повышает уязвимость судоходства для хакерского информационного воздействия. Ситуация усугубляется существующим на данный момент низким уровнем "информированности о кибербезопасности" [4].

Таким образом, необходимость решения вопросов обеспечения информационной безопасности в морском секторе обусловлена объективными условиями, сложившимися в результате естественного развития ИКТ. В этой связи целесообразно исследовать и проанализировать накопленный в данной сфере опыт мирового сообщества, отдельных государств и Европейского союза с целью научной оценки и определения возможностей использования этого опыта в морской практике Российской Федерации.

К настоящему времени Европейским союзом приняты необходимые меры по разработке эффективной политики в области обеспечения информационной безопасности, в том числе в морском секторе. Разрабатывается соответствующая нормативная правовая база и проведен ряд актуальных исследований. В 2004 г. Постановлением № 460/2004 Европейского парламента и Совета ЕС [5] учреждена организация, которая занимается вопросами информационной безопасности Европейского союза – Агентство Европейского союза по сетевой и информационной безопасности (The European Union Agency for Network and Information Security, ENISA). Первый доклад, посвященный анализу аспектов информационной безопасности в морском секторе, опубликован ENISA в декабре 2011 г. В документе представлена базовая основа обеспечения кибербезопасности и сформулированы рекомендации по устранению рисков [6].

Закключение. К настоящему времени использование ИКТ стало одним из факторов развития человеческого общества. Новые технологии и научные достижения оказывают существенное влияние на интенсивность и повышение качества эксплуатации ресурсов и пространств Мирового океана. Технологическое расширение морехозяйственной активности сопровождается возрастанием количества новых вызовов и угроз, создающих опасность нанесения ущерба жизненно важным сферам жизнедеятельности человека. Наибольшие угрозы связаны с морскими отраслями, функционирование и развитие которых зависит от использования современных программно-аппаратных средств (систем), прежде всего, морского судоходства. К области особо уязвимых объектов можно отнести практически весь парк морских грузовых и пассажирских судов, средства навигационно-гидрографического и гидрометеорологического обеспечения, средства управления и связи.

Данные факторы целесообразно учитывать при планировании отраслевого развития морского транспорта и обеспечивающей его береговой инфраструктуры Российской Федерации, а также для системной оценки показателей эффективности морехозяйственной деятельности в целом как составной части экономического развития нашей страны.

СПИСОК ЛИТЕРАТУРЫ

1. Указ Президента РФ от 5 декабря 2016 г. № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации": Утверждено Президентом Российской Федерации 5 декабря 2016 г. // ГАРАНТ: информационно-правовой портал. URL: <http://www.garant.ru/products/ipo/prime/doc/71456224/> (дата обращения: 4.09.2017).
2. Глушков С.В., Кислов К.В. Анализ состояния информационной безопасности в морском секторе. В мире научных открытий. 2015. № 6.1 (66). – С. 534-547.
3. Lars Jensen. Technology Challenges in Maritime Cyber-Resilience // Innovation Management Review. April 2015: website. URL: http://timreview.ca/sites/default/files/article_PDF/Jensen_TIMReview_April2015.pdf (дата обращения: 31.08.2017).
4. Safety and Shipping Review 2015. // Allianz Global Corporate & Specialty SE: website. URL: https://www.allianz.com/v_1427190309000/media/press/document/other/Shipping-Review-2015.pdf (дата обращения: 2.09.2017).

6. Regulation (EC) № 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency // EU law and publications: website. URL: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML> (дата обращения: 3.09.2017).
7. Analysis of cyber security aspects in the maritime sector // The European Union Agency for Network and Information Security. December 19, 2011: website. URL: <https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1> (дата обращения: 12.08.2017).

УДК 623.8.9

К ВОПРОСУ О ПОВЫШЕНИИ ИНФОРМАЦИОННОГО КАЧЕСТВА МОРСКОГО ОБЪЕКТА

Кружилин Роман Вячеславович
НИИ ОСИС ВМФ ВУНЦ ВМФ «Военно-морская академия»
Россия, Санкт-Петербург, ул. Разводная, 17
email: rim_rim72@mail.ru

Аннотация: В статье рассмотрены специфика и направления повышения безопасности подводных объектов за счет интеграции робототехнического комплекса

Ключевые слова: интеграция, робототехнический комплекс, эффективность, информационное обеспечение

QUESTION OF THE INCREASE INFORMATION THE QUALITY OF THE MARINE FACILITY

Kruzhilin Roman Vyacheslavovich
SRI OSIS Navy Naval Forces Naval Academy "Naval Academy"
Russia, St. Petersburg, st. Divorce, 17
email: rim_rim72@mail.ru

Abstract: The article presents the specificity and improving the security of underwater objects through the integration of the robotic complex

Keywords: integration, robotic system, efficiency, information support

Введение. Применение робототехнических комплексов (РТК) необходимо, в том числе, в ситуациях, когда применение традиционных средств нецелесообразно, или связано с риском для жизни и здоровья людей, или иными неоправданно тяжкими последствиями.

Интеграция робототехнических комплексов в состав морских подводных объектов при решении ими поставленных задач является одним из направлений, как повышения качества информационного обеспечения, так и средством нейтрализации определенных негативных свойств.

Следует отметить, что почти все проекты РТК с широким спектром решаемых задач создавались в интересах военных организаций, о которых сказано достаточно полно и много.

В настоящее время в определенных ситуациях средства, входящие в состав подводного объекта, по ряду объективных причин недостаточно полно могут освещать окружающую обстановку. Интеграция же РТК должна способствовать решению такой проблемы и, как следствие, позволить повысить устойчивость функционирования подводного объекта.

Исходя из существующего уровня развития технологий, по дистанции обнаружения подводных целей РТК проигрывают подводным объектам - носителям. Данное обстоятельство не позволяет повысить зону освещенности носителя с опасных направлений на ходу.

В то же время, применение РТК с носителя для поиска, обнаружения, классификации представляющих опасность для носителя объектов (средств) может быть целесообразным. В результате ожидается повышение устойчивости носителя от такого рода опасностей и, соответственно, повышение информационного качества решения поставленных задач.

Однако, качественное решение задач мониторинга окружающей обстановки робототехническими комплексами в интересах повышения устойчивости подводного объекта (носителя) возможно только в реальном масштабе времени, что требует поиска целого ряда специфических технологических решений по обеспечению информационного качества объекта.

Таким образом, интеграция в состав морского объекта (носителя) РТК может информационно качественнее решать задачи поиска и обнаружения объектов на дне, в толще водного слоя, на ее поверхности, демаскирования объекта, уничтожения миноподобных и других объектов и т.д. Однако, для определения наиболее целесообразных задач, поставленных перед РТК в интересах повышения устойчивости подводного объекта (носителя), требуется проведение специфических исследований с соответствующим системно-техническим и военно-экономическим обоснованием.

СПИСОК ЛИТЕРАТУРЫ

1. Макаренко С.И. Робототехнические комплексы военного назначения - современное состояние и перспективы развития. Системы управления, связи и безопасность. 2016, № 2. С73-132.
2. Сиденко К.С., Голобоков С.А. Автономные обитаемые подводные аппараты-носители минного оружия. Россия и АТР, 2009, № 2. С.119-130.

УДК 629.12

СЕРВИСЫ, ТЕХНОЛОГИИ, УЯЗВИМОСТИ, УГРОЗЫ И ЗАЩИТА BLUETOOTH

Кузнецова Нина Александровна

Санкт-Петербургский государственный морской технический университет,
Россия, Санкт-Петербург, ул. Лоцманская, 3,
email: kuznecova-nina@list.ru

Аннотация: В статье указаны основные термины по всем пунктам указанные в теме. Наиболее распространенные угрозы и защита.

Ключевые слова: уязвимость, угроза, безопасность.

SERVICES, TECHNOLOGIES, VULNERABILITIES, THREATS AND PROTECTION OF BLUETOOTH

Kuznetsova Nina

State Marine Technical University of St. Petersburg,
Russia, Saint-Petersburg, Lotsmanskaya Str. 3,
email: kuznecova-nina@list.ru

Abstract: The article contains the main terms for all the items indicated in the topic. The most common threats and protection.

Keywords: vulnerability, threat, security.

Введение. Bluetooth – название, давно установившееся в технологии, которая используется для беспроводного подключения портативных электронных устройств; основана на использовании радиорелейных линий короткого диапазона. Это позволяет различным устройствам подключаться, будучи физически не связанными друг с другом.

Bluetooth может использоваться для создания беспроводной персональной сети (PAN). При этом обеспечивается быстрая и надёжная передача данных. Bluetooth предлагает беспроводной доступ к Интернету (для таких устройств как портативные компьютеры, КПК и т.д.).

Bluetooth имеет как плюсы, так и минусы в своей задаче. Однако при всех плюсах есть у него 3 огромных минуса: невысокая дальность действия, низкая (в сравнении с тем же wi-fi) скорость и огромное количество мелких и не очень недоработок.

Есть несколько разных видов атак на bluetooth-устройства, начиная от безобидных (типа BlueSnarf), кончая полноценными DoS-атаками, международными звонками без ведома владельца телефона и просто похищением СМС (BlueBug).

Актуальность темы заключается в ее повседневности, т.к. у каждого современного человека есть смартфон, у которого в стандартных функциях имеется Bluetooth. Современная гарнитура связана с данной функцией.

Цель работы: Изучить достоинства и недостатки, технологии, сервисы, типы угроз и защиту Bluetooth.

Заключение. В данной работе были проведены краткие ознакомление с технологией Bluetooth. За эти года постарались не только ударники компьютерного труда, но и хакеры, которые добиваются успехов. Взломав ваше устройство через bluetooth хакер, конечно, может прочитать ваши смс-ки, позвонить в другую страну, но это все детские шалости по сравнению с тем, что можно было бы сделать с машиной, управляемой элементами, соединёнными Bluetooth. Про плюсы системы говорить приятно, но цель работы была рассмотреть и недостатки. Через пару лет Bluetooth-технология еще больше вольется в нашу жизнь, что люди уже не смогут себе представить, как вообще существовали все это время без нее.

СПИСОК ЛИТЕРАТУРЫ

1. Bluetooth и ваша безопасность [Электронный ресурс] // сост: Stem А. Москва, [15 апреля 2013]. URL: <https://www.kaspersky.ru/blog/bluetooth-i-vasha-bezopasnost/733/> (Дата обращения: 23 сентября 2017).

УДК 004.056

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

Лавренова Анна Алексеевна

Санкт-Петербургский государственный морской технический университет,
Россия, Санкт-Петербург, ул. Лоцманская, 3,
email: lavrenova-anna@yandex.ru

Аннотация: В статье рассмотрено общее понятие цифровой подписи и ее устройство.

Ключевые слова: цифровой подписи (ЦП), электронной цифровой подписью (ЭЦП).

DIGITAL SIGNATURE

Lavrenova Anna

State Marine Technical University of St. Petersburg,
Russia, Saint-Petersburg, Lotsmanskaya Str. 3,
email: lavrenova-anna@yandex.ru

Abstract: the article considers the General concept of digital signature and its device.

Keywords: *digital signature (CPU), electronic digital signature (EDS).*

Требования экономики и развитие технологий привело к созданию и применению различных аналогов собственноручной подписи (АСП). На сегодняшний день используется большой набор различных АСП – факсимильные подписи, PIN коды, биометрические (например, отпечаток большого пальца правой руки, и т.д), системы цифровой подписи (ЦП).

Существует несколько схем построения цифровой подписи: на основе алгоритмов симметричного шифрования и на основе алгоритмов асимметричного шифрования. На основе асимметричных схем созданы модификации цифровой подписи, отвечающие различным требованиям.

Среди всех возможных технологий ЦП выбрана одна, строго определенная в Федеральном законе «Об электронной цифровой подписи», принятом в 2002 г. и названная электронной цифровой подписью (ЭЦП). ЭЦП – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, позволяющий идентифицировать владельца сертификата ключа подписи и установить отсутствие искажения информации в электронном документе. Электронный документ, заверенный ЭЦП, допускается в арбитражный процесс в качестве письменного доказательства и имеет правовой статус документа.

ЭЦП реализуется с помощью системы с открытым ключом. Данная система подразумевает использование ключевой парой, состоящей из: открытого ключа и секретного ключа. Главное свойство ключевой пары: по секретному ключу легко вычисляется открытый ключ, но по известному открытому ключу практически невозможно вычислить секретный.

Для формирования подписи используется закрытый ключ пользователя. ЭЦП представляет собой математическую функцию от содержимого подписываемых данных и секретного ключа, вычисляемую по стандартизованному алгоритму, предусмотренному ГОСТ 34.102002 в результате вычисления формируется пара чисел префикс и суффикс электронноцифровой подписи. Байтовые представления полученных чисел, записанные друг за другом, объявляются цифровой подписью.

Процедура проверки подлинности подписи включает в себя следующую последовательность шагов. Сначала из ЭЦП подписи выделяются ее префикс и суффикс. Затем с использованием специальной математической процедуры и открытого ключа вычисляется значение, которое должно быть префиксом ЭЦП. Затем оба полученных значения сравниваются. Если они совпадают, то данные считаются подлинными. Если полученные значения не совпадают, подпись считается недействительной.

Таким образом, для проверки подписи необходим открытый ключ или его сертификат. Использование сертификата предпочтительнее, поскольку он содержит не только открытый ключ, но и данные о владельце.

СПИСОК ЛИТЕРАТУРЫ

1. Информационный портал «Национальный Открытый Институт» [Электронный ресурс]. – «Криптографическая основа безопасности» 10 лекция – Режим доступа: <http://www.intuit.ru>. – Дата доступа: 23.09.2017.
2. Официальный сайт «Юридическая Россия» [Электронный ресурс]. – Режим доступа: <http://www>. <http://law.edu.ru>. – Дата доступа: 25.09.2017.

УДК 681.3.067

ОСОБЕННОСТИ РАЗРАБОТКИ СИСТЕМ ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ БОРЬБЫ ЗА ЖИВУЧЕСТЬ ПОДВОДНОЙ ЛОДКИ С УЧЕТОМ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Левоева Инга Валерьевна, Мудрова Алёна Александровна
АО «Концерн «НПО «Аврора»,
Россия, Санкт-Петербург, ул. Карбышева, 15,
emails: LevoevalV@avrova.spb.ru, MudrovaAA@avrova.spb.ru

Аннотация: В статье рассмотрен подход к разработке систем информационной поддержки борьбы за живучесть на судах ВМФ. Показаны особенности обеспечения информационной безопасности.

Ключевые слова: *система информационной поддержки борьбы за живучесть, информационная безопасность, информационная поддержка.*

THE FEATURES OF THE DEVELOPMENT OF INFORMATION SUPPORT SYSTEMS OF FIGHT FOR SURVIVABILITY OF SUBMARINE WITH THE INFORMATION SECURITY REQUIREMENTS

Levoeva Inga, Mudrova Alena

Concern Aurora Scientific and Production Association JSC,
Russia, Saint-Petersburg, Carbyshev Str. 15,
emails: LevoevalV@avrova.spb.ru, MudrovaAA@avrova.spb.ru

Abstract: The article examines the approach to the development of information support systems of fight for survivability. The features of information security are represented.

Keywords: *information support system of fight for survivability, information security, information support.*

Введение. Системы информационной поддержки (СИП) относятся к классу информационных систем и предназначены для формализации и актуализации задач прогнозирования, оценки и управления состоянием корабля и техническими средствами (ТС) при повседневной эксплуатации и при борьбе за живучесть (БЗЖ). Кроме того, в задачи таких автоматизированных систем (АС) традиционно входит обработка сведений, составляющих государственную тайну, и, следовательно, АС должны соответствовать ряду требований, предъявляемым к автоматизированным системам в защищенном исполнении (АСЗИ).

Разрабатываемые СИП включены в единую информационную сеть комплексной системы управления техническими средствами (КСУ ТС) и располагают всей динамической информацией о технических средствах, действиях операторов и информацией от внешних комплексов, которые классифицируются как центральные координирующие системы управления (ЦКСУ). С аппаратной точки зрения ЦКСУ – это пультовые стойки, включенные в информационную сеть КСУ ТС. ИП ЦКСУ может располагаться на отсечных приборах и на ноутбуках, включенных в информационную сеть.

К функциям современных ЦКСУ относятся: организация сетевого обмена КСУ ТС прием из СУ ТС и из внешних комплексов массивов информации о состоянии технических средств (включая массивы информации для регистрации); координированное управление ТС через операторов и руководство действиями личного состава отсеков в нормальных режимах эксплуатации и при возникновении аварийной ситуации; формирование, накопление и регистрация информации для анализа работы ТС, действий операторов и ведения вахтенной отчетности; просмотр на мониторе зарегистрированной информации; автоматическое формирование сигналов тревог-команд по каналам колоколо-ревунной сигнализации (КРС) и передача информации о состоянии ТС и решениях по БЗЖ на АРМ КК.

С точки зрения информационной безопасности к функциям ЦКСУ относятся:

- обеспечение безопасного межсетевого взаимодействия с применением сертифицированного программного комплекса межсетевого экранирования (ПК МЭ);
- аутентификация и идентификация непривилегированных (операторы системы) и привилегированных (администратор безопасности и супер-пользователь (root)) пользователей АСЗИ с целью обеспечения защиты от несанкционированного доступа к информации;
- регистрация и учёт событий в системе;
- обеспечение целостности программных средств и обрабатываемой информации;
- сигнализация попыток нарушения защиты;
- периодическое тестирование системы защиты информации от несанкционированного доступа (СЗИ НСД);
- восстановление СЗИ НСД.

Содержательная часть информационной поддержки разрабатывается на основе эксплуатационной документации заказа ЦКБ-проектанта, документации по БЖ и документов МО РФ.

Организационные и технические решения по созданию системы защиты информации в системе информационной поддержки разрабатываются:

- на основании ГОСТ в части защиты информации от НСД в АСЗИ;
- на основании руководящих документов Гостехкомиссии, регламентирующих требования к системе защиты информации и средствам защиты информации;
- на основе требований ТЗ на изделие в части защиты информации;
- на основании приказов МО РФ по обеспечению безопасности информации на объектах МО РФ.

Информационная поддержка обеспечивает выполнение следующих задач:

- представление обобщенных схем систем заказа с отображением текущего состояния основного оборудования и арматуры этих систем и рекомендациями по их переключению в штатные режимы системы;
- формирование рекомендаций КБЧ-5 по управлению ТС при различных аварийных ситуациях;
- представление параметров, необходимых для контроля различных ТС;

- представление информации о расположении помещений по настилам заказа с расположенным на них основным оборудованием;
 - автоматизированные модули для расчетных задач.
- Комплекс средств защиты системы, в свою очередь, обеспечивает:
- идентификацию, проверку подлинности и контроль доступа субъектов в систему; к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ; к программам; к томам, каталогам, файлам, записям, полям записей;
 - управление потоками информации;
 - регистрацию и учет входа/выхода субъектов доступа в/из систему (узел сети); запуска/завершения программ и процессов (заданий, задач); доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи; доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей; изменения полномочий субъектов доступа; создаваемых защищаемых объектов доступа;
 - учет носителей информации.
 - очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей;
 - сигнализацию попыток нарушения защиты;
 - обеспечение целостности программных средств и обрабатываемой информации.
 - физической охраны средств вычислительной техники (сигнализация; установка пломб и др.)
 - наличие администратора (службы) защиты информации в АСЗИ;
 - периодическое тестирование СЗИ НСД;
 - наличие средств восстановления СЗИ НСД;
 - экстренное уничтожение машинных носителей информации, содержащей сведения, составляющие государственную тайну;
 - использование сертифицированных средств защиты.

Заключение. Использование СИП повышает эффективность и скорость принятия руководителем БЗЖ правильных решений за счет визуализации расположения помещений и происходящих в них процессов. Расчетные задачи позволяют в кратчайшее время определить критическое состояние и теряемые функции заказа. При повседневном использовании система предоставляет всю необходимую для контроля и принятия решений динамическую, справочную и расчетную информацию. Соблюдение требований информационной безопасности при разработке АСЗИ, в свою очередь, сохраняет эксплуатационные характеристики системы при внедрении средств защиты. Решения по защите должны обеспечивать минимально допустимые потери производительности, надежности и удобства управления СИП БЖ.

СПИСОК ЛИТЕРАТУРЫ

1. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Гостехкомиссия России, Москва, 1992.
2. Корчанов В.М., Сус Г.Н., Ушакова Н.П. Опыт НПО «Аврора» по созданию систем информационной поддержки / Системы управления и обработки информации: Научн.-техн. сб./ ОАО «Концерн «НПО «Аврора». СПб, 2010, № 19, с. 93 - 101.

УДК 78.25.01.51

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЭКСПЛУАТАЦИИ ТЕХНИЧЕСКИХ СРЕДСТВ КОРАБЛЕЙ ВМФ

Москаленко Василий Александрович, Коваленко Дмитрий Игоревич, Калюта Николай Георгиевич
Военный институт дополнительного профессионального образования ВУНЦ ВМФ «ВМА»,
Россия, Санкт-Петербург, проспект Заневский, дом. 4,
emails: vasmoskalenko@mail.ru.

Аннотация: В статье рассмотрена проблема аварийности технических средств кораблей ВМФ и определены основные направления организационного и технического пути её решения.

Ключевые слова: безопасная эксплуатация, опасное состояние эксплуатации, опасный фактор, показатель безопасности эксплуатации, показатель риска, поражающий фактор.

SECURITY MAINTANANCE OF OPERATION OF TECHNICAL EQUIPMENT OF THE NAVAL SHIPS

Vasily Moskalenko, Dmitriy Kovalenko, Nikolay Kalyuta
Military Institute of additional professional education, Military Training and Research
Centre of the Navy "Naval Academy",
4, Zanevsky av., Saint-Petersburg, Russia.
email: vasmoskalenko@mail.ru

Abstract: The article discusses the problem of the accidents of technical equipment of the Naval ships and identifies the main directions of the organizational and technical solutions.

Keywords: *safe operation, dangerous state of operation of technical equipment, dangerous factor, indicator of safe operation, risk indicator, damage factor.*

Введение. Безопасность личного состава при эксплуатации технических средств продолжает оставаться низкой. Техническая аварийность на кораблях ВМФ, к сожалению, не сокращается. Основные силы брошены на разбирательства, констатацию факта аварии, тогда как необходимо думать о причинах. Пока же, если что и делается, то в авральном порядке. Для решения проблемы технической аварийности нужна система, которая способна управлять эксплуатацией технических средств кораблей. Необходим переход от чисто контрольных функций флагманских специалистов соединений к участию в фактических мероприятиях технического обслуживания и эксплуатации и, соответственно, руководству обеспечением безопасности личного состава.

Система работы флагманских специалистов по предотвращению технической аварийности должна быть направлена:

- на идентификацию источников опасности при эксплуатации технических систем;
- мониторинг и, на его основе, прогноз аварийных состояний технических средств;
- выполнение технических мер по повышению надежности эксплуатации механизмов;
- учет человеческого фактора;
- профессиональную подготовку специалистов и руководителей, эксплуатирующих оборудование кораблей.

Проблема безопасности эксплуатации технических средств носит общефлотский характер и требует комплексного подхода, формирования единого понимания данной проблемы, ответственности должностных лиц за результат и последствия принимаемых управленческих решений. Практическая деятельность офицеров-управленцев по обеспечению безопасности эксплуатации технических средств должна быть построена на следующих принципах:

- принцип приоритета безопасности экипажа кораблей;
- принцип интегральной оценки опасностей, так как управление риском включает эксплуатацию технических средств во всех режимах и различной обстановке;
- принцип допустимых режимов эксплуатации с учетом следующих аспектов:
 - а) технические средства должны эксплуатироваться на номинальных режимах;
 - б) должны быть проведены все технические виды обслуживания;
 - в) при продлении межремонтных сроков необходимо не просто оформление документов на продления, а должен быть выполнен весь регламент обслуживания, разработанный проектантом.

Состав мероприятий, которыми должна обеспечиваться безопасность при эксплуатации технических средств, должен учитывать следующие нормальные состояния технических средств: работающая аварийно-предупредительная сигнализация; сопротивление изоляции корабля в норме; предохранительные клапаны в строю и проверены; приборы проверены и работают; закрытия установлены и закреплены; заземления установлены; виброакустические характеристики механизмов в норме и т.д.

Необходимо контролировать выполнение всех рекомендаций КБ-проектанта по обеспечению безопасности при эксплуатации технических средств.

В настоящее время полностью определен круг теоретических и практических рекомендаций по безопасности военной службы Министерством обороны. Например, даются конкретные указания разработчику эксплуатационной документации, которые должен указать разработчик в эксплуатационной документации по техническому обслуживанию агрегатов (систем) ВВТ, включая следующие мероприятия:

- назначение технического освидетельствования механизма, периодичность его проведения на различных стадиях штатной эксплуатации и режимах хранения агрегатов (систем) ВВТ, а также продолжительность времени (в часах), необходимого для проведения этой работы;
- случаи внеочередного (досрочного) технического освидетельствования объекта;
- содержание и порядок проведения работ по подготовке объекта к техническому освидетельствованию (демонтаж, слив продукта, чистка, промывка, нейтрализация, сборка грузовых макетов) и требования к средствам технического освидетельствования;
- перечень стендов, контрольно-измерительных приборов, приспособлений, принадлежностей, инструмента, материалов и оборудования, необходимых для выполнения работ по техническому освидетельствованию, с указанием мест их размещения;
- схему (маршрут) осмотра узлов и элементов, обеспечивающих техническую безопасность объекта, с указанием дефектов и браковочных признаков, при наличии которых этот объект не может быть допущен к эксплуатации;
- перечень и последовательность проведения технологических работ, по проверке в работе (на функционирование) механизмов, электрооборудования, устройств и приборов безопасности;
- технологические карты проведения гидравлических испытаний сосудов, баллонов; в картах указываются номенклатура и спецификация средств технического освидетельствования и их

местонахождение, а также нормы расходуемых материалов при проведении технического освидетельствования;

- технические требования на дефектацию и ремонт, а также способы устранения дефектов;
- порядок приведения агрегата (системы) в исходное состояние после технического освидетельствования.

На результатах таких исследований формируются количественные и качественные параметры принимаемых управленческих решений, конструкторско-технологических и эксплуатационных нормативно-технических документов, заключений комиссий по анализу аварий и катастроф. Наиболее обобщающими считаются такие критерии как: риски для жизни и жизнедеятельности.

В условиях, когда нет возможности изменить технические средства, наука призвана разрабатывать надежные методы диагностики, продления ресурса безаварийной эксплуатации действующих механизмов, определить перспективы создания будущих технических систем, найти решения защиты человека, корабля от аварийных ситуаций и организации борьбы за живучесть.

Таким образом, важнейшая задача прикладной науки состоит в определении основных принципов безопасности сложных технических систем, построении классификации аварий и катастроф, предупреждения и смягчении их последствий.

По результатам исследований составляются необходимые для принятия управленческих решений прогнозные и оценочные карты.

Перспектива представляется, как движение внутрь сложной технической системы, к проектированию их по критериям безопасности. При этом учитывается, что в такой системе в процессе эксплуатации могут возникнуть цепочки событий, которые в обычной ситуации не приводят к опасным состояниям, но при определенном стечении обстоятельств могут стать причиной чрезвычайных ситуаций.

Заключение. Министерство обороны определяет, что система безопасности должна обеспечивать руководителей различных уровней: дорожными картами проведения работ с учетом времени и затрат на них; ремонтными ведомостями для различных организаций; заявками на запасные детали для организаций МТО; учет выполненных работ и главное - контролировать качество их выполнения.

СПИСОК ЛИТЕРАТУРЫ

1. Руководство по обеспечению безопасности военной службы в ВС РФ. Приказ МО РФ от 22.07. 2015 № 444.
2. О совершенствовании работы по обеспечению безопасности военной службы в ВС РФ. Приказ МО РФ от 03.04.2013 .

УДК 629.12

МОНИТОРИНГ И УПРАВЛЕНИЕ КОМПЛЕКСНОЙ БЕЗОПАСНОСТЬЮ МОРСКОГО ПОРТА

Пантелейкин Сергей Викторович

Санкт-Петербургский государственный морской технический университет

Россия, Санкт-Петербург, ул. Лоцманская, 3,

email: 12ser34@mail.ru

Аннотация: В статье рассмотрены системы обеспечения безопасности морских портов и судов.

Ключевые слова: морской порт, система, безопасность, суда

MONITORING AND MANAGEMENT OF INTEGRATED MARITIME SECURITY

Panteleikin Sergey

State Marine Technical University of St. Petersburg

Russia, Saint-Petersburg, Lotsmanskaya Str. 3,

email: 12ser34@mail.ru

Abstract: The article deals with the security systems of seaports and ships.

Keywords: seaport, system, security, ships

Введение. Морской порт - совокупность объектов инфраструктуры, расположенных на отдельно отведенных территориях и акватории, и предназначенных для обслуживания судов, обслуживания пассажиров, осуществления операций с грузами, в том числе их перевалки, и других услуг, обычно оказываемых в морском порту, а также взаимодействия с другими видами транспорта.

В настоящее время одним из актуальных вопросов в морских портах является обеспечение безопасности объектов. Обеспечение безопасности порта предназначено для исключения и предотвращения случаев хищений, диверсионных и террористических актов, а также предотвращения других противоправных действий, способных привести к серьезным социально-политическим последствиям и экологическим катастрофам.

Основной целью планирования мероприятий обеспечения морской безопасности в морском порту является создание единой системы безопасности в интересах защиты государства, судов, их

экипажей и пассажиров, перевозимого груза, объектов управления движением судов, средств связи и объектов навигации, портовых сооружений и обслуживающего персонала от незаконных актов и других инцидентов.

Международной общественностью признано, что Россия находится в числе передовых государств, наиболее ответственно реализующих международные требования по охране судов и портов. Правительством прилагается максимум усилий для того, чтобы защищенность критически важных и потенциально опасных объектов от угроз техногенного, природного характера и террористических актов соответствовала самым строгим требованиям.

Исследованы основные системы безопасности морских портов. Они включают в себя: систему контроля и управления доступом, систему охранной сигнализации, два типа РЛС и телевизионные камеры для наблюдения за контролируруемыми зонами и объектами с высокой разрешающей способностью - так называемые оптико-электронные комплексы. Исследуемые системы играют важную роль в обеспечении защиты морских портов.

Закключение. В связи с неослабевающей угрозой терроризма вопросам обеспечения безопасности уделяется все большее внимание. Для этого используются самые совершенные средства тревожной сигнализации, охранного телевизионного наблюдения, что позволяет предотвращать различные виды правонарушений, включая террористические акты. Вопросы обеспечения безопасности постоянно находятся под контролем руководства Большого порта «Санкт-Петербург», что дает весьма значимые результаты, но, тем не менее, требуют непрерывного совершенствования.

СПИСОК ЛИТЕРАТУРЫ

1. ЗАО "Компания Безопасность" [Электронный ресурс]. URL: <http://www.bezopasnost.ru/about/articles/detail/42/1042/> (Дата обращения: 24 сентября 2017).
2. Правовое положение капитана морского порта и его функции по обеспечению безопасности мореплавания" [Электронный ресурс] URL: <https://m.studwood.ru/881728/pravo/zaklyuchenie> (Дата обращения: 24 сентября 2017).

УДК 629.12

СОЦИАЛЬНЫЕ СЕТИ В ИНТЕРНЕТЕ

Пархатский Дмитрий Дмитриевич

Санкт-Петербургский государственный морской технический университет,
Россия, Санкт-Петербург, ул. Лотманская, 3,
email: dimario@mail.ru

Аннотация: Рассмотрены популярные социальные сети, их свойства и влияние на людей.

Ключевые слова: социальные сети, интернет, глобальная паутина.

SOCIAL NETWORK ON THE INTERNET

Parkhatskiy Dmitriy

State Marine Technical University of St. Petersburg,
Russia, Saint-Petersburg, Lotsmanskaya Str. 3,
email: dimario@mail.ru

Abstract: The article considers the popular social network, their pros and cons, and impact on people.

Keywords: social network, internet, global web

«Интернет», как всемирная информационная система, образующая киберпространство, особую реальность, порождает киберкультуру со своими понятиями, ценностями, образом мыслей и языком, является сегодня одной из главных составляющих становления информационного общества без границ и неопределенном масштабе.

Первые телекоммуникационные сети, прародители нынешней Глобальной паутины, изначально не предполагались как средство общения. Целью их создания были скорее совместные вычисления, а также доступ к компьютерным базам данных.

Термин «социальная сеть» появился в работе Джеймса Барнса «Классы и собрания в норвежском островном приходе» еще в 1954 году. Это социальная структура, состоящая из группы узлов, и которыми являются социальные объекты, и связей между ними (социальных взаимоотношений). Первым массово используемым способом компьютерно-опосредованного общения стала электронная почта, e-mail, появившись в середине 60-х годов прошлого века. Следующей вехой в развитии компьютерно-опосредованной коммуникации стало появление в 1980 году в США компьютерной сети Usenet. Далее, информационный рывок происходит в развитии системы почтовых сообщений – это ньюсгруппы или же телеконференции. Сервисная система, позволяющая общаться пользователям в реальном времени, была создана в 1988 году финским студентом Ярмо Ойкаринен.

Наиболее популярные социальные сети в странах СНГ: ВКонтакте (vkontakte.ru), Одноклассники (odnoklassniki.ru), Мой мир (mail.ru), Фейсбук, (facebook.com), Твиттер (twitter.com).

Актуальность проблемы заключается в том, что в течение последних нескольких лет веб-сервисы, построенные на социальном взаимодействии, стали объектом внимания самых широких слоев общества. Интернет перенасыщен информацией различного рода, отражающей прямо противоположные, взаимоисключающие точки зрения. Социальные сети за кратчайший срок стали популярны, возник интерес к веб-страницам. Для многих коммерческих, политических и прочих деятелей интернет – это способ дохода.

Цель работы – исследование природы социальных сетей и выявление их достоинств и недостатков. В связи с этим были решены следующие задачи: проследить историю развития социальных сетей; выявить наиболее популярные в настоящий момент социальные сети; выяснить имеют ли место и каковы негативные последствия несут социальные сети, какие проблемы существуют в связи с использованием социальных сетей.

Заключение: В результате исследования было выявлено, что более половины людей в мире младше 30 лет, и 96% тех, кто родился в новом веке, состоят в социальных сетях. Социальные сети на данный момент являются самым популярным времяпровождением в Интернете. Одна из восьми супружеских пар встретила благодаря социальным сетям. Чтобы получить 50 миллионов пользователей радио потребовалось 38 лет, телевидению – 13 лет, Интернету – 4 года.

Социальные сети – это не мимолетная «прихоть». Это фундаментальный прорыв в том, как мы общаемся. Сформулированы предложения по использованию и развитию ресурсов социосетей.

СПИСОК ЛИТЕРАТУРЫ

1. Мелюхин, И.С. Информационное общество: истоки, проблемы, тенденции развития/ И.С. Мелюхин. – М.: Аспект Пресс, 2009. – 19 с.
2. Безуглов, И. Г., Лебединский Б. Б., Безуглов А. И. Основы научного исследования: учебное пособие для аспирантов и студентов-дипломников/ И.Г. Безуглов, Б.Б. Лебединский, А.И. Безуглов – М.: Академический Проект, 2008, - 29 с.

УДК 621.192, 623.9, 681.518

ОСНОВЫ МЕТОДИКИ ПОСТРОЕНИЯ ВИЗУАЛИЗИРОВАННЫХ ЛОГИКО-ВЕРОЯТНОСТНЫХ МОДЕЛЕЙ СТРУКТУРНО-СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ

Поленин Владимир Иванович¹, Сущенко Дмитрий Андреевич²

Россия, Санкт-Петербург, Ушаковская наб., 17/1, Военный учебно-научный центр ВМФ «Военно-морская академия»

emails: ¹polenin@mail.ru, ²sushenkov_dmitri@mail.ru

Аннотация: В статье решается актуальная задача системного анализа, связанная с созданием модульных визуализированных логико-вероятностных моделей элементов, с использованием которых облегчается сборка структурных схем функционирования структурно-сложных объектов и систем в целом. Модульные структурные схемы отвечают требованиям унификации и комбинированного отражения влияния одновременно всех основных обычно учитываемых факторов и свойств. Визуальное программирование позволяет программировать, используя графические или символьные элементы, которыми можно манипулировать согласно некоторым правилам. Полученные результаты позволяют пользователям общего логико-вероятностного метода (ОЛВМ) создавать модели с требуемыми целевым назначением и свойствами, что обычно представляет собой значительные трудности

Ключевые слова: структурно-сложные объекты и системы; неблагоприятные и поражающие факторы; логико-вероятностные модели и методы; показатели надежности; эффективности и риска.

BASES OF THE TECHNIQUE OF CREATION OF THE MODELS OF STRUCTURAL AND DIFFICULT TECHNICAL SYSTEMS VISUALIZED BY LOGIKO-VEROYATNOSTNYH

Vladimir Polunin¹, Sushchenkov Dmitry Andreevich²

Russia, Saint-Petersburg, Ushakov nab., 17/1,

Military educational scientific center of Navy "Naval Academy"

emails: ¹polenin@mail.ru, ²sushenkov_dmitri@mail.ru

Abstract: In article the relevant problem of the system analysis connected with creation of the modular visualized logiko-probabilistic models of elements with which use assembly of block diagrams of functioning of structural and difficult objects and systems in general is facilitated is solved. Modular block diagrams meet the requirements of unification and the combined influence reflection of at the same time all major usually considered factors and properties. Visual programming allows to program, using graphic or symbolical elements which can be manipulated according to some rules. The received results allow users of the general logiko-probabilistic method (GLPM) to create models with the required purposes and properties that usually represents considerable difficulties

Keywords: *structurally complex objects and systems; and adverse effects; of logical-probabilistic models and methods; reliability; efficiency and risk.*

Одной из важных задач системного анализа структурно-сложных объектов является задача создания модульных структурных схем функционирования элементов, с использованием которых облегчается сборка структурных схем функционирования структурно-сложных объектов и систем в целом. В частности, именно на такой подход к созданию структурных схем функционирования структурно-сложных объектов и систем ориентирован программный комплекс автоматизированного структурного моделирования ПК АСМ «АРБИТР» [1], реализующий информационную технологию ОЛВМ [4].

При этом задача системного анализа функционирования структурно-сложных объектов состоит в создании таких структурных схем функционирования элементов и систем, которые комбинированно отражали бы влияние одновременно всех основных обычно учитываемых факторов и свойств и позволяли бы вычислять системные характеристики систем одновременно по всем основным обычно интересующим показателям.

К числу обычно учитываемых факторов и свойств технических систем относятся техническая безотказность элементов системы, воздействие внешних неблагоприятных факторов, стойкость элементов к этому воздействию и характер аварийных отказов (с развитием или без развития аварии). К числу обычно интересующих показателей относятся показатели устойчивости их функционирования и риска (ожидаемого ущерба), связанного с воздействием неблагоприятных внешних факторов.

Следует отметить, что при применении известных сетевых методов и программных комплексов, использующих логико-вероятностные методы, например, RELAX, Risk Spectrum и др., решение задачи создания единых моделей, учитывающих как нормальные условия функционирования, так и внешние неблагоприятные и поражающие факторы, является недоступным.

Второй задачей методического обеспечения моделирования, решение которой обеспечивается программным комплексом «АРБИТР», является задача визуального программирования – способа создания программ путем манипулирования графическими объектами вместо написания кода в текстовом виде. Визуализированное моделирование представляет собой подобие термина «Визуальное программирование», принятого в информационных технологиях [3, 5].

Примером может являться унифицированный язык моделирования UML (англ. Unified Modeling Language) в области разработки программного обеспечения моделирования бизнес-процессов. Другими примерами языков визуального программирования являются: Microsoft Visual Programming Language, язык для робототехники, Simulink MATLAB, AnyLogic.

MS Visual Studio и Delphi являются визуальными средами программирования, но не визуальными языками программирования.

Следует обратить внимание на то, что как ОЛВМ, так и упомянутые выше программные средства имеют предметной областью модели, которые можно отразить ориентированными графами. В ОЛВМ, AnyLogic и исследовании операций такого рода модели являются событийными моделями третьего уровня.

ОЛВМ при поддержке ПК АСМ также представляет собой систему визуального программирования, которая базируется на графическом отображении модели в форме ориентированных графов. Эту систему можно расширить до уровня визуализированного моделирования, что представляет собой ориентированные графы, элементы которых совмещаются с элементами графической формы модели вооруженной борьбы. В этом и состоит сущность предлагаемой информационной технологии.

Разработан комплекс визуализированных логико-вероятностных моделей, обеспечивающий пользователю ОЛВМ сборку необходимых моделей по некоторым формальным правилам.

В качестве примера рассмотрена модель и методика функционирования топливного трубопровода в агрессивной (опасной) среде, которые легко воспроизводятся визуальными средствами ОЛВМ. После их создания средствами ОЛВМ задача анализа устойчивости функционирования и риска (ожидаемого ущерба) исследуемой системы, связанных с воздействием неблагоприятных внешних факторов, решается автоматически. Адекватность итоговой схемы понятиям и состояниям полной устойчивости и полного риска и корректность ее логической реализации подтверждаются тем, что эти состояния-антиподы образуют полную группу событий и сумма их вероятностей удовлетворяет условию нормировки (равенства единице).

Выводы

Решена одна из важных задач системного анализа структурно-сложных объектов – задача создания модульных структурных схем функционирования элементов, с использованием которых облегчается сборка структурных схем функционирования структурно-сложных объектов и систем в целом. Результаты решения задачи ориентированы на информационную технологию ОЛВМ, реализованную в программных комплексах ПК АСМ 2001 и «АРБИТР».

Разработан комплекс визуализированных логико-вероятностных моделей процесса вооруженной борьбы, обеспечивающий пользователю ОЛВМ сборку необходимых моделей по некоторым

формальным правилам. Полученные результаты обеспечивают реализацию принципа доступности методов и технологии ОЛВМ для широкого круга пользователей и способствуют объективизации системных исследований структурно-сложных опасных производственных объектов и вооруженного противоборства.

СПИСОК ЛИТЕРАТУРЫ

1. АРБИТР, Программный комплекс автоматизированного структурно-логического моделирования и расчета надежности и безопасности систем (ПК АСМ СЗМА) базовая версия 1.0 / Автор Можаяев А.С. Правообладатель ОАО «СПИК СЗМА». // Свидетельство об официальной регистрации № 2003611101. – М.: РОСПАТЕНТ РФ, 2003.
2. Волгин Н.С., Махров Н.В., Юровский В.А. Исследование операций. Часть I. - Л.: ВМОЛА, 1978. - 301 с.
3. Моисеев Н.Н. Математические задачи системного анализа. – М.: Наука, 1981, 488с.
4. Поленин В.И., Рябинин, И.А., Свиринов С.К., Гладкова И.А. Применение общего логико-вероятностного метода для анализа технических, военных организационно-функциональных систем и вооруженного противоборства // Монография, научное издание / Под ред. А.С. Можаяева. – СПб: СПб-региональное отделение РАЕН, 2011. – 416 с.
5. Визуальное программирование: URL: http://life-prog.ru/view_zam2.php?id=162/ – 2017.

УДК 629.12.001.2

ПРОБЛЕМЫ КОМПЛЕКСИРОВАНИЯ И ИНТЕГРАЦИИ АСУ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Согонов Сергей Александрович, Алексеев Анатолий Владимирович, Хруцкий Олег Валентинович,
Равин Александр Александрович

Санкт-Петербургский государственный морской технический университет,
Россия, Санкт-Петербург, ул. Лоцманская, 3,
emails: ssogonov@mail.ru, 17151@bk.ru, obx47@mail.ru, ravinlki@mail.ru

Аннотация: В статье рассмотрены специфика и концепция решения проблем комплексирования и интеграции автоматизированных систем управления в защищенном исполнении.

Ключевые слова: комплексирование; интеграция; системный анализ, синтез, оптимизация.

PROBLEMS OF AGGREGATION AND INTEGRATION OF ACS IN A SECURE EXECUTION

Sergey Sogonov, Anatoly Alekseev, Oleg Khrutsky, Alexander Ravin
State Marine Technical University of St. Petersburg,
Russia, Saint-Petersburg, Lotsmanskaya Str. 3,
emails: ssogonov@mail.ru, 17151@bk.ru, obx47@mail.ru, ravinlki@mail.ru

Abstract: The article examines the specifics and the concept of resolving problems of aggregation and integration of automated control systems in the protected execution.

Keywords: aggregation; integration; system analysis, synthesis, optimization.

Введение. Все большее значение при автоматизации объектов морской техники и инфраструктуры (ОМТИ) в условиях активного внедрения новых информационных технологий, включая технологии информационной безопасности (ИБ), приобретают задачи комплексирования и интеграции средств ИБ и систем управления безопасностью ОМТИ. При этом, понятие комплексирования предусматривают объединение на стадии проектирования в комплекс нескольких аппаратно-программных средств с целью повышения качества и эффективности комплекса в целом, в том числе по критериям производительности, надежности и ИБ. Интеграция также представляет собой процесс объединения частей в целое с целью, в первую очередь, эффективного совместного использования отдельных (автономных) элементов в целое, в систему. Но при этом, как правило, без изменения архитектуры и параметров интегрируемых элементов системы в силу ограниченных возможностей, так как интегрируются готовые решения в целом. При этом, как правило, возникает известный ряд проблем, включая критическую проблему ИБ.

Актуальность и значимость проблем комплексирования и интеграции автоматизированных систем (АС), в первую очередь, систем управления (АСУ), а, тем более, в защищенном исполнении (АСЗИ), обусловлена рядом новых обстоятельств, включая:

- тенденцию последнего десятилетия, заключающуюся в возрастании сложности архитектуры АС и многозначности решаемых функциональных задач, используемых алгоритмов и программно-аппаратных средств, а также резкого возрастания сложности интерфейса «АСУ-Операторы АСУ», обеспечения ИБ АС и автоматизированных ОМТИ в целом;

- существенное возрастание, как следствие, стоимости разрабатываемых и эксплуатируемых АСЗИ, а также соответствующих рисков различного рода - технических, экономических, информационных, экологических, техногенных, социальных и т.п.;

- резкое возрастание сложности модельного представления разрабатываемых комплексов и систем, процессов функционирования и оценивания их качества (как проектной меры оценки соответствия предназначению) и эффективности (как меры реализации проектных оценок качества);

– неполноту реализации научных рекомендаций по эффективному комплексированию и интеграции АСЗИ, что, в свою очередь, приводит к снижению возможностей технологического развития, низкой конкурентной способности и тому подобных нежелательных последствий.

В этой связи представляется целесообразным новый подход к анализу и выработке новых, перспективных путей решения проблем комплексирования технологических решений и интеграции АСЗИ на ОМТИ. В основу этого подхода должны быть положены современные положения теории системного анализа и синтеза сложных эргатических (человеко-машинных) систем на основе:

- адекватного модельного представления функционирования АСЗИ, достигаемых показателей качества и эффективности в процессе эксплуатации АСЗИ;
- диагностирования и прогнозирования «поведения» каждого элемента АСЗИ и систем в целом;
- факторного анализа влияния характеристик АСЗИ на их качество и эффективность;
- количественного оценивания и прогнозирования конкурентной способности и перспективности развития АСЗИ, как с учетом технологических факторов, так и факторов социальных.

При этом вариантный анализ проектных системных, архитектурных, алгоритмических и технических решений и, безусловно, их оптимизация должны базироваться на реализации современных возможностей вычислительной техники по квалиметрическому обоснованию ранжирования качества этих вариантов, обоснованию оптимальных путей наращивания конкурентной способности и оптимальных путей перспективного развития. Следует отметить, что сегодня с учетом проблемы сложности решения задач ИБ АСЗИ среди специалистов доминируют чаще скептические взгляды, что сопровождается переходом к эвристике в управлении ОМТИ. Тем самым, еще более обостряется комплекс проблем, связанный не только с безопасной эксплуатацией объектов, но и потерей конкурентной способности и перспективности, потер технологической независимости.

В этих условиях именно переход к парадигме непрерывного оценивания, мониторинга, контроля системных показателей качества и эффективности АСЗИ при доминировании автоматических алгоритмов оценки состояния и минимизации числа автоматизированных процедур позволит обеспечить существенный скачок уровня проектного и эксплуатационного качества современных АСЗИ, безопасности их эксплуатации, минимизации рисков возникновения аварийных ситуаций и аварий, техногенных катастроф. При этом, главное – обеспечить безопасность персонала при эксплуатации объектов морской техники, включая критически важные типы кораблей и судов, морских платформ, подводных трубопроводов и других ОМТИ. Более того, при эффективном решении системных задач проектирования и эксплуатации АСЗИ ОМТИ такой подход позволит решить одну из главных и ключевых проблем современных сложных эргатических систем – минимизировать негативное влияние субъективных свойств операторов АСЗИ, так называемого и пресловутого «человеческого фактора». Тем самым перейти на качественно новый уровень информационно безопасных систем автоматизации, гарантированно обеспеченных как от ошибок операторов, их возможной некомпетентности или отсутствия должного опыта, так и от возможностей самых различных несанкционированных действий, обусловленных человеческим фактором персонала, включая нелояльность поведения, а также обусловленных целым спектром террористических угроз.

Состояние развития поднятой проблемы и решаемых сегодня задач исследований, по нашему мнению, не позволяет выйти на требуемый условиями мирового рынка уровень конкурентной способности создаваемых средств и систем автоматизации, представляет определенную национальную угрозу развития. Это отчасти обусловлено недооценкой важности системных аспектов анализа и синтеза технологических решений на предыдущем эволюционном этапе их развития.

Значимость предлагаемого пути решения рассмотренных проблем, по нашему мнению, состоит в использовании далеко не реализованных в полном объеме научно-технических возможностей поиска конструктивных (эффективных, конкурентно способных) и оптимальных технических решений, отвечающих, прежде всего, системным требованиям к АСЗИ, в том числе:

- количественного представления качества решаемых системных задач, его мониторингу с возможностью адаптивного реагирования на опасные тренды;
- введения контура управления в состав решаемых АСЗИ задач по квалиметрическому обеспечению контроля правильности, проектного качества и эффективности принятых управленческих решений как непосредственно лицами, принимающими решения (ЛПР), так и их обосновывающими (ЛОР) и исполняющими (ЛИР);
- введения в состав решаемых АСЗИ задач контура организационно-технического и административного мониторинга и управления качеством жизненного цикла АСЗИ, ОМТИ и создаваемой продукции, товаров и услуг с адекватным «прозрачным» спектром вариантов решений;
- создания практических условий по реализации одного из важнейших концептуальных принципов комплексной безопасности ОМТИ – обеспечения её информационной прозрачности.

Обоснованность предлагаемого авторами концептуального пути решения поставленных проблем и задач, поднятых организационно-научных проблем развития АСЗИ подтверждена результатами многочисленных вариантов численного моделирования для различных классов ОМТИ, а также рядом полученных в ходе исследований опытных данных, приведенными результатами апробации и практической реализации представленных материалов.

Заключение. Концептуальное решение современных проблем комплексирования и интеграции АСЗИ, обусловленных, прежде всего, резким возрастанием их сложности, следует искать, по мнению авторов, в первую очередь, на пути максимальной реализации научно-технических возможностей современного системного анализа, синтеза и оптимизации технологических решений с использованием контура непрерывного измерения, оценивания и прогнозирования системного состояния АСЗИ и ОМТИ в целом с максимизацией числа принимаемых автоматических решений и минимизацией числа автоматизированных процессов.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А.В. Концептуальные аспекты управления развитием критических объектов морской техники и морской инфраструктуры / Морские интеллектуальные технологии, 2015, № 2 (28), т. 1, с. 47 – 57.
2. Равин А, Хруцкий О. Прогнозирование технического состояния оборудования. LAP LAMBERT Academic Publishing, 2014.

УДК 681.518.54

СИСТЕМА ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ ОПЕРАТОРА ЭНЕРГЕТИЧЕСКОЙ УСТАНОВКИ

Хруцкий Олег Валентинович, Алексеев Анатолий Владимирович, Согонов Сергей Александрович
Петербургский государственный морской технический университет,
Россия, Санкт-Петербург, ул. Лощманская, 3,
emails: obx47@mail.ru, 17151@bk.ru, ssogonov@mail.ru

Аннотация: в докладе рассматривается вариант построения системы информационной поддержки оператора энергетической установки на примере дизель-генераторной установки.

Ключевые слова: дизель- генераторная установка, текущее техническое состояние, оператор, информационная поддержка.

SYSTEM OF INFORMATION SUPPORT OF THE OPERATOR OF THE POWER PLANT

Oleg Khrutsky, Anatoly Alekseev, Sogonov Sergey
State Marine Technical University of St. Petersburg,
Russia, Saint-Petersburg, Lotsmanskaya Str. 3,
emails: obx47@mail.ru, 17151@bk.ru, ssogonov@mail.ru

Abstract: the report considers the option of constructing a system of information support of the operator of the power plant, for example a diesel generator set.

Keywords: diesel generator set, the current technical condition, the operator, information support.

Введение. В работе [1] отмечается, что по данным института машиноведения им. А.А. Благонравова РАН значимость человеческого фактора в техногенных катастрофах в различных отраслях техносферы составляет от 0,35 до 0,85. При этом, до настоящего времени термин «человеческий фактор» благодаря неоднозначности его определения широко используется учёными и специалистами применительно к самым разным случаям: при разработке условий жизнедеятельности человека, в исследованиях рисков из-за ошибочных решений и действий человека в экономике, политике, производстве, при конструировании эргатических систем - «человек-машина» и рабочих мест оператора таких систем и т.д. Ошибки управления в эргатических системах наиболее часто связаны с неверным принятием решений операторами. Естественно, что подобные ошибки при управлении техническими системами могут иметь серьёзные и далеко идущие последствия, зависящие от функциональной значимости системы и числа объектов, входящих в эту систему и лимитирующих её работоспособность и безопасность. В статье рассматривается один из вариантов построения системы информационной поддержки оператора энергетической установки на примере дизель-генераторной установки.

Дизель-генераторная установка (ДГУ) может в любой период эксплуатации находиться в одном из трёх состояний [2]: текущее техническое обслуживание (ТО), готовность к пуску и автоматический пуск (АП) или работа на нагрузку (РН). Все три состояния можно представить замкнутой граф-схемой состояний: «ТО-АП-РН». В любом из этих состояний принимает определённое участие человек. В данном случае человек – это оператор ДГУ, иначе лицо принимающее решение (ЛПР) или обслуживающий персонал.

В зависимости от текущего технического состояния ДГУ, оператор должен выполнять строго определённые функции. При этом, как показывают статистические данные, аварийность, в частности, судовых технических средств обусловлена, как правило, нарушением инструкций по эксплуатации и обслуживанию, а также некачественными и (или) несвоевременными профилактическими осмотрами и ремонтами. В указанных случаях существует прямое или косвенное влияние «пресловутого человеческого фактора». В идеале, чтобы уменьшить это влияние, необходимо максимально возможно снизить долю участия человека во всех процедурах по управлению и техническому обслуживанию ДГУ, т.е. практически полностью автоматизировать их. В настоящее время это, как правило, не представляется возможным. В результате возникает противоречие. С одной стороны, для увеличения

срока безаварийной эксплуатации ДГУ необходимо уменьшить количество влияний на её техническое состояние, исходящих от человека. С другой стороны, человек должен выполнять определённые действия для поддержания заданного технического состояния ДГУ. Как видно, это противоречие не позволяет (и вряд ли в ближайшей перспективе позволит) полностью исключить человека из цикла эксплуатации ДГУ.

Поскольку суть «вредного влияния», оказываемого человеком на ДГУ, определяется именно человеческим фактором, то требуется уменьшить это влияние. Будем под человеческим фактором понимать его физические и психологические особенности, не позволяющие его рассматривать как идеального исполнителя. Именно благодаря этому фактору человек не способен долго выполнять монотонную работу. В тоже время, благодаря этому фактору человек способен работать в условиях дефицита информации, что не свойственно искусственно созданным системам. Кроме того, независимо от уровня сложности техники, только человек способен принять решение (при соответствующей информационной поддержке) о степени опасности для окружающей среды и общества действия или бездействия технического объекта.

Рассматривая создаваемую систему с точки зрения уменьшения ошибок человека при управлении ДГУ, целесообразно под человеческим фактором понимать совокупность всех трудно учитываемых и, практически, не формализуемых характеристик: физические и психологические свойства, отношение к выполняемой работе, целеустремлённость, инициативность, уверенность в своих действиях, имеющийся опыт работы и т.п.

Схему эвристической модели взаимодействия между человеком и ДГУ с учётом человеческого фактора можно представить как «Ч-СИП-ДГУ», где Ч - человек, СИП – система информационной поддержки. В такой схеме циркулируют следующие информационные потоки: полный поток информации, исходящий от человека к ДГУ и включающий сумму двух потоков – правильные команды и действия оператора и ошибочные команды и действия, обусловленные человеческим фактором. В свою очередь, от ДГУ к человеку исходит поток контрольно-диагностической информации. Данный исходящий поток содержит информацию, которую человек может воспринять и (или) осознать и информацию, которую он не воспринимает в силу психологических или других причин. Если не воспринимаемую информацию обработать с учётом «человеческого фактора», то можно снизить неопределённость при принятии решения человеком, что, в свою очередь, уменьшит количество неправильных решений и снизит объём информационного потока от человека к ДГУ. Реализация двух данных функций позволит уменьшить информационную нагрузку человека и оптимизировать его работу.

Из сказанного следует, что «человеческий фактор» определяет скорость восприятия и объём воспринимаемой человеком информации, а также качество анализа информации и суть вносимых не совсем верных (неверных) решений. С точки зрения управления ДГУ «человеческий фактор» не имеет значения сам по себе, но важно его влияние на процесс выработки решения при управлении ДГУ. И здесь основную роль должна играть СИП. Какова же должна быть структура СИП? Поскольку данная система является информационно связующей между человеком и ДГУ, то она должна в прямом информационном канале «человек - ДГУ» содержать фильтр человеческого фактора (ФЧФ), обеспечивающий контроль и отсеивание ошибочных действий человека. В обратный информационный канал «ДГУ - человек» должен быть включён лингвистический процессор (ЛП), обеспечивающий представление человеку сведений о работе ДГУ на проблемно-ориентированном языке, который будет являться упрощённой версией естественного языка. При этом СИП должна хранить информацию фактографических данных о работе в нештатных ситуациях ДГУ, моделировать текущую ситуацию технического состояния ДГУ и обеспечивать, собственно, подбор необходимой человеку информации в соответствии с текущей ситуацией.

Заключение. СИП может быть реализована на базе современных микропроцессорных устройств сбора и обработки информации. Ориентировочная стоимость СИП с учётом аппаратно- программных средств и набора необходимых датчиков, контролирующих техническое состояние функционально значимых узлов ДГУ, не должна превысить (2...4) стоимости используемых микропроцессорных регуляторов скорости ДГУ. В то же время только неправильная настройка микропроцессорного регулятора скорости дизеля, под влиянием человеческого фактора может привести, в лучшем случае, к простоя дизеля, а для настройки регулятора может потребоваться вызов специалиста от фирмы-изготовителя.

СПИСОК ЛИТЕРАТУРЫ

1. Доброборский Б.С. Безопасность машин и человеческий фактор. СПбГАСУ.- СПб., 2011.
2. Литов Д.В. Универсальный алгоритм управления дизель-генераторными установками/ Судостроение, 1995, №2/3.
3. Хруцкий О.В. Техническая диагностика. СПбГМТУ.- СПб., 2005.

УДК 629.12

**ИНТЕЛЛЕКТУАЛЬНАЯ ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ АДМИНИСТРАТОРА ИБ
ТИПОВЫХ ОМТИ**

Стрельцов Егор Сергеевич
Санкт-Петербургский государственный морской технический университет,
Россия, Санкт-Петербург, ул. Лоцманская, 3,
email: streltsove@gmail.com

Аннотация: Рассмотрена актуальность и типовое решение для построения интеллектуальной поддержки принятия решений администратора информационной безопасности на основе метода сигнатурного обнаружения и противодействия кибератакам.

Ключевые слова: информационная сфера; объекты информатизации; технологии безопасности; информационная безопасность; сигнатура.

INTELLIGENT DECISION SUPPORT ADMINISTRATOR IB MODEL FRTO

Egor Archers
Saint-Petersburg state marine technical University,
Russia, Saint-Petersburg, street Pilot, 3,
email: streltsove@gmail.com

Abstract: Considers the relevance and the standard solution for building intelligent decision support administrator information security based on the method signature-based detection and cyber-attack prevention.

Keywords: information sphere; information objects; security technology; information security; signature.

Системы обнаружения – это неотъемлемая часть современного мира, где практически все страны имеют свой «информационный щит». Главная задача своевременно выявить злоумышленников и не дать им возможности получить интересующую их информацию. Но как сделать так, чтобы своевременно можно было бы получить данные о взломе?

Для этого существует отдельный класс систем обеспечения защиты информации по предотвращению атак (Intrusion Prevention Systems или сокращено IPS)

Встречаются ситуации, когда функции IPS ограничивают возможностями firewall. Однако, в firewall безопасность зависит от того, как организовано ограничение доступа к своей сети, а в IPS – от умения программистов-производителей писать безошибочные алгоритмы поиска атак в сетевом трафике.

IPS в корпоративных сетях являются частью многоэшелонированной системы защиты, поскольку интегрируются с другими средствами защиты: межсетевыми экранами; сканерами безопасности; системами управления инцидентами и, даже, антивирусными средствами.

В итоге, для каждой атаки сегодня имеются возможности не только идентифицировать ее, а затем оповестить администратора или заблокировать, но и провести полный анализ инцидента: собрать пакеты, идущие от атакующего; инициировать расследование; произвести устранение уязвимости путем модификации пакета.

Главный вопрос в том, как же противодействовать этим кибератакам?

Как известно, кибератак не избежать. Ещё не создали настолько совершенную программу, которая будет распознавать все виды атак, вирусов, спама и т.д.

Чем больше будет антивирусных систем, тем больше будет новых вирусов, которые будут обходить эти системы.

В этом контексте одним из конструктивных направлений обеспечения информационной безопасности ресурсов личности, общества, государства следует считать технологии сигнатурных методов выявления вторжений.

Вместе с тем, сигнатурные системы всегда будут «отставать» от возможностей киберпреступников, на стороне которых в этом случае всегда будет оставаться внезапность вторжения.

Поэтому требуется поиск альтернативных «оборонительной тактике» методов противодействия с позиций «наступательной тактики» и эффективного противоборства в целом информационным вторжениям.

Но главным их свойством и требованием, предъявляемым к сигнатурным системам обнаружения и противодействия кибератакам, по нашему мнению, следует считать автоматический характер адаптации (самонастройки) к атаке и её автоматическое «включение» для нейтрализации вторжения, либо информационного подавления самого киберпреступника с его информационными ресурсами.

СПИСОК ЛИТЕРАТУРЫ

1. <http://www.securitylab.ru/contest/358500.php>

УДК 629.12.001

ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЕ ПОЛОЖЕНИЯ ФОРМИРОВАНИЯ И РАЗВИТИЯ ПСМВ КАК ЛАБОРАТОРИИ И ЦЕНТРА ФОРМИРОВАНИЯ СОВРЕМЕННЫХ IS-КОМПЕТЕНЦИЙ

Тюрин Иван Сергеевич, Разживин Никита Сергеевич, Жуланова Дарья Николаевна
Санкт-Петербургский государственный морской технический университет,
Россия, Санкт-Петербург, ул. Лощманская, 3,
emails: cotip@bk.ru

Аннотация: Обобщен опыт организации и проведения в Санкт-Петербургском государственном морском техническом университете факультативного двухлетнего цикла специализированных тренингов в рамках созданного Центра освоения технологий информационного противоборства. Обоснован комплекс организационно-методических положений по созданию и развитию Полигона сетевых межвузовских взаимодействий (ПСМВ) как творческой лаборатории специализирующихся в области информационной безопасности студентов, магистрантов и аспирантов в обеспечение Центра формирования современных IS-компетенций.

Ключевые слова: информационное противоборство; компетенции; освоение технологий; полигон сетевого межвузовского взаимодействия; соревнование по CTF.

ORGANIZATIONAL-METHODICAL PROVISION OF FORMATION AND DEVELOPMENT OF PSPS AS A LABORATORY AND CENTER OF FORMATION OF THE MODERN IS-COMPETENCES

Ivan Tyurin, Nikita Razzhivin, Daria Zhulanova
Saint-Petersburg state marine technical University,
Russia, Saint-Petersburg, street Pilot, 3,
emails: iapbgks@bk.ru

Abstract: It summarizes the experience of organizing and conducting at the St. Petersburg state marine technical University optional two-year cycle of specialized training within the new Center of technology of information warfare. Justified complex of organizational and methodological provisions for the creation and development of the Polygon network of inter-institutional interactions (PSPS) as a creative laboratory specializing in the field of information security students, undergraduates and graduate students in providing the Center with the formation of the modern IS-expertise.

Keywords: information warfare; competences; learning; polygon network of University cooperation; competition in CTF.

Острую необходимость создания и масштабной апробации многочисленных методов и технологических решений по обеспечению информационной безопасности (ИБ), информационного противодействия (ИПД) и в комплексе – информационного противоборства (ИП) обуславливает сегодня интенсивное развитие разнородных подсистем защиты информации в составе современных автоматизированных систем в защищенном исполнении (АСЗИ). С учетом их ключевого значения в составе современных систем обеспечения комплексной безопасности производственных комплексов и систем, социальных информационных сетей и систем и т.п. к качественной апробации и освоению новых IS-технологий предъявляются крайне высокие методические, технологические, организационные и квалификационные требования. Однако, должных для этого ресурсов, в первую очередь, для учебных процессов выделяется крайне недостаточное количество. Это приводит к соответствующим ресурсным потерям на этапе использования средств и систем ИБ. А, тем более, при необходимости ИПД. Но, более всего, это приводит к потерям качества обеспечения защищенности информационных ресурсов (ИР), включая невосполнимые и критические.

В этих условиях одним из внутренних ресурсов восполнения названной системной уязвимости и очевидных угроз развития сравнительно новой, но бурно развивающейся отрасли систем автоматизации управления в защищенном исполнении, по нашему мнению, может быть партнерское формирование лабораторий и центров компетенций с использованием малоресурсоёмких (виртуальных) «площадок» освоения и отработки высокотехнологичных проектных и конструкторских решений. Именно в этом контексте в 2014 г. была предложена и разработана концепция, а в 2015 г. создан в Санкт-Петербургском государственном морском техническом университете (хорошо известной «Корабелке») факультативный Центр освоения технологий информационного противоборства (ЦОТИП) с проведением циклов специализированных тренингов [1 - 3].

В развитие принципов и накопленного опыта ЦОТИП в рамках инновационного проекта [4] предлагается рассмотреть, обсудить, в том числе со специалистами высоко авторитетной межрегиональной конференции «ИБРР-2017», следующие основные организационно-методические положения формирования и развития ПСОИП с пилотным проектом в межвузовском формате типа Полигона сетевого межвузовского взаимодействия (ПСМВ) [1 - 3], как лаборатории и центра формирования современных IS-компетенций:

Систематический (например, ежемесячно) взаимный обмен информацией и опытом в данной предметной области между студентами, магистрантами, аспирантами и профессорско-преподавательским составом заинтересованных ВУЗов и других учебных заведений с использованием технологий видеоконференций, вебинаров и т.п. Это будет способствовать формированию виртуальной партнерской консолидации распределенных интеллектуальных и ИР в интересах повышения потенциала, качества и защищенности ИР участников взаимодействия, формирования Партнерского центра компетенций в области IS-технологий.

Освоение перспективных технологий ИП, обобщение и ранжирование лучших практик на основе систематизации данных и квалиметрического оценивания технологий ИБ, ИПД и комплексного ИП в целом в интересах ускоренного практического освоения и внедрения лучших проектных и управленческих решений в организациях и на предприятиях с учетом всех публикуемых данных.

Формирование межвузовского и партнерского научно-технического сообщества и потенциала специалистов по ИП, объединения их для решений сложных, наукоемких и ресурсоемких проектов, в том числе в формате регулярного проведения соревнований по ИП, например, в формате соревнований CTF с целью повышения уровня квалификации участников взаимодействия, формирования региональной команды для участия в международных соревнованиях.

Теоретическое обобщение и моделирование процессов ИП, их анализ, синтез и оптимизация, а также разработка теории практики создания, построения, освоения и эксплуатации средств и технологий автоматизации процессов и АСЗИ, локализации информационных инцидентов на различных объектах, включая критические – объекты морской техники и инфраструктуры (ОМТИ).

Развитие и совершенствование практических навыков ИБ, ИПД и комплексного ИП студентов, магистрантов, аспирантов и преподавателей на основе проведения межвузовских сетевых тренингов практикующими специалистами смежных специализаций (администраторы ИБ, программисты, системные администраторы, специалисты по комплексной защите информации).

Проведение совместных инновационных проработок по моделированию процессов межсистемного и внутрисистемного взаимодействия в защищенном исполнении. Это будет, безусловно, способствовать виртуальной партнерской консолидации распределенных интеллектуальных, информационных ресурсов (знаний, умений и навыков, владений), программных и аппаратных ресурсов ВУЗов для взаимной отработки и использования на площадке ПСМВ (ПСОИП) технологий межсетевого и межобъектового взаимодействия, что даже для хорошо технологически обеспеченных вузов может быть недоступным в силу специфики масштабов сетевых инцидентов.

Интенсивное освоение подсистем и технологий не только защиты информации (ИБ), но и технологий ИПД, что сегодня приобретает востребованное и ключевое значение для систем обеспечения комплексной безопасности. Это будет способствовать в свете требований одной из стратегических целей Доктрины информационной безопасности РФ (5.12.2016, ст. 20, 22, 26, 27) поддержке инновационного и ускоренного развития систем обеспечения ИБ, отрасли информационных технологий и электронной промышленности, достижения конкурентноспособности ИТ и развития научно-технического потенциала.

Создание межвузовской технологической базы для сетевого взаимодействия и мониторинга состояния защищенности выделенных ресурсов, сегментов Интернета, а также моделирования и межвузовской тренажерной отработки технологий и задач ИП (сетевое противоборство, включая имитационное моделирование задач сетевых ИИ, атак, сражений, хаккинга и т.п.).

Разработка учебно-методических комплексов по технологиям ИП с формированием, ведением и актуализацией баз данных и знаний по технологиям ИБ, ИПД и комплексному ИП, а также лучшим практикам преподавания дисциплин по этим дисциплинам.

Тем самым, создание и развития ПСМВ, как лаборатории и центра формирования современных IS-компетенций позволит уже в ближайшее время обеспечить организационно-техническое, научно-техническое и информационно-прозрачное пространство (площадку) для межвузовского взаимодействия при решении ресурсоемких и наукоемких проблем ИБ, ИПД и ИП в целом. В качестве контактной точки такого взаимодействия и сотрудничества предлагаем почтовый адрес – cotip@bk.ru.

СПИСОК ЛИТЕРАТУРЫ

1. Согонов С.А., Алексеев А.В., Тюрин И.С., Разживин И.С., Жуланова Д.Н., Филиппова А.С., Шитикова К.А., Кальбфляйш В.А. Предложение по созданию полигона сетевого межвузовского взаимодействия и моделирования процессов информационного противоборства / Региональная информатика «РИ-2016»: Материалы конференции. \ СПОИСУ. – СПб, 2016, с. 458 – 459.
2. Тюрин И.С., Алексеев А.В. Особенности реализации Системы поддержки принятия решений Администратора ЦОТИП в варианте "СПРУ-ИБ" / Региональная информатика «РИ-2016»: Материалы конференции. \ СПОИСУ. – СПб, 2016, с. 459-460.
3. Тюрин И.С., Жуланова Д.Н., Разживин И.С., Филиппова А.С., Согонов С.А., Алексеев А.В. Центр освоения технологий информационного противоборства и борьбы за информационную живучесть объектов морской техники и морской инфраструктуры / Корабельная энергетика: из прошлого в будущее: материалы Всероссийского межотраслевого научно-технического форума. – СПб.: Изд-во СПбГМУ, 2017, с. 479 – 483.
4. Алексеев А.В., Барабаш П.А., Жигadlo В.Э., Зикратов И.А., Ныров А.П. Концепция Полигона сетевой межобъектовой отработки технологий управления и обеспечения превосходства в инфосфере / Информационная безопасность регионов России «ИБРР-2017»: Материалы конференции. \ СПОИСУ. – СПб, 2017 (в печати).

УДК 629.12.001.2

СОСТАВ И ТРЕБОВАНИЯ К СИСТЕМЕ МОНИТОРИНГА И УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ОМТИ

Тюрина Виктория Викторовна, Тюрин Иван Сергеевич
Санкт-Петербургский государственный морской технический университет,
Россия, Санкт-Петербург, ул. Лощманская, 3,
email: tyurinaviktoria7@gmail.com, lefes123@gmail.com

Аннотация: Рассмотрены и сформулированы требования к архитектуре и функциям системы мониторинга, поддержки принятия и управления комплексной безопасностью ОМТИ.

Ключевые слова: мониторинг; реальный масштаб времени; человеческий фактор; требования, безопасность.

COMPOSITION AND REQUIREMENTS TO THE MONITORING AND SAFETY MANAGEMENT SYSTEM OMTI

Victoria Tiurina, Ivan Tiurin
State Marine Technical University of St. Petersburg,
Russia, Saint-Petersburg, Lotsmanskaya Str. 3,
emails: tyurinaviktoria7@gmail.com, lefes123@gmail.com

Abstract: Reviewed and formulated the requirements to the architecture and functions of the monitoring system, making support and management of integrated security OMTI.

Keywords: monitoring, real time scale, human factor, requirements, security.

Системы мониторинга и управления комплексной безопасностью различного назначения с годами приобретают все большие возможности и становятся весьма значимыми при использовании в сложных технических системах, в том числе и для управления информационной безопасностью объектов морской техники и морской инфраструктуры (ОМТИ). Сегмент управления безопасностью является одним из самых сложных в связи с большим количеством критериев и показателей, которые требуется реализовывать, анализировать и сопоставлять. В результате этого данный сегмент требует непрерывного совершенствования алгоритмов мониторинга и их реализации. Для правильного выбора с экономической и практической точки зрения нужно сначала определить требования и состав к системе мониторинга, целью чего и явились результаты представляемого исследования [1].

Анализ источников с целью определения состава и требований к системе мониторинга информационной безопасности ОМТИ показал. Мониторинг и управление объектами осуществляются при помощи стандартных средств сетевого управления (Web, SSH, Telnet, консольный порт, а также SNMP), SMS-сообщений и e-mail в следующих режимах: ручной мониторинг - пользователь регулярно подключается к устройству регистрации и/или специализированному серверу и проверяет состояние входных данных; регулярный мониторинг по расписанию - сервер системы регулярно в соответствии с заданным расписанием проверяет состояние информационных служб и объектов контроллеров. При достижении минимально или максимально допустимых значений пороговых или других заданных величин запускает соответствующие сценарии обработки; мониторинг событий, формируемых интеллектуальными сенсорами и их сетями - реализуется объектовым оборудованием и информационными системами и доставляемых на сервер системы в асинхронном режиме, где события обрабатываются в соответствии с их приоритетом и значимостью; проактивный мониторинг - реализуется путем формирования прогнозных оценок по рискам на основе анализа всех доступных потоков данных и их аналитики, баз знаний и лучших практик с целью предотвращения вероятных критических событий.

Сбор информации от датчиков и управление технологическим оборудованием на объектах должны, в общем случае, базироваться на сравнительно простых и гибких технических вариантах построения системы, включая распределение датчиков и контроллеров в пределах технологической площадки, совместное использование продуктов различных производителей.

Исходя из приведенного выше каждая система мониторинга, работающая в различных режимах, будет иметь различные требования к системе. Но можно выделить общие требования для всех режимов работы системы мониторинга информационной безопасности: Система не должна быть избыточна. Системы мониторинга обрабатывают огромное количество информации, поэтому избыточность является одним из важнейших факторов системы. Работа в реальном масштабе времени. Неотъемлемая часть мониторинга, особенно в рамках управления информационной безопасностью, - это работа в реальном масштабе времени, чтобы реагировать на все инциденты безопасности. Своевременность реагирования играет решающую роль в данной системе в рамках информационной безопасности, потому что любые задержки могут сказаться на последствиях атаки или инцидента безопасности для предприятия, объекта или ОМТИ в целом. Дружественный интерфейс. Система мониторинга также должна сводить к минимуму вероятность ошибок в результате человеческого фактора. Для этого интерфейс, посредством которого пользователь или оператор

работает с данной системой, должен быть максимально понятен и позволять охватывать всю систему в целом. Интеллектуальная поддержка оператора. При принятии решения в критической ситуации операторам свойственно совершать ошибки, так как время на принятие решение сильно ограничено и нет возможности оценить состояние ситуации объективно и полно. Для этого и нужна система интеллектуальной поддержки оператора при мониторинге обстановки, которая должна, выполнив ряд вариантных оценок, представлять несколько вариантов принятия решений в конкретной ситуации. Это позволит как уменьшить время принятия решения, так и свести ошибки принятия решения оператора к минимуму [1, 2].

В результате изучения источников был сделан вывод, что для качественного функционирования системы мониторинга требуется следующий минимальный структурный состав:

- устройства сбора информации с первичных датчиков (сенсоров) состояния объектов мониторинга, включая средства коммутации потоков данных (управляемые и неуправляемые);
- локальная вычислительная сеть, например, для предприятия, на (250...300) АРМ с серверами хранения и обработки данных группы объектов с общим числом порядка 10;
- регистраторы событий различного вида сообщений, аудио- и видеоданных, включая стационарные и подвижные, с общим числом, например, для судна класса газовоз – порядка (2,5...3,5) тысяч. Для предприятия типа конструкторского бюро – порядка (1,5...2,0) тысяч;
- контроллеры управления устройствами систем жизнеобеспечения зданий и сооружений, контроля доступа в здания, сооружения, на территорию предприятия, видеонаблюдения, индикации и отображения состояния объектов, мониторинга групповых и индивидуальных рабочих мест пользователей;
- средства администрирования системы безопасности с установленным программным обеспечением процесса администрирования Службы безопасности и системы разграничения доступа к оборудованию и информационным ресурсам системы;
- средства хранения и доступа к базам данных информационных ресурсов Службы безопасности предприятия с достаточной емкостью памяти, производительностью, длительностью времени хранения архивов данных (истории событий) и обработки запросов пользователей на поиск и представление данных для принятия решений; имеющий достаточный объем памяти для длительного хранения данных мониторинга предприятия, а также производительность, обеспечивающую требуемую скорость обработки запросов пользователей;
- рабочие места операторов (АРМ) системы, обеспечивающие работу в локальной компьютерной сети предприятия с заданным уровнем доступа к оборудованию и средствам коллективного (группового) отображения информации, с общим числом сервисов – не менее 20;
- избыточность в системе в интересах обеспечения надежности с резервированием – порядка 2-3 при гарантированной непрерывности функционирования с минимальным временем останова вычислительных процессов («зависаний») – не более 10 мин/сутки;
- охват контуром автоматизации процессов функционирования ОМТИ – не менее 95% при охвате контуром интеллектуальной поддержки автоматизируемых процессов – не менее 70% (по отношению к общему числу действий (нажатий клавиши «Enter») оператора);
- минимальный цикл управления КБ, прежде всего, информационной – от 2 минут;
- дружелюбность интерфейса «АРМ-Оператор» - должен позволять оператору со средним уровнем подготовленности за счет всплывающих подсказок, аудио-комментариев, предупреждений и т.п. сигналов, самостоятельно освоить за 10 часов и безошибочно реализовывать требования Руководства оператора при объеме текстовой его части – не более 3-5 страниц.

Таким образом, результаты проведенного анализа позволяют перейти к следующей фазе обоснования архитектуры и функционала системы мониторинга обстановки, поддержки принятия решений и управления комплексной безопасностью, включая информационную, типового ОМТИ (СПРУ-КБ), инвариантную к специфике ОМТИ, – разработке и обоснованию технических решений по реализации данных требований, их опытной отработке и внедрению.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А.В., Тюрин И.С. Технология и программный комплекс мониторинга и управления защищенностью информационных ресурсов предприятия / Информационная безопасность регионов России (ИБРР-2015). IX Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30 октября 2015 г.: Материалы конференции / СПОИСУ. – СПб., 2015, с. 258 – 259.
2. Тюрин И.С. Система поддержки принятия решений и управления администратором Центра освоения технологий информационного противоборства СПбГМТУ: Выпускная квалификационная работа – СПб.: СПбГМТУ, 2016. – 112 с.

УДК 004.8

**ИНТЕЛЛЕКТУАЛЬНАЯ ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ АДМИНИСТРАТОРА ИБ
ТИПОВЫХ ОМТИ**

Тюрин Иван Сергеевич

Санкт-Петербургский государственный морской технический университет,
Россия, Санкт-Петербург, ул. Лоцманская, 3,
email: lefes123@gmail.com

Аннотация: Рассмотрена актуальность и типовое решение интеллектуальной системы поддержки принятия решений администратора информационной безопасности.

Ключевые слова: сложные системы; человеческий фактор; информационная безопасность; интеллектуальные системы; машинное обучение.

INTELLECTUAL SUPPORT FOR ADMINISTRATOR'S ACCEPTANCE OF TYPICAL OMS

Tiurin Ivan

State Marine Ttechnical University of St. Petersburg,
Russia, Saint-Petersburg, Lotsmanskaya Str. 3,
email: lefes123@gmail.com

Abstract: In the theses, the relevance and the standard solution of the intellectual decision support system of the information security administrator.

Keywords: complex systems, human factor, information security, intelligent systems, machine learning.

В настоящее время идет сильный рост популярности машинного обучения в контексте интеллектуальных систем. В связи с этим появилось огромное количество литературы, исследований, примеров и книг о том, как это происходит, зачем и каким способом это выполнять. Можно ли такие системы называть интеллектуальными, учитывая, что они принимают какие-либо решения на основе полученных данных в режиме обучения, то ответ конечно - да. Область информационной безопасности (ИБ) оказалась сильно «заинтересована» в данной технологии, так как именно в ИБ это нужно, как нигде. Огромное количество данных, большие, сложно структурированные, распределенные системы требуют постоянной интеллектуальной поддержки в их использовании и обслуживании. Особенно, при поддержке требуемого уровня безопасности систем. Высокая сложность способствует росту ошибок по вине «человеческого фактора», что может являться критическим для жизни всей системы в целом.

При управлении информационной безопасностью типовых ОМТИ перед администратором ИБ встает схожая проблема. Традиционная нехватка человеческих ресурсов вынуждает оператора исследовать только основные датчики (источники информации) о ситуации или инциденте, а также в краткие сроки на основе этих данных принимать критически важное решение, что влечет за собой ошибку или не оптимальное решение с большой долей вероятности.

В СПбГМТУ было выполнено исследование и разработана система интеллектуальной поддержки принятия решений администратора ИБ в базовом макетном варианте СПРУ-ИБ.1, которая позволяет охватить ряд источников информации и на основе руководящих документов рекомендовать одно или несколько решений по инциденту информационной безопасности для администратора ИБ. В настоящее время выполняется доработка СПРУ-ИБ.1 на предмет добавления таких интеллектуальных параметров как база данных вариантов решений (БД-Р) и автоматическое (самостоятельное) принятие решений в условиях отсутствия обратной связи с оператором СПРУ-ИБ. В этой связи расширен ряд критериев, на основе которых можно будет доработать и обучить систему интеллектуальной поддержки принятия решений. Основная сложность состоит в определении «самодостаточной» системы критериев, которых должно быть достаточно, чтобы принять или сформировать решение по инциденту информационной безопасности сети. Следующим этапом является формирование и наработка правильных, с точки зрения машинного обучения данных для вырабатывания интеллектуального параметра системы – БД-Р, на основе которой СПРУ-ИБ.2 будет принимать решение. На данном этапе также проблемным вопросом является формирование достаточных данных («нормы безопасности») для получения результата с точки зрения информационной безопасности типового ОМТИ.

Заключительным этапом формирования БД-Р будет являться обучения системы на основе полученных данных и вырабатывание отчета о проведенном обучении. Для это требуется организовать тестовые испытания, где будут как векторы атак и параметры из полученных ранее данных, так и новые для СПРУ-ИБ.2, чтобы подтвердить ее «интеллектуальную» составляющую в выработке и принятии решений.

Решение этих задач позволит доработать основной комплекс системы поддержки принятия решений информационной безопасности (СПРУ-ИБ.2) для включения в состав объекта информатизации (типового ОМТИ), в качестве которых могут быть использованы ранее

разработанные программно-аппаратные комплексы СОТМУ-ТЦ и СОТМУ-С, а также Центра освоения технологий информационного противоборства.

За интеллектуальными системами стоит будущее, но они не возможны без человеческого участия в виде разработки, корректировки, обучения этих систем. Их формирование и участие в деятельности человека неизбежны, так как человек (оператор ОМТИ, администратор ИБ ОМТИ) не может объективно и в краткие сроки оценивать состояние больших и распределенных организационно-технических и информационных систем. Выполненный анализ и обобщение достигнутых к настоящему времени результатов, обсуждение их со специалистами непременно будут этому способствовать.

СПИСОК ЛИТЕРАТУРЫ

1. Тюрин И.С. Система поддержки принятия решений и управления администратора Центра освоения технологий информационного противоборства СПбГМТУ: Выпускная квалификационная работа – СПб.: СПбГМТУ, 2016. – 112 с.
2. Алексеев А.В., Тюрин И.С. Анализ технологий мониторинга защищенности информационных ресурсов объектов морской техники и инфраструктуры / XIV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2014)». Санкт-Петербург, 29-31 октября 2014 г.: Материалы конференции. \ СПОИСУ. – СПб, 2014, с. 441 – 442.
3. Тюрин И.С., Алексеев А.В. Анализ технологии «10-strike» для решения задачи мониторинга безопасности информационных ресурсов объектов морской техники и инфраструктуры. Там же, с. 479 – 480.

УДК 004.05

АНАЛИЗ УЯЗВИМОСТЕЙ И СРАВНЕНИЕ МЕТОДОВ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ

Узбекова Юлия Шамилевна

Санкт-Петербургский государственный морской технический университет,
Россия, Санкт-Петербург, ул. Лоцманская, 3,
email: ayluy13mama@list.ru

Аннотация: В статье рассмотрены наиболее распространенные виды атак на веб-приложения и способы решения данной проблемы.

Ключевые слова: защита, уязвимость, взлом, безопасность.

VULNERABILITY ASSESSMENT AND COMPARISON OF METHODS OF PROTECTION OF WEB APPLICATIONS

Usbekova Julia

State Marine Technical University of St. Petersburg,
Russia, Saint-Petersburg, Lotsmanskaya Str. 3,
email: ayluy13mama@list.ru

Abstract: The article examines the most common types of attacks on web applications and ways to solve this problem.

Keywords: security, vulnerability, break-in, safety.

Введение. Современный мир нельзя представить без веб-приложений. Их применение широко распространено в науке, образовании, торговле, что безусловно приводит к возникновению желающих незаконно воспользоваться чужим трудом.

В этой связи ниже рассмотрена актуальная проблема обеспечения защиты веб-приложений от возможных уязвимостей и атак.

В настоящее время количество и виды атак на веб-приложения весьма велико. Наиболее распространенные из них – это SQL-инъекции, XSS-инъекции и file inclusion. Все они направлены на получение злоумышленником доступа к разного уровня информации вплоть до полного контроля над атакуемым сервером.

В известной литературе утверждается, что самой распространённой сегодня атакой является XSS-инъекция. Ей подвержены почти все веб-приложения.

В ходе анализа были исследованы методы защиты от вышеназванных атак. Каждый из них имеет свои особенности, но основным способом избежать данных угроз является тщательный анализ и фильтрация всех пришедших в запросах данных.

Исследуемые уязвимости являются одними из самых распространенных и встречаются практически во всех веб-приложениях. Поэтому умение определять наличие угроз является немаловажным фактором для владельца и работника.

Объём создаваемых технологий, которые позволяют обеспечивать требуемый уровень информационной безопасности, постоянно растёт, однако увеличивается и число методов их обхода. Также реализуются новые виды атак, которые часто малозаметны даже для опытных специалистов сферы защиты информации.

Технология безопасной разработки – это одна из современных методик обеспечения безопасности веб-приложений, которая позволяет выявить уязвимости на этапе его создания. Данная

процедура «обходится» владельцу намного дешевле, чем восстановление веб-приложения после проведенной на него атаки.

Межсетевой экран, как метод обеспечения информационной безопасности веб-приложений, используют уже давно. Данный элемент позволяет производить контроль и фильтрацию трафика, блокируя атаки в режиме реального времени.

Заключение. Взлом веб-приложений и защита веб-приложений – это действия не способные существовать отдельно друг от друга. Именно злоумышленники подвигают разработчиков на повышение уровня информационной безопасности. Если бы они постоянно не находили путей обхода, то рассматриваемая проблема была бы решена. Технологии постоянно совершенствуются, создавая все новые препятствия для злоумышленников. Но сколько бы их не создавалось, рано или поздно найдётся способ обхода. Поэтому так важно использовать самые современные средства обеспечения информационной безопасности.

Таким образом, исследования по данной теме позволяют подтвердить известную тенденцию: какой бы метод защиты не использовался, можно лишь на определенное время сократить риск взлома веб-приложений, избавиться же от данной проблемы окончательно, вероятно, нельзя, как подтверждается практикой. Именно поэтому тема анализа уязвимости и разработки методов защиты веб-приложений остается актуальной сегодня и будет актуальна, как можно полагать с учетом публикуемых данных, в будущем.

СПИСОК ЛИТЕРАТУРЫ

1. Низамутдинов М. Ф. Тактика защиты и нападения на Web-приложения – СПб.: БВХ, 2005 - 432 с.
3. Жуков Ю. В. Основы веб-хакинга. Нападение и защита (2-е изд.) – СПб.: Питер, 2012 – 206 с.



ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

УДК 378.126.018

МУЛЬТИМЕДИЙНЫЕ ТЕХНОЛОГИИ В СОХРАНЕНИИ КУЛЬТУРНОГО НАСЛЕДИЯ

Барабаш Павел Александрович¹, Ляшенко Татьяна Васильевна²

¹ Смольный институт Российской академии образования,
Россия, Санкт-Петербург, Полюстровский пр., 59,

² Художественно-технический институт,
Россия, Санкт-Петербург, пр. Культуры, 31,
email:ltv56@mail.ru, barabash_p@yahoo.com

Аннотация: В статье анализируются определяющие тенденции и проблемы использования мультимедиа технологий в сохранении культурного наследия. Рассматриваются основные понятия и сущностные характеристики мультимедийных технологий. Раскрываются роль и пути использования компьютерной графики в практике создания мультимедийных произведений.

Ключевые слова: компьютерная графика; мультимедиа технологии; культурное наследие; электронные издания.

MULTIMEDIA TECHNOLOGIES IN PRESERVATION OF CULTURAL HERITAGE

Pavel Barabash¹, Tatiana Lashenko²

¹Smolny Institute of the Russian Academy of Education,
Russia, St. Petersburg, Polyustrovsky ave., 59,

² Art and technical institute,
Russia, St. Petersburg, Culture ave. 31
email:ltv56@mail.ru, barabash_p@yahoo.com

Abstract: This article analyzes the defining tendencies and challenges associated with using multimedia technologies in preservation of cultural heritage. It discusses the basic concepts and inherent characteristics of multimedia technologies. This article also explores the role and usage of computer graphics in multimedia works.

Keywords: computer graphics; multimedia technology; cultural heritage; electronic editions.

Цифровые технологии обусловили бурное развитие такого феномена современной информационной цивилизации, как мультимедиа. Первоначально этот термин (от лат. *multum* «много» + *media* «среда»), первые упоминания о котором в зарубежных энциклопедических изданиях появились в 1970-х гг., обозначал совокупность средств для обработки и представления видео-, аудио- и печатной информации. Однако очень скоро были оценены, по сути, безграничные возможности, которые обеспечивал компьютер, оснащенный разными устройствами для работы с различного рода данными, когда видеоряды, текстовая и аудиоинформация, компьютерная графика и анимация могут быть произвольным образом скомпонованы, изменены и отображены в другой форме представления данных. Это открыло перспективы применения мультимедиа-компьютера в самых разных видах деятельности, прежде всего творческих, и обусловило появление одной из новых технологических форм информационного общества – технологии мультимедиа, которая открывает принципиально новый уровень обработки информации и интерактивного взаимодействия человека с компьютером. Таким образом, мультимедиа – это особый вид компьютерной технологии, который объединяет в себе как традиционную статическую визуальную информацию (текст, графику), так и динамическую – речь, музыку, видеофрагменты, анимацию и т.п. Поэтому мультимедийные технологии, позволившие объединить, а точнее – реально интегрировать возможности компьютерной, аудио-, видео- и телевизионной техники, разных информационных технологий, на сегодняшний день многими исследователями рассматриваются как приоритетные, в наибольшей степени отражающие специфику современной цифровой цивилизации и культуры, создающей новые формы социального взаимодействия, социальных коммуникаций, не подчиняющиеся законам какого-либо определенного государства, не ограниченные языком или социальными барьерами.

Интегративная природа мультимедиа, а также их все более расширяющееся технологическое применение в самых разных целях и сферах деятельности обуславливают смысловую

расплывчатость, неоднозначность и даже, можно сказать, «нетерминологичность» слова мультимедиа. Сам термин «мультимедиа» в том виде, как он представлен в отечественных исследованиях – своего рода миф. Его расплывчатость и неопределенность нередко приводит к теоретическим ошибкам и неправомерным выводам, в том числе и в научных текстах [1]. Различные специалисты трактуют это понятие по-разному, в частности, как: комплексное средство передачи информации; фундаментальная коммуникативная среда; технологии интеграции компьютерных и видеотехнологий, совокупность программных и аппаратных средств, ориентированных на обработку звука, видео, передачи тактильной информации (в перспективе) и т.д.

Действительно, мультимедиа может выступать и как технологии, реализующие возможности конвергенции информации разных типов, и как информационный продукт, созданный с использованием данных технологий, и как программное и аппаратное обеспечение, нацеленное на обработку и представление разнотипной информации, и даже как собирательное понятие для различных технологий, которые объединены в определенной программе каким-либо способом. В силу этого трудно дать полное и однозначное определение этому термину, однако можно говорить о тех или иных особенностях мультимедиа, определяющих специфику этого явления.

Для понимания сущности мультимедиа важно учитывать, что этот феномен самым непосредственным образом связан с так называемой экранной культурой – культурой подачи и восприятия информации с экрана, средством, позволившим задействовать в дополнение к традиционным статическим средствам передачи графики динамическую (а позже и звуковую) составляющую. Экранная культура, в свою очередь, является дальнейшим развитием книжной культуры, однако очевидно, что это совершенно новый и уникальный для своего времени тип культуры, возникший благодаря техническому прогрессу в сочетании с новыми идеями реализации данных им возможностей. Иными словами, возникновение этой культуры стало возможным, когда появились технические средства, позволяющие реализовать заложенные в ней возможности, но в то же время ее появление было вызвано необходимостью обеспечить взаимодействие людей с этими техническими средствами.

Важным условием формирования культуры мультимедиа следует считать возникновение компьютерной графики как средства технической реализации, позволяющего достичь решения целого ряда задач по гуманизации технической культуры. Уникальность компьютерной графики определяется тем, что, будучи ориентированной на функционирование в среде, имеющей имманентную текстовую природу, она позволила за счет поднятия на новый уровень абстракции описать явления и объекты, этой природе изначально чуждые. Компьютерная графика – это мост между миром чисел, преимущественно технических текстов и логики и миром чистого искусства (здесь речь идет именно о произведениях визуального искусства). В этом можно усмотреть определенный парадокс компьютерной графики, которая на сегодняшний день также стала элементом как технической, так и гуманитарно-эстетической культуры.

Компьютерная графика находится в постоянном развитии, что позволяет ей открывать новые грани искусства, создавать новые жанры, такие как трехмерная графика, фрактальная графика и т.д., важнейшими ее качествами являются массовость, быстрота реакции на требования, выдвигаемые жизнью. При этом специалистами, исследующими философские и культурологические аспекты компьютерной графики, отмечается, что с ней связаны существенные трансформации эстетических восприятий, так как «именно восприятие, а не артефакт, процесс, а не результат сотворчества, оказывается в центре теоретического интереса» – происходит «трансформация эстетических восприятий» [21]. Это обусловлено тем, что многим произведениям компьютерной графики, предназначенным для функционирования в цифровой, компьютерно-технической среде, свойственно такое явление, как интерактивность. Среда, которую формирует компьютерная графика, позволяет пользователю тесно взаимодействовать с ней, создавая новую реальность, в которую погружается взаимодействующий с этой средой субъект. Мысленная интерпретация реальности заменяется воздействием материальными, трансформирующими материальными, художественными объектами. Возникает понятие виртуального мира, воплощающего в себе «двойственный смысл, мнимость, кажимость и истинность» [4], погружаясь в который зритель начинает сам влиять на произведение, становясь как бы его неотъемлемой составляющей, и это погружение формирует новый тип эстетического сознания. Феномен виртуальной реальности в настоящее время изучается как самостоятельное явление, неотъемлемо интегрированное в культуру современного общества, хотя оценивается исследователями оно неоднозначно.

Наконец, в большой степени способствовало развитию мультимедиа появление гипертекстовой технологии, позволяющей представить текст в виде нелинейной иерархической структуры. Весь текст делится на фрагменты, и каждый видимый на экране компьютера фрагмент дополняется связями с другими фрагментами в виде ссылок или гиперссылок. Это позволяет уточнить информацию об изучаемом объекте и двигаться в разных направлениях, выбирая интересующие пользователя ссылки. Поэтому центральным понятием концепции гипертекста является понятие «навигация», которое означает управление процессом перемещения в информационном пространстве из узла отправления в некоторый узел прибытия.

Так или иначе, явление мультимедиа как соединение возможностей экранной культуры с интерактивностью и иными средствами манипулирования информацией открывает широкие возможности, которые могут быть использованы в самых разных целях. Это и возможность одновременного использования нескольких каналов восприятия, что позволяет усилить совокупное информационное воздействие; и возможность виртуализации и визуализации сложно воспроизводимых в реальных условиях процессов в силу их дороговизны, опасности, недоступности для непосредственного восприятия; и возможность визуализации абстрактных процессов путем наглядного их представления в виде разного рода моделей. Кроме того, мультимедиа сегодня постоянно находится в непрерывном развитии, приобретая новые черты, такие как возможность управления голосом и жестами, скоро, вероятно, можно будет говорить о предметно-тактильном управлении информацией и т.д.

Эти особенности дают основания для представлений о том, что мультимедиа – нечто большее, чем комплексное информационное средство и даже совокупность информационно-коммуникационных технологий. С этой точки зрения представляется правомерным говорить о том, что мультимедиа – форма художественного творчества новыми средствами или совокупность технологий и идей. Это форма синергетическая, синтезирующая в себе различные формы подачи информации, объединяющая в себе принципиально различные ее виды и дающая возможность интерактивного взаимодействия с ней, что позволяет более интенсивно вовлечь воспринимающего в процесс восприятия.

Визуальная и звуковая информация, помещенная в единое информационное пространство, не может оставаться простым эквивалентом исходного содержания: появляется эффект добавленного содержания от формы. Как подчеркивает О.В.Шлыкова, «дизайн мультимедиа объединяет выразительные средства пространственных и временных искусств, которые не просто взаимодействуют, оставаясь самостоятельными феноменами, но существуют неразрывно». Таким образом, графика, звук и иные выразительные средства составляют единый, гармонизированный интерфейс и контент мультимедийного продукта [4].

В современных условиях мультимедиа выступает как новое средство коммуникации, добавляя новые недоступные ранее возможности обмена информацией, что обуславливает темпы роста знания, обмена идеями и, в конечном итоге, темпы развития современного общества. Появляются новые типы сообществ – объединения людей вне географических и других границ, новые формы обмена идеями, новые формы контроля и учета информации. Меняются не только пространственные, но и временные представления людей, поскольку цифровая информация распространяется со скоростью света.

Культура, некоторым стихийным образом сложившаяся вокруг этого явления, в настоящее время успела получить значительное развитие и продолжает успешно развиваться, в соответствии с достижением новых уровней технического прогресса. Мультимедийная культура, по мнению Б.В. Светлова, представляет собой целостное единство материальных и духовных феноменов, причем совокупность первых связана с функционированием глобальных компьютерных сетей, систем мультимедиа, а совокупность вторых определяется понятием виртуальной реальности в ее более широком определении. Одной из ключевых ценностей данной культуры выступает эстетическая потребность. Сама мультимедийная культура есть среда функционирования эстетических потребностей и репрезентативная модель для их изучения: «Так как сущность эстетической потребности составляет потребность в гармонии, мультимедийная культура является очередной попыткой человечества (субъекта) установить гармонию с природой (окружающим объективным миром)» [3]. Мультимедийная культура призвана способствовать удовлетворению этой потребности в условиях современной массовой медиакультуры, для которой характерна фрагментация информации. Из этого выводится важная особенность мультимедийной культуры: ей свойственна компрессия эстетических ценностей в пространстве и времени. Такая компрессия предполагает адаптацию уже накопленного культурного багажа человечества к выразительным средствам этой культуры: создание различных произведений (фильмов, презентаций, интернет-порталов) по мотивам таких первоисточников является типичным примером подобной компрессии.

Поэтому вполне закономерно, что технологии мультимедиа становятся приоритетным направлением исследований по созданию мультимедийных продуктов, ориентированных на широкую аудиторию, и получают все большее распространение в культуре, искусстве, науке и образовании для сохранения их достижений.

В настоящее время в мире создано большое количество разнообразных мультимедийных произведений, которые могут применяться и активно применяются в культурологической практике разных стран: мультимедиа-справочники по музеям, городам, историческим памятникам, выдающимся деятелям и т.п. Многие страны мира стремятся «оцифровать» культурное наследие в целях его сохранения на основе широкого использования информационных и коммуникационных технологий, и прежде всего мультимедийных, которые предлагают новые перспективы и поразительные возможности для этого, подтверждая тем самым, что человечество находится на пороге новой информационной революции. В то же время сегодня в разных странах уровень информационно-технологической модернизации сферы культуры различен, что связано и с общим уровнем информатизации в стране, и

с национально-культурной спецификой, и способностью образовательных систем и учреждений готовить специалистов в области мультимедиа.

Собственно, поэтому производство мультимедийных продуктов со сложной функциональностью сегодня представляет собой интенсивно развивающийся сегмент, хотя он появился на рынке информационных технологий сравнительно недавно. На его появление и бурное развитие активно реагируют все рыночные субъекты: мировые компании – производители программного обеспечения и мультимедийного оборудования, предлагающие все более совершенные и функциональные средства создания этих продуктов; многочисленный и постоянно пополняющийся отряд предприятий профессионально, и не очень, занимающихся созданием мультимедиа- и Web-ресурсов; государство, выступающее в роли регулятора зарождающейся индустрии. Так, в нашей стране разработан Госстандарт (ГОСТ 7.83–2001 «Электронные издания. Основные виды и выходные сведения»), определяющий и упорядочивающий понятийный аппарат и терминологию новой информационной отрасли, и предприняты меры по государственной регистрации и охране прав создаваемой продукции.

Согласно этому стандарту, электронные издания, созданные с применением мультимедийных технологий, получили название мультимедийные электронные издания, под которыми понимается совокупность информации различной природы, присутствующей равноправно и взаимосвязано для решения определенных разработчиком задач, причем эта взаимосвязь обеспечивается соответствующими программными средствами.

Безусловно, речь идет об определенном классе мультимедийных информационных систем, мультимедиа приложениях, реализуемых по Web-CD технологиям. ГОСТ определяет и видовую структуру мультимедийных электронных изданий, подразделяя их на научные, научно-популярные, производственно-практические, учебные, справочные, досуговые, рекламные и художественные электронные издания. Для создания художественных электронных изданий, способных служить сохранению культурного наследия, требуются специалисты новой формации.

В соответствии с потребностями культурологической практики, а также с учетом уже полученных результатов, необходимо продолжить исследовательскую работу по таким актуальным для сохранения культурного наследия направлениям, как выявление этических и правовых аспектов создания и использования мультимедийных произведений, разработка мониторингового инструментария и критериев оценки качества электронных изданий, а также подготовка таких специалистов мультимедиа, как режиссеры, сценаристы, художники и писатели.

СПИСОК ЛИТЕРАТУРЫ

1. Деникин А.А. Мультимедиа и искусство: от мифов к реалиям: [Электронный документ] // «Художественная культура». - 2014. - N 3(12). - С.26-43. (<http://sias.ru/publications/magazines/kultura/2014-3/yazyki/843.html>).
2. Мультимедийные технологии в библиотечном образовании: монография / Т.В. Ляшенко. – СПб. : Изд-во РГПУ им. А.И.Герцена, 2010. – 304 с.
3. Светлов Б.В. Эстетические потребности личности в сфере мультимедийной культуры: автореф. дис. ... канд. филос. наук / Б.В. Светлов; Ин-т философии НАН РБ. – Минск, 2003. – 22 с.
4. Шлыкова О.В. Феномен мультимедиа = Multimedia Phenomenon: Технологии эпохи электронной культуры / О.В. Шлыкова; МГУКИ.– М., 2003. – 268 с.

УДК 004.05

МАНИПУЛИРОВАНИЕ СОЗНАНИЕМ В ХОДЕ ПРОЦЕССОВ «ЦВЕТНЫХ РЕВОЛЮЦИЙ»: СИСТЕМНЫЙ ПОДХОД

Борейко Андрей Андревич

Северо-Западный институт управления – филиал РАНХиГС

Россия, Санкт-Петербург, В.О., Средний пр. В.О., 57/43,

email: aarongungnir@mail.ru

Аннотация: В статье рассмотрен механизм манипулирования сознанием широких слоёв населения в ходе, так называемых, «цветных революций», который приводит к нестабильности политической системы и последующей смене политического режима. Теоретическими основаниями данного исследования являются уже ставшие «классическими» теории «Культурной гегемонии» А. Грамши, «Относительной депривации» Т. Гарра, «Политической системы» Д. Истона.

Ключевые слова: информационно-психологическая безопасность, манипулирование сознанием, «цветные революции», смена политического режима.

MANIPULATION WITH CONSCIOUSNESS IN THE "COLORED REVOLUTIONS": SYSTEM ANALYSIS APPROACH

Andrey Boreiko

The North-West Institute of Management, branch of RANEPA

Russia, Saint-Petersburg, Sredniy prospect, Vasilyevsky Island, 57/43

email: aarongungnir@mail.ru

Abstract: The article presents with the mechanism of manipulating the consciousness of the broad stratum of the population in the course of the so-called "color revolutions", which leads to instability of the political system and the subsequent change of the political regime. Theoretical grounds for this study are already the "classical" theories of A. Gramsci's Cultural hegemony, T. Garr's "Relative Deprivation", D. Easton's Political System.

Keywords: *information-psychological security, manipulation of consciousness, "color revolutions", the regime change.*

Введение. На сегодняшний день для ряда «цветные революции» являются реальной угрозой безопасности. Многие политические режимы, по разным причинам, подвержены риску внешнего вмешательства с целью из смены. Отельные приёмы дестабилизации «цветных революций» могут применяться не только на государственном, но и на региональном уровне.

Сами по себе «цветные революции» являются продуктом послевоенного времени: в условиях ограниченности применения военного инструментария по дестабилизации и дальнейшему демонтажу политических режимов резко возрос спрос на ненасильственные методы решения подобных задач. Некоторые крупнейшие акторы мирового политического поля прибегают к открытому применению силы лишь в крайних случаях, предпочитая формировать пространство вокруг себя по средствам «мягкой силы».

В ряде стран, в которых прошли процессы смены политических режимов, называемые «цветными революциями», отсутствовали ярко выраженные социально-экономические предпосылки для подобного рода событий. Данные факты заставляют исследователей обращаться к проблеме изучения природы «цветных революций» с новых позиций: структурных, функциональных, системных, - с целью поиска эффективных средств противодействия подобным угрозам.

В рамках данного исследования предложен системный подход применительно к изучению процессов смены политических режимов на постсоветском пространстве. Классический системный подход был предложен Дэвидом Истон в ряде его работ. Согласно его взглядам, политическая система представляет собой модель взаимодействия между социальной средой и политическими субъектами через обмен сигналами (информацией) и реакцией на эти сигналы. Модель «вход-выход» подразумевает наличие реакции/её отсутствия на требование социальной среды. Сама по себе модель взаимодействия является в определённой мере замкнутой: требование – реакция – реакция на реакцию или новое требование. Но на каждом ключевом этапе данные взаимодействия подвергаются влиянию внешней среды. В конечном счёте, они также определяют эти требования. «Цветная революция» по своей сути является результатом дестабилизации системы – её неспособности адекватно реагировать на импульсы социальной среды.

В рамках «цветных революций» ключевым моментом является формирование в социальной среде таких требований, которые: а) создают требования заведомо невыполнимые политическими субъектами; б) но воспринимаемые социальной средой как бескомпромиссные к исполнению.

Требований, которые в различных «цветных революциях» похожи друг на друга, несут на себе сильный отпечаток Западной политической и экономической модели. Здесь целесообразно вспомнить еще одну модель, предложенную Антонио Грамши, а именно теорию культурной гегемонии. Краткое её изложение: небольшой группе людей удастся успешно управлять большинством благодаря синтезу принуждения и согласия. Принуждение – это насилие в чистом виде. Но только за счет этого добиться подчинения невозможно. Общество необходимо убедить подчиняться, т.е. добиться его согласия на управление им. Согласие и есть гегемония управляющих. Достигается эта гегемония за счет распространения в умах большинства людей (населения) норм и ценностей – по сути своей, массовой культуры. В ходе «цветных революций» происходит разрушение существующего культурного ядра и его частичная подмена новыми нормами и ценностями. Именно они и формируют завышенные ожидания и повышенные требования к политическим институтам. Источником распространения новых культурных норм и ценностей являются средства массовой информации и особенно глобальная сеть Интернет.

Для понимания того, как завышенные ожидания конвертируются в политическое действие может быть использована теория относительной депривации, предложенная Тедом Гарром. Относительная депривация – это ценностный разрыв между имеемыми благами и их психологическим восприятием. Не так важно, что у вас есть на само деле, чем то, как вам это преподносится. В процессе искажения действительности – приукрашивании новых ценностей и ниспровержения старых, - ключевая роль отводится именно СМИ. В конечном счёте, относительная депривация приводит к недовольству и своим положениям и действующим политическим институтам, так как они не могут этого положения изменить. Как мы видели выше, сделать этого политические институты не могут по определению – это противоречит существующей культурной модели. Контр-элите необходимо лишь канализировать скопившуюся агрессию в политическое русло.

Заключение. «Цветные революции» являются гораздо более сложным феноменом, чем просто результатом пропагандистской деятельности. Они представляют из себя сложный многоуровневый

механизм по разрушению самих основ существования конкретного политического режима. Угроза «цветных революций» становится наиболее высокой для лимитрофных государств.

СПИСОК ЛИТЕРАТУРЫ

1. Гарт Т. Р. Почему люди бунтуют. – СПб.: Питер, 2005, 461 с.
2. Гоним В. Революция 2.0: Документальный роман / Пер. с англ. Т. Даниловой. – СПб.: Издательская группа «Лениздат», «Команда А», 2012. 352 с.
3. Грамши А. Избранные произведения: Т. 2. — М., Изд. иностранной литературы, 1957. 311 с.
4. Лафлэнд Дж. Техника государственного переворота//Оранжевые сети: от Белграда до Бишкека. Отв. ред. Н.А. Нарочницкая; [ред. и сост. Е.А.Бондарева]. – СПб.: Алетейя, 2008, С. 23-38.
5. Лиллекер Д. Политическая коммуникация. Ключевые концепты/ Пер. с англ. С.И.Остнек. – Х.: Изд-во «Гуманитарный Центр», 2010, 300 с.
6. Майерс Д. Социальная психология. — 7-е изд. — СПб.: Питер, 2010, 794 с.
7. Маклюэн Г.М. Понимание Медиа: Внешнее расширение человека / Пер. с англ. В. Николаева; Зал. Ст. М.Вавилова – М. Жуковский: «КАНОН-пресс-Ц», «Кучково поле», 2003, 464 с.
8. Манойло. А. Цветные революции и гибридные войны // Стратегия России [Электронный ресурс]. URL:http://sr.fondedin.ru/new/fullnews_arch_to.php?subaction=showfull&id=1435762375&archive=1438588795&start_from=&ucat=14& (дата обращения 13.12.2015)
9. Почепцов Георгий. Революция.ком. Основы протестной инженерии. – М.: «Европа», 2005, 532 с.
10. Урнов М.Ю. Эмоции в политическом поведении. – М.: Аспект Пресс, 2008, 240 с.
11. Helvey, R. L. On Strategic Nonviolent Conflict: Thinking About the Fundamentals [Электронный ресурс]. URL: <http://www.aeinstein.org/organizations/org/OSNC.pdf> (дата обращения 10.10. 2012).
12. Sharp G. From Dictatorship to Democracy. A Conceptual Framework of Liberation [Электронный ресурс]. URL: <http://www.aeinstein.org/organizations/org/FDTD.pdf> (дата обращения 10.10. 2012)
13. Easton D. An Approach to the Analysis of political Systems\ World Politics, Vol 9, № 3 (Apr. 1957), pp. 383-400.

УДК 007

ПРИМЕНЕНИЕ СЕТЕЦЕНТРИЧЕСКОЙ КОНЦЕПЦИИ УПРАВЛЕНИЯ В ЦИФРОВОМ ОБЩЕСТВЕ

Верзун Наталья Аркадьевна, Колбанев Михаил Олегович, Яковлев Сергей Алексеевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5,
emails: verzun.n@unecon.ru, mokolbanev@mail.ru, sayakovlev@list.ru

Аннотация: В докладе рассматриваются примеры деятельности цифрового общества, базирующиеся на использовании сетевцентрической концепции управления. Рассматривается модель и этапы цифрового земледелия, эффективная реализация которых на практике требует применения сетевцентрического подхода к организации деятельности: выращиванию растениеводческой продукции.

Ключевые слова: *сетевцентрический подход к управлению; цифровое общество; цифровое земледелие; информационная решетка; интеллектуальное сельское хозяйство.*

THE APPLICATION OF NETWORK-CENTRIC MANAGEMENT CONCEPT IN A DIGITAL SOCIETY

Verzun Natalya, Kolbanev Mikhail, Yakovlev Sergey
The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
emails: verzun.n@unecon.ru, mokolbanev@mail.ru, sayakovlev@list.ru

Abstract: The report discusses examples of digital companies based on the use of network-centric management concept. In particular, consider the model and the stages of digital agriculture, the effective implementation of which in practice requires the use of a network-centric approach to the organization of activities: farming of plant products.

Keywords: *network-centric approach to management; digital society; digital agriculture; information grid; intelligent agriculture.*

Инфраструктурной основой любой сетевцентрической деятельности в цифровом обществе являются инфокоммуникации, современный этап развития которых связывают с внедрением совокупности технологий третьей платформы информатизации. К ним относят несколько групп технологий (облачные и туманные вычисления; интернет вещей; большие данные; мобильный широкополосный доступ; наложенные сервисы) [1, 2]. Применение данных технологий значительно расширяет возможности использования информационных ресурсов в различных отраслях деятельности, повышая их эффективность [3, 4]. В докладе рассматриваются примеры деятельности цифрового общества, базирующиеся на использовании сетевцентрической концепции управления [5]. В частности, рассматривается модель и этапы цифрового земледелия (digital farming, digital agriculture), эффективная реализация которых на практике требует применения сетевцентрического подхода к организации деятельности: к выращиванию растениеводческой продукции.

Цифровое (точное) земледелие ориентировано на максимальное использование всех, задействованных в выращивании агрокультур ресурсов (земли, семян, воды, удобрений, сельскохозяйственной техники, топлива и пр.). Развитие точных систем – инновационное направление

в оздоровлении сельского хозяйства во всем мире [6]. Основная цель цифрового земледелия – получение максимального урожая при минимальных затратах ресурсов, что становится возможным благодаря организации агротехнических мероприятий в соответствии с реальными потребностями выращиваемых в данном месте культур [7].

Основными инструментами цифрового земледелия выступают мониторинг текущего состояния посевов и анализ многолетних данных. Наблюдение за посевами предполагает «накрытие» всей площади с посадками информационной решеткой (инфокоммуникационной сетью), которую составляют различные технические средства наблюдения: беспилотные летательные аппараты [8], искусственные спутники Земли, датчики, видеокамеры и пр. Информация, получаемая непрерывно в режиме реального времени от различных средств мониторинга сельскохозяйственной территории, составляющих информационную решетку, затем может использоваться «на местах» для управления исполнительными элементами, или доставляться в облако для дальнейшей обработки/анализа.

В случае использования «на местах»: децентрализовано, на основании полученных данных, принимаются решения по координации действий исполнительных устройств (систем полива, освещения, охраны, сельскохозяйственных роботов и машин) при проведении различных агротехнических операций: посев, полив, удобрение, рыхление, сбор урожая и пр.

Собранные данные используются не только «на местах», но и передаются «в облако», где происходит накопление, обработка, анализ информации, получаемой от средств мониторинга, «накрывающих» территорию многочисленных сельскохозяйственных угодий. По результатам манипуляций с данными можно планировать посев сельскохозяйственных культур; формировать стратегии ухода за ними; предсказывать распространение вредителей и болезней на ранних стадиях; создавать прогнозные карты урожайности, термограммы почвы и пр.

Внедрение цифровых технологий в сельское хозяйство (в частности, в земледелие) позволит сделать сельское хозяйство более технологичным, интеллектуальным, эффективным и устойчивым. Однако, для полного раскрытия потенциала цифрового сельского хозяйства необходимо: создание соответствующего правового поля и налаживания экономических стимулов, а также формирование развитой цифровой инфраструктуры. Последнее особенно сложно реализуемо в условиях сельской местности и существующей проблемы цифрового неравенства.

СПИСОК ЛИТЕРАТУРЫ

1. Максимцев И. А., Колбанёв М. О., Коршунов И. Л., Левкин И. М., Микадзе С. Ю. О технологических основаниях новой доктрины информационной безопасности Российской Федерации / Новые горизонты глобального мира: сб. науч. тр. / Балт. Гос. Техн. ун-т. СПб. – 2015. – С.270–281.
2. Верзун Н. А., Колбанёв М. О., Татарникова Т. М. Технологическая платформа четвертой промышленной революции / Геополитика и безопасность. – 2016. – № 2 (34). – С.73–78.
3. Верзун Н. А., Ипатов О. С., Колбанев М. О. Интернет вещей и информационно-технологическая безопасность / Технологии информационно-экономической безопасности: сб. статей сотр. каф. ИС и Т. – СПб.: Изд-во СПбГЭУ, 2016. – С.37–43.
4. Верзун Н. А., Колбанёв М. О., Омелян А. В. RFID-технологии для эффективности и безопасности документооборота / Технологии информационно-экономической безопасности: сб. статей сотр. каф. ИС и Т. – СПб.: Изд-во СПбГЭУ, 2016. – С.44–51.
5. Верзун Н. А., Ипатов О. С., Колбанёв М. О. О сетевых моделях цифровой экономики // Сборник: Информационные технологии цифровой экономики: сб. статей. – СПб.: Изд-во СПбГЭУ, 2017. – С.35–41.
6. Шилерова Е., Овчинников А. С., Балашова Н. Н. Использование принципов точного земледелия для управления бизнесом. Using the principles of the precision agriculture for a business management // Известия НВ АУК. 2015. №1 (37). – С.218–223.
7. Махотлова М. Ш. Технологии и основные направления точного земледелия // Символ науки. 2016. №1-3. – С.51–53.
8. Вырелкин А. Д., Выборнова А. И., Кучерявый А. Е. Исследование возможности применения БПЛА как мобильного шлюза летающей сенсорной сети для наземных автономных сенсорных сетей / Информационные технологии и телекоммуникации. 2016. Том 4. №1. С.29–36.

УДК 004.056.5

ЗАЩИТА ИНФОРМАЦИИ И ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Карташов Павел Николаевич

Санкт-Петербургский государственный экономический университет, кафедра информационных систем и технологий (ИСИТ),

Россия, 191023, Санкт-Петербург, улица Садовая, дом 21.

Вход в университет с набережной канала Грибоедова, дом 30/32.

torgul@bk.ru

Аннотация: С каждым годом всё большее количество информации сохраняется и обрабатывается в цифровом виде. Разнообразные «девайсы» и «гаджеты» стали неотъемлемой частью жизни большинства людей. Помимо рабочей или финансовой информации устройства стали нести в себе и огромное количество личных, конфиденциальных данных. В связи с этим активно развиваются различные программные и аппаратные средства защиты информации. А потому в системе человек-компьютер всё более уязвимым звеном становится не машина, а сам человек. В статье рассмотрены проблемы защиты информации, связанные именно с человеческим фактором.

Ключевые слова: защита информации; безопасность; социальная инженерия; человеческий фактор.

DATA PROTECTION AND THE HUMAN FACTOR

Kartashov Pavel

The St. Petersburg State Economical University
Russia, St. Petersburg, Sadovaya str. 21,
torgul@bk.ru

Abstract: From year to year more and more information is stored and processed in digital forms. A variety of "devices" and "gadgets" have become an integral part of most people's lives. Besides working or financial data, the devices now carry a huge amount of personal, confidential information. For that matter various software and hardware methods of information protection are actively developing. Therefore, in the human-computer system, the increasingly vulnerable component is not the machine, but the person himself. The article deals with the problems of data protection, in the context of the human factor.

Keywords: data protection; security; social engineering, human factor.

В современном мире информация является одним из ценнейших ресурсов. Утечка данных может привести к весьма печальным последствиям, начиная от крупных финансовых потерь и заканчивая человеческими жертвами. Согласно ISO/IEC 2382:2015 информационная система представляет собой систему, предназначенную для хранения, поиска и обработки информации, к которой также относятся организационные ресурсы (человеческие, технические, финансовые и т.д.), которые обеспечивают и распространяют информацию.

По мере развития технологий всё больше информации хранится и обрабатывается именно в электронном виде. Разнообразные «девайсы» и «гаджеты» могут иногда поведать о человеке больше, чем его окружение. Столь привычные и уже незаменимые в обычной жизни устройства сохраняют в себе фотографии, видеозаписи, переписки, рабочие документы, различную финансовую и прочую конфиденциальную информацию. Они как будто «впитывают» и несут в себе часть жизни своего владельца. А потому неудивительно, что эту оцифрованную информацию человек стремится защитить максимально надёжно. И со временем пользователю начинает казаться, что если он надёжно защитит свой компьютер (планшет, телефон, локальную сеть – неважно), то его информация будет в безопасности. Однако не стоит забывать, что в системе человек-компьютер уязвимым звеном всегда будет оставаться не машина, а сам человек.

При подготовке и обучении специалистов в информационной сфере, особое внимание надо уделять человеческому фактору и его роли в информационных системах. Так, предлагая своим студентам подготовить выступления по темам «угрозы информационной безопасности» и «методы защиты информации», я неоднократно сталкивался с тем, что наиболее подробно они рассматривали всю техническую сторону вопроса: системы контроля доступа, персональную идентификацию, ключи и шифрование данных, защиту сетей, программно-технические методы и т.д. Дыры в безопасности, связанные с человеческим фактором, обычно комментировались дежурной фразой «применять организационные методы защиты». Примеры подобных уязвимостей обычно приводились с трудом, не хватало понимания того, как через слабости человека пробивается брешь в информационной безопасности.

Если провести анализ известных случаев взломов и проникновений в защищённые информационные системы, то вы увидите, что большинство из них были связаны именно с человеческим фактором. Случаи умышленной кражи, порчи или уничтожения информации сотрудниками внутри своей организации мы сейчас рассматривать не будем. Такие проблемы чаще всего решаются на уровне подбора кадров и жёсткого разграничения доступа. Последствия же разбираются постфактум с привлечением ответственных за безопасность внутри организации, а также соответствующих служб органов внутренних дел.

Для нас интерес представляют ситуации, когда человек неумышленно оставляет «открытые двери» в информационной безопасности и не придаёт должного значения произошедшему с целью минимизации последствий. Как примеры можно упомянуть потерю рабочего пропуска или банковской карты без дальнейшей их блокировки, удаление или изменение какой-либо информации по неосторожности, оставление в доступных местах записанных паролей, ключей доступа, конфиденциальной информации и т.п.

В подобных случаях сотрудникам должна изначально по всем ключевым моментам разъясняться ситуация с личной ответственностью за информацию, с которой они работают. Должны быть составлены соответствующие инструкции. Необходимо проводить беседы и разъяснять порядок действий в той или иной ситуации для минимизации негативных последствий.

Отдельным пунктом стоит упомянуть случаи, когда злоумышленники проникают внутрь защищенной информационной системы, пользуясь обычными слабостями человеческого характера. Чаще всего это связано с тем, что на многие события люди реагируют автоматически, привычным для них способом. Об этом писал в своей книге «Психология влияния» Роберт Чалдини. Серьезно и

аналитически человек реагирует только на ту информацию, на которую у него есть время и желание, в остальных случаях реакция обычно идёт по типу «щёлк, зажужжало». Также у сотрудников, чья работа однообразна, утомительна и предполагает обработку большого количества информации, часто срабатывает рефлекс: позвонили и сказали, что надо сделать - делаем. В качестве примера подобных действий Роберт Чалдини упоминает эксперимент, проводившийся психологами, которые обзванивали медсестёр в больницах и, представившись врачом, давали распоряжение ввести смертельную дозу препарата пациенту. Медсёстры понимали, что делают, но в силу загруженности по работе и давления авторитета позвонившего, шли выполнять поставленную задачу. Останавливали их уже на входе в палату. Подобные методы воздействия получили название социальная инженерия.

Одним из родоначальников социальной инженерии был Кевин Митник, который в своей книге «Искусство обмана» прямым текстом говорит о том, что намного проще получить доступ, воздействуя на людей, чем пытаться взломать систему.

Задача с проникновением в чужую информационную систему намного упрощается, если провести предварительную разведку и заготовиться сведениями, находящимися в открытом доступе: имена сотрудников или знакомых (особенно руководства, друзей, родственников), номера телефонов, род занятий, увлечения и т.д. Всё это может быть использовано как для проникновения на объект, так и для последующего воздействия через телефон, смс, электронную почту и т.д.

Выбрав «жертву», злоумышленник попытается втереться в доверие, ссылаясь на доступную ему информацию. После чего он может уговорить или сообщить ему что-то, или же выполнить какие-то действия. Подобным образом сейчас работают мошенники, действующие через социальные сети или телефон, выманивая у доверчивых людей деньги.

Для проникновения в организации чаще всего используются рядовые сотрудники, которые хоть и не обладают высоким уровнем допуска, но могут открыть доступ к «следующей ступени». Полученные сведения собираются, анализируются и используются для воздействия на сотрудника более высокого ранга.

Для противодействия подобным мошенническим действиям необходимо регулярно проводить инструктажи сотрудников. Стоит разъяснить им, что информация, которую легко найти в открытом доступе, не может служить для авторизации.

Разрабатывая «организационные методы защиты информации», необходимо понимать, что, даже обнаружив какую-то угрозу и проинструктировав о ней сотрудников или просто близких вам людей, нельзя быть до конца уверенным, что эта информация останется навсегда усвоенной. Регулярные инструктажи по защите информации должны быть частью вашей системы безопасности наравне с программно-техническими методами.

СПИСОК ЛИТЕРАТУРЫ

1. Верзун Н.А., Колбанев М.О., Татарникова Т.М. Аспекты безопасности информационно-экономической деятельности // Технологии информационно-экономической безопасности: сб. статей сотр. каф. ИС и Т. – СПб.: Изд-во СПбГЭУ, 2016. – С.52–56.
2. Митник К. Д., Саймон В. Л. Искусство обмана. М.: Компания АйТи, 2004. 359 с.
3. Чалдини Р, Психология влияния. СПб: Питер, 2011. 304 с.

УДК 004.056, УДК 327

ОСОБЕННОСТИ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ В ИНТЕРНЕТЕ

Левкин Игорь Михайлович,¹ Науменко Ксения Андреевна², Виткова Лидия Андреевна³

¹Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Россия, 199178 Россия, Санкт-Петербург, Средний проспект В.О., 57/43

²Ленинградский государственный университет им. А.С. Пушкина, Россия, 196605, Санкт-Петербург. Пушкин, Петербургское шоссе, 10

³Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Россия, 193232, Санкт-Петербург, пр. Большевиков 22, emails: lev.kin@yandex.ru, ksn@glorystory.ru, iskinlidia@gmail.com

Аннотация: Влияние информационной среды, информационного окружения на общий психологический климат в отдельных микро- и макро- единицах неоспоримы. С ростом уровня проникновения интернета и все более глубоким погружением человека в информационную среду, информационно-психологическое воздействие имеет максимально широкий охват. За последние 30 лет методики реализации скрытых информационно-психологических операций значительно эволюционировали и теперь информация способна оказать влияние на миллионы людей в максимально сжатые сроки. В связи с этим наблюдается острая необходимость как в выявлении различных элементов воздействия на информационно-психологическое поле государства, общества и личности, так и разработка способа своевременного реагирования на элементы воздействия, с целью проведения превентивных и защитных мероприятий.

Ключевые слова: информационно-психологическая безопасность, информационная безопасность, мониторинг, воздействие, распознавание

THE FEATURES OF INFORMATION-PSYCHOLOGICAL INFLUENCE ON THE INTERNET

Levkin Igor, Ksenia Naumenko¹, Lidia Vitkova²

¹Russian Academy of national economy and state service under the RF President, 199178, Russia, Saint-Petersburg, Sredniy prospect, Vasilyevsky Island, 57/43

²Leningrad state University n. a. A. S. Pushkin, Russia, Saint-Petersburg. Pushkin, Petersburg shosse, 10³. Federal State Budget-Financed Educational Institution of Higher Education The Bonch-Bruевич Saint - Petersburg State University of Telecommunications, Russia, Saint-Petersburg, Prospekt Bolsheviko, 22 – 1, emails: lev.kin@yandex.ru, ksn@glorystory.ru, lidia@glorystory.ru

Abstract: The influence of the information environment, information environment on the overall psychological climate in separate micro - and macro - units is undeniable. With the growing level of Internet penetration and the deeper the immersion of a person in the information environment, information-psychological influence has the broadest possible coverage. Over the past 30 years methods for the implementation of covert information and psychological operations has evolved considerably and now the information is able to influence millions of people in the shortest possible time. In this regard there is an urgent need to identify the different elements of influence on the information-psychological field of the state, society and personality, and a method for timely response to stimulation elements, with the purpose of carrying out preventive and protective measures.

Keywords: information-psychological security, information security, monitoring, impact, recognition

Введение. Информационно-психологическое воздействие на общий политический климат того или иного города и государства было известно со времен появления античных полюсов и даже ранее. Во времена античности непосредственное влияние оказывали философы, ораторы и политики. С появлением таких религий как, например, христианство, массовое влияние стало осуществляться непосредственно через священнослужителей. Но, даже при появлении средств массовой информации и телевидения, контроль информационной сферы на определенной территориальной единице был доступен и возможен. При этом использовались такие механизмы защиты как «ограничение», «цензура», «предоставление единообразной информации».

В условиях информационного общества роль информационно-психологического воздействия на социум существенно возросла. Это связано с высокими потенциальными возможностями современных телекоммуникационных систем, которые способны легко сформировать информационное поле требуемой направленности.

Одним из таких примеров является информационное поле вокруг событий 1980-х годов, война между Аргентиной и Великобританией за две британские территории в Южной Атлантике: Фолклендская война. В то время как официально в Великобритании цензура не была установлена, вся информации могла быть получена исключительно из одного источника, тем самым различные точки зрения и трактовка событий исключались. Другой случай, буквально через 10 лет, война в Персидском заливе. Здесь пресса контролировалась уже более основательно, руководство американской и британских армий предоставляли горы информации, но независимым репортерам не гарантировали защиту объединенных войск. Таким образом, при внешней видимости открытости были созданы условия, когда получить иную точку зрения независимым репортёрам было просто опасно для жизни. Более того, были назначены офицеры по связи с общественностью, функция которых заключалась в специальной подборке информационных материалов (включая видеосюжеты), которые считались наиболее «подходящими» для передачи представителям СМИ [1].

Современные методы информационно-психологического воздействия на целевую аудиторию с уверенностью можно назвать изощрёнными. Так, например, понятия «демократия», «права человека», «принципы гуманизма», «свобода слова» и даже «экология» являются все лишь предлогом для осуществления вмешательства во внутренние дела того или иного государства и даже осуществление прямых интервенций как с применением вооруженных сил, так и с помощью «мирных механизмов», и информационная война становится нашей ежедневной заботой.

Вместе с тем, погружение в информационное поле общества и государства обеспечивает возможность распознавания и идентификации провокационных информационных потоков, в том числе в социальных сетях. Это же является и одной из ключевых особенностей информационно-психологического противодействия в Интернете, так как эта сеть создана и остается, в первую очередь, всемирной объединенной сетью как для хранения информации, так и для ее передачи.

Обработка и идентификация данных полученных из социальных медиа источников требует алгоритмических и инфраструктурных решений, позволяющих учитывать специфику данных (характерный язык общения, возможность не раскрывать свою личность), а также их размерность. К примеру, база данных социальной сети Facebook содержит более 1 миллиарда пользовательских аккаунтов и более 100 миллиардов связей между ними. Каждый день пользователи добавляют более 200 миллионов фотографий и оставляют более 2 миллиардов комментариев к различным объектам

сети [2]. В этих условиях создаются технологии, которые позволяют эффективно селективировать информацию, необходимую для оценки состояния различных сфер общественной деятельности. Так, в настоящее время находятся на пике своего развития технологии "Социальная аналитика" и "Большие данные". В частности, исследованиями социальных данных активно занимаются университеты Карнеги-Меллон, Стэнфорд, Оксфорд, INRIA, а также компании Facebook, Google, Yahoo!, LinkedIn и многие другие. В России, например, в ИСП РАН для анализа социальных медиа был разработан ряд оригинальных методов, которые были объединены в технологию, получившую название TALISMAN. Данная технология изначально нацелена на работу с большими данными, и использует наиболее перспективные открытые решения из стека технологий Big Data: Apache Spark, GraphX, MLlib и др. [3, 4]. При этом, в условиях информационно-психологического противостояния наиболее важными характеристиками существующих систем мониторинга являются скорость и полнота. Сегодня необходимо строить и внедрять в процессы управления информационной безопасностью государства и общества, решения, превосходящие аналоги по обоим параметрам. Использование систем потоковой обработки больших данных позволяет достичь высокой скорости анализа и получать аналитические отчеты по объектам мониторинга в течение нескольких минут после публикации информации.

Заключение. Методы информационно-психологического воздействия на широкие круги населения в сети Интернет будут постоянно совершенствоваться. Это предполагает необходимость разработки эффективных способов вскрытия негативных информационных потоков.

СПИСОК ЛИТЕРАТУРЫ

1. Баришполец В.А. Области применения информационно- психологического воздействия/ В.А. Баришполец // Радиоэлектроника. Наносистемы. Информационные технологии. 2014. Т. 6. № 1. С. 52-79.
2. Говорова Н. В. Комплексная Арктическая политика ЕС. Аналитическая записка № 13, 2016 (№ 43)/ ФГБУН Институт Европы РАН
3. Коршунов А. Анализ социальных сетей: методы и приложения /Коршунов А., Белобородов И., Бузун Н., Аванесов В., Пастухов Р., Чихрадзе К., Козлов И., Гомзин А., Андрианов И., Сысоев А., Ипатов С., Филоненко И., Чуприна К., Турдаков Д., Кузнецов С.//Труды Института системного программирования РАН. 2014. Т. 26. № 1. С. 439-456.
4. Турдаков Д.Ю. Способ интеграции профилей пользователей онлайн-социальных сетей/ С.О. Бартунов, А.В. Коршунов, Д.Ю. Турдаков, Н.Н. Кузюрин, Парк Сеунг-таек, Рыу Вонхо, Ли Хыунгдонг // Тип: патент на изобретение Номер патента: 2469389, РФ, 2012г. Дата регистрации: 08.11.2011г. Номер заявки: 2011145077/08

УДК 005.33

ИНФОРМАЦИОННЫЙ ПОТЕНЦИАЛ СУБЪЕКТА РОССИЙСКОЙ ФЕДЕРАЦИИ И СИТУАЦИОННЫЙ ЦЕНТР КАК ИНСТРУМЕНТ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМ ПОТЕНЦИАЛОМ

Мальмберг Сергей Александрович

Северо-Западный институт управления — филиал РАНХиГС (Санкт-Петербург),

Россия, Санкт-Петербург, Средний проспект В.О., 57/43,

email: smalmberg@mail.ru

Аннотация: В статье рассмотрено понятие «Информационный потенциал субъекта Российской Федерации» как одного из важнейших факторов при государственном управлении и концепция «Ситуационный центр», направленная на поддержку принятия управленческих решений путем управления информационным потенциалом.

Ключевые слова: *информационный потенциал, ситуационный центр*

INFORMATION POTENTIAL OF THE FEDERAL SUBJECT OF RUSSIA AND THE SITUATION CENTER AS A TOOL FOR MANAGING INFORMATION POTENTIAL

Malmberg Sergei

North-West Institute of Management — branch of the Russian Presidential Academy of National Economy and Public Administration (Saint-Petersburg, Russian Federation),

Russia, Saint-Petersburg, Sredniy prospect, Vasilyevsky Island, 57/43,

email: smalmberg@mail.ru

Abstract: The article presents the concept of «Information potential of a federal subject of Russia» as one of the most important factors in public administration and the concept «Situation center» aimed at supporting the adoption of management decisions by managing the information potential.

Keywords: *information potential, situation center*

Введение. При описании текущего исторического периода развития общества ученые и специалисты используют термин «информационная эпоха» [1], понимая под этим доминирующую позицию информационных технологий в ежедневной трудовой и бытовой деятельности человека. Такое понимание вещей обуславливает проведение интенсивной политики информатизации всех сфер жизни общества. В Российской Федерации информатизация общества является частью государственной политики, реализуемой в рамках государственной программы «Информационное общество (2011–2020)» [2]. С целью координации проведения информатизации российского общества

для улучшения качества жизни и условий ведения предпринимательской деятельности, в соответствии с Постановлением Правительства Российской Федерации №735 от 26 августа 2013 года, учрежден совет по региональной информатизации [3].

Политика информатизации, направленная на все сферы жизни общества, приводит к тому, что при стратегическом планировании того или иного вида деятельности, отдельно необходимо учитывать ее информационную составляющую.

Рассмотрим данный фактор в контексте управления субъектом Российской Федерации.

Потенциал, как одно из базовых понятий экономической теории, позволяющий определить уровень социально-экономического развития [4], применяется и на региональном государственном уровне. Как правило, потенциал региона представляют, как совокупность следующих составляющих: финансового, природноресурсного, геополитического, производственного, инвестиционного, инновационного, трудового (кадрового) и культурного потенциалов, а также различных характеристик социального развития [5].

Однако события последних лет показывают, что наиболее активно взаимодействие на региональном, общегосударственном и парадипломатическом уровне происходит в информационном поле (информационном пространстве) [6], сформировавшемся в последние десятилетия в соответствии с упомянутой выше информационной эпохой. В настоящее время отсутствует единый взгляд на измерение возможностей субъекта России в информационном пространстве. Многие научные и массовые издания применяют для этого термин «информационный потенциал» [7].

С учетом принятых определений информационного потенциала [8], [9], информационный потенциал субъекта России можно определить, как способность удовлетворить информационные потребности общества посредством систематизированной и защищенной информации, проводить политику информатизации региона, организовать научную работу в части информатизации и информационной безопасности, влиять на внутреннее и внешнее информационное поле, отражать и предупреждать злонамеренные компьютерные воздействия на жизненно важные региональные объекты согласно сформированной федеральной политике в области информационной безопасности.

На основе изложенного можно сделать очевидный вывод: без наличия эффективных инструментов по управлению информационным потенциалом региона руководство региона не может проводить государственную политику по управлению регионом, по обеспечению безопасности и улучшению качества жизни граждан.

Любое управленческое решение должно быть предварено комплексным мониторингом всех составляющих потенциала региона и безопасности жизнедеятельности в регионе, получением данных аналитической обработки огромного массива информации о социально-экономических и хозяйственных показателях, актуальной информацией от силовых структур в части обеспечения безопасности в регионе. На основе полученных данных должен быть проведен многофакторный статический анализ с целью прогнозирования дальнейшего развития ситуации и предложены варианты управленческих решений с применением сценарного подхода дальнейшей реализации ситуации.

На выполнение такого функционала направлена концепция «Ситуационного центра» [10] в основе которой лежит ряд информационных систем, получающих и обрабатывающих информацию от силовых структур и исполнительных органов власти в режиме реального времени, на основе которой выполняется прогнозирование и рассматриваются варианты возможных решений и последствия их принятия. При этом полученная информация должна быть проверена на адекватность, точность и достоверность.

Для регионов, граничащих с иностранными государствами, в особенности со странами-членами НАТО, должен учитываться внешнеполитический фактор.

В своей ежедневной работе Ситуационный центр также использует протоколы обмена с Ситуационными центрами других субъектов федерации, а также с Ситуационным центром Президента России, правительства, полномочных представителей Президента в федеральных округах, объединенных в систему распределенных ситуационных центров. Взаимодействие между сотрудниками ситуационных центров, представителями федеральных и силовых структур проходит по защищенной правительственной системе видеоконференцсвязи.

В результате работы Ситуационного центра формируется аналитический материал, который направлен на поддержку принятия управленческих решений.

Заключение. Таким образом, Ситуационный центр дает возможность управлять информационным потенциалом субъекта Российской Федерации и как следствие позволяет руководству субъекта Российской Федерации наилучшим образом выполнять свои государственные полномочия.

СПИСОК ЛИТЕРАТУРЫ

1. Буряк В. В. «Глобальное гражданское общество и сетевые революции». / Виктор Буряк. — Симферополь: ДИАИПИ, 2011. — 152 с.
2. Государственная программа «Информационное общество» (2011–2020 годы) [Электронный ресурс]. - Режим доступа: <http://minsvyaz.ru/ru/activity/programs/1/> (дата обращения 26.08.2017).
3. Совет по региональной информатизации [Электронный ресурс]. - Режим доступа: <http://minsvyaz.ru/ru/activity/advisories/5/>

(дата обращения 26.08.2017).

4. Гацалова Л.Б., Парсиева Л.К. Современные механизмы регулирования региональной демографической политики в условиях экономической нестабильности // Современные проблемы науки и образования. – 2013. – № 5.
5. Дзобелова В.Б. Развитие финансово-кредитных отношений в малом бизнесе: диссертация ... кандидата экономических наук: 08.00.10 – Владикавказ, 2006. – 174 с.
6. Манойло А.В. Государственная информационная политика в особых условиях. - М.: МИФИ, 2003
7. Молчанов Н.А. Информационный потенциал зарубежных стран как источник угроз военной безопасности РФ // Военная мысль. 2008. № 10. С. 2-9.
8. Решение Совета глав правительств Содружества Независимых Государств от 4 июня 1999 года "О Концепции информационной безопасности государств-участников Содружества Независимых Государств в военной сфере"
9. Большая Энциклопедия Нефти и Газа [Электронный ресурс]. - Режим доступа: <https://www.ngpedia.ru/id297281p1.html> (дата обращения 26.08.2017).
10. Мельников А.С., Голованова Т.В., Кашин А.Г. Ситуационный центр Санкт-Петербурга: базовые технологии и возможности / Интернет и современное общество: Труды XI Всероссийской объединенной конференции (28-30 октября 2008 г., Санкт-Петербург) СПб.: Факультет филологии и искусств СПбГУ, 2008. – С. 165-167.

УДК 004.056:007.51

ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛА ОТ НАПАДЕНИЙ, ИСПОЛЬЗУЮЩИХ ТЕХНОЛОГИИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Солодяников Александр Владимирович¹, Сухостат Валентина Васильевна²,
Антонова Любовь Сергеевна³

^{1,3} ООО «Ассоциация специалистов по безопасности»,
Россия, 194100, Санкт-Петербург, ул. Катмировская, 7

² Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, 197101, Санкт-Петербург, Кронверкский проспект, 49,
emails: solod000@yandex.ru, suhostat@mail.ru, antonova.ls@mail.ru

Аннотация: Специфичность целенаправленных атак на оператора методами социальной инженерии требует усиленного внимания к обеспечению информационной безопасности (ИБ) современной организации. В статье рассмотрены методы защиты от нетехнических угроз для ИБ и развития компетентности сотрудников противостоять опасностям социальной инженерии.

Ключевые слова: социальная инженерия, информационная безопасность, тестирование на проникновение, обучение сотрудников.

ORGANIZATION OF EMPLOYEE PROTECTION FROM SOCIAL ENGINEERING ATTACKS

Solodyannikov Alexander¹, Sukhostat Valentina², Antonova Liubov³

^{1,3} "Association of security professionals" LLC,

Russia, 194100, St. Petersburg, Kantemirovskaya st., 7,

² Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics
Russia, 197101, St. Petersburg, Kronverkskiy pr., 49,
emails: solod000@yandex.ru, suhostat@mail.ru, antonova.ls@mail.ru

Abstract: Specificity of purposeful attacks on the operator by methods of social engineering requires increased attention to the information security (IS) of a modern organization. The methods of protection from non-technical threats for IS and development of competence of employee to resist the dangers of social engineering are considered in the article.

Keywords: social engineering, information security, penetration testing, employee training.

Введение. Потенциальной угрозой ИБ современной организации может быть проявление человеческого фактора. Поэтому важно своевременно усилить политику безопасности компании, учитывающую защиту от нападений, использующих технологии социальной инженерии. Далее описываются общие стратегии ослабления и нейтрализации методов несанкционированного доступа к информационной инфраструктуре предприятия на основе слабостей человеческого фактора.

Меры физической безопасности. Разработанные и внедренные четкие и сжатые политики безопасности требуют периодической проверки, чтобы определить состояние информирования о безопасности среди сотрудников с целью выявления и устранения потенциальных недостатков. Так, постоянное напоминание сотрудникам о реализации реальной угрозы в любое время наряду с всеобъемлющим охватом систем видеонаблюдения в сочетании с четко определенным периметром контролируемой зоны обуславливает обеспечение физической безопасности, закрывает доступ злоумышленников к ценным ресурсам компании.

Применение программных средств. В борьбе с социальной инженерией значимость приобретает и развертывание ряда защитных программных средств. При этом следует учитывать, что использование программных средств, с одной стороны, может быть эффективным в борьбе с некоторыми типами атак методами социальной инженерии, с другой, – может оказаться совершенно бесполезным при других видах атак.

Специальные меры по предотвращению нападений, использующих технологии социальной инженерии. Другие специальные меры могут оказаться очень эффективной стратегией предотвращения атак методами социальной инженерии. Подобные меры включают активный мониторинг, агрессивную аутентификацию и учет пользователей, использование целевых алгоритмов машинного обучения и анализа. Так после проверки системы, допустимо ее самообучение на способность различать законные и незаконные действия пользователя, несоответствие данных. Эффективность систем машинного и поведенческого обучения способствует обнаружению и предотвращению сложных атак методами социальной инженерии. Пример: целевой фишинг.

Таким образом, механизмы внутренней безопасности, а также другие решения безопасности могут служить мощным щитом защиты предприятий от атак методами социальной инженерии.

Постоянно меняющаяся динамика в современном ИТ-мире и разнообразный характер потенциальных угроз требует информирования о них и обучения управленческого и технического штата компаний, включая ведущих менеджеров и правление компании, технический и сервисный персонал, службу поддержки, службу безопасности, бизнес-менеджеров о текущих правилах и процедурах безопасности. Так как политика безопасности содержит процедуры и рекомендации, которые диктуют методы защиты данных и активов организации, то политики также должны быть защищены от несанкционированного доступа, который может помочь злоумышленникам получить представление о внутренней работе компании.

Применение компаний достаточных мер безопасности и уверенность в защите от нападения предопределяют поиск другого мнения об уровне обеспечения информационной безопасности своей организации. Для этого проводится тестирование на проникновение. Основная цель данного мероприятия заключается в установлении технических уязвимостей и слабых мест в сети, системах и приложениях. Значимым становится и тот факт, что многие фирмы наряду с тестированием на проникновение, определяют перспективы безопасности и предприимчивых сотрудников.

Наиболее эффективной стратегией смягчения последствий в сфере социальной инженерии является образование. С периодическим и систематическим обучением по вопросам безопасности и частым напоминанием о необходимости оставаться начеку и проявлять бдительность в отношении подозрительного поведения компании могут эффективно превратить свое слабое звено в сильное.

Формы организации и методы повышения квалификации и информирования сотрудников о разнообразных потенциальных угрозах ИБ организации.

Обучение на месте. Такая форма организации обучения заключается в создании условий для внутри корпоративного обучения, в подготовке кого-либо из сотрудников (или в приглашении внешнего тренера), который сможет проводить регулярное обучение навыкам безопасности для персонала компании.

Инtranет. Инtranет организации может быть применим в реализации программ повышения квалификации и информирования сотрудников по учебному пособию, размещенном в интрасети.

Скринсейверы. Заставки могут играть большую роль в повышении информирования о безопасности среди сотрудников, могут использоваться для отображения коротких напоминаний о сохранении пароля в безопасности, запрете на выезд, сообщении о подозрительном поведении соответствующим отделам и т.д.

Онлайн-курсы. Работодатели могут использовать один из многих онлайн-провайдеров для обучения безопасности. Доступные образовательные ресурсы интернета способствуют развитию знаний сотрудников о рисках, связанных с социальной инженерией.

Таким образом, наличие разнообразных методов обучения обуславливает повышение информирования о разнообразном характере потенциальных угроз социальной инженерии для ИБ предприятия. Следствием является адекватное осознание сотрудниками рисков, создаваемых атакующими. При этом работодатель автоматически получает преимущество в этой битве; у бизнеса меньше шансов пострадать от нападения из-за того, что их обученный персонал проявляет должную осмотрительность, чтобы защитить компанию.

Заключение. Многоуровневая программа защиты от разнообразного характера потенциальных угроз социальной инженерии для ИБ организации может быть эффективной в силу компетентности сотрудников понимать и признавать общие методы эксплуатации, используемые социальными инженерами. Поэтому современные организации должны тратить свое время и силы, чтобы убедиться, что их сотрудники защищены от нападений, использующих технологии социальной инженерии, предпринимая превентивные меры.

СПИСОК ЛИТЕРАТУРЫ

1. Гатчин Ю.А. Методика оценки защищенности оператора информационных систем в условиях деструктивных информационных воздействий / Ю.А. Гатчин, В.И. Поляков, В.В. Сухостат, Н.В. Малков // Вестник компьютерных и информационных технологий. 2015. №2 (128). С. 54-59.
2. Митник К. Искусство вторжения: Пер. с англ. — Семенова А.В. — М.: Компания АйТи, ДМК Пресс, 2005. — 280 стр.
3. Салем М., Хаммуде М. Defense Methods Against Social Engineering Attacks [Электронный ресурс] URL: https://www.researchgate.net/publication/319097404_Defense_Methods_Against_Social_Engineering_Attacks (дата обращения 19.09.2017)

УДК 004.056.53

ЧТО ТАКОЕ СОЦИАЛЬНЫЙ ИНЖИНИРИНГ

Хайруллов Артем Вадимович, Галлямова Миляуша Равильевна
Государственный университет морского и речного флота имени адмирала С.О. Макарова,
Россия, Санкт-Петербург, ул. Двинская, 5,
emails: 1516evro@mail.ru, Miljausha-18@mail.ru

Аннотация: В статье рассматривается социальная инженерия. Социальная инженерия в контексте информационной безопасности относится к психологическим манипуляциям людьми, для совершения ими действий, либо разглашения конфиденциальной информации. Применяется для сбора информации, мошенничества или доступа к системе, путем получения доверия у оппонента.

Ключевые слова: политика безопасности, информационная безопасность, социальный инжиниринг, социальный инженер, несанкционированный доступ.

WHAT IS SOCIAL ENGINEERING

Khairullov Artem, Gallyamova Milyausha
Admiral Makarov State University of Maritime and Inland Shipping,
Russia, St. Petersburg, Dvinskaya str. 5,
emails: 1516evro@mail.ru, Miljausha-18@mail.ru

Abstract: This article discusses a social engineering. Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access.

Keywords: security policy, information security, social engineering, social engineer, unauthorized access.

Введение. Область информационной безопасности является динамично развивающейся дисциплиной. Хотя эффективность мер безопасности для защиты конфиденциальной информации растет, люди остаются восприимчивыми к манипуляции и человеческий фактор остаётся самым слабым звеном.

При получении доступа к сети применяется один из самых популярных методов взлома, так называемый социальный инжиниринг, на который, уделяют меньше всего внимания. Социальный инжиниринг формируется на управлении человеком, используя его личные качества, для получения желаемых целей. Социальная инженерия - это самый тяжелый вид атаки, относительно защиты против него, потому что он не может быть защищен только аппаратным или программным обеспечением. Успешная защита требует эффективной информационной безопасности, начиная с политики безопасности и руководящих документов, заканчивая оценкой уязвимости.

Успех социальной инженерии зависит от способности злоумышленниками манипулировать жертвой в выполнении определенных действий или предоставления конфиденциальной информации. Сегодня социальная инженерия признана одной из величайших угроз безопасности, стоящих перед организациями. Социальное проектирование отличается от традиционного взлома, в том смысле, что атаки социальной инженерии не обязательно предполагают эксплуатацию программного обеспечения или систем. В случае успеха многие атаки социальной инженерии позволяют злоумышленникам получить законный, санкционированный доступ к конфиденциальной информации.

Социальная инженерия в контексте информационной безопасности, относится к психологической манипуляцией людьми, с целью сбора информации, мошенничества, или получения доступа к системе.

Социальный инжиниринг, совместно с техническими знаниями, используют для достижения следующих целей:

1. Сбор информации о потенциальной жертве.
2. Получение информации, необходимой для несанкционированного доступа.
3. Вынуждение объекта совершить необходимые социальному инженеру действия.
4. Атака социального инженера разделяется на три стадии подготовки:
5. Определение точной цели.
6. Сбор информации об объекте обработки.
7. Разработка плана действий, моральная подготовка/тренировка.

Основными причинами успешных реализаций атак социальных инженеров являются такие черты характера человека, как: страх, любопытство, жадность, превосходство, ввеликодушие и жалость, доверчивость, лень.

Теперь рассмотрим распространенные техники и виды атак, которыми пользуются социальные инженеры:

1. Претекстинг – эта техника использует преднамеренно продуманный сценарий, чтобы привлечь целевую жертву и сделать так, чтобы жертва дала информацию или выполнила действия, которые были бы вряд ли выполнены в обычных условиях.

2. Фишинг – это метод, который обманным путем получает конфиденциальную информацию, посылая массовые рассылки электронным письмом от имени популярных брендов, а также личных сообщений внутри различных сервисов. 2

3. Вишинг – данная техника использует поддельную IVR систему, чтобы воссоздать, законно звучащие, официальные звонки от банковских и других IVR систем.

4. Фаминг – перенаправление жертвы по ложному интернет-адресу.

5. Услуга за услугу – эта техника предполагает под собой звонок злоумышленника в организацию по корпоративному (внутреннему) телефону.

6. Троянский конь (троянская программа) – это вредоносная программа, которая используется для сбора информационных ресурсов, нарушения работы системы противника, либо доступа в саму систему.

7. "Дорожное яблоко" – данная техника использует физические носители и опирается на любопытство или жадность жертвы.

8. Сбор информации из открытых источников.

9. Обратный социальный инжиниринг. Это тот случай, когда жертва сама рассказывает социальному инженеру нужные ему данные. Многие люди для более быстрой работы или устранения неполадок, добровольно сообщают логины и пароли, а также другие конфиденциальные сведения.

10. Человеческий отказ в обслуживании.

11. Личный визуальный контакт.

12. Системы обмена мгновенными сообщениями (IM).

13. Анализ мусора.

14. Личностные подходы. Одна из самых простых методик социального инжиниринга. В данной технике используют четыре основных разновидности подхода: запугивание, убеждение, использование доверительных отношений, помощь.

Закключение. В результате мы видим, как важно защищать информационную безопасность со стороны психологии, так как самое слабое звено в системе – это человеческий фактор.

Полностью уберечь себя от атак социального инжиниринга практически невозможно, но можно соблюдать некоторые правила, благодаря которым можно добиться очень высоких результатов.

Основные рекомендации, которых стоит придерживаться любому сотруднику:

1. Постоянно изучать новые методы защиты информационной безопасности и не забывать повторять старые.

2. Проходить тренинги, которые будут повышать бдительность.

3. Соблюдать элементарные правила безопасности, несмотря ни на что.

4. Быть аккуратным и сосредоточенным.

5. Не доверять посторонним людям.

6. Не открывать конфиденциальную информацию по телефону или электронной почте, если это не прописано в политике безопасности.

7. Правильно обращаться с документами и физическими носителями, а также их устраниением.

8. Ответственно относиться к работе.

9. Важно помнить, что любое должностное лицо может стать жертвой социального инженера.

СПИСОК ЛИТЕРАТУРЫ

1. Социальное проектирование: концепции и решения [Электронный ресурс] http://www.infosectoday.com/Articles/Social_Engineering.htm#.WS20jKAzqoj (последнее обращение: 12.09.2017).
2. Социальная инженерия [Электронный ресурс] [https://en.wikipedia.org/wiki/Social_engineering_\(security\)](https://en.wikipedia.org/wiki/Social_engineering_(security)) (последнее обращение: 12.09.2017).
3. Социальная инженерия [Электронный ресурс] http://ru.wikipedia.org/wiki/Социальная_инженерия (последнее обращение: 11.09.2017).



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АРКТИЧЕСКОГО РЕГИОНА

УДК: 004.4

ПРИМЕНЕНИЕ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ РАБОТЫ ДОБЫВАЮЩИХ СКВАЖИН

Вирстюк Анастасия Юрьевна, Микшина Виктория Степановна
Сургутский государственный университет
emails: Nastua5.1991@mail.ru, mikshinavs@gmail.com

Аннотация: В статье рассмотрены существующие гидродинамические и промыслово-статистические модели, применяемые для анализа эффективности работы добывающих скважин, выделены проблемы их применения в современных условиях нефтедобычи и предложено создание адаптационных геолого-промысловых моделей, учитывающих современное состояние добывающих скважин.

Ключевые слова: добывающие скважины; эффективность; регрессия.

USING MATHEMATICAL MODELS IN THE ASSESMENT OF THE EFFICIENCY WORK OF OIL WELLS

Anastasiya Virstyuk, Viktoria Mikshina
Surgut State University
emails: Nastua5.1991@mail.ru, mikshinavs@gmail.com

Abstract: The article deals with current hydrodynamic and industrial statistical models for analyses of the efficiency work of oil wells. Also, problems of their using in the modern oil recovery are highlighted and it is proposed the creation of adaptive geological industrial models considering the modern state of oil wells.

Keywords: oil wells, efficiency, regression.

Введение. Финансовая устойчивость нефтегазодобывающего предприятия в значительной степени зависит от эффективного использования фонда добывающих и нагнетательных скважин.

Для определения эффективности их работы требуется изучение большого количества показателей: дебит, приемистость, обводненность продукции и т.п. Кроме того, по мере разработки месторождений появляется потребность в анализе трудноизвлекаемых запасов нефти, запасов с высокой степенью выработанности, профиля приемистости и притока скважин и т.п., что приводит к появлению новых параметров, характеризующих работу скважин. Вследствие анализа ограниченного количества показателей и отсутствия учета новых, существующие математические модели эффективности работы скважин недостаточно адекватно описывают реальное положение дел на месторождениях.

Промыслово-статистические и адаптационные модели. Для оценки и прогнозирования показателей разработки скважин (и как следствие эффективности их работы) были разработаны промыслово-статистические методы прогноза, применение которых очень важно особенно на поздних стадиях разработки месторождений.

На данный момент разработано более 40 промыслово-статистических методов прогноза показателей разработки. Разработанные методы описываются кривыми вытеснения.

Промыслово-статистические методы прогноза характеризуются оперативностью (экспрессностью), простотой; основываются на минимальном количестве исходных данных. Но с другой стороны, промыслово-статистические методы характеризуются рядом отрицательных черт. Во-первых, при применении экстраполяционных методов погрешность оценки показателей разработки возрастает с ростом промежутка экстраполяции. Во-вторых, на ранних стадиях разработки методы характеризуются низкой результативностью, так как показатели разработки не обладают необходимой долей стационарности (поэтому применение кривых вытеснения обоснованно только при обводненности более 50%). В-третьих, все кривые вытеснения получены эмпирическим путем на основе обобщения промысловых данных ограниченного количества месторождений, вследствие чего они могут быть не вполне корректны для месторождений (скважин), имеющих другие особенности работы. В-четвертых, для построения аппроксимационной зависимости выбирается ограниченный прямолинейный участок кривой, но не менее 5-6 и не более 10-12 точек. И, наконец, в – пятых, объективных критериев отбора характеристик не существует, расчет ведется как минимум по 3 зависимостям, по которым коэффициент детерминации наиболее близок к 1.

Поэтому в настоящее время всё большее внимание обращено на адаптационные геолого-промысловые модели (АГПМ), которые могут быть подобраны для скважин с любыми характеристиками и условиями работы. Благодаря этим моделям осуществляется анализ за короткий промежуток времени (в отличие от геолого-промысловых методов), поэтому экстраполяционная ошибка не накапливается. Но следует отметить, что даже для одного и того же параметра (к примеру, для нефтедобычи) уравнение регрессии, на основе которого и строятся АГПМ, может приобретать различный вид, так как пласты и скважины имеют различные эксплуатационные характеристики – обводненность более или менее 50%, однородность или неоднородность, малая или высокая вязкость нефти и т.д.

Таким образом, адаптационные геолого-промысловые модели являются очень трудоемкими, и их применение возможно и целесообразно в рамках программных средств, благодаря которым будет проводиться предварительный анализ геолого-технических параметров скважин и подбираться необходимая модель и соответствующее ей уравнение регрессии. Кроме того, АГПМ позволяют определить зависимость одного нефтепромыслового параметра от нескольких других, что является необходимым для комплексного анализа работы скважины, в частности, для определения эффективности работы, которая для нефтяных и нагнетательных скважин может складываться из различных характеристик (к примеру, распределение закачки по пластам, профиль приемистости и т.п.), а не только на основании дебита или приемистости.

Для оценки существующих промыслово-статистических и разрабатываемых адаптационных геолого-промысловых моделей был произведен следующий анализ. Для одной и той же скважины X с определенными соотношениями Q нефти (Q_n) и Q жидкости ($Q_{жид}$) сначала были построены две промыслово-статистические зависимости (по Камбарову и Сазонову).

В случае с АГПМ для анализа скважин с различными эксплуатационными характеристиками требуется разбить все исследуемые скважины на группы (провести так называемую классификацию) для того, чтобы подобрать определенный вид уравнения регрессии для каждой из них.

Для определения эффективности работы добывающей нефтяной скважины необходимо провести анализ дебита скважины и дополнительных показателей:

Геолого-физические: вязкость и плотность пластовой нефти, пластовая температура, содержание парафинов, пористость и проницаемость пласта, коэффициент вариации нефтенасыщенности, толщина пластов и пропластков, коэффициенты неоднородности, песчанистости и расчлененности пласта, относительные запасы нефти.

Технологические: темпы отбора жидкости, соотношение закачки и отбора жидкости, плотность сетки скважин и интерферирующие нагнетательные скважины, текущие запасы нефти на скважину.

Скважину X , рассматриваемую в качестве примера, можно определить к группе скважин с маловязкой нефтью и однородным объектом разработки. Вязкость пластовой нефти этой скважины составляет не более 5 МПа*с, комплексный коэффициент неоднородности не более 6.

Учитывая всё вышесказанное, можно определить уравнение множественной регрессии для скважин с маловязкой нефтью и однородным пластом: эффективность работы скважины в данном случае будет зависеть от вязкости нефти, толщины пропластков и комплексного коэффициента неоднородности.

Заключение. Оценка адекватности рассматриваемых моделей проводилась с помощью F -критерия Фишера. И в первом, и во втором случаях построенная регрессия является значимой, но при использовании адаптационной геолого-промысловой модели коэффициент детерминации составляет 99%, а для промыслово-статистических моделей порядка 95%. Соответственно анализ дополнительных показателей работы скважин позволяет дать более точную и правильную оценку эффективности работы добывающих скважин и соответствует современным условиям процесса нефтедобычи на месторождениях.

СПИСОК ЛИТЕРАТУРЫ

1. Григулецкий В.В. Обводнение месторождений - коренной вопрос современности российской нефтегазовой отрасли [Электронный ресурс] // Технологии ТЭК. 2007 URL: http://www.oilcapital.ru/edition/technik/archives/technik/technik_02_2007/108204/public/108222.shtml (дата обращения: 29.04.2017).
2. Гамилова Д.А., Буренина И.В. Управление фондом скважин на основе комплексной оценки эффективности их эксплуатации [Электронный ресурс] // Электронный научный журнал «Нефтегазовое дело». 2007. N1. URL: http://ogbus.ru/authors/Gamilova/Gamilova_1.pdf. (дата обращения: 21.04.2017).
3. Токарев М.А., Чинаров А.С. Статистические методы прогноза нефтеотдачи и оценки эффективности воздействия на пласт: учеб.пособие. Уфа: ООО «Монография», 2007.

УДК 004.02

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АРКТИЧЕСКОГО РЕГИОНА

Голубева Мария Геннадьевна, Абрамова Кристина Владимировна
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Россия, Санкт-Петербург, ул. Двинская, д 5/7
email: mariigolubeva@gmail.com, Kris410@yandex.ru

Аннотация: Стремительно развивающийся Арктический регион России и Северный Морской путь в частности из-за уникальности природно-климатических условий требует совершенствования имеющихся методов достижения информационной безопасности и возможности применения нестандартных решений.

Ключевые слова: Арктический шельф, информационная безопасность, развитие Арктики, каналы связи, прогнозы.

INFORMATION SECURITY IN THE ARCTIC REGION

Golubeva Maria, Abramova Kristina
Admiral Makarov State University of maritime and inland shipping
Russia, St. Petersburg, Dvinskaya str. 5/7,
email: Kris410@yandex.ru, mariigolubeva@gmail.com

Abstract: Rapidly developing Arctic region of Russia and The Northern Sea Route of Russia, due to the uniqueness of the natural and climate conditions, require improvements of existing methods of achieving information security and possibility of applying non-standard solutions.

Keywords: Arctic shelf, information security, development of Arctic, methods of connection, forecasts.

Введение. Исследования, произведенные на сегодняшний день, дают основание предполагать, что шельф арктических морей и его склон - место залегания богатейших месторождений, как энергоносителей (нефть, газ, конденсат, битум), так и множества других полезных ископаемых (от драгоценных и редкоземельных металлов до строительных материалов). Российская арктическая подводная часть представляет собой побережье арктических морей и большую часть шельфовых территорий России (в которые кроме арктических входят черноморский, азовский, балтийский, дальневосточный шельфы). Российский шельф составляет порядка 20% всего шельфа Мирового океана. Именно здесь, на шельфе и материковой части, находятся основные запасы полезных ископаемых в виде крупных месторождений, которые уже открыты или известны в качестве прогнозных ресурсов. И это не только нефть и газ, как принято считать, но и уголь, медно-никелевые руды, олово, редкие металлы и редкоземельные элементы, золото, платиноиды, вольфрам, хром, титан и многое другое, что необходимо сегодня для эффективного развития промышленности и сложных технологий.

В настоящее время Россия вступила в новую стадию освоения Арктики. На сегодняшний день в регионе открыто 594 месторождения нефти, 159 месторождений газа, 2 месторождения никеля и более 350 месторождений золота, а также крупные месторождения угля, черных, цветных, редких металлов, полиметаллов, радиоактивных элементов, алмазов, нерудного и химического сырья [1].

Наиболее рациональным способом доставки грузов и исследования месторождений шельфа являет Северный Морской Путь. Экстремальные условия региона ставят непростую задачу для достижения поставленных целей в обеспечении должного уровня безопасности, ведь большие перспективы России ставят перед ней не только вопрос о том, как правильно распорядиться имеющимися уже сейчас ресурсами, но и теми, что будут освоены в будущем. Арктика - настолько особый регион мира с экстремальными природно-климатическими условиями, с низким уровнем хозяйственного – очагового — освоения и, как следствие, удаленностью от промышленных центров и большой ресурсоемкостью хозяйственной деятельности, что для достижения поставленных целей требуются нестандартные решения.

В России разработана концепция информационной безопасности, включающая в себя множество направлений и методов. Её роль для арктических регионов подтверждается созданием системы освещения обстановки в Арктике. В частности, освещения обстановки в Арктическом бассейне вопросами совершенствования информационно-телекоммуникационных сетей и их развитием. Дальнейшее развитие этого направления необходимо для развёртывания наших сил и средств для решения ресурсных, экологических и прикладных задач в Арктическом регионе. Информационные методы обеспечения безопасности мореплавания характеризуются тем, что в них предметом деятельности является информация, сообщаемая посредством тех или иных материальных носителей, но не сами эти носители [2].

К информационным методам можно отнести следующие:

- Издание и использование навигационных и других морских карт, пособий и руководств для плавания, их поддержание на уровне современности;
- Передача и прием оперативной навигационной информации;
- Передача и прием гидрометеорологической информации;
- Передача и прием сообщений о бедствии, сообщений с сигналами срочности и безопасности;
- Применение различных видов сигнализации на море;
- Зрительное, слуховое, радиолокационное, радиотехническое, гидроакустическое наблюдение за
 - обстановкой;
 - Выполнение навигационных наблюдений, обработка и анализ их результатов;

- Лоцманская проводка;
- Применение систем управления движением судов (СУДС);
- Выполнение расчетов по остойчивости и непотопляемости судов и т.п.

Арктический бассейн является одной из баз для Российского Северного флота. Несомненно, российский военный флот является крупнейшим и сильнейшим флотом бассейна, но на данный момент он базируется только в западной части (Мурманск, Архангельск, Североморск...). По факту введение судов типа 'Иван Папанин' заказанных Министерством обороны РФ у Адмиралтейских верфей в 2016 году должно защитить национальные интересы России в центральной и восточной частях Арктики, участвовать в спасательных операциях. Но двух заказанных судов данного типа несомненно будет недостаточно для столь обширной территории [3].

Информационная безопасность связана с выполнением военных задач и задач гуманитарной сферы. Это касается обеих областей, так как первостепенной задачей является обеспечение безопасности плавания по Северному морскому пути. Необходимо налаживание надежных и безопасных каналов связи для передачи прогнозов погоды и ледовой обстановки.

Вся территория мирового океана поделена на 21 зону. Для каждой зоны выбрана страна координатор обеспечивающая безопасность мореплавания путем передачи навигационных и метеорологических сообщений через спутник. Страна-координатор поддерживает бесперебойную передачу такой информации всем судам в ее зоне. Для района Арктического шельфа это зоны XX и XXI [4].

К сожалению, на побережье, вблизи этих, зон находятся незначительное количество портов – городов в которых могут быть расположены станции обработки и приема информации (Тикси, Певек, Диксон...). Качество данной информации тоже может вызывать сомнение, ведь точность информации прямопропорционально зависит от плотности навигации, так как суда, являясь плавучими метеорологическими станциями, в свою очередь, передают такую информацию. Ледокольная проводка, а именно ее обеспечение, усовершенствование логистической базы, позволяющей ледоколам получать информацию о судах, нуждающихся в проводке и судах, терпящих бедствие, создание дополнительных Морских Спасательных Координационных центров (MRCC), локальных центров передачи навигационных и метеорологических сообщений NAVTEX (NAVigational TELeX 490kHz и 518kHz) являются первостепенными задачами на ближайшие 5 лет. Увеличение объемов судовождения в зоне Арктического шельфа даст резкий толчок к повышению уровня безопасности региона благодаря постоянной передаче сообщений непосредственно из этих зон и постоянного мониторинга погодных явлений территории [5].

Заключение. В настоящее время в связи с началом освоения арктических месторождений, развитием транзитного судоходства, ростом числа рейсов в Арктику, значение Арктического шельфа значительно возросло. Сейчас решается задача экономического развития Арктического региона при условии сохранения уникальной природы Арктики. Работа идет в разных направлениях: в сфере законодательного регулирования, развития инфраструктуры, совершенствования тарифного регулирования и организации плавания судов, повышения уровня информационной безопасности региона. Благодаря политике развития Арктики, строительству портов типа Сабетта, открытие новых месторождений газа типа 'Приразломная', освоение арктики продвигается вперед большими шагами.

СПИСОК ЛИТЕРАТУРЫ

1. Правовой статус Арктики- [Электронный ресурс]. URL: <http://www.zakon.kz/203585-pravovojj-status-arktiki.html>
2. Мальцев А.С., Вильский Г.Б., Шон Н.Т. Информационная безопасность судна // Состояние и совершенствование безопасности информационно-телекоммуникационных систем. Сборник научных трудов. – Николаев: НПИ, 2009.
3. Analysis of cyber security aspects in the maritime sector, ENISA-2011. / [Электронный ресурс]. URL: <https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1>
4. Канышев, В., Сергуни, А. Арктика на перекрестке геополитических интересов [Текст]: / В. Канышев, А. Сергуни // Мировая экономика и международные отношения. - 2010. - № 9.А.В.
5. А.В. Загорский. Военная безопасность в Арктике. [Текст]:/Арктический регион: Проблемы международного сотрудничества: Хрестоматия в 3 томах / Рос. совет по межд. делам [под общ. ред. И.С. Иванова].

УДК327+316 012+004

АЛЬТЕРНАТИВНАЯ КОНЦЕПЦИЯ СОЗДАНИЯ ИНТЕГРАЛЬНОЙ СИСТЕМЫ МОНИТОРИНГА ОБСТАНОВКИ В АРКТИКЕ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ

Зимин Николай Семенович¹, Митько Арсений Валерьевич²

¹Холдинг Компания «Ленинец», Россия, Санкт-Петербург, Днепропетровская ул., 9

²Арктическая Академия Наук, Россия, Санкт-Петербург, Искровский пр. 22-175
emails: arseny73@yandex.ru

Аннотация: В статье рассмотрены проблемы обеспечения информационной безопасности при ведении хозяйственной и иной деятельности в арктических регионах и основные направления их разрешения на основе реализации Доктрины информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. N 646), а также формирования единой системы управления Арктической зоной Российской Федерации с соответствующим центром управления. Это

соответствует динамике геополитической ситуации, определяющей необходимость экономического каркаса и соответствующего инфокоммуникационного каркаса единой системы связи и управления в условиях интенсивных процессов глобализации.

Ключевые слова: Информационная безопасность, центр управления, единая система связи и управления, геополитические факторы, глобализация.

ALTERNATIVE CONCEPTION OF INTEGRAL SYSTEM OF SITUATION MONITORING IN ARCTIC FOR SECURITY LIFE-SUPPORT PROVIDING

Zimin Nikolay¹, Mitko Arseniy

¹Holding Company "Leninets", Russia, St. Petersburg, Dnepropetrovskaya Str., 9

²Arctic Academy of Sciences, Russia, St. Petersburg, Iskrovsky Ave 22-175

emails: arseny73@yandex.ru

Abstract: The article presents problems of information security in Arctic providing in condition of different fields of activity and main directions of its decision on base of Doctrine of information security providing of Russian Federation (app.by RF Prezident 5 of Desember 2016 N 645) and so of forming of unite control system for arctic zone RF with correspondence control centre. It is corresponds to geo-policy situation dynamic, determining necessity of economic frame and corresponding infocommunication frame of control for intensive globalization process.

Keywords: Information security, control center, unit system of control and communication, geo-policy factor, globalization.

В последнее десятилетие на основании действующих федеральных документов - Стратегия национальной безопасности Российской Федерации до 2020 года, законы №ФЗ-16 «О транспортной безопасности», №ФЗ-35 «О противодействии терроризму», №ФЗ-261 «О морских портах в Российской Федерации...», Указ Президента РФ №1167 «О неотложных мерах по повышению борьбы с терроризмом», Постановление Правительства РФ №324 «Об утверждении Положения о федеральной системе защиты морского судоходства от незаконных актов, направленных против безопасности мореплавания» и др., различные ведомства самостоятельно и независимо друг от друга развивают автоматизированные системы мониторинга обстановки (АСМО) для обеспечения безопасности жизнедеятельности в рамках своего назначения. Вместе с тем, в соответствии с Концепцией формирования и развития единого информационного пространства Российской Федерации и соответствующих государственных информационных ресурсов, одобренной решением Президента РФ №Пр-1694, в основу государственной политики в рассматриваемой области должна быть положена интеграция информационных ресурсов различных ведомств, независимо от форм собственности. Отсутствие интеграции информации систем мониторинга обстановки различного ведомственного подчинения приводит к:

- дублированию различными министерствами и ведомствами работ по созданию элементов, комплексов и систем освещения обстановки;
- распылению государственных ресурсов, выделяемых из бюджета страны на работы по получению и управлению информацией об обстановке;
- низкой эффективности использования данных и снижению качества обслуживания потребителей информацией об обстановке.

Интегрирование информации ведомственных систем мониторинга обстановки наиболее целесообразно производить на региональном уровне, т.к., именно здесь они получают максимальный объем информации об обстановке и имеют возможность наиболее эффективно ее использовать, в связи с чем должны создаваться региональные интегральные автоматизированные системы мониторинга обстановки (РИАСМО) путем объединения информации ведомственных АСМО, совместно действующих в едином регионе.

Разработанная по поручению Правительства Российской Федерации №СИ-П7-2273 от 10.04.2010 концепция системы освещения обстановки в Арктическом регионе (СОО в Арктике) предусматривает ее создание путем интеграции существующих и перспективных средств освещения обстановки наземного, морского, воздушного и космического базирования, а также центров обработки и распределения информации различной ведомственной принадлежности, т.е. предлагается создать СОО в Арктике на принципах, заложенных в разрабатываемой в РФ с 2002 года Единой системе освещения надводной и подводной обстановки (ЕГСОНПО).

Основными концептуальными предложениями по СОО в Арктике являются:

- цель создания системы – формирование единого информационного пространства систем государственного и военного управления Российской Федерации путем интеграции информационных ресурсов, систем и средств мониторинга (освещения) обстановки различного ведомственного подчинения;
- назначение системы – обеспечение органов государственного и военного управления России обобщенными данными об обстановке и состоянии среды в масштабе, близком к реальному времени и данными о движениях надводных, подводных и воздушных целей;

– метод построения системы – интеграция ресурсов, существующих, создаваемых и развивающихся информационных систем различного ведомственного подчинения;

– организационная системообразующая структура – главный информационный центр (федеральный уровень) и информационные центры регионального уровня.

Таким образом, в соответствии с рассматриваемой концепцией СОО в Арктике должна содержать региональный информационный центр (РИЦ) сбора и обработки информации, связанный каналами обмена информацией с АСМО других ведомств, действующих в Арктическом регионе. В связи с этим, при практической реализации такой системы необходимо будет решить множество сложнейших, зачастую противоречивых, задач, таких как:

– определить общегосударственного (межведомственного) хозяина и эксплуатационщика СОО в Арктике, действующего одинаково ответственно в интересах всех заинтересованных ведомств, использующих информацию системы; этот вопрос применительно к ЕГСОНПО был решен путем поручения Военно-морскому флоту решения вопросов ее создания и эксплуатации, в связи с чем она фактически превратилась из Единой Государственной в ведомственную систему ВМФ;

– обеспечить сбор и обработку общей информации с максимальными точностями и минимальными задержками, присущими одному из участников интегральной СОО – береговой системе управления движением судов (СУДС) Росморречфлота, что потребует огромных капитальных вложений в модернизацию и замену средств технического наблюдения других ведомственных участников системы;

– обеспечить функционирование всех ведомственных АСМО с приоритетом интересов интегральной СОО, т.е. ведомственным структурам должны быть навязаны требования сверх необходимых каждой из них для выполнения своего назначения, вплоть до регламента ежедневного функционирования.

Предлагаемая нецентрализованная схема построения РИАСМО позволяет избежать всех указанных выше недостатков СОО в Арктике, при этом не нужен будет единый хозяин системы, а достаточно будет назначить государственный межведомственный орган научно-методического сопровождения согласованного развития ведомственных АСМО в рамках РИАСМО. Таким координирующим органом в каждом регионе может стать соответствующий филиал или институт Российской Академии Естественных Наук; применительно к Арктическому региону выполнение указанной функции может быть возложено на Арктическую Академию Наук.

Предлагаемый способ реализации РИАСМО был апробирован на практике при выполнении ОКР «Разработка и изготовление фрагмента регионального звена Федеральной интегрированной системы контроля надводной обстановки в территориальных водах и в 200-мильной экономической зоне РФ для Кольского залива» в рамках Федеральной целевой программы «Реструктуризация и конверсия ОПК» (1998-2001 гг.).

В существующих условиях эскалации террористической деятельности особое место среди задач обеспечения безопасности жизнедеятельности занимает задача предупреждения угроз террористического и криминального характера важным объектам инфраструктуры различных ведомств. Террористические и криминальные угрозы могут приводить к нарушениям функционирования объектов на длительный срок, к большим экономическим потерям и человеческим жертвам. За рубежом, наряду с силами проведения специальных операций, стремительными темпами развиваются технологии, позволяющие создавать роботизированные технические средства и, прежде всего, автономные необитаемые и необслуживаемые малоразмерные аппараты для решения задач специальных операций. В связи с этим, для обеспечения эффективной охраны важных объектов, необходимо в составе ведомственных АСМО предусматривать специальные локальные автоматизированные подсистемы контроля обстановки (АСКО), работающие прежде всего по малым и сверхмалым целям, таким как малое плавсредство, автомобиль, дельтаплан, пешеход, пловец и т.п.

СПИСОК ЛИТЕРАТУРЫ

1. Рябинин И.А. Надежность и безопасность сложных систем. СПб.: Политехника, 2000. –248с.
2. Применение общего логико-вероятностного метода для анализа технических, военных организационно-функциональных систем и вооруженного противоборства // Монография, научное издание / В.И. Поленин, И.А. Рябинин, С.К. Свирин, И.А. Гладкова. Под ред. А.С. Можаяева. – СПб: СПб-региональное отделение РАЕН, 2011.
3. Хряпин А.Л., Афанасьев В.А. Концептуальные основы стратегического сдерживания. – Военная мысль, № 1, 2005. С. 8-12.

УДК 621.396.9

ОЦЕНКА ВНУТРИСИСТЕМНОЙ ЭЛЕКТРОМАГНИТНОЙ СОВМЕСТИМОСТИ СЕТИ РАДИОСВЯЗИ С КОДОВЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ

Крячко Александр Федотович, Антонов Кирилл Валерьевич

Санкт-Петербургский государственный университет аэрокосмического приборостроения,

Россия, Санкт-Петербург, ул. Большая Морская 67, лит.А

e-mails: Kartovan@gmail.com, kaf21@guap.ru

Аннотация: Проанализирована и рассмотрена внутрисистемная электромагнитная совместимость сети радиосвязи с кодовым разделением каналов. Для решения поставленной задачи

оценили уровень приема пилот-сигнала в пределах зоны покрытия базовых станций, зоны обслуживания базовых станций и уровни сигналов в прямом и обратном каналах связи по критерию сигнал-шум.

Ключевые слова: Электромагнитная совместимость, радиосвязь, интерферирующий сигнал, соотношение сигнал-шум.

EVALUATION OF THE INTERNAL SYSTEM ELECTROMAGNETIC COMPATIBILITY OF THE RADIOCOMMUNICATION WITH CODE DIVISION MULTIPLE ACCESS

Kryachko Alexander, Antonov Kirill
Saint-Petersburg State University of Aerospace Instrumentation
Russia, St. Petersburg, Bolshaya Morskaya str. 67
e-mails: Kartovan@gmail.com, kaf21@guap.ru

Abstract: Intrasytem electromagnetic compatibility of a radio network with a code division multiple access were analyzed and considered. To solve this problem, we estimated the reception level of the pilot signal within the coverage area of the base stations, the service areas of the base stations, and the signal levels in the forward and reverse communication channels by the signal-to-noise criterion.

Keywords: Electromagnetic compatibility, radio communication, interfering signal, signal-to-noise ratio.

Несмотря на интенсивное развитие систем мобильной связи, значительное внимание уделяется разработкам и внедрению систем абонентского доступа для обслуживания труднодоступных районов. Сети сотовой связи с кодовым разделением каналов могут быть построены на основе односотовых кластеров, что позволяет достичь максимальной повторяемости частот и обеспечить высокую спектральную эффективность и пропускную способность.

Для определения зоны надежного действия систем фиксированного радиодоступа необходимо с достаточной степенью точности прогнозировать зоны покрытия отдельных базовых станций. При этом качество связи и связанный с ним тип используемых аппаратных средств требует оценки внутрисистемной электромагнитной совместимости. С этой целью требуется оценить энергетический потенциал радиолинии, основанный на применении статистического и дифракционного подходов.

В системе связи с кодовым разделением каналов для передачи информации по каналам множественного доступа, размещенным на одной несущей частоте, используют один передатчик базовой станции. Поэтому максимальное значение мощности передатчика базовой станции является фактором, ограничивающим размеры ячеек сети связи. Поэтому требуется проверка ограничения максимальной мощности передатчика базовой станции при заданной плотности трафика в зоне охвата сети.

Многолучевое распространение радиоволн ухудшает качество передачи информации вследствие межсимвольной интерференции и является причиной медленных и быстрых замираний сигнала. Анализ замираний необходим для оценки внутрисистемной электромагнитной совместимости и заданных характеристик качества связи.

Для решения поставленной задачи необходимо оценить уровень приема пилот-сигнала в пределах зоны покрытия базовых станций, зоны обслуживания базовых станций и уровни сигналов в прямом и обратном каналах связи по критерию сигнал-шум/

В обратном канале расчет мощности интерферирующих сигналов будем проводить с учетом абонентских станций, попадающих в зону помех сектора базовой станции, ограничений на потери по мощности в радиоканале, а также равенства средних потерь и медленных замираний на трассах распространения сигнала в прямом и обратном каналах:

СПИСОК ЛИТЕРАТУРЫ

1. Бабков В.Ю., Вознюк М.А., Михайлов П.А. Сети мобильной связи. Частотно-территориальное планирование. – М.: Горячая линия-Телеком, 2006. – 536 с.
2. Берлин А.Н. Цифровые сотовые системы связи. – М.: Эко-Трендз, 2007. – 296 с.

УДК 327+316.012+004

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АРКТИКЕ

Митько Валерий Брониславович
Ленинградское отделение ЦНИИ связи, Россия, Санкт-Петербург, Варшавская ул., 11
emails: vmitko@yandex.ru, vmitko@arcticas.ru

Аннотация: В статье рассмотрены проблемы обеспечения информационной безопасности при ведении хозяйственной и иной деятельности в арктических регионах и основные направления их разрешения на основе реализации Доктрины информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. N 646), а также формирования единой системы управления Арктической зоной Российской Федерации с соответствующим центром управления. Это соответствует динамике геополитической ситуации, определяющей необходимость экономического

каркаса и соответствующего инфокоммуникационного каркаса единой системы связи и управления в условиях интенсивных процессов глобализации.

Ключевые слова: Информационная безопасность, центр управления, единая система связи и управления, геополитические факторы, глобализация.

PROBLEMS OF INFORMATION SECURITY IN ARCTIC PROVIDING

Mitko Valery

The Leningradian Branch of communication CNIL, Russia, Saint-Petersburg, Varshavskaya st., 11

emails: vmitko@yandex.ru, vmitko@arcticas.ru

Abstract: The article presents problems of information security in Arctic providing in condition of different fields of activity and main directions of its decision on base of Doctrine of information security providing of Russian Federation (app. by RF Prezident 5 of Desember 2016 N 645) and so of forming of unite control system for arctic zone RF with correspondence control centre. It is corresponds to geo-policy situation dynamic, determining necessity of economic frame and corresponding infocommunication frame of control for intensive globalization process.

Keywords: Information security, control center, unit system of control and communication, geo-poliy factor, globalization.

Арктика является особым регионом. В течение многих лет Арктическая академия наук выступала с обоснованием выделения Арктического региона России в особый регион с системой управления более прочной и гибкой, чем в советские годы это определялось Госпланом и Директивами правящей партии. Можно утверждать, что многие оппоненты формирования такой структуры на федеральном уровне с соответствующим центром управления (ибо устойчивое развитие любого региона невозможно без единой системы управления с эффективно работающим центром, наделённым соответствующими полномочиями) отчасти имели основания для таких выводов. Возможно такие мнения основывались на реальных предпосылках недостаточно развитой транспортной и инфокоммуникационной системы, ведомственной разобщённости, неготовности компетенций руководителей регионов, входящих в этот макрорегион, но сегодняшние условия переформатирования мироустройства настолько стали зависеть от решения арктических проблем, что промедление в реализации арктической миссии России становится просто недопустимым. Именно это обусловило новую интерпретацию участия стран евразийского континента в формировании единого подхода к проекту века «один пояс-один путь», где роль России, а также многие мероприятия с участием этих стран в решении арктических евразийских проблем существенно повышается, о чём неоднократно свидетельствуют результаты встреч руководителей России и Китая. Исследования влияния основных факторов, в первую очередь геополитических, показывают, что существуют рычаги международного сотрудничества в обеспечении устойчивого развития Арктики и политическая воля российского руководства играет здесь преобладающую роль при любой системе управления. Это обуславливает необходимость формирования российского экономического, транспортного и инфокоммуникационного каркаса этого региона под единой системой управления, обеспечивающего его функционирование в повседневных условиях и в чрезвычайных ситуациях.

Доктрина информационной безопасности определяет национальные интересы Российской Федерации в информационной сфере как значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы, а информационная безопасность Российской Федерации - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Применительно к арктическому региону отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий, затрудняет формирование системы международной информационной безопасности, направленной на достижение стратегической стабильности и равноправного стратегического партнерства. Участниками системы обеспечения информационной безопасности являются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и

граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности.

Исследователи в этой области выделяют следующие группы проблем: проблемы гуманитарного характера, связанные с неправомерным использованием персональных данных граждан, вмешательством в частную жизнь, дезинформацией; проблемы экономического и правового характера, связанные с кражей, искажением коммерческой и финансовой информации, неправомерным использованием интеллектуальной собственности, промышленным шпионажем и информационными кампаниями, направленными на причинение имиджевого ущерба организациям; проблемы политического характера, связанные с информационными войнами, электронной разведкой, нацеленной на раскрытие государственной тайны, доступом к автоматическим системам управления критически важных объектов государства, искажением информации и дезинформацией руководителей различного уровня государственной власти. На стратегическом конгрессе «Интегрированное управление разработкой нефтегазоконденсатных месторождений» кампании Газпром нефть важность информационных потоков в системах разработки месторождений подчёркивалась их сравнением с кровеносной системой на основании скелета – экономики. Это значит, что, проблема информационной безопасности фактически охватывает все сферы общественной и государственной жизни, включая хозяйственную деятельность, затрагивает реализацию национальных интересов страны.

В тех же источниках подчёркивается, что в странах Арктического региона, а также других государствах, для которых представляет интерес территория Арктики, система информационной безопасности включает деятельность специализированных служб, направленную на защиту информационного пространства страны и проведение специальных операций против противника. В частности, в США киберкомандование (USCYBERCOM) было основано в 2009 году, его задачами являются защита военных сетей от кибератак, проведение собственных кибератак и операций, обеспечивающих свободу действий США и их союзников в киберпространстве и блокирующих аналогичные действия противника. Подобные структуры уже созданы в Китае, НАТО, в Эстонии. Министерство обороны Российской Федерации заявило о создании подобных кибервойск лишь к концу 2013 года.

Для решения проблемы информационной безопасности на международном уровне представляют интерес сведения о странах-источниках кибератак, которые регистрируются Deutsche Telekom. По итогам сентября 2013 года в Топ 15 на первом месте по количеству атак были США, на 5-м месте - Канада, на 7-м - Российская Федерация. Эти сведения позволяют характеризовать условно круг информационно-агрессивных государств мира.

Помимо представленных данных о позициях стран в мировом рейтинге информационной незащищенности и агрессивности показательными являются сведения о развитости информационно-коммуникационных технологий среди стран Арктического региона. Заметим, что развитость или отсталость страны по данному показателю не является прямым свидетельством уровня информационной безопасности, а лишь указывает на актуальность для государства и его готовность к использованию всего потенциала современных технологий.

В частности, можно обратиться к индексу сетевой готовности 2013 года (Networked Readiness Index), который рассчитывается Всемирным экономическим форумом с 2002 года. Данный индекс включает показатели состояния деловой и нормативно-правовой среды с точки зрения информационных технологий, инновационного потенциала, государственной позиции относительно развития информационных технологий, государственных затрат на их развитие и т.д. Примечательно, что большинство стран Арктического региона вошли в первую десятку, которую возглавляет Финляндия. Канада заняла 12-е место, Исландия - 17-е. Российская Федерация занимает 54-е место из 144, поднявшись по сравнению с 2012 годом на две позиции вверх.

Всё сказанное свидетельствует о необходимости интенсификации решения проблем информационной безопасности в Арктике и одним из важных направлений считать формирование единой инфокоммуникационной системы, обеспечивающей ситуационный центр «Арктика» в системе управления Арктической зоной РФ.

СПИСОК ЛИТЕРАТУРЫ

1. Рябинин И.А. Надежность и безопасность сложных систем. СПб.: Политехника, 2000. –248с.
2. Применение общего логико-вероятностного метода для анализа технических, военных организационно-функциональных систем и вооруженного противоборства // Монография, научное издание / В.И. Поленин, И.А. Рябинин, С.К. Свиригин, И.А. Гладкова. Под ред. А.С. Можаяева. – СПб: СПб-региональное отделение РАЕН, 2011.
3. Хряпин А.Л., Афанасьев В.А. Концептуальные основы стратегического сдерживания. – Военная мысль, № 1, 2005. С. 8-12.

УДК 327+316.012+004

МОДЕЛЬ ОЦЕНКИ СТРАТЕГИЧЕСКОЙ УСТОЙЧИВОСТИ ГОСУДАРСТВА В АРКТИКЕ

Поленин Владимир Иванович¹, Митько Валерий Брониславович²

¹ Арктическая академия наук, Россия, Санкт-Петербург, Искровский пр., 22-175

² Ленинградское отделение ЦНИИ связи, Россия, Санкт-Петербург, Варшавская ул., 11
emails: vmitko@yandex.ru, vmitko@arcticas.ru

Аннотация: В статье рассмотрены проблемы обеспечения информационной безопасности при ведении хозяйственной и иной деятельности в арктических регионах и основные направления их разрешения на основе реализации Доктрины информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. N 646), а также формирования единой системы управления Арктической зоной Российской Федерации с соответствующим центром управления. Это соответствует динамике геополитической ситуации, определяющей необходимость экономического каркаса и соответствующего инфокоммуникационного каркаса единой системы связи и управления в условиях интенсивных процессов глобализации и обеспечения информационной безопасности.

Ключевые слова: Информационная безопасность, центр управления, единая система связи и управления, геополитические факторы, глобализация.

MODEL OF STRATEGIC STATE SUSTAINABILITY IN ARCTIC EVALUATION

Polenin Vladimir¹, Mitko Valery²

¹Arctic Academy of Sciences, Russia, Saint-Petersburg, Iscrovsky av., 22-175

²Leningradian Branch of communication CNII, Russia, Saint-Petersburg, Varshavskaya st., 11
emails: vmitko@yandex.ru, vmitko@arcticas.ru

Abstract: The article presents problems of information security in Arctic providing in condition of different fields of activity and main directions of its decision on base of Doctrine of information security providing of Russian Federation (appr. by RF Prezident 5 of December 2016 N 645) and so of forming of unite control system for arctic zone RF with correspondence control centre. It is corresponds to geo-policy situation dynamic, determining necessity of economic frame and corresponding infocommunication frame of control for intensive globalization process and information security providing.

Keywords: Information security, control center, unit system of control and communication, geo-polity factor, globalization.

Часто в публикациях осуществляется подмена или отождествление понятия «стратегическая устойчивость государства» с понятием «стратегическая устойчивость военной организации государства». С военной организацией государства (ВОГ), как и всякой военной организацией, правомерно соотносить свойство «стойкость», т. е. в данном случае употреблять понятие «стойкость военной организации государства».

Неверная постановка задачи определяет появление многословных размытых соподчиненных определений, уводящих от сути проблемы. Вместе с тем, к этим определениям следует подходить со строгостью формализмов, характерных для инженерных приложений с ориентацией на системный подход, самый общий взгляд на суть проблемы.

В частности, в данном случае целесообразно воспользоваться формализмами технической системологии.

Под устойчивостью понимается способность системы сохранять свойства, необходимые для функционирования по своему назначению, определяемую различными совместными комбинациями ее свойств надежности, стойкости и живучести. В отношении устойчивости государства дополним это определение условиями либо отсутствия (предотвращения) вооруженной агрессии, либо ее успешного отражения с незначимыми потерями (ущербом).

Таким образом, в масштабах государства следует говорить о стратегической устойчивости самого государства, а не о стратегической устойчивости его военной организации, которая играет соподчиненную роль. Как упоминалось выше, в контексте стратегической устойчивости государства речь должна идти о стойкости ВОГ.

Под стойкостью ВОГ следует понимать показатели стратегического сдерживания: состав вооруженных сил, в т. ч. сил общего назначения и ядерных сил; их готовность к отражению возможных угроз; живучесть группировок вооруженных сил; эффективность вооруженных сил.

Формальная логико-вероятностная модель взаимосвязи перечисленных факторов и свойств системы (государства) представлена ниже.

Эта модель понимается следующим образом.

Модель надежности государства определяется уровнем его экономического могущества как фактора надежности существования и развития.

С одной стороны, при наличии фактора угрозы имеет место обеспечение безопасности государства путем осуществления внешнеполитической деятельности по предотвращению угрозы агрессии, а в случае неудачи этой деятельности – путем отражения агрессии на уровне, характеризуемом стойкостью ВОГ (левая часть схемы). Формально величину устойчивости государства можно определить как надежность сохранения и развития экономического могущества при условии либо предотвращения агрессии надлежащей внешнеполитической деятельностью, либо отражения непредотвращенной агрессии. С другой стороны, при не предотвращении агрессии или недостаточной стойкости ВОГ имеет место риск частичной или полной утраты экономического могущества.

В Федеральном законе РФ «О промышленной безопасности опасных производственных объектов», дано следующее определение: «ожидаемый ущерб (полный риск) – математическое ожидание величины ущерба от возможной аварии опасного производственного объекта (ОПО) за определенное время». Устойчивыми являются выражения типа: «приемлем риск потери, поражения, утраты и т.п. такого-то объема, доли, части объекта». Понятие риска употребляется также в отношении меры возможности ущерба определенного уровня, например, «высокий, средний, низкий, х-процентный уровень риска аварии». В дальнейшем понятие риска будет использоваться в смысле, определенном Федеральным законом, как математическое ожидание величины ущерба.

Таким образом, в масштабах государства устойчивость системы характеризует безопасность, а неустойчивость – риск, характеризующийся ожидаемым ущербом.

Эта модель устойчивости системы (государства) претендует на свойства необходимости и достаточности, а также на роли как описательно-объяснительную, так и конструктивно-методологическую, позволяющую решать поставленные задачи исследования теоретических и методологических аспектов оценки стратегической устойчивости государства в интересах ее совершенствования.

Так, модель позволяет формально определить три пути или способа обеспечения устойчивости и безопасности государства:

1. Самый дорогостоящий путь (способ) – полного учета внешних факторов и парирования угроз на уровне национальной безопасности

2. Путь (способ) неполного учета внешних факторов и частичного парирования угроз на уровне государственной безопасности

3. Путь (способ), ориентирующий на безусловность мирного сосуществования или успешность мероприятий по предотвращению угрозы вооруженной агрессии

В целом эти пути (способы) характеризуют стратегическую устойчивость государства:

– первый – по принципу национальной безопасности;

– второй – по принципу государственной безопасности, ориентирующемуся на период функционирования существующей политической системы государства;

– третий – по принципу государственной безопасности мелких государств, для которых никакие мероприятия по укреплению стойкости ВОГ не являются значимыми по отношению к окружающим странам, и потому бесполезны.

Реализация политики обеспечения стратегической стабильности государства на уровне национальной безопасности достигается как созданием стойкой военной организации государства, так и установлением государственной монополии на стратегические виды сырья, экономики и оборону, поскольку «невидимая рука рынка» видит в них лишь средства получения прибыли.

СПИСОК ЛИТЕРАТУРЫ

1. Рябинин И.А. Надежность и безопасность сложных систем. СПб.: Политехника, 2000. –248с.
2. Применение общего логико-вероятностного метода для анализа технических, военных организационно-функциональных систем и вооруженного противоборства // Монография, научное издание / В.И. Поленин, И.А. Рябинин, С.К. Свирин, И.А. Гладкова. Под ред. А.С. Можаяева. – СПб: СПб-региональное отделение РАЕН, 2011.
3. Хряпин А.Л., Афанасьев В.А. Концептуальные основы стратегического сдерживания. – Военная мысль, № 1, 2005. С. 8-12.

УДК 004.056

ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ И ЦЕЛОСТНОСТИ ДАННЫХ, ПЕРЕДАВАЕМЫХ БЕСПИЛОТНЫМИ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ В АРКТИЧЕСКОМ РЕГИОНЕ

Шкоркина Елена Николаевна, Александрова Елена Борисовна
Санкт-Петербургский политехнический университет Петра Великого,
Россия, Санкт-Петербург, ул. Политехническая, 29,
emails: elenashkorkina@gmail.com, elena.aleksandrova@ibks.ftk.spbstu.ru

Аннотация: В работе предложен новый подход к обеспечению конфиденциальности и целостности данных, передаваемых беспилотными летательными аппаратами в сетях FANET в климатических условиях Арктического региона. В его основе лежит использование парадигмы личностной криптографии совместно с авторст-алгоритмами. Предложено использование личностной схемы, содержащей в себе функцию шифрования совместно с подписью.

Ключевые слова: личностная криптография, личностная схема шифрования с подписью, аутсорсинг, самоорганизующиеся сети беспилотных летательных аппаратов

ENSURING THE PRIVACY AND INTEGRITY OF DATA TRANSMITTED BY UNMANNED AERIAL VEHICLES IN ARCTIC REGION

Shkorkina Elena, Alexandrova Elena
Peter the Great Saint-Petersburg Polytechnic University,
Russia, Saint-Petersburg, ul. Polytechnique, d. 29,
emails: elenashkorkina@gmail.com, elena.aleksandrova@ibks.ftk.spbstu.ru

Abstract: A new approach to ensuring the confidentiality and integrity of data transferred by unmanned aerial vehicles in FANET in Arctic region is proposed. It is based on the use of the identity-based cryptography paradigm in conjunction with outsourcing algorithms. An identity-based signcryption scheme is proposed, that simultaneously fulfils both functions of digital signature and public key encryption in a logically single step, and with a cost significantly lower than that required by the traditional signature and encryption approach.

Keywords: *identity-based cryptography, identity-based signcryption scheme, outsourcing, FANET*

Современный этап исследования Арктического региона невозможно представить без беспилотных летательных аппаратов (БПЛА). Еще пару лет назад их использование было невозможно ввиду неприспособленности к жестким арктическим погодным условиям. Низкие минусовые температуры повреждали электронику, а сильные ветра делали не под силу полет по заданному курсу. С тех пор все изменилось: фирмы-производители стали использовать точные навигационные системы с коррекцией GPS/ГЛОНАСС, а диапазон рабочих температур стал соответствовать суровым климатическим условиям Арктики.

На данный момент БПЛА в Арктике используются для мониторинга работы напорных нефтепроводов, навигации в арктических льдах, поисково-спасательных работ, картографирования, сбора метеорологических данных. Кроме того, осуществляется доставка грузов из городов на корабли, полярные станции и месторождения природных ископаемых. Такое применение БПЛА в Арктическом регионе крайне актуально в весенне-осенний период, когда отсутствует наземное сообщение, а также в случаях, когда использование вертолётной техники экономически невыгодно.

Эффективный мониторинг Арктического региона может быть осуществлен посредством самоорганизующихся сетей БПЛА (FANET, Flying Ad-Hoc Networks). Во время работы летательный аппарат получает фото или видео ледовой обстановки, метеорологические данные и т.д. Ввиду ограниченности встроенной памяти хранение большого количества полученных данных невозможно. В таком случае необходима удаленная выгрузка данных материалов на наземную станцию для хранения или оперативной обработки без нарушения их конфиденциальности и целостности. Кроме того, необходимо разделять материалы, полученные с разных летательных аппаратов.

Основным компонентом БПЛА является полетный контроллер, в состав которого входит вычислительный модуль. В зависимости от производителя в него может быть встроен процессор разрядностью 8, 16 или 32 бита. Однако все они имеют пониженное энергопотребление, и, как следствие, малые вычислительные возможности. Помимо этого, обеспечение криптографической защиты не должно отрицательно влиять на полетную функцию БПЛА. В таком случае сеть FANET можно рассматривать как одноранговую самоорганизующуюся сеть, объединяющую маломощные устройства. Для обеспечения конфиденциальности и целостности в такой сети необходимо применять малоресурсную криптографию.

Один из компонентов сети FANET представляет собой наземную станцию, которая не ограничена в энергопотреблении и имеет значительно большие по сравнению с БПЛА вычислительные возможности. Предлагается использовать ее не только как криптографический вычислительный сервер в аутсорс-протоколах, но и как доверенный орган в протоколах идентификационной (личностной) криптографии.

Парадигма личностной криптографии в сети FANET позволяет обеспечить конфиденциальность и целостность данных с помощью протоколов, совмещающих функциональность цифровой подписи и шифрования [1]. Затраты на выполнение такого протокола будут меньше, чем суммарные затраты на выполнение шифрования и подписи по отдельности. При этом личностная криптография позволяет отказаться от громоздкой для сети маломощных устройств инфраструктуры открытых ключей и перенести на наземную станцию вычисления, требуемые при генерации секретного ключа пользователя. В качестве идентификатора БПЛА можно использовать его имя в сети.

Для выполнения шифрования совместно с подписью маломощное устройство в соответствии с современными протоколами должно уметь не только эффективно выполнять операцию умножения точки эллиптической кривой на число, но и вычислять билинейное отображение. Снизить рабочие нагрузки вычислителей для данных операций можно с помощью аутсорс-протоколов, позволяющих передать вычисления на криптографический сервер наземной станции. Для операции умножения точки эллиптической кривой на число может быть адаптирован аутсорс-алгоритм возведения в степень [2], а для вычисления билинейного отображения один из соответствующих аутсорс-алгоритмов [3, 4].

Несмотря на все плюсы такого подхода, существенной проблемой является необходимость сохранить секрет в тайне от внешнего сервера. Кроме того, маломощное устройство должно иметь возможность проверить правильность значения, вычисленного внешним устройством. Первая проблема успешно решается на уровне самого аутсорс-алгоритма с помощью правильного разделения вычислительно сложной математической задачи на части. Для решения второй проблемы предлагается подписывать сообщения от серверов по протоколу неоспоримой подписи, адаптированному для этой задачи в работе [5].

Таким образом, с помощью предложенного подхода можно эффективно решить проблемы информационной безопасности, обеспечив конфиденциальность и целостность данных, полученных БПЛА в процессе выполнения задач, актуальных для Арктического региона.

СПИСОК ЛИТЕРАТУРЫ

1. Malone-Lee J. Identity-Based Signcryption //IACR Cryptology ePrint Archive. – 2002. – Т. 2002. – С. 98.
2. X. J. Lin, L. Sun, H. Qu, X. Zhang. New Approaches for Secure Outsourcing Algorithm for Modular//Cryptology ePrint Archive. – 2016. – №045.
3. Lin X. J., Qu H., Zhang X. New Efficient and Flexible Algorithms for Secure Outsourcing of Bilinear Pairings//Cryptology ePrint Archive. – 2016. – № 076.
4. O. Arabaci, M. S. Kiraz, I. Sertkaya, O. Uzunkol. More Efficient Secure Outsourcing Methods for Bilinear Maps//Cryptology ePrint Archive. – 2016. – №960.
5. Шкоркина Е.Н., Александрова Е.Б. Использование неоспоримой подписи для верификации аутсорс-сервера//Информатика и кибернетика (ComCon-2017): сборник докладов студенческой научной конференции Института компьютерных наук и технологий 3–8 апреля 2017 года. – СПб.: Изд-во Политехн. ун-та, 2017.



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭКОЛОГИИ

УДК 550.8

СОСТАВЛЕНИЕ ПРОСТРАНСТВЕННОЙ МОДЕЛИ И ПРОГНОЗНОЙ КАРТЫ УЧАСТКА ГУБА ДОЛГАЯ – ОЗЕРО БОЛЬШОЕ ТОРФЯНОЕ

Ахметшина Анастасия Борисовна
Санкт-Петербургский национальный исследовательский университет
Россия, Санкт-Петербург, Кронверкский проспект, 49,
email: nastya-demenkova@rambler.ru

Аннотация. В статье рассмотрены основы работы в программе QGIS. Разработана методика построения картографических изображений пространственных динамических моделей. Результатами работы является прогнозная карта восстановления растительности участка во времени.

Ключевые слова: моделирование; картография; пространственная модель; прогнозная карта.

COMPILATION OF THE SPATIAL MODEL AND THE FORECAST MAP OF THE SITE DOLGAYA – LAKE GREAT PEAT

Akhmetshina Anastasia
St. Petersburg National Research University information technology, mechanics and optics,
Russia, St. Petersburg, Kronverksky Prospect, 49,
email: nastya-demenkova@rambler.ru

Abstract. The article discusses the basics of work in the QGIS program. A technique for constructing cartographic images of spatial dynamic models has been developed. The result of the work is the forecast map of the restoration of the vegetation of the site in time.

Keywords: modeling; cartography; spatial model; forecast map.

Введение. Соловецкие острова являются ООПТ и требуется особый контроль за действующей нагрузкой на ландшафт. Целью работы является построение картографического изображения пространственной динамической модели. В ходе работы рассмотрен модельный участок и исходные таксономические описания. Представленные результаты исследования позволяют оценить видовой и количественный состав участка. С помощью QGIS была проведена работа по оцифровке карты участка и оценка антропогенного воздействия на участок.

Выводы:

- построено картографическое изображение пространственной динамической модели;
- с помощью GIS-технологий выявлено площадное соотношение участков;
- построено картографическое изображение пространственной динамической модели антропогенного воздействия на участок;
- построено картографическое изображение пространственной динамической модели восстановления растительности участка;
- построено картографическое изображение пространственной динамической модели через 10, 20 и 30 лет;
- рассчитаны площади восстановления во времени.

Исследование показало, что через 10 лет растительность участка восстановится на 35%, через 20 лет – на 80%, через 30 лет – на 88%.

СПИСОК ЛИТЕРАТУРЫ

1. Кобелева Н.В. Системная региональная диагностика природной среды: Учебное пособие. – СПб: Изд-во «Лема», 2010. – 38 с.;
2. GRASS-PROJECT. Geographic resource analysis support system. 2013. [Электронный ресурс]. URL: <http://grass.osgeo.org> (дата обращения: 30.04.2017).

УДК 504.03(021)

ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ АКВАТОРИИ РЕКИ НЕВЫ, СВЯЗАННАЯ С РАЗЛИВАМИ НЕФТЕПРОДУКТОВ

Биненко Виктор Иванович, Родионов Владимир Зенонович
Санкт-петербургский научно-исследовательский центр экологической безопасности РАН
Россия, Санкт-Петербург, Корпусная ул., 18
emails: vibinenko@mail.ru

Аннотация: В статье оценена частота нефтеразливов по отношению к числу нефтеналивных танкеров проходящих по реке Неве за период с 1999 по 2016 года. Выполнен забор и измерение концентрации следовых углеводородов в невоской воде на основе использования Фурье-спектрометра на волновом числе 2900см^{-1} и АН-2 на длине волны 3.42 мкм. Отдельные концентрации углеводородов после нефтеразливов в реке изменялись в пределах (0,35-0,04) мг/л, что в основном выше предельно допустимых концентраций 0,05 мг/л. Проведена оценка рисков и экологического ущерба от нефтеразливов на р. Неве.

Ключевые слова: нефтепродукты, концентрация, риск, экологический ущерб.

ECOLOGICAL SAFETY OF WATER AREA OF THE NEVA RIVER ASSOCIATED WITH OIL SPILLS

Binenko Victor, Rodionov Vladimir
Saint Petersburg scientific research center for ecological safety RAS,
Russia, Saint Petersburg, Korpusnaya st., 18
emails: vibinenko@mail.ru

Abstract: The article assesses the frequency of oil spills in relation to the number of oil tankers passing through the Neva river for the period 1999 to 2016. Performed sampling and concentration measurement of trace hydrocarbons in the Neva water usage-based Fourier transform spectrometer in the wave number 2900cm^{-1} and AN-2 at a wavelength of 3.42 microns. Individual concentrations of hydrocarbons after oil spills in the river varied (0.35-0.04) mg/l, which is largely above the maximum permissible concentrations of 0.05 mg/L. the evaluation of risks and environmental damage from oil spills on the Neva river.

Keywords: petroleum products, concentration, risk, environmental damage.

Введение. Проблема загрязнения Невы нефтепродуктами является актуальной, так как водозабор для водоснабжения города Санкт-Петербурга осуществляется с центральной части её акватории. На основе собранной статистики оценена частота нефтеразливов по отношению к числу нефтеналивных танкеров, проходящих по реке Неве за период с 1999 по 2016 года. По данным Комитета по природопользованию ежегодное количество разливов нефтепродуктов в акватории р. Невы и Финского залива колеблется от 27 до 220.

Все виды среднегодового сброса нефтепродуктов в водные объекты в период с 1999 по 2016 годы был в пределах от 300 т до 580т. Количество собранной нефтеводяной смеси за последние годы был в пределах от 30 до 60т.

Заключение. Выполнен забор и измерение концентрации следовых углеводородов в невоской воде на основе использования Фурье-спектрометра на волновом числе 2900см^{-1} и АН-2 на длине волны 3.42 мкм. Отдельные концентрации углеводородов в реке изменялись в пределах (0,35-0,04) мг/л, что выше предельно допустимых концентраций 0,05 мг/л. Проведена оценка рисков и экологического ущерба от нефтеразливов на р. Неве.

СПИСОК ЛИТЕРАТУРЫ

1. Биненко В.И., Берковиц А.В. Оценка риска аварийных разливов нефти в акваториях Финского залива и реки Невы Материалы 8-ой межд. конференции «Акватерра-2005» СПб., 14-16 июня 2005 г., 132-139.
2. Биненко В.И., Берковиц А.В. Экологические риски, связанные с транспортировкой углеводородов, и безопасность Балтийского моря. Проблемы безопасности и ЧС №3, 2006 83-96.
3. Биненко В.И., Донченко В.К., Растоскуев В.В. Риски и экологическая безопасность природно-хозяйственных систем Санкт-Петербурга, СПбГУ, 2012, 353 с.
4. Охрана окружающей среды: природопользование и обеспечение экологической безопасности в Санкт-Петербурге в 2016 году/ под ред. И. А. Григорьева, И. А. Серебряцкого-СПб: ООО «Сезам-принт» 2017. - 472с.

УДК 338.624.03

ВКЛАД МЕТАНА В ЗАГРЯЗНЕНИЕ АТМОСФЕРНОГО ВОЗДУХА НАД Г. САНКТ-ПЕТЕРБУРГОМ

Биненко Виктор Иванович¹, Северюхина Анастасия Сергеевна²

¹Санкт-петербургский научно-исследовательский центр экологической безопасности РАН,
Россия, 197110, Санкт-Петербург, Корпусная ул., 18

²ООО «ПетербургГаз»

Россия, 191180, Санкт-Петербург, ул. Гороховая 63/2 тел. +7(812)335 59 44
emails: vibinenko@mail.ru, stasynord@mail.ru

Аннотация: В статье рассмотрен вклад метана в загрязнение атмосферного воздуха над г. Санкт-Петербургом в результате эксплуатации газораспределительных сетей ООО «ПетербургГаз». Проведено сравнение фоновых концентраций CH_4 на ст. Териберка (1870+-30) млрд⁻¹, над г.С.Петербург (2060+-50) млрд⁻¹ и за городом (1950+-40) млрд⁻¹.

Ключевые слова: парниковые газы, метан, инцидент, риск, экологический ущерб

THE CONTRIBUTION OF METHANE IN AIR POLLUTION OVER THE CITY OF ST. PETERSBURG

Binenko, Victor¹, Severyukhina Anastasia²

¹Russia, Sankt-Petersburg, Sankt-Petersburg scientific research center for ecological safety RAS, Russia, 197110, St. Petersburg, Corpusnay str, 18

²ООО "Peterburggaz"

Russia, 191180, Sankt Petersburg, St. Gorokhovaya str., 63/2

emails: vibinenko@mail.ru, stasynord@mail.ru

Abstract: the article considers the contribution of methane in air pollution over the city of St. Petersburg in the operation of gas distribution networks, LLC "Peterburggaz". A comparison of the background concentrations of CH_4 at the station Teriberka (1870+- 30)bn-1, over the city of St. Petersburg (2060+- 50) bn-1i (1950+- 40)bn-1.

Keywords: greenhouse gases, methane, incident, risk, environmental damage

Введение. Парниковый эффект в атмосфере и, в частности. «остров тепла» над городом связаны с наличием малых газовых примесей, которые имеют полосы поглощения достаточной интенсивности в инфракрасной ИК-области электромагнитного спектра излучения. К ним относятся: водяной пар (H_2O), относительная концентрация которого в атмосфере по объёму может достигать 2 % и более /с увеличением температуры/, углекислый газ (CO_2), концентрация которого составляет около 0.04%, метан (CH_4) с концентрацией близкой к 2 млн⁻¹, и ряд других. При этом молекулы (CH_4) на порядки эффективнее поглощают ИК излучение, чем молекулы(CO_2).

Предприятие ООО «ПетербургГаз» по городу Санкт-Петербургу имеет 552 газорегуляторных пунктов и 7450,7 километров распределительных газопроводов. Основным загрязняющим веществом, выбрасываемым в атмосферный воздух при эксплуатации данного оборудования, является метан, чей вклад в загрязнение атмосферного воздуха над городом оценён на основе статистики инцидентов в 2015-2016 гг. в разных районах города, а с использованием программы «Эколог 3» выявлены направления рассеяния метана, выполнены расчёты возможных рисков инцидентов с природным газом по формуле Пуассона и экологического ущерба от них.

Заключение. Оказалось, что наиболее загрязненными районами города являются Кировский и Пушкинский, где отношение максимальных концентраций метана к ПДК 6,3 и 3,8 соответственно, но в целом средняя концентрация метана по городу не превышает установленный норматив и равен 0,03 $\text{C}_m/\text{ПДК}$, что составляет 1,53 мг/м³. За исследуемый период на газораспределительных трубопроводах города Санкт-Петербурга произошло в сумме 159 инцидента, которые повлекли за собой утечки природного газа объемом в 169 293,6 м³ или 111 056,6 тонн, а величина экологического ущерба, выплаченная предприятием, составила 466 165,8 тыс. рублей. Если фоновая концентрация CH_4 на ст. Териберка оценивается как (1870+-30) млрд⁻¹, то над г.С.Петербург (2060+- 50) млрд⁻¹, а за городом (1950+- 40)млрд⁻¹. Данные наземных, лидарных измерений с вертолёта концентрации CH_4 атмосфере, а также с помощью гиперспектрометра AIRS установленного на спутнике Aqua не противоречивы и сопоставимы.

Рассмотрены основные причины, способствующие возникновению аварий и инцидентов на газораспределительных сетях в городе и меры по минимизации рисков их возникновения.

СПИСОК ЛИТЕРАТУРЫ

1. Биненко В.И., Северюхина А.С. Оценка экологической безопасности газораспределительных сетей в г.Санкт-Петербурге Региональная экология 2016.N.2 (44)-3(45) 68-75.
2. Биненко В.И., Донченко В.К., Растоскуев В.В. Риски и экологическая безопасность природно-хозяйственных систем Санкт-Петербург, СПбГУ, 2012, 353 с.
3. Методические указания по проведению анализа риска для опасных производственных объектов газотранспортных предприятий ОАО «Газпром». Москва, 2009.

УДК 5040.054

ОЦЕНКА ЭКОЛОГИЧЕСКИХ РИСКОВ ПРИ РЕКОНСТРУКЦИИ МЕСТОРОЖДЕНИЯ В АРКТИЧЕСКОЙ ЗОНЕ РФ

Быковская Елена Александровна, Кустикова Марина Александровна,
Саусярис Эдгарас Стасевич, Маюрова Александра Сергеевна
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский пр., 49,
emails: brownies@mail.ru, marinakustikova@mail.ru, sev_51@mail.ru

Аннотация: В работе исследуются экологические риски в Арктической зоне Российской Федерации: их возникновение, возможные угрозы для данного региона и других зон, последствия и способы решения возникших проблем. В ходе работы проанализировано конкретное месторождение, где в данный момент происходит добыча углеводородов: описаны все возможные экологические риски, вероятность их возникновения и возможные последствия.

Ключевые слова: экологические риски, экологическая безопасность, Арктическая зона, добыча углеводородов.

ASSESSMENT OF ENVIRONMENTAL RISKS AT THE RECONSTRUCTION OF THE FIELD IN THE ARCTIC ZONE OF THE RUSSIAN FEDERATION

Bykovskaia Elena, Kustikova Marina, Sausiaris Edgaras, Maiurova Aleksnadra

University ITMO

emails: brownies@mail.ru, marinakustikova@mail.ru, sev_51@mail.ru

Abstract: In this article investigates environmental risks in the Arctic zone of the Russian Federation: their occurrence, possible threats to the region and other areas, the consequences and ways to solve the problems that have arisen. In the course of the work, a specific field was analyzed, where hydrocarbons are currently produced: all possible environmental risks, the likelihood of their occurrence and possible consequences are described.

Keywords: ecological risks, ecological safety, Arctic zone, hydrocarbon production

Введение. Одним из направлений нормализации окружающей среды является анализ экологических рисков и создание системы управления ими. При этом возникает необходимость, с одной стороны, количественной оценки вероятности возникновения процессов и явлений, снижающих качество окружающей среды, а с другой стороны, количественной оценки возможных ущербов от их проявления.

В последние годы актуальной проблемой стал анализ и прогноз негативных изменений (зачастую катастрофических) качества окружающей среды в результате добычи углеводородов.

На данный момент идут усиленные антропогенные нагрузки на Ямало-Ненецкий автономный округ в связи с добычей углеводородов, в частности с проведением реконструкции в Медвежьем нефтегазоконденсатном месторождении (НГКМ Медвежье), которое планируется закончить к концу 2018 г. Поэтому данная тема исследования является очень актуальной в настоящее время.

Целью исследования является выявление и оценка экологических рисков при добыче углеводородов в Арктической зоне Российской Федерации.

В задачи следования входит:

- рассмотрение понятия «экологические риски»;
- изучение методов оценки экологических рисков;
- анализ особенности Арктической зоны РФ;
- выявление и оценка экологических рисков при добыче углеводородов в Арктической зоне РФ;
- рассмотрение законодательства РФ и правовых документов, связанных с регулированием деятельности в Арктической зоне;
- анализ мирового опыта и международного регулирования деятельности человека в Арктике;
- анализ российского природоохранного законодательства с точки зрения его эффективности для защиты Арктической зоны;
- выявление и оценка экологических рисков при проведении реконструкции нефтегазоконденсатного месторождения Медвежье в ЯНАО.

Краткая характеристика полученных результатов.

Исследовано понятие экологический риск, которое означает вероятность получения определенного ущерба в результате проявления фактора экологической опасности или их совокупности по отношению к конкретному объекту оценки. Оценка экологического риска осуществляется с помощью математического расчета вероятности наступления неблагоприятных событий, вероятного ущерба и вреда окружающей среде. Сложные природно-климатические факторы, удаленность от промышленных центров усугубляет положение Арктики в случае утечки углеводородов, что повлияет не только на ухудшение среды данной зоны, но и на весь мир в целом.

В ходе исследования выявлено, что документы, определяющие в настоящий период развитие Арктической зоны и регламентирующие осуществление в данном регионе различных видов деятельности, так же, как и существующий проект закона, не в полной мере отражают сущность идеи устойчивого развития. Экологические аспекты устойчивого развития оказываются незакрепленными в нормативных правовых актах, теряются за многочисленными уточнениями понимания данного термина, дополнительными характеристиками экономической направленности.

В ходе работы проведен анализ проектной документации по реконструкции нефтегазоконденсатного месторождения «Медвежье» в ЯНАО, на основании которого выявлены возможные экологические риски и разработаны рекомендации по снижению вероятности их

возникновения. Поскольку экологические риски, которые могут возникнуть при реконструкции, не исключаются, то была проведена их оценка по степени наносимого ущерба и по вероятности возникновения риска.

Выводы. Сложные природно-климатические условия Арктической зоны РФ, в частности ЯНАО, в котором располагается НГКМ Медвежье, требуют значительных усилий для поддержания легкоразрушимой экологической системы.

В рекомендациях, которые должны быть в проектных документах, специалисты обязаны прописывать четкие критерии для контроля качества объектов реконструкции с целью исключить негативные моменты, связанные с третьей степенью возможного наносимого ущерба экологической среде ЯНАО.

Разработанные в данном исследовании рекомендации должны минимизировать возможность экологических рисков при реконструкции, либо при условии его возникновения снизить их отрицательное действие.

Самые вероятные экологические риски возникают на второй стадии реконструкции НГКМ Медвежье при проведении строительно-монтажных работ, они составляют 56% от всех возможных рисков и именно эта стадия требует повышенного внимания специалистов в области экологии, инженерии и права. Совмещение этих трех навыков позволит обеспечить минимизацию возникновения экологических рисков и защиту экологической системы в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Богоявленский В.И., Богоявленский И.В., Будагова Т.А. Экологическая безопасность и рациональное природопользование в Арктике и Мировом океане // Бурение и нефть, 2013. - № 12. - С. 10 – 16.
2. Тихомиров Н.П. Методы анализа и управления эколого-экономическими рисками. М.: ЮНИТИ-ДАНА, 2013. – 350 с.
3. Шмаль А.Г. Национальная система экологической безопасности (методология создания). г. Бронницы: МУП ИКЦ «БНТВ», 2014. – 200 с.

УДК 543.422

АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНАЯ СИСТЕМА ДЛЯ КОНТРОЛЯ СОСТАВА ДЕЗИНФИЦИРУЮЩИХ РАСТВОРОВ СОДЕРЖАЩИХ ПОЛИГЕКСАМЕТИЛЕНГУАНИДИН

Василевский Александр Михайлович, Герасимов Владимир Александрович,
Коноплев Георгий Асадович, Кострин Дмитрий Константинович, Степанова Оксана Сергеевна,
Ухов Андрей Александрович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5,
emails: gakonoplev@mail.ru

Аннотация: В докладе рассмотрены методика и аппаратура для определения концентрации полигексаметиленгуанидина в поликомпонентных дезинфицирующих средствах медицинского назначения по УФ спектрам поглощения. Приводятся основные характеристики автоматизированного спектроанализатора, дано описание программного обеспечения. Анализируются результаты испытаний разработанной системы в сравнении с данными, полученными по общепринятой методике фотометрирования с эозином.

Ключевые слова: спектрофотометрия; дезинфицирующие средства; ультрафиолетовая область; полигексаметиленгуанидин.

AUTOMATED INFORMATION-MEASURING SYSTEM FOR CONTROL OF THE COMPOSITION OF DISINFECTANTS CONTAINING POLYGEXAMETHYLENGUANIDINE

Vasilevsky Aleksandr, Gerasimov Vladimir, Konoplev Georgii, Kostrin Dmitrii, Stepanova Oksana,
Ukhov Andrey
St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
emails: gakonoplev@mail.ru

Abstract: The technique and equipment for UV spectrophotometric determination of the concentration of polyhexamethylene guanidine in multicomponent disinfectants for medical use are considered. The basic characteristics of the automated spectrophotometer and software are given. The results of tests of the developed system are analyzed in comparison with the data obtained according to the conventional photocolormetric method with eosin.

Keywords: spectrophotometry; disinfectants; ultraviolet region, polyhexamethylene guanidine

Полигексаметиленгуанидин гидрохлорид (ПГМГ) является достаточно перспективным биоцидным веществом, которое используется при создании композиционных дезинфицирующих средств. ПГМГ не накапливается в паренхиматозных органах теплокровных животных и человека, не опасен при ингаляционном воздействии, не оказывает тератогенного и мутагенного воздействия на

организм человека, хорошо совместим с различными материалами, обладает хорошей моющей способностью [1]. В связи с малой токсичностью, отсутствием неприятного запаха и раздражающего действия на кожные покровы, ПГМГ широко применяется в составе дезинфицирующих средств медицинского назначения, в частности растворов для обработки рук хирургов, обработки кожи, операционного и инъекционного полей, окончательной дезинфекции мебели, полов и стен в операционных, обработки белья и т.д. Концентрация ПГМГ в готовых растворах может колебаться от 1 г/л до 100 г/л в зависимости от области применения [2].

В процессе промышленного производства дезинфицирующих средств (ДС) требуется проведение регулярного контроля содержания ПГМГ как на разных технологических этапах, так и в готовом продукте. Допустимая погрешность определения концентрации не должна превышать 15%. Стандартная методика определения концентрации ПГМГ в растворах основана на фотометрировании с эозином в видимой области спектра на длине волны 544 нм. Эта методика требует предварительной пробоподготовки и калибровки, сложна и требует больших временных затрат, что затрудняет ее применение, особенно при серийном производстве.

Применение прямого абсорбционного спектрального анализа в ультрафиолетовой (УФ) области для определения концентрации ПГМГ дает возможность существенно сократить время анализа и снизить его трудоемкость за счет устранения этапа сложной пробоподготовки. При этом может быть заметно повышена эффективность технологического контроля ДС на основе ПГМГ.

Спектральные исследования моно- и поликомпонентных ДС на основе ПГМГ показали:

- УФ спектр поглощения водного раствора ПГМГ имеет характерную форму с очень широкой полосой, максимум которой приходится на область короче 200 нм, при этом на длинноволновом крыле отмечается слабо выраженный максимум на длине волны 262.5 нм;

- спектр поглощения ДС на основе ПГМГ с добавлением ПАВ включает дополнительные полосы на длинах волн 225.5 нм и 274.3 нм.

Исследованные спектры представляют собой комбинацию очень широких бесструктурных полос, которые сильно перекрываются между собой, поэтому определение концентрации ПГМГ и других компонентов в рассматриваемых средах по величине оптической плотности на одной или нескольких длинах волн в рамках классического подхода к абсорбционному спектральному анализу многокомпонентных растворов невозможно.

В связи с этим была разработана оригинальная методика анализа ДС, в которой для определения концентрации ПГМГ используется вся информативная спектральная область 220...350 нм. На основе предложенной методики создана информационно-измерительная система, включающий в себя автоматизированный УФ спектроанализатор с ПЗС фотоприемником и специализированное программное обеспечение.

Система включает в себя источник УФ излучения дейтериевую лампу ДНМ-15, полихроматор на основе вогнутой дифракционной решетки, оптический затвор с электромагнитным управлением, ПЗС фотоприемник и микроконтроллер. В приборе используется ПЗС TCD1304, производства фирмы Toshiba. Данный ПЗС фотоприемник закрыт защитным стеклом, не пропускающим УФ излучение, что не позволяет использовать его в системе регистрации без модификации. Модификация стандартного ПЗС фотоприемника заключается в удалении входного защитного стекла и покрытии поверхности кристалла специальным оптическим УФ прозрачным клеем. Клей выполняет две функции – он обеспечивает защиту поверхности кристалла фотоприемника, а также устраняет эффект интерференции, возникающей в тонкой пленке оксида кремния, нанесенной на поверхности ПЗС на этапе ее изготовления [4]. В состав устройства также входит кюветное отделение с автоматизированной кареткой, где устанавливаются кюветы с дистиллированной водой и исследуемым раствором. Кюветы под управлением микроконтроллера устанавливаются на требуемую позицию с помощью шагового двигателя.

Для получения информации о составе раствора в процессе измерений на кюветы последовательно направляется поток излучения источника УФ излучения. Прошедший через кюветы поток разлагается в спектр и направляется на ПЗС. Сигнал с ПЗС фотоприемника усиливается, с помощью АЦП преобразуется в цифровой код, проходит предварительную обработку с целью минимизации шумов [5] и передается на ПК, снабженный специализированным программным обеспечением.

Перед каждым измерением проводится внутренняя калибровка, в ходе которой измеряются темновой сигнал ПЗС и сигнал 100% пропускания, соответствующий интенсивности излучения, прошедшего через кювету с дистиллированной водой. Затем измеряется спектр пробы и вычисляется коэффициент пропускания исследуемой среды.

Основные этапы обработки измеренных спектров включает в себя:

1. Сглаживание измеренного спектра методом скользящего среднего;
2. Предварительный анализ – проверку спектра на соответствие уровня спектрального пропускания в информативной области измеренного спектра заданным критериям для обеспечения необходимой фотометрической точности;

4. Пересчет спектра пропускания в спектр поглощения в соответствии с законом Бугера-Ламберта-Бера;
5. Идентификацию раствора, в ходе которой измеренный спектр последовательно сравнивается со спектрами препаратов, имеющихся в базе данных программы, при этом в качестве критерия сравнения используется коэффициент подобия;
6. Расчет концентрации компонентов ДС по разработанной методике;
7. Проверка достоверности анализа путем сравнения восстановленного и измеренного спектров;
8. Сохранение результатов анализа и спектральных данных на диске в виде текстовых файлов с возможностью экспорта в MS Excel.

Для проверки достоверности результатов определения концентрации ПГМГ были приготовлены растворы ДС таким образом, что концентрация ПГМГ в пробах составляла от 0.05 до 1.5 г/л. Затем пробы подвергались анализу по принятой методике фотометрирования с эозином и по предложенной методике с помощью разработанной ИИС. Всего было исследовано семь проб различной концентрации, измерения повторялись трехкратно. Сопоставление полученных данных показало, что в диапазоне концентрации 0.05 до 0.4 г/л результаты определения концентрации ПГМГ по обеим методикам хорошо согласуются друг с другом; погрешность измерения концентрации в указанном диапазоне не превышает 10%. В области больших концентраций ПГМГ в пробах фотометрирование с эозином не дает достоверных результатов, в то время как предложенная методика позволяет работать вплоть до концентраций 1.5...2 г/л с погрешностью не более 15% на верхней границе диапазона.

Таким образом, разработанная методика и оптико-электронная информационно-измерительная система дают возможность проводить определение концентрации ПГМГ в поликомпонентных ДС с погрешностью, не превышающей 15%. По сравнению с принятой методикой, основанной на фотометрировании с эозином, существенно сокращено время анализа, упрощена процедура пробоподготовки, расширен рабочий диапазон концентраций.

СПИСОК ЛИТЕРАТУРЫ

1. Ерофеев В.Т., Комохов П.Г., Светлов Д.А. и др. Защита зданий и сооружений от микробиологических повреждений биоцидными препаратами на основе гуаниди-на. СПб.: Наука, 2009. 192 с.
2. Афиногенова А.Г., Краснова М.В., Афиногенов Г.Е. Инструкция по применению и методам контроля качества дезинфицирующего (кожный антисептик) средства "Тефлекс-А", производства ЗАО "Софт протектор". СПб: 2007 г.
3. А.А. Бабушкин, П.А. Бажулин, Ф.А. Королев и др. Методы спектрального анализа, М.: Изд-во МГУ, 1962. – 510 с.
4. Пихтин А.Н., Колгин Е.А., Ухов А.А. Подавление интерференционных искажений спектральной чувствительности в спектрометрах с ПЗС-фотоприемниками. Известия СПбГЭТУ «ЛЭТИ», Изд-во СПбГЭТУ, СПб, №2 2003. – С 7-10.
5. Юдин Р. В., Кострин Д. К., Шишов Д. И., Ухов А. А. Повышение точности и воспроизводимости результатов колориметрических измерений светоизлучающих диодов. Известия СПбГЭТУ «ЛЭТИ», №3 2013, С.8-13.

УДК 528.94

ПРОСТРАНСТВЕННАЯ ДИНАМИЧЕСКАЯ МОДЕЛЬ РЕГИОНАЛЬНОГО УРОВНЯ ОКРЕСТНОСТИ ОЗЕРА КРАСНОЕ

Воронцова Екатерина Николаевна
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский проспект, 49
email: voronakathy1004@gmail.com

Аннотация: составление пространственной динамической модели для участка Соловецкого острова и характеристика системы.

Ключевые слова: пространственная динамическая модель, запас древесины через 10 лет, матрица таксономического описания, легенда динамической модели.

SPATIAL DYNAMIC MODEL OF THE REGIONAL LEVEL OF THE LAKE KRASNOYE SURROUNDINGS

Vorontsova Ekaterina
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronversky prospect, 49
email: voronakathy1004@gmail.com

Abstract: the compilation of a spatial dynamic model for the Solovetsky Island site and the characteristics of the system.

Keywords: spatial dynamic model, wood stock after 10 years, matrix of taxonomic description, legend of dynamic model.

Введение. Актуальность работы можно обосновать несколькими причинами. Во-первых, это возможность открытия набирающих все большую популярность экологических троп на участке Соловецких островов. Во-вторых, с помощью полученных карт и характеристики системы можно

осуществлять прогноз дальнейших изменений в системе. И наконец, немаловажная причина – безопасное природопользование, характеристика системы через инвариант позволяет выявить, где и как можно «пользоваться» данным участком островов, не нанося ущерба природе.

Задачи:

1. Составить карту пространственной динамической модели по экологическим нишам.
2. Составить карты моделей увлажнения, структуры почвы, превышений.
3. Охарактеризовать систему с помощью инварианта.

С помощью данных, взятых из таксационных описаний участка, была составлена матрица таксационных описаний, которая была поделена в соответствии с легендой, составленной по экологическим нишам, встречающимся на данном лесоустойчивом участке.

Далее работа проводилась на основе программы Q-GIS, где карта лесоустойчивого участка была привязана к космическому снимку и были составлены структуры пространственных динамических моделей по типам леса, увлажненности и типам почв

В ходе работы была составлена карта пространственной динамической модели по экологическим нишам, карта моделей увлажнения, структуры почвы, взяты данные о превышениях из топографической основы, дана характеристика системы с помощью инварианта.

Заключение. В конце работы:

1. Была создана пространственная динамическая модель.
2. Был произведен расчет объемов древесины разных видов.
3. Были составлена легенда к динамической модели карты.

На ее основе были созданы 5 карт, отображающих восстановление древесного яруса после антропогенного вмешательства.

СПИСОК ЛИТЕРАТУРЫ

1. Кобелева Н.В. Системная региональная диагностика природной среды: Учебное пособие. – СПб: Изд-во «Лема», 2010. – 38 с.
2. Бакланов Н.А. Геосистемы с пересекающимися структурами. Ландшафтоведение: теория и методы, региональные исследования. М., 2006, с. 33-35.

УДК 528.94

РАЗРАБОТКА ПРОСТРАНСТВЕННОЙ ДИНАМИЧЕСКОЙ МОДЕЛИ: ЭКОЛОГО-ЭКОНОМИЧЕСКАЯ МОДЕЛЬ КАРТЫ ДРЕВЕСНЫХ ЗАПАСОВ

Герасимов Константин Романович, Хворостовский Артемий, Кравцов Илья
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский проспект, 49
email:gearuse@gmail.com

Аннотация: В статье рассмотрена методика построения пространственной динамической модели на основе лесотехнической схемы и таксономического описания Соловецких островов.

Ключевые слова: пространственная динамическая модель, запас древесины через 10 лет, матрица таксономического описания, легенда динамической модели.

DEVELOPMENT OF THE SPATIAL DYNAMIC MODEL: ECOLOGO-ECONOMIC MODEL OF THE CARD OF WOOD RESERVES

Gerasimov Konstantin Romanovich, Khvorostovskiy Artemiy, Kravtsov Ilya
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronversky prospect, 49
email:gearuse@gmail.com

Abstract: The technique of constructing a spatial dynamic model based on the forestry scheme and the taxonomic description of the Solovetsky Islands is considered in the article.

Keywords: spatial dynamic model, wood stock after 10 years, matrix of taxonomic description, legend of dynamic model.

Введение. Природные ландшафты Соловецких островов представляют собой целостный объект, который является сложной системой, состоящей из объектов живой природы, а именно растительности, в рамках исследования. Данные исследования заключают в себе огромную ценность, как для промышленности, использующей древесину в качестве сырья, так для экологического мониторинга лесных ресурсов нашей страны.

Целью моей работы является разработка эколого-экономической динамической модели карты прогноза древесных запасов через 10 лет, на выделенном мне районе.

Задачи:

- Создание карты пространственной динамической модели

- Расчет древесной составляющей на Га
- Разработка легенды к динамической модели
- Создание на основе модели 5 карт, отображающий процесс сукцессии с результатом через 10 лет.

Для создания модели использовались часть лесоустроительной карты масштабом 1:25000, таксономическое описание данной местности. Первым делом в программе эксель составляется матрица таксономического описания, все данные выстраиваются по порядковому номеру выдела. Из этой матрицы создаем легенду. Для этого нужно провести ранжирование по определенным признакам, после чего формируются группы с одинаковыми признаками. Легенда будет состоять из 5 основных групп и 9 подгрупп по экологическим нишам, Весь смысл легенды кроется в ее нормировке, она состоит из букв и цифры. Цифра - это номер группы по порядку, буква обозначает сукцессионный ряд, то есть все участки со временем станут самым первым под буквой «А», переход одного ряда в другой составляет 10 лет.

Заключение. В конце работы:

- Была создана пространственная динамическая модель.
- Был произведен расчет объемов древесины разных видов.
- Были составлена легенда к динамической модели карты.

На ее основе были созданы 5 карт, отображающих восстановление древесного яруса после антропогенного вмешательства.

СПИСОК ЛИТЕРАТУРЫ

1. Кобелева Н.В. Системная региональная диагностика природной среды: Учебное пособие. – СПб: Изд-во «Лема», 2010. – 38 с.
2. Бакланов Н.А. Геосистемы с пересекающимися структурами. Ландшафтоведение: теория и методы, региональные исследования. М., 2006, с. 33-35.

УДК 004.67; 004.89; 621.3.068

КОГНИТИВНЫЙ МОНИТОРИНГ ЭКСТРЕМАЛЬНЫХ СОСТОЯНИЙ В МНОГОМЕРНЫХ ВРЕМЕННЫХ РЯДАХ ДАННЫХ О ПРИРОДНЫХ СИСТЕМАХ

Горохов Владимир Леонидович¹, Бузников Анатолий Алексеевич¹, Витковский Владимир Валентинович²

¹ Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5,

² Специальная Астрофизическая Обсерватория РАН,
Россия, Нижний Архыз

Аннотация: В статье рассмотрены алгоритмы визуализации многомерных временных рядов с целью обнаружения аномалий и вторжений в системы сбора и мониторинга природных систем

Ключевые слова: когнитивная машинная графика; непараметрическое обнаружение сигналов;

COGNITIVE MONITORING OF EXTREME STATES IN MULTIDIMENSIONAL TIME DATA RANGES ON NATURAL SYSTEMS

Gorokhov Vladimir¹, Buznikov Anatoli¹, Vitkovskiy Vladimir²

¹ Saint Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov st., 5

² Special Astrophysical Observatory of the Russian Academy of Sciences, Russia, Nizhniy Arkhyz

Abstract: The article present algorithms of visualization of multidimensional time series for the purpose of detection of anomalies of monitoring of natural systems.

Keywords: cognitive machine graphics; non-parametric signal detection.

Введение. В данной работе приводятся модернизированные алгоритмы динамического проецирования многомерных временных рядов, обеспечивающие генерацию когнитивных образов многомерных рядов. Когнитивные образы позволяют визуализировать многомерные взаимные корреляции и тем самым обнаруживать экстремальные состояния объектов мониторинга. Практика применения когнитивной машинной графики показала, что малые, но синхронные изменения характеристик носят синергетический характер и часто являются предвестниками чрезвычайных ситуаций. Предлагаются алгоритмы когнитивной визуализации многомерных временных рядов. Обозначим набор из p временных рядов в виде d_j ($j=1, \dots, p$), наблюдаемого в n временных точках. Значение d_j во временной точке t обозначается $\{d_{jt}\}$, а совокупность (p, n) значений d матрицей D . Как и одномерном случае D рассматривается как реализация случайного процесса. В общем случае, вектор строка из D может содержать тренд, сезонность и осцилляции. Многомерные ковариации и корреляции, а также взаимные многомерные ковариации и корреляции в виде квадратных матриц описывают зависимости внутри рядов и их синхронизмы для любых запаздываний s . Пусть входные

данные описываются матрицей : $D = \{d_{ij}\}$; $i = (1, n)$, $j = (1, p)$, где d_{ij} – действительные значения переменных (измеряемых параметров, признаков), n – число актов измерения всех p параметров объекта в последовательности времени наблюдения, p – число измеряемых параметров (признаков) объектов наблюдения. Многомерный временной ряд представляется в виде облака n точек в p -мерном пространстве параметров. Далее, будем полагать это p -мерное пространство параметров евклидовым R^p , что упрощает дальнейшие рассуждения (рассмотренные далее алгоритмы остаются рабочими в подходящих базисах аффинного пространства и ряда других базисов). Строятся отображения Φ как проекции этого облака на двумерную плоскость Q^2 , проходящую через начало координат пространства R^p . Пусть в Q^2 заданы единичные ортогональные вектора u и v , используя их несложно вычислить координаты (x, y) проекции данных на двумерную гиперплоскость Q , где исходная матрица данных D описывает облако точек T в многомерном пространстве параметров. Алгоритм строит непрерывную последовательность положений Q^2 , образующих “траектории”, вдоль которых и отслеживается динамика образа.

Закключение. Когнитивная система визуализации позволяет визуализировать многомерные временные ряды и их аномалии.

СПИСОК ЛИТЕРАТУРЫ

1. Горохов В.Л., Муравьев И.П. Когнитивная машинная графика. Методы динамических проекций и робастная сегментация многомерных данных. Методология, методики и интерфейсы. Монография. СПб.: ИНЖЭКОН. 2007, 173 с.

УДК 004.67; 004.89; 621.3.068

КОГНИТИВНОЕ ОБНАРУЖЕНИЕ АНОМАЛИЙ И ВТОРЖЕНИЙ В МНОГОМЕРНЫХ ВРЕМЕННЫХ РЯДА ДАННЫХ ГИДРОЛОГИЧЕСКОГО МОНИТОРИНГА СКВАЖИН

Горохов Владимир Леонидович, Бузников Анатолий Алексеевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5

Аннотация: В статье рассмотрены примеры визуализации многомерных временных рядов с целью обнаружения аномалий и вторжений в системы сбора и мониторинга в гидрологии.

Ключевые слова: когнитивная машинная графика; непараметрическое обнаружение сигналов.

COGNITIVE DETECTION OF ANOMALIES AND INVASIONS IN MULTIDIMENSIONAL TIME RANGE OF HYDROLOGICAL MONITORING DATA OF WELLS

Gorokhov Vladimir, Buznikov Anatoli
The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,

Abstract: The article presents examples of visualization of multidimensional time series for the purpose of detecting anomalies and intrusions in the systems of collection and monitoring in hydrology.

Keywords: Cognitive machine graphics; non-parametric signal detection.

Введение. Предлагаются алгоритмы выявления сигналов неизвестной формы в многомерных временных рядах с последующим представлением отдельных временных рядов от каждой скважины как точек многомерном пространстве параметров этих скважин. С помощью средств когнитивной машинной графики эти данные образуют когнитивные образы, в которых наглядно видно как аномальное поведение параметров этих скважин может быть выявлено в случае многомерных терабайтных массивов. Поэтому предлагается для выявления аномалий в поведении скважин использовать когнитивный анализ многомерных временных рядов по каждой скважине и затем предлагается непараметрические статистики количественной оценки этих аномалий в многомерных рядах. На первом этапе осуществляется когнитивный анализ многомерных временных рядов в отдельных объектах с целью выявления характерных аномалий в поведении временных трендов (сигналов) по каждой характеристике объекта (например, скважине). На основании этого анализа можно сформировать модель сигналов в многомерных временных рядах и выделить фрагменты рядов, не содержащих аномальных трендов со всей очевидностью. Это позволит использовать метод контраста при формировании модели сигнала (аномалии, тренда). Затем предлагаются непараметрические статистики количественной оценки этих аномалий, применяемые к многомерным временным рядам. На втором этапе с помощью этих статистик осуществляется своеобразная «свертка» многомерных рядов в набор точечных оценок величины аномалий в этих временных рядах параметров одного объекта. Оценки аномалий по отдельным параметрам объекта можно рассматривать как своеобразную нормировку временных рядов. На третьем этапе весь набор объектов мониторинга можно представить, как множество точек многомерном пространстве аномалий характеристик этих объектов. Это множество точек в многомерном пространстве характеристик можно

снова представить виде когнитивного образа, теперь уже всего множества объектов. Только теперь выявление отдельных облаков в этом когнитивном образе будет показывать, насколько велики аномалии, и каким техническим объектам эти аномалии соответствуют.

Заключение. Когнитивная система визуализации позволяет выявлять аномальные изменения в многомерных данных даже если эти аномалии малы, но синхронны по параметрам.

СПИСОК ЛИТЕРАТУРЫ

1. The United Kingdom Offshore Oil and Gas Industry Association (Oil and Gas UK) / Accident statistics for Offshore Units on the UKCS 1990–2007, 2009. URL: <http://www.oilandgasuk.co.uk/cmsfiles/modules/publications/pdfs/EC024.pdf>.
2. Горохов В.Л., Муравьев И.П. Когнитивная машинная графика. Методы динамических проекций и робастная сегментация многомерных данных. Методология, методики и интерфейсы. Монография. СПб.: ИНЖЭКОН. 2007, 173 с.

УДК 528.946

СТРУКТУРА ЭКОСИСТЕМ МЕЖОЗЕРЬЯ ДОЛГОЕ-ПОДСЕКИРНОЕ НА ТОПОЛОГИЧЕСКОМ УРОВНЕ

Кувардина Мария Юрьевна

Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский пр., 49,
email: marykuv@mail.ru

Аннотация: В статье рассмотрены структурные особенности фито-экосистем межозерья Долгое-Подсекирное на топологическом уровне.

Ключевые слова: экосистема; структура; экологическая ниша; инвариант.

STRUCTURE OF DOLGOE-PODSEKIRNOE INTER-LAKES ECOSYSTEMS AS THE TOPOLOGICAL LEVEL

Kuvarдина Mariya

Saint Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronverksky avenue 49,
email:marykuv@mail.ru

Abstract: The article presents structural features of phyto-ecosystems of inter-lake Dolgoe-Podsekirnoe on topological level.

Keywords: ecosystem; structure; ecological niche; invariant.

Введение. Структура экосистемы - естественное функционально-морфологическое членение экосистемы на подсистемы и блоки, играющие в экосистеме роль структурных элементов.

Под видовой структурой понимается количество видов, образующих экосистему, и соотношение их численностей. Видовое разнообразие - очень важное свойство экосистем. С ним связана устойчивость систем к неблагоприятным факторам среды. Положение вида, которое он занимает в общей системе биоценоза, комплекс его биоценологических связей и требований к абиотическим факторам среды называют экологической нишей вида. Экологическая ниша вида зависит не только от абиотических условий среды, но и в не меньшей мере от его биоценологического окружения.

Характер занимаемой экологической ниши определяется как экологическими возможностями вида, так и тем, насколько эти возможности могут быть реализованы в конкретных биоценозах.

Характеристика исследуемого участка: межозерье Долгое-Подсекирное представлено такими видами растительности как:

- Древесный ярус: сосна, береза, ель;
- Кустарнички: черника, брусника;
- Мхи: долгомошные, зеленомошные.
- Преобладающий тип почвы – подзолистая.
- Заключение. В статье были выполнены следующие задачи:
 - по исходным данным описаний территориальных участков была построена матрица;
 - проведен Q анализ (на наличие сходства между территориальными участками);
 - проведен R анализ (на наличие сходств видового состава);
 - определена экологическая ниша.

СПИСОК ЛИТЕРАТУРЫ

1. Кобелева Н.В. Системная региональная диагностика природной среды: Учебное пособие. – СПб: Изд-во «Лема», 2010. – 38 с.
2. Акимова Т.А., Хаскин В.В. Экология: Учебник для вузов. - М.: ЮНИТИ-ДАНА, 2001.

УДК 504.054

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ МЕТОДОВ ОБРАБОТКИ СИГНАЛОВ И ИЗОБРАЖЕНИЙ В ЗАДАЧАХ ЭКСПРЕСС ВИБРОДИАГНОСТИКИ НА ОБЪЕКТАХ ТЭКМалышев Григорий Сергеевич¹, Гришканич Александр Сергеевич², Локтаев Кирилл Виленинович³¹ Опытнo-конструкторское Бюро Машиностроения им. И.И. Африкантова,
Россия, Нижний Новгород, Бурнаковский пр-д, 15,²Радиевый институт имени В. Г. Хлопина, Россия, Санкт-Петербург, 2-й Мушинский пр., 28³Национальный исследовательский ядерный университет «МИФИ»,
Россия, Москва, Каширское ш., 31

emails: gr1g0r@yandex.ru, Grishkanich@ya.ru, loktaev@bk.ru

Аннотация: Цифровая обработка сигналов (ЦОС) имеет большое фундаментальное и прикладное значение в современной радиотехнике и смежных с нею областях. Ее методы используются для разработки и исследования радиоэлектронных устройств и систем различного назначения, а ее средства – для их аппаратно-программной реализации. ЦОС как направление науки и техники зародилась в 50-ые годы XX столетия. Однако, даже в наши дни применение цифровых методов обработки сигналов и изображений считается чем-то экзотическим. Во многом это связано с тем, что цифровая обработка сигналов изучается на радиотехнических специальностях, выпускники которых редко устраиваются на предприятия тяжёлого машиностроения. Поэтому важно показать преимущество данного метода в сравнении с другими подходами. В данной статье рассматриваются возможности цифровой обработки сигналов и изображений для решения текущих производственных задач, которые актуальны не только для нашего предприятия, но и для отрасли в целом. К таким задачам относятся виброакустические исследования и определение параметров асинхронных двигателей. Естественно, что в ряде случаев невозможно отказаться от использования специализированной аппаратуры. Но опыт внедрения программ цифровой обработки на нашем предприятии показал, что в случае измерений, к которым не предъявляются требования высокой точности, появляется возможность отказаться от применения дорогостоящего измерительного оборудования. Что и продемонстрировано в данной работе.

Ключевые слова: цифровая обработка сигнала, измерительное оборудование, алгоритм Кэнни, виброакустические исследования

USING DIGITAL SIGNAL AND IMAGE PROCESSING METHODS IN VIBRODIAGNOSTIC EXPRESS OBJECTS ON FACILITIESMalyshev Gregory¹, Grishkanich Alexander², Loktaev Kirill³¹ OAO I. I. Afrikantov OKB Mechanical Engineering,
Russia, Nizhny Novgorod, Burnakovskiy Ave., 15,² V. G. Khlopin Radium Institute, Russia, St. Petersburg, 2nd Murinsky Ave, 28,³ National Research Nuclear University MEPhI, Russia, Moscow, Kashirskoe shosse, 31.

emails: gr1g0r@yandex.ru, Grishkanich@ya.ru, loktaev@bk.ru

Abstract: Digital signal processing (DSP) is of great fundamental and applied importance in modern radio engineering and related areas. Its methods are used to develop and study radio electronic devices and systems for various purposes, and its means for their hardware and software implementation. DSP as a direction of science and technology was born in the 50th years of the XX century. However, even nowadays the use of digital signal and image processing methods is considered something exotic. In many respects this is due to the fact that digital signal processing is studied in radio engineering specialties, graduates of which are rarely arranged for heavy engineering enterprises. Therefore, it is important to show the advantage of this method in comparison with other approaches. This article deals with the possibilities of digital processing of signals and images to solve current production problems that are relevant not only for our enterprise, but also for the industry as a whole. Such tasks include vibroacoustic research and determination of the parameters of asynchronous motors. Naturally, in some cases it is impossible to refuse the use of specialized equipment. But the experience of introducing digital processing programs at our enterprise has shown that in the case of measurements that do not require high accuracy, it becomes possible to abandon the use of expensive measuring equipment. As demonstrated in this paper.

Keywords: digital signal processing, measuring equipment, Canny algorithm, vibroacoustic research.

В условиях современной конкурентоспособности и импортозамещения была разработана программа, которая позволяла бы путём компьютерной обработки изображений колеблющегося объекта определять частоту и амплитуду колебаний. Данная программа позволяет фиксировать на изображении границу «объект-фон». Координата этой границы заносится в память компьютера, и таким образом мы получаем эпюру колебания. Далее к полученной кривой мы применяем спектральные методы обработки сигнала, что позволяет выявить основные характеристики колебания – это спектр колебаний, частота доминирующей гармоник, её амплитуда. Основная сложность состояла в

определении границы «объект-фон». Эта задача была решена с использованием алгоритма Кэнни, который основан на построении поля градиента яркости изображения. Этот метод цифровой обработки хорошо описан в научной литературе, но на предприятии такая программа использована впервые.

Актуальность выполненной работы связана с тем, что внедрение программы даёт ряд преимуществ:

Для измерений, не требующих высокой точности определения амплитуды колебаний, появляется возможность отказаться от применения дорогостоящего измерительного оборудования;

Бесконтактные измерения позволяют решить проблему монтажа датчиков виброускорений в труднодоступных местах. Причём данная задача часто технически нереализуема без нарушения целостности образца;

Пропадает необходимость применять материалы, изолирующие датчики от водной среды.

Кроме того, массо-габаритные характеристики датчиков таковы, что их установка на конструкцию будет существенно влиять на измеряемые характеристики. Наконец, характеристики датчиков зависят от температуры и давления. Бесконтактные измерения позволяют решить эти проблемы. Программа была опробована на вибростенде предприятия. Были проведены тестовые измерения параметров вибрации трубки длиной 600 мм. Задавались различные частоты и амплитуды виброперемещений. Измерения проводились двумя методами - с помощью датчиков виброускорений и с помощью метода цифровой обработки изображений, полученных высокоскоростной камерой. Камера и макрообъектив были предоставлены лабораторией гидро- и аэродинамических испытаний. При частоте возбуждения от 80-2000 Гц и амплитудах, больших 20 мкм, наблюдается хорошее совпадение результатов. Для амплитуд, меньших 20 мкм появляются различия, которые связаны с тем, что использованный макрообъектив 1:1 не даёт достаточного увеличения объекта. Однако, существуют макрообъективы с куда большим увеличением, которые позволят, в перспективе, измерять перемещения в доли микрон. Если же речь идёт о колебаниях с амплитудами в сотни микрон, результаты, полученные двумя методами, практически совпадают (даже при использовании макрообъектива 1:1), что говорит о перспективности нового метода.

Цифровая обработка сигналов позволяет решить проблему измерения скольжения асинхронных электродвигателей с закрытым валом. Скольжение является одной из важнейших характеристик электродвигателя. Для измерения скольжения используется катушка индуктивности, в которой поля статора и ротора наводят ЭДС индукции. Частота скольжения – это фактически частота низкочастотной огибающей этого сигнала. В ГОСТ 7217-87 для определения этой частоты предлагается использовать гальванометр, стрелка которого отклоняется в такт низкочастотной огибающей. Посчитав количество колебаний стрелки за фиксированный интервал времени, мы определяем частоту скольжения. Расчёт скольжения производится на калькуляторе. Поэтому была поставлена задача найти новый метод измерения скольжения и произвести его экспериментальную проверку. Для достижения этой цели было предложено вместо использования гальванометра, использовать цифровой программный фильтр.

Новый метод позволил полностью автоматизировать процесс измерения скольжения. Произведена оценка погрешности измерений. Погрешность составила 2,5 %, что меньше погрешности измерений с помощью гальванометра. Эксперименты, проведённые для электродвигателя насоса, показали, что оба метода дают совпадение результатов с точностью до второго знака после запятой, но при этом новый метод позволяет вычислять скольжение каждые три секунды и с большей точностью.

СПИСОК ЛИТЕРАТУРЫ

1. Гонсалес Р., Вудс Р. Цифровая обработка изображений. Издание 3-е, исправленное и дополненное. М.: Техносфера, 2012. – 1104 с.

УДК 504.064.36/004.62

ПРЕДСТАВЛЕНИЕ ОТКРЫТЫХ ДАННЫХ МОНИТОРИНГА АТМОСФЕРЫ ДЛЯ ПОВЫШЕНИЯ ИНФОРМИРОВАННОСТИ НАСЕЛЕНИЯ О СОСТОЯНИИ ОКРУЖАЮЩЕЙ СРЕДЫ

Мателенок Игорь Владимирович, Мелентьев Владимир Владимирович

Санкт-Петербургский государственный университет аэрокосмического приборостроения,

Россия, Санкт-Петербург, ул. Большая Морская, 67,

emails: igor_matelenok@mail.ru, vv.melentyev@mail.ru

Аннотация: Рассмотрены возможности повышения информативности и удобства использования открытых данных мониторинга атмосферного воздуха в Санкт-Петербурге. Предложены оптимальные для визуальной оценки формы представления данных мониторинга. Описана разработанная технология автоматического создания информационных продуктов в виде карт-схем загрязнения атмосферы.

Ключевые слова: автоматизированная система мониторинга; карты загрязнения атмосферного воздуха; мониторинг состояния атмосферы; открытые данные

REPRESENTATION OF AIR MONITORING OPEN DATA FOR RAISING PUBLIC AWARENESS OF ENVIRONMENTAL STATE ISSUES

Matelenok Igor, Melentyev Vladimir
State University of Aerospace Instrumentation,
Russia, St. Petersburg, Bolshaya Morskaya str. 67,
emails: igor_matelenok@mail.ru, vv.melentyev@mail.ru

Abstract: Opportunities for improving information value and convenience of use of public air monitoring data products for Saint-Petersburg were considered. Forms of data representation which are optimal for visual assessment were proposed. Developed technique of automatic generation of data products in the form of thematic air pollution maps was described.

Keywords: *automated system of environmental monitoring; air monitoring; air pollution maps; open data*

В последние годы наметилась тенденция к повышению открытости информации по вопросам, традиционно относящимся к ведению государственных органов и представляющим особую важность для здоровья и качества жизни населения Российской Федерации. Одним из таких вопросов является обеспечение экологической безопасности. Сети мониторинга (основной из которых является ЕСГЭМ), призваны удовлетворить запросы ведомств, научных организаций, частных компаний, а также рядовых граждан в части своевременного получения достоверной информации о состоянии окружающей среды. Однако в настоящее время перечень наборов данных, размещаемых в открытом доступе, весьма ограничен. Также такие данные зачастую не обладают удобством в использовании из-за особенностей выбранных организациями-операторами форм представления.

Мониторинг воздуха населенных мест является неотъемлемым звеном в системе обеспечения экологической безопасности [1]. Наиболее развитыми среди существующих в России являются системы мониторинга атмосферы в Москве и Санкт-Петербурге. Так, сеть АСМ-АВ, поддерживаемая ГГУП СФ «Минерал», объединяет более 20 станций в Санкт-Петербурге [2]. Получаемая с этих постов контроля информация после обработки оперативно размещается на страницах веб-сайта комитета по природопользованию, охране окружающей среды и обеспечению экологической безопасности и экологическом портале Санкт-Петербурга.

Доступные рядовым пользователям текстовые отчеты, несмотря на наличие в них подробных пояснений к результатам измерений, не позволяют быстро оценить обстановку в масштабах целого города. Аналогичным недостатком обладает и тематический слой находящейся в открытом доступе интерактивной карты, отражающей пространственную и временную изменчивость характеристик загрязнения атмосферы. Взгляду пользователя оказывается недоступна информация сразу по нескольким станциям мониторинга, а сохранение данных возможно лишь в форматах, малопригодных для дальнейшего автоматизированного анализа.

Предлагается дополнить указанные формы представления открытых данных мониторинга атмосферы картами-схемами пространственной изменчивости загрязнения воздуха. В качестве базового продукта в этом случае могут выступать карты-схемы, построенные по данным, усредненным за сутки. Также оптимальным будет регулярное размещение в открытом доступе карт-схем, отражающих пространственные вариации характеристик загрязнения с интервалами усреднения в месяц, квартал и год. В настоящей работе предложены цветовые решения и схемы наполнения карт-материалов, призванные сделать более удобным визуальный анализ данных конечными пользователями.

К настоящему моменту разработана и запущена в тестовую эксплуатацию на кафедре инноватики и интегрированных систем качества Санкт-Петербургского государственного университета аэрокосмического приборостроения (ГУАП) технология автоматизированного создания описанных информационных продуктов по открытым данным мониторинга [3]. Она основана на использовании открытого программного обеспечения и обеспечивает оперативное создание карт-схем по данным с Экологического портала Санкт-Петербурга. Технологическая цепочка включает в себя этапы получения исходных данных за необходимые даты с ресурсов сети Интернет, формирования производных файлов с численными оценками характеристик загрязнения и создания итоговых информационных продуктов – карт-схем. Программный код написан на языке R, благодаря функциональным дополнительным пакетам предоставляющим широкие возможности для работы с разнообразными геопространственными данными, числовой и текстовой информацией, размещенной в сети Интернет. Доступ к картам-схемам организован через специальный раздел сайта Института инноватики и базовой магистерской подготовки ГУАП [4]. В настоящее время в распоряжении пользователей имеются карты-схемы за 2017 г.

Получаемые карты-схемы соединяют в себе универсальную черно-белую подложку, отображающую водные объекты, дорожную сеть и массивы древесной растительности, легенду с дополнительными пояснительными подписями и цветные тематические слои, характеризующие пространственную изменчивость содержания конкретных загрязнителей в атмосферном воздухе.

Цветовой диапазон, используемый для визуализации отношения фиксируемой концентрации к ПДК в среднесуточном выражении, охватывает 256 градаций от зеленого до красного.

Проведенная работа позволяет компенсировать отдельные недостатки форматов представления данных, имеющихся в открытом доступе, и делает более удобным визуальный анализ информации о загрязнении атмосферы в Санкт-Петербурге. В дальнейшем планируется расширить набор автоматически генерируемых информационных продуктов и перечень доступных вариантов оформления карт-схем.

СПИСОК ЛИТЕРАТУРЫ

1. Черногаева Г. М., Малеванов Ю. А., Журавлева Л. Р. Мониторинг загрязнения окружающей среды в Российской Федерации: организация наблюдений, обобщение и распространение информации // Проблемы экологического мониторинга и моделирования экосистем. 2015. Т. 26. № 2. С. 128-138.
2. Азёмов Д. Т. Система мониторинга атмосферного воздуха Санкт-Петербурга // Окружающая среда Санкт-Петербурга. 2016. № 2 (2). С. 8-14.
3. Мателенок И.В. Автоматическая генерация информационных продуктов на основе открытых данных атмосферного воздуха // Вестник СГУГиТ [Электронный ресурс]. 2017. Т. 22. №3.
4. Сайт института инноватики и базовой магистерской подготовки ГУАП [Электронный ресурс]. URL: <http://fiqm.ru/>

УДК 528.94

СОЗДАНИЕ СТРУКТУРНО-ДИНАМИЧЕСКОЙ МОДЕЛИ ТИПОВ ВЫДЕЛОВ ТЕРРИТОРИИ И ПРОГНОЗНОЙ ТЕМАТИЧЕСКОЙ КАРТЫ РАСПРЕДЕЛЕНИЯ ЛЕСОВ ПО КЛАССАМ ВЛАЖНОСТИ ПОЧВ НА ПРИМЕРЕ ЦЕНТРАЛЬНО-ЮГО-ЗАПАДНОЙ ЧАСТИ О. СОЛОВЕЦКОГО

Носова Анастасия Олеговна

Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,

Россия, Санкт-Петербург, Кронверкский пр., 49, email: mast225856@yandex.ru

Аннотация: Работа посвящена вопросу создания структурно-динамической модели типов выделов территории и прогнозную тематическую карту распределения лесов по классам влажности почв на примере центрально-юго-западной части острова Соловецкого.

Ключевые слова: моделирование пространственных данных; геоинформационные системы; тематическая карта; структурно-динамическая модель.

CREATION OF THE STRUCTURAL-DYNAMIC MODEL OF TYPES OF AREAS OF TERRITORY AND PREDICTIVE THEMATIC MAP OF DISTRIBUTION OF FORESTS BY CLASSES OF SOIL MOISTURE ON THE EXAMPLE OF THE CENTRAL-SOUTHWEST PART OF SOLOVETSKY ISLAND

Nosova Anastasiia

ITMO University

Russia, St. Petersburg, Kronverkskyavenue 49,
email: mast225856@yandex.ru

Abstract: The article is devoted to the question of creation of the structural-dynamic model of types of areas of territory and predictive thematic map of distribution of forests by classes of soil moisture on the example of the central-southwest part of Solovetskyisland.

Keywords: modeling of spatial data; geoinformation systems; thematic map; structural-dynamic model.

Введение. Соловецкие острова – поистине уникальный природный уголок, не имеющий аналогов во всём мире. Эта особенная территория - небольшой архипелаг, утопающий в водах Белого моря, являет собой настоящий музей под открытым небом, удачно сочетающий на своих землях природные, исторические и культурные богатства. На данный момент тематических карт для этой территории нет, поэтому данная работа актуальна. В настоящее время в науке и технике для описания тех или иных объектов, процессов или явлений традиционно применяются литературные, статистические, картографические, аэро- и космические материалы и данные [1]. Источниками данных для выполнения данной работы будут являться таксономические описания и лесоустроительная карта исследуемого участка.

Цель работы: создать структурно-динамический граф типов выделов территории и прогнозную тематическую карту распределения лесов по классам влажности почв.

Задачи:

- 1) используя таксономические описания и лесоустроительную карту, составить матрицу исходных данных;
- 2) проранжировать строки матрицы по подросту, экологическим нишам, основному дереву, влажности, чтобы составить легенду для будущей карты;
- 3) составить легенду, в которой с увеличением цифры усиливается степень заболоченности выдела, а буква показывает степень лесовосстановления;
- 4) оцифровать карту в программе QGIS;

- 5) создать тематическую карту - схему распределения лесов по классам влажности почв;
- 6) создать структурно-динамический граф типов выделов территории;
- 7) создать прогнозную тематическую карту - схему распределения лесов по классам влажности почв.

Исследуемая территория находится в центрально-юго-западной части острова Соловецкого. Ширина составляет примерно 2,3 км, длина – 2,5 км. На ней находится 188 лесотаксационных выделов.

С помощью классификации, позволяющей отразить мозаичность природных параметров, его гомогенные, гетерогенные особенности и произвести типизацию гетерогенных территориальных единиц по признаку структурного подобия, на основе матрицы исходных данных была составлена легенда, отражающая структуру и динамику леса [2]. В программе QGIS была оцифрована лесоустроительная карта. Выделы были пронумерованы и раскрашены в соответствии с номерами легенды.

На основе легенды был составлен структурно-динамический граф типов выделов. В центре его находятся коренные леса, в средней части – квазикоренные, во внешнем круге – болота. С помощью графа можно проследить процесс восстановления коренных лесов, а также установить, как изменяется тип леса при изменении влажности.

Была составлена тематическая карта распределения лесов по классам влажности почв и прогнозная (если уровень грунтовых вод поднимется на 1 м) тематическая карта распределения лесов по классам влажности почв.

Итак, были выполнены все поставленные задачи. Цель работы была достигнута.

СПИСОК ЛИТЕРАТУРЫ

1. Ковин Р. В. Геоинформационные системы: учебное пособие / Р. В. Ковин, Н. Г. Марков. – Томск: Изд-во Томского политехнического университета, 2008. – 175 с.
2. Кобелева Н.В. Крупномасштабное эколого-фитоценотическое картографирование на основе аэроснимков и ГИС-технологий (на примере центральной части Тазовского полуострова) // Известия Самарского научного центра РАН, 2012. – Т. 14. – №1(6). – С. 1607-1617.

УДК 681

ИНФОРМАЦИОННАЯ И ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ПРИРОДНОЙ СРЕДЫ

Павлова Светлана Михайловна

Смольный университет Российской академии образования

Россия, Санкт-Петербург, Полюстровский пр.59

emails: spavlova222@mail.ru

Аннотация: Актуальность задачи качества жизни человека и информационной безопасности определяет особую важность обеспечения объективности и достоверности получаемой в процессе мониторинга информации. Ведь любое решение становится полезным и оптимальным, только когда оно основано на объективных и достоверных данных. Эта проблема понимается на сегодняшний день широким кругом ученых и практиков, связанных с философскими, математическими и информационными вопросами природоохранной и природопользовательской деятельности. Для более общих задач статистического мониторинга свойств сложного объекта, ориентированного на его специфику.

Ключевые слова: экология, экспертная система; информационная безопасность; ноосфера, биосфера, мониторинг.

INFORMATION AND ECOLOGICAL SECURITY OF ENVIRONMENT

Pavlova Svetlana Michailovna

Smolny university of the Russian Academy of Education

Russia, St. Petersburg, Polyustrovsky Ave 59,

emails: spavlova222@mail.ru

Abstract: Relevance of a problem of quality of human life and information security defines special importance of ensuring objectivity and reliability of information received in the course of monitoring. After all, any decision becomes a useful and optimal one only when it is based on some objective and reliable information. This problem refers to a wide range of scholars and practitioners associated with the philosophical, mathematical and informational issues on environmental and natural activities for more general problems of statistical monitoring of the properties of a complex object.

Keywords: ecology, expert system, information security, monitoring, noosphere, biosphere.

Введение. В настоящее время чрезвычайно важными и актуальными становятся проблемы информационных технологий, связанные с экологической безопасностью. Концепция экологической безопасности, сформулированная Н.Ф. Реймерсом, связывает допустимые темпы преобразования окружающей среды со способностью человека адаптироваться к новым экологическим факторам. В

мире в целом необходимо в первую очередь стимулировать работы по своевременной компенсации пагубного влияния негативных тенденций информатизации на здоровье человека и формирующиеся черты молодого поколения. Кроме того, научное направление развития информационного общества поможет определить приоритеты в инвестиционной политике, в модернизации образования и других сферах [1].

Поэтому, сохранение и нормальное функционирование нашей планеты первую очередь определяется иерархией сложнейших информационных связей. В значительной степени идет попытка осмысления реалий информатизации общества и нового научного направления – информационной и экологической безопасности, развитие информационного общества. Усложнение его инфраструктуры требует тщательного и продуманного управления ресурсами, овладения новыми средствами и методами обработки информации. Наиболее значимыми областями являются геоинформационные системы, системы подготовки и обработки анализа данных, моделирование природных и техногенных процессов.

В настоящее время геоинформационные системы активно используются для решения научных и практических задач: включая информационную безопасность, обеспечение безопасности качества жизни человека и т.д. Поэтому взрыв интереса к геоинформационным системам, стремительность их внедрения, различная сфера применения, стратегическое значение геоинформатики дают ей право претендовать на место одной из наиболее перспективных информационных технологий. В настоящее время исследуются проблемы, связанные с сущностью экологической информации, анализируется метод моделирования, как один из информационных методов обеспечения управления охраной окружающей среды экологический мониторинг. Дается оценка геоинформационных технологий как одного из основных средств обработки экологической информации и формирования единого экологического информационного пространства. Неотъемлемым атрибутом современного технологического производства является требование контроля за влиянием на окружающую среду, социальной и экологической ответственностью предприятий [2].

Сегодня сложилась качественно иная ситуация: накопленных знаний в целом столько, что их невозможно освоить не только отдельному человеку, но и научному сообществу. Вместе с тем информационные технологии в экологии делают каждый фрагмент знания общедоступным. Изменения задачи, стоящей перед институтом, повлечет за собой новые и качественные изменения информационных технологий и методов ориентации в информационном пространстве. Сведения об антропогенном факторе влияния на вид, учитываемые ЭС «АССИСТЕНТ-БИОЛОГ», можно разделить на две большие группы. Это - антропогенная нагрузка на среду обитания и антропогенная нагрузка на популяцию. Антропогенная нагрузка на среду обитания включает сведения об антропогенном разрушении среды обитания вида — вырубке лесов, распашке земель, химическом, радиационном и ином загрязнении этой среды, интродукции чуждых данной местности видов (биологическое загрязнение) и о последствиях этого загрязнения (сужение кормовой базы, исчезновение водных источников, изменения в отношениях конкуренции). Антропогенная нагрузка на популяцию — это, в основном, охота, так как ЭС «АССИСТЕНТ-БИОЛОГ» предназначена для мониторинга популяций, прежде всего, промысловых животных. Может включаться в этот раздел и информация о гибели животных от дорожно-транспортных происшествий, от применения ядохимикатов в сельском и лесном хозяйстве и т. п. Конечно, если антропогенное влияние не только негативно, а включает в себя также и охрану, лимитирование промысла, зимнюю подкормку, те или иные приемы восстановления среды обитания (лесонасаждение, например) — эти сведения также должны входить в характеристику антропогенного фактора.

Закключение. Разработка концепций ноосферной экологии, связана с генетической безопасностью населения, особенно актуальна в условиях кардинальной перестройки общества с информационной экологической безопасностью. Сейчас задача состоит прежде всего в том, чтобы выработать новую комплексную интегрированную систему охраны биосферы и уже на ее основе осуществлять более разумный дифференцированный подход к вопросам применения информационных технологий в экологии. Фундаментальные процессы обеспечивающие природное равновесие связаны с определенными потоками вещества и энергии через все уровни биосферы. Конечно, ноосферная идея и биосфера имеют характеристику, направленную на консолидацию и усложнение. Для построения информационного общества необходимы кардинальные изменения в культуре, чтобы посредством информационного образования изменить сознание и мировоззрение людей. Победа разума — это единственный выход для человечества.

СПИСОК ЛИТЕРАТУРЫ

1. Мэгарран Э. Экологическое разнообразие и его измерение. — М.: Мир, 1992.- 368 с.
2. В.Е. Болтнев Экология.- Издательство : ТНТ 2012.- 352. — ISBN9785941782581

УДК 528.94

СТРУКТУРНАЯ МОДЕЛЬ ЮЖНОЙ ЧАСТИ БОЛЬШОГО СОЛОВЕЦКОГО ОСТРОВА

Позднякова Виктория Владимировна
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский проспект, 49,
email: viktoriya.17@mail.ru

Аннотация: В статье представлена структурная модель южной части Большого Соловецкого острова. Для этого было проведено математическое районирование, а также найдены коэффициенты гетерогенности для выделенных профилей.

Ключевые слова: южная часть Большого Соловецкого острова, профиль, математическое районирование, коэффициент гетерогенности, коэффициент гомогенности.

STRUCTURAL MODEL OF THE SOUTHERN PART OF THE GREAT SOLOVETSKY ISLAND

Pozdniakova Viktoriia
Saint Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University),
Russia, St. Petersburg, Kronverkskyavenue 49,
email: viktoriya.17@mail.ru

Abstract: the article presents a structural model of the southern part of the Great Solovetsky Island. For this, mathematical zoning was carried out, and also the heterogeneity coefficients for the selected profiles were found.

Keywords: southern part of the Great Solovetsky Island, profile, mathematical zoning, heterogeneity coefficient, homogeneity coefficient.

Введение. Соловецкие острова — федеральное государственное учреждение культуры, один из крупнейших музеев-заповедников России. Составление структурной модели для Большого Соловецкого острова еще не проводилось. В своей работе я рассматривала южную часть Большого Соловецкого острова.

Целью работы являлось - выявить структурные особенности южного участка Большого Соловецкого острова.

В задачи входило: выделить 4 района на южном участке Соловецкого острова в зависимости от структуры; получить пространственные характеристики выделенных районов; найти коэффициенты гетерогенности.

Для составления структурной модели природной среды было выделено 4 обособленных элементарных (для данного уровня организации информации) однородных по определенному признаку или набору признаков природных объектов, характеризующихся присущими им природными особенностями, географической привязкой [2]. Далее проводилось математическое районирование. Затем – составление матриц анализируемых данных и просчет их по алгоритму региональной классификации с целью выделения системы региональных природных единиц. После составления матрицы и нахождения мер сходства были найдены соотношения площадей по профилям и их сравнение.

На первом этапе были выделены следующие профили: район 1 западная часть южной части Большого Соловецкого острова, район 2 середина южной части Большого Соловецкого острова, район 3 восточная часть и район 4 – южная, мыс Печак.

После проведения математического районирования и составления матриц, были найдены меры сходства: для районов 1-2 коэффициент меры сходства = 0,1; 1-3 коэффициент меры сходства = 0,7; 1-4 коэффициент меры сходства = 0,2; 2-3 коэффициент меры сходства = 0,03; 2-4 коэффициент меры сходства = 0,5; 3-4 коэффициент меры сходства = 0,4. Исходя из полученных данных, самый высокий коэффициент гетерогенности между 1 и 3 районами, что отражает их структурное сходство, а самый низкий между 2 и 3 районами.

В результате были получены пространственные характеристики выделенных районов. Район 1 характеризуется большим количеством пустошей и каменистыми россыпями; район 2 характеризуется верховыми сфагновыми болотами; район 3 характеризуется как березово-сосновый долгомошный лес; район 4 как березовый лес.

СПИСОК ЛИТЕРАТУРЫ

1. Ковин Р. В. Геоинформационные системы: учебное пособие / Р. В. Ковин, Н. Г. Марков. – Томск: Изд-во Томского политехнического университета, 2008. – 175 с.
2. Кобелева Н.В. Крупномасштабное эколого-фитоценотическое картографирование на основе аэроснимков и ГИС-технологий (на примере центральной части Тазовского полуострова)//Известия Самарского научного центра РАН, 2012. – Т. 14. – №1(6). – С. 1607-1617.

УДК 631.445:631.415:632.122:632.125 +502.55:504.05

МОДЕЛЬ ФОРМИРОВАНИЯ ОЦЕНКИ АДДИТИВНОГО ЭКОЛОГИЧЕСКОГО УЩЕРБА ОТ ОБЪЕКТОВ ПРОШЛОГО ЭКОЛОГИЧЕСКОГО УЩЕРБА

Романюк Людмила Павловна, Петухов Валерий Васильевич
Санкт-Петербургский научно-исследовательский центр экологической безопасности
Российской академии наук,
Россия, Санкт-Петербург, Корпусная ул., 18,
email: lpr53@mail.ru

Аннотация: В составе современных проблем экологической безопасности территорий и регионов существенное значение имеют объекты прошлого (накопленного) экологического ущерба (ПЭУ). Действующие методы оценки воздействия таких объектов на геосистемы практически не учитывают геоэкологические особенности природно-хозяйственных систем и синергетическое взаимодействие всех типов воздействий. При этом, ни один из показателей состояния не может полностью отражать экологическую ситуацию, поскольку экологический эффект зависит от устойчивости экосистем к этим типам воздействий. Также существует вероятность взаимной компенсации некоторых измеряемых показателей.

Ключевые слова: *прошлый экологический ущерб; природно-хозяйственные системы; экосистемы; ГИС-технологии; моделирование*

MODEL FOR COMPLEX ASSESSMENT OF ENVIRONMENTAL DAMAGE FROM BROWNFIELDS

Romanjuk Ludmila, Petukhov Valery
Saint-Petersburg Research Center for Ecological Safety RAS
Russia, St-Petersburg, Korpusnaya st., 18,
email: lpr53@mail.ru

Abstract: Ecological damage from brownfields is a significant part of the modern environmental problems. Currently used methods for impact assessment of such objects on geosystems practically do not consider geoecological features of natural-economic systems and synergetic interaction of different types of influences. At the same time, none of indexes of a state cannot reflect completely an ecological situation as its ecological effect depends on resistance of ecosystems to these types of influences. Also there is a probability of a cancellation of indexes.

Keywords: *accumulated ecological damage; natural-economic systems; ecosystems; GIS-technologies; simulation*

Введение. Проблема типологии, оценки и устранения ПЭУ как элемент обеспечения экологической безопасности обладает высшим приоритетом административно-территориальных образований. Однако до сих пор отсутствуют проектно-методические основы и апробированные способы для оценок уровней экологической опасности ПЭУ и подбора адекватных инженерно-экологических мероприятий по его ликвидации.

До сих пор адекватная эколого-экономическая оценка объектов ПЭУ ограничивается формализованным составом показателей категоризации, не учитывающих геоэкологические особенности природно-хозяйственных систем, в которых расположены такие объекты, а критерием экологического состояния природных сред, как известно, служит преимущественно комплекс пространственных и динамических показателей - нормативов загрязнений.

Существующие математические методы анализа экологических данных основаны на гипотезах об определенных свойствах наборов данных и поэтому применимы только для решения частных задач и не решают задачу отбора наиболее информативных показателей в целом. В связи с этим в настоящее время являются актуальными задачи разработки новых методов анализа имеющихся экологических данных исследуемой территории.

Заключение. Задачами исследований было:

- изучение системных связей между элементами ПЭУ различной типологии, характерных типов негативного влияния в специфических геоэкологических условиях геосистем и природно-хозяйственных систем;
- разработка критериальной базы параметров ПЭУ;
- разработка модели информационной системы для оценки синергетического экологического ущерба и формирования перечня мероприятий по его ликвидации.

Исследованы геосистемы с накопленным экологическим ущербом как особая разновидность природно-техногенных систем, которые организованы в виде множества территориальных объектов различной размерности.

Разработана методика выделения репрезентативных показателей на основе графоаналитической модели при комплексной оценке и картографировании экологического состояния территорий средствами геоинформационных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Петухов В.В., Питулько В.М., Кулибаба В.В. Инвентаризация региональных объектов прошлого экологического ущерба / Региональная экология. 2016. № 4 (46). С. 71-79
2. Кулибаба В. В., Петухов В. В., Зинатулина Е. И., Меринова Е. С. Рекультивированные карьеры Приневской низменности — специфическая разновидность объектов накопленного экологического ущерба / Региональная экология, 2016, № 1 (43). С. 108-114.

УДК 551.501.45

ПРИМЕНЕНИЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ В ЦЕЛЯХ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ, ДЕЯТЕЛЬНОСТИ СИЛОВЫХ СТРУКТУР И ОТРАСЛЕЙ ЭКОНОМИКИ РОССИИ

Тимошук Александр Сергеевич, Доронин Александр Павлович, Калустов Ярослав Игоревич
Военно-космическая академия имени А.Ф.Можайского,
Россия, Санкт-Петербург, ул. Красного курсанта, 16
email: astim2@yandex.ru

Аннотация: В статье рассмотрены вопросы применения беспилотных летательных аппаратов (БПЛА) в целях повышения качества оперативного информационного обеспечения экологической безопасности деятельности силовых структур и отраслей экономики России. Обоснована актуальность использования БПЛА в задачах экологического контроля военных объектов.

Ключевые слова: беспилотные летательные аппараты, экологическая безопасность, окружающая среда, информационное обеспечение.

THE USE OF DRONES FOR INFORMATION SUPPLY OF ECOLOGICAL SAFETY ACTIVITIES, LAW ENFORCEMENT AGENCIES AND BRANCHES OF THE RUSSIAN ECONOMY

Timoshchuk Aleksandr, Doronin Aleksandr, Kalustov Yaroslav
Military Space academy named after A. F. Mozhayskiy,
Russia, St. Petersburg, Krasnogo kursanta st., 16
email: astim2@yandex.ru

Abstract: the article considers about the development drones to the problem of environmental safety activities of law enforcement agencies and branches of the Russian economy. Relevance of use drones in the problems of ecological monitoring military objects.

Keywords: drones, ecological safety, environment, monitoring, information assurance.

Введение. В настоящее время уровень развития методов и технических средств информационного обеспечения экологической безопасности (ИОЭБ) позволяет решать большой объем задач по наблюдению, оцениванию и прогнозированию последствий деятельности силовых структур и отраслей экономики России на окружающую среду [1]. Однако, выполнение регламентированной руководящими документами задачи по оцениванию экологической обстановки использованием контактных средств ИОЭБ может оказаться невозможным или неэффективным по соображениям оперативности и безопасности. В таких ситуациях целесообразно использование дистанционных средств ИОЭБ, в частности использование беспилотных летательных аппаратов.

Вопросы применения БПЛА в целях повышения качества оперативного информационного обеспечения экологической безопасности деятельности силовых структур и отраслей экономики России.

Основными техническими средствами (ТС) дистанционного ИОЭБ являются ТС дистанционного зондирования Земли (ДЗЗ), устанавливаемые на космических аппаратах (КА) и авиационные ТС, устанавливаемые как на пилотируемых летательных аппаратах (самолетах, вертолетах, аэростатах), так и на различных типах БПЛА [2]. Данные космического ИОЭБ позволяют получать наиболее оперативные и крупномасштабные сведения о состоянии окружающей среды и решать большой перечень экологических задач. Наиболее эффективными для осуществления ИОЭБ в интересах ВС РФ являются КА с ТС ДЗЗ оптико-электронного (или) радиолокационного диапазонов. Однако, возможности ИОЭБ данным космического ДЗЗ в оперативной обстановке обладают рядом существенных недостатков, способных негативно влиять на скорость и правильность принятия решения. По сравнению с космическими ТС ДЗЗ более высокой оперативностью обладают ТС ИОЭБ, используемые в пилотируемой авиации. Однако и авиационные ТС ИОЭБ обладают рядом недостатков (необходимость согласования с надзорными органами использование авиационных средств, большие экономические затраты на материально-технические и людские ресурсы, высокая зависимость от метеорологических условий, высокие риски потери личного состава и техники при осуществлении ИОЭБ в зонах военных (боевых) действий).

По сравнению с использованием ТС ИОЭБ пилотируемой авиации, использование беспилотных авиационных средств лишено большинства этих недостатков. Прогресс в развитии новых

конструкционных материалов, силовых установок, источников питания, микроэлектроники и информационных технологий обеспечил возможность применения беспилотной авиации для решения обширного круга востребованных задач, где использование ТС космических аппаратов или ТС пилотируемой авиации экономически нецелесообразно или практически невозможно. Кроме того, в настоящее время ряд БПЛА принят на вооружение в силовых структурах РФ, где они широко и успешно применяются в целях разведки, координации и других военных задач, что делает БПЛА наиболее перспективной платформой для ИОЭБ при минимальных затратах и позволяет своевременно реагировать на экстремальные ситуации в сложных погодных условиях или в труднодоступной местности. Время необходимое для подготовки аппарата к повторному запуску в большинстве случаев не превышает 25 минут, что удовлетворяет критерию непрерывности наблюдения. Из выше перечисленного следует, что по сравнению с традиционными средствами воздушного наблюдения (самолетами и вертолетами) БПЛА имеют ряд существенных преимуществ: низкие капитальные и эксплуатационные затраты, высокая мобильность и полная автономность, отсутствие риска для личного состава, простота эксплуатации. Так же следует отметить, что для ИОЭБ могут использоваться БПЛА двойного назначения, выполняющие иные основные задачи (разведка, координирование).

Закключение. Таким образом, применение технологий БПЛА весьма актуально для ИОЭБ деятельности силовых структур и отраслей экономики России, для чего рекомендуется использовать первую очередь штатные БПЛА, оснастив их соответствующими ТС и программным обеспечением ИОЭБ.

СПИСОК ЛИТЕРАТУРЫ

1. Шмалько С.А., Доронин А.П., Петроченко В.М., Тимошук А.С. Основные причины, обуславливающие необходимость организации и проведения экологического мониторинга в районах деятельности Вооруженных Сил Российской Федерации // Труды II Всероссийской научной конференции «Экология и космос» имени академика К.Я. Кондратьева. – СПб.: ВКА им. А.Ф. Можайского, 2015. – С. 281–286.
2. Шмалько С.А., Доронин А.П., Петроченко В.М., Тимошук А.С. Существующие и перспективные средства сбора и обработки экологической информации в интересах экологической безопасности деятельности Вооруженных Сил Российской Федерации // Труды II Всероссийской научной конференции «Экология и космос» имени академика К.Я. Кондратьева. – СПб.: ВКА им. А.Ф. Можайского, 2015. – С. 286–291.

УДК 621.384.3:528.74

ЭКОЛОГИЧЕСКАЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕПЛОВОГО АВИАЦИОННОГО МОНИТОРИНГА САНКТ-ПЕТЕРБУРГА

Шилин Борис Владимирович

Научно-исследовательский центр экологической безопасности РАН,
Россия, Санкт-Петербург, Корпусная ул., 18
email: bshilin@rambler.ru

Аннотация: В Санкт-Петербурге уделяется большое внимание вопросам загрязнения водных объектов, в том числе реки Невы. Периодически проводится авиационный мониторинг сбросов сточных вод в акваторию р. Невы и Невской губы. технические средства и методика тепловой аэросъемки могут быть успешно реализованы в любом регионе РФ с большими площадями водных объектов.

Ключевые слова: тепловая аэросъемка, сбросы сточных вод.

ECOLOGICAL AND INFORMATION SECURITY OF THERMAL AERIAL MONITORING OF SAINT PETERSBURG

Shilin Boris

Scientific-Research Centre for Ecological Safety RAS,
Russia, Saint-Petersburg, Korpusnaya st., 18
email: bshilin@rambler.ru

Abstract: In St. Petersburg, much attention is paid to the problem of water pollution, including area of the Neva river. Monitoring based on the aerial survey of wastewater discharges in the Neva river and the Gulf of Finland is carried out periodically. The developed technique of thermal aerial survey can be successfully applied in any region of Russian Federation with the big areas of water objects.

Keywords: thermal aerial survey, sewage discharge.

Тепловая аэросъемка в режиме мониторинга города эффективно применяется при решении задач экологической безопасности акваторий и системы теплоснабжения. Используются отечественные авиационные серийные тепловизоры. Аэросъемка акваторий выполнялась в 1990, 2002, 2009–2010 гг. В каждом случае составлялись карты-схемы источников загрязнений их каталоги. В 1990 году было обнаружено более 320 источников (сбросов), в 2002 году – 66 и в 2009–2010 гг. – 74. Всё это свидетельствует о существенном сокращении антропогенной нагрузки на акватории и эффективности природоохранных работ «Водоканала-СПб».

Впервые тепловая аэросъемка теплосетей примерно для половины площади города была выполнена в 1986 году. И сразу было обнаружено более двухсот аномалий. Бала осуществлена их классификация, соответствующие их каталоги были переданы службам эксплуатации. После перерыва 1990-х гг. с 2002 года начались регулярные аэросъемки южной части города на площади около 229 кв. км. Составлялись тепловые карты, карты аномалий на теплотрассах и каталоги аномалий, привязанных к карте. До 2014 года аэросъемка проводилась семь раз. Существенно повысилась целенаправленность и эффективность ремонтных работ, появилась возможность осуществлять объективный контроль путём сравнения результатов залётов разных лет. Последнее показало, что среднее число аномалий на теплосетях – 250-300 – не уменьшается: одни устраняются, другие появляются, особенно на старых сетях.

Информационная безопасность материалов тепловой аэросъемки обеспечивается конфиденциальностью данных местоположения объектов против несанкционированного вмешательства в их функционирования.

СПИСОК ЛИТЕРАТУРЫ

1. Гаврилов Д.С., Шилин Б.В. Мониторинг загрязнений акваторий с помощью авиационного тепловизионного комплекса // Оптический журнал. 2004. Т. 71. № 3. С.77-82.
2. Шилин Б.В., Молодчинин И.А. Контроль состояния окружающей среды тепловой аэросъемкой. -М: Недра, 1992. -76 с.
3. Тронин А.А., Шилин Б.В. Мониторинг шлейфов городских очистных сооружений Санкт-Петербурга аэрокосмической тепловой съёмкой // Современные проблемы дистанционного зондирования земли из космоса. 2008. №5. Том 2. С. 586-594.

УДК 742.012

МОДЕРН УМЕРЕННОГО ПЛАНА

Ярошевич Людмила Ивановна

Санкт-Петербургский государственный институт кино и телевидения,
Россия, Санкт-Петербург, ул. Правды, 13,
email: ludmila-arttech@rambler.ru

Аннотация: В статье рассмотрено подчиненное положение стиля Модерн по отношению к Классицизму с точки зрения аудиовизуального восприятия единой системы стилей. Подчеркивается значение зрелого Классицизма и Ампира в формировании композиционного центра, создающего интенсивное, контрастное восприятие в сравнении Модерном.

Ключевые слова: экология, аудиовизуальное восприятие; стилевое моделирование; аналогии представления данных; образовательные программы

MODERN OF MEDIUM PLAN

Yaroshevich Ludmila Ivanovna

The St. Petersburg state institute of film and television
Russia, St. Petersburg, Pravda str.13,
email: ludmila-arttech@rambler.ru

Abstract: The article presents the subordination of art Nouveau in relation to Classicism. Visible analogies in presentation of the data. It underlines importance of Mature Classicism and Empire in the formation of a composite centre of the city.

Keywords: ecology, the analogies of data presentation; audiovisual perception; the subordination of art Nouveau in relation to Classicism; the value of Mature Classicism and Empire in the formation of a composite centre of the city; educational program

Введение. Система аудиовизуального восприятия человека - одна на все случаи получения и передачи информации. Поэтому есть смысл говорить о композиции картинной плоскости градостроительного плана, по аналогии с правилами представления данных в живописи, графике, архитектурном стилевом дизайне, музыке, литературе и т.д. К моменту возникновения Модерна центры городов были уже сформированы в предыдущие эпохи. Например, "Архитектура зрелого классицизма и Ампира отличалась укрупнением масштаба городских ансамблей", что позволяет и сегодня считать их композиционными центрами, возведенными на интенсивном контрасте с последующей застройкой городских пространств, а Модерн считать иерархически соподчиненным по отношению к ним. Кстати говоря, итальянское слово *moderato*, означает умеренный темп в музыке.

Как изменялся архитектурный стилевой дизайн в конце XIX начале XX вв. Модерн в переводе с французского языка означает – современный. Что означало быть современным в начале XX века?

Безусловно, технический прогресс, модернизированное оборудование, новые материалы использовались в строительстве зданий. Все это уже описано в литературе по искусствоведению.

С началом массового строительства городское пространство постепенно уплотнялось. Архитектурный образ, в виде отдельно стоящего здания или ансамбля становился все менее актуальным. В то же время развивалось пространство улиц, линейное пространство. Время диктовало

к нему новые требования. Здания выстраивались в ряд, вдоль улицы. Нужно было иметь чувство меры, особую деликатность, чтобы не превышать "пределы" декоративно-художественной общности фасадов. К примеру, современники критиковали Павла Сюзора за излишества декора в оформлении здания Кредитного банка на Екатерининском канале (ныне канал Грибоедова).

"Впервые после долгих лет забвения была увидена и осознана ценность иерархически построенной, композиционно завершенной структуры классических российских городов, и в первую очередь Петербурга с его великолепными дворцово-парковыми ансамблями" – пишет доктор архитектуры, профессор Т. А. Славина, подчеркивая необходимость рассматривать архитектурные представления данных с точки зрения визуального восприятия [1].

Приближение фасадов к визуальному восприятию частично лишило зрителя естественного открытого пространства. Возникшие экологические проблемы "заставили человека", моделировать, т.е. превращать фасады зданий в картинные плоскости, на которых возникал образ мира. Эстетика городского пространства это – не только приятный глазу декор-украшение. Главная причина возникновения дизайна в городской среде – необходимость создать условия для фиксации и рассеяния внимания в искусственной среде. А это, уже вопрос безопасности. Всякая фиксация внимания, пройдя необходимый цикл развития, должна заканчиваться рассеиванием внимания.

В заключение следует сказать о том, что просматриваются аналогии в области представления данных, связанные с аудиовизуальным восприятием. Подчеркивается необходимость соблюдения иерархической системы, потому что она более всего соответствует естественному восприятию информации человеком. В процессе совершенствования технологий образования, улучшения качества рабочих программ, при практическом осуществлении имитационного моделирования, следует учитывать законы восприятия.

СПИСОК ЛИТЕРАТУРЫ

1. История русской архитектуры: Учебник для вузов// Пилявский В.И., Славина Т.А., Тиц А.А., Ушаков Ю.С., Заушкевич Г.В., Савельев Ю.Р. - Издание второе, переработанное и дополненное - Санкт-Петербург, Стройиздат, СПб, 1994, 525с.
2. Ярошевич Л.И. Изображения - фазовые диаграммы аудиовизуального восприятия. Материалы XXIII международной научно-методической конференции "Современное образование: содержание, технологии, качество", "ЛЭТИ", 21 апреля 2017, т.1, 299с.



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИОКОМПЬЮТИНГЕ

УДК 004.05

ПОДХОД К ПОСТРОЕНИЮ СИСТЕМЫ УПРЕЖДАЮЩЕЙ ДИАГНОСТИКИ УЯЗВИМОСТЕЙ ПЕРСОНАЛА К СОЦИОИНЖЕНЕРНЫМ АТАКАМ

Абрамов Максим Викторович

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Россия, Санкт-Петербург, 14 линия, 39

Санкт-Петербургский государственный университет,

Россия, Санкт-Петербург, Петергоф, Университетский пр-кт, 28,

email: mva16@list.ru

Аннотация: На основании анализа фрагментов профилей уязвимостей пользователей и информации об их уровне доступа к критическим элементам информационной системы становится возможным автоматизировать разработку комплекса рекомендаций для лиц, принимающих решения в отношении укрепления информационной безопасности организаций и их информационных систем в срезе социоинженерных угроз.

Ключевые слова: социоинженерные атаки; информационная безопасность; защита пользователя; защита информации; система упреждающей диагностики.

APPROACH TO THE CONSTRUCTION OF THE DETERMINING DIAGNOSTIC SYSTEM OF PERSONNEL VULNERABILITY TO SOCIAL ENGINEERING ATTACKS

Abramov Maksim

St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,

Russia, St. Petersburg, 14 Line, 39,

Saint-Petersburg University,

Russia, St. Petersburg, Peterhof, Universitetsky prosp. 28,

email: mva16@list.ru

Abstract: Based on the analysis of fragments of profiles of user vulnerabilities and information on their level of access to critical elements of the information system, it becomes possible to automate the development of a set of recommendations for decision-makers in strengthening information security of organizations and their information systems in the context of socio-engineering threats.

Keywords: social engineering attacks; information security; user protection; information protection; predictive diagnostics system.

Введение. В последнее время атаки на информационные системы стали происходить чаще, приносить большие убытки и требовать больше ресурсов и времени для установления виновных в подобных преступлениях. Статистика инцидентов нарушения информационной безопасности последних лет демонстрирует тенденцию к стремительному росту не только убытков компаний и затрат ресурсов на расследование подобных преступлений, но и к росту доли инцидентов, связанных с социоинженерными атаками [1–7,11]. Проблемы анализа защищённости пользователей информационных систем от социоинженерных атак, выявления сотрудников компании, наиболее уязвимых к подобным воздействиям, принятия оперативных решений, способствующих минимизации вероятности успеха атаки, а значит и к нивелированию рисков утечки конфиденциальной информации, стоят сегодня особенно остро, что отмечается экспертами в области информационной безопасности, а также представителями компаний, ставших жертвами кибератак [10, 12]. Данный тезис описывает постановку задачи построения систем упреждающей диагностики уязвимостей персонала к социоинженерным атакам и подходы к её решению.

Для построения систем упреждающей диагностики уязвимостей персонала к социоинженерным атакам необходимо решить задачу выявления пользователей, наиболее уязвимых к социоинженерным атакующим воздействиям. Для этого на основе формализации моделей комплекса «критичные документы – информационная система – пользователь – злоумышленник», где информационная система представлена в виде графа с узлами, отвечающими программно-техническим компонентам системы и пользователям, а ребра — связям между программно-техническими компонентами,

пользователями и между компонентами и пользователями, будут строиться фрагменты профилей уязвимостей пользователей [8, 9]. Для имитации социоинженерных атакующих воздействий будут использованы модернизированные методы теории графов, теорий вероятностных графических моделей, сэмпирования по Гиббсу. На основе этих оценок будут предлагаться рекомендации для лиц, принимающих решения.

Заключение. Полученные результаты позволят существенно повысить уровень защиты пользователей информационной системы от социоинженерных атак злоумышленников за счёт повышения эффективности и адресности применения профилактических мер. Разработанная система автоматической или автоматизированной подготовки рекомендаций по повышению уровня защищённости критических документов будет способствовать оперативности и корректности принятия решений уполномоченными лицами.

СПИСОК ЛИТЕРАТУРЫ

1. 2012 Cost of Cyber Crime Study: United States, Ponemon Institute, October 2012. P. 30. URL: http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf
2. 2013 Cost of Cyber Crime Study: United States, Ponemon Institute, October 2013. P. 30. URL: http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf
3. 2014 Cost of Cyber Crime Study: United States, Ponemon Institute, October 2014. P. 30. URL: http://resources.idgenterprize.com/original/AST-0130677_2014_US_Cost_of_Cyber_Crime_Study_FINAL_2.pdf
4. 2015 Cost of Cyber Crime Study: United Kingdom, Ponemon Institute, October 2015. P. 31. URL: <http://cybersecuritysummit.co.uk/wp-content/uploads/2015/06/2015-UK-CCC-FINAL-3.pdf>
5. 2016 Cost of Cyber Crime Study & the Risk of Business Innovation: Global, Ponemon Institute, October 2016. P. 37. URL: <http://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf>
6. First Annual Cost of Cyber Crime Study, Ponemon Institute, July 2010. P. 23. URL: http://www.greycastlesecurity.com/resources/documents/Ponemon_Cost_of_CyberCrime_Study_07-10.pdf
7. Second Annual Cost of Cyber Crime Study, Ponemon Institute, August 2011. P. 30. URL: http://www.ponemon.org/local/upload/file/2011_2nd_Annual_Cost_of_Cyber_Crime_Study%20.pdf
8. Абрамов М.В., Азаров А.А., Тулупьева Т.В., Тулупьев А.Л. Модель профиля компетенций злоумышленника в задаче анализа защищённости персонала информационных систем от социоинженерных атак // Информационно-управляющие системы. 2016. №4. С. 77–84.
9. Азаров А.А., Тулупьева Т.В., Суворова А.В., Тулупьев А.Л., Абрамов М.В., Юсупов Р.М. Социоинженерные атаки. Проблемы анализа. СПб.: Наука, 2016. 352 с.
10. Блинкова О. Среднегодовой убыток от киберпреступности составил для российских компаний \$2,4 млн // IT News. Октябрь 2015. #10(242)
11. Информационная безопасность бизнеса. Исследования текущих тенденций в области информационной безопасности бизнеса // Лаборатория Касперского. http://media.kaspersky.com/pdf/IT_risk_report_Russia_2014.pdf (дата обращения: 30.08.2017)
12. Юзбекова И. Сбербанк оценил годовой ущерб России от киберпреступлений в \$1 млрд [Электронный ресурс]// РБК.-2015. (09.12.2015).- URL: http://www.rbc.ru/technology_and_media/09/12/2015/566837819a7947e4cbc991b6 (дата обращения: 15.01.2016)

УДК 004.8

ПОСТРОЕНИЕ СТРАТЕГИИ ЗАЩИТЫ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ СОЦИОИНЖЕНЕРНЫХ АТАКУЮЩИХ ВОЗДЕЙСТВИЙ ЗЛОУМЫШЛЕННИКА

Азаров Артур Александрович¹, Хлобыстова Анастасия Олеговна²

¹ Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14 линия, 39

² Санкт-Петербургский государственный университет,
Россия, г. Санкт-Петербург, Петергоф, Университетский пр., 28
emails: artur-azarov@yandex.ru, Hastia0698@yandex.ru.

Аннотация: Возможность разбиения пользователей на группы, основывающиеся на оценке степени уязвимости, полученной при помощи цифровых отпечатков.

Ключевые слова: социоинженерные атаки, цифровые следы.

CONSTRUCTION OF THE STRATEGY FOR THE PROTECTION OF USERS OF INFORMATION SYSTEMS FROM THE SOCIAL ENGINEERING ATTACKS

Artur Azarov¹, Khlobystova Anastasia²

¹ St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,
Russia, St. Petersburg, 14 Line, 39,

² Saint-Petersburg State University,
Russia, St. Petersburg, Peterhof, Universitetsky prosp. 28,
emails: artur-azarov@yandex.ru, Hastia0698@yandex.ru

Abstract: The ability to split users into groups based on vulnerability assessment obtained with the help of digital fingerprints.

Keywords: social engineering attacks, digital footprint.

Одним из негативных итогов повсеместной информатизации современного общества является повышение количества киберпреступлений. При этом, программно-технические уязвимостями не всегда являются первопричинами утечки конфиденциальной информации. Исследования в области информационной безопасности [1, 2] показывают рост инцидентов безопасности, связанными с компрометацией пользователей информационных систем через применение злоумышленниками социинженерных атакующих воздействий.

Очевидным решением для борьбы с подобными атакующими воздействия злоумышленника является обучение сотрудников организации. Вместе с тем, для снижения затрат организации, заказывающей обучение сотрудников, могут быть использованы методы построения профиля уязвимостей пользователя на основании степени выраженности психологических особенностей личности [3, 4]. Данный подход позволяет выявить наименее защищенных пользователей, основные особенности пользователей, которые влияют на уязвимости и могут быть использованы злоумышленником для реализации социинженерных атакующих воздействий. Таким образом, могут быть разработаны индивидуальные траектории обучения пользователей, что приведет к существенному повышению индивидуальной защищенности пользователей, и, как следствие, к повышению защищенности информационной системы в целом.

Делая вывод, необходимо отметить, что обеспечение безопасности информационной системы не сводится исключительно к реализации всех возможных технических средств защиты. Обучение пользователей и защита их от возможных социинженерных атакующих воздействий злоумышленника также имеет существенное влияние на общий уровень защищенности информационных систем.

СПИСОК ЛИТЕРАТУРЫ

1. 2015 Cost of Cyber Crime Study: United Kindom, Ponemon Institute, October 2015. P. 31. URL: <http://cybersecuritysummit.co.uk/wp-content/uploads/2015/06/2015-UK-CCC-FINAL-3.pdf>
2. 2016 Cost of Cyber Crime Study & the Risk of Business Innovation: Global, Ponemon Institute, October 2016. P. 37. URL: <http://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf>
3. Абрамов М.В., Азаров А.А., Тулупьева Т.В., Тулупьев А.Л. Модель профиля компетенций злоумышленника в задаче анализа защищенности персонала информационных систем от социинженерных атак // Информационно-управляющие системы. 2016. №4. С. 77–84.
4. Азаров А.А., Тулупьева Т.В., Суворова А.В., Тулупьев А.Л., Абрамов М.В., Юсупов Р.М. Социинженерные атаки. Проблемы анализа. СПб.: Наука, 2016. 352 с.

УДК 004.05

АНАЛИЗ ПРОФИЛЕЙ СОЦИАЛЬНОЙ СЕТИ В КОНТЕКСТЕ СОЦИОИНЖЕНЕРНЫХ АТАК

Багрецов Георгий Игоревич

Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия, 39,
email: gbagretsov@gmail.com

Аннотация: В существующей модели пользователя, основанной на оценке степени выраженности его уязвимостей, предполагается, что все данные, необходимые для построения профиля уязвимостей, необходимо получать посредством анкетирования. В данном докладе рассмотрены различные подходы к автоматизации оценки психологического профиля пользователя социальных сетей. Решение этой задачи позволит значительно упростить и ускорить построение профиля уязвимостей пользователя информационной системы.

Ключевые слова: социинженерные атаки; информационная безопасность; уязвимость пользователя; профиль уязвимостей пользователя; анализ социальных сетей

SOCIAL NETWORK PROFILES ANALYSIS IN THE CONTEXT OF SOCIO-ENGINEERING ATTACKS

Bagretsov Georgiy

St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences,
14-th Linia, VI, No. 39, St. Petersburg, 199178, Russia,
email: gbagretsov@gmail.com

Abstract: In the existing model of user that is based on the evaluation of his or her vulnerabilities severity, it is assumed that all the data needed to build a vulnerabilities profile is obtained via surveys. In this research, various approaches to automating the evaluation of social networks user's psychological profile are considered. Solving this problem will significantly simplify and speed up the construction of the users vulnerabilities profiles.

Keywords: social engineering attacks; informational security; user vulnerability; user vulnerabilities profile; social networks analysis

В настоящее время анализу защищенности пользователей информационных систем от социотехнических (социинженерных) атак уделяется крайне мало внимания. Однако, различные исследования показывают, что наиболее распространённые инциденты информационной

безопасности тесно связаны с манипулятивными воздействиями на человека [1, 5]. Этот факт обуславливает необходимость в разработке специальных моделей и методов, использующихся в целях защиты пользователей от манипулятивных воздействий, а также для получения различного рода рекомендаций по обеспечению безопасности.

Одной из разработанных ранее моделей является модель пользователя, основанная на его уязвимостях и психологических характеристиках [2]. В предыдущих исследованиях было установлено, что существует зависимость степени выраженности той или иной уязвимости пользователя от его психологического портрета. Однако, не было построено способа эффективно и достоверно построить такой портрет. Все данные, необходимые для корректной оценки, необходимо получать посредством анкетирования пользователей, что может требовать большого количества времени и других ресурсов.

В данной работе представлен подход к автоматизированному построению психологического профиля пользователя информационной системы на основе анализа информации его профиля в социальных сетях, поскольку в современном мире социальные сети являются кладью полезной информации о человеке, о его интересах, увлечениях, действиях [4]. Ранее для решения этой задачи были предприняты попытки использовать текстовую информацию [3]. Однако для наиболее полной и правдоподобной картины необходимо анализировать информацию различного рода: текстовую, аудиовизуальную, а также мета-информацию. Для каждого типа информации следует разработать отдельные методы ввиду разнородности данных. Планируется использовать различные методы решения задачи, в частности широкий спектр методов машинного обучения.

СПИСОК ЛИТЕРАТУРЫ

1. Kevin D. Mitnick and William L. Simon. The art of deception: Controlling the human element of security. John Wiley & Sons, 2011.
2. А.А. Азаров, Т.В. Тулупьева, А.В. Суворова, А.Л. Тулупьев, Абрамов М.В., Р.М. Юсупов. Социоинженерные атаки: проблемы анализа. Наука, СПб, 2016.
3. Г.И. Багрецов, Т.В. Тулупьева. Классификация текстовых записей по степени выраженности психологических особенностей // Всероссийская научная конференция по проблемам информатики «СПИСОК-2017», Санкт-Петербург, 25–27 апреля 2017 года
4. Екатерина Фролова. Самые популярные социальные сети в России 2016. URL: <http://www.pro-smm.com/populyarnye-socialnyeseti-v-rossii-2016/>.
5. Информационная безопасность бизнеса. Исследования текущих тенденций в области информационной безопасности бизнеса // Лаборатория Касперского. URL: http://media.kaspersky.com/pdf/IT_risk_report_Russia_2014.pdf (дата обращения: 20.09.2017).

УДК 004.942

УСЛОВИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КЛИНИЧЕСКОЙ СФЕРЕ СИСТЕМЫ ЗДРАВООХРАНЕНИЯ

Блюм Владислав Станиславович

Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия, 39,
email: vlad@blum.spb.su

Аннотация: В статье рассмотрены условия информационной безопасности пациентов, которая обеспечивается новой организацией цифровой клинической медицинской информации и достижением ею свойств полноты, достоверности и доступности для автоматизированной обработки. Рассмотрена телекоммуникационная структура единой государственной информационной системы здравоохранения, обеспечивающей сбор и сохранение полного объема первичной медицинской информации. Предложена динамическая информационная (математическая) модель полной, достоверной и доступной для автоматизированной обработки первичной медицинской информации. Модель описывает процесс сбора электронных персональных медицинских записей и формирования федеральной базы интегрированных электронных медицинских карт.

Ключевые слова: информационная безопасность пациентов; электронная персональная медицинская запись; интегрированная электронная медицинская карта.

CONDITIONS OF INFORMATION SECURITY IN THE CLINICAL SPHERE HEALTH SYSTEMS

Blum Vladislav

St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,
Russia, St. Petersburg, 14 Line, 39
email: vlad@blum.spb.su

Abstract: The article considers the information security conditions for patients, which is provided by a new organization of digital clinical medical information and the achievement of its completeness, reliability and accessibility features for automated processing. The telecommunication structure of the unified state health information system providing collection and preservation of the full volume of primary medical information is considered. A dynamic information (mathematical) model of complete, reliable and accessible for automated

processing of primary medical information is proposed. The model describes the process of collecting electronic personal medical records and the formation of a federal database of integrated electronic medical records.

Keywords: *information safety of patients; electronic personal medical record; integrated electronic medical record.*

Введение. Информационная безопасность пациентов складывается из гарантированного сбора и непрерывного автоматического контроля полной интегрированной цифровой истории болезни пациента для раннего обнаружения дефектов оказания медицинской помощи.

Предложена математическая модель формирования динамической базы интегрированных электронных медицинских карт (ИЭМК). Рассмотрены некоторые алгоритмы непрерывного мониторинга ИЭМК с целью управления лечебно-диагностическим процессом.

Заключение. «Цифровая» медицина создаёт новые, принципиально иные информационные условия для управления лечебно-диагностическим процессом на основе формирования полного информационного медицинского портрета пациента и его непрерывного анализа с учётом реального времени.

СПИСОК ЛИТЕРАТУРЫ

1. Блюм В.С., Заболотский В.П. Мысленный эксперимент по организации учета и обработки информационных медицинских услуг. Врачи и информационные технологии, №4 2009. С.27–35
2. Tarakanov A. O., Skormin V. A., Sokolova S. P. Immunocomputing: Principles and Applications. New York.: Springer, 2003, 230 p.
3. Блюм В.С., Заболотский В.П. Иммунная система и *иммунокомпьютинг*. Математическая морфология. Электронный математический и медико-биологический журнал (том 6 выпуск 4, 2007). Зарегистрировано 29.01.2008 под номером 0420700004/0039.
4. Блюм В.С. Инновационная государственная система медицинской статистики. АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЭКОНОМИКИ И УПРАВЛЕНИЯ. 2015.- 80-88 с.

УДК 004.05

ПОДХОД К ПОСТРОЕНИЮ ПРОФИЛЯ КОМПЕТЕНЦИЙ ЗЛОУМЫШЛЕННИКА В ЗАДАЧЕ АНАЛИЗА ЗАЩИЩЁННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОТ СОЦИОИНЖЕНЕРНЫХ АТАК

Бушмелев Федор Витальевич¹, Абрамов Максим Викторович^{1,2}

¹ Санкт-Петербургский государственный университет,

Россия, Санкт-Петербург, Петергоф, Университетский пр-кт, 28,

² Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Россия, Санкт-Петербург, 14 линия, 39

emails: fedebushe@gmail.com, mva16@list.ru

Аннотация: В последнее время прослеживается тенденция активного роста количества успешных инцидентов социоинженерных атак. Чтобы оценить вероятность успеха социоинженерного атакующего воздействия необходимо агрегировать существенное количество факторов. Одним из таких факторов выступает оценка потенциального злоумышленника. Данная статья посвящена проблеме оценки потенциального злоумышленника через построение его профиля компетенций.

Ключевые слова: *социоинженерные атаки; информационная безопасность; защита пользователя; защита информации; профиль компетенций злоумышленника.*

APPROACH TO THE BUILDING OF THE ATTACKER COMPETENCIES PROFILE IN THE PROBLEM OF THE PROTECTION OF THE INFORMATION SYSTEM FROM SOCIAL ENGINEERING ATTACKS

Bushmelev Fedor¹, Abramov Maksim^{1,2}

¹ Saint-Petersburg University,

Russia, St. Petersburg, Peterhof, Universitetsky prosp. 28,

² St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,

Russia, St. Petersburg, 14 Line, 39,

emails: fedebushe@gmail.com, mva16@list.ru

Abstract: Recently, there has been a trend of active growth in the number of successful incidents of socio-engineering attacks. To assess the probability of success of a socio-engineered attack, it is necessary to aggregate a significant number of factors. One of these factors is the evaluation of a potential attacker. This article is devoted to the problem of assessing a potential attacker through the construction of his competence profile.

Keywords: *social engineering attacks; information security; user protection; information protection; attacker's competencies profile;*

Введение. Информационные технологии сегодня являются неотъемлемой частью жизнью современного человека. Ежедневно люди взаимодействуют с большим количеством информационных

систем: на работе, на учебе, в магазинах, дома и т.д. Такое глубокое внедрение в нашу жизнь помимо предоставляемых возможностей несет в себе множество рисков, в частности, связанных с обеспечением информационной безопасности. Отметим, что исследования в области защиты информации ведутся давно, получены существенные результаты, позволяющие снижать вероятность успеха атаки злоумышленника. Но большая часть этих результатов относится к защите информационных систем от программно-технических атак [7, 8]. Но, к сожалению, несмотря на это, компании продолжают терпеть большие убытки от инцидентов, связанных с компрометацией информационных систем. Информация о таких инцидентах часто освещается в СМИ [1-3]. Сложившаяся ситуация отчасти объясняется тем, что различные отрасли обеспечения информационной безопасности развивались неравномерно. Социальные аспекты защищенности изучены слабо, в отличие от аппаратно-технических. Таким образом исследования в области обеспечения защиты пользователей от социоинженерных атак являются актуальными.

Одна из задач обеспечения защиты пользователей информационной системы от социоинженерных атак заключается в анализе степени защищенности. Для решения этой задачи предлагается набор моделей «критичные документы — информационная система — персонал — злоумышленник» [4–6]. Наиболее проработанной в этом комплексе является модель персонала. Тем не менее помимо оценки пользователей информационной системы важно иметь представление о потенциальных злоумышленниках. Основу модели злоумышленника представляет модель профиля компетенций злоумышленника. Для построения профиля компетенций злоумышленника предлагается подход, состоящий из трёх этапов, представленных ниже.

Этап 1. По модели пользователя строится граф, корнем которого являются «критичные документы». Потомки корневого элемента — пользователи, имеющие к критичным документам доступ, их потомки — сотрудники, тесно связанные с первыми и т.д.

Этап 2. Производится обход графа в глубину. Такой выбор обоснован тем, что при проходе облегчаются вычисления, когда у сыновей имеется общий внук. В каждом узле высчитывается/обновляется запись с информацией о компетенциях злоумышленника. Если узел имеет несколько сыновей, то создается дополнительная запись для каждой новой ветки.

Этап 3. Для записей, имеющих одинаковые конечные узлы, производится объединение и далее осуществляется многофакторная комбинация всех записей, для составления общего представления о компетенциях злоумышленника.

Заключение. Таким образом мы имеем подход к построению профиля компетенций злоумышленника, основанный на информации из модели пользователя. Отметим, что представленный подход обладает высокой вычислительной сложностью и требует больших объемов памяти. Планируется его модернизацию и улучшение.

СПИСОК ЛИТЕРАТУРЫ

1. Phil Muncaster. UK Fraud Attacks Hit 20 Million in Q2. [Электронный ресурс] // URL: <https://www.infosecurity-magazine.com/news/uk-fraud-attacks-hit-20-million-in/> (дата обращения 14.09.2017)
2. Виктория Чернышева. Вирус Gooligan взломал миллион аккаунтов Google. [Электронный ресурс] // URL: <https://rg.ru/2016/12/01/virus-gooligan-vzломal-million-akkauntov-google.html> (дата обращения 13.09.2017)
3. Номер мобильного телефона Макрона слили в сеть. [Электронный ресурс] // URL: <https://lenta.ru/news/2017/09/18/macronportable/> (дата обращения 20.09.2017)
4. Абрамов М.В., Азаров А.А., Тулупьева Т.В., Тулупьев А.Л. Модель профиля компетенций злоумышленника в задаче анализа защищенности персонала информационных систем от социоинженерных атак // Информационно-управляющие системы. 2016. №4. С. 77–84.
5. Азаров А.А., Тулупьева Т.В., Суворова А.В., Тулупьев А.Л., Абрамов М.В., Юсупов Р.М. Социоинженерные атаки. Проблемы анализа. СПб.: Наука, 2016. 352 с.
6. Багрецов Г.И., Шиндарев Н.А., Абрамов М.В., Тулупьева Т.В. Подходы к автоматизации сбора, структурирования и анализа информации о сотрудниках компании на основе данных социальной сети. // Труды VII всероссийской научно-практической конференции «Нечёткие системы, мягкие вычисления и интеллектуальные технологии» HCMBIT–2017 (г. Санкт-Петербург, 3–7 июля, 2017 г.). — в 2 т. Т. 1. — СПб.: Политехника-сервис, 2017. С. 9–16
7. Котенко И. В., Степашкин М. В. Перспективные направления исследований в области компьютерной безопасности. // Защита информации. 2006. № 2. С. 46–57.
8. Котенко И. В., Степашкин М.В., Богданов В.С. Системы-имитаторы: назначение, функции, архитектура и подход к реализации. // Изв. вузов. Приборостроение, Т. 49. 2006. №3. С. 3–8.

УДК 004.056

ПРИМЕНЕНИЕ МЕТОДОВ DATA MINING ДЛЯ ПОЛУЧЕНИЯ ИНФОРМАЦИИ О ПОЛЬЗОВАТЕЛЯХ СОЦИАЛЬНЫХ СЕТЕЙ

Зегжда Дмитрий Петрович, Лемец Андрей Александрович, Павленко Евгений Юрьевич
Санкт-Петербургский политехнический университет Петра Великого,
Россия, Санкт-Петербург, ул. Политехническая, 29,
emails: dmitry.zegzhda@ibks.ftk.spbstu.ru, a.a.lemets@gmail.com, pavlenko@ibks.spbstu.ru

Аннотация: Описаны подходы к получению информации о пользователях социальных сетей с использованием методов интеллектуального анализа данных. Разработана иерархическая модель

классификации получаемых данных, описывающая извлекаемую информацию из социальных сетей. Она позволяет определить, какие алгоритмы следует использовать для определенного класса информации, а также понять взаимодействие между этими классами. Предложен подход, основанный на итеративном методе глубокого поиска, интеллектуального анализа и выявления информации о владельце учетной записи. Данный подход использует разработанные алгоритмы анализа социального графа, идея которых заключается в кластеризации и дальнейшем анализе сообществ пользователей внутри него, идентификации пользователей разных социальных сетей, анализе текстовой информации, а также использовании поисковых машин и ресурсов сети Интернет.

Ключевые слова: интеллектуальный анализ данных; социальные сети; социальный граф; анализ социальных данных.

USING DATA MINING METHODS FOR OBTAINING INFORMATION ABOUT USERS IN SOCIAL NETWORKS

Zegzhda Dmitry, Lemets Andrey, Pavlenko Evgeny
Peter the Great St.Petersburg Polytechnic University,
Russia, St.Petersburg, Polytechnicheskaya, 29,

emails: dmitry.zegzhda@ibks.ftk.spbstu.ru, a.a.lemets@gmail.com, pavlenko@ibks.spbstu.ru

Abstract: This article describes the developed approaches for obtaining information about social networks' users based on methods of data mining. Particular attention is devoted to the hierarchical model for classification of the received data, which describes the information extracted from social networks. This model allows choosing which algorithms should be used for a particular class of information. The proposed approach implies an iterative deep searching method, intellectual analysis and revealing information about account owner identity using the developed algorithms for social graph analysis. The idea of the algorithm is to cluster and further analyze user communities within social graph, identify users on different social networks, analyze text information. It is also described an algorithm of using search engines and Internet resources.

Keywords: data mining; social networks; social graph; social mining.

Введение. Одним из основных направлений для борьбы терроризмом является противодействие терроризму в сети Интернет, поскольку террористические организации для вербовки своих сторонников по всему миру активно используют социальные сети, мессенджеры и другие средства взаимодействия и распространения информации между людьми.

По словам главы Антитеррористического центра стран, входящих в Содружество Независимых Государств, А. Новикова, с 2014 по 2017 год количество публикаций с экстремистским содержанием в Интернете возросло более чем в шесть раз. При этом выявление и блокировка учетных записей вербовщиков не приносят никаких результатов, поэтому наиболее эффективным средством противодействия террористам является выявление вербуемых пользователей и оперативное установление личности владельцев данных учетных записей с использованием информации, указанной в профиле социальной сети.

Определение информации о владельце учетной записи является одной из основополагающих проблем анализа социальных данных. Например, в работе [1] автор предлагает несколько алгоритмов по выявлению схожих признаков пользователей социальных сетей, а также алгоритм, позволяющий определить город пользователя социальной сети Facebook. Для решения этой задачи автор разработал модель определения местоположения владельца профиля и его друга, которая позволяет повысить точность определяемого местоположения. Это вероятностная модель, которая рассматривает два основных источника географической информации: список атрибутов профиля, указанных в биографии, например, школа или ВУЗ, а также информацию о пользователях, которые указаны в списке друзей. Идея алгоритма состоит в том, чтобы рассматривать изучаемого пользователя и каждого из его друзей. Основным недостатком рассмотренного метода является то, что он использует только информацию, указанную в профиле, что сильно ограничивает количество данных, которые можно получить о пользователе с помощью социальной сети.

В работе [2] авторы предлагают анализировать текстовую информацию с целью выявления связи между субъектами в социальной сети. Авторы анализируют информацию только между двумя субъектами, не учитывая других пользователей. Хотя, чаще всего, связь объединяет сообщество людей, что повышает точность информации, полученной при анализе именно сообщества людей.

Существует также большое количество работ, например, [3], [4], [5] в которых рассматриваются методы получения интересов пользователей на основе их социальных профилей, с целью таргетированного продвижения товаров и услуг группам с требуемыми параметрами, к которым могут относиться пол, возраст, уровень образования, политические взгляды. Данная информация не позволяет произвести идентификацию владельца учетной записи, в отличие, например, от места работы, жительства или учебных заведений, которые он окончил. К тому же, возникающие ошибки слабо влияют на полученный результат, в отличие от ошибок, возникающих при идентификации пользователя.

Авторами данной работы предлагается итеративный метод интеллектуального поиска, анализа и выявления скрытой информации о пользователе с использованием его профилей в социальных сетях, а также другой информации, которую можно получить с использованием открытых источников.

Для обработки полученной информации была разработана иерархическая модель классификации данных, представляющая их как множество явной и косвенной информации. Явная информация – это множество векторов, содержащих сведения со страницы пользователя, которые необходимо подтвердить, поскольку могут быть несоответствия с реальной информацией. Косвенная информация – множество векторов, содержащих сведения, которые требуют дополнительного анализа. Формальная задача анализа – построить отображение из множества косвенной информации во множество явной информации.

Косвенная информация представляет собой подмножество других пользователей и групп, а также медиаконтент, текстовую информацию и указания на другие ресурсы сети Интернет. Для того, чтобы учитывать связи между получаемой информацией, она проецируется на ориентированный граф.

Для извлечения фактов из неструктурированного текста используется парсер, который включает в себя токенизатор, сегментатор и морфологический анализатор, для которого были разработаны грамматики, позволяющие извлекать из текста ФИО, даты, аббревиатуры и названия, а также номера групп и классов. Для повышения точности, после извлечения информация соотносится с множеством уже обработанной информации.

После получения информации осуществляется построение социального графа. Выделив в нем сообщества и используя эвристическое предположение о том, что члены сообществ связаны некоторыми общими признаками, такими как место учебы, работы или общими интересами, происходит их поиск и восстановление. Также осуществляется поиск дополнительной информации в сети Интернет, который на данном этапе включает в себя обработку текстовой информации с сайтов учебных заведений.

Для идентификации учетных записей пользователей в разных социальных сетях используется проекционная модель, основанная на анализе информации и связей с другими пользователями. Модель применима в том случае, если есть члены сообществ, указавшие ссылки на профили в других социальных сетях.

Заключение. Предложенный метод позволяет осуществлять поиск, анализ и выявление скрытой информации о пользователе с использованием его профилей в социальных сетях, а также других сведений, полученных с использованием открытых источников. Таким образом, разработанный подход является эффективным средством для оперативного установления данных о владельцах учетных записей социальных сетей.

СПИСОК ЛИТЕРАТУРЫ

1. Han X. Mining user similarity in online social networks: analysis, modeling and applications: дис. – Evry, Institut national des télécommunications, 2015. Яз. англ.
2. J. Mori, T. Tsujishita, Y. Matsuo, M. Ishizuka. Extracting relations in social networks from the web using similarity between collective contexts. – Proceedings of the 5th International Semantic Web Conference, 2006. 14 с.
3. Tang J., Aggarwal C., Liu H. Recommendations in signed social networks //Proceedings of the 25th International Conference on World Wide Web. – International World Wide Web Conferences Steering Committee, 2016. – С. 31-40.
4. He J., Chu W. W. A social network-based recommender system (SNRS). – Springer US, 2010. – С. 47-74.
5. Campbell W. M., Dagli C. K., Weinstein C. J. Social network analysis with content and graphs //Lincoln Laboratory Journal. – 2013. – Т. 20. – №. 1. – С. 62-81.

УДК 004.04

СИНТЕЗ ТРЕТИЧНОЙ СТРУКТУРЫ АЛГЕБРАИЧЕСКОЙ БАЙЕСОВСКОЙ СЕТИ НА БАЗЕ ОРИЕНТИРОВАННОГО ГРАФА ВТОРИЧНОЙ СТРУКТУРЫ

Золотин Андрей Алексеевич

Санкт-Петербургский государственный университет,
Россия, Санкт-Петербург, Университетская набережная, 7–9,

Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия В.О., 39,
emails: andrey.zolotin@gmail.com

Аннотация: Алгебраические байесовские сети являются одним из классов вероятностных графических моделей. В статье рассмотрен алгоритм синтеза третичной структуры алгебраической байесовской сети по вторичной структуре, представляемой графом смежности. Детализированы основные шаги алгоритма и дано описание операций, производимых на каждом из шагов. Предложенный алгоритм позволяет генерировать третичную структуру алгебраической байесовской сети, используемую как в алгоритмах логико-вероятностного вывода, так и в задачах, связанных с обучением иных видов глобальных структур. Особенностью рассматриваемого алгоритма является то, что он использует направленный граф вторичной структуры.

Ключевые слова: вероятностные графические модели, алгебраические байесовские сети, третичная структура, синтез структур, машинное обучение, экспертные системы.

SYNTHESIS OF ALGEBRAIC BAYESIAN NETWORK TERTIARY STRUCTURE BASED ON SECONDARY STRUCTURE DIRECTED GRAPH

Zolotin Andrey

St. Petersburg State University,
Russia, St. Petersburg, University emb. 7-9
St. Petersburg Institute for Informatics and Automation of the RAS,
Russia, St. Petersburg, 14 line V.O., 39,
emails: andrey.zolotin@gmail.com

Abstract: The article Algebraic Bayesian networks are one of the classes of probabilistic graphical models. The report considers algorithm for synthesis of the tertiary structure of an algebraic Bayesian network with respect to a secondary structure represented by an adjacency graph. The main steps of the algorithm are provided in details and a description of the operations performed at each step is given. The proposed algorithm generates a tertiary structure of an algebraic Bayesian network, used both in algorithms of probabilistic-logic inference and in problems related to the global structures learning. A specialty of the considered algorithm is that it uses a directed graph of the secondary structure.

Keywords: probabilistic graphical models, algebraic Bayesian networks, tertiary structure, structure learning, machine learning, expert systems.

Введение. Алгебраические байесовские сети (АБС), предложенные в конце прошлого века профессором В.И. Городецким [1], являются вероятностной графической моделью родственной байесовским сетям доверия(БСД). Однако, в отличие от БСД модель АБС предоставляет возможность обработки интервальных оценок вероятностей, что создает задел для работы с нечеткими(неполными) данными. Одним из важнейших аппаратов, определенных над АБС является совокупность алгоритмов синтеза глобальных структур, включающая как алгоритмы синтеза конкретного графа смежности, так и алгоритмы синтеза множества всех возможных представителей выбранной структуры. В данной работе мы будем использовать терминологию и устоявшийся в рамках теории алгебраических байесовских сетей математический аппарат [2].

Алгоритмы, предложенные А.А. Фильченковым [3] и развитые в работах на базе лаборатории ТИМПИ СПИИРАН [4], подразумевают работу с множествами сепараторов и вершин именно как с множествами, не делая большой упор на графовую составляющую. Кроме того, прямой и жадный алгоритмы могут давать различные результаты в разные проходы алгоритмы из-за неупорядоченности формируемого множества вершин минимального графа смежности. В связи с этим в данной работе предлагается рассмотреть следующий подход, более полагающийся на графовую составляющую. Ниже приведем последовательность шагов алгоритма для формирования минимального графа смежности АБС.

1. Сформировать множество вершин вторичной структуры АБС и отсортировать их по убыванию нагрузок;

2. Задать направление ребрам графа вторичной структуры, основываясь на правиле, что каждое ребро направлено от той вершины, нагрузка которой стоит पहले в отсортированном массиве нагрузок (иначе говоря, от вершины с большей нагрузкой к вершине с меньшей нагрузкой);

3. Взять из массива нагрузок(вершин) первую вершину и добавить ее в МГС. Затем добавить все вершины, к которым идут исходящие ребра из данной вершины;

4. Повторить шаг (3) для вершин, добавленных только что в МГС и добавить в МГС все вершины, к которым идут исходящие ребра из данных вершин. При добавлении вершины в МГС стоит отмечать ее в графе маркером "included", позволяющим избежать добавления излишних ребер в МГС. Данный шаг повторяется до тех пор, пока из любой вершины, добавленной в МГС не будет выходить ни одного ребра;

Наконец взять следующую вершину из массива с вершинами еще не добавленную в МГС и повторить для нее алгоритм, начиная с шага номер (3)

Заключение. Результатом данного алгоритма будет являться МГС, так как на каждом шаге мы добавляем в структуру МГС вершину и ребро только в том случае, если данная вершина была ранее недостижима. Алгоритм можно варьировать за счет пропуска шага (4) и переходу сразу к шагу (5) — в данном случае граф смежности может формироваться несвязным подграфами, которые в определенный момент соединятся. Предложенный алгоритм развивает теорию алгебраических сетей в частности и вероятностных графических моделей в целом. На основании программной реализации алгоритма планируется провести сравнительный статистический анализ времени работы алгоритмов генерации МГС.

СПИСОК ЛИТЕРАТУРЫ

1. Городецкий В.И. Алгебраические байесовские сети — новая парадигма экспертных систем // Юбилейный сборник трудов

- института Отделения информатики, вычислительной техники и автоматизации РАН. Т. 2. М.: РАН. 1993. С. 120–141.
2. Тулупьев А.Л., Николенко С.И., Сироткин А.В. Байесовские сети: логико-вероятностный подход. СПб.: Наука. 2006. 607 с.
 3. Фильченков А.А., Тулупьев А.Л., Сироткин А.В. Минимальные графы смежности алгебраической байесовской сети: формализация основ синтеза и автоматического обучения // Нечеткие системы и мягкие вычисления. 2011. Т. 6. № 2. С. 145–163.
 4. Зотов М.А., Левенец Д.Г., Тулупьев А.Л., Золотин А.А. Синтез вторичной структуры алгебраических байесовских сетей: инкрементальный алгоритм и статистическая оценка его сложности // Научно-технический вестник информационных технологий, механики и оптики. 2016. Т. 16. № 1. С. 122–132.

УДК 57.054

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ РЕЗОНАТОРОВ, ОБЕСПЕЧИВАЮЩИХ ЗАЩИТУ ОТ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

Копыльцов Александр Васильевич

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5,
email: kopyl2001@mail.ru

Аннотация: Рассмотрена задача математического моделирования взаимодействия резонаторов «АЙРЭС» с электромагнитным излучением. Резонатор «АЙРЭС» представляет собой кремниевую пластинку (диаметр 7,5 мм, толщина 1 мм), на которой методом травления по определенному алгоритму нанесены круговые щели (шириной 1 мкм и глубиной 1,2 мкм), рисунок которых выполнен на основе аффинных преобразований. Пластика изготавливается из кремния, текстолита и других диэлектриков. Линейные размеры пластики (диаметр, толщина) и щелей (ширина, глубина) могут достигать нескольких сантиметров и миллиметров, соответственно. При взаимодействии электромагнитного поля с резонатором наблюдается отражение, преломление и поглощение. При моделировании рассматривались различные варианты облучения. По длине волны расчеты проводились от долей микрометра до нескольких десятков сантиметров, т.е. от видимого света до радиоволн. Облучение осуществлялось как от дискретного количества источников (от одного до нескольких сотен), так и непрерывного (от пластин и полусфер). Если на пластинку падает волна с некоторой частотой, то результирующая волна, отходящая от пластики, представляет собой суперпозицию двух волн (за счет падающей волны и за счет слабо связанных электронов атомов пластики). Расчеты на компьютере показали, что результирующая волна имеет другие характеристики по сравнению с падающей волной (над центральной частью резонатора период колебаний увеличивается в 3,2 раза, а частота убывает в 3,2 раза), т.е., резонатор работает как преобразователь частоты электромагнитного излучения.

Ключевые слова: электромагнитное излучение; взаимодействие с веществом; математическое моделирование; защита от излучения.

MATHEMATICAL MODELING OF RESONATORS PROVIDING PROTECTION AGAINST ELECTROMAGNETIC RADIATION

Alexander Kopyltsov

Saint-Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str., 5,
e-mail: kopyl2001@mail.ru

Abstract: In the article the problem of mathematical simulation of the interaction of "AIRES" resonators with electromagnetic radiation is considered. Resonator "AIRES" is a silicon plate (diameter 7.5 mm, thickness 1 mm), on which etched by a certain algorithm, circular slots (1 μm wide and 1.2 μm deep), whose pattern is made on the basis of affine transformations. The plate is made of silicon, textolite and other dielectrics. Linear dimensions of the plate (diameter, thickness) and slits (width, depth) can reach several centimeters and millimeters, respectively. When the electromagnetic field interacts with the resonator, reflection, refraction and absorption are observed. Various types of irradiation were considered in the simulation. The wavelengths were calculated from micrometer fractions to several tens of centimeters, i.e. from visible light to radio waves. Irradiation was carried out both from a discrete number of sources (from one to several hundred), and continuous (from plates and hemispheres). If a wave with a certain frequency falls on the plate, then the resulting wave from the plate is a superposition of two waves (due to the incident wave and due to the weakly bound electrons of the plate atoms). Calculations on the computer showed that the resulting wave has other characteristics in comparison with the incident wave (the oscillation period increases 3.2 times, and the frequency decreases 3.2 times), that is, the resonator works as a frequency converter for electromagnetic radiation.

Keywords: electromagnetic radiation; interaction with matter; mathematical modeling; protection against radiation.

Рассмотрена задача математического моделирования взаимодействия резонаторов «АЙРЭС» с электромагнитным излучением [1], [2], [3], [4], [5], [6], [7], [8], [9], [10]. Резонатор «АЙРЭС» представляет собой кремниевую пластинку (диаметр 7,5 мм, толщина 1 мм), на которой методом травления по определенному алгоритму нанесены круговые щели (шириной 1 мкм и глубиной 1,2 мкм), рисунок которых выполнен на основе аффинных преобразований. Пластика изготавливается из кремния, текстолита и других диэлектриков. Линейные размеры пластики (диаметр, толщина) и щелей (ширина, глубина) могут достигать нескольких сантиметров и миллиметров, соответственно. При взаимодействии электромагнитного поля с резонатором наблюдается отражение, преломление и поглощение. По длине волны расчеты проводились от долей микрометра до нескольких десятков сантиметров, т.е. от видимого света до радиоволн. При моделировании рассматривались различные варианты облучения, как от дискретного количества источников (от одного до нескольких сотен), так и непрерывного (от пластин и полусфер). Если на пластинку падает волна с некоторой частотой, то результирующая волна, отходящая от пластики, представляет собой сумму двух слагаемых, образующихся за счет падающей волны и за счет слабо связанных внешних электронов атомов пластики. В экспериментах, проведенных на крысах линии Вистар, помещенных в клетку Фарадея и подвергнутых электромагнитному облучению с помощью Wi-Fi роутера, показано, что генетические характеристики крыс отличаются в зависимости от наличия или отсутствия резонаторов, а также от их количества расположенных на стенках клетки Фарадея и режимов облучения. Освещенность пластики, на которой размещены крысы, прямо пропорциональна интенсивности излучения и косинусу угла между нормалью к освещаемой поверхности и направлением падающего излучения и обратно пропорциональна квадрату расстояния от источника излучения до освещаемой пластики. Расчеты на компьютере показали, что если мощность источника равна 0,25 Вт (максимум 0,6 Вт) и расстояние от источника излучения до поверхности равно 0,5 м, то освещенность этой поверхности равна 0,1-0,2 лк. Если же на стороны клетки Фарадея повесить 4 резонатора, то освещенность поверхности увеличится примерно на 10 % на частоте падающего излучения и появится освещенность за счет отражения от резонаторов на частоте в 3,2 раза меньшей частоты падающего излучения. Математическая модель представлена в виде системы дифференциальных уравнений в частных производных. Рассматривались различные варианты граничных и начальных условий, в частности, без учета или с учетом взаимовлияния напряженности на резонаторе и в окружающем пространстве, наличие или отсутствие стоков в центре или по краям резонатора. Расчеты на компьютере показали, что результирующая волна имеет другие характеристики по сравнению с падающей волной. Например, над центральной частью резонатора возникает электромагнитная волна, изменяющаяся в пространстве и во времени, длина которой увеличивается в 3,2 раза, а частота убывает в 3,2 раза. Над другими частями резонатора тоже характеристики волн изменяются. Таким образом, резонатор работает как преобразователь частоты электромагнитного излучения, в частности, частота результирующего излучения уменьшается. Исходя из того, что меньшие частоты приносят меньше вреда живому организму, можно сделать вывод, что резонатор может использоваться как устройство обеспечивающее защиту от электромагнитного излучения. На основании экспериментальных данных и расчетов на компьютере можно прийти к выводу, что резонаторы «АЙРЭС» могут быть использованы для защиты людей от электромагнитных полей, что особенно актуально в больших городах и на производстве. Резонатор также можно использовать при разработке электронных замков, поскольку, подбирая материал резонатора, рисунок на поверхности резонатора и другие характеристики, можно получить на выходе определенную частоту излучения, если известны характеристики падающего излучения.

СПИСОК ЛИТЕРАТУРЫ

1. Серов И.Н., Лукьянов Г.Н., Копыльцов А.В. Безопасность электромагнитного излучения при его взаимодействии с самоаффинной поверхностью // Материалы IV Санкт-Петербургской межрегиональной конференции «ИБРР-2005». СПб: СПОИСУ. 14-16 июня, 2005, С.75.
2. Серов И.Н., Копыльцов А.В., Лукьянов Г.Н. Взаимодействие полупроводниковой пластины с самоаффинным рельефом поверхности с электромагнитным излучением // Нанотехника (инженерный журнал), 2006, № 4(8), С. 44-49.
3. Серов И.Н., Копыльцов А.В., Лукьянов Г.Н. Взаимодействие электромагнитного излучения с поверхностями с самоаффинным рельефом. // Белая книга «Исследования в области наночастиц, наноструктур и нанокompозитов в Российской Федерации», М: 2006, С.165-166.
4. Серов И.Н., Копыльцов А.В., Лукьянов Г.Н. Математическое моделирование взаимодействия электромагнитного излучения с кремниевой самоаффинной поверхностью. Материалы научн.-практ. конф. «Голография ЭКСПО-2006», М: 2006.
5. Копыльцов А.В., Серов И.Н., Лукьянов Г.Н. Математическое моделирование взаимодействия электромагнитного излучения с кремниевой самоаффинной поверхностью. Вестник ИНЖЕКОНА, серия «технические науки», 2007, С.199-205.
6. Kopyltsov A., Lukyanov G., Serov I. Coherent emission of Electromagnetic Radiation from the surface of semiconductor plate with the self-affine relief // The 3rd International IEEE Scientific Conference on Physics and Control (PhysCon 2007). September, 3rd-7th, Potsdam, Germany.
7. Kopyltsov A.V., Lukyanov G.N., Serov I.N. Modelling of the interaction between electromagnetic radiation and semiconductor silicon surface having affine relief // HoloExpo-2007, Moscow, Russia. P. 143-146.
8. Копыльцов А.В., Лукьянов Г.Н., Серов И.Н. Моделирование на кластере высокопроизводительных параллельных вычислений взаимодействия электромагнитного излучения с полупроводниковой пластинкой с самоаффинным рельефом. Материалы XII Санкт-Петербургской международной конференции «Региональная информатика - 2010», СПб: СПОИСУ, 2010, С.49.
9. Копыльцов А.В., Коршунов К.А., Лукьянов Г.Н., Серов И.Н. Распределенные вычисления взаимодействия электромагнитного излучения со структурированной поверхностью // Региональная информатика (РИ-2016). Юбилейная XV Санкт-

Петербургская международная конференция «Региональная информатика (РИ-2016)». Санкт-Петербург, 26-28 октября 2016 г.: Материалы конференции. \ СПОИСУ. – СПб, 2016. С. 526.

10. Копыльцов А.В., Коршунов К.А., Лукьянов Г. Н., Серов И.Н. Распределенные вычисления взаимодействия электромагнитного излучения со структурированной поверхностью // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 2 / СПОИСУ. – СПб., 2016. С. 383-387

УДК 57.054

АЛГОРИТМ ОЦЕНИВАНИЯ БЕЗОПАСНОСТИ ПОСТУПАЮЩЕЙ СЛАБО ФОРМАЛИЗОВАННОЙ ИНФОРМАЦИИ

Копыльцов Антон Александрович

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5,
email: kopyl2001@mail.ru

Аннотация: Рассмотрены проблемы безопасности при обработке слабо формализованной информации. Задача состоит в том, как неформализованную информацию формализовать таким образом, чтобы не исказить смысл и выявить какую-либо опасность, содержащуюся в слабо формализованной информации. Предполагается, что имеется объект наблюдения и система наблюдения, с большим количеством разнообразных датчиков. Объектом наблюдения может быть техническая система с установленными на ней датчиками, с которых снимается периодически слабо формализованная информация и обрабатывается. Система наблюдения включает в свой состав модули, например, модули ответственные за видеoinформацию, аудиoinформацию и другие. Система наблюдения и объект наблюдения могут работать без сбоев или со сбоями. Если система наблюдения работает без сбоев, то все в порядке. Если же в процессе работы системы появляются сбои, то систему нужно диагностировать. Исходными данными служат названия возможных неисправностей системы. Неисправности (выход из строя) модулей характеризуются конечным множеством признаков, представленных в виде набора вопросов, имеющих ответы либо «да», либо «нет». Алгоритм основан на том предположении, что вновь поступающая информация не должна в какой-то степени противоречить имеющейся информации, поступившей от разных модулей. Причины несоответствия поступающей информации имеющейся информации могут быть различными: либо сбой в системе (неисправность объекта наблюдения, датчиков, каналов связи и т.д.), либо целенаправленный вывод системы из строя, т.е. вредительство.

Ключевые слова: безопасность, слабо формализованная информация; обработка информации.

SAFETY ESTIMATION ALGORITHM THE ARRIVING WEAKLY FORMALIZED INFORMATION

Anton Kopyltsov

Saint-Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str., 5,
e-mail: kopyl2001@mail.ru

Abstract: In the article discusses security issues when processing weakly formalized information. The task is how to formalize information that has not been formalized in such a way as to not distort the meaning and reveal any danger contained in weakly formalized information. It is assumed that there is an observation object and a surveillance system, with a large number of different sensors. The object of observation can be a technical system with sensors installed on it, from which periodically weakly formalized information is removed and processed. The monitoring system includes modules, for example, modules responsible for video information, audio information and others. The surveillance system and the object of observation can work without failures or with failures. If the monitoring system works without failures, then everything is in order. If there are failures during the operation of the system, then the system needs to be diagnosed. The initial data are the names of possible system malfunctions. Failures of modules are characterized by a finite set of characteristics, represented as a set of questions with answers either "yes" or "no". The algorithm is based on the assumption that the incoming information should not to some extent contradict the available information received from the different modules. The reasons for the inconsistency of the incoming information of the available information can be different: either a failure in the system (failure of the object of observation, sensors, communication channels, etc.), or a purposeful system failure, i.e. sabotage.

Keywords: safety; weakly formalized information; data processing.

Формализованная информация может быть переведена в слабо формализованную с целью ее сокрытия, т.е. она будет доступна только тому, кому предназначена. Например, во многих языках используются иносказания, понятные только носителям языка. Фактически из формализованной информации делают неформализованную информацию. Задача состоит в том, как неформализованную информацию формализовать таким образом, чтобы не исказить смысл и выявить какую-либо опасность, содержащуюся в слабо формализованной информации [1], [2], [3], [4], [5], [6], [7],

[8], [9], [10]. Предполагается, что имеется объект наблюдения и система наблюдения, с большим количеством разнообразных датчиков. Объектом наблюдения может быть техническая система с установленными на ней датчиками, с которых снимается периодически слабо формализованная информация и обрабатывается. Система наблюдения и объект наблюдения могут работать без сбоев или со сбоями. Под сбоем понимаем ненормальную (неправильную) работу системы, т.е. когда система работает с ошибками. Прежде чем оценивать работоспособность объекта наблюдения необходимо убедиться, что система наблюдения работает удовлетворительно, т.е. слабо формализованная информация, поступающая с датчиков, достоверная. Система наблюдения включает в свой состав модули, например, модули ответственные за видеоинформацию, аудиоинформацию и другие. Количество и наименование модулей зависит от конкретной задачи. Если система наблюдения работает без сбоев, то все в порядке. Если же в процессе работы системы появляются сбои, то систему нужно диагностировать. Исходными данными служат названия возможных неисправностей системы. В начале работы системы можно использовать вероятности сбоев работы модулей. Эти вероятности могут быть определены на основе данных работы системы за предыдущий период, например, за прошедший год. Если же такая информация отсутствует, то можно считать, в первом приближении, что вероятности выхода из строя модулей одинаковые. Эти вероятности в процессе работы системы, при конкретных условиях будут, в случае необходимости, корректироваться. Неисправности (выход из строя) модулей характеризуются конечным множеством признаков, представленных в виде набора вопросов, имеющих ответы либо «да», либо «нет». Алгоритм основан на том предположении, что вновь поступающая информация не должна в какой-то степени противоречить имеющейся информации, которая поступила от разных модулей. То есть, если поступающая информация соответствует имеющейся информации, то уровень безопасности равен единице, а если она противоречит информации по нескольким модулям, то уровень безопасности равен отношению числа модулей с противоречивой информацией к числу всех модулей. Причины несоответствия поступающей информации имеющейся информации могут быть различными: либо сбой в системе (неисправность объекта наблюдения, датчиков, каналов связи, системы наблюдения и т.д.), либо целенаправленный вывод системы из строя, т.е. вредительство. Алгоритм включает 7 этапов: ввод данных, выбор вопроса, формирование нового списка неисправностей, выбор нового задаваемого вопроса, выбор исключаемых из списка вопросов, оценивание количества оставшихся неисправностей, коррекция вероятностей возникновения неисправностей. Если система работает без сбоев, то считается, что уровень безопасности равен единице. Если система работает неудовлетворительно, то выявляем с помощью алгоритма модули, которые не работают или работают неудовлетворительно, и определяем их количество. А именно, берем тесты, которые включают вопросы для нескольких модулей, и выявляем с помощью алгоритма модули, которые не прошли проверку и ранжируем их по количеству сбоев. После этого с помощью алгоритма определяем причину их неисправности. Это может быть либо сбой в системе, либо целенаправленный вывод системы из строя, т.е. вредительство. В этом случае безопасность меньше единицы.

СПИСОК ЛИТЕРАТУРЫ

1. Копыльцов А.А., Копыльцов А.В. Алгоритм обработки слабо формализованной информации, поступающей от технических систем // Известия СПбГЭТУ «ЛЭТИ» (известия государственного электротехнического университета), серия «Информатика, управление и компьютерные технологии». 2012. № 8. С. 30 – 36.
2. Копыльцов А.А. Модель классификации информации и алгоритм ее предварительной обработки для статических и динамических объектов // Известия СПбГЭТУ «ЛЭТИ» (известия государственного электротехнического университета), серия «Информатика, управление и компьютерные технологии». 2013. № 6. С. 134–139.
3. Копыльцов А.А. Программа для обработки слабо формализованной информации, поступающей от технических систем // Свидетельство о государственной регистрации программы для ЭВМ № 2013617310. Правообладатель: ФГБОУ ВПО «Санкт–Петербургский государственный электротехнический университет «ЛЭТИ» им В.И. Ульянова (Ленина)» (СПбГЭТУ). Заявка № 2013615041. Дата поступления 19 июня 2013 г. Дата государственной регистрации в Реестре программ для ЭВМ 08 августа 2013 г.
4. Копыльцов А.А., Копыльцов А.В. Обработка слабо формализованной информации, поступающей от технических систем // Вестник Нижневартского государственного гуманитарного университета. 2013. № 1. С. 32–36.
5. Копыльцов А.А. Алгоритм коррекции связей между фрагментами слабо формализованной информации и генерация новой информации // Вестник Нижневартского государственного университета. 2014. № 3. С. 28–34.
6. Копыльцов А.А., Копыльцов А.В. Обобщенный алгоритм обработки слабо формализованной информации и его применение // Вестник Нижневартского государственного университета. 2014. № 35. С. 35–44.
7. Копыльцов А.А. Обработка слабо формализованной информации в живых и технических системах // Материалы Всероссийской научно-практической конференции студентов, магистров, аспирантов «Современное программирование» (16–17 апреля 2014 г.). Нижневартск: Издательство Нижневартского государственного университета. 2014. С. 117–121.
8. Копыльцов А.А. Применение обобщенного алгоритма обработки слабо формализованной информации для управления неравновесной химической реакцией // Инженерный вестник Дона. 2015. № 1. ч.2. URL: ivdon.ru/ru/magazine/archive/n1p2y2015/2812
9. Копыльцов А.А. Обобщенный алгоритм обработки слабо формализованной информации и его приложения // Вестник Нижневартского государственного университета. 2015. № 5. С. 27–37.
10. Копыльцов А.А. Разработка параллельного алгоритма для обработки слабо формализованной информации // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 2 / СПОИСУ. – СПб., 2016. С. 378-381.

УДК 004.853

ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОПРЕДЕЛЕНИЯ АВТОМАТИЧЕСКИ УПРАВЛЯЕМЫХ УЧЕТНЫХ ЗАПИСЕЙ В СОЦИАЛЬНЫХ СЕТЯХ

Малышев Егор Валерьевич, Павленко Евгений Юрьевич, Зегжда Петр Дмитриевич
Санкт-Петербургский политехнический университет Петра Великого,
Россия, Санкт-Петербург, ул. ул. Политехническая, 29,
emails: egorpw@yandex.ru, jekon92@mail.ru

Аннотация: В статье рассмотрен способ применения искусственной нейронной сети, предназначенной для обнаружения автоматически управляемых учетных записей в социальных сетях.

Ключевые слова: защита информации; социальные сети; боты в социальных сетях; нейронная сеть; обнаружение ботов.

USE OF NEURAL NETWORK FOR DETECTION AUTOMATICALLY CONTROLLED ACCOUNTS IN SOCIAL NETWORKS

Malyshev Egor, Pavlenko Evgeniy, Zegzhda Peter
Peter the Great St. Petersburg Polytechnic University
Russia, St. Petersburg, Politehnicheskaya st., 29
emails: egorpw@yandex.ru, jekon92@mail.ru

Abstract: In the paper the problem of identifying automatically managed accounts (bots) in social networks, and provides a method of detection based on the application of machine learning methods.

Keywords: information security; social networks; bots in social networks; neural network; bot detection.

Введение. Социальные сети становятся одной из наиболее популярных площадок для общения по статистическим данным, более 30% населения планеты являются их активными пользователями. Социальные сети предлагают пользователю возможность коммуникации, средства для обмена знаниями и впечатлениями, а также служат источником новостей. Изначально социальные сети использовались как средство общения, нахождения новых знакомств, однако в настоящее время пользователи стремятся получить актуальную информацию на основе полученных данных. Люди регулярно заходят в социальные сети с целью получения новостей, информации о политической и экономической обстановке в стране и мире. На сегодняшний день одним из самых популярных методов общения социально и политически активных слоев населения являются социальные сети, при этом они предоставляют не только средства общения, но и возможность активного выражения своей позиции и обсуждения наиболее острых вопросов.

Стоит отметить тот факт, что большинство пользователей указывают на своей странице достоверную информацию о себе, такую как имя, фамилию, год рождения, город проживания, возраст, сферы увлечений и т.п. Более того, пользователи сами объединяются в группы на основе общих интересов и увлечений. Данная информация представляет собой большую ценность, поскольку с ее помощью появляется возможность группирования и классификации пользователей по различным признакам, в том числе по увлечениям и сфере интересов. В тематических группах, в свою очередь, публикуются новости и записи, просматриваемые большинством участников, в результате у пользователя, просматривающего последние новости, на их основе формируется мнение о сложившейся обстановке в стране и мире.

Возможность разбиения пользователей социальной сети на группы по различным признакам является важным фактором, обуславливающим использование социальных сетей для воздействия на мнение пользователей, формирования общественной позиции. В настоящее время социальные сети являются инструментом для формирования общественного мнения, в том числе, для стимулирования пользователей на совершение различных нелегитимных действий (проведение несанкционированных митингов, восстаний, протестов, вплоть до государственных переворотов). Однако для сильного воздействия на общество необходима массовость продвигаемой идеи: большое число постов, комментариев, создание соответствующих сообществ. Для этой цели используются автоматически управляемые аккаунты (боты), которые контролируются лицами, заинтересованными в продвижении своих идей в широкие массы. Они имеют возможность создания крупномасштабных, в большинстве состоящих из ботов, сообществ, характеризующихся соответствующим социальным настроением и ориентированных на формирование определенной гражданской позиции у пользователей социальной сети.

Для решения описанной проблемы распознавания автоматически управляемых аккаунтов, предлагается использовать методы машинного обучения, в частности нейронные сети, поскольку они хорошо себя зарекомендовали в решении задач распознавания образов. В настоящее время существующие методы противодействия ботам в социальных сетях недостаточно эффективны так как они основываются на детектировании при помощи модераторов, борьба с автоматизацией процессов происходит при помощи капчи. Из этого можно сделать выводы о том, что в настоящий момент

блокировка ботов возможна только после проявления их активности, при этом модераторы физически не смогут проверить все подозреваемые аккаунты.

Для распознавания образов принято решение об использовании персептрона, использующего метод обратного распространения ошибки. Метод обратного распространения ошибки – метод обучения многослойного персептрона. Основная идея данного метода состоит в распространении сигналов ошибки от выходов сети к ее входам, в направлении, обратном прямому распространению сигналов в обычном режиме работы. Алгоритм обратного распространения ошибки является одним из методов обучения многослойных нейронных сетей прямого распространения, называемых также многослойными персептронами. Многослойные персептроны успешно применяются для решения многих сложных задач, в том числе задач распознавания образов.

Для обучения разработанной нейронной сети подготовлена обучающая выборка, при помощи которой произведена настройка весов сети. Для успешного обучения необходимы как вектора, описывающие страницы ботов, так и вектора, описывающие реальных пользователей. Для получения выборки реальных пользователей были использованы страницы друзей и страницы друзей-друзей, а также верифицированные страницы (страницы, подтвержденные администрацией социальной сети). Для получения выборки заблокированных пользователей была сохранена информация о 100 000 последних зарегистрированных пользователях (были использованы идентификационные номера с 366000000 по 366100000). Через неделю информация о аккаунтах была получена повторно, из них 26 500 было заблокировано, полученная выборка была использована для обучения в качестве ботов.

Заключение. В результате на основе полученной выборки произведено обучение (настройка весов) нейронной сети, таким образом, чтобы она была способна распознавать ботов в социальных сетях. При этом разработанный прототип возможно использовать для проверки групп на наличие в них ботов, и в дальнейшем обнаруживать и предотвращать попытки влияния на мнения общественных масс.

СПИСОК ЛИТЕРАТУРЫ

1. Number of social network users worldwide from 2010 to 2019. Доступно с <http://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/>.
2. Python и нейронные сети. Доступно с <http://proft.me/2010/12/8/python-i-nejronnye-seti/>.

УДК 004.8

АНАЛИЗ ЧУВСТВИТЕЛЬНОСТИ ЛОКАЛЬНОГО ЛОГИКО-ВЕРОЯТНОСТНОГО ВЫВОДА В МАТЕМАТИЧЕСКОЙ БИБЛИОТЕКЕ ALGBN MATH LIBRARY

Мальчевская Екатерина Андреевна
Санкт-Петербургский государственный университет,
Россия, Санкт-Петербург, Университетская набережная, 7–9,
Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия, 39,
email: katerina.malch@gmail.com

Аннотация: Основным аппаратом по обработке алгебраических байесовских сетей является логико-вероятностный вывод. Анализ чувствительности результата некоторого вида вывода от входных данных позволяет оценить точность рассматриваемого алгоритма и, при необходимости, дать основание для его дальнейшей модификации. Реализована надстройка над разработанной математической библиотекой AlgBN Math Library, позволяющая получить оценку чувствительности для некоторых видов локального логико-вероятностного вывода и входных данных.

Ключевые слова: вероятностные графические модели; алгебраические байесовские сети; логико-вероятностный вывод; анализ чувствительности.

LOCAL PROBABILISTIC–LOGIC INFERENCE SENSITIVITY ANALYSIS IN MATHEMATICAL LIBRARY ALGBN MATH LIBRARY

Malchevskaya Ekaterina
The St. Petersburg State University,
Russia, St. Petersburg, Universitetskaya Emb. 7-9,
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,
Russia, St. Petersburg, 14 Line, 39,
email: katerina.malch@gmail.com

Abstract: The main apparatus for processing algebraic Bayesian networks is the probabilistic-logic inference. Sensitivity analysis of some type of inference and connection of the result from the input data makes it possible to estimate the accuracy of the algorithm and, if necessary, give grounds for its further modification. The calculation layer, which allows to obtain a sensitivity estimates for some types of local logic-probabilistic inference and input data, is implemented over the developed mathematical library AlgBN Math Library.

Keywords: *probabilistic graphical models; algebraic Bayesian networks; probabilistic-logic inference; sensitivity analysis.*

Введение. Алгебраические байесовские сети как один из классов вероятностных графических моделей могут быть использованы для обработки данных с неопределенностью. Они представляются ненаправленными графами с идеалами конъюнктов, в классическом случае, в узлах. Конъюнкты строятся над некоторым фиксированным набором символов – алфавитом. Конъюнктам может быть приписана, как скалярная (точечная), так и интервальная оценка вероятности истинности. Основным аппаратом по проверке согласованности заданных оценок, получения новых знаний, является логико-вероятностный вывод. Выделяют два уровня вывода: локальный и глобальный. В локальном случае рассматривается только один фиксированный идеал конъюнктов с оценками вероятности истинности его элементов (фрагмент знаний), в случае глобального вывода мы рассматриваем всю сеть, как систему и учитываем влияние изменений в одном конкретном фрагменте знаний на всю сеть.

В рамках теории алгебраических сетей существует несколько видов логико-вероятностного вывода: проверка и поддержание непротиворечивости, задачи априорного и апостериорного вывода. Ранее была разработана и реализована математическая библиотека AlgBN Math Library на языке программирования C#, позволяющая осуществлять локальный логико-вероятностный вывод над фрагментами знаний. Для уравнений по осуществлению таких видов вывода требуется производить анализ их чувствительности от входных данных, то есть наблюдать, насколько колеблется результат, в зависимости от входных данных. Данный показатель важен при анализе точности алгоритма. Таким образом была разработана и реализована надстройка над математической библиотекой, позволяющая провести вычислительные эксперименты по анализу чувствительности некоторых видов локального логико-вероятностного вывода.

Заключение. Надстройка для проведения вычислительных экспериментов по анализу чувствительности логико-вероятностного вывода над математической библиотекой AlgBN Math Library позволяет получать конкретные оценки, а в дальнейшем строить графики зависимости оценки от разброса входных данных. Надстройка покрывает некоторые виды локального логико-вероятностного вывода. Ближайшей целью является расширение ее на глобальный вывод в алгебраических байесовских сетях.

СПИСОК ЛИТЕРАТУРЫ

1. Золотин А.А., Тулупьев А.Л., Сироткин А.В. Матрично-векторные алгоритмы локального апостериорного вывода в алгебраических байесовских сетях над пропозициями квантами // Научно-технический вестник информационных технологий, механики и оптики. 2015. Т. 15. № 4. С. 676–684.
2. Тулупьев А.Л. Алгебраические байесовские сети. Глобальный логико-вероятностный вывод в деревьях смежности. // Учебное пособие. СПб, 2007. 37 с.
3. Тулупьев А.Л., Николенко С.И., Сироткин А.В. Байесовские сети: логико-вероятностный подход. СПб: Наука, 2006. 607 с.

УДК 004.027.31

ЯЗЫКОВЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Микони Станислав Витальевич

Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия, д. 39,
e-mail: spiiras@iias.spb.su

Аннотация: Рассматривается языковой уровень информационной безопасности. Обсуждается влияние английского языка на продуктивность отечественных научных публикаций. Приводятся примеры влияния плохого знания национального языка на качество публикаций. Предлагаются меры для повышения качества научных публикаций.

Ключевые слова: *информационная безопасность, национальный язык, английский язык, научная публикация.*

LANGUAGE PROBLEMS OF INFORMATION SECURITY

Mikoni Stanislav

St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,
Russia, St. Petersburg, 14 Line, 39,
e-mail: spiiras@iias.spb.su

Abstract: The language level of information security is considered. The influence of English on the productivity of Russian scientific publications is discussed. Examples of the impact of poor knowledge of the national language on the quality of publications are given. Measures are proposed to improve the quality of scientific publications.

Key words: *information security, national language, English, scientific publication*

Согласно ГОСТ 7.0-99 информация – это сведения, воспринимаемые человеком и (или) специальными устройствами как отражение фактов материального или духовного мира в процессе коммуникации. Однако восприятие мира человеком неоднозначно. Так сложилось, что в ходе развития человечества разные цивилизации сформировали свой «угол зрения» на окружающий мир. Англосаксонская цивилизация со своим меркантильным взглядом на мир добилась на нынешнем уровне развития человечества наибольших успехов в удовлетворении материальных потребностей людей. Это послужило поводом её теоретикам выдвинуть лозунг конвергенции в развитии человечества. В переводе на русский язык конвергенция означает схождение в противоположность дивергенции, как расхождению. Естественно, что под точкой схождения они понимают либеральную организацию общества с английским языком в его основе. Недаром первичным условием вхождения в эту цивилизацию является изучение английского языка, на что тратятся огромные средства.

С одной стороны, использование английского языка решает проблему межнационального общения, что не удалось сделать с помощью искусственного языка эсперанто. И это хорошо. С другой стороны, навязывается взгляд на мир глазами носителями этого языка. А это не только плохо, но и вредно своими последствиями. «Заставь дурака Богу молиться, он и лоб расшибёт!». Так мы внедряли западный взгляд на мир. То, что в России всегда считалось служением, ретивые российские реформаторы по примеру западных гуру стали называть бизнесом и услугами. Трудно, например, принять за бизнес-процесс воспитательную работу преподавателя, работающего на ставке, а услугой – его преподавательскую деятельность. Подобные новации, как и весь болонский процесс, серьёзно подрывали качество российского инженерного образования. Только неимоверными усилиями энтузиастов удалось сохранить подготовку специалистов по ряду направлений.

Не менее вредно схождение англоязычной и русской терминологии. Приведём цитату из научной публикации своих коллег: «На этапе экспликации интенционал классификационного поля (КП) раскрывается в опоре на имплицитность двух онтологий, выраженную в положениях о гомологичности, доминантности, совместимости, частотности и референтной соотнесённости, а экстенционал КП строится на идеях прототипичности и сходности (по-русски – сходства)».

Такой кириллоязычный текст не расшифруешь даже со словарём! Кодировщики машинных слов могут позавидовать. Злоумышленник, прочитавший такой текст, точно зависнет! Спрашивается, для какой категории читателей пишутся такие тексты? Русский человек, даже владеющий английским языком, их не поймёт, иностранец читать не будет. Выходит, не случайно Казахстан решил переходить на латиницу, чтобы читать научные работы в оригинале, не испорченные кириллицей. В языковой сфере теряем своего естественного союзника. В этом факте усматривается и «заслуга» наших учёных.

Но, ведь, на такую конвергенцию и направлены усилия наших западных «партнёров»: нужно прекратить воспроизводство чужих идей. Они отлично продемонстрировали это на «человеческом» материале, введя понятие третьего пола, который не способен на размножение. Этот пример, кстати, очень показателен и для самой идеи конвергенции. Если теоретически предположить, что она реализуема, то общечеловеческая либеральная цивилизация на этом и прекратит своё существование, лишив себя развития. А оно, согласно закону диалектики «единства и борьбы противоположностей» рождается только в борьбе.

В сфере науки многие российские учёные отдают предпочтение англоязычным публикациям, хотя на признание российской науки на Западе это никак не повлияло. За четверть века получено всего две нобелевских премии, причём учёными советской формации. Возможно, причина этого лежит в не прорывном характере публикаций российских учёных. Любители иностранных терминов обосновывают их применение тем фактором, что «наука интернациональна». Да, наука интернациональна, но язык-то национален! Полностью интернационален только язык математики, поскольку лишён предметного смысла. А вот философия различных цивилизаций на их взгляд на мироустройство национальна. И нельзя смешивать наднациональные объективные законы с отношением к ним человека («что для русского хорошо для немца смерть»).

Отметим более глубокую, на наш взгляд, причину отсутствия отечественных прорывных работ или, по крайней мере, их малое количество. Окунувшись в англоязычную литературу и готовя свои работы на английском языке, большинство наших учёных не могут сравниться с носителями этого языка для того, чтобы подняться на более высокие ступени обобщения. Поэтому большинство работ наших учёных носит технологический характер в плане улучшения существующих технологий и решения частных задач. Но хуже всего то, что многие российские учёные не способны квалифицировано писать работы на своём родном языке, не понимая его глубинных понятий и подменяя их иноязычными терминами. В этом смысле показательная классификация самоорганизующихся систем по возрастанию сложности свойств, предложенная в учебнике по системному анализу. Во первых, такое научное понятие отсутствует. Во вторых, неспособность применить в междисциплинарной модели обобщающие понятия (Umbrella terms), выраженные на родном языке, не могла ни породить эклектическую классификацию.

Здесь уместно отметить, что автор не отвергает пользы английского языка. Он полезен не только для общения с англоязычным миром, но и как инструмент для решения частных задач. Примером являются языки программирования высокого уровня, использующие лаконизм английского

языка. А вот в сфере обобщений востребовано глубокое знание русского языка, поскольку по мере приближения к философским понятиям мы приближаемся к самобытности своего восприятия мира.

Мало научиться иностранному языку. Нужно научиться мыслить категориями его носителя. В этом смысле показательна грубейшая ошибка наших западных «партнёров». Мысля меркантильными категориями своего общества, они ввели экономические санкции против России, что заставило её руководство наконец-то, всерьёз озаботиться проблемами отечественной промышленности и сельского хозяйства. Наш народ оказался терпеливым (не привыкать!), а американская мечта о российской бензоколонке не сбылась. Не случайно, видя крах своей политики в отношении России, ЦРУ объявило приём на работу носителей русского языка, чтобы выполнять аналитическую работу со знанием характера русского человека, а не абстрактного гражданина мира.

Смысл информационной безопасности заключается в том, что нужно делать то, что понятно нам и не понятно противнику. В научной сфере действуем наоборот – пишем тексты, непонятные своему читателю и из кожи вон лезем, чтобы ублажить англоязычного читателя нашими достижениями. На это направлены все балльные оценки продуктивности учёных. Пора и в этой сфере пересмотреть приоритеты публикаций, памятуя заявления нашего руководства, что «конфронтация с Западом – это надолго». Иначе получается, что хотим одного, а делаем другое. В плане стимулирования научных публикаций полезно было бы оценивать их не с точки зрения языка (английского или русского), а с точки зрения их востребованности.

Что касается национального языка, то нас волнует нарушение равновесия в пользу иностранных терминов. Восстановлению равновесия должны способствовать сами учёные, озабоченные чрезмерным засорением родного языка и его всё большим отдалением от первородных корней. К решению этой задачи следует привлекать профессиональных лингвистов. Необходимо также повысить качество терминологических стандартов, привлекая к их разработке опытных специалистов, известных своими работами в соответствующей области. Следовало бы ввести такой критерий оценивания работы, как её понятность для носителя языка.

Исследования, выполненные по данной тематике, проводились при финансовой поддержке грантов РФФИ № 16-08-01277, № 17-01-00139, госзадания Министерства образования и науки РФ №2.3135.2017/К, в рамках бюджетных тем №№0073–2014–0009, 0073–2015–0007.

СПИСОК ЛИТЕРАТУРЫ

1. С.В. Микони. Системный взгляд на современную терминологию. / Сборник научных трудов XIX-й междунар. конф. «Системный анализ в проектировании и управлении», 1-3 июля 2015. Ч.1. – СПб.: Изд-во Политехн. ун-та, 2015.с. 62-71.

УДК 004.05

ВОССТАНОВЛЕНИЕ ПРОФИЛЯ УЯЗВИМОСТЕЙ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВАНИИ ИНФОРМАЦИИ, КОТОРАЯ МОЖЕТ БЫТЬ ПОЛУЧЕНА ИЗ СОЦИАЛЬНЫХ СЕТЕЙ

Слёзкин Никита Евгеньевич¹, Азаров Артур Александрович²

¹ Санкт-Петербургский государственный университет,

Россия, Санкт-Петербург, Петергоф, Университетский пр-кт, 28,

² Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Россия, Санкт-Петербург, 14 линия, 39

emails: ne.slezkin@gmail.com, artur-azarov@yandex.ru

Аннотация: В статье рассмотрен подход к формированию профиля уязвимостей пользователей на основании интегрированного профиля пользователя, построенного на основании данных из социальных сетей.

Ключевые слова: профиль уязвимостей пользователя, социоинженерная атака, интегрированный профиль пользователя.

CONSTRUCTING USER'S VULNERABILITIES PROFILE ON THE BASIS OF INFORMATION EXTRACTED FROM SOCIAL NETWORKS

Slezkin Nikita¹, Artur Azarov²

¹ Saint-Petersburg University,

Russia, St. Petersburg, Peterhof, Universitetsky prosp. 28,

² St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,

Russia, St. Petersburg, 14 Line, 39,

emails: ne.slezkin@gmail.com, artur-azarov@yandex.ru

Abstract: The article is devoted to the construction of user's vulnerabilities profile based on an integrated user profile formed on data extracted from social networks.

Keywords: *user's vulnerabilities profile, social engineering attack, integrated user profile.*

Повсеместное распространение сети Интернет, ускорившееся с появлением сравнительно дешевого мобильного доступа к сети, приводит к вовлечению все большего количества людей в различные социальные сети. Как и любое явление, влияющее на жизнь людей, оно попало под пристальное внимание ученых со всего мира. В связи с этим, количество работ, в той или иной степени связанных с изучением взаимодействия пользователей в социальных сетях, постоянно растет. Данные, которые могут быть получены на основе анализа социальных сетей, позволяют изучать пользователей с различных позиций. Так, например, могут быть построены различные графы взаимодействия пользователей, может быть проведен анализ их постов, комментариев, предпочтений в сообществах, аудиозаписях и другой информации, содержащейся на их персональных страницах. Легкая доступность и открытость такого объема информации о пользователях позволяет злоумышленникам строить более изощренные социоинженерные атаки с целью получения конфиденциальных данных, которыми обладают данные пользователи [8–11]. Данный проект нацелен на консолидацию данных о пользователях различных социальных сетей с целью восстановления психологических особенностей пользователей, и, позднее, построения профиля уязвимостей пользователя, что, в последствии, позволит выработать ряд мер для обеспечения безопасности конфиденциальных данных и защите пользователей информационных систем от злонамеренного воздействия злоумышленника.

Основной сложностью при работе с данными пользователей в социальных сетях является неполная и недостоверная информация, которая указывается пользователями на своих персональных страницах. Вместе с тем, данная проблема может быть решена в случае рассмотрения большего количества факторов, указанных на персональной странице пользователя, а также с помощью анализа аккаунтов пользователя в других социальных сетях, в случае их наличия. Так, например, при рассмотрении параметров среднего возраста друзей пользователя и их места жительства, может быть определен возраст пользователя, владеющего рассматриваемым аккаунтом. По данным исследования [4] пользователи в большинстве случаев пользуются более чем одной социальной сетью. Например, большинство авторов Инстаграм являются активными пользователями других соцсетей — доля кросспостинга из Инстаграм в другие соцсети превышает 50% сообщений. Поэтому может быть построен интегрированный профиль пользователя, на основании данных из различных социальных сетей. Таким образом, интегрированный профиль пользователя будет строиться на основании достоверной и проверенной информации.

Таким образом, на основании построенного интегрированного профиля пользователя могут быть более достоверно восстановлены психологические особенности пользователя, построен соответствующий профиль уязвимостей пользователя и, соответственно, выработаны меры по противодействию социоинженерным атакующим воздействиям злоумышленника.

СПИСОК ЛИТЕРАТУРЫ

1. Абрамов М.В., Азаров А.А., Тулупьева Т.В., Тулупьев А.Л. Модель профиля компетенций злоумышленника в задаче анализа защищенности персонала информационных систем от социоинженерных атак // Информационно-управляющие системы. 2016. №4. С. 77–84.
2. Азаров А.А., Тулупьева Т.В., Суворова А.В., Тулупьев А.Л., Абрамов М.В., Юсупов Р.М. Социоинженерные атаки. Проблемы анализа. СПб.: Наука, 2016. 352 с.
3. Информационная безопасность бизнеса. Исследования текущих тенденций в области информационной безопасности бизнеса // Лаборатория Касперского. http://media.kaspersky.com/pdf/IT_risk_report_Russia_2014.pdf (дата обращения: 30.08.2017).
4. Социальные сети в России, зима 2015-2016 Цифры, тренды, прогнозы // Brand Analytics. <http://blog.br-analytics.ru/socialnye-seti-v-rossii-zima-2015-2016-cifry-trendy-prognozy/> (дата обращения: 24.09.2017)

УДК 311.2 + 616-036.22

АВТОМАТИЧЕСКОЕ ИЗВЛЕЧЕНИЕ ДАННЫХ О ДЛИНАХ ИНТЕРВАЛОВ МЕЖДУ ПОСЛЕДОВАТЕЛЬНЫМИ ЭПИЗОДАМИ ИЗ ОПРОСНИКА О ПОСЛЕДНИХ ЭПИЗОДАХ ПОВЕДЕНИЯ

Столярова Валерия Фуатовна

Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук,

Россия, Санкт-Петербург, 14 линия В.О., 39

email: valerie.stoliarova@gmail.com

Аннотация: В статье предлагается алгоритм автоматического извлечения информации о длинах интервалов между последовательными эпизодами из базы данных ответов на вопросы о последних эпизодах поведения. Для наблюдений, в которых присутствует несколько вариантов ответов (к примеру, 22 сентября, неделю назад, во вторник) в качестве момента эпизода выбран наиболее точный ответ. Кроме длины интервала, алгоритм позволяет получить информацию о типе ответа респондента, что важно при дальнейшей фаззификации или грануляризации ответов на естественном языке. Алгоритм реализован на языке программирования R и апробирован на данных, собранных на базе кожно-венерологического диспансера №9 Калининского района Санкт-Петербурга, в мае–ноябре

2011 года. Автоматическое извлечение данных о длинах интервалов между последовательными эпизодами является частью комплекса программ по автоматизации сбора данных и оценки интенсивности поведения и позволяет как обнаруживать ошибки заполнения базы данных, так и генерировать готовую для построения оценок интенсивности поведения информацию.

Ключевые слова: *рискованное поведение; последние эпизоды; неточная информация.*

AUTOMATED INTER-EPISODE INTERVAL LENGTH DATA RETRIEVAL FROM DATABASE FOR LAST EPISODES QUESTIONNAIRE

Stoliarova Valeriia

The Federal State Institution of Science St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences,
Russia, St. Petersburg, 39, 14th Line VO
email: valerie.stoliarova@gmail.com

Abstract: The article presents the algorithm for automated data retrieval from database for last episodes of person's behavior questionnaire. Data needed from the questionnaire is inter-episode interval length. The most exact answer is chosen for observations with multiple answers (e.g. Tuesday, September 22nd, a week ago). The algorithm allows one to retrieve information about type of the answer, which is needed for fuzzification and granularization of natural language answers. The algorithm is written on R language and implemented for data collected in STD clinic No.9 in Kalininskiy district of St. Petersburg, May through November 2011. Automated inter-episode interval length data retrieval algorithm is a part of program complex for automated data collection and intensity estimation. The algorithm allows one to check for database inconsistencies and generate ready-to-use data for intensity estimation.

Keywords: *risky behavior; last episodes; inexact knowledge*

Введение. Задача оценки интенсивности поведения возникает в тех областях, в которых поведение связано с тем или иным риском. К примеру, в эпидемиологии модель Белла-Тревино связывает интенсивность эпизодов разных типов рискованного поведения с вероятностью передачи неизлечимых инфекций (таких как ВИЧ, гепатит С и т.д.) [3]. Приведем еще пример. Известно, что недостаток определенных питательных веществ (например, кальция) негативно сказывается на развитии плода [2]. Поэтому в области акушерства и гинекологии бывает оценить количество тех или иных питательных веществ, которые получает беременная женщина в повседневном рационе питания с целью его коррекции. Для оценки используют дневниковый метод, в котором пациентка указывает частоту употребления определенных классов продуктов питания [2]. В первом случае применение классических способов оценки интенсивности рискованного поведения (прямое измерение и дневниковые метод) недоступно. Во втором случае требуется быстрая и удобная оценка интенсивности употребления определенных видов продуктов, что может помочь в своевременной диагностике нехватки питательных веществ.

Как показывают пилотные опросы, ответы на стандартные вопросы типа "Как часто Вы употребляете..." часто являются смещенными или вообще не связанными с действительностью. Этим обусловлен переход к вопросам о последних эпизодах поведения и о рекордных интервалах между ними. Как показывают пилотные опросы, припоминание такой информации не составляет для респондентов труда [1]. Для удобного сбора информации был создан автоматизированный инструментарий для опроса респондентов об эпизодах рискованного поведения [1]. Варианты ответа разделены на пять групп: относительные временные характеристики, точная дата, временные характеристики, выраженные «бытовым» языком, вариант «не помню» и «другое». Кроме того, возможны различные классы ответов: последовательные (респондент отсчитывает эпизоды поведения от предыдущего эпизода), вложенные (респондент отсчитывает все эпизоды от момента интервью) и смешанные.

В данной статье предлагается алгоритм автоматического извлечения информации о длинах интервалов между последовательными эпизодами из базы данных ответов на вопросы о последних эпизодах поведения. Для наблюдений, в которых присутствует несколько вариантов ответов (к примеру, 22 сентября, неделю назад, во вторник) в качестве момента эпизода выбран наиболее точный ответ. Кроме длины интервала, алгоритм позволяет получить информацию о типе ответа респондента, что важно при дальнейшей фаззификации или грануляризации ответов на естественном языке. Алгоритм реализован на языке программирования R и апробирован на данных, собранных на базе кожно-венерологического диспансера №9 Калининского района Санкт-Петербурга, в мае–ноябре 2011 года [1].

Заключение. Автоматическое извлечение данных о длинах интервалов между последовательными эпизодами является частью комплекса программ по автоматизации сбора данных и оценки интенсивности поведения и позволяет как обнаруживать ошибки заполнения базы данных, так и генерировать готовую для построения оценок интенсивности поведения информацию.

СПИСОК ЛИТЕРАТУРЫ

1. Суворова А.В., Мусина В.Ф., Тулупьева Т.В., Тулупьев А.Л., Красносельских Т.В., Фильченков А.А., Азаров А.А., Абдала Н. Автоматизированный инструмент для опроса респондентов об эпизодах рискованного поведения: первичный анализ результатов применения // Труды СПИИРАН. 2013. Вып. 26. С. 175-193.
2. Курмачева, Н. А., Рогожина, И. Е., Топорова, Е. Е., Аккузина, О. П. Эффективность коррекции потребления кальция у женщин с риском осложненного течения беременности // Лечение и профилактика. 2013. Вып. 2. С.64-69.
3. Суворова, А. В., Тулупьев, А. Л., Пашенко, А. Е., Тулупьева, Т. В., Красносельских, Т. В. Анализ гранулярных данных и знаний в задачах исследования социально значимых видов поведения // Компьютерные инструменты в образовании. 2010. № 4. С. 30-38.

УДК 004.94

МОДЕЛИРОВАНИЕ НЕТОЧНОСТИ ОТВЕТОВ В БАЙЕСОВСКОЙ СЕТИ ДОВЕРИЯ ДЛЯ ОЦЕНИВАНИЯ СОЦИАЛЬНО-ЗНАЧИМОГО ПОВЕДЕНИЯ РЕСПОНДЕНТОВСуворова Алена Владимировна¹, Акульшина Ольга Дмитриевна²¹ Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Россия, Санкт-Петербург, 14 линия, 39,² Санкт-Петербургский государственный университет, Россия, Санкт-Петербург, Университетская наб., 7-9, emails: suvalv@gmail.com, 9.svarog@gmail.com

Аннотация: В работе предложено ввести в существующую модель оценки интенсивности социально-значимого поведения новые скрытые переменные, которые учитывают возможную неточность ответов респондентов, и исследовано влияние такой модификации на качество предсказания модели на основе байесовской сети доверия.

Ключевые слова: байесовские сети доверия; социально-значимое поведение; рискованное поведение; скрытые переменные; последние эпизоды

IMPRECISION OF RESPONSES MODELING IN THE BAYESIAN BELIEF NETWORK FOR RESPONDENT'S SOCIALLY SIGNIFICANT BEHAVIOR ESTIMATIONSuvorova Alena¹, Akulshina Olga²¹ Saint Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, Russia, Saint Petersburg, 14 Lane 39,² Saint Petersburg State University, Russia, Saint Petersburg, Universitetskaya Emb. 7-9, emails: suvalv@gmail.com, 9.svarog@gmail.com

Abstract: We propose introducing new latent variables considering possible imprecision of responses into existing model of socially significant behavior rate estimates. We explore the impact of modification on quality of the model's predictions.

Keywords: bayesian belief networks; socially significant behavior; risky behavior; latent variables; last episodes

Необходимость оценки социально-значимого поведения индивида возникает во многих задачах психологии, социологии, эпидемиологии. Однако непосредственное измерение числа эпизодов такого поведения часто невозможно [1], поэтому для этого используются косвенные методы оценки.

Для моделирования социально-значимого поведения на основе данных о нескольких последних эпизодах такого поведения используются байесовские сети доверия. Они позволяют представить сложные взаимосвязи между элементами модели в виде разложения на более простые элементы, что упрощает описание всей системы и ее интерпретацию [2].

Ранее в работах [3], [4] был предложен подход, использующий данные о последних трех эпизодах социально-значимого поведения и о максимальном и минимальном промежутках между эпизодами за определенный период времени для построения модели на основе байесовской сети доверия, применяемой в дальнейшем для оценивания характеристик подобного поведения.

Отметим, что оценки по модели, построенной согласно такому подходу, могут быть смещены из-за неточности сведений об эпизодах поведения, т.к. ответы, полученные от респондентов, не всегда соответствуют реальности (респондент может не помнить точного ответа на вопрос или намеренно исказить его).

Чтобы учесть данный особенность исходных данных, предлагается ввести в модель дополнительные скрытые переменные, соответствующие реальным сведениям об эпизодах. Наблюдаемые переменные в таком случае будут учитывать возможную погрешность в ответах.

Целью работы является исследование подобной модификации и изучение ее влияния на качество предсказания полученной модели.

СПИСОК ЛИТЕРАТУРЫ

1. Суворова А.В. Гибридные оценки параметров социально-значимого поведения по сверхмалой неполной совокупности наблюдений // Труды СПИИРАН. 2013. Вып. 1(24). С. 116–134.
2. Тулупьев А.Л., Николенко С.И., Сироткин А.В. Байесовские сети: логико-вероятностный подход. СПб.: Наука, 2006. 607 с.
3. Суворова А.В., Тулупьев А.Л., Сироткин А.В. Байесовские сети доверия в задачах оценивания интенсивности рискованного поведения. // Нечеткие системы и мягкие вычисления. 2014. Т. 9, №2. С. 115–129.
4. Суворова А.В., Тулупьев А.Л. Структурный синтез байесовской сети доверия по пуассоновской модели поведения // XV национальная конференция по искусственному интеллекту с международным участием КИИ-2016 (3–7 октября 2016 г., г. Смоленск, Россия). Труды конференции. В 3-х томах., Смоленск: Универсум, 2016, Т. 3. С. 139–147.

УДК 004.94

АНАЛИЗ ТЕКСТОВОЙ ИНФОРМАЦИИ ПОСТОВ В СОЦИАЛЬНОЙ СЕТИ КАК ОСНОВА ПСИХОЛОГИЧЕСКОГО ПРОФИЛЯ ПОЛЬЗОВАТЕЛЯСуворова Алёна Владимировна¹, Тулупьева Татьяна Валентиновна^{1,2}¹ Санкт-Петербургский институт информатики и автоматизации РАН,
Россия, Санкт-Петербург, 14 линия, 39,² Северо-Западный институт управления – филиал РАНХиГС,
Россия, Санкт-Петербург, Средний пр. В.О., 57,
emails: suvalv@gmail.com, tv100a@mail.ru

Аннотация: Социальные процессы, происходящие в Интернет-пространстве, способны оказывать глубокое влияние на жизнь общества за пределами всемирной сети. Как следствие, изучение особенностей отражения личностных особенностей пользователей в интернет-контенте остается актуальным. В работе рассмотрены результаты классификации постов на основе методов автоматического анализа текста и взаимосвязь полученных классов с личностными особенностями пользователей.

Ключевые слова: моделирование поведения; социальные сети; анализ текста; психологический профиль; социальный компьютеринг

TEXT ANALYSIS OF PUBLICATIONS ON SOCIAL NETWORKING SITE AS THE BASIS FOR USER'S PSYCHOLOGICAL PROFILESuvorova Alena¹, Tulupyeva Tatiana²¹ St. Petersburg Institute for Informatics and Automation of the RAS,
Russia, St. Petersburg, 14th Line, 39,² North-West Institute of Management, branch of RANEPa,
Russia, St. Petersburg, Sredniy prospect 57,
emails: suvalv@gmail.com, tv100a@mail.ru

Abstract: Social processes in Internet have great impact on the society life outside the global network. Hence, to study how Internet content reflects the personal characteristics of users is of current interest. The paper presents the results of the post classification based on the methods of automatic text analysis and examines the relationship between the post classes and the personal characteristics of users.

Keywords: behavior modeling; social network site; text analysis; psychological profile; social computing

Социальные процессы, происходящие в Интернет-пространстве, отличаются повышенным разнообразием, динамичностью, и что особенно важно, способны оказывать глубокое влияние на жизнь общества за пределами всемирной сети [5], [9]. Социальные сети для многих стали неотъемлемой и важной частью жизни, в них отражаются и частично формируются потребности и ценности пользователей [1], [4]. Социальные сети рожают новую культуру со своими понятиями, ценностями, образом мыслей и языком. Анализ социальных сетей дает интересные данные при изучении как индивидуального, так и коллективного поведения [6], [7], [10].

Информацию, которую пользователь размещает на своей странице в социальной сети можно рассматривать как продукт деятельности, который несет в себе отпечатки особенностей конкретного человека. Значит, по размещенной информации можно строить предположения о психологических особенностях пользователя социальной сети.

Посты в социальных сетях – один из видов «цифровых следов», которые оставляют пользователи и к которым относительно легко получить доступ. Вместе с тем, посты каждого отдельного пользователя и некоторые другие характеристики его аккаунта представляют собой достаточно содержательную систему, в которой проявляются когнитивные, эмоциональные и поведенческие компоненты общения, и которая отражает или преломляет самые разные аспекты его деятельности [8], [11]. Таким образом, эта система становится достаточно значимым объектом исследований для информатики и психологических наук, а также источником сведений для развития методов экспресс-диагностики при психотерапии, организации образовательного процесса, выстраивании отношений в сложных ситуациях.

Были проведены пилотные полевые исследования для сбора данных о психологических особенностях, опрошено 162 студента различных ВУЗов Санкт-Петербурга. В результате предыдущих исследований были выделены классификационные признаки для постов (публикаций) в профиле социальной сети, проведены эксперименты, показавшие согласованность предложенной классификации [2], [3].

В работе рассмотрены результаты анализа текстовой составляющей постов, публикуемых авторами на персональных страницах социальной сети ВКонтакте. Для каждого участника исследования был проведен сбор данных из аккаунтов респондентов в социальной сети ВКонтакте с помощью средств API ВКонтакте, в частности, прикладных библиотек vkR (язык R), VkNet (C#), по целому ряду факторов: интересные страницы, количество друзей, доступность личной информации, анализ комментариев стены, включая текстовую информацию из публикуемых ими постов на стене профиля (в течение шести месяцев, предшествующих дате опроса).

Для последующего включения в модели тексты были предобработаны: проведено распределение постов по классам (с учетом разработанной в предыдущих исследованиях классификации [2]), автоматическое выделение тем (тематическое моделирование) методом LDA, адаптированным для коротких текстов и анализ настроений (sentiment analysis) для определения позитивности-негативности поста.

Затем были выявлены взаимосвязи между личностными особенностями пользователей и характеристиками их профилей в социальной сети, с акцентом на результаты анализа текстовой информации. Проведено сравнение экспертной и автоматической классификации постов.

СПИСОК ЛИТЕРАТУРЫ

1. Титов В. В. Интернет как пространство трансформации системы коммуникативных идентичностей российского общества: по материалам международного исследования World Internet project (WIP) // Мониторинг общественного мнения: экономические и социальные перемены. – 2013. – № 3 (115).
2. Тулупьева Т.В., Суворова А.В., Азаров А.А., Тулупьев А.Л., Бордовская Н.В. Возможности и опыт применения компьютерных инструментов в анализе цифровых следов студентов-пользователей социальной сети // Компьютерные инструменты в образовании. – 2015. – № 5. – С. 3-13
3. Тулупьева Т.В., Тафинцева А.С., Тулупьев А.Л. Подход к анализу отражения особенностей личности в цифровых следах // Вестн. психотерапии. – 2016. – № 60 (65). – С. 124-137.
4. Amichai-Hamburger Y., Hayat Z. The impact of the Internet on the social lives of users: A representative sample from 13 countries // Computers in Human Behavior. – 2011. – Т. 27. №. 1. – С. 585-589.
5. Bond R. M. et al. A 61-million-person experiment in social influence and political mobilization // Nature. – 2012. – Т. 489. №. 7415. – С. 295-298.
6. Chen C. S., Chang S. F., Liu C. H. Understanding knowledge-sharing motivation, incentive mechanisms, and satisfaction in virtual communities // Social Behavior and Personality: an international journal. – 2012. – Т. 40. №. 4. – С. 639-647.
7. Duhe S. An overview of new media research in public relations journals from 1981 to 2014 // Public Relations Review. – 2015. – Т. 41. №. 2. – С. 153-169.
8. Martinez M. G., Walton B. The wisdom of crowds: The potential of online communities as a tool for data analysis // Technovation. – 2014. – Т. 34. – №. 4. – С. 203-214.
9. Muchnik L., Aral S., Taylor S. J. Social influence bias: A randomized experiment // Science. – 2013. – Т. 341. – №. 6146. – С. 647-651.
10. Ren Y. et al. Building Member Attachment in Online Communities: Applying Theories of Group Identity and Interpersonal Bonds // Mis Quarterly. – 2012. – Т. 36. – №. 3. – С. 841-864.
11. Sun N., Rau P. P. L., Ma L. Understanding lurkers in online communities: A literature review // Computers in Human Behavior. – 2014. – Т. 38. – С. 110-117.

УДК 004.05

ПОСТРОЕНИЕ СОЦИАЛЬНОГО ГРАФА СОТРУДНИКОВ КОМПАНИИ НА ОСНОВании ИНФОРМАЦИИ, ПОЛУЧАЕМОЙ ИЗ СОЦИАЛЬНЫХ СЕТЕЙ, ДЛЯ РАСЧЁТА ВЕРОЯТНОСТИ УСПЕХА СОЦИОИНЖЕНЕРНОЙ АТАКИ

Сулейманов Алексей Александрович¹, Тулупьева Татьяна Валентиновна^{1,2},
Тулупьев Александр Львович^{1,2}

¹ Санкт-Петербургский государственный университет,
Россия, Санкт-Петербург, Петергоф, Университетский пр-кт, 28,

² Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Россия, Санкт-Петербург, 14 линия, 39

emails: lex.suleimanov@gmail.com, tvt100a@mail.ru, alexander.tulupjev@gmail.com

Аннотация: Данное исследование направлено на анализ не прямых угроз, а опосредованных, т.е. таких, при которых внедрение в информационную систему компании злоумышленником происходит с использованием более чем одного сотрудника компании, при этом воздействие на некоторых из них происходит посредством манипуляций, проводимых коллегами атакуемого. Для оценки успешности такого рода атаки важно понимать характер отношений между сотрудниками.

Ключевые слова: социоинженерные атаки; информационная безопасность; защита пользователя; защита информации; социальный граф.

CONSTRUCTION OF THE SOCIAL GRAPH OF THE COMPANY'S EMPLOYEES ON THE BASIS OF INFORMATION RECEIVED FROM SOCIAL NETWORKS TO CALCULATE THE PROBABILITY OF SUCCESS OF THE SOCIAL-ENGINEERING ATTACK

Suleimanov Aleksei¹, Tulupyeva Tatiana^{1,2}, Tulupjev Alexander^{1,2}

¹ Saint-Petersburg University,

Russia, St. Petersburg, Peterhof, Universitetsky prosp. 28,

² St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,
Russia, St. Petersburg, 14 Line, 39,

emails: lex.suleimanov@gmail.com, tv100a@mail.ru, alexander.tulupjev@gmail.com

Abstract: This study is aimed at analyzing not direct threats, but indirect ones. such that the introduction of an attacker into the company's information system occurs with the use of more than one employee of the company, while the impact on some of them occurs through manipulations conducted by the colleagues of the attacker. To assess the success of this type of attack, it is important to understand the nature of the relationship between employees.

Keywords: *social engineering attacks; information security; user protection; information protection; attacker's competencies profile; social graph.*

Введение. Исследования в области обеспечения защиты пользователей от социоинженерных атак являются сегодня очень актуальными [1, 3]. В современной действительности большинство успешных атак на инфраструктуру компаний так или иначе задействуют сотрудников компании, как точку входа в систему. Таким образом, для обеспечения комплексной защиты, которая бы учитывала все возможные векторы атак необходимо понимать, какие сотрудники умышленно или неумышленно могут стать орудием в руках заинтересованных в краже данных лиц. Защита пользователей от социоинженерных атак предполагает построение их профилей уязвимостей [2]. Профиль уязвимостей пользователя ассоциирован с его психологическими особенностями, которые можно получать разными способами: из психологических тестов, от экспертов, через выбор стратегии в специальной компьютерной игре или на основе информации в социальной сети.

Данное исследование направлено на анализ не прямых угроз, а опосредованных, т.е. таких, при которых внедрение в информационную систему компании злоумышленником происходит с использованием более чем одного сотрудника компании, при этом воздействие на некоторых из них происходит посредством манипуляций, проводимых коллегами атакуемого. Для оценки успешности такого рода атаки важно понимать характер отношений между сотрудниками. Очевидно, что если между коллегами дружеские или более близкие отношения, то вероятность социоинженерного атакующего воздействия возрастает и наоборот, вероятность успеха такого воздействия ниже, если между коллегами неприязненные отношения. Согласно ряду подходов, представленных в [2], для решения данной задачи удобно строить социальные графы взаимодействия, в которых указывается вероятность успеха атаки одного сотрудника при успешной атаке другого. Такие графы взаимодействия пользователей системы компании принято строить полными, однако данный подход не подходит для довольно крупных компаний, насчитывающих сотни и тысячи сотрудников, так как он содержит много лишней информации (в случаях низкой вероятности успешных атак), что, в свою очередь, усложняет расчеты. В рамках данной работы рассматриваются методы сокращения графов для увеличения продуктивности систем, моделирующих социоинженерные атаки, а также модернизация логики построения коэффициентов (в случаях, когда из-за заинтересованности сотрудников в проведении успешной атаки вероятность ее успеха резко возрастает). Материалами для этого исследования могут служить данные из социальных сетей, а также характеристики сотрудников, собираемые специальными департаментами компаний. Социальные сети могут предоставить довольно обширную информацию о характере взаимоотношений между сотрудниками, степени их доверия, а также пролить свет на их личностные особенности, которые используются злоумышленниками для достижения положительного результата своей деятельности.

Заключение. В результате данного исследования планируется получить алгоритм построения социального графа взаимодействия сотрудников компании, который сможет в разы упростить вычисления потенциальных угроз, а также позволит «на лету» изменять параметры данного графа для достижения лучших результатов в рамках обеспечения безопасности компании от социоинженерных атак, затрагивающих группы пользователей. Также предполагается найти общие черты таких уязвимых мест, для обеспечения быстрого реагирования служб обеспечения безопасности компаний.

СПИСОК ЛИТЕРАТУРЫ

1. Абрамов М. В., Азаров А. А., Тулупьева Т. В., Тулупьев А. Л. Модель компетенций профиля злоумышленника. // Информационно-управляющие системы. 2016. N 4. С. 77-84.
2. Азаров А.А., Тулупьева Т.В., Суворова А.В., Тулупьев А.Л., Абрамов М.В., Юсупов Р.М. Социоинженерные атаки. Проблемы анализа. СПб.: Наука, 2016. 352 с.
3. Багрецов Г.И., Шиндарев Н.А., Абрамов М.В., Тулупьева Т.В. ПОДХОДЫ К АВТОМАТИЗАЦИИ СБОРА, СТРУКТУРИРОВАНИЯ И АНАЛИЗА ИНФОРМАЦИИ ОСОТРУДНИКАХ КОМПАНИИ НА ОСНОВЕ ДАННЫХ СОЦИАЛЬНОЙ СЕТИ // Труды VII всероссийской научно-практической конференции «Нечёткие системы, мягкие вычисления и интеллектуальные технологии» НСМВИТ-2017 (г. Санкт-Петербург, 3-7 июля, 2017 г.). — в 2 т. Т. 1. — СПб.: Политехника-сервис, 2017. С. 9-15.

УДК 004.891

**СИНТЕЗ МОДЕЛИ СОЦИАЛЬНО-ЗНАЧИМОГО ПОВЕДЕНИЯ КАК БАЙЕСОВСКОЙ СЕТИ
ДОВЕРИЯ СО СКРЫТЫМИ ПЕРЕМЕННЫМИ**

Торопова Александра Витальевна

Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия, 39
email: alexandra.toropova@gmail.com

Аннотация: Моделирование поведения пользователей – это одна из главных задач для обеспечения информационной безопасности в социокomпьютинге. Модель социально-значимого поведения, оценивающая такой параметр как интенсивность поведения была синтезирована как байесовская сеть доверия со скрытыми переменными.

Ключевые слова: байесовские сети доверия; БСД; модель социально-значимого поведения.

**SYNTHESIS OF A SOCIALLY SIGNIFICANT BEHAVIOR MODEL AS A BAYESIAN BELIEF
NETWORK WITH HIDDEN VARIABLES**

Toropova Aleksandra

St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences,
Russia, St. Petersburg, 14 Line, 39.
email: alexandra.toropova@gmail.com

Abstract: User behavior modeling is one of the main tasks for information security in sociocomputing. A Socially significant behavior model that estimates such a parameter as the behavior intensity was synthesized as a Bayesian belief network with hidden variables.

Keywords: bayesian belief network; BBN; socially significant behavior model.

Введение. Для обеспечения информационной безопасности в социокomпьютинге необходимо решить задачу моделирования поведения пользователей социальных сетей. С помощью модели социально-значимого поведения можно оценить один из важнейших параметров – его интенсивность.

Данная модель основана на сведениях о последних эпизодах поведения, полученных от респондентов. Поскольку эти сведения могут быть неточны, а в некоторых случаях даже заведомо ложны (в зависимости от социального одобрения или неодобрения поведения промежутки между последними эпизодами могут быть уменьшены или наоборот увеличены), мы вносим их в модель как скрытые переменные. Байесовские сети доверия являются наиболее подходящим инструментом для синтеза модели социально-значимого поведения, так как они обладают возможностями объединения нескольких видов информации, например, полученной от экспертов или статистически, работы с неполной или неточной информацией и другими полезными свойствами. Для синтеза модели на языке C# с использованием библиотеки Smile было создано программное обеспечение, которое обеспечивает более удобную работу с моделью.

Заключение. Полученные результаты могут быть использованы не только для обеспечения информационной безопасности в социокomпьютинге, но и в других областях, например, в социологии и эпидемиологии.

СПИСОК ЛИТЕРАТУРЫ

1. GeNie&SMILE // URL: <http://download.bayesfusion.com/files.html?category=Academia> (дата обращения 07.09.2017).
2. Суворова А.В., Тулупьев А.Л., Сироткин А.В. Байесовские сети доверия в задачах оценивания интенсивности рискованного поведения // Нечеткие системы и мягкие вычисления. 2014. Т. 9, № 2. С. 115-129.
3. Торопова А.В., Суворова А.В. Анализ модели социально-значимого поведения со скрытыми переменными // XX Международная конференция по мягким вычислениям и измерениям (SCM-2017). Сборник докладов в 2-х томах. Санкт-Петербург. 24-26 мая 2016 г. Т.1. С. 81–84.
4. Торопова А.В. Использование скрытых переменных в модели социально-значимого поведения // Нечеткие системы, мягкие вычисления и интеллектуальные технологии (НСМВИТ-2017): труды VII всероссийской научной-практической конференции (г. Санкт-Петербург, 3–7 июля, 2017 г.). — в 2 т. Т. 2. — СПб.: Политехника-сервис, 2017. С. 159-165.
5. Тулупьев А. Л., Сироткин А. В., Николенко С. И. Байесовские сети доверия: логико-вероятностный вывод в ациклических направленных графах. СПб.: Изд-во С.-Петерб. ун-та, 2009. 400 с.

УДК 004.8

**АЛГЕБРАИЧЕСКИЕ БАЙЕСОВСКИЕ СЕТИ КАК ИНСТРУМЕНТ АГРЕГИРОВАНИЯ
СТАТИСТИЧЕСКОЙ И ЭКСПЕРТНОЙ ИНФОРМАЦИИ В ЗАДАЧАХ СОЦИАЛЬНОГО
КОМПЬЮТИНГА**

Тулупьев Александр Львович

Санкт-Петербургский институт информатики и автоматизации РАН,
Санкт-Петербургский государственный университет,
Россия, С.-Петербург, 14-я линия В.О., 39;
email: alexander.tulupyev@gmail.com

Аннотация: В докладе рассмотрено приложения алгебраических байесовских сетей и родственных вероятностных графических моделей к задачам агрегирования неполной, неточной, нечисловой информации, возникающих в социальном компьютеринге.

Ключевые слова: вероятностные графические модели, социальный компьютеринг, алгебраические байесовские сети, агрегирование информации, знания с неопределенностью

ALGEBRAICAL BAYESIAN NETWORKS AS A TOOL FOR STATISTICAL AND EXPERT INFORMATION AGGREGATION FOR SOCIAL COMPUTING APPLICATIONS

Tulupyevev Alexander

St. Petersburg Institute for Informatica and Automation of the Russian Academy of Sciences,
St. Petersburg State University,
Russia, St. Petersburg, 14th Line V.O., 39,
email: alexander.tulupyevev@gmail.com

Аннотация: В докладе рассмотрено приложения алгебраических байесовских сетей и родственных вероятностных графических моделей к задачам агрегирования неполной, неточной, нечисловой информации, возникающих в социальном компьютеринге.

Ключевые слова: вероятностные графические модели, социальный компьютеринг, алгебраические байесовские сети, агрегирование информации, знания с неопределенностью

Алгебраические байесовские сети (АБС) --- это логико-вероятностные графические модели знаний с неопределенностью, в которых математической моделью фрагмента знаний выступают идеалы конъюнктов со скалярными или интервальными оценками вероятности их истинности, а над самим набором фрагментов знаний (первичной структурой АБС) построен граф смежности, рассматриваемый как ее вторичная структура и используемый в различных видах логико-вероятностного вывода [2]. Помимо двух указанных видов глобальных структур рассматриваются другие возникающие системы графов [3], которые участвуют или используются в синтезе согласованных оценок истинности (априорном и апостериорном логико-вероятностном выводе, проверке и поддержании непротиворечивости моделей), в визуализации АБС, в машинном обучении АБС (при формировании локальных и глобальных структур) и др.

Одной из особенностей задач, возникающих в социальном компьютеринге, является то, что оказываются доступными большие объемы данных при небольших затратах на ее приобретение. Вместе с тем, такие данные могут содержать пропуски значений, а также отражать не все интересующие исследователя стороны изучаемого объекта или процесса: например, большие данные могут быть доступны об он-лайн поведении пользователя, а офф-лайн поведение может быть оценено лишь экспертно.

Таким образом, встает задача комбинирования (или, более строго, агрегирования) неполных, неточных, нечисловых данных, знаний, сведений из разнородных источников для последующего построения модели изучаемого явления или процесса. Примером таких сведений с экспертной стороны может быть структура модели, которая используется в задачах оценки интенсивности социально значимого поведения по сведениям о его последних эпизодах [1]. Еще одним примером может послужить сведения от эксперта, что вероятность какого-то сложного события превосходит вероятность другого [3]. Наконец, при пропусках в выборке могут появляться интервальные частотные оценки вероятностей событий [2].

АБС дают возможность комбинировать оценки такого рода. За счет учета требований аксиоматики вероятностей, а также взаимного влияния полученных оценок, могут быть получены новые, более точные оценки вероятностей. Такие оценки вероятностей окажутся представленными в форме АБС --- системы, свойства которой изучены. На основе АБС уже можно проводить различные виды логико-вероятностного вывода или использовать ее, в частности, для синтеза байесовских сетей доверия.

СПИСОК ЛИТЕРАТУРЫ

1. Азаров А.А., Тулупьева Т.В., Суворова А.В., Тулупьев А.Л., Абрамов М.В., Юсупов Р.М. Социоинженерные атаки. Проблемы анализа. СПб.: Наука, 2016. 352 с.
2. Тулупьев А.Л., Сироткин А.В., Николенко С.И. Байесовские сети доверия: логико-вероятностный вывод в ациклических направленных графах. СПб.: Изд-во С.-Петербург. ун-та, 2009. 400 с.
3. Тулупьев А.Л., Тулупьева Т.В., Суворова А.В., Абрамов М.В., Золотин А.А., Зотов М.А., Азаров А.А., Мальчевская Е.А., Левенев Д.Г., Торопова А.В., Харитонов Н.А., Бирилло А.И., Сольницев Р.И., Микони С.В., Орлов С.П., Толстов А.В. Мягкие вычисления и измерения. Модели и методы: монография. В 3 тт. Том III / под ред. д.т.н., проф. С.В. Прокопчиной. М.: ИД "НАУЧНАЯ БИБЛИОТЕКА", 2017. 300 с.

УДК 159.9.07: 316.454.52

ЭКСПРЕСС-ДИАГНОСТИКА ОСОБЕННОСТЕЙ ЛИЧНОСТИ ПО ЦИФРОВЫМ СЛЕДАМ

Тулупьева Татьяна Валентиновна

Санкт-Петербургский институт информатики и автоматизации РАН, Северо-Западный институт
управления РАНХиГС, Санкт-Петербургский государственный университет
email: tv100a@mail.ru

Аннотация: В статье рассмотрен подход к возможности предварительной экспресс-диагностики психологических особенностей пользователя по анализу его цифровых следов. Под цифровыми следами понимается информация, которую пользователь размещает на своей странице в социальной сети. В исследовании приняли участие 110 человек (студентов вузов Санкт-Петербурга), средний возраст 20,25 лет, девушек – 66,4 %, юношей – 33,6 %. Были проанализированы и идентифицированы согласно разработанной классификации 2906 постов, опубликованных пользователями за 6 месяцев до проведения тестирования. В исследовании для идентификации постов применялась разработанная авторами ранее двухуровневая классификация постов. В настоящей работе представлены выявленные взаимосвязи между типами размещенных на странице пользователя постов и психологическими особенностями.

Ключевые слова: социальные сети, цифровые следы, личностные особенности, ценностные ориентации, классификация постов

EXPRESS DIAGNOSTICS OF PERSONAL TRAITS BY DIGITAL TRACKSIvanov Oleg¹, Petrov Sergey²

Saint-Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, North-West
Institute of Management of The Russian Presidential Academy of National Economy and Public
Administration, Saint-Petersburg State University
email: tv100a@mail.ru

Abstract: The article considers approach to preliminary express-diagnostics of user's psychologic features by analyzing his digital traces. Term «digital traces» is used for denoting information that a user publishes at his personal profile in social networks. The research covers 110 respondents (students of Saint Petersburg higher education institutions), average age 20,25 years, female – 66,4 %, male – 33,6 %. During the research 2906 posts, published over last 6 months prior to testing, were analyzed and identified. A special two-level classification, developed by authors earlier, was used for posts' identification. The article deals with revealed correlations between types of posts published and psychologic features of social network account user.

Keywords: social networks, digital traces, personal traits, value orientations, post classification

Введение. Электронные социальные сети сегодня являются уже неотъемлемой частью современного общества [2]. О. М. Шахмартова и Е. Ю. Болтага в своей работе [4] рассматривают различные точки зрения на проблему «виртуальной реальности» в современной психологии. По их мнению, «компьютеризация общества является важнейшим фактором формирования коммуникативного сознания» — то есть на смену реальному собеседнику приходит виртуальный. Интернет как «пятое измерение» и новая сфера человеческой жизнедеятельности состоялась, и с каждым днем она будет иметь для каждого пользователя всё большее значение [4]. В связи с тем, что интернет занимает всё больше времени в жизни современного человека и игнорировать их влияние на жизнь молодежи невозможно [1] в научном сообществе всё чаще можно встретить исследования, посвящённые поведению людей в интернете, изучению интернет-зависимости, изучению социальных коммуникаций в интернете, влиянию социальных сетей на человека, изучению социально-психологических функций социальных сетей и т.п.

Посты в социальных сетях — один из видов «цифровых следов», которые оставляют пользователи и к которым относительно легко получить доступ. Вместе с тем, посты каждого отдельного пользователя и некоторые другие характеристики его аккаунта представляют собой достаточно содержательную систему, в которой проявляются когнитивные, эмоциональные и поведенческие компоненты общения, и которая отражает или преломляет самые разные аспекты его деятельности. Таким образом, эта система становится достаточно значимым объектом исследований для психологических наук, а также источником сведений для развития методов экспресс-диагностики при психотерапии, организации образовательного процесса, выстраивании отношений в сложных ситуациях. Также этот метод может быть использован для мониторинга изменения настроения больших социально-значимых групп.

С целью изучения возможностей определения личностных особенностей пользователя при помощи анализа аккаунтов социальных сетей было организовано пилотное исследование, позволившее собрать данные 2 способами: с помощью опроса респондентов и с помощью обработки личных страниц указанных респондентов в социальной сети «В контакте». В исследовании приняли участие 110 человек (студентов вузов Санкт-Петербурга), средний возраст 20,25 лет, девушек – 66,4 %, юношей – 33,6 %.

Были проанализированы и идентифицированы согласно разработанной классификации 2906 постов, опубликованных пользователями за 6 месяцев до проведения тестирования. В исследовании для идентификации постов применялась разработанная авторами ранее двухуровневая классификация постов, первый уровень которой содержит три атрибута: информационный, эмоциональный, побудительно-деятельностный [3]. Такая классификация не только проще воспринимается, но и позволяет сформулировать более четкие критерии классификации для экспертов, что увеличивает согласованность даваемых ими оценок

Были выявлены взаимосвязи между типами размещенных на странице пользователя постов и психологическими особенностями. Среди связей особо хочется выделить, что, например, информационные посты размещают пользователи более старшего возраста, со склонностью к мечтательности и экспериментированию, но не считающих удовольствие наслаждения важной ценностью в жизни, а размещение эмоционально негативного поста связано с повышенной чувствительностью, художественным восприятием мира и действием двух механизмов психологической защиты: вытеснение и рационализация, то есть, эмоционально негативные посты являются своего рода способом облегчения своего состояния в проблемной ситуации. Кроме того, стоит обратить внимание, что и размещение изображения на аватаре также может дать дополнительную информацию о пользователе. В целом, знаний таких особенностей позволяет более рационально или более целенаправленно получить первоначальную информацию о пользователе и предположить его личностные особенности без личного контакта с человеком.

Закключение. Психологи накопили достаточно богатый диагностический инструментарий, но его нельзя применить в онлайн исследованиях, не делая их чрезмерно дорогими. Вместе с тем, нарастает число онлайн исследований, одним из выходов которых являются так называемые «большие данные». Однако пока эти большие данные неинтерпретируемы или плохоинтерпретируемы, т.к. требуют увязки с традиционными психологическими исследованиями. Описанное исследование как раз и является одним из «мостиков», который в конце концов обеспечит активное использование социальных сетей в диагностических целях.

СПИСОК ЛИТЕРАТУРЫ

1. Магомедова С. З., Камилова Р. Ш. Влияние социальных сетей // Международный научно-исследовательский журнал. № 6-3 (13), 2013. Стр. 87–88.
2. Садыгова Т.С. Социально-психологические функции социальных сетей // Вектор науки Тольяттинского государственного университета. Серия: Педагогика, психология. № 3, 2012. Стр. 192–194.
3. Тулупьева Т.В., Тулупьев А.Л., Ющенко Н.А. Проявление ценностных ориентаций пользователей социальных сетей в контенте персональных страниц (на примере сети «В контакте») // Вестник психотерапии. 2014. № 52(57), С. 37-50.
4. Шахмартова О. М., Болтага Е. Ю. Психологические аспекты общения в социальных сетях виртуальной реальности // Известия Пензенского государственного педагогического университета им. В.Г. Белинского. № 24, 2011. Стр. 1002–1008.

УДК 004.05

АЛГОРИТМЫ ПОДДЕРЖАНИЯ НЕПРОИВОРЕЧИВОСТИ В АЛГЕБРАИЧЕСКИХ БАЙЕСОВСКИХ СЕТЯХ В РАМКАХ БИБЛИОТЕКИ ALGBN MATH LIBRARY

Харитонов Никита Алексеевич

Санкт-Петербургский государственный университет,

Россия, Санкт-Петербург, Университетская набережная, 7–9,

Санкт-Петербургский институт информатики и автоматизации Российской академии наук,

Россия, Санкт-Петербург, 14 линия, 39,

email: nikita.kharitonov95@yandex.ru

Аннотация: Основным аппаратом для проверки соответствия оценок вероятности конъюнктов в алгебраических байесовских сетях законам вероятностной логики являются алгоритмы поддержки непротиворечивости. На данный момент разработаны алгоритмы поддержания непротиворечивости в ациклических алгебраических сетях. Они реализованы в математической библиотеке AlgBN Math Library, посвященной работе с алгебраическими байесовскими сетями.

Ключевые слова: вероятностные графические модели; алгебраические байесовские сети; непротиворечивость

ALGORITHMS FOR CHECKING CONSISTENCY IN ALGEBRAIC BAYESIAN NETWORKS IN LIBRARY ALGBN MATH LIBRARY

Kharitonov Nikita

The St. Petersburg State University,

Russia, St. Petersburg, 11 Lieutenant Shmidt Emb,

St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,

Russia, St. Petersburg, 14 Line, 39,

email: nikita.kharitonov95@yandex.ru

Abstract: The main apparatus for checking the correspondence of estimates of the probability of conjuncts in algebraic Bayesian networks to the laws of probability logic are the algorithms for maintaining consistency. At the moment, algorithms for maintaining consistency in acyclic algebraic networks have been developed. They are implemented in the mathematical library AlgBN Math Library, dedicated to work with algebraic Bayesian networks.

Keywords: *probabilistic graphical models; algebraic Bayesian networks; consistency*

Введение. Алгебраические байесовские сети являются одним из классов вероятностных графических моделей. Они представляются в виде ненаправленных графов с идеалами конъюнктов в узлах. В отличие от других вероятностных графических моделей, например, байесовских сетей доверия, алгебраические байесовские сети поддерживают работу с интервальными оценками вероятности истинности. Существует математическая программная библиотека AlgBN Math Library, позволяющая работать с ациклическими алгебраическими байесовскими сетями.

Алгебраические байесовские сети подчиняются законам вероятностной логики, которые необходимо проверять. Для описания соответствия оценок вероятности истинности конъюнктов в созданной имеющейся алгебраической байесовской сети используется такое понятие, как непротиворечивость. Всего выделяют четыре степени непротиворечивости: локальная, экстернальная, интернальная и глобальная. В библиотеке AlgBN Math Library реализованы алгоритмы проверки степеней непротиворечивостей, соответствующих ациклическим алгебраическим байесовским сетям.

Заключение. Часть математической библиотеки AlgBN Math Library, реализующая алгоритмы проверки непротиворечивости, позволяет получать алгебраические байесовские сети соответствующих степеней непротиворечивости. В дальнейшем планируется оптимизация существующих подходов.

СПИСОК ЛИТЕРАТУРЫ

1. Золотин А.А., Тулупьев А.Л., Сироткин А.В. Матрично-векторные алгоритмы локального апостериорного вывода в алгебраических байесовских сетях над пропозициями квантами // Научно-технический вестник информационных технологий, механики и оптики. 2015. Т. 15. № 4. С. 676–684.
2. Тулупьев А.Л., Николенко С.И., Сироткин А.В. Байесовские сети: логико-вероятностный подход. СПб: Наука, 2006. 607 с.



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

УДК 004.056.53

ИССЛЕДОВАНИЕ СОЗДАНИЯ БЕЗОПАСНЫХ ПРОГРАММ ДЛЯ ВЫСОКОПРОИЗВОДИТЕЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ ПЛАТФОРМЫ

Бежан Роман Романович, Медведев Михаил Сергеевич, Арустамов Сергей Аркадьевич
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский пр., 49,
emails: romanbezhan@gmail.com, mmedvedev.793@mail.ru, sergey.arustamov@gmail.com

Аннотация: В статье рассмотрены способы создания безопасных программ на примере высокопроизводительной вычислительной платформы SAP HANA, различные реализации и сценарии атак, а также методы их защиты. В ходе исследования был использован подход - исследование безопасных программ с применением готовых автоматических программных решений.

Ключевые слова: JavaScript; XSJS; высокопроизводительная вычислительная платформа; SAP HANA; UI, безопасность программ.

RESEARCH OF ERP SECURE PROGRAMS CREATION

Bezhan Roman, Medvedev Mikhail, Sergey Arustamov
The St. Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, 49 Kronverksky Pr.,
emails: romanbezhan@gmail.com, mmedvedev.793@mail.ru, sergey.arustamov@gmail.com

Abstract: The article presents different ways of creation of secure programs by example of ERP SAP HANA, various attack scenarios and implementation, as well as ways of securing programs. In the time of research there was special kind of analysis used – the analysis with the implementation of ready-made automatic software-based solutions.

Keywords: JavaScript; XSJS; Enterprise Resource Planning; SAP HANA; UI5; application security.

В быстро меняющемся информационном мире ежедневно создаются новые информационные технологии, которые успешно находят свое применение в бизнесе. Но с использованием новых технологий, неизбежно появляются новые риски их использования благодаря невыявленным возможным программным уязвимостям. Лидером по созданию высокопроизводительных вычислительных платформ является компания SAP, головной офис которой расположен в Германии. В качестве высокопроизводительной вычислительной платформы, для исследования создания безопасных программ, была выбрана система SAP HANA с установленным фреймворком UI5. SAP HANA – это специализированная бизнес платформа, основной особенностью которой, является использование оперативной памяти для вычислений аналитики в режиме реального времени (технология «In Memory»), а также создание и использование программ для управления бизнес процессами [1].

Для исследования создания безопасных программ для высокопроизводительной вычислительной платформы SAP HANA, за список возможных угроз была выбрана выборка часто встречаемых угроз в программах согласно исследованию, за 2017 год открытого проекта по безопасности OWASP [2]. Были рассмотрены угрозы: уязвимость внедрения кода, некорректная аутентификация и управление сессией, межсайтовый скриптинг, ослабленный контроль доступа, небезопасная конфигурация, утечка чувствительных данных, недостаточная защита от атак, подделка межсайтовых запросов, использование компонентов с известными уязвимостями, недостаточно защищенные API. Угрозы были изучены и применены согласно контексту высокопроизводительной вычислительной платформы.

В процессе исследования был сконфигурирован специализированный стенд, для разработки безопасных программ для высокопроизводительной вычислительной платформы, на примере открытого решения Eclipse Luna [3]. В качестве первоначально тестируемых приложений были выбраны программы, основой которых служит язык XSJS. XSJS - язык программирования, созданный компанией SAP на основе языка JavaScript. Были написаны программы на данном языке с учетом

выборки часто встречаемых угроз проекта OWASP. При исследовании созданных приложений использовалось готовое программное решение – сканер уязвимостей и исходного кода CheckMarx. Данный сканер выявил устаревшую версию библиотеки пакета jQuery [4], которая имела в себе уязвимость межсайтового скриптинга DOM. Дальнейшее исследование показало, что уязвимость была закрыта специальным дополнительным кодом, написанным отдельно от данной библиотеки.

Заключение. В ходе создания безопасных программ для высокопроизводительной вычислительной платформы на примере платформы SAP HANA и программ на языке XSJS были выявлены угрозы, согласно выборке открытого проекта по обеспечению OWASP, а также ее закрытие средствами производителя. Так как исследование проводилось с применением готовых автоматических программных решений, в дальнейших планах проведение анализа вручную. Также, учитывая другие поддерживаемые языки программирования для написания собственных бизнес приложений платформой SAP HANA, предполагается рассмотреть другие языки, помимо XSJS.

СПИСОК ЛИТЕРАТУРЫ

1. Хабрахабр, блог компании SAP [Электронный ресурс] / Режим доступа: <http://habrahabr.ru/company/sap/blog/252539/> (18.09.2017)
2. OWASP, Top 10 Application Security Risks [Электронный ресурс] / Режим доступа: https://www.owasp.org/index.php/Top_10_2017-A2-Broken_Authentication_and_Session_Management (18.09.2017)
3. Википедия, Eclipse [Электронный ресурс] / Режим доступа: [https://ru.wikipedia.org/wiki/Eclipse_\(среда_разработки\)](https://ru.wikipedia.org/wiki/Eclipse_(среда_разработки)) (18.09.2017)
4. Википедия, jQuery [Электронный ресурс] / Режим доступа: <https://ru.wikipedia.org/wiki/JQuery> (18.09.2017)

УДК 004.942

УСЛОВИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КЛИНИЧЕСКОЙ СФЕРЕ СИСТЕМЫ ЗДРАВООХРАНЕНИЯ

Блюм Владислав Станиславович

Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия, 39,
email: vlad@blum.spb.su

Аннотация: В статье рассмотрены условия информационной безопасности пациентов, которая обеспечивается новой организацией цифровой клинической медицинской информации и достижением ею свойств полноты, достоверности и доступности для автоматизированной обработки. Рассмотрена телекоммуникационная структура единой государственной информационной системы здравоохранения, обеспечивающей сбор и сохранение полного объема первичной медицинской информации. Предложена динамическая информационная (математическая) модель полной, достоверной и доступной для автоматизированной обработки первичной медицинской информации. Модель описывает процесс сбора электронных персональных медицинских записей и формирования федеральной базы интегрированных электронных медицинских карт.

Ключевые слова: информационная безопасность пациентов; электронная персональная медицинская запись; интегрированная электронная медицинская карта.

CONDITIONS OF INFORMATION SECURITY IN THE CLINICAL SPHERE HEALTH SYSTEMS

Blum Vladislav

St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,
Russia, St. Petersburg, 14 Line, 39
email: vlad@blum.spb.su

Abstract: The article considers the information security conditions for patients, which is provided by a new organization of digital clinical medical information and the achievement of its completeness, reliability and accessibility features for automated processing. The telecommunication structure of the unified state health information system providing collection and preservation of the full volume of primary medical information is considered. A dynamic information (mathematical) model of complete, reliable and accessible for automated processing of primary medical information is proposed. The model describes the process of collecting electronic personal medical records and the formation of a federal database of integrated electronic medical records.

Keywords: information safety of patients; electronic personal medical record; integrated electronic medical record.

Введение. Информационная безопасность пациентов складывается из гарантированного сбора и непрерывного автоматического контроля полной интегрированной цифровой истории болезни пациента для раннего обнаружения дефектов оказания медицинской помощи.

Предложена математическая модель формирования динамической базы интегрированных электронных медицинских карт (ИЭМК). Рассмотрены некоторые алгоритмы непрерывного мониторинга ИЭМК с целью управления лечебно-диагностическим процессом.

Заключение. «Цифровая» медицина создаёт новые, принципиально иные информационные условия для управления лечебно-диагностическим процессом на основе формирования полного информационного медицинского портрета пациента и его непрерывного анализа с учётом реального времени.

СПИСОК ЛИТЕРАТУРЫ

1. Блюм В.С., Заболотский В.П. Мысленный эксперимент по организации учета и обработки информационных медицинских услуг. Врач и информационные технологии, №4 2009. С.27–35
2. Tarakanov A. O., Skormin V. A., Sokolova S. P. Immunocomputing: Principles and Applications. New York.: Springer, 2003, 230 p.
3. Блюм В.С., Заболотский В.П. Иммунная система и *иммунокомпьютинг*. Математическая морфология. Электронный математический и медико-биологический журнал (том 6 выпуск 4, 2007). Зарегистрировано 29.01.2008 под номером 0420700004/0039.
4. Блюм В.С. Инновационная государственная система медицинской статистики. АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЭКОНОМИКИ И УПРАВЛЕНИЯ. 2015.- 80-88 с.

УДК 004.052.2

ЗАЩИТА ИНФОРМАЦИИ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА В МНОГОУРОВНЕВЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Бондаренко Игорь Борисович, Шиманчук Сергей Николаевич
Санкт-Петербургский национальный исследовательский университет
Россия, Санкт-Петербург, Кронверский проспект, 49,
emails: igorlitmo@rambler.ru, shimanchuk.s@gmail.com

Аннотация: В данной работе рассмотрены структура многоуровневых автоматизированных систем, существующие проблемы и способы их комплексной защиты, с учётом всех возможных ограничений. Для реализации защиты данных систем также были рассмотрены основы многоагентного подхода, благодаря которому, можно не просто осуществлять поиск оптимального решения на каждом уровне, но и учитывать взаимосвязи между всеми уровнями системы.

Ключевые слова: *информационные технологии; информация; многоуровневая автоматизированная система; многоуровневая система защиты; многоагентный подход.*

PROTECTION OF CONFIDENTIAL INFORMATION IN AUTOMATED MULTI-LEVEL SYSTEM

Bondarenko Igor, Shimanchuk Sergey
St. Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronverksky Pr. 49,
emails: igorlitmo@rambler.ru, shimanchuk.s@gmail.com

Abstract: This paper discusses the structure of multi-level automated systems, the existing problems and their comprehensive protection, taking into account all the possible restrictions. To implement data protection systems and bases were considered multi-agent approach, thanks to which, you can't just search for the optimal solution in each level, but also take into account the relationships between all levels of the system.

Keywords: *information technology; information; multilevel automated system; multi-level protection system; multi-agent approach.*

Введение. Роль информационных технологий в современном мире невозможно переоценить. Всё, с чем имеет дело человек в любой сфере деятельности тесно связано с какой-либо техникой, на которой хранится и обрабатывается самый ценный ресурс двадцать первого века – информация.

Информация может быть не критичной, т.е. общедоступной, распространение которой обычно не влечёт за собой тяжких последствий и ущерба её владельцу, но она также может быть и конфиденциальной, распространение которой третьим лицам может привести к большим потерям.

С использованием сложных автоматизированных систем (далее АС), проблема защиты информации усложняется, так как необходимо не просто осуществление некоторой совокупности технических или организационных мер, а создание целостной системы мероприятий и применения специфических средств и методов по защите информации во всей системе.

Архитектура сложных АС представляет собой многоуровневую иерархическую систему. Низший уровень – это датчики и исполнительные механизмы, которые могут иметь встроенный микроконтроллер и цифровой интерфейс. Первый уровень составляют программируемые логические контроллеры и устройства ввода-вывода. На втором уровне располагаются рабочие станции с установленными системами диспетчерского управления, которые осуществляют мониторинг и анализ действий оператора, аварийных ситуаций и запуск управляющих процедур. В третьем уровне объединяются автоматизированные системы управления и автоматизированные системы управления

процессами. В зависимости от масштабов предприятия варьируется количество уровней в АС и может осуществляться интеграция с четвёртым уровнем – высшего руководства, которое может быть удалённым [1].

Таким образом, необходимо обеспечить достаточную защищённость каждого уровня иерархической системы, предварительно определив все возможные актуальные угрозы перехвата информации. Для нулевого уровня актуальным будет съём информации путём использования побочных электромагнитных наводок и использование акустоэлектрического сигнала. Первый уровень необходимо защищать от съёма информации по акустическому каналу, съёму информации с окон, от специальных фотоаппаратов, электросетевых подслушивающих устройств и специальных средств приёма побочных электромагнитных наводок. Со второго по четвёртый уровень к вышеперечисленным каналам утечки информации добавляются съём информации с помощью высокочастотного навязывания, с телефонной линии связи, закладных устройств и диктофонов, а также видеосъёмки [2].

Кроме того, при обеспечении защиты необходимо учитывать возможные ограничения, которые могут быть габаритными, аппаратными, ограничениями по стоимости или ресурсам. Данные ограничения задаются владельцем систем исходя из целей создания системы защиты и бюджета, выделенного на создание данной системы.

Сложность решения многоуровневой защиты также заключается в том, что множество оптимальных решений, найденных на подуровнях, не означают, что достигнут оптимум для всей системы в целом. Это происходит из-за существования межуровневых связей, которые влияют на процесс нахождения решения, и приводят к тому, что сам процесс решения имеет лавинообразный характер.

Состав средств и методов, входящих в комплексную систему защиты определяется на основе проведения процедуры обследования объекта защиты, однако концепция комплексной защиты должна удовлетворять следующим требованиям:

- использовать все механизмы защиты;
- рационально реализовывать все необходимые мероприятия по защите информации на базе достигнутого уровня прогресса;
- должны существовать механизмы практической реализации требуемого уровня защищённости информации [3].

Одним из решений защиты автоматизированных систем, с целью увеличения их времени функционирования является внедрение в систему блоков, которые осуществляют диагностику, реорганизацию и адаптацию структуры, подстраивая её под условия функционирования и учитывая потери от неблагоприятных воздействий. При этом работоспособные ресурсы перераспределяются и используются для достижения основной цели, но вместе с тем, отбираются у менее значимых процессов. Тем самым, количество решаемых задач уменьшается в пользу основного процесса, вследствие этого падает качество функционирования, но время функционирования растёт.

Также существует и другой подход для решения данной задачи, который заключается в выделении координирующих переменных, определяющих взаимосвязи нижних и верхних уровней. При этом необходимо декомпозировать всю систему на подсистемы с меньшей размерностью для решения локальных оптимизационных задач. После этого определяют межуровневые коэффициенты взаимосвязи и рассчитывают матрицы для коэффициентов отдельных подуровней.

Однако данный подход для систем с большой размерностью представляет сложную вычислительную задачу, особенно если учитывать разного рода ограничения.

В связи с этим, наиболее практичным и действующим решением для защиты сложных АС предлагается представление данных АС через многоагентную систему, которая позволяет найти оптимальное рабочее решение обеспечения безопасности на каждом уровне защищаемой АС, учитывая при этом существующие в системе межуровневые связи.

Структура такой многоагентной системы может включать в себя следующих агентов: агент-координатор уровня управления, датчиков, технологического оборудования, диспетчерского уровня, а также управляющего поискового агента. Агенты-координаторы будут являться реактивными агентами, осуществляющие распределение оптимальной защиты на каждом уровне, в соответствии с допущенными ограничениями. Взаимодействие всех агентов-координаторов осуществляется через управляющего поискового агента, на котором программируются все допущенные ограничения. Выбор оптимального рабочего решения будет осуществляться с использованием муравьиного или генетического алгоритмов, в зависимости от характеристик и размерности защищаемых АС.

Заключение. Таким образом, на сегодняшний день не существует эталонной модели защиты сложных автоматизированных систем. Поэтому необходимо выстраивать свою методику защиты, объединяя несколько подходов и используя различные алгоритмы, осуществляющие поиск оптимальных решений. А также рассматривать многоуровневую АС как единую систему, чтобы получать адекватную оценку состояния системы защиты и находить действительно оптимальное решение для всей системы в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Коробейников А.Г., Бондаренко И.Б., Прохожев Н.Н., Михайличенко О.В. Принятие технических решений с помощью многоагентных систем // NB: Кибернетика и программирование – 2013. – №1. – С. 16-20.
2. Алексенко В.Н., Дреус Ю.Г. Основы построения системы защиты производственных предприятий и банков. // Учебное пособие.- М.: МИФИ, 1996.
3. Семкин С.Н., Беляков Э.В., Гребенев С.В., Козачок В.И., Основы организационного обеспечения информационной безопасности объектов информатизации: Учебное пособие. – М.: Гелиос АРВ, 2004-265с.

УДК 004.056

**ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ НСД С ИСПОЛЬЗОВАНИЕМ
БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ**

Брагина Елизавета Константиновна, Егоров Илья Эдуардович
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский проспект, 49,
emails: AlisBrain@mail.ru, mynameisiliaegorov@gmail.com

Аннотация: В статье исследуется проблема минимизации возможности получения несанкционированного доступа к информационным системам, в которых хранится и обрабатывается информация ограниченного доступа. Рассматривается метод биометрической аутентификации основанный на оценке эмоциональной экспрессии и мимики идентифицируемого пользователя путем постоянного скрытого мониторинга при помощи web-камеры. Приводится определение эмоций, анализируются методы определения эмоции по выражению лица, используемые экспертами. Сделан вывод о необходимости автоматизации процесса распознавания эмоций по выражению лица и мимике исследуемого человека. Охарактеризованы и проанализированы современные системы распознавания эмоций и методы машинного обучения. По результатам анализа для увеличения точности распознавания эмоций в алгоритме работы данных систем предложено использовать методы системы кодирования активности лицевых мышц, адаптированные для использования машиной и методы машинного обучения.

Ключевые слова: *информационные системы, информационная безопасность, биометрическая аутентификация, распознавание эмоций, система кодирования активности лицевых мышц, технологии машинного обучения.*

**INCREASING THE PROTECTION OF INFORMATION FROM UNAUTHORIZED ACCESS USING
BIOMETRIC AUTHENTICATION**

Bragina Elizaveta, Egorov Ilia
Saint Petersburg National Research University of Information Technologies, Mechanics and Optics,
49 Kronverksky Pr., St. Petersburg, 197101, Russia,
emails: AlisBrain@mail.ru, mynameisiliaegorov@gmail.com

Annotation: The article explores the problem of minimizing the possibility of obtaining unauthorized access to information system in which restricted information is stored and processed. The method of biometric authentication based on the evaluation of emotional and face expressions of an identified user is being considered by means of constant hidden monitoring with help of web camera. The definition of emotions is given, methods for determining emotion by facial expressions, used by experts, are analyzed. The conclusion is made about the necessity of the automation the process of recognizing emotions by expressing the face and facial expressions of the person being studied. Characterized and analyzed modern systems of recognition of emotions and methods of machine learning. Based on the results of the analysis, to increase the accuracy of the recognition of emotions in the algorithm of the operation of these systems, it is proposed to use methods of the coding system for the activity of facial muscles, adapted for use by the machine and methods of machine learning.

Keywords: *information systems, information security, biometrical authentication, emotion recognition, system of coding facial muscles, machine learning technologies.*

Введение. В наше время неотъемлемой частью всевозможных сфер повседневной деятельности человека стало использование информационных систем (далее – ИС). ИС используются для хранения, обработки и поиска информации, в том числе и информации ограниченного доступа. Право доступа к данной информации ограничено установленными законами, нормами и правилами [1], поэтому существует потребность в обеспечении её информационной защищенности, а, следовательно, и информационной защищенности ИС.

Достижение состояния защищённости информации в ИС обеспечивается созданием комплексной системы защиты, одной из главных составляющих которой являются методы защиты от несанкционированного доступа (далее – НСД).

Основой программно-технических средств защиты от НСД являются процедуры идентификации (пользователь называет себя) и аутентификации (проверки подлинности) пользователей [2].

Существуют три типа метода аутентификации, однако первые два типа, которые являются более традиционными для современного человека, процедуры аутентификации (основанные на знании чего-либо, на владении чем-либо) имеют существенные недостатки, такие как: простота подбора, риск кражи или утери, копирование и т.д. Третий метод (основанный на части самого пользователя) – биометрическая аутентификация или аутентификация на основе биометрических характеристик (далее – БХ) имеет следующие преимущества:

- БХ удобно использовать благодаря отсутствию необходимости контакта;
- БХ невозможно потерять или забыть, т. к. они являются частью идентифицируемого пользователя (далее – ИП);
- значительно затруднены передача и подделка БХ.

Проанализировав современные методы биометрической аутентификации можно смело сказать то, что метод, основанный на оценке эмоционального состояния и мимики, является наиболее перспективным, т. к. его использование снижает вероятность возникновения ошибок первого и второго рода, тем самым повышая защищенность ИС [3].

Рассматриваемый авторами метод биометрической аутентификации основан на оценке эмоциональной экспрессии и мимики ИП путем постоянного скрытого мониторинга при помощи web-камеры.

Алгоритм данного метода описан далее.

Шаг 1. Создание базы данных личных карточек пользователей.

В личных карточках пользователей должна храниться информация об исследовании эмоциональной экспрессии и мимики ИП во время повседневной работы в ИС, а именно: атласы фотоизображений (размеченные фотографии ИП), основные характеристики динамики эмоциональной экспрессии, результаты определения эмоций и анализ эмоционального состояния с учетом влияния внешних факторов.

Шаг 2. Распознавание эмоций ИП в динамической форме.

Распознавание эмоций ИП в динамической форме осуществляется по средствам web-камеры с достаточным уровнем характеристик (тип матрицы, разрешение, оптика, чувствительность матрицы и т.д.), установленной на автоматизированном рабочем месте.

Шаг 3. Сравнение результатов шага «2» с базой данных, созданной на шаге «1».

Под сравнением следует понимать выявление отклонений результатов постоянного определения эмоций от эталонов, хранящихся в базе данных.

Шаг 4. Анализ результатов сравнения.

Последующий анализ данных отклонений заключается в определении возможности возникновения инцидента (на данном шаге система определяет возможность несанкционированных действий пользователя).

Шаг 5. Предпринятие соответствующих действий/мер.

Далее система должна предпринять соответствующие действия/меры, например, подать предупреждающий сигнал на пост охраны

Закключение. Оправданность идеи создания системы биометрической аутентификации с предложенным алгоритмом работы обусловлена выдвинутыми авторами гипотезами:

- эмоциональному состоянию и мимике человека свойственны постоянные изменения в зависимости от внешних и внутренних факторов, но при этом проявление эмоций – это подсознательный процесс, что практически исключает возможность сокрытия и подмены, используемой БХ;
- лицо человека, который замыслил некоторую атаку на ИС, будет выражать конкретные эмоции, которые будут отличаться от повседневных;
- выбранная БХ (эмоции и мимика) одинаково проявляется у представителей различных культур;
- использование данного метода биометрической аутентификации снизит вероятности возникновения ошибок первого и второго рода, позволит применять аутентификацию прозрачно для пользователя и выявлять НСД уже после выполнения входа в систему.

СПИСОК ЛИТЕРАТУРЫ

1. Домарев В. В. Безопасность информационных технологий. Системный подход //К.: ООО ТИД Диа Софт. – 2004.
2. Методы и средства защиты от несанкционированного доступа // URL: <http://www.panasenko.ru/Articles/77/77.html> (дата обращения: 11.03.2017).
3. Брагина Е.К., Соколов С.С. Современные методы биометрической аутентификации: обзор, анализ и определение перспектив развития. – Вестник Астраханского государственного технического университета. – 2015. – №. 1.

УДК 004.77

РАЗРАБОТКА АППАРАТНО-ПРОГРАММНОГО КОМПЛЕКСА ИДЕНТИФИКАЦИИ СОСТОЯНИЯ ОБЪЕКТОВ И СУБЪЕКТОВ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИЙ ИНТЕРНЕТ ВЕЩЕЙДикий Дмитрий Игоревич¹, Артемьева Виктория Денисовна²¹ Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики,

Россия, Санкт-Петербург, Кронверкский пр., 49,

² Балтийский федеральный университет им. И. Канта,

Россия, Калининград, ул. А. Невского, 14а,

emails: dimandikiy@mail.ru, vika_med2019@mail.ru

Аннотация: В статье рассмотрен подход к проектированию аппаратно-программного комплекса, главной задачей которого является идентификация движимых и недвижимых объектов с применением технологий Интернет вещей. Данный подход планируется использовать при создании автоматизированной системы в рамках образовательного учреждения высшего образования. Это накладывает особые требования к разрабатываемому комплексу. Например, он должен работать как на идентификацию передвижения людей (людских потоков), так и материальных ценностей. Основа подхода заключается в использовании радиочастотных пассивных меток (RFID), с помощью которых можно пометить объекты и регистрировать их местоположение в реальном времени.

Ключевые слова: проектирование; RFID; аппаратно-программный комплекс; идентификация; локация

DEVELOPMENT OF HARDWARE AND SOFTWARE IDENTIFY THE STATE OF OBJECTS AND SUBJECTS WITH APPLICATION OF TECHNOLOGIES OF INTERNET OF THINGSDikii Dmitrii¹, Artemeva Viktoriia²¹ Saint Petersburg National Research University of Information Technologies, Mechanics and Optics, Russia, St. Petersburg, Kronverksky Ave 49,² Immanuel Kant Baltic Federal University,

Russia, Kaliningrad, A. Nevsky Street 14a,

emails: dimandikiy@mail.ru, vika_med2019@mail.ru

Abstract: The article describes the approach to designing hardware-software complex, whose main task is to identify movable and immovable objects with the use of technologies the Internet of things. This approach will be used for creation of automated system in educational institutions of higher education. This imposes special requirements to develop the complex. For example, it needs to work on the identification of the movement of persons (flows of people: students, teachers) and material assets (computers, expensive equipment). The approach is to use passive radio frequency tags (RFID), with which you can mark the objects and record their location in real time.

Keywords: design; RFID; the hardware-software complex; identification; location

Введение. Системы мониторинга положения объектов с начала 2000х находят свое применение во многих сферах жизни человека. Одним из ярких примеров, является использование компанией Amazon системы определения положения объектов в складских помещениях и магазинах [1]. Однако данные технологии могли бы быть хорошо применимы в образовательных организациях, например, для мониторинга посещения студентами лекций и семинаров и т.д.

Описание подхода. Аппаратно-программный комплекс (АПК) предназначен для решения задач идентификации и определения места положения помеченных субъектов, документов и объектов материальных ценностей на заданных территориях. Объекты и субъекты накладываются одним или несколькими видами меток: графические (штрих коды, QR-коды), RFID-метки — пассивные метки; средства для идентификации в режиме реального времени (WiFi/GPS/GPRS-трекеры). Определение их позиции (наличия) осуществляется с помощью стационарных и портативных сканеров графических и RFID-меток [2], а также использования WiFi роутеров, мобильных и стационарных средств сотовой связи. Идентификация субъектов и объектов определяется с помощью распознавания сигнатур всех типов меток, а также средств идентификации в режиме реального времени. АПК применяется для выполнения проверочных, инвентаризационных и исследовательских мероприятий, определяющих выполнение заданных требований по наличию и месту расположения субъектов и объектов, например, проверка комплектности документов, посещаемость зон мероприятий (в частности, студентов и преподавателей в аудиториях, участников конференции). АПК и отдельные компоненты будут эксплуатироваться в крытых помещениях или в уличных условиях при диапазоне рабочих температур от 0 до 50°C. Централизованный сбор идентификационной информации позволит реализовывать мониторинг в режиме реального времени положения и некоторых признаков состояния идентифицируемых объектов и субъектов.

Примеры процессов, в которых может применяться АПК: мониторинг потоков критических документов в кампусе учреждения высшего образования; отслеживание положения различных материальных ценностей; определение наличия документов, участников конференций и других.

Основное назначение аналогичных систем состоит в контроле человеческих потоков в учебных заведениях (в частности «Система контроля и управления доступом на основе систем SALTO XS4 RFID» [3], «RFID портал» рабочая частота UHF 860-960 МГц), либо в управлении складами или архивами (в частности, ТЭНДО: RFID-архив [4], «Система защиты бумажных носителей информации» рабочая частота UHF 860-960 МГц). Сведения об идентификации комплексных процессов с участием персон, материальных ценностей и документов в учебном заведении (в частности, для определения события выноса конкретного устройства или документа конкретной персоной из конкретного помещения) найти не удалось.

Заключение. Таким образом, в целях обеспечения своевременного и успешного расследования инцидентов информационной безопасности внутри образовательных учреждений имеет смысл создать автоматизированную систему мониторинга перемещения движимых и недвижимых объектов. На данный момент разработаны все необходимые технологии и протоколы для выполнения этой задачи. Поэтому стоит уделить внимание разработке такой системы идентификации объектов в реальном времени.

СПИСОК ЛИТЕРАТУРЫ

1. How 'Amazon Go' works: The technology behind the online retailer's groundbreaking new grocery store // [Электронный ресурс] URL: <https://www.geekwire.com/2016/amazon-go-works-technology-behind-online-retailers-groundbreaking-new-grocery-store/> (дата обращения: 21.09.2017).
2. Brennan D, Kolaja J Real Time Location System using Passive UHF RFID // 15th International Carpathian Control Conference (ICCC). 2014. С. 58-62.
3. Концепция построения СКВД (системы контроля и управления доступом) учреждения системы здравоохранения на основе систем SALTO. // [Электронный ресурс] SaltoSystems URL: <http://saltosystems.ru/application/helthcare.php> (дата обращения: 21.09.2017).
4. Комплексная автоматизация бизнес процессов // [Электронный ресурс] URL: <http://www.tendo.ru/> (дата обращения: 21.09.2017).

УДК 004.056

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ КИБЕРФИЗИЧЕСКИХ СИСТЕМ НА ОСНОВЕ ГОМЕОСТАТА

Зегжда Петр Дмитриевич, Зегжда Дмитрий Петрович, Павленко Евгений Юрьевич

Санкт-Петербургский политехнический университет Петра Великого,

Россия, Санкт-Петербург, ул. Политехническая, 29

emails: kafedra@ibks.spbstu.ru, dmitry.zegzhda@ibks.ftk.spbstu.ru, pavlenko@ibks.spbstu.ru

Аннотация: Проведен анализ существующих подходов к управлению безопасностью киберфизических систем (КФС). Предложена стратегия гомеостатического управления безопасностью, основанная на удержании КФС в области функциональной устойчивости. Описана структура гомеостата и разработана модель работы гомеостата с использованием логических предикатов. Рассмотрены критерии оценки функциональной устойчивости КФС, представлены результаты экспериментальных исследований, показывающие возможность применения предложенных критериев.

Ключевые слова: информационная безопасность, гомеостаз, управление безопасностью, безопасность киберфизических систем, гомеостат, апостериорная защита.

SECURITY MANAGEMENT OF CYBER-PHYSICAL SYSTEMS BASED ON HOMEOSTAT

Zegzhda Petr, Zegzhda Dmitry, Pavlenko Evgeny

The St. Petersburg State Polytechnic University of Peter the Great,

Russia, St. Petersburg, Polytechnicheskaya str. 29,

emails: kafedra@ibks.spbstu.ru, dmitry.zegzhda@ibks.ftk.spbstu.ru, pavlenko@ibks.spbstu.ru

Abstract: An analysis of existing approaches to safety management of cyber-physical systems (CPS) is conducted. A strategy of homeostatic safety management based on the retention of CPS in the field of functional stability was proposed. The structure of the homeostat is described and a model of homeostat work is developed using logical predicates. The criteria for assessing the functional stability of CPS are considered, the results of experimental studies showing the possibility of applying the proposed criteria

Keywords: information security, security management, homeostat, security of cyber-physical.

Введение. Активное развитие технологий межмашинного взаимодействия и концепции Интернета вещей, облачных технологий и аппаратной виртуализации, их интеграция с промышленными системами и комплексами привели к появлению киберфизических систем (КФС), сочетающих в себе как информационную, так и технологическую составляющую, и автономно от человека реализующих технологические процессы путем взаимного обмена данными. КФС

обеспечивают совокупное функционирование элементов кибернетического и физического пространств, интегрированных с вычислительными ресурсами, динамически изменяя свое состояние в зависимости от внешних условий и внутренних факторов. Повсеместная интеграция КФС с промышленными отраслями деятельности делает киберугрозы на объекты крайне критичными. Успешная реализация кибератак на КФС влечет за собой не только финансовые потери и ограничения на технологическое развитие страны, но и риски угрозы жизни и здоровью населения, риски возникновения экологических катастроф, угрозу национальной безопасности страны [1].

Существующая методология управления безопасностью не может быть эффективно применена в КФС в силу того, что КФС состоят из огромного числа разнородных компонентов, способных менять свое поведение. Таким образом, необходимо разработать новую методологию управления безопасностью таких систем, касающуюся обеспечения как безопасности информации (ее конфиденциальности, целостности и доступности), так и корректности протекания технологических процессов, реализуемых системами [2].

Благодаря высокой способности к коммуникации компонентов КФС и наличию единого центра управления, у КФС появляется свойство самоадаптации, которое и является основой для предлагаемой системы защиты. Авторами предлагается применить биоинспирированный гомеостатический подход для расширения понятия стратегии динамической защиты, позволяющий обеспечить сохранение внутренней среды и стабильности ее функционирования. Гомеостаз КФС заключается в обеспечении относительного равновесия системы, поддерживаемого за счет механизмов саморегуляции [3].

Любая КФС может быть представлена в виде графа, вследствие чего изменения в ее структуре будут касаться либо изменения параметров устройств (вершин графа), либо связей между устройствами (ребер графа), либо структуры всего графа. По аналогии с биологическими системами, для КФС предлагается выделить три уровня гомеостаза, основываясь на графовом представлении:

1. Гомеостаз на уровне параметрического управления технологическими процессами.

2. Гомеостаз на уровне управления связями между компонентами КФС.

3. Архитектурный гомеостаз, осуществляющий полную перенастройку КФС, ее параметров управления и связей между компонентами.

Для каждого типа гомеостаза авторами предлагается подход к контролю функциональной устойчивости: для гомеостаза на уровне параметрического управления предлагается использовать значение главной компоненты матрицы, состоящей из значений параметров управления элементов КФС; для гомеостаза на уровне управления связями предлагается использовать графовые показатели устойчивости, а для архитектурного гомеостаза – показатели фрактальности (самоподобия).

Заключение. Предлагаемая авторами стратегия гомеостатического управления безопасностью КФС учитывает специфику предметной области КФС и анализирует систему на уровне реализации технологических процессов, т.е., на логическом уровне. Выделенные уровни гомеостаза содержат все доступные изменения для графа, описывающего КФС, а значит, учитывают все возможные атаки на КФС, а предлагаемые способы контроля функциональной устойчивости на каждом уровне позволяют обеспечить оптимальное управление КФС.

СПИСОК ЛИТЕРАТУРЫ

1. Zegzhda D.P. Sustainability as a criterion for information security in cyber-physical systems / D. P. Zegzhda // Automatic Control and Computer Sciences. - 2016. - №8. - P. 813-819.
2. Зегжда Д. П. Устойчивость как критерий информационной безопасности компьютерных систем [Текст] / Зегжда Д. П. Проблемы информационной безопасности. Компьютерные системы. №2. 2016. С. 12-20.
3. Рохлов В. С., История развития учения о гомеостазе [Текст] / Рохлов В. С., Трофимов С. Б. Общая биология. №22 (797), 2015.

УДК 004.056

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. ФИШИНГ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ ЕМУ

Ильченко Лидия Михайловна, Уваров Роман Валерьевич, Зайцев Святослав Игоревич

Санкт-Петербургский национальный исследовательский университет

информационных технологий, механики и оптики,

Россия, Санкт-Петербург, Кронверкский пр., 49,

Государственный университет морского и речного флота имени адмирала С.О. Макарова

Российская Федерация, 198035, г. Санкт-Петербург, ул. Двинская, 5/7

email: Lidiya9510@yandex.ru, Sunilink@yandex.ru

Аннотация: В данной работе рассматриваются такие методы социальной инженерии, как фишинг, вишинг и спуфинг, а также методы противодействия им.

Ключевые слова: социальная инженерия, фишинг, спуфинг, TCP/IP, UDP вишинг.

SOCIAL ENGINEERING. PHISHING AND METHODS OF COUNTERING IT

Ilchenko Lydia, Uvarov Roman, Zaytsev Svyatoslav

Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics

197101, Russia, St. Petersburg, 49 Kronverksky Pr.
Admiral Makarov State University of Maritime and Inland Shipping
198035, Russia, St. Petersburg, Dvinskaya st., 5/7
email: Lidiya9510@yandex.ru, Sunilink@yandex.ru

Abstract: In this paper we consider such methods of social engineering as phishing, wishing and spoofing, as well as methods of countering them.

Keywords: social engineering, phishing, spoofing, TCP / IP, UDP vishing.

Введение. Существует множество векторов потенциальной атаки, рассматриваемых в рамках информационной безопасности, среди них особую популярность имеют технические каналы утечки информации: вибро-акустические, акустоэлектрические, оптические каналы, утечки по каналам ПЭМИН и др. [1]. В связи с чем постоянно развиваются средства противодействия потенциальным атакам. На сегодняшний день, обойти средства криптографической защиты информации, безупречные протоколы безопасности, средства физической защиты и пр. фактически невозможно, однако, руководители и специалисты по защите информации часто пренебрегают угрозами со стороны инсайдеров [2.]

Действия внутреннего злоумышленника можно разделить на умышленные и неумышленные действия, имеющие негативный характер.

Доля утечек информации по вине сотрудников сокращается в течение последних четырех лет в мире [3], однако, это скорее связано с увеличением числа атак внешнего нарушителя, поскольку невозможно добиться сокращения инцидентов халатного или злоумышленного отношения к конфиденциальным данным одним лишь внедрением технических средств защиты информации. [4]

Социальная инженерия. На сегодняшний день на первый план выходит не новый, но редко рассматриваемый источник угроз – социальная инженерия.

Под социальной инженерией здесь и далее будет пониматься инструмент внешнего нарушителя, посредством которого реализуется атака на системы с использованием человеческого фактора, направленный на нарушение конфиденциальности, целостности и (или) доступности информационных ресурсов.

Целевой фишинг – техника в социальной инженерии, направленная на получение сведений конфиденциального характера с применением средств электронной коммуникации, и выступая от другого физического или юридического лица [5].

Основным различием целевого и массового фишинга является то, что при целевом фишинге жертвами становятся сотрудники какой-то конкретной, заранее выбранной организации, либо заранее намеченное физическое лицо, в то же время при массовом фишинге жертвами становятся случайные пользователи средств электронной коммуникации [6].

Чаще всего фишинг реализуется посредством электронной почты, непосредственно само письмо содержит в себе вредоносное вложение либо ссылку на фальшивый web-ресурс, содержащий форму с требованием ввести конфиденциальную информацию. Распознать фишинговую атаку бывает проблематично по причине постоянного совершенствования техник. Тем не менее для большинства фишинговых писем характерен ряд признаков:

- сообщение имеет экстренный характер;
- сообщение содержит запрос личных сведений;
- сообщение содержит изображение в теле письма;
- сообщение содержит поддельные URL-адреса, отличающийся от оригинального одним или несколькими символами;

– сообщение содержит нереалистичные обещания [7];

– сообщение содержит вложение, в роли которого может выступать вредоносное программное обеспечение. Примечательно то, что расширение вложения может быть скрыто или искусственно изменено, а иконка соответствовать любому неисполняемому файлу, расширение которого указано. Кроме этого, к файлу может быть присоединен ярлык, содержащий настоящее расширение файла. Также вложение может использовать технологию RTLO или RLO (Right-to-Left) для зеркального отображения символов в названии файла. Существует множество других способов изменить вложенный файл, выше перечислена лишь часть из них.

Также фишеры часто использовали эксплойты, которые могут предоставить доступ уязвимым к процессам и приложениям, а также ко всей операционной системе. Данные угрозы актуальны практически для всех операционных систем, включая Windows, Linux, IOS, MacOS, Android. Многие современные антивирусы снабжены системой защиты от эксплоитов, однако пользователи зачастую сами пренебрегают предупреждениями со стороны антивирусных программ. Если они не будут раскрыты, у злоумышленника будет доступ к необходимым ему ресурсам неограниченное время.

По данным на 2013 год в 94% фишинговые письма содержат вредоносные вложения, и только в 6% случаев содержат вредоносные ссылки [8].

Условно к разновидности фишинга можно отнести атаки вида спуфинг

Спуфинг – вид атаки, реализованной путем подмены адреса отправителя, либо передаваемых пакетов с целью обмана системы безопасности. В зависимости от целей, спуфинг может быть локальным и сетевым. При локальном атака направлена на операционную систему, сетевой спуфинг же направлен на информационную систему в целом.

Одним из основных видов спуфинга являются атаки на транспортный уровень, в частности на протоколы TCP/IP, UDP:

NetBIOS/NBNS spoofing – метод, актуальный для ОС Windows, реализуется во время резолвинга сетевого имени путем подмены DNS сервера на ложный. Если запрос к серверу оказался безуспешным, то операционная система попытается реализовать резолвинг с помощью NetBIOS. А злоумышленнику достаточно выдать себя за SOMEPC, во время широковещательного запроса.

IP spoofing – атака, реализующаяся с помощью подмены IP-адреса отправителя с целью вызова ответных пакетов на ложный адрес [9]. На этом методе спуфинга построен ряд DoS-атак. Необходимо отметить, что наиболее подвержен атакам этого уровня протокол UDP, так как не имеет механизмов противодействия им. Для защиты от спуфинга IP – адреса является отправка ответного пакета на адрес отправителя, обычно злоумышленником используется недействительный (случайный) адрес, вследствие чего ответ не придет [10].

ARP спуфинг – вид атак в Ethernet сетях, направленный на перехват трафика между отдельными хостами, расположенными в пределах одного широковещательного домена. Базируется на уязвимостях протокола ARP и реализуется путем подмены mac-адреса. Современные фаерволы способны распознавать данный вид атак. А также минимизировать возможность реализации данной угрозы способом использование агр-таблиц на ключевых частях сети.

DNS Cache Poisoning (DNS-спуфинг) – атаки, направленные на изменение данных кэша доменных имен. Данный вид атак может быть предотвращен на стороне сервера путем уменьшения степени доверия сторонним данным, а также путем игнорирования любых DNS-записей, не относящихся изначальному запросу [11].

Кроме этого, к фишинговым категориям спуфинга относится подмена e-mail адреса отправителя на ложный. Чаще всего применяется в массовом фишинге, и на сегодняшний день большинство почтовых сервисов оборудовано средствами «антиспама», что позволило минимизировать угрозу со стороны данной категории атак [12]. Также известны случаи спуфинга номеров в VoIP-сетях [13], номеров в SMS-сообщениях и подмены номеров в голосовой почте [14]. Многие направления спуфинга является полноценной самостоятельной атакой, например, GPS спуфинг – атака, направленная на GPS-приемники и реализуется путем использования более мощного передатчика [15], и Referrer spoofing — подмена реферера [16].

Вишинг – метод фишинговых атак через телефонные коммуникации. Злоумышленник совершает телефонный звонок жертве под видом другого физического, юридического или должностного лица, с которым у жертвы установлены доверительные отношения. Самым надежным способом защиты является не сообщать информацию ограниченного доступа во время телефонных разговоров [17].

Таким образом, получение информации от пользователей возможно не только путем сложных технологических манипуляций, но путем использования банальной невнимательности или халатности субъектов. Что побуждает руководителей и сотрудников службы все большее внимание уделять человеческому фактору, ведь методы социальной инженерии работают везде, где хоть на одном этапе обработки информации присутствует человек.

СПИСОК ЛИТЕРАТУРЫ

1. Громыко И. А. Общая парадигма защиты информации: проблемы защиты информации в аспектах математического моделирования: монография / И. А. Громыко. — Х.: ХНУ имени В. Н. Каразина. 2014. — 216с.
2. Гридин А. Краткое введение в социальную инженерию, 2010. URL: <https://habrahabr.ru/post/83415/> (дата обращения 15.09.2017).
3. Утечки данных организаций в результате умышленных или неосторожных действий внутреннего нарушителя. Сравнительное исследование 2013-2015 гг. // Аналитический центр InfoWatch, 2017. URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_052016.pdf?rel=1 (дата обращения 16.09.2017).
4. Глобальное исследование утечек конфиденциальной информации в 2014 году // Аналитический центр InfoWatch, 2017. URL: http://ibsmol.ru/InfoWatch_global_report_2014.pdf (дата обращения 16.09.2017).
5. Кузнецов, М. В. Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов. — Санкт-Петербург: БХВ-Петербург, 2007. — 368 с.
6. Интернет-мошенничество фишинг: механизм, виды и способы противодействия - 2015. URL: <https://www.exocur.ru/internet-moshennichestvo-fishing-mehanizm-vidyi-i-sposobyi-protivodeystviya/> (дата обращения 15.09.2017).
7. Кондурак В. П. Защита от фишинг-атак, 2009. URL: <http://www.securrity.ru/articles/20-zashhita-ot-fishing-atak.html> (дата обращения 17.09.2017).
8. Морозов А. В., Шахов В. Г. Анализ атак на беспроводные компьютерные интерфейсы // ОНВ. 2012. №3 (113). URL: <http://cyberleninka.ru/article/n/analiz-atak-na-besprovodnye-kompyuternye-interfeysy> (дата обращения: 17.09.2017).
9. Хохлов Н. С. Обзор уязвимостей Wi-Fi сигнализации в системах автоматизированного управления зданиями / Хохлов Николай Степанович, Михайлов Дмитрий Михайлович, Смирнов Александр Сергеевич // Вестник ВИ МВД России. 2014. №1. С.277-281.
10. Сапожников А. А. Наблюдение аномалий в сети // Вестник ЮУрГУ. Серия: Компьютерные технологии, управление, радиоэлектроника. 2009. №26 (159). С.62-65.

11. Облачный хостинг в Европе (vps/vds) Предотвращение спуфинга адресов и защита электронной почты при помощи SPF-записи. 2016. URL: <https://www.8host.com/blog/predotvrashenie-spufiga-adresov-i-zashhita-elektronnoj-pochty-pri-pomoshhi-spf-zapisi/> (дата обращения: 17.09.2017).
12. Johnny Gabel Hack a Voicemail Account Using SpoofApp. 2012. URL: <https://computer-pranks.wonderhowto.com/how-to/hack-voicemail-account-using-spoofapp-0133304/> (дата обращения: 17.09.2017).
13. Абдеева З. Р. Проблемы безопасности электронной коммерции в сети Интернет // ПСЭ. 2012. №1. С.172-175.
14. GPS: глушилки, спуфинг и уязвимости // Блог компании Хакспейс Neuron. 2015. URL: <https://habrahabr.ru/company/neuronspace/blog/254877/> (дата обращения: 17.09.2017).
15. Christopher Hadnagy Phishing Dark Waters: The Offensive and Defensive Sides of Malicious E-mails / Christopher Hadnagy, Michele Fincher – United States of America, Indiana, Indianapolis: John Wiley & Sons, Inc., 2015. 277 с.
16. Антонов И. О. Способы мошенничества с использованием платёжных карт как элемент криминалистической характеристики данного вида преступлений / Антонов Игорь Олегович, Шалимов Анатолий Николаевич // Учен. зап. Казан. ун-та. Сер. Гуманит. науки. 2013. №4. С.196-203.

УДК 004.056

СОВРЕМЕННЫЕ НЕЙРОСЕТЕВЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ КИБЕРУГРОЗ В СЕТЯХ VANET/FANET/MARINET

Калинин Максим Олегович, Зегжда Петр Дмитриевич
Санкт-Петербургский политехнический университет Петра Великого,
Россия, Санкт-Петербург, ул. Политехническая, 29,
emails: max@ibks.spbstu.ru

Аннотация: В докладе рассмотрены методы современных нейросетей, которые пригодны для решения актуальной задачи обнаружения кибервторжений в перемещающихся сетях транспортных средств.

Ключевые слова: беспилотный транспорт, кибербезопасность, обнаружение вторжений, нейронная сеть, вейвлет, глубокое обучение, LSTM, спайк, метанейросеть, IT-экосистема, нейрофреймворк, VANET, FANET, V2V

MODERN NEURAL NETWORK METHODS OF INTRUSION DETECTION IN VANET/FANET/MARINET

Kalinin Maxim, Zegzhda Peter
Peter the Great St. Petersburg Polytechnic University,
Russia, St. Petersburg, Polytechnicheskaya street, 29,
emails: max@ibks.spbstu.ru

Abstract: The paper reviews a set of modern methods of intrusion detection based on application of innovative neural networks.

Keywords: autonomous transport, cybersecurity, intrusion detection, neural network, wavelet, deep learning, LSTM, spike, meta-neural network, IT ecosystem, neuroframework, VANET, FANET, V2V.

При финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы» (Соглашение №14.575.21.0131 от 26.09.2017, уникальный идентификатор Соглашения RFMEFI57517X0131).

Введение. Интернетизация и кибернетизация транспортной среды привела к резкому увеличению объемов информации, которую требуется обрабатывать системам обнаружения вторжений (СОВ) в режиме реального времени. Например, сетевая инфраструктура из 1000 транспортных единиц, в каждой из которых имеется CAN-шина с 20 ECU, генерирует 400 млн. массивов признаков, которые могут оказывать влияние на перемещение, управление и кибербезопасность транспортного средства. Большие данные усложняют задачу разработки СОВ – первичными становятся задачи по обеспечению эффективности, в первую очередь – производительности СОВ: обнаружение попыток вторжений должно проходить в реальном масштабе времени для уменьшения вероятности нарушения работы транспортного средства.

Известны различные решения задачи обнаружения киберугроз: статистический подход; прогнозирование шаблона; искусственные нейронные сети (ИНС) [1,2]. Аппарат ИНС предоставляет возможности по параллельному процессированию данных и выявлению скрытых зависимостей и отклонений. Несмотря на то, что нейросетевые методы активно развиваются уже много лет, в последнее время наблюдается всплеск интереса к этой области, что связано с развитием IT-технологий и с возникшей потребностью в быстрой обработке объемных массивов данных. ИНС обеспечивают существенные преимущества перед другими методами адаптивной обработки данных: учет скрытых зависимостей между признаками; автоматический выбор и оптимизация значимых признаков для классификации объектов; решение интеллектуальных задач путем аппроксимации.

Методы обработки данных machine learning и data mining не работают с зависимостями непосредственно и вынуждены использовать контроль эвристик. Только ИНС обладают двумя последними свойствами и решают эту задачу изначально. Традиционные ИНС – многослойные персептроны с логическими передаточными функциями, модульные ИНС прямого и обратного распространения – при всей

своей универсальности и гибкости, не удовлетворяют возросшим требованиям к объему обучающих выборок (проблема насыщения на больших данных), обладают низким коэффициентом эффективности (в большинстве традиционных ИНС – не выше 95%), долго обучаемы и неспособны построить зависимость достаточной сложности. Кроме того, для традиционных ИНС характерна чрезмерная избыточность (ширина и глубина структуры ИНС) и ресурсоемкость (рост требований к объему памяти и процессорной мощности вычислительной платформы), а для задач оперативного контроля безопасности беспилотного транспорта и выявления киберугроз необходимы компактные и быстрые ИНС [3-5].

Перспективными являются исследования относительно следующих типов ИНС:

а) «мягкие» (soft) нейросети (вейвлет-нейросети и нечеткие ИНС), которые позволяют модифицировать функциональный базис ИНС, по которому производится разложение искомой зависимости, перевести его в базис soft computing («мягких вычислений»), и за счет этого оптимизировать габариты, ресурсные требования и скорость работы ИНС;

б) ИНС с многослойной топологией с предварительной настройкой весов нейронов для решения задач классификации методом самоорганизации – рекуррентные ИНС и сети с длинной и короткой временной памятью (LSTM-нейросети);

в) генеративные соревнующиеся ИНС на основе дискриминативных алгоритмов для решения задач обучения эффективных признаков представлений, обучения без учителя, обучения по смешанным наборам размеченных и неразмеченных данных, с использованием алгоритма формирования обучающих выборок с различными значениями признаков;

г) импульсные (спайковые) ИНС на основе реалистичных моделей нейронов, пригодные для реализации на малоресурсных и малоэнергозатратных устройствах для решения сложных задач;

д) сложные ИНС (гетерогенные ансамбли нейросетей и метанейросети) – объединение различных типов ИНС в единый комплекс с выбором разных нейросетевых модулей (нейрофреймворков) и возможностью самообучения для разных условий решения и усиления результативности.

Заключение. Указанные виды ИНС позволяют увеличить объем обучающей выборки до сотен миллионов признаков, динамически адаптировать свою конфигурацию под изменяющиеся условия задачи и реакцию на обучение, обучать ИНС с адаптивной архитектурой, адаптивно строить отображения с высокой нелинейностью, и за счет этого учитывать такую особенность кибербезопасности в динамической сети транспортных средств как меняющиеся зависимости между контролируемыми параметрами.

СПИСОК ЛИТЕРАТУРЫ

1. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto. Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method // International Journal of Network Security. – 2007. – Vol.5, No.3. – P. 338 – 346.
2. Khattab M. Ali Alheeti, Anna Gruebler, Klaus McDonald-Maier: An Intrusion Detection System Against Black Hole Attacks on the Communication Network of Self-Driving Cars // Conference: 6th International Conference on Emerging Security Technology (EST-2015), At Brunswick, Germany. – 2015.
3. Arnab Mitra, Rajib Ghosh, Apurba Chakraborty, Debleena Srivastva. An Alternative Approach to Detect Presence of Black Hole Nodes in Mobile Ad-Hoc Network Using Artificial Neural Network // International Journal of Advanced Research in Computer Science and Software Engineering. – 2013. – Vol. 3, Issue 3. – P. 113– 122.
4. Sandeep Kumar Arora, Shivani Vijan and Gurjot Singh Gaba. Detection and Analysis of Black Hole Attack using IDS // Indian Journal of Science and Technology. – 2016. – Vol. 9, Issue 20.
5. Nikita Patel, Jay Amin. Detection of Blackhole Attack Using Intrusion Detection System in AODV Based MANET // International Journal of Advance Engineering and Research Development (IJAERD). – 2014. – Vol. 1, Issue 5. – P. 1– 7.

УДК 519.87

АСИММЕТРИЯ ВРЕМЕНИ В ТЕОРИИ ПРОГНОЗИРОВАНИЯ СОСТОЯНИЯ СЛОЖНЫХ ДИНАМИЧЕСКИХ СИСТЕМ

Острейковский Владислав Алексеевич, Денисова Татьяна Юрьевна, Шевченко Елена Николаевна
Сургутский государственный университет
Россия, ХМАО-Югра, Сургут, пр-т Ленина, 1
emails: ostreykovsky_va@surgut.ru, denisovasever86@bk.ru, elenan_27@mail.ru

Аннотация: В статье рассмотрены вопросы асимметрии времени при анализе будущего состояния сложных динамических систем

Ключевые слова: модусы времени; асимметрия времени; прошлое-настоящее-будущее; постулаты времени.

ASYMMETRY OF TIME IN THE THEORY OF FORECASTING THE STATE OF COMPLEX DYNAMICAL SYSTEMS

Vladislav Ostreykovsky, Tatyana Denisova, Elena Shevchenko, Surgut State University
Lenina av. 1, Surgut, Russia
emails: ostreykovsky_va@surgut.ru, denisovasever86@bk.ru, elenan_27@mail.ru

Abstract: The article considers the asymmetry of time in the analysis of the future state of complex dynamical systems

Keywords: *time modes; asymmetry of time; past-present-future; postulates of time.*

Введение. Еще в древности в «Физике» Аристотеля (IV в. до н.э.) появилась идея о специфике модусов времени и его асимметрии. Позднее в работах Августина Блаженного, Р.Декарта, Б.Спинозы, И.Ньютона, Г.Лейбница аспекты проблемы времени «прошлое-настоящее-будущее» в целом и реальность каждого из его модусов получили дальнейшее развития [1]. XX век ознаменовался новыми исследованиями фактора времени в теории систем для структурно и функционально сложных динамических объектов. Работы А.М.Ляпунова, И.Р.Пригожина, в основе которых уже был использован современный аппарат функционального анализа, доказали наличие асимметрии времени на математическом уровне [2].

Основная часть. К настоящему моменту времени можно констатировать следующее: теория асимметрии времени при описании состояния структурно и функционально сложных систем превратилась в строгую теорию. Разработаны и доказаны ряд постулатов теории асимметрии времени такие, как: постулаты, вытекающие из теории марковских процессов, постулат К.Шеннона, базирующийся на одном из центральных фундаментальных постулатов физики о сохранении сущности физических процессов при прогнозировании поведения систем. Нельзя не отметить постулат Н.М.Седякина, сформулировавшего один из законов теории надежности, суть которого заключается в утверждении: надежность объекта в будущем зависит от величины выработанного им ресурса в прошлом и не зависит от того, как выработан этот ресурс к настоящему моменту времени.

В постулате А.М.Ляпунова доказано, что для поведения хаотических динамических систем понятие траектории утрачивает смысл через некоторое характерное время. При этом если расстояние между любыми точками первоначально сколь угодно малое затем экспоненциально возрастает со временем.

В заключение необходимо привести постулаты И.Р.Пригожина для хаотических динамических систем:

- 1)хаос приводит к включению стрелы времени в фундаментальное динамическое описание поведения системы. Эволюция систем при $t \rightarrow +\infty$ и при $t \rightarrow -\infty$ различна;
- 2)все системы, допускающие несводимое вероятностное описание, считаются хаотическими;
- 3)законы, описывающие хаотические системы, соответствуют вероятностям и включают в себя необратимость.

Заключение. В настоящее время при описании будущего состояния сложной динамической системы необходимо учитывать фактор асимметрии времени, базируясь на современных методах функционального анализа.

СПИСОК ЛИТЕРАТУРЫ

1. Денисова Т.Ю. Философский и научный подходы к пониманию времени: перспективы синтеза / Т.Ю.Денисова // Актуальные проблемы гуманитарных и естественных наук. – 2017. – №3 (98). Ч. III. – С.161–165.
2. Острейковский В.А. Феномен «Время» в теории прогнозирования техногенного риска сложных динамических систем / В.А.Острейковский, Е.Н.Шевченко // Надежность и качество сложных систем. – Пенза. – 2016. – №4. –С.3–12.

УДК 004.04+658.5

ИМПОРТОЗАМЕЩАЮЩЕЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ В ПРАКТИКЕ ПРОИЗВОДСТВЕННЫХ ИСПЫТАНИЙ МАШИНОСТРОИТЕЛЬНЫХ ИЗДЕЛИЙ

Первухина Елена Львовна, Осипов Константин Николаевич, Тимофеев Илья Сергеевич
Севастопольский государственный университет России, Севастополь

ул. Университетская 33
email: pervukhina14@mail.ru

Аннотация: Предлагается математическое обеспечение автоматизированных производственных испытаний сложных машиностроительных изделий для отечественных машиностроительных предприятий на основе новых программ испытаний и современных информационных технологий.

Ключевые слова: *моделирование, программы испытаний, прикладное программное обеспечение.*

IMPORT-SUBSTITUTION SOFTWARE IN THE PRACTICE OF ACCEPTING TESTING FOR MACHINE-BUILDING PRODUCTS

Pervukhina Elena, Osipov Konstantin, Timofeev Iliya
Sevastopol State University, Russia, Sevastopol, str. Universitetskay 33
email: pervukhina14@mail.ru

Abstract: The proposed software to control acceptance testing of the machine building products is based on advanced methods and programing approaches.

Key words: *mathematic modeling, applied software.*

Взятый страной курс на переход к передовым цифровым, интеллектуальным производственным технологиям имеет целью повысить конкурентоспособность отечественной продукции, в том числе машиностроительной. Производственные испытания сложных машиностроительных изделий до сих пор требуют больших энергетических и трудовых ресурсов, не всегда обеспечивая достоверные решения о соответствии их характеристик, требуемым ГОСТ Р или ТУ, и готовности к будущей эксплуатации. Использование на отдельных предприятиях автоматизированных стендов со встроенным программным обеспечением (ПО) позволяет снизить трудоемкость процесса испытаний и процент поступающих в эксплуатацию дефектных изделий, однако значительная часть стендов иностранного производства, что означает дополнительные расходы предприятия на их закупку, обслуживание, обновление и обучение части персонала зарубежным технологиям и иностранным языкам.

Целью работы является создание математического обеспечения автоматизированных производственных испытаний сложных машиностроительных изделий для отечественных машиностроительных предприятий на основе новых программ испытаний, позволяющих достичь требуемой достоверности решений, принимаемых в реальном времени поступления экспериментальной информации относительно годности выпускаемых изделий к эксплуатации при заданном техническом уровне стендов.

В основе разработанных алгоритмов лежат следующие методы и технологии:

- 1) многомерный статистический анализ и выявление причинно-следственных зависимостей между параметрами, характеризующими техническое состояние изделий, и параметрами, отражающими процессы их функционирования;
- 2) адаптивных алгоритмы обработки экспериментальной информации;
- 3) распределенная межпроцессорная обработка данных, получаемых со стендового оборудования;
- 4) модели распределенной обработки больших потоков данных (например, MapReduce);
- 5) машинное обучение.

После настройки полученные многомерные модели являются основой выработки решений о текущем техническом состоянии испытуемых изделий и тенденции его изменения.

Предложен алгоритм выбора программ испытаний, в том числе предполагающих неустановившиеся режимы работы изделий, на которых проявляются опасные для дальнейшей эксплуатации дефекты сборки. Программно реализуемая интеллектуальная функция оператора испытаний по прогнозированию предаварийного технического состояния испытуемых изделий позволяет сократить затраты на испытания. Созданные программные модули сбора, хранения и анализа данных, многомерное хранилище сокращают время автоматической обработки и передачи данных из оперативной базы данных в хранилище.

СПИСОК ЛИТЕРАТУРЫ

2. Б.Я. Советов, В.В. Цехановский. Информационные технологии: теоретические основы. Учебное пособие. СПб: Лань, 2017 г. 444 с.

УДК 004.05

МЕТОДЫ ИЗВЛЕЧЕНИЯ ДАННЫХ С ИЗОЛИРОВАННЫХ МАШИН

Романов Александр Алексеевич

Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Россия, Санкт-Петербург, ул. Большая Морская, 67,
emails: R0man0vAleks@yandex.ru

Аннотация: Статья посвящена изучению методов извлечения информации с изолированных машин. В статье представлены некоторые методы извлечения информации с машин, не имеющих сетевых подключений или какой-либо опасной периферии.

Ключевые слова: компьютерная безопасность; защита данных; хищение информации; взлом.

METHODS OF DATA EXTRACTION FROM ISOLATED MACHINES

Romanov Alexander

The St. Petersburg State University of Aerospace Instrumentation,
Russia, St. Petersburg, Bolshaya Morskaya str., 67,
emails: R0man0vAleks@yandex.ru

Abstract: The article is dedicated to studying of methods of extract information from isolated machines. Some methods of extract information from machines without network connection or any dangerous peripherals are shown in the article.

Keywords: computer security; data protection; theft of information; hacking.

Введение. В современном мире информация стала важнейшим ресурсом во всех отраслях нашей жизни. Именно по этой причине мы стараемся защитить её всеми возможными средствами. Распространено мнение, что основной угрозой для данных, хранящихся на компьютерах, является подключение к сети или использование потенциально опасной периферии. В своей статье я хочу рассказать о нескольких методах извлечения информации с изолированных машин, то есть таких машин, которые не имеют сетевых подключений или какой-либо опасной периферии.

Одним из таких методов является передача данных с помощью мигания индикатора использования жёсткого диска. Такие индикаторы присутствуют в большинстве персональных компьютеров и ноутбуков. Данные светодиоды обладают возможностью мерцания с частотой 6000 раз в секунду, а передавать информацию можно, используя двоичный код, где горящий светодиод обозначает 1, а потухший - 0.

Другим методом может быть использование подключенных наушников в качестве микрофона. Как известно, на аппаратном уровне микрофон и наушники не сильно отличаются друг от друга. Этот факт даёт возможность использовать наушники для улавливания колебаний воздуха в радиусе примерно 6 метров от заражённой машины, а запись можно осуществить, обратив выходной канал звуковой карты во входной.

Ещё одним способом извлечения информации является использование USB девайса в качестве RF-трансммиттера. Для применения этого метода подойдёт практически любая флешка, при этом нет необходимости каким-либо образом её модифицировать. Чтобы начать передачу данных, достаточно отправить на USB устройство последовательность нулей, это создаст электромагнитное излучение в диапазоне от 240 до 480 МГц. Управляя данным процессом, можно научить ресивер воспринимать излучение как поток нулей и единиц. Таким образом, можно получить возможность передавать информацию на расстояние до трёх метров, если устройство имеет провод, который может быть использован как антенна, можно увеличить расстояние передачи до восьми метров.

В качестве ещё одного метода можно применить прослушивание звуков работы жёсткого диска. SSD для данного метода не подойдут, так как не имеют движущихся частей, а шум HDD и SSHD с помощью программы, управляющей позиционером диска, можно использовать для передачи данных. В качестве приёмника подойдёт любое устройство, оснащённое микрофоном и расположенное вблизи корпуса заражённой машины.

Также для извлечения информации можно использовать электромагнитное излучение видеокарты, которое воспринимается FM приёмником мобильного телефона. Этот метод позволяет использовать обычный мобильный телефон для распознавания сигнала видеокарты заражённого компьютера. С помощью данной технологии исследователям удалось получить информацию с расстояния до семи метров.

Заключение. В данной статье представлены лишь некоторые из способов, которыми могут воспользоваться злоумышленники для хищения данных, однако, все они требуют, чтобы машина изначально была заражена вредоносной программой, что уже, вероятно, является непростой задачей. В качестве основных способов обеспечения безопасности можно назвать необходимость лучше контролировать область в непосредственной близости от вероятного объекта интереса злоумышленников и запрет на использование каких-либо устройств, подверженных модификациям в одном помещении с данной машиной. Также, вероятно, стоит ограничить обзор со стороны на рабочее место и подумать об экранировании стен в помещении.

СПИСОК ЛИТЕРАТУРЫ

1. Mordechai Guri, Boris Zadov, Eran Atias, Yuval Elovici. LED-it-GO Leaking (a lot of) Data from Air-Gapped Computers via the (small) Hard Drive LED. Ben-Gurion University of the Negev. Cyber Security Research Center.
2. Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. SPEAKE(a)R: Turn Speakers to Microphones for Fun and Profit. Ben-Gurion University of the Negev. Cyber Security Research Center.
3. Mordechai Guri, Matan Monitz, Yuval Elovici. USBee: Air-Gap Covert-Channel via Electromagnetic Emission from USB. Ben-Gurion University of the Negev. Cyber Security Research Center.
4. Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. DiskFiltration: Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise. Ben-Gurion University of the Negev. Cyber Security Research Center.
5. How to leak sensitive data from an isolated computer (air-gap) to a near by mobile phone - AirHopper.
URL: <http://cyber.bgu.ac.il/content/how-leak-sensitive-data-isolated-computer-air-gap-near-mobile-phone-airhopper>.

УДК 004.7.056.53

МЕТОДИКИ И ИНСТРУМЕНТЫ АУДИТА СЕТЕВОЙ БЕЗОПАСНОСТИ

Садикова Анастасия Александровна, Титова Юлия Алексеевна, Савков Сергей Витальевич
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский пр., 49,
emails: nastya.sadkoo@mail.ru, titova.yulishna@mail.ru, sergsavkov@gmail.com

Аннотация: Со временем сетевая инфраструктура усложняется, расширяются виды приложений и данных. Все эти изменения приводят к тому, что при осуществлении системы

информационной безопасности, пользователь может не заметить некоторые уязвимости сети. В связи с этим необходимо проведение регулярного аудита безопасности. В данной статье обобщены виды аудита сетевой безопасности, рассмотрены методологии IAM и SAFETAG, а также особенности их проведения. Приведена краткая характеристика некоторых сканеров уязвимостей. Сделан вывод о том, что, хотя аудит безопасности и носит рекомендательный характер, он является необходимым для обеспечения целостности и конфиденциальности персональных данных людей, так или иначе связанных с организацией.

Ключевые слова: аудит, тест на проникновение, сканеры уязвимостей, методология аудита, SAFETAG, IAM, сетевая безопасность, международные стандарты безопасности.

METHODS AND TOOLS OF THE AUDIT OF NETWORK SECURITY

Sadikova Anastasia, Titova Yulia, Savkov Sergei

Saint Petersburg National Research University of Information Technologies, Mechanics and Optics «ITMO»,
Russia, St. Petersburg, Kronverkskiy prospekt, 49

emails: nastya.sadkoo@mail.ru, titova.yulishna@mail.ru, sergsavkov@gmail.com

Abstract: Over time, the network infrastructure becomes more complex, the types of applications and data expand. All these changes lead to the fact that when implementing an information security system, a user may not notice some network vulnerabilities. In this regard, it is necessary to conduct a regular security audit. This article summarizes the types of network security audit, examines the methodologies of IAM and SAFETAG, as well as specifics of their conduct. A brief description of some vulnerability scanners is given. It is concluded that, although the security audit is advisory in nature, it is necessary to ensure the integrity and confidentiality of the personal data of people in one way or another related to the organization.

Keywords: audit, penetration testing, vulnerability scanners, audit methodology, SAFETAG, IAM, network security, international safety standards.

Введение. В современном мире сетевая безопасность имеет колоссальное значение. Под сетевой безопасностью понимают комплекс требований, которые предъявляются к инфраструктуре компьютерной сети, при выполнении которых обеспечивается защита сетевых ресурсов от несанкционированного доступа и эффективное функционирование сети в целом. Одной из задач организации является предоставление своим сотрудникам безопасного доступа к сетевым ресурсам в любое время. Для решения задачи безопасности сети на предприятии проводят аудит сетевой безопасности. В коммерческих организациях руководство озабочено обеспечением безопасности своих активов, поэтому понимает важность проведения аудита. В некоммерческих организациях (далее – НКО) аудиту уделяется намного меньше внимания. Такое пренебрежение чревато тем, что персональные данные граждан, которые по ряду причин обратились в конкретную НКО, а также сотрудников, работающих в данной НКО, могут попасть в руки злоумышленников. Аудит безопасности информационных систем — это их проверка, тестирование, которое должно выявить потенциальные опасности и уязвимости в защите. При этом используется принцип сравнения результатов теста с неким идеалом, установленным целями аудита, а также личным опытом самого аудитора. При этом должно учитываться множество самых разнообразных факторов, в том числе и информация о компании: область её деятельности, размер фирмы и прочее [1]. Целями проведения аудита безопасности являются:

- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов информационной системы (далее – ИС);
- оценка текущего уровня защищенности ИС;
- локализация узких мест в системе защиты ИС;
- оценка соответствия ИС существующим стандартам в области информационной безопасности;
- выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.

Существует три вида аудита:

1. Активный аудит;
2. Экспертный аудит;
3. Аудит на соответствие стандартам.

Экспертный аудит можно условно представить, как сравнение состояния информационной безопасности с «идеальным» описанием. Результаты экспертного аудита могут содержать разноплановые предложения по построению или модернизации системы обеспечения информационной безопасности.

Суть аудита на соответствие стандартам наиболее приближена к тем формулировкам и целям, которые существуют в финансовой сфере — при проведении данного вида аудита состояние информационной безопасности сравнивается с неким абстрактным описанием, приводимым в стандартах.

Более подробно будет рассмотрен активный аудит сетевой безопасности.

Заключение. Аудит как средство защиты информации носит сугубо рекомендательный характер, другими словами, эта процедура не привносит изменений в саму систему. Однако анализ полученных данных позволяет говорить о мерах защиты от несанкционированного доступа к конфиденциальным ресурсам. Сканеры безопасности охватывают довольно обширную сферу проблем, поэтому благодаря их использованию можно не только искать уязвимые программы в сети, но и изменять политику безопасности, реагируя на обнаруженные проблемы [2]. При планировании проверки состояния системы информационной безопасности важно не только точно выбрать вид аудита, исходя из потребностей и возможностей компании, но и не ошибиться с выбором исполнителя. Результаты любого вида аудита содержат рекомендации по модернизации системы обеспечения информационной безопасности. Если аудит проводит консалтинговая компания, которая кроме консалтинговой деятельности занимается еще и разработкой собственных систем защиты информации, она, по понятным причинам, заинтересована в том, чтобы результаты аудита рекомендовали организации использовать её продукты. Для того чтобы рекомендации на основе аудита были действительно объективными, необходимо, чтобы компания-аудитор была независима в выборе используемых систем защиты информации и имела большой опыт работы в области информационной безопасности [3].

СПИСОК ЛИТЕРАТУРЫ

1. Кравчук Д. И., Коркушко Д. А. Аудит безопасности корпоративных информационных систем // Молодой ученый. — 2015. — №10. — С. 697-700.
2. Обзор бесплатных инструментов для аудита web-ресурсов и не только. [Электронный ресурс]. – Режим доступа: <https://habrahabr.ru/post/125206/>, свободный. Яз. рус. (дата обращения 26.12.2016)
3. Аудит безопасности: когда и чем проводить? // CNews – Издание о высоких технологиях. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/articles/audit_bezopasnosti_kogda_i_chem_provodit_, свободный, Яз. рус. (дата обращения 26.12.2016)

УДК 004.056.5

ПОВЫШЕНИЕ ТОЧНОСТИ МЕТОДОВ СТЕГАНОАНАЛИЗА ПУТЕМ ОПТИМИЗАЦИИ ПАРАМЕТРОВ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ

Сивачев Алексей Вячеславович, Михайличенко Ольга Викторовна
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, пр. Кронверкский, 49
email: sivachev239@mail.ru, crypto_ifmo@mail.ru

Аннотация: В статье рассмотрена задача обнаружения факта встраивания в область дискретного вейвлет-преобразования и рассмотрены причины недостаточной эффективности современных методов стеганоанализа. Показано, что причина недостаточной эффективности современных методов стеганоанализа связана с большой степенью разброса используемых для обнаружения встраивания параметров, составляющих опорный вектор. По итогам исследования в статье предложена методика, позволяющих улучшить эффективность современных методов стеганоанализа с помощью специализированного вейвлета.

Ключевые слова: *стеганография, методы стеганоанализа, бинарная классификация, дискретное вейвлет преобразование*

INCREASE OF ACCURACY OF STEGANOANALYSIS METHODS BY OPTIMIZING PARAMETERS OF WAVELET-TRANSFORMATION

Sivachev Alexey, Mikhailichenko Olga
St. Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, Saint-Petersburg, Kronverkskiy pr., 49
email: sivachev239@mail.ru, crypto_ifmo@mail.ru

Аннотация: This article deals with problem of detecting the fact of embedding into the wavelet transform domain. This article shows the reasons of low efficiency of modern methods of steganoanalysis. It is shown that the reason for low efficiency of modern methods of steganoanalysis is associated with a high dispersion of the parameters used to detect the embedding. According to the results of the research, the article suggests a technique that allows improving the efficiency of modern methods of steganoanalysis using a specialized wavelet.

Ключевые слова: *steganography, methods of steganalysis, binary classification, discrete wavelet transformation*

Введение. На сегодняшний день существует и находит широкое применение большое количество методов скрытия информации в цифровых изображениях с использованием стеганографии.

Значительный прогресс наблюдается в области разработки стеганографических методов вейвлет (ДВП) области встраивания. Увеличение интереса к встраиванию информации в область ДВП изображения связано с распространением формата сжатия изображений JPEG 2000, который основан на использовании ДВП. Для противодействия противоправному использованию стеганографии [2] на сегодняшний день разработаны методы стеганоанализа, которые должны выявлять факт стеганографического встраивания в область дискретного вейвлет-преобразования цифровых изображений. Множество современных методов стеганоанализа в области ДВП основаны на методах машинного обучения. На сегодняшний день не существует универсальных методов стеганоанализа, которые позволяли бы однозначно определить факт встраивания в цифровое изображение [2]. Точность обнаружения встраивания в область ДВП на сегодняшний день не позволяет гарантировать абсолютную успешность пассивного противодействия с их применением. Например, авторы метода [3] приводят данные по точности разработанного ими метода, согласно которым наилучшая точность метода [3] составляет 80% корректно классифицированных изображений при 20% объеме встраивания от максимального объема встраивания. Т.е. около 20% изображений классифицируются неверно. В случае снижения объема встроенной полезной нагрузки процент корректных результатов скорее всего еще более снизится, а некорректных результатов соответственно возрастет. Таким образом исследования направленные на повышение точности обнаружения факта встраивания в область ДВП изображения являются актуальными.

Исследование предметной области. Многие из существующих методов стеганоанализа, например, методы [3-5], основаны на использовании значений статистических моментов областей коэффициентов LL, HL, LH, HH, получаемых при дискретном вейвлет-преобразовании изображения в качестве основы для вектора параметров, используемых в последствии для классификации изображений с использованием методов машинного обучения. Как показали исследования стеганографическое встраивание оказывает заметное влияние на значения данных статистических моментов, однако значения данных статистических моментов обладают заметным разбросом значений, что приводит к тому, что множества значений статистического момента для оригинальных и для стего изображений имеют значительную область пересечения. Значительное пересечение множеств значений для оригинальных и стего изображений не позволяет однозначно классифицировать изображение как оригинальное или стего изображение с использованием данных статистических моментов. Исследования показывают, что степень пересечения множеств значений статистических моментов для оригинальных и стего изображений зависит от набора низко- и высокочастотных коэффициентов, используемых для дискретного вейвлет-преобразования.

Заключение. Зависимость между степенью пересечения множеств значений статистических моментов для оригинальных и стего изображений и используемым вейвлетом позволяет подобрать специализированный вейвлет, который позволит уменьшить область пересечений для множеств значений оригинальных и стего изображений, либо подобрать специализированный вейвлет который оценит погрешность значений статистических моментов. На основании выявленной зависимости можно предложить методику, которая позволит повысить эффективность использования статистических моментов, что позволит повысить эффективность современных методов стеганоанализа.

СПИСОК ЛИТЕРАТУРЫ

1. SPYCRAFT: The Secret History of the CIA's Spytechs from Communism to Al-Qaeda [Электронный ресурс]: Central Intelligence Agency – Режим доступа: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol52no2/spycraft-the-secret-history-of-the-cia2019s.html> (Дата обращения 05.03.2017)
2. Prokhozhev N., Mikhailichenko O., Sivachev A., Bashmakov D., Korobeynikov A.G. Passive Steganalysis Evaluation: Reliabilities of Modern Quantitative Steganalysis Algorithms [Текст], Advances in Intelligent Systems and Computing. 2016. Vol. 451. pp. 89-94.
3. Gireesh Kumar T., Jithin R., Deepa D. Shankar Feature Based Steganalysis Using Wavelet Decomposition and Magnitude Statistics [Текст], Advances in Computer Engineering (ACE), 2010, pp. 298-300
4. Farid Hany Detecting Steganographic Messages in Digital Images [Текст], Technical Report TR2001-412, Dartmouth College, Computer Science Department, 2001

УДК 004.72

ПРОБЛЕМА АНОНИМНОСТИ В СЕТИ ИНТЕРНЕТ СРАВНЕНИЕ МЕТОДОВ АНОНИМИЗАЦИИ ПОЛЬЗОВАТЕЛЯ

Титова Юлия Алексеевна, Садикова Анастасия Александровна, Савков Сергей Витальевич
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, пр-кт Кронверкский, 49
emails: titova.yulishna@mail.ru, nastya.sadkoo@mail.ru, sergsavkov@gmail.com

Аннотация: Сейчас все большее количество людей беспокоит проблема анонимности в сети Интернет. К сожалению, полностью обезопасить себя нельзя, однако, используя методы анонимизации, риски можно свести к минимуму. В статье рассмотрены самые популярные методы,

позволяющие обеспечивать анонимность и информационную безопасность в сети Интернет, такие как различные Proxy-серверы, VPN-серверы, сети Tor, I2P, и метод «крышевания» доменов. Рассмотрен принцип их работы, проанализированы основные преимущества и недостатки. Сделаны выводы, что каждый метод разработан для определённых целей, а значит, при выборе способа анонимизации следуют руководствоваться конкретными задачами, которые стоят перед пользователем.

Ключевые слова: анонимизация; прокси-сервер; VPN; Tor; I2P

THE PROBLEM OF ANONYMITY IN THE INTERNET NETWORK COMPARISON OF METHODS OF USER ANONYMIZATION

Titova Yulia, Sadikova Anastasia, Savkov Sergei

Saint Petersburg National Research University of Information Technologies, Mechanics and Optics,

Russia, St. Petersburg, Kronverkskiy prospekt, 49

emails: titova.yulishna@mail.ru, nastya.sadkoo@mail.ru, sergsavkov@gmail.com

Abstract: Now an increasing number of people are concerned about the problem of anonymity on the Internet. Unfortunately, you can not completely protect yourself, however, using anonymization methods, risks can be minimized. The article covers the most popular methods that allow anonymity and information security on the Internet, such as various Proxy servers, VPN servers, Tor networks, I2P, and the method of domain "fronting". The principle of their work is considered, the main advantages and disadvantages are analyzed. It is concluded that each method is designed for certain purposes, and therefore, when choosing the method of anonymization, follow specific tasks that are faced to the user.

Keywords: anonymization; proxy-server; VPN; Tor; I2P

Введение. Ведущие специалисты в области информационной безопасности утверждают, что полной анонимности в сети Интернет добиться практически невозможно. Поэтому среднестатистический пользователь, считающий себя анонимом, является таковым лишь формально. Словарь Ожегова даёт следующее определение слову анонимность: Без указания имени того, кто пишет, сообщает о чем-либо [1]. Действительно, пользователи сети Интернет стараются не указывать свои личные данные на подозрительных сайтах, однако это не гарантирует анонимности в сети. Большинство Web-серверов ведёт контроль посещаемости, а значит IP адреса устройств, с которых был выполнен вход на сайт, остаются в базе данных, где также фиксируется активность пользователя на сайте. Помимо этого, задействуются социальные сети. Так, к примеру, по официальным данным, Facebook, MySpace и несколько других социальных сетей продавали личные данные рекламным компаниям, которые в дальнейшем использовали их для поиска имён потребителей, контактных данных и другой личной информации [2]. Таким образом, осуществляется взаимодействие сайтов, в процессе которого происходит обмен информацией и составление полноценной характеристики о каждом клиенте. Более продвинутые пользователи пытаются оградить себя от этого и прибегают к различным изобретательным подходам для достижения анонимности. Но это им не всегда удается, поскольку в настоящее время со стороны, как государства, так и частных организаций активно ведется борьба с анонимностью в сети Интернет. Принимаются меры по деанонимизации: устанавливаются обязательная идентификация пользователей при использовании общественных точек доступа, блокируются прокси-серверы и анонимные сети, контролируется трафик с помощью технологии DPI и пр.

Методы анонимизации зачастую используются злоумышленниками, с целью избежать наказания за правовые нарушения [3]. В борьбу с ними вступают правоохранительные органы, которые при помощи способов деанонимизации устанавливают реальную личность преступника, его место нахождения, активность в сети Интернет и прочую необходимую информацию.

В этом и заключается проблема анонимности в сети Интернет. Всегда будут люди, которые хотят защитить информацию о себе. А в противовес им будут существовать организации, которые пытаются извлечь выгоду из обладания личными данными пользователей, и правоохранительные органы, задача которых деанонимизировать и наказать правонарушителя. Поэтому способы анонимизации в сети интернет будут рассмотрены с различных позиций.

Заключение

В работе были рассмотрены подходы к обеспечению анонимности в сети. Ни один способ на сегодняшний день не может обеспечить полной анонимизации пользователя. Поэтому задача анонимизации сводится к тому, чтобы для деанонимизации требовались недостижимые вычислительные ресурсы или такой объем времени раскрытия, что по его истечению деанонимизация была бы уже не актуальной. Также при использовании различных методов возникают сопутствующие трудности. Поэтому, выбирая средства, следует учитывать, какой ценой будет обеспечиваться анонимность. Для того чтобы избавиться от некоторых недостатков того или иного метода анонимизации прибегают к комбинированию различных методов. Как показывает практика, на каждый метод анонимизации создаются средства, позволяющие обойти его. Поэтому, вероятнее всего, «панацеи» в средствах обеспечения анонимизации создано не будет. Со стороны нашего государства

отношения в сфере информационной безопасности регулируются 23 и 24 статьей Конституции РФ. Каждый имеет право на неприкосновенность частной жизни, однако реализация этого права в руках каждого участника информационного обмена. Знание элементарных основ информационной безопасности решит большую часть проблем обеспечения анонимности.

СПИСОК ЛИТЕРАТУРЫ

1. Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка. – 4-е изд. – М., 1997.
2. Steel, E., Jessica E. Vascellaro. Facebook, MySpace Confront Privacy Loophole // www.wsj.com, 21.05.2010. Точный адрес статьи: <http://www.wsj.com/articles/SB10001424052748704513104575256701215465596>.
3. Милославская Н.Г., Евтеев К.Б. Защита он анонимного доступа // Известия Южного федерального университета. Технические науки. 2003. №4 том 33 С. 220.
4. Гришина Н.В. Интернет-трафик: защита сетевых ресурсов организации // Прикладная информатика. 2006. №1 С. 72-76.
5. Радайкин М.Ф. Кратко о проблеме анонимности в сети интернет // Пробелы в российском законодательстве. Юридический журнал. 2013. №2 С. 25-28.
6. Рябко Е.И. Калейдоскоп VPN технологий // Т-Comm – Телекоммуникации и Транспорт. 2009. №5 С. 16-20.
7. Денисова Т.Б. Безопасность услуги VPN // Вестник Самарского государственного технического университета. Серия: технические науки. 2005. №33 С. 168-171.
8. Иванов С.Н. Преступление в сфере высоких технологий: проблемы документирования компьютерных преступлений // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2012. № 18 С. 70-74.
9. Кузичкина О.А. Сеть Tor как способ подключения к «глубокому» интернету // Интеллектуальный потенциал XXI века: ступени познания. 2014. №25 С. 129-131.

УДК 004.056.53 (003.26)

АНАЛИЗ ПРОТОКОЛА X-PACE

Шенец Николай Николаевич, Трухина Екатерина Евгеньевна
Санкт-Петербургский политехнический университет Петра Великого
Россия, Санкт-Петербург, ул. Политехническая, 29,
emails: shenets@ibks.spbstu.ru, ktoniya@gmail.com

Аннотация: В статье рассмотрена модификация протокола аутентификации и выработки ключа на основе пароля (PACE). Разработано приложение-макет для исследования протокола, предложена методика его испытаний. Проведены эксперименты, которые подтверждают улучшение характеристик модифицированной версии X-PACE по сравнению с оригиналом.

Ключевые слова: PACE; аутентификация на основе пароля.

STUDY OF THE X-PACE PROTOCOL

Shenets N, Trukhina E
¹ Peter the Great St. Petersburg Polytechnic University,
Russia, St. Petersburg, Polytechnicheskaya str. 29,
emails: shenets@ibks.spbstu.ru, ktoniya@gmail.com

Abstract: The modified version of the password authenticated connection establishment (PACE) protocol is considered. The program model for experiments and testing procedure are developed. Experimental results confirms improvement of characteristics of X-PACE in comparison with PACE.

Keywords: PACE; password based authentication.

Введение. Протокол Password Authenticated Connection Establishment (PACE) [1], разработанный федеральным управлением по информационной безопасности Германии (BSI) в 2007 году, позволяет двум сторонам сформировать общий, только им известный ключ, используя при этом короткий (низкоэнтропийный) пароль. Данный протокол используется преимущественно в smart-картах и разработан специально для них. Ранее нами была предложена модификация X-PACE [2] протокола PACE, позволяющая ускорить его выполнение без изменения криптографической стойкости. Для этого операция зашифрования на первом этапе заменяется операцией XOR. В данной статье приводятся результаты экспериментального анализа протокола X-PACE.

Результаты анализа. Базовый протокол PACE подразумевает использование различных криптографических алгоритмов шифрования и контроля целостности (криптонаборов). Наряду с зарубежными криптоалгоритмами (SHA-256 [3], AES и 3DES [4]) были использованы и отечественные («Стрибог» [5], «Магма» и «Кузнечик» [6]). Особенностью протокола PACE является то, что результатом его первого этапа является 256-битная последовательность (ключ), выработанная на основе низкоэнтропийного пароля. Для обеспечения стойкости протокола необходимо, чтобы возможные генерируемые последовательности были случайными (псевдослучайными). Однако для оценки случайности таких коротких последовательностей большинство известных наборов статистических тестов непригодно. Хорошо известные статистические тесты являются состоятельными лишь при достаточно большом объеме выборки. Поэтому основная задача экспериментального исследования состояла в выборе подходящего набора статистических тестов и определения методики тестирования.

Для выбора подходящих тестов использовались известные батареи тестов: Д. Кнута, Дж. Марсальи (DIEHARD), батарея тестов NIST, пакеты CRYPT-X и TESTU01. Вместе с этим изучались работы [7], [8], [9] по тестированию коротких последовательностей для составления адекватной методики тестирования. В результате оказалось, что наиболее подходящими в данных условиях являются некоторые тесты из батареи тестов NIST с использованием методики, предложенной F. Sulak [9].

Были отобраны и реализованы следующие тесты:

- Частотный побитовый тест (Frequency test).
- Частотный блочный тест (Frequency Test within a Block).
- Частотный целочисленный тест (Integer Frequency Test).
- Тест кумулятивных сумм (Cumulative Sums Test);
- Тест серий (Runs test);
- Проверка максимальной длины серии в блоке (Test for the Longest Run of Ones in a Block);
- Тест пересекающихся m -грамм (Serial test);
- Тест на основе приращения энтропии (Approximate Entropy Test);
- Тест на основе линейной сложности (Linear Complexity Test);
- Тест на основе профиля линейной сложности (Linear Complexity Profile Test).

– Был разработан программный макет на языке Java с использованием эмулятора Java-card. В макете были реализованы: базовый протокол PACE и модифицированный протокол X-PACE с подключением различных криптонаборов, а также статистические тесты согласно методике тестирования, предложенной в [9].

Закключение. В результате экспериментов было показано, что модифицированная версия X-PACE протокола PACE не уступает исходной по качеству генерируемых на первом этапе ключей. Более того, оказалось, что лучшим криптонабором по этому критерию является пара отечественных алгоритмов «Стрибог» и «Магма».

СПИСОК ЛИТЕРАТУРЫ

1. Ullmann M., Kügler D., Neumann H., Stappert S., Vögeler M. Password Authenticated Key Agreement for Contactless Smart Cards // Communications of the ACM, 2008.
2. Шенец Н.Н., Трухина Е.Е. X-PACE: Модифицированный протокол аутентификации на основе слабого пароля // Проблемы информационной безопасности. Компьютерные системы. 2016, № 4, С. 106–112.
3. FIPS PUB 108-4. 2015.
4. ISO/IEC 18033-3:2010 Information technology. Security techniques. Encryption algorithms. Part 3: Block ciphers. 2010.
5. ГОСТ Р. 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. Москва: Стандартинформ, 2012.
6. ГОСТ Р. 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. Москва: Стандартинформ, 2015.
7. Soto J. Randomness Testing of the AES Candidate Algorithms // NIST Interagency or Internal Report (NIST IR) 6390, September 1999.
8. Doganaksoy A., Ege B., Kocak O., Sulak F. Cryptographic Randomness Testing of Block Ciphers and Hash Functions // Cryptography ePrint Archive: Report 2010/564, 11 November 2010.
9. Sulak F. Statistical analysis of block ciphers and hash functions // Publication of the Middle East Technical University Ph.D Examinations, February 2011.

УДК 004.056

ПРИМЕНЕНИЕ ИЗОГЕНИЙ ЭЛЛИПТИЧЕСКИХ КРИВЫХ ДЛЯ ПОСТРОЕНИЯ СХЕМЫ ГРУППОВОЙ ПОДПИСИ

Штыркина Анна Александровна, Ярмач Анастасия Викторовна, Александрова Елена Борисовна
Санкт-Петербургский политехнический университет Петра Великого,
Россия, Санкт-Петербург, ул. Политехническая, 29,
emails: anna10.94@yandex.ru, nastyayarmak238@gmail.com, elena.aleksandrova@ibks.ftk.spbstu.ru

Аннотация: В работе предлагается применение задачи поиска изогений суперсингулярных кривых для построения схемы групповой подписи. Представленный протокол основан на доказательстве с нулевым разглашением и является модификацией схемы короткой групповой подписи BBS применительно к задаче вычисления изогений. Рассмотрен вопрос генерации эллиптических кривых для криптосистем на изогениях.

Ключевые слова: суперсингулярные эллиптические кривые; изогении; групповая подпись.

ISOGENY-BASED GROUP SIGNATURE

Shtyrkina Anna, Yarmak Anastasiya, Aleksandrovna Elena
Peter the Great St.Petersburg Polytechnic University,
Russia, St. Petersburg, Polytechnicheskaya str. 29,
emails: anna10.94@yandex.ru, nastyayarmak238@gmail.com, elena.aleksandrova@ibks.ftk.spbstu.ru

Abstract: The article proposes group signature scheme based on supersingular elliptic curve isogenies. The protocol is modified short group signature BBS applied to the problem of computing isogenies combined with zero-knowledge proof protocol. Explorations of elliptic curves generation methods for isogeny-based cryptosystems are presented.

Keywords: *supersingular elliptic curve; isogeny, group signature.*

Введение. Стремительное развитие квантовых технологий привело к тому, что в настоящее время актуальным вопросом в криптографии является разработка и использование новых задач для построения криптосистем, которые бы являлись стойкими к атакам на квантовом компьютере. Одной из таких задач является задача поиска изогений эллиптических кривых, которая может быть использована для создания широкого класса криптографических протоколов, в частности, групповых подписей.

Групповая подпись – один из видов цифровой подписи, который обладает свойством сохранения анонимности подписывающего. Данная концепция заключается в том, что сообщения могут быть подписаны только членами группы, а определение авторства является достаточно трудоемкой задачей. В случае, когда необходима идентификация подписывающего пользователя, третья доверенная сторона, например, менеджер группы, может использовать специальную «лазейку» для однозначного раскрытия автора.

В системах, где используется групповая подпись, нет необходимости для каждого устройства хранить пару «открытый ключ – закрытый ключ». Каждому члену группы сопоставляется закрытый ключ, а проверка подписи осуществляется с помощью единственного открытого ключа группы.

Широкое применение групповые подписи находят в распределенных системах, где анонимность узлов является необходимым условием безопасности сети. Например, в Smart Grid-системах или в «умных» системах энергоснабжения при компрометации данных могут возникнуть проблемы, начиная от скачка напряжения в доме и заканчивая обесточиванием крупного завода. В настоящее время активно развиваются распределенные сети с подвижными объектами, такими как автомобили (VANET-сети) или БПЛА (FANET-сети). Для обеспечения безопасности данных в таких сетях могут быть использованы динамические групповые подписи.

Изогией эллиптических кривых называется рациональное отображение, сохраняющее неподвижным бесконечно удаленную точку. Такое отображение может использоваться как для расчета числа точек эллиптической кривой с помощью алгоритма SEA [1], так и в качестве инструмента для анализа сложности задачи дискретного логарифмирования в группе точек эллиптической кривой [2].

Использование задачи вычисления изогении для построения криптосистем впервые было предложено в работах [3, 4], которые содержали описание схемы с возможностью депонирования ключей (key-escrow system) на основе изогенных кривых, а также протокол установления ключа Диффи–Хеллмана и протокол шифрования Эль-Гамала на изогениях несуперсингулярных кривых. В 2011 году был опубликован квантовый алгоритм, который позволил снизить сложность задачи нахождения несуперсингулярных кривых с экспоненциальной до субэкспоненциальной [5]. Позднее для построения протоколов на изогениях стали использоваться суперсингулярные кривые, обеспечивающие экспоненциальную стойкость криптосистем. На сегодняшний день опубликованы схема неоспоримой подписи [6], схема подписи вслепую [7], а также алгоритм шифрования Эль-Гамала [8]. Открытая библиотека SIDH [9], выпущенная компанией Microsoft, содержит основные функции, необходимые для работы с изогениями суперсингулярных кривых, что позволяет реализовывать протоколы на практике и исследовать их эффективность.

Процесс генерации несуперсингулярных кривых для криптосистем на изогениях состоит из нескольких этапов. Для криптографических приложений необходимо учитывать ряд параметров, влияющих на уровень стойкости. Так, одним из требований к изогенным эллиптическим кривым является большое простое число классов мнимого квадратичного порядка, что значительно снижает скорость вычисления полинома, задающего число классов. Этап нахождения такого полинома представляется одним из самых трудоемких, даже если использовать полиномы Вебера, имеющие значительно меньшую длину коэффициентов по сравнению с полиномами Гильберта и Аткина–Морана. Генерация суперсингулярных кривых для криптосистем на изогениях не требует трудоемких вычислений и может быть достаточно легко реализована на практике [10].

Структура разработанной схемы групповой подписи на изогениях схожа с протоколом короткой групповой подписи BBS. Для того чтобы получатель сообщения был уверен в принадлежности подписывающего к группе, в схеме BBS используется доказательство с нулевым разглашением. В работе [8] предложена схема доказательства с нулевым разглашением на изогениях суперсингулярных кривых. В результате модификации протокола BBS и внедрения в него схемы доказательства с нулевым разглашением была разработана схема групповой подписи, обладающая следующими свойствами: анонимность, возможность раскрытия личности подписывающего только менеджером группы, корректность, невозможность фальсификации, устойчивость к сговору.

Открытым параметром данного протокола является суперсингулярная эллиптическая кривая, которую назовем инициализирующей. Каждому узлу сети, или члену группы, сопоставим точку-

идентификатор на этой кривой. Используя случайно выбранную секретную изогению, отображающую точки инициализирующей кривой в точки общеизвестной кривой, менеджер генерирует закрытый ключ для каждого члена группы. Ключ представлен парой значений: образ точки-идентификатора на общеизвестной кривой и секретная пользовательская изогения, ядро которой – идентифицирующая точка.

Формирование подписи сводится к нахождению пользовательской кривой с помощью секретного для каждого члена группы изогении. В процессе подписи используются две вспомогательные изогении, ядра которых сгенерированы с помощью случайной точки, а также с помощью образа точки-идентификатора на пользовательской кривой. От полученных данных вычисляется хэш-образ, который вместе со вспомогательной информацией включается в подпись. Таким образом, пользователь доказывает знание своей секретной пользовательской изогении, не раскрывая ее, с помощью протокола доказательства с нулевым разглашением. Верификация подписи заключается в проверке достоверности присланных данных с помощью протокола доказательства с нулевым разглашением и построением вспомогательных изогений. В случае разногласий авторство подписи может быть раскрыто с помощью дуальной изогении менеджера, позволяющей по образу на общеизвестной кривой получить точку-идентификатор пользователя на инициализирующей кривой.

Заключение. В работе проанализированы протоколы групповых подписей, рассмотрены сферы их применения. Предложен протокол групповой подписи, сочетающий в себе групповую подпись BBS и доказательство с нулевым разглашением на основе задачи поиска изогении суперсингулярных кривых.

СПИСОК ЛИТЕРАТУРЫ

1. Schoof R. Counting points on elliptic curves over finite fields //J. Théor. Nombres Bordeaux. – 1995. – Т. 7. – №. 1. – С. 219-254.
2. Jao D., Miller S. D., Venkatesan R. Do all elliptic curves of the same order have the same difficulty of discrete log? //ASIACRYPT. – 2005. – Т. 3788. – С. 21-40.
3. Teske E. An elliptic curve trapdoor system / E. Teske // Journal of Cryptology. – Vol. 19(1). – P. 115-133.
4. Rostovtsev A., Public-key cryptosystem based on isogenies / A. Rostovtsev, A. Stolbunov // Cryptology ePrint Archive. Report 2006/145. - 2006. – Режим доступа: <https://eprint.iacr.org/2006/145.pdf>
5. Childs A., Jao D., Soukharev V. Constructing elliptic curve isogenies in quantum subexponential time / A. Childs A., D. Jao, V. Soukharev //Journal of Mathematical Cryptology. – 2014. -Vol8(1). – P. 1–29.
6. Jao D., Soukharev V. Isogeny-based quantum-resistant undeniable signatures //International Workshop on Post-Quantum Cryptography. – Springer, Cham, 2014. – С. 160-179.
7. Chandrasekaran V. Isogeny-based quantum-resistant undeniable blind signature scheme. – 2016.
8. De Feo, L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies/ L. De Feo, D. Jao, J. Plut // Post-Quantum Cryptography. – Lecture Notes in Computer Science. –2006. –Vol.4341. – P.193-210.
9. Costello C., Longa P., Naehrig M. Efficient algorithms for supersingular isogeny Diffie-Hellman //Annual Cryptology Conference. – Springer Berlin Heidelberg, 2016. – С. 572-601.
10. Bröker, R. Constructing supersingular elliptic curves / R. Bröker // J. Comb. Number Theory. – 2009. – Vol. 1(3). – P. 269–273.



ПОДГОТОВКА И ПЕРЕПОДГОТОВКА КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 378.126.018

МУЛЬТИМЕДИЙНЫЕ ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ: ПРОБЛЕМЫ СОЗДАНИЯ И ИСПОЛЬЗОВАНИЯ

Барабаш Павел Александрович¹, Ляшенко Татьяна Васильевна²

¹ Смольный институт Российской академии образования,
Россия, Санкт-Петербург, Полюстровский пр., 59,

²Художественно-технический институт,
Россия, Санкт-Петербург, пр. Культуры, 31,
email:ltv56@mail.ru, barabash_p@yahoo.com

Аннотация: В статье анализируются определяющие тенденции и проблемы создания и реализации мультимедийных образовательных технологий; рассматриваются основные понятия, сущностные характеристики и типология информационных мультимедийных образовательных технологий, используемых в обучении; раскрываются проблемы внедрения информационно-мультимедийных технологий в практику отечественного образования.

Ключевые слова: мультимедиа технологии; образование; электронные издания; мультимедийные учебно-методические комплексы.

MULTIMEDIA EDUCATIONAL TECHNOLOGIES: PROBLEMS OF CREATION AND USE

Pavel Barabash¹, Tatiana Lashenko²

¹Smolny Institute of the Russian Academy of Education
Russia, St. Petersburg, Polyustrovsky ave., 59,

²Art and technical institute,
Russia, St. Petersburg, Culture ave. 31
email:ltv56@mail.ru, barabash_p@yahoo.com

Abstract: This article analyzes the defining tendencies and challenges of creating and putting into practice multimedia educational technologies. It discusses the basic concepts, inherent characteristics and typology of the informational multimedia educational technologies. This article explores challenges associated with putting informational multimedia technologies into practice within domestic education.

Keywords: multimedia technology; education; electronic editions; multimedia educational lecture materials.

В зарубежной образовательной практике накоплен значительный опыт применения мультимедиа-технологий в обучении, которое признается мировой тенденцией, обеспечивающей основу для создания принципиально новой технологии приобретения научных знаний, новых педагогических подходов к преподаванию и усвоению знаний, соответствующих запросам информационного общества. Сущностные особенности мультимедиа позволяют говорить о наличии значительного образовательного, дидактического потенциала у данной технологии, что уже сегодня подтверждено целым рядом исследований как зарубежных, так и отечественных авторов, хотя научное осмысление этого феномена фактически находится на начальном этапе [1]. Поэтому вполне закономерно, что технологии мультимедиа становятся приоритетным направлением исследований по созданию информационных продуктов, ориентированных на массовую аудиторию, и получают все более широкое распространение: уже сегодня они применяются в науке, искусстве, рекламе, и многих других областях.

Вместе с тем на сегодняшний день образовательные мультимедиа-технологии пока еще не оказывают столь кардинального влияния на парадигму образования и связываются прежде всего с использованием учебных мультимедиа-средств в образовании, которые, в соответствии с их типологическими особенностями, подразделяются на следующие основные разновидности: мультимедиа с линейным представлением учебных материалов; гипертекстовые мультимедиа (с нелинейным представлением учебных материалов); мультимедийные обучающие программы или образовательные курсы.

Причем основанием для их выделения служат не столько структурные характеристики, сколько дидактические особенности применения этих средств в обучении. Так, мультимедиа-приложения (продукты, программы, проекты и т.п.), имеющие линейную структуру представления содержания, во многом аналогичны по форме обычной книге или традиционной лекции, поскольку для них характерна фиксированная последовательность изложения материала. Одни из них включают линейную «навигацию», аналогичную содержанию книги, или системы поиска; другие позволяют визуально отследить сложные для изучения темы. Однако в любом случае, обучаемый при работе с таким приложением может лишь перемещаться вперед или назад по изучаемому материалу, контролируя работу приложения только в определении того, какой именно материал он хочет изучать.

Структура приложений с нелинейно упорядоченной мультимедиа-информацией, которая может быть записана на различных носителях данных в компьютере, на компакт-дисках или предоставляться через Интернет, может иметь характер иерархического дерева или совокупности таблиц в реляционных базах данных. Часто такие приложения основываются на технологиях гипертекста или гипермедиа, в которых отдельные элементы информации снабжаются статическими или динамическими связями – ссылками, позволяющими переходить на другие приложения или на другие элементы данного приложения.

При работе с такими мультимедиа-приложениями пользователь не только может выйти на интересующий его раздел или применить систему поиска, но также формировать индивидуальную траекторию изучения материала, управляя последовательностью перехода от одного раздела к другому с помощью системы меню или иных средств визуализации.

Мультимедиа-приложения последней разновидности, часто связанные с целым учебным курсом, позволяют разбить сложные задачи на части и помогают структурировать последовательность выполнения учебных задач, а также предполагают использование средств активизации познавательной деятельности обучаемых, обеспечивая для этого необходимую поддержку. В практике обучения используются два основных типа такого рода приложений: обучающие, которые представляют информацию по изучаемой предметной области и организуют изучение материала; контролирующие, которые в процессе выполнения обучаемым заданий проверяют их правильность и позволяют выявлять ошибки, например, программы-тренажеры (проверка правописания, счетно-логических навыков).

На сегодняшний день в мире создано большое количество разнообразных мультимедийных объектов, которые могут применяться и активно применяются в образовательной практике разных стран: мультимедиа-справочники по многим предметам, музеям, городам и т.д., игровые ситуационные тренажеры, мультимедийные обучающие системы, позволяющие организовывать учебный процесс с использованием новых технологий, и др. Многие страны мира в настоящее время стремятся модернизировать систему образования на основе широкого использования информационных и коммуникационных технологий, и прежде всего мультимедийных, которые предлагают новые перспективы и поразительные возможности для обучения, подтверждая тем самым, что человечество находится на пороге образовательной революции. В то же время сегодня в разных странах уровень информационно-технологической модернизации образования различен, что связано и с общим уровнем информатизации в стране, и с национально-культурной спецификой образовательной системы и педагогических представлений.

В российской практике образования как изучение мультимедийных технологий, их возможностей и специфики, так и их использование в процессе обучения и преподавания пока еще только начинается и сталкивается с определенными сложностями, главным образом, материально-технического характера (ограниченное применение специальных устройств, позволяющих проецировать материал с компьютера на большой экран, недостаточное и бессистемное комплектование фонда программного обеспечения, отсутствие в большинстве образовательных организаций, в том числе высшего образования, полноценных мультимедийных аудиторий и т.п.). Однако сегодня уже ни у кого не вызывает сомнения, что мультимедийная технология даже на нынешнем этапе развития выводит общение между обучаемым и компьютером на новый уровень, расширяет спектр форм и средств информационного обмена в процессе образования.

Возможности обучающих систем, реализованных на базе технологии мультимедиа, позволяют интегрировать аудиовизуальную информацию любых форм (текст, графика, видео, анимации и др.) и представлять ее на экране, реализуя интерактивный диалог пользователя с системой, повышают мотивации обучения, способствуют эмоциональному восприятию информации и формированию умений реализовывать разнообразные формы самостоятельной деятельности по обработке информации [3, с. 382].

Вследствие этого внедрение мультимедийных средств и технологий в образование должно опираться на фундаментальные научные исследования, причем не только и не столько технико-технологического, сколько философского, социологического, культурологического, психологического, педагогического характера. Сегодня такие исследования пока немногочисленны, но они уже охватывают самые разные аспекты проявления этого феномена в современном мире, включая и его применение в образовании. Такие исследования позволяют более четко ставить образовательные

цели внедрения информационно-коммуникационных технологий в учебный процесс с учетом специфики образования (общее или профессиональное, техническое или гуманитарное и т.д.), осуществлять целесообразный и оптимальный отбор технологических средств обучения, обеспечивающих эффективность образовательной деятельности и получение запланированных результатов.

Однако, с другой стороны, общий низкий уровень применения информационно-коммуникационных технологий в обучении, обусловленный ограниченными ресурсными (техническими, финансовыми, человеческими и др.) возможностями образовательных учреждений, сдерживает развитие теоретических представлений и методологических оснований в этой области научно-педагогических исследований. Многие теоретические обобщения сегодня еще невозможны вследствие того, что процессы информатизации образования, в частности учебного процесса, в нашей стране находятся в стадии активного становления и интенсивно развиваются. Так, значительные сложности представляет решение проблем типологизации и классификации мультимедийных образовательных технологий, применяемых в отечественном образовании. Практика показывает, что любые мировые тенденции, как правило, получают специфическое преломление в отечественной образовательной среде, а поэтому принятые и получившие распространение в других странах модели и стратегии применения мультимедиа в учебных целях также могут существенно измениться в процессе адаптации к российским условиям. Это диктует необходимость опираться в исследовании процессов информационно-технологической модернизации образования в большей мере на изучение отечественных тенденций и практики.

Наиболее доступной на сегодняшний день, и поэтому привлекающей внимание специалистов формой использования мультимедийных технологий в образовании является создание локальных и сетевых электронных учебных изданий.

Производство электронных продуктов со сложной функциональностью сегодня представляет собой интенсивно развивающийся сегмент, хотя он появился на рынке информационных технологий сравнительно недавно. На его появление и бурное развитие активно реагируют все рыночные субъекты: мировые компании – производители программного обеспечения и мультимедийного оборудования, предлагающие все более совершенные и функциональные средства создания этих продуктов; многочисленный и постоянно пополняющийся отряд предприятий профессионально, и не очень, занимающихся созданием мультимедиа- и Web-ресурсов; государство, выступающее в роли регулятора зарождающейся индустрии. Так, в нашей стране разработан Госстандарт (ГОСТ 7.83–2001 «Электронные издания. Основные виды и выходные сведения»), определяющий и упорядочивающий понятийный аппарат и терминологию новой информационной отрасли, и приняты меры по государственной регистрации и охране прав создаваемой продукции. Согласно этому стандарту, электронные издания, созданные с применением мультимедийных технологий, получили название мультимедийные электронные издания, под которыми понимается совокупность информации различной природы, которая присутствует равноправно и взаимосвязано для решения определенных разработчиком задач, причем эта взаимосвязь обеспечивается соответствующими программными средствами.

Безусловно, речь идет об определенном классе мультимедийных информационных систем, мультимедиа приложениях, реализуемых по Web-CD технологии. ГОСТ определяет и видовую структуру мультимедийных электронных изданий, подразделяя их на научные, научно-популярные, производственно-практические, учебные, справочные, досуговые, рекламные и художественные электронные издания. Активно формируется система экспертизы и сертификации таких изданий.

В 2012 году состоялся Первый Форум вузовских издателей «Электронные учебные издания в современном вузе. Стратегия подготовки и создания» при участии Европейской Экономической палаты (EEIG). В работе Форума приняли участие представители около 40 вузов различных регионов России. По словам директора НТЦ «Информрегистр» Е. И. Козловой наибольшая доля электронных изданий (46%) сосредоточена в сфере образования и основными факторами, тормозящими развитие этого рынка, являются: нелегитимная продукция; консерватизм читателей и издателей; недостаточная оснащённость компьютерами и Интернетом; низкий уровень освоения информационных технологий; низкая издательская культура. 4 февраля 2016 года в Издательском доме НИУ ВШЭ состоялся Круглый стол «Электронная книга в вузовском издательстве: производство, дистрибуция прав» на котором, в рамках профессиональной дискуссии, были обозначены основные векторы развития электронного книгоиздания.

Применение локальных электронных учебных изданий в процессе обучения, в зависимости от их специфики, может быть направлено на достижение различных дидактических целей, и, соответственно, различными по своим характеристикам будут образовательные технологии – как совокупность и последовательность алгоритмизированных операций, – основой которых данные мультимедийные объекты выступают. Однако общим для них является то, что применение мультимедийных учебных средств принципиально не меняет характер и структуру процесса обучения, во многом сохраняющего традиционный характер трансляции знаний (информации) на основе субъект-объектных отношений преподавателя и студентов. Это позволяет объединить образовательные

технологии данной разновидности в одну группу понятием «мультимедийное сопровождение учебного процесса».

Как показывает практика отечественного образования, применение мультимедийных технологий в обучении на сегодняшний день фактически ограничивается разработкой именно мультимедийного сопровождения лекционных занятий, что неудивительно, поскольку даже это связано с большими трудностями и требует от специалистов значительных усилий. Вместе с тем, несмотря на все сложности, эта форма применения технологии мультимедиа получает все большее распространение в образовании, поскольку такие лекции уже имеют целый ряд преимуществ по сравнению с традиционными.

Однако, перспективы развития информационно-коммуникационных технологий в образовании связываются с разработкой и применением таких образовательных технологий, которые позволят кардинально изменить характер процесса обучения: позиции преподавателя и обучающегося, способы получения и представления знаний, формы и методы развивающего педагогического воздействия и т.д. Причем важно, чтобы эти системные изменения обеспечили повышение эффективности и качества образования, позволили преодолеть те негативные факторы, которые обуславливают кризисное состояние современного образования, создали оптимальные условия для его модернизации. И именно возможности сетевых мультимедийных образовательных технологий открывают сегодня перспективы для решения этой важнейшей социальной задачи [4].

На российском рынке информационной продукции в последние годы появилось большое количество мультимедийных средств учебного назначения размещенных в Интернете. По мере компьютеризации и материально-технического оснащения образовательных учреждений эти мультимедийные продукты становятся им все более доступными. В то же время их качество и идеология далеко не всегда отвечают потребностям конкретных научно-педагогических коллективов учебных заведений, особенно высших, и поэтому во многих вузах, в большей мере, по сравнению с другими образовательными учреждениями, обладающих необходимыми для этого ресурсами создание таких мультимедийных учебных средств осуществляется собственными силами.

Мультимедийные технологии данной разновидности позволяют предельно расширить пространство образования за счет развития различных форм дистанционного обучения, что может рассматриваться как определяющий фактор в обеспечении непрерывности образования, являющейся в современном динамично изменяющемся и интегрированном мире его сущностной характеристикой.

Это обуславливает актуальность и необходимость создания мультимедийных образовательных технологий организации учебного процесса.

В практике отечественного образования уже есть примеры создания и внедрения в инновационном порядке образовательных технологий, которые могут быть отнесены к данной группе. Наиболее полно реализовать возможности мультимедиа технологий данной разновидности, на наш взгляд, на сегодняшний день позволяет организация учебного процесса в вузе на базе мультимедийного учебно-методического комплекса дисциплины.

Понятие «мультимедийный учебно-методический комплекс (МУМК)» получает все более широкое распространение в образовании, однако разные специалисты наполняют его разным содержанием и смысловым объемом.

По мнению ряда исследователей, МУМК является наиболее оптимальным видом электронного учебного издания, который в полной мере использует особенности мультимедийных технологий, поскольку изначально включает в себя гипертекст, видео- и аудиоприложения, анимацию, большое количество иллюстративного материала, интерактивные блоки, позволяющие закреплять учебный материал в игровой форме, а также осуществлять контроль знаний учащегося. Важным и неотъемлемым его свойством является интерактивность, так как именно она позволяет обеспечить большую акцентированность обучающегося на учебном процессе. Выдача новой информации происходит в ответ на соответствующие действия, и это является дополнительным стимулом для изучения работы программы-МУМК и погружения в учебный процесс. Использование МУМК позволяет добиться повышения понимания учебного материала, развития творческих способностей, обеспечить деятельностный подход к обучению [2, 5]. Благодаря четкому структурированию информационных единиц становится возможным избежать проблем с фрагментарностью и хаотичностью восприятия новой информации и связанным с этими факторами рассеиванием внимания, что позволяет обучающимся сконцентрироваться на усвоении материала.

Таким образом, на сегодняшний день в отечественном образовании именно мультимедийные учебно-методические комплексы создают реальную возможность для разработки и внедрения в практику обучения полноценных компьютерных курсов, а значит – для кардинального качественного преобразования самого процесса обучения.

Это обуславливает актуальность и необходимость создания и использования мультимедийных образовательных технологий организации учебного процесса.

СПИСОК ЛИТЕРАТУРЫ

1. Мультимедиа в образовании: специализированный учебный курс / Бент Б. Андресен, Катя Ван ден Бринк; авторизованный пер. с англ. – 2-е изд., испр. и доп. – М.: Дрофа, 2007. – 224 с. – (Информационные технологии в образовании).

- Мультимедийные технологии в библиотечном образовании : монография / Т.В. Ляшенко. – СПб. : Изд-во РГПУ им. А.И. Герцена, 2010. – 304 с.
2. Словарь-справочник по педагогике / Авт.-сост. В.А. Мижериков; Под общ. ред. П.И. Пидкасистого. – М.: ТЦ Сфера, 2004. – 448 с.
 3. Падерин В.Н. Использование мультимедийных технологий в обучении студентов вузов: [Электронный документ] // Управление экономическими системами: электронный научный журнал. -2016.- № (87) 5. (<http://uecs.ru/uecs-87-872016/item/3935-2016-05-13-07-42-59>).
 4. Романченко Т.Н. Электронный учебник как средство формирования информационной культуры студентов: автореф. дис. ... канд. пед. наук / Т.Н. Романченко. – Саратов, 2005. – 22 с.

УДК 004.056.53

ЛАБОРАТОРНЫЙ ПРАКТИКУМ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»

Барабаш Павел Александрович, Панасенко Михаил Александрович
Смольный институт Российской академии образования,
Россия, Санкт-Петербург, Полюстровский пр., д. 59,
email: barabash_p@yahoo.com, panasenko16.01.93@mail.ru

Аннотация: в докладе рассматриваются особенности функционирования лабораторного практикума по учебной дисциплине «Безопасность информационных систем». Приведен перечень лабораторных работ, цели и задачи при их выполнении студентами.

Ключевые слова: безопасность информационных систем; сервер безопасности; система защиты информации; учетные записи.

LABORATORY PRACTICUM ON EDUCATIONAL DISCIPLINE "SECURITY OF INFORMATION SYSTEMS"

Barabash Pavel, Panasenko Mikhail
Smolny Institute of the Russian Academy of Education,
Russia, St. Petersburg, Polyustrovsky ave., 59,
e-mail: barabash_p@yahoo.com, panasenko16.01.93@mail.ru

Abstract: the report discusses the features of functioning of a laboratory practical work on discipline «Security of information systems». The following is the list of labs, aims and objectives with their students.

Keywords: the security of information systems; server security; security system information; accounts.

Учебная дисциплина «Безопасность информационных систем» относится к блоку Б1.В вариативной части учебного плана по направлению подготовки 09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ (уровень бакалавриата).

В соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по указанному направлению подготовки, дисциплина поддерживает следующие компетенции:

- понимание сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности (ОПК-4);
- владение основными методами защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий (ОК-12);
- знание своих прав и обязанностей как гражданина своей страны, способность использовать действующее законодательство и другие правовые документы в своей деятельности, демонстрировать готовность и стремление к совершенствованию и развитию общества на принципах гуманизма, свободы и демократии (ОК-9).

Трудоемкость учебной дисциплины составляет 108 часов, из которых 16 часов – лекционных и 24 часа запланировано на выполнение лабораторных работ.

Лабораторный практикум включает 10 лабораторных работ, предназначенных закрепить у студентов навыки практической работы со специальными программными средствами защиты информации.

Лабораторная работа №1 призвана ознакомить студентов с процессами загрузки виртуальной машины и установки на ней Windows Server 2003.

Лабораторная работа №2 знакомит с общими принципами работы сервера безопасности и предполагает его установку.

Лабораторная работа №3 посвящена изучению вопросов администрирования сервера безопасности (СБ), работой с консолью СБ.

Лабораторная работа №4 предлагает загрузить виртуальную машину Windows и установить на ней ОС Windows 7.

Лабораторная работа №5 посвящена установке системы защиты информации (СЗИ).

Лабораторная работа №6 знакомит студентов с подсистемой управления доступом и полномочиями на управление этой системой.

Лабораторная работа №7 предназначена для работы с учетными записями в СЗИ.

Лабораторная работа №8 посвящена тонким настройкам учетных записей в СЗИ, в частности, определению числа разрешенных сеансов для данной учетной записи, смене пароля для авторизации средствами ОС, смене пароля с помощью оболочки администратора, работе с сессиями-исключениями, работе с заблокированными пользователями.

Лабораторная работа №9 позволяет ознакомить студентов с вариантами тонкой настройки учетных записей для контроля доступа и устройств, в частности, с разделами настройки полномочия на управление контролем устройств, разграничением доступа к устройствам, понятиями дискреционного принципа разграничения доступа к устройствам и мандатного доступа.

Лабораторная работа №10 оперирует с вариантами тонкой настройки учетных записей для настройки Домена безопасности и работы с ним в среде СБ. Студенты осуществляют ввод клиента в домен безопасности (ДБ), ввод защищенного компьютера в ДБ, вывод клиента из ДБ, настройки ДБ, настройку сервера лицензий для СБ, производят визуализацию топологии Домена безопасности.

После выполнения каждой лабораторной работы студенты создают отчет, представляющий собой текстовый файл, оформленный в соответствии с определенными требованиями, содержащий скриншоты (снимки экрана компьютера) операций с описанием процедур выполнения. Отчет размещается в личном кабинете электронной образовательной среды института. Таким образом, формируется часть портфолио студента, в соответствии с требованиями ФГОС ВО.

СПИСОК ЛИТЕРАТУРЫ

1. Б.Я. Советов, В.В. Цехановский. Информационные технологии: теоретические основы. Учебное пособие. СПб: Лань, 2017 г. 444 с.

УДК 004.89

МОДЕЛИРУЮЩИЙ УЧЕБНО-ТРЕНИРОВОЧНЫЙ ТРЕНАЖЕР ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОГО ФУНКЦИОНИРОВАНИЯ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ

Богданов Тимур Рушанович, Яшин Александр Иванович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, д. 5,
emails: tbogdanov@gmail.com; vvchehanovsky@mail.ru

Аннотация: Рассматривается организация учебно-тренировочного тренажера для моделирования поведения объектов геоинформационных систем. Тренажер включает базу геопространственных данных территории, обстановки, объектов. Тренажер осуществляет симуляцию учебно-тренировочной обстановки в соответствии со сценарием поведения объектов ГИС.

Ключевые слова: геоинформационные системы; мобильные объекты; симуляции поведения объектов обучение профессиональных кадров; учебно-тренировочный тренажер оперативной обстановки

SIMULATION TRAINING SIMULATOR TO ENSURE THE SAFE OPERATION OF GEOGRAPHIC INFORMATION SYSTEMS

Bogdanov Timur, Yashin Alexander
The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
emails: tbogdanov@gmail.com; vvchehanovsky@mail.ru

Abstract: Discusses the organization of the training simulator is to simulate the behavior of objects in geographic information systems. The simulator includes a database of geospatial data of site, situation and objects. The simulator carries out the simulation training environment in accordance with scenarios of behavior of objects of a GIS.

Keywords: geographic information systems; mobile objects; simulation of the behavior of objective objective professional staff; a training simulator operational environment.

Обеспечение безопасного функционирования геоинформационных систем (ГИС) в значительной степени связано с квалификацией ответственного кадрового состава, принимающего определенные командные решения. Среди специализированных профессиональных задач, связанных с разнородным комплексным анализом объектов и ситуаций ГИС, существует набор задач, подразумевающих обязательное наличие опыта непосредственной работы профессиональных кадров в реальных условиях. Область решения задач ГИС связана с моделированием поведения мобильных объектов, включающего их передвижение и отображением на программно-применяемых картах ландшафта территории и территориально-распределенных объектов ГИС. Специфика работы ГИС сопряжена с высокой маневренностью объектов и четким описанием обстановки для формирования и установления поведения и передвижения объектов ГИС. Для обеспечения безопасного функционирования современной

высокотехнологичной распределенной системы был поставлен вопрос разработки специализированного методологического инструментария, способного моделировать ситуативное поведение разнородных мобильных объектов, оценивать обстановку по полученным оперативным данным, обеспечивать возможность принятия определенных командных решений ответственным лицом.

Учебно-тренировочный тренажер является моделирующим симулятором оперативной обстановки; моделей поведения объектов ГИС; сценариев тренировочных занятий ГИС; базой геопространственных данных территории, обстановки, объектов. Ядро моделирования тренажера осуществляет симуляцию учебно-тренировочной обстановки в соответствии с заданным сценарием. Под моделированием понимается решение формализованной задачи, ассоциированной с некоторой сущностью, называемой программным агентом. Имитационная модель включает планирование и прогнозирование поведения агентов, определение четких взаимосвязей между восприятием агентом окружающей обстановки и формированием реакций на нее. На картах территории отображаются передвижения мобильных объектов, данные об изменении координат получаются с разных территориально распределенных источников. Производится анализ передвижения объектов, включая определение семантики объекта по характеру движения, построение маршрута передвижения, а также прогнозирование последующих позиционных характеристик объекта. Основная сложность моделирования заключается в определении моделей поведения отдельных сущностей (программных агентов). Для достижения наибольшего эффекта от обучения тренажер предоставляет широкие возможности по изменению разнообразных факторов и условий решения задач ГИС, поэтому модель каждого из программных агентов должна предусматривать регистрацию возникающих изменений и соответствующим образом перестраивать свое поведение. В ходе симуляции поведения объектов ГИС воссоздаются модели поведения всех расположенных в области установленной карты программных агентов и отмечаются передвижения мобильных объектов на выбранном участке карты. Выбор географической карты и геопространственной расстановки подконтрольных единиц входит в перечень необходимых действий ответственного лица или системы моделирования. Моделирование поведения объекта включает в себя прогнозирование его последующих позиционных характеристик. На каждом шаге моделирования происходит обновление параметров всех контролируемых объектов согласно модели поведения агента. При необходимости создаются новые сущности и формируются их модели поведения. Предложен графический инструментарий для формирования моделей поведения программных агентов и составления сценариев учебно-тренировочных занятий, что дает возможность производить расширение системы для новых задач и увеличивать размерности ГИС.

Архитектура моделирующего учебно-тренировочного тренажера является гибкой с точки зрения добавления новых сущностей и моделей их поведения, что поддерживается пользовательским графическим редактором, позволяющим вносить собственную логику в поведение новых или уже существующих объектов. Наличие определенной общепонятной нотации в рамках предложенного редактора дает возможность однозначно описывать модели поведения различной сложности. Применяются иерархические графовые структуры, которые могут наглядно отображать зависимости выполнения тех или иных действий программного агента от его состояния и условий внешней среды. Применена собственная модификация структуры описания моделей поведения, называемой «деревья поведения» (англ. Behavior trees) с более высокоуровневой абстракцией над деревьями поведения и одновременной специальной модификацией общепринятой нотации.

Помимо трансляции построенного графа в программную модель дерева поведения, предусмотрена функция её прямого и обратного преобразования в некоторый стандартизованный формат данных, что предоставляет возможность сохранения и последующего воссоздания исходных моделей для их импортирования как обратно в редактор, так и в ядро моделирования без необходимости повторной сборки исходного кода программного комплекса.

Обучение профессиональных кадров для работы в контуре ГИС с помощью моделирующего учебно-тренировочного тренажера для обеспечения безопасного функционирования ГИС предоставляет широкие возможности по освоению различных ситуаций с изменением разнообразных факторов и условий по ходу проведения занятий на тренажере, что влечет за собой перемены в структуре модели поведения программных агентов и принуждает обучаемого соответствующим образом корректировать свои действия. Формирование контекста занятия преподавателем или куратором состоит из нескольких этапов, первый из которых заключается в выработке сценария проведения учебно-тренировочного занятия, для некоторых сущностей программных агентов есть возможность переключения тренажера в ручной режим управления обучаемым прямо во время тренировки. Максимальное сближение реальной работы ГИС с режимами работы моделирующего учебно-тренировочного тренажера значительно повышает безопасность функционирования ГИС за счет заметного сокращения искажающего влияния человеческого фактора кадрового обслуживания объектов системы и управляющих действий ответственных лиц, принимающих решения по всем уровням функционирования ГИС.

СПИСОК ЛИТЕРАТУРЫ

1. Б.Я. Советов, В.В. Цехановский. Информационные технологии: теоретические основы. Учебное пособие. СПб: Лань, 2017 г. 444 с.

УДК 371.1

ИССЛЕДОВАНИЕ КАЧЕСТВА ОБРАЗОВАНИЯ ПРИ ПОДГОТОВКЕ СОТРУДНИКОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Большакова Людмила Валентиновна, Кузьмина Кристина Александровна,
Яковлева Наталья Александровна
Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, ул. Летчика Пилютова, 1,
emails: blv5505@mail.ru, kristina26.97@mail.ru, kumirova@mail.ru

Аннотация: В статье рассмотрен новый подход к оценке качества образования будущих сотрудников в сфере информационной и экономической безопасности с применением математико-статистических методов и метода экспертных оценок. Результаты, полученные с помощью предлагаемого подхода, могут быть использованы для совершенствования программ обучения студентов (курсантов) и выявления степени сформированности профессиональных компетенций выпускаемых вузами специалистов.

Ключевые слова: качество образования; методика оценки; метод экспертных оценок; тестирование; эксперты.

A STUDY OF THE QUALITY OF EDUCATION IN THE TRAINING OF PERSONNEL IN THE FIELD OF ENSURING INFORMATION AND ECONOMIC SECURITY

Bolshakova Lyudmila, Kuzmina Kristina, Yakovleva Natalia
The St.-Petersburg University of the Ministry of Internal Affairs of Russia,
Russia, St. Petersburg, Pilot Pilyutov Street 1,
emails: blv5505@mail.ru, kristina26.97@mail.ru, kumirova@mail.ru

Abstract: The article describes a new approach to the assessment of the quality of education of future employees in the field of information and economic security with the use of mathematical-statistical methods and expert judgment. The results obtained using the proposed approach can be used to improve learning programmes students (cadets) and identify the level of formation of professional competences produced by universities.

Keywords: the quality of education; methods of evaluation; method of expert evaluations; testing; experts.

Введение. Приоритетным направлением в образовательной деятельности вуза является освоение обучающимися образовательных программ и применение ими на практике полученных знаний. Следует отметить, что вузами накоплен достаточно большой опыт оценивания качества подготовки выпускников. В последние годы активно применяются такие методики оценивания как Интернет – экзамен, социологические исследования (мнение преподавателей, опросы работодателей). Однако эти методики вызывают критику специалистов в сфере высшего образования, а основной действующий подход (тестирование) не отражает реального положения дел.

Особенностью авторской методики является универсальность ее применения, что позволяет оценить качество профессиональной подготовки курсантов (студентов) на различных уровнях, как в рамках структурного подразделения (группа, курс) или в рамках вуза, так и на федеральном уровне. Таким образом, данная методика может применяться как преподавателями, при оценке знаний курсантов (студентов) на семинарских и практических занятиях, при приеме зачетов, экзаменов, так и Федеральной службой по надзору в сфере образования и науки при сравнении качества образования различных вузов.

Методика, предлагаемая авторами, состоит из двух этапов.

На первом этапе исследуются вопросы изменения уровня владения профессиональными знаниями от курса к курсу для конкретного учебного заведения. Разумным здесь будет предположение, что уровень подготовки студента или курсанта находится в прямой зависимости от номера курса, на котором он обучается, поскольку его осведомленность в тех или иных вопросах растет с каждым годом по мере накопления и усвоения получаемых знаний. Основная работа первого этапа состоит в проведении тестирования обучающихся по некоторым, заранее определенным, профильным дисциплинам. Проводиться данная процедура может, например, для учащихся первого, третьего и четвертого курсов. Всем тестируемым предлагаются одинаковые тесты; время, предоставляемое обучаемым на их решение, должно быть ограничено и заранее оговорено. Существенным моментом также является то, что задания в проводимом тестировании необходимо, на взгляд авторов, подчинить определенному требованию: вопросы должны быть составлены таким образом, чтобы для их понимания тестируемому не требовалось наличия специальных знаний. Опрашиваемому должна быть доступна суть вопроса, даже если он не располагает, как компетентный специалист, достаточными сведениями в рассматриваемой области; однако правильный ответ дать человеку, не получившему профильного образования, будет не просто. Для составления тестов предполагается создание рабочей

группы, состоящей из экспертов, которые способны профессионально оценить качество образования в вузе: преподаватели учебного заведения или же, возможно, практические работники. Анализ результатов первого этапа должен быть проведен с использованием различных математико-статистических методов и представлением в наглядной форме для удобства анализа, оценки результатов и формирования выводов о качественном уровне знаний опрошенных групп.

Суть второго этапа заключается в сопоставлении результатов, показанных обучающимися в данном вузе, с теми, что были получены от практических работников. В основе второго этапа лежит метод экспертных оценок. Необходимо отметить, что наиболее существенным моментом в данном сравнении будет являться выявление степени согласованности данных полученных от этих двух групп опрашиваемых. Если согласованность мнений курсантов и практических работников по отдельности подтверждается, то далее проверяется согласованность ответов между общими результатами курсантов и общими результатами практических работников. Проанализировав экспертные данные можно сформулировать выводы относительно степени согласованности мнений курсантов и практических работников, а, следовательно, о том, насколько теоретические знания, усвоенные обучающимися, совпадают с мнением опытных специалистов, ежедневно решающих профессиональные задачи в данной сфере на практике.

Стоит отметить, что также можно провести сравнение полученных результатов среди различных вузов, что позволит определить, учащиеся какого учебного заведения показали как наиболее высокий, так и самый низкий результат, а, следовательно, и отметить среди них тот вуз, которое успешнее осуществляет подготовку кадров заданной специальности.

Заключение. Подводя итог вышеизложенному, необходимо отметить, что, так как исследование качества образования при подготовке сотрудников в сфере информационной и экономической безопасности является в настоящее время актуальной и важной проблемой, то методика определения уровня образования имеет особое значение. Результаты, полученные с помощью предложенной методики можно использовать для совершенствования программ обучения студентов (курсантов) и выявления степени сформированности профессиональной компетенции выпускаемых вузами специалистов.

СПИСОК ЛИТЕРАТУРЫ

1. Иванченко И. В. Проблема повышения качества образования в вузе // Молодой ученый. 2016. №5.1. С. 18-21.
2. Орлов А. И. Теория принятия решений – Экзамен, 2005. 656 с.
3. Примакин А.И., Большакова Л.В. Метод экспертных оценок в решении задач обеспечения экономической безопасности хозяйствующего субъекта. - Вестник Санкт-Петербургского университета МВД России. 2012. №1. С. 191-200.
4. Кунтурова Н.Б., Яковлева Н.А., Подход к оцениванию профессиональной компетентности специалистов силовых структур по видам деятельности при организации контроля формирования профессиональной компетентности. - Вестник Санкт-Петербургского университета МВД России. 2016. №2 (70). С. 146-151.
5. Вилков В.Б., Большакова Л.В., Черных А.К., Яковлева Н.А. Применение методов оптимизации при выработке решений в обучении курсантов в образовательных организациях силовых структур. - Вестник Санкт-Петербургского университета МВД России. 2017. №2 (74). С. 165-173.

УДК 378.145

О НЕОБХОДИМОСТИ ПОДГОТОВКИ И ПЕРЕПОДГОТОВКИ КВАЛИФИЦИРОВАННЫХ КАДРОВ В СФЕРЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Бурлов Вячеслав Георгиевич, Грачев Михаил Иванович, Примакин Алексей Иванович
Санкт-Петербургский университет МВД России,
Россия, Санкт-Петербург, улица Летчика Пилютова, 1,
emails: burlovvg@mail.ru, mig2500@mail.ru, a.primakin@mail.ru

Аннотация: В статье рассмотрены вопросы необходимости подготовки и проведения переподготовки квалифицированных кадров в сфере безопасности информационных технологий в правоохранительной сфере кафедры специальных информационных технологий Санкт-Петербургского университета МВД России с целью повышения эффективности деятельности как правоохранительных органов, так и безопасности в целом.

Ключевые слова: безопасность; информационные технологии; управленческие решения; Web-технологии; правоохранительная сфера.

ABOUT NECESSITY OF PREPARATION AND RETRAINING OF QUALIFIED PERSONS IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

Burlov Vyacheslav, Grachev Mikhail, Primakin Alexey
Ministry of Internal Affairs Sankt-Peterburgsky university of Russia,
Russia, St. Petersburg, Pilot Pilyutov Street, 1,
emails: burlovvg@mail.ru, mig2500@mail.ru, a.primakin@mail.ru.

Abstract: The article considers the issues of the need to train and conduct retraining of qualified personnel in the field of information security in the law enforcement sphere of the Special Information

Technologies Department of the St. Petersburg University of the Ministry of Internal Affairs of Russia in order to improve the effectiveness of both law enforcement agencies and security in general.

Keywords: *security; information technologies, management solutions, Web technologies, law enforcement.*

Введение. Повсеместное развитие и внедрение Web-технологий в повседневную деятельность человека, как облегчает ему выполнение поставленных перед ним задач, так и накладывает определенную ответственность за сохранение персональной и служебной информации, а порой и конфиденциальной информацией с которой он работает в своей повседневной деятельности. Для правоохранительных органов, сохранение баз данных и предотвращение их кражи из государственных учреждений является одной из приоритетных задач.

Разработанный и подписанный 9 мая 2017 года Указ Президента Российской Федерации №203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы», ставит целью создание условий для формирования в России общества знаний. Особое внимание уделяется обеспечению защиты информационной инфраструктуры Российской Федерации, замены импортного оборудования и программного обеспечения. Ключевым направлением повышения конкурентоспособности российских информационных и коммуникационных технологий отводится на развитие науки, техники, технологий и что особенно важно подготовке квалифицированных кадров в сфере информационных и коммуникационных технологий [1].

В другом не менее важном документе, а именно в Указе Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», основным направлением обеспечения информационной безопасности в области науки, технологий и образования выделяют развитие и подготовку кадрового потенциала в области обеспечения информационной безопасности и применения информационных технологий [2].

Таким образом, профессиональная подготовка и переподготовка кадров в сфере безопасности информационных технологий, выносятся как крайне важные. В Санкт-Петербургском университете МВД России осуществляется подготовка специалистов по технической специальности: «Безопасность информационных технологий в правоохранительной сфере» (Специализация № 1 «Технологии защиты информации в правоохранительной сфере»). Эти направления подготовки для университета являются новыми и требуют особого подхода в организации учебного процесса и создании материально-технической базы.

Выпускники, получив соответствующую квалификацию, направляются в свой комплектующий отдел от которого они направлялись на учебу. Зачастую в своей повседневной деятельности они сталкиваются с состоянием неопределенности, когда необходимо выбрать наиболее правильное управленческое решение. И только проанализировав имеющиеся информационные данные, которые могут также быть не точны, частично не правильны или просто ошибочны мы переходим к мыслительному процессу со всеми за и против для принятия наиболее подходящего правильного решения. В настоящее время Web-технологий помогают им проводить анализ имеющихся данных, что ускоряет процесс принятия наиболее подходящего и правильно управленческого решения. [3].

Если же затронуть подразделения, обеспечивающие безопасность дорожного движения, то управление безопасностью дорожного движения есть многогранный сложный процесс. Особыми возможностями для повышения эффективности управления безопасностью дорожного движения обладают Web – технологии. Лицо, принимающее решение, формирует процессы обеспечения безопасности дорожного движения в форме модели своего решения. В рамках направления использования информационных технологий для управления безопасностью дорожного движения следует рассмотреть разработку математической модели управления безопасностью дорожного движения, учитывающей возможности Web-технологий. В основу аналитической динамической модели положен закон сохранения целостности объекта. Разработка системы управления безопасности дорожного движения на основе предлагаемой модели позволит повысить оперативность управления безопасностью дорожного движения при удовлетворении требований гарантии достижения цели управления [4].

Заключение. Во процессе стремительного развития информационных технологий и компьютеризации практически всех сфер жизнедеятельности человека возросло количество атак с использованием компьютерных технологий, приводящих к хищению информации, информационных ресурсов и информационных систем, что не могло не отразиться на развитии таких направлений подготовки и переподготовки кадров, которые в последующем смогут противостоять данным угрозам. Дальнейшее развитие и подготовка специалистов по технической специальности: «Безопасность информационных технологий в правоохранительной сфере» считаю приоритетным и заслуживающим внимания.

СПИСОК ЛИТЕРАТУРЫ

1. Указ Президента Российской Федерации от 09.05.2017 № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы [Электронный ресурс]. URL: <http://publication.pravo.gov.ru/Document/View/0001201705100002> (дата обращения: 11.09.2017).

2. Указ Президента Российской Федерации от 05.12.2016 г. № 646 [Электронный ресурс]. URL: <http://www.kremlin.ru/acts/bank/41460> (дата обращения: 11.09.2017).
3. Burlov V.G., Grachev M. I., Shlygina N. S. «Adoption of management decisions in the context of the uncertainty of the emergence of threats» // 2017 XX IEEE International Conference on Soft Computing and Measurements (SCM) [Электронный ресурс]. URL: <http://ieeexplore.ieee.org/document/7970510/> (дата обращения: 11.09.2017).
4. Burlov V.G., Grachev M. I. «Development of a Mathematical Model of Traffic Safety Management with Account for Opportunities of Web Technologies» // Transportation Research Procedia [Электронный ресурс]. URL: <https://doi.org/10.1016/j.trpro.2017.01.023> (дата обращения: 11.09.2017).

УДК 007

СЕТЕЦЕНТРИЗМ – ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКАЯ ОСНОВА ЦИФРОВОГО ОБЩЕСТВА

Верзун Наталья Аркадьевна¹, Колбанев Михаил Олегович¹, Касаткин Виктор Викторович²

¹ Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5,

² Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия, 39,
emails: verzun.n@unecon.ru, mokolbanev@mail.ru, v.v.kasatkin@iias.spb.su

Аннотация: Описываются причины появления, основные принципы и характерные особенности новой сетевцентрической парадигмы управления. Сетевцентризм рассматривается как информационно-технологическая основа цифрового общества, как подход к управлению деятельности человека, способный адаптивно подстраиваться под глобальные вызовы современности.

Ключевые слова: *сетевцентризм; сетевцентрический подход к управлению; цифровая экономика; цифровая модель.*

NETWORK-CENTRIC – INFORMATION-TECHNOLOGY-BASED DIGITAL SOCIETY

Verzun Natalya¹, Kolbanev Mikhail¹, Kasatkin Victor²

¹ The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,

² St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,
Russia, St. Petersburg, 14 Line, 39
emails: verzun.n@unecon.ru, mokolbanev@mail.ru, v.v.kasatkin@iias.spb.su

Abstract: Describes the causes, underlying principles and characteristic features of the new network-centric management paradigm. Network-centric is seen as information-technology-based digital society, as a promising approach to the management of human activities capable of adaptive to adapt to global challenges.

Keywords: *network-centric, network-centric approach to governance; digital economy; digital model.*

Доклад посвящен концепции сетевцентризма, которая рассматривается авторами как информационно-технологическая основа цифрового общества. Анализируются происхождение и эволюция понятия «сетевцентризм». Возникший на рубеже веков, изначально данный термин использовался в военной сфере для определения войны нового типа – сетевцентрической (или сетевцентричной) [1]. Однако, вскоре тема сетевцентризма из изданий военного, политического характера «перекочевала» в работы экономической, социально-экономической, гуманитарной и пр. направленностей, а идеи сетевцентрического подхода к управлению вышли за рамки военной сферы и сегодня приобрели более широкое «гражданское» значение [2, 3].

Традиционный подход к управлению, основанный на жесткой вертикали власти, «не справляется» в условиях динамично, неожиданно и непредсказуемо меняющейся обстановки, наличия большого числа неопределенностей, растущих объемов информации, требуемых для адекватной оценки ситуации и т.д., которые характерны для цифровой экономики. На смену ему приходят новые подходы к управлению деятельности человека, способные адаптивно подстраиваться под глобальные вызовы современности [4]. С этим связана и появление новой парадигмы управления – так называемой поствизерновской кибернетики [5], компонентом которой является, в частности, сетевцентризм.

Основой для цифровой экономики (и цифрового общества в целом) постепенно становится сетевцентризм. Сетевцентрический подход к управлению деятельности рассматривается как одно из перспективных направлений в развитии кибернетики и как новая методология деятельности современного человека. Уже сегодня в той или иной степени сетевцентрические системы и связанные с ними методы управления используются в различных областях деятельности: в системе государственного управления, в социальной и финансовой сфере, в экономике и образовании.

Также есть и более узкое понятие термина сетевцентризм: под ним подразумевается необходимость в насыщении систем управления современными средствами инфокоммуникаций, которые являются информационно-коммуникационной основой всякой сетевцентрической деятельности современного человека. Обществом постепенно осознается ключевая, ведущая роль инфокоммуникаций в развитии человечества [6-10]. Инфокоммуникация – базовая технология

цифрового общества и цифровой экономики; она является и объектом бизнеса, и инструментом предпринимательства, и предметом сервиса, и инфраструктурой экономики, и средством для человеческого и профессионального общения [11-15].

Излагаются основные принципы сетецентрического подхода к управлению деятельностью, который: ориентирован на повышение её эффективности; предусматривает отход от централизованной модели управления и наделение правом самостоятельного принятия решений периферические (местные) органы; предполагает совместное использование информации при устойчивом взаимодействии всех системных уровней.

Характерными особенностями сетецентрических систем являются:

- цифровое описание всех объектов предметной области;
- распределенная неоднородная сетевая архитектура;
- точность информационного описания всех событий;
- совместная мобильность сетевых объектов;
- охват территорий произвольных размеров и конфигурации;
- работа в реальном масштабе времени;
- надежность и неуязвимость всего комплекса информационных ресурсов [16-21] и др.

По мнению авторов, сегодня сетецентризм [22] надо понимать, как концепцию деятельности, в основе которой лежит стремление накрыть пространство (территорию) инфокоммуникационной сетью для комплексных измерений в реальном времени параметров пространства, формирования цифровых моделей всех его объектов, создания единой среды информационного взаимодействия и обеспечения согласованности действий всех участников, под которыми теперь понимаются не только люди, но технические устройства, программные компоненты.

СПИСОК ЛИТЕРАТУРЫ

1. Осипов В. Ю. Куприянов А. А. Принципы сетецентрического подхода и их применимость при решении задач управления силами (войсками). URL: http://www.apu.npomars.com/images/pdf/17_11.pdf
2. Кудж С. А. Принципы сетецентрического управления в информационной экономике // Госсоветник. 2013. №4. URL: <http://cyberleninka.ru/article/n/printsipy-setetsentricheskogo-upravleniya-v-informatsionnoy-ekonomike>
3. Верзун Н. А., Ипатов О. С., Колбанёв М. О. О сетецентрических моделях цифровой экономики // Сборник: Информационные технологии цифровой экономики: сб. статей. – СПб.: Изд-во СПбГЭУ, 2017. С.35–41.
4. Новиков Д. А. Кибернетика: Навигатор. История кибернетики, современное состояние, перспективы развития. – М.: ЛЕНАНД, 2016. –160 с.
5. Хохлова М. Н. Гармогенез. Поствинеровская кибернетика / Русский инженер. 2013. – №2(37). – С.34–35.
6. Верзун Н. А., Колбанёв М. О., Михайлов С. В. Информационные технологии в периодизации истории / Ученые записки Международного банковского института. Вып. 13. – СПб.: Изд-во МБИ. – 2015. – С.150–161.
7. Максимцев И. А., Колбанёв М. О., Коршунов И. Л., Левкин И. М., Микадзе С. Ю. О технологических основаниях новой доктрины информационной безопасности Российской Федерации / Новые горизонты глобального мира: сб. научн. тр./ Балт. Гос. Техн. ун-т. СПб. – 2015. – С.270–281.
8. Колбанев М. О., Коршунов И. Л., Левкин И. М. Проблемы информационно-технологической деятельности / Изв. вузов. Приборостроение. – 2017. – Т.60, № 2. – С.105–109.
9. Верзун Н. А., Колбанев М. О., Омелян А. В. Введение в инфокоммуникационные технологии и сети Future Networks: учебное пособие. – СПб.: Изд-во СПбГЭУ, 2016. – 51 с.
10. Колбанёв М. О., Татарникова Т. М. Физические ресурсы информационных процессов и технологий / Научно-технический вестник информационных технологий, механики и оптики (Scientificand Technical Journal of Information Technologies, Mechanicand Optics). – 2014. – № 6 (94). – С.113–122.
11. Коршунов И. Л. Состояние и концепция развития информационных технологий в сфере сервиса / Изв. вузов. Приборостроение. – 2014. Т. 57. № 9. – С.7–10.
12. Верзун Н. А., Колбанёв М. О., Татарникова Т. М. Технологическая платформа четвертой промышленной революции / Геополитика и безопасность. – 2016. – № 2 (34). – С.73–78.
13. Головкин Ю. Б., Гусаренко А. С. Информационная система кредитования юридических лиц в банке / Актуальные инновационные исследования: наука и практика. – 2010. № 3. – С.14–29.
14. Быстряков Д. С., Ипатов О. С., Колбанёв М. О. Система аромобезопасности. // Технологии информационно-экономической безопасности: сб. статей сотр. каф. ИС и Т. – СПб.: Изд-во СПбГЭУ, 2016. – С.31–36.
15. Головкин Ю. Б., Кромина Л. А., Ярцев Р. А. Автоматизация заказа литературы для вуза по показателям содержательной значимости изданий / Изв. вузов. Приборостроение. 2017. Т. 60, № 2. С.110–116.
16. Богатырев В. А., Богатырев С. В. Надежность мультикластерных систем с перераспределением потоков запросов / Изв. вузов. Приборостроение - 2017. - Т. 60. - № 2. - С.171–177.
17. Емельянов А. А., Коршунов И. Л. Оценка затрат на системы информационно-экономической безопасности / Технологии информационно-экономической безопасности: сб. статей сотр. каф. ИС и Т. – СПб.: Изд-во СПбГЭУ, 2016. – С.63–69.
18. Левкин И. М. Информационно-экономическая безопасность как специфический элемент экономической безопасности / Технологии информационно-экономической безопасности: сб. статей сотр. каф. ИС и Т. – СПб.: Изд-во СПбГЭУ, 2016. – С.79–89.
19. Колбанёв М. О., Коршунов И. Л., Левкин И. М. Информационно-экономические угрозы и механизмы их формирования / Геополитика и безопасность. – 2016. – № 1 (33). – С.85–89.
20. Верзун Н. А., Колбанёв М. О., Татарникова Т. М. Аспекты безопасности информационно-экономической деятельности / Технологии информационно-экономической безопасности: сб. статей сотр. каф. ИС и Т. – СПб.: Изд-во СПбГЭУ, 2016. – С.52–56.
21. Верзун Н. А., Ипатов О. С., Колбанев М. О. Интернет вещей и информационно-технологическая безопасность / Технологии информационно-экономической безопасности: сб. статей сотр. каф. ИС и Т. – СПб.: Изд-во СПбГЭУ, 2016. – С.37–43.
22. Верзун Н.А., Колбанёв М.О., Касаткин В.В. Инфокоммуникационная среда, реализующая сетецентрический подход к управлению деятельностью / Перспективные направления развития отечественных информационных технологий: материалы III межрегиональной научно-практической конференции. Севастополь 19-23 сентября 2017 г. – Севастополь: "РИБЕСТ", 2017. – С.76-78.

УДК 621.39

РАЗВИТИЕ ПРИНЦИПОВ ПОСТРОЕНИЯ СЕТЕЙ ЭЛЕКТРОСВЯЗИВерзун Наталья Аркадьевна¹, Колбанев Михаил Олегович¹, Ипатов Олег Сергеевич²¹ Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5,² Санкт-Петербургский политехнический университет Петра Великого,
Россия, Санкт-Петербург, ул. Политехническая, 29,
emails: verzun.n@unecon.ru, mokolbanev@mail.ru, ipatov_os@spbstu.ru

Аннотация: Рассматривается эволюция сетей электросвязи сквозь призму формирования и развития базовых принципов их построения, перечень которых пополняется вместе с возникновением новых концепций создания, организации и функционирования сетей связи.

Ключевые слова: *сеть электросвязи; мультисервисная сеть; сети будущего; принцип построения сети.*

DEVELOPMENT OF THE PRINCIPLES OF BUILDING TELECOMMUNICATION NETWORKSVerzun Natalya¹, Kolbanev Mikhail¹, Ipatov Oleg²¹ The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,² St. Petersburg Polytechnic University Peter the Great,
Russia, St. Petersburg, Polytechnicheskaya str. 29,
emails: verzun.n@unecon.ru, mokolbanev@mail.ru, ipatov_os@spbstu.ru

Abstract: The evolution of telecommunication networks is considered through the prism of the formation and development of the basic principles of their construction, the list of which is supplemented with the emergence of new concepts for the creation, organization and operation of communication networks.

Keywords: *telecommunication network; multiservice network; networks of the future; principle of building a network.*

Введение. В докладе рассматривается эволюция сетей электросвязи сквозь призму формирования и развития принципов построения сетей связи, перечень которых пополнялся вместе с появлением новых концепций их создания, организации и функционирования, возникших в связи с непрерывным обновлением требований к телекоммуникациям и с расширением спектра предоставляемых инфокоммуникационных услуг.

Авторы выделяют следующие базовые принципы построения сетей:

1. Принцип распространения данных, который следует из коммуникационной сущности сетей связи. Сеть должна создавать материальные объекты, способные перемещаться в пространстве и переносить информацию пользователей.

2. Принцип мультиплексирования физических цепей. Сеть должна мультиплексировать физические цепи первичной сети и формировать типовые каналы для распространения данных.

3. Принцип коммутации информационных потоков. Сеть должна использовать коммутацию для организации доступа большого количества пользователей к ограниченной группе общесетевых канальных и других ресурсов [1].

4. Принцип идентификации (или адресуемости) всех элементов сетей. Сеть должна однозначно адресовать пользователей и свои узловые, станционные и оконечные элементы. Для передачи адресной информации по сети должны быть разработаны системы сигнализации.

Вышеперечисленные четыре принципа относятся к традиционным сетям электросвязи. С учетом особенностей сетей NGN они были дополнены следующими [2]:

5. Принцип мультисервисности. Инфокоммуникационная сеть должна содержать единую мультисервисную сеть, которая обеспечивает не только мультиплексирование линий связи, но и коммутацию трафика всех пользователей и наложенных систем.

6. Принцип множественного доступа к глобальным сетям [3-5]. Инфокоммуникационная сеть должна использовать множественный доступ многих пользователей к общим ресурсам последней мили. Предложены, на основе анализа международных рекомендаций по созданию сетей будущего (Future Networks), принципы построения сетей, которые в отличие от ранее существовавших дополнительно учитывают требования современных инфокоммуникационных услуг, сложно реализуемых с использованием имеющихся сетевых технологий, а также потребности цифрового общества (цифровой экономики) [6, 7].

7. Принцип предоставления услуг. В сетях будущего ввод новых услуг не должен требовать существенных капитальных вложений и эксплуатационных затрат. Надо обеспечить возможность лавинообразного числа и объема услуг.

8. Принцип организации данных. Данными для сети будущего должна стать вся цифровая Вселенная. Доступ к ним должен быть легким, быстрым и качественным независимо от местоположения пользователя. Должна обеспечиваться персонализация всех процессов работы с данными.

9. Принцип экологичности. Сети будущего должны быть экологически безопасны для окружающей среды. Технические решения должны минимизировать влияние на экосистему, сократить потребление всех ресурсов, включая энергию [8-17].

10. Принцип социально-экономической направленности. Сети будущего должны устранить цифровое неравенство за счет снижения затрат на жизненный цикл услуг и типового широкополосного доступа, что в свою очередь послужит стимулом для развития цифровой экономики.

11. Принцип единого идентификатора пользователя услуг. Предполагается переход к единому, заново присваиваемому, идентификатору для всех пользователей, которыми в сетях нового поколения будут не только люди, но и умные вещи. Идентификатор станет единым и не будет зависеть от: местоположения пользователя, типа (вида) устройства, с которого идет обращение к инфоуслугам, используемого при этом протокола сетевого уровня.

12. Принцип виртуализации ресурсов. В сети FN должна поддерживаться виртуализация сетевых ресурсов, которая обеспечит логическое разделение между сервисами; совместное использование физической сетевой инфраструктуры многими виртуальными ресурсами, а также позволит создавать объединенные ресурсы.

Заключение. Для того чтобы сети связи нового поколения удовлетворяли требованиям цифровой экономики они должны создаваться и функционировать согласно этим принципам: традиционным и новым, возникшим с появлением концепции сетей будущего.

СПИСОК ЛИТЕРАТУРЫ

1. Кожанов Ю. Ф., Колбанёв М. О. Технология инфокоммуникации. – Курск: Науком, 2011. – 260 с.
2. Кожанов Ю. Ф., Колбанёв М. О. Интерфейсы и протоколы сетей следующего поколения теория и практика: учебное пособие. – СПб.: ГУАП, 2010. – 372 с.
3. Верзун Н. А., Колбанёв М. О., Коршунов И. Л., Микадзе С. Ю. Основы моделирования информационных систем множественного доступа : учеб. пособие. – СПб.: Изд-во СПбГЭУ. – 2015. – 138 с.
4. Верзун Н. А., Колбанёв М. О., Омелян А. В. Регулируемый множественный доступ в беспроводной сети умных вещей / Омский научный вестник. Сер. Информатика, вычислительная техника и управление. – 2016. – № 4 (148). – С. 147–151.
5. Верзун Н. А. Модель процесса передачи информации в двухуровневой ассоциации систем множественного доступа. / Региональная информатика и информационная безопасность. Сборник трудов. СПб общество информатики, вычислительной техники, систем связи и управления. 2016. СПб., С.145–149.
6. Верзун Н. А., Колбанёв М. О., Омелян А. В. Введение в инфокоммуникационные технологии и сети Future Networks: учебное пособие. – СПб.: Изд-во СПбГЭУ, 2016. – 51 с.
7. Верзун Н. А., Касаткин В. В., Колбанёв М. О. Цифровые технологии: инфокоммуникации и экономика / Сборник: Информационные технологии цифровой экономики: сб. статей. – СПб.: Изд-во СПбГЭУ, 2017. – С.29–34.
8. Росляков А. В. Оценка энергоэффективности будущих сетей / Информационные технологии и телекоммуникации. – 2015. – №3(11). – С.54–64.
9. Росляков А. В. Оценка энергопотребления будущих сетей / Электросвязь. – 2016. – №8. – С.43–50.
10. Колбанев М. О. Верзун Н. А., Омелян А. В. Об энергетической эффективности сетей пакетной передачи данных / Изв. вузов. Приборостроение. – 2014. – Т.57, № 9. – С.42–46.
11. Верзун Н. А., Колбанев А. М., Колбанев М. О. Энергетическая эффективность помехоустойчивого кодирования в беспроводных сетях интернета вещей / Изв. вузов. Приборостроение. – 2017. – Т.60, № 2. – С.143–149.
12. Верзун Н. А. Колбанев М. О., Пойманова Е. Д. Энергетические характеристики процесса долговременного хранения данных / Изв. вузов. Приборостроение. – 2017. – Т.60, № 2. – С.158–164.
13. Верзун Н. А., Колбанёв М. О., Шамин А. А. Энергетическая эффективность взаимодействия в беспроводных сенсорных сетях / Информационные технологии и телекоммуникации. 2017. Т.5. № 1. – С.88–96.
14. Верзун Н. А., Колбанёв М. О., Некоторые аспекты энергетической эффективности информационного взаимодействия / Региональная информатика и информационная безопасность. Сборник трудов. СПб общество информатики, вычислительной техники, систем связи и управления. 2015. СПб. С.327–330.
15. Воробьев А. И., Колбанев А. М., Колбанев М. О. Зеленые информационные технологии / Ученые записки Международного банковского института. Вып. 12. – СПб.: Изд-во МБИ, 2015. – С.153–165.
16. Воробьев А. И., Колбанёв А. М., Колбанёв М. О. Модель оптимизации энергопотребления умными вещами. Известия СПбГЭТУ ЛЭТИ. 2015. Т.7. – С.46–49.
17. Воробьев А. И., Колбанёв А. М., Колбанёв М. О. Экологическая безопасность информационных технологий / Геополитика и безопасность. – 2015. – № 4 (32). – С.90–99.

УДК 007

ОБОБЩЕННАЯ МОДЕЛЬ ДЕЯТЕЛЬНОСТИ В ЦИФРОВОМ ОБЩЕСТВЕ

Верзун Наталья Аркадьевна, Колбанев Михаил Олегович, Цехановский Владислав Владимирович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5,
emails: verzun.n@unecon.ru, mokolbanev@mail.ru, vccehanovsky@mail.ru

Аннотация: Предлагается обобщенная модель деятельности в условиях цифрового общества, основанная на процедурах преобразования объектов разной природы в цифровую форму (или модель) и обратно, которые стали возможны благодаря достижениям в области информационных технологий. Излагаются признаки общества, которые позволяют реализовать рассматриваемую модель на практике. Рассматриваются примеры реализации модели.

Ключевые слова: цифровое общество; обобщенная модель деятельности; цифровая модель объекта; информационные технологии; трансформация деятельности.

A GENERALIZED MODEL OF ACTIVITIES IN A DIGITAL SOCIETY

Verzun Natalya, Kolbanev Mikhail, Cehanovsky Vladislav
The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5,
emails: verzun.n@unecon.ru, mokolbanev@mail.ru, vvcehanovsky@mail.ru

Abstract: Proposed generalized model activities in a digital society, based on the procedures of transformation of objects of different nature into digital form (or model) and back, made possible by advances in information technology. Outlines the characteristics of companies that will help you implement the model in practice. This article discusses examples of the implementation of the model.

Keywords: digital society; a generalized activity model; product model; information technology; transformation activities.

Информационное общество достигло очередного этапа развития – стало цифровым, т.е. обществом в котором деятельность реализуется через цифровое представление объектов [1]. В докладе авторами предлагается обобщенная модель деятельности в условиях цифрового общества, основанная на процедурах преобразования объектов разной природы в цифровую форму (или цифровую модель) и обратно, которые стали возможны благодаря достижениям в области цифровой информационной технологии и могут использоваться и уже используются, практически, в любых областях деятельности людей [2]. Представлены примеры возможной реализации обобщенной модели деятельности на практике: аддитивное производство (additive manufacturing) [3] и цифровое (точное) земледелие (precision agriculture) [4].

В общем случае реализация обобщенной модели деятельности на практике предполагает, что общество обладает рядом признаков:

- опора на цифровые информационные технологии;
- сетевая архитектура и цифровая коммуникация [5-7];
- цифровая форма представления объектов деятельности;
- виртуализация цифровых технологий работы с объектами;
- ориентация на знания, представленные в цифровом виде;
- инновационная движущая сила развития [8];
- интеграция и глобализация за счет стандартизированной формы цифровых объектов;
- конвергенция и высокая динамика изменений;
- трансформация всех видов деятельности и др.

Результатом реализации представленной обобщенной модели деятельности на практике будет возникновение цифровой экономики, цифровой политики, цифрового образования, цифровой медицины, цифровой культуры и спорта, цифрового государства, цифрового сельского хозяйства, цифрового транспорта, цифровой безопасности, цифровой энергетики, цифровой экологии и т.д.

СПИСОК ЛИТЕРАТУРЫ

1. Советов Б. Я., Колбанёв М. О., Татарникова Т. М. Информационное общество: современные состояние, проблемы, технологии и перспективы. // Инновации в информационно-аналитических системах. – 2015, – Выпуск 11. – URL: <http://iias.ru/index.php/sborniki/vypusk-11>.
2. Колбанев М. О., Коршунов И. Л., Левкин И. М. Проблемы информационно-технологической деятельности / Изв. вузов. Приборостроение. – 2017. – Т.60, № 2. – С.105–109.
3. Гибсон Я., Розен Д., Стакер Б. Технологии аддитивного производства. Трёхмерная печать, быстрое прототипирование и прямое цифровое производство. М.: Техносфера, 2016. – 656 с.
4. Шаяхметов М. Р., Дубровин И. А. Точное земледелие (precision agriculture) – путь к ресурсосбережению // ОНВ. 2013. №1 (118). URL: <http://cyberleninka.ru/article/n/tochnoe-zemledelie-precision-agriculture-put-k-resursosberezheniyu>.
5. Верзун Н. А., Касаткин В. В., Колбанёв М. О. Цифровые технологии: инфокоммуникации и экономика // Сборник: Информационные технологии цифровой экономики: сб. статей. – СПб.: Изд-во СПбГЭУ, 2017. С.29–34.
6. Верзун Н. А., Колбанев М. О., Татарникова Т. М. Технологическая платформа четвертой промышленной революции / Геополитика и безопасность. – 2016. – № 2 (34). – С.73–78.
7. Юдина Т. Н. Осмысление цифровой экономики. Теоретическая экономика, №3, 2016. – С.12–16.
8. Левкин И. М., Ковалев А. П., Морозова Е. Ю. Пути совершенствования информационного обеспечения инновационной деятельности предприятия / Управленческое консультирование 2016, № 5. С.112–120.

УДК 681.518

ОСОБЕННОСТИ ПЕРЕДАЧИ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ В МОДУЛЬНОЙ УЧЕБНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ

Журавлев Антон Евгеньевич
ГУМРФ имени адмирала С.О. Макарова
Россия, Санкт-Петербург, ул. Двинская, 5/7,
email: zhuravlevae@gumrf.ru

Аннотация: В статье рассмотрены основные аспекты обмена персональной информацией между модулями учебной информационной системы образовательной организации. Отмечены основные модели организационной структуры такого программно-аппаратного комплекса и приведены

его основные особенности внедрения в действующее информационное поле академических подразделений без отрыва от учебного процесса.

Ключевые слова: учебная система, модульная архитектура, дистанционное обучение, передача данных.

PERSONAL INFORMATION TRANSMISSION SPECIFIC IN THE MODULAR E-LEARNING INFORMATION SYSTEM

Zhuravlev Anton

Admiral Makarov SUMIS

Russia, St. Petersburg, Dvinskaya str. 5/7,

email: zhuravlevae@gumrf.ru

Abstract: The article presents main aspects of the of personal information transmission in the educational organization e-learning information system units. Notes the organizational structure basic model its information system and given introduction in the current information field of academic units without departing from the educational process main features.

Keywords: training system; modular architecture, e-learning, data transmission.

Эффективность образовательного процесса легко оценить в рамках имеющихся коэффициентов и рейтингов. Однако, чтобы оценить эффективность использования имеющихся в распоряжении учебной организации ресурсов, особенно человеческих, необходимо вводить во многом индивидуальные системы аттестации и оценки. Следует понимать, что данный показатель с одной стороны напрямую влияет на итоговую оценку эффективности работы образовательной организации, а с другой стороны во многом зависит от человеческого фактора, а данная зависимость крайне сложно формализуема. Для повышения эффективности использования кадрового состава и прочих (технических, экономических) ресурсов предлагается рассматривать учебный курс как модульный бизнес-процесс, представляющий собой минимальную операционную единицу учебного процесса. В таком случае становится возможным бремя выработки и принятия наиболее эффективного и оптимального управленческого решения переложить на соответствующий модуль автоматизированной информационно-справочной системы (АИСС) обслуживающей рассматриваемую образовательную организацию.

Процесс формирования обратной связи в информационной системе (ИС) в виде некоего воздействия не является действием, реализующим процедуру процесса перехода управляемого объекта из одного состояния в другое, где ее использование и заканчивается. Механизм принятия решений на основе модульных бизнес-процессов является субъектом управления логикой взаимодействия различных бизнес-структур, потому для повышения эффективности его использования необходимо, чтобы автоматизированная система сочетала в себе не только механизм выработки непосредственного оптимального решения, но и функционал для поддержания некоего достаточного уровня его оптимальности в случае определения массива источника данных как переменного, который на момент воздействия на систему считался константой. Кроме этого, оптимизация управления системного такого уровня сложности представляется невозможным без оперирования эмпирическими данными, полученными в результате накопления некоторой статистической информации о внутренних системных процессах. Таким образом, задача выработки и принятия оптимального решения является лишь частью комплексной системы управления образовательной организацией в целом и учебного процесса в частности.

Многофакторность задачи, мультимодальность объекта автоматизации, сложная формализуемость операционных единиц обуславливают необходимость проведения достаточно глубокого, комплексного исследования вопроса и накладывают на исследуемую математическую модель множество ограничений и высокий уровень вхождения. Перечисленные особенности, особенно в случае необходимости сохранения математической модели на прежнем уровне сложности (в рамках текущего порядка) неизбежно влекут повышение ресурсоемкости процесса. Исходя из этого факта, задача дополнительно расширяется по критерию эффективности использования ресурсов.

В АИСС используется программный коммутатор с функцией шлюза, реализованный на базе интегратора, потому весь его обменный функционал можно рассматривать как модель локальной вычислительной сети и межсетевого взаимодействия. Клиентскими узлами в данной модели выступают объекты работы интегратора, т.е. компоненты, подлежащие организации взаимодействия. Роль сервера и контроллера берет на себя образующая АИСС «ВУЗ». Таким узлом является и рассматриваемая подсистема.

Функционал шлюза в рассматриваемой модели реализован комплексом генетических алгоритмов, реализующих постулаты теории приближений относительно потоков и каналов передачи данных как объектов мутаций отбора. Коммутатор интегратора реализует систему распределенного хранения и передачи данных путем инициализации авторизованных туннелей класса «коммутатор-узел». В том числе за счет этого, данная сетевая модель во многом наследует идеи семантической

модели данных «сущность-связь», не только хранящей объекты данных, но и раскрывающей их смысловое обеспечение и взаимосвязь друг с другом.

Развитие топологии данной сетевой модели во времени напрямую зависит от этапа внедрения интегратора в действующее информационное поле. Так, на раннем этапе, когда при сохранении существующих прямых связей между различными ИС вида «система-система» и «система-поле» выстраиваются новые связи вида «интегратор-система» и «интегратор-поле» топология является полностью наследуемой, сохраняя все ее основные особенности, достоинства и недостатки.

На промежуточном этапе, при частичном сохранении связей «система-система» разрушается большинство связей типа «система-поле», функционал которых полностью заменяется совокупностью связей «интегратор-система» и «интегратор-поле», топология становится сетевой и по структуре напоминает граф, вершиной которого является интерфейс ввода-вывода АИСС.

На заключительном этапе внедрения полностью разрушаются остаточные связи типов «система-система» и «система-поле», тем самым исключая прямое взаимодействие между различными ИС информационного поля. Топология модели взаимодействия программных компонентов трансформируется в полноценную звезду, в центре которой находится интегратор, лучами являются связи типов «интегратор-система» и «интегратор-поле», а вершинами становятся ИС программного комплекса.

Одним из основных критериев оценки эффективности функционирования АИСС такого класса является показатель (коэффициент) масштабируемости модели и системы в зависимости от числа клиентских модулей ИС и задействованных систем обеспечения безопасности. В соответствии с проведенными исследованиями при пиковых нагрузках актуальная топология АИСС по данному показателю демонстрирует рост в 17-21% по отношению к ее предыдущей версии, что в перспективе обеспечит значительно большую эффективность внедрения новых и модернизацию существующих компонентов без снижения уровня защищенности персональной информации.

Автоматизация процесса аттестации знаний повышает общую эффективность процесса обучения. Из процесса проверки знаний и навыков полностью или частично исключается субъективность аттестующего, что обеспечивает скорость, точность и непредвзятость результатов. Гибкость настройки АИСС гарантирует простую и быструю адаптацию задействованных в процессе аттестации сотрудников к инновационным механизмам оценки способностей контингента обучающихся. Объединение подсистем инфополя в единый информационный организм предоставляет беспрецедентные возможности по сверхоперативному мониторингу, контролю и управлению ресурсами учебной организации, а также становится наиболее эффективным средством антикризисного управления.

Говоря о рассматриваемой ИС в целом, с точки зрения комплексной АИСС информационной экосистемы образовательной организации следует признать не только ее актуальность, но и истинную незаменимость. Так, например, она позволяет реализовать адекватную реальным условиям систему поощрений сотрудников и слушателей, не прибегая к каким-либо существенным материальным затратам. Реальная же ценность ИС выражается в возросшем на два порядка количестве активных пользователей обучающей электронной ИС в течение одного учебного года. В перспективе, демонстрируемый рост показателей успешности образовательной организации самым благоприятным образом скажется на всей сфере ее деятельности.

СПИСОК ЛИТЕРАТУРЫ

1. Журавлев А.Е. Разработка и внедрение интегрируемой программно-аппаратной системы тренинга и аттестации на примере транспортного ВУЗа / Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. — СПб.: ГУМРФ имени адмирала С. О. Макарова, 2016. — Вып. 6 (40). — 260 с. Стр. 242-251.
2. Журавлев А.Е. Внедрение тестовой системы на базе решения «1С:Экзаменатор» и ее адаптация к актуальным ФГОС / Новые информационные технологии в образовании: Сборник научных трудов 17-й международной научно-практической конференции "Новые информационные технологии в образовании" (Инновации в экономике и образовании на базе технологических решений "1С") 31 января—1 февраля 2017 г. /Под общ. ред. проф. Д.В. Чистова. Часть 2.— М.: ООО "1С-Публишинг", 2017. 389 с.: илл. Стр. 75-78

УДК 347.775

ФОРМИРОВАНИЕ И ИСПОЛЬЗОВАНИЕ В УЧЕБНОМ ПРОЦЕССЕ СИТУАЦИОННОГО ЦЕНТРА ДЕЛОВОЙ РАЗВЕДКИ

Левкин Игорь Михайлович, Микадзе Сергей Юрьевич
Санкт-Петербургский государственный экономический университет
Россия, Санкт-Петербург, улица Садовая, 21,
email: lev.kin@yandex.ru, mik@finec.ru

Аннотация: В статье рассмотрены особенности построения и использования учебных ситуационных центров при подготовке бакалавров в сфере деловой разведки. Приведены примеры учебных задач, которые могут решаться в индивидуальном порядке и в составе рабочих подгрупп.

Ключевые слова: учебный ситуационный центр, деловая разведка, основные виды занятий.

FORMATION AND USE IN THE EDUCATIONAL PROCESS OF THE SITUATIONAL CENTER FOR BUSINESS INTELLIGENCE

Levkin Igor, Mikadze Sergey

Saint-Petersburg state economic University

Russia, Saint-Petersburg, Sadovaya street, the house 21,

email: lev.kin@yandex.ru, mik@finec.ru

Abstract: the article considers the features of the construction and use of training centers in the preparation of bachelors in the field of business intelligence. Examples of learning tasks that can be addressed individually and in the composition of the working groups.

Keywords: *educational situation centre, business intelligence, principal occupations.*

Введение. Подготовка бакалавров по направлениям Информационные технологии в деловой разведке и Деловая аналитика предполагает формирование, в частности, таких компетенций как умение: пользоваться научными методами выявления и систематизации данных об окружающем мире; пользоваться необходимыми методами добытия (сбора), обработки, анализа и синтеза информации для оценки конкурентной, экономической, финансовой и других видов обстановки; применять автоматизированные системы сбора, систематизации и научной интерпретации экономической и других видов информации; осуществлять оптимальный выбор пакетов прикладных программ математической обработки, анализа и синтеза результатов профессиональных исследований; разрабатывать математические модели функционирования экономических систем с использованием инструментов и методов системного анализа для управления бизнесом; и другие.

Формирование этих компетенций невозможно без решения практических задач в сфере цифровой экономики [1]. При этом многие из этих задач предполагают последовательное решение некоторого связанного множества частных задач, выполняемых индивидуально, а также задач, выполняемых в составе групп из 3 – 4-х студентов и более с использованием информационных систем коллективного пользования. К числу таких задач можно отнести задачи: оценки и прогнозирования конкурентной, экономической, транспортной, социально-психологической и других видов обстановки; моделирование экономических, информационных и других угроз, прогнозирование их формирования, развития и степени опасности в различных условиях обстановки; оценки сильных и слабых сторон конкурентов и выпускаемой ими продукции; выявления конкурентоспособности хозяйствующего субъекта; разработки предложений по совершенствованию бизнес-процессов в информационной сфере; разработка фрагментов информационной системы умного города; разработка фрагментов системы управления большими данными, промышленного интернета (интернета вещей), технологии виртуальной и дополненной реальностей и другие.

Эффективное решение этих задач невозможно без создания и внедрения в учебный процесс учебных ситуационных центров (УСЦ), которые не только помогают принимать управленческие решения, но и служат средством обучения специалистов [2,3]. По опыту эксплуатации УСЦ при обучении в их среде знания формируются «эволюционно» на основании экспериментов с соответствующими моделями. Правила работы, критерии и методы оценки обучающихся могут значительно изменяться, что не позволяет использовать традиционный подход к обучению. Таким образом, само функционирование УСЦ предопределяет переход в учебном процессе к инновационным, субъектно- и деятельностно-ориентированным методам обучения (эволюционному обучению, рефлексивно-гуманистической психологии, педагогике сотворчества, проективной педагогике и др.). Самостоятельной проблемой становится разработка методики оценки деятельности учащегося в коллективе (в рамках учебного процесса в среде УСЦ) при отсутствии четко сформулированной цели.

К основным видам занятий, которые целесообразно проводить в УСЦ можно отнести: лекции демонстрации, лекции дискуссии, практические занятия по разработке технических и программных средств, семинар, решение многоэтапных и групповых бизнес-кейсов, деловая игра. Кроме того, на территории УСЦ могут проходить защиты курсовых и выпускных квалификационных работ.

Важной функцией УСЦ должна также стать возможность проведения научных исследований в рамках студенческого научного общества (так, например, в состав центра предлагается включить лабораторию интернет вещей), а также осуществление научно-практической деятельности в рамках хозяйственной деятельности с научными, промышленными и бизнес структурами.

УСЦ деловой разведки может быть построен как совокупность программно-технических средств, научно-математических методов и инженерных решений для автоматизации процессов отображения, моделирования, анализа ситуаций и управления. Он должен позволять автоматизировать обработку самой ситуации, а не только исходных данных, необходимых для ее последующего выявления и анализа субъектом. При этом в таком УСЦ должна быть обеспечена возможность решения двух групп практических задач: задачи программно-технического обеспечения (доработка используемой техники и программных продуктов, разработка фрагментов и макетов информационных систем и технологий цифровой экономики); задачи анализа ситуаций и принятия управленческие решения.

Решение задач обеих групп может осуществляться в двух режимах – индивидуальном и коллективном. В первом случае каждый студент может работать только в своей фиксированной области и не согласовывает свою деятельность с другими членами группы. Во втором случае студенты могут работать над решением общей проблемы и должны учитывать возможные влияния своих решений на деятельность коллег.

Программно-техническое обеспечение УСЦ должно обеспечивать: доступ к информационному пространству, возможность формирования и предоставления пользователям обобщенной информации, возможность анализа агрегированных данных; возможность использования средств прогнозирования, выявления тенденций исследуемого явления или процесса; ситуационное (динамическое) моделирование как возможность получить ответ на вопрос «что будет, если», позволяющее вносить возмущения и определять возможные последствия, связанные с наступлением того или иного события; формирование рекомендаций по выбору одного из многих вариантов решения; возможность проведения оценки рисков при расчете шансов реализации прогноза; возможность разработки и совершенствования программно-технических решений.

В вопросах деловой разведки УСЦ должен обеспечить следующие возможности [4]: демонстрацию основных видов, форм и способов конкурентной борьбы; юридическое сопровождение деловой разведки; моделирование технологических процессов добытия и обработки информации в деловой разведке; моделирование информационных систем, решающих задачи деловой разведки; оценивать свойства информационных источников в документной, электронной, предметно-вещевой и одушевленной средах и определять пространственно-временные характеристики фрагментов информационного пространства с целью ориентирования на них средств добытия информации при решении конкретных информационных задач; разрабатывать априорные словари информационных признаков обстановок и ситуаций, деятельности хозяйствующих субъектов; строить информационно-признаковые модели угроз различной природы; отрабатывать методы автоматизированного и автоматического добытия информации в сети Internet; разрабатывать базы данных по всей совокупности задач деловой разведки; использовать современные методы автоматизированной обработки информации, в том числе основанные на методах искусственного интеллекта (например, методы автоматического перевода с различных языков); использовать методы автоматизированной разработки отчетно-информационных документов; разрабатывать модели и методики решения основных задач деловой разведки (моделирование и методика вскрытия конкурентных угроз; изучение конкурентной обстановки и бизнес-процессов; анализ конкурента; определение конкурентоспособности, сильных и слабых сторон создаваемых продуктов; исследование конкурентоспособности фирмы; разведка намерений конкурента; оценка лояльности персонала внутри хозяйствующего субъекта и динамики ее изменения, выявление центров напряженности; вскрытие фальсифицированных данных, поступающих в высшие эшелоны управления компании от собственных сотрудников и исключение дезинформации высшего руководства и другие); оценивать эффективность деловой разведки.

Закключение. Внедрение УСЦ в учебный процесс позволит существенно повысить его эффективность как на уровне бакалавриата, так и на более высоких уровнях образовательных траекторий.

СПИСОК ЛИТЕРАТУРЫ

1. Государственная программа «Информационное общество» (2011–2020 годы) // Распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р [Электронный ресурс]. - Режим доступа: <http://minsvyaz.ru/ru/activity/programs/1/> (дата обращения 26.08.2017).
2. Ситуационные центры в образовании [Электронный ресурс]. - Режим доступа: http://it-claim.ru/Library/Articles/publications_Philippovich_Andrew/sit_centres_education/sit_centres_in_education.htm (дата обращения 26.08.2017).
3. В МГИМО построена система учебных ситуационных центров [Электронный ресурс]. - Режим доступа: http://www.cnews.ru/news/line/v_mgimo_postroena_sistema_uchebnyh (дата обращения 26.08.2017).
4. Левкин И.М., Микадзе С.Ю. Добывание и обработка информации в деловой разведке. – СПб.: НИУ ИТМО, 2015.

УДК 378

К ВОПРОСУ ПОДГОТОВКИ РАЗРАБОТЧИКОВ ПЕРСПЕКТИВНОГО ОТЕЧЕСТВЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Первухина Елена Львовна, Шалимова Елена Михайловна
Севастопольский государственный университет,
Россия, Севастополь, ул. Университетская, д. 33,
emails: pervukhina14@mail.ru, elesh@mail.ru

Аннотация: Анализируется роль образовательных стандартов в подготовке ИТ-специалистов, разрабатывается методология совершенствования образовательных программ.

Ключевые слова: образовательный стандарт; компетенция; специалист; дисциплина.

TO THE QUESTION OF Training OF DEVELOPERS for THE Advanced National SOFTWARE

Pervukhia Elena, Shalimova Elena

Sevastopol State University

Russia, Sevastopol, Universitetskaya Str. 33,

emails: pervukhina14@mail.ru, elesh@mail.ru

Abstract: The role of educational standards in the training of IT professionals is analyzed. The methodology to improve the curriculum is developed.

Keywords: *educational standard; competence; specialist; study discipline.*

Государственная политика обеспечения информационной безопасности РФ предполагает создание отечественных цифровых, интеллектуальных производственных технологий. Для этого требуется большое количество высококвалифицированных ИТ-кадров, владеющих не только современными программными средствами, но и методами системного анализа и компьютерного моделирования сложных объектов реального мира различной физической природы. Еще одной отличительной особенностью требуемых ИТ-кадров является их готовность предвидеть будущие задачи экономики нового технологического уклада, повышать уровень своей квалификации на основе фундаментальных знаний и быть готовыми к работе в составе большой междисциплинарной (часто, международной) команды специалистов.

Современные федеральные образовательные стандарты третьего поколения предусматривают профессиональные компетенции, соответствующие указанным требованиям, и предоставляют вузам больше самостоятельности в разработке учебных планов. В результате этого некоторые вузы снижают количество аудиторных часов, отводимых на дисциплины математического и естественнонаучного циклов, увеличивая при этом объем часов самостоятельной работы.

Это не позволяет будущим специалистам изучать реальные процессы на системном уровне, ограничивает в дальнейшем их возможности создания креативных междисциплинарных сред и платформ. В результате, даже самым успешным выпускникам может потребоваться значительное время на адаптацию к условиям работодателей. Конечно, самостоятельная работа студентов является неотъемлемой частью учебного процесса, однако это только дополнение к образовательному процессу, которое не может заменить полноценной аудиторной работы студентов под руководством преподавателя.

Выходом из ситуации должны быть сбалансированные учебные планы, способствующие формированию у будущих ИТ-специалистов системного алгоритмического мышления, что предполагает возвращение к традиционным методам преподавания математики, безусловно учитывая развитие математического образования и новые математические теории (хаоса, теория катастроф, фракталов и т.п.)

Целью работы является создание методологии совершенствования образовательных программ подготовки ИТ-специалистов, ориентированных на развитие у обучаемых общих и профессиональных компетенций в решении междисциплинарных задач.

СПИСОК ЛИТЕРАТУРЫ

1. Б.Я. Советов, В.В. Цехановский. Информационные технологии: теоретические основы. Учебное пособие. СПб: Лань, 2017 г. 444 с.

УДК 002(094)

К ВОПРОСУ ПОДГОТОВКИ КАДРОВ ДЛЯ ЦИФРОВОЙ ЭКОНОМИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Резунков Димитрий Андреевич¹, Иманов Гейдар Мамедович², Резункова Ольга Петровна²

¹Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Россия, Санкт-Петербург, ул. Большая Морская, 67,

²Смольный институт РАО,

Россия, Санкт-Петербург, Полюстровский пр., 59

emails: mityarezu@gmail.com, ararog@mail.ru

Аннотация: Распоряжением правительства РФ от 28 июля 2017 года №1632-р утверждена программа «Цифровая экономика Российской Федерации». Программой определены цели, задачи, направления и сроки реализации основных мер государственной политики по созданию необходимых условий для развития в России цифровой экономики, в которой данные в цифровом виде являются ключевым фактором производства во всех сферах социально-экономической деятельности, что является необходимым условием повышения конкурентоспособности страны, качества жизни граждан, обеспечения экономического роста и национального суверенитета. Для управления программой определены пять базовых направлений развития цифровой экономики в России на период до 2024 года, это: нормативное регулирование, кадры и образование, формирование исследовательских

компетенций и технических заделов, информационная инфраструктура и информационная безопасность.

Ключевые слова: программа «Цифровая экономика Российской Федерации», цифровые технологии в образовательном процессе, модель образовательного процесса с учетом требований цифровой экономики.

TO THE QUESTION OF TRAINING FOR THE DIGITAL ECONOMY OF THE RUSSIAN FEDERATION

Rezunkov Dimitry¹, Imanov Geidar², Rezunkova Olga²

¹Saint Petersburg State University of Aerospace Instrumentation,
Russia, St. Petersburg, Bolshaya Morskaya Str., 67,
Smolny Institute of the Russian Academy of Education,
Russia, St. Petersburg, Polyustrovsky prospect, 59
emails: mityarezu@gmail.com, ararog@mail.ru;

Abstract: By the order of the government of the Russian Federation from July 28, 2017 №1632-r the program "Digital economy of the Russian Federation" was approved. The program defines the goals, objectives, directions and timeframes for the implementation of the main measures of state policy to create the necessary conditions for the development of the digital economy in Russia, in which the data in digital form is a key factor in production in all spheres of social and economic activity, which is a prerequisite for improving the country's competitiveness, the quality of life of citizens, ensuring economic growth and national sovereignty. Five basic directions of development of the digital economy in Russia for the period up to 2024 are defined for the program management: normative regulation, personnel and education, development of research competences and technical facilities, information infrastructure and information security.

Keywords: the program "Digital Economy of the Russian Federation", digital technologies in the educational process, the model of the educational process taking into account the requirements of the digital economy.

В 1995-ом году американский информатик Николас Негропonte (Массачусетский университет) ввел в употребление термин "цифровая экономика". Сейчас этим термином пользуются во всем мире, он вошел в обиход политиков, предпринимателей, журналистов. В прошлом году один из главных докладов Всемирного банка содержал отчет о состоянии цифровой экономики в мире (доклад вышел под названием "Цифровые дивиденды"). Красной нитью через этот доклад проходят три мысли. 1) широкое распространение Интернета, мобильной связи и информационно-компьютерных технологий (ИКТ) становится основой для создания цифровой экономики. 2) цифровая экономика многих стран мира находится в стадии бурного развития. 3) цифровая экономика приведёт к радикальному преобразованию мира со знаком «плюс».

За период 2005-2015 гг. количество пользователей Интернета выросло более чем втрое: с 1 миллиарда до 3,2 миллиарда. Авторы доклада ВБ называют данное явление «цифровой революцией». Авторы доклада настаивают, что польза от «цифровой революции» станет ещё ощутимее («цифровые дивиденды» - ещё больше), если распространение ИКТ будет стимулироваться и направляться государствами. Охват должен быть 100-процентным. Никаких «теневых зон» на планете остаться не должно! Реальные «цифровые дивиденды» появятся также при условии, что ИКТ будут более широко использоваться не только на бытовом уровне (связь, общение между людьми), но и в экономике. Человечество должно перейти от традиционной экономики к «цифровой экономике».

Однако до сих пор содержание этого понятия остается размытым, четкого определения нет. К термину "цифровая экономика" существует два подхода: первый подход "классический": цифровая экономика — это экономика, основанная на цифровых технологиях и при этом правильное характеризовать исключительно область электронных товаров и услуг (телемедицина, дистанционное обучение, продажа медиконтента и пр.), второй подход — расширенный: "цифровая экономика" — это экономическое производство с использованием цифровых технологий (Р. Мещеряков). Есть и другое определение «Цифровая экономика — это экономика, основанная на новых методах генерирования, обработки, хранения, передачи данных, а также цифровых компьютерных технологиях», А. Энговатова. "В рамках данной экономической модели, — подчеркивает А. Энговатова, — кардинальную трансформацию претерпевают существующие рыночные бизнес-модели, модель формирования добавочной стоимости существенно меняется, значение посредников всех уровней в экономике резко сокращается. Кроме того, увеличивается значение индивидуального подхода к формированию продукта, — ведь теперь мы можем смоделировать все, что угодно" Обобщая, можно сказать, что цифровой экономикой можно охватить все то, что поддается формализации, то есть, превращению в логические схемы.

По словам главы государства, проект развития цифровой экономики в России стоит в одном ряду с такими масштабными преобразованиями, как массовое железнодорожное строительство в XIX веке и электрификация страны в первой половине XX столетия. Путин считает, что развитие цифровой экономики - беспрецедентный по своему масштабу, значению и влиянию на жизнь страны и каждого

конкретного человека проект, который предстоит реализовать, "опираясь на накопленный технологический, интеллектуальный потенциал". Владимир Путин призвал задействовать все имеющиеся у России ресурсы для того, чтобы совершить рывок в развитии цифровой экономики. Глава государства уверен, что Россия ни в коем случае не должна отстать в мировой гонке новых технологий.

Поэтому распоряжением правительства РФ от 28 июля 2017 года №1632-р утверждена программа «Цифровая экономика Российской Федерации». Программа подготовлена Минкомсвязью России во исполнение перечня поручений Президента России по реализации Послания Федеральному Собранию (№Пр-2346 от 5 декабря 2016 года). Президент России 19 июля поручил включить программу «Цифровая экономика» в перечень основных направлений стратегического развития РФ до 2018 года и на период до 2025 года. Решение принято на заседании совета по стратегическому развитию и приоритетным проектам.

Согласно описанию программы, ее суть — создание «правовых, технических, организационных и финансовых условий для развития цифровой экономики» в России и интеграции ее с цифровыми экономиками членов Евразийского экономического союза.

Программа должна создать основу для развития в России цифровой экономики. Документ состоит из восьми направлений, которые делятся на три раздела: "Среда", "Платформы и технологии" и "Рынки и отрасли экономики". Главный фокус программы направлен на два базовых раздела. Первый включает в себя нормативное регулирование, инфраструктуру, кадры и информационную безопасность. Второй будет играть роль "цифрового фундамента" и станет точкой опоры для дальнейших процессов цифровой трансформации.

В документе уделяется много внимания российскому компьютерному, серверному и телекоммуникационному оборудованию и программному обеспечению. Согласно программе, к концу срока ее реализации доля иностранного софта и оборудования, закупаемого госорганами, должна снизиться до 10% и 50% соответственно. Кроме того, составители программы предлагают устанавливать российские антивирусные программы на все компьютеры, ввозимые в Россию.

По словам Владимира Путина, Россия находится среди ведущих стран мира по динамике распространения широкополосного интернета и беспроводных сетей. С 2010 по 2016 гг. доля домашних хозяйств, имеющих доступ к интернету, выросла до 74,8%, а средняя скорость интернета в России за прошлый год выросла на 29%, что соответствует уровню Франции и Италии. "Наша столица Москва входит в число мировых лидеров по применению цифровых технологий в современной городской инфраструктуре, опережая такие мегаполисы как Торонто, Токио, Гонконг, Барселона и Сидней", - отметил глава государства. Президент констатировал, что по отдельным индексам Москва входит в тройку лидеров, а, например, по уровню использования цифровых сервисов при взаимодействии государства с гражданами - на первом месте в мире. "К началу 2017 г. российский рынок коммерческих центров хранения и обработки данных вырос до 14,5 млрд рублей", - сообщил президент. Благодаря высокому уровню компетенций российских IT-специалистов компании РФ предлагают уникальные программные решения, которые используются в том числе и при создании "умных городов".

Кроме того, как отмечается в проекте программы, Россия должна укрепить свое положение на мировом рынке услуг по обработке и хранению данных. Сейчас ее доля в мировом объеме оказания таких услуг составляет менее 1%, а согласно программе, к 2024 году этот показатель должен вырасти до 10%. Также к этому времени 97% российских домохозяйств должны будут иметь широкополосный доступ в интернет со скоростью не менее 100 МБит/с, а все города-миллионники должны будут обзавестись устойчивым покрытием 5G.

Программа «Цифровая экономика», по информации РБК, предполагает и появление в России к 2024 году минимум десяти высокотехнологичных предприятий в сфере высоких технологий. Вузы при этом должны будут выпускать по 120 тыс. специалистов в сфере IT в год. Кроме того, должны быть реализованы не менее 30 исследовательских проектов в области цифровой экономики с объемом бюджета не менее 100 млн руб.

Федеральные и региональные органы власти в 2017 г. потратят на информационные технологии около 200 млрд руб., сообщил Владимир Путин. В конце июня помощник российского президента по экономическим вопросам Андрей Белоусов рассказал, что правительство рассматривает возможность создания в России фонда цифровой экономики объемом 100 млрд руб.

Программой определены цели, задачи, направления и сроки реализации основных мер государственной политики по созданию необходимых условий для развития в России цифровой экономики, в которой данные в цифровом виде являются ключевым фактором производства во всех сферах социально-экономической деятельности, что является необходимым условием повышения конкурентоспособности страны, качества жизни граждан, обеспечения экономического роста и национального суверенитета.

Для управления программой определены пять базовых направлений развития цифровой экономики в России на период до 2024 года. К базовым направлениям отнесены нормативное регулирование, кадры и образование, формирование исследовательских компетенций и технических заделов, информационная инфраструктура и информационная безопасность.

Функции проектного офиса по реализации программы "Цифровая экономика Российской Федерации" осуществляет автономная некоммерческая организация "Аналитический центр при Правительстве Российской Федерации"; функции федерального органа исполнительной власти, ответственного за реализацию направлений "Нормативное регулирование" и "Кадры и образование" Программы, осуществляет Министерство экономического развития Российской Федерации; функции федерального органа исполнительной власти, ответственного за реализацию направлений "Формирование исследовательских компетенций и технологических заделов", "Информационная инфраструктура" и "Информационная безопасность" Программы, осуществляет Министерство связи и массовых коммуникаций Российской Федерации.

В систему управления реализацией программы "Цифровая экономика Российской Федерации", утвержденной распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р, входят: а) Правительственная комиссия по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности; б) подкомиссия по цифровой экономике Комиссии; в) автономная некоммерческая организация "Аналитический центр при Правительстве Российской Федерации"; г) автономная некоммерческая организация "Цифровая экономика", учреждаемая ведущими организациями в сфере цифровой экономики; д) центры компетенций по направлениям Программы, определяемые автономной некоммерческой организацией "Цифровая экономика"; е) рабочие группы по направлениям Программы, формируемые автономной некоммерческой организацией "Цифровая экономика" из представителей заинтересованных федеральных органов исполнительной власти, центров компетенций, проектного офиса и иных организаций; ж) федеральные органы исполнительной власти, ответственные за реализацию направлений Программы; з) заинтересованные органы государственной власти, органы государственной власти субъектов Российской Федерации и организации.

Автономная некоммерческая организация "Цифровая экономика": а) формирует рабочие группы, а также организует и координирует их деятельность; б) определяет центры компетенции, а также координирует их деятельность (в том числе при подготовке проектов планов мероприятий в целях исключения дублирования и противоречий, которые могут иметь место в проектах планов мероприятий); в) проводит оценку эффективности реализации Программы (в том числе подготавливает сводный ежегодный доклад об эффективности реализации Программы, а также определяет порядок подготовки такого доклада); г) подготавливает предложения по внесению изменений в функциональную структуру; д) осуществляет мониторинг информационных ресурсов органов государственной власти Российской Федерации, органов Евразийского экономического союза, на которых для общественного (публичного) обсуждения размещаются проекты нормативных правовых актов, в целях определения таких нормативных правовых актов, принятие (издание) которых может оказать влияние на выполнение планов мероприятий, и направляет результаты мониторинга в подкомиссию; е) взаимодействует с бизнес-, научно-образовательными и иными сообществами и выявляет их потребности в области цифровой экономики; ж) осуществляет мониторинг развития цифровой экономики и цифровых технологий, формирует форсайты и прогнозы развития цифровой экономики и цифровых технологий, а также подготавливает предложения по основным направлениям развития цифровой экономики; з) осуществляет поддержку "стартапов" и субъектов малого и среднего предпринимательства в области разработки и внедрения цифровых технологий путем их информационной акселерации (популяризации, обучения новым бизнес-моделям, навигации в системе управления, координации с другими участниками и ряд других мер) и инвестиционной акселерации.

28 августа 2017 г. №1030 утверждены постановлением Правительства Российской Федерации правила разработки, мониторинга и контроля выполнения планов мероприятий по реализации программы "Цифровая экономика Российской Федерации".

Настоящие Правила устанавливают порядок разработки, мониторинга и контроля выполнения планов мероприятий по реализации программы "Цифровая экономика Российской Федерации", утвержденной распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р. Планы мероприятий формируются на основе принципов проектного управления с учетом требований методических указаний, утвержденных решением подкомиссии по цифровой экономике Правительственной комиссии по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности. Информационное взаимодействие в ходе разработки, мониторинга и контроля выполнения планов мероприятий, включая официальное направление соответствующих документов, осуществляется путем их размещения в единой информационной системе электронного взаимодействия участников реализации Программы. Проект плана мероприятий подготавливается с соответствующей пояснительной запиской и финансово-экономическим обоснованием. В состав мероприятий в том числе могут быть включены разработка проектов правовых актов и иных документов, проведение исследований и разработок, реализация инвестиционных и технологических проектов, организация и проведение конференций, создание организаций и осуществление их реорганизации, оценка удовлетворенности качеством услуг, разработка образовательных программ, проведение учебных курсов и другие мероприятия.

В связи с задачами Программы руководство Смольного института РАО поставило перед собой цель по расширению применения цифровых технологий в образовательном процессе. На «Экономическом» и факультете «Информационные технологии» нормативно, технологически и содержательно обеспечен курс информатики и информационно-коммуникационных технологий в программах общего образования. Однако численность подготовки кадров и соответствие образовательных программ нуждам цифровой экономики недостаточны. В процедурах итоговой аттестации недостаточно применяются цифровые инструменты учебной деятельности, процесс не включен целостно в цифровую информационную среду. Поэтому руководство Смольного института РАО поставило перед собой задачу по созданию ключевых условий для подготовки кадров цифровой экономики; совершенствованию системы образования, которая должна обеспечивать цифровую экономику компетентными кадрами; мониторингирование рынка труда, который должен опираться на требования цифровой экономики и создание системы мотивации по освоению необходимых компетенций и участию кадров в развитии цифровой экономики России.

С учетом требований к компетенциям цифровой экономики в Смольном институте РАО будут обновлены образовательные программы в целях использования в учебной деятельности, в том числе при государственной итоговой аттестации, общепользовательских и профессиональных цифровых инструментов. Образовательные программы профессионального образования в области цифровой экономики предусматривают изучение отечественных и зарубежных разработок.

Будет разработана или выбрана информационная система поддержки индивидуального профиля компетенций обучающегося, для каждого обучающегося будет создан профиль компетенций где будет фиксироваться персональная траектория развития в соответствии с правилами, определяемыми уполномоченной на федеральном уровне организацией, для этого Смольный институт будет использовать образовательные технологии и электронное обучение во всех видах и формах деятельности обучающихся в соответствии с требованиями цифровой экономики.

В институте создается система раннего выявления, поддержки и сопровождения высокомотивированных и талантливых обучающихся на основе профиля компетенций и персональных траекторий развития, в рамках которой предусмотрена грантовая поддержка педагогов, работающих с высокомотивированными талантливыми студентами. Обеспечена инфраструктура для развития предпринимательских навыков и стимулирования деловой активности обучающихся.

Также предполагается разработать и реализовать программы повышения квалификации, профессиональной переподготовки, непрерывного профессионального развития педагогических кадров, обеспечившая их готовность реализовывать современные модели образовательного процесса с учетом требований цифровой экономики.

Развитию цифровой экономики России сегодня препятствуют новые вызовы и угрозы, прежде всего: проблема обеспечения прав человека в цифровом мире, в том числе при идентификации (соотнесении человека с его цифровым образом), сохранности цифровых данных пользователя, а также проблема обеспечения доверия граждан к цифровой среде; угрозы личности, бизнесу и государству, связанные с тенденциями к построению сложных иерархических информационно-телекоммуникационных систем, широко использующих виртуализацию, удаленные (облачные) хранилища данных, а также разнородные технологии связи и оконечные устройства; наращивание возможностей внешнего информационно-технического воздействия на информационную инфраструктуру, в том числе на критическую информационную инфраструктуру; рост масштабов компьютерной преступности, в том числе международной; отставание от ведущих иностранных государств в развитии конкурентоспособных информационных технологий; зависимость социально-экономического развития от экспортной политики иностранных государств; недостаточная эффективность научных исследований, связанных с созданием перспективных информационных технологий, низкий уровень внедрения отечественных разработок, а также недостаточный уровень кадрового обеспечения в области информационной безопасности. Целью направления, касающегося информационной безопасности, является достижение состояния защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет и устойчивое социально-экономическое развитие Российской Федерации в условиях цифровой экономики, что предполагает: обеспечение единства, устойчивости и безопасности информационно-телекоммуникационной инфраструктуры Российской Федерации на всех уровнях информационного пространства; обеспечение организационной и правовой защиты личности, бизнеса и государственных интересов при взаимодействии в условиях цифровой экономики; создание условий для лидирующих позиций России в области экспорта услуг и технологий информационной безопасности, а также учет национальных интересов в международных документах по вопросам информационной безопасности. Разработка и реализация мероприятий Программы базируется на основополагающих принципах информационной безопасности, включающих: использование российских технологий обеспечения целостности, конфиденциальности, аутентификации и доступности передаваемой информации и процессов ее обработки; преимущественное использование отечественного программного обеспечения и оборудования;

применение технологий защиты информации с использованием российских криптографических стандартов.

СПИСОК ЛИТЕРАТУРЫ

1. Кунгуров Д. Россиян ждет цифровая экономика. Высокие технологии способны реанимировать слабую экономику [Электронный ресурс]. – Режим доступа: <https://utro.ru/articles/2016/12/04/1307336.shtml> (дата обращения: 14.12.2016).
2. Петросян А. Что нужно знать о цифровой экономике и ее перспективах- [Электронный ресурс]. – Режим доступа: <http://www.kommersant.ru/doc/3063024> (дата обращения: 14.12.2016).

УДК 378.1

ПОДХОД К МОДЕРНИЗАЦИИ МНОГОУРОВНЕВОЙ СИСТЕМЫ ВЫСШЕГО ОБРАЗОВАНИЯ В РОССИИ В УСЛОВИЯХ СОВРЕМЕННЫХ ВНУТРЕННИХ И ВНЕШНИХ УГРОЗ

Советов Борис Яковлевич¹, Касаткин Виктор Викторович²

¹Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5,

²Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия, 39,
emails: bysovetov@mail.ru, v.v.kasatkin@iias.spb.su

Аннотация: Обсуждается подход к модернизации многоуровневой системы высшего образования в условиях современных угроз и санкций. Предложен подход, реализующий линейную схему подготовки бакалавра, магистра и специалиста. Обсуждаются варианты реализации линейной схемы подготовки кадров на примере направлений подготовки кадров «Информационные системы и технологии» в структуре укрупненной группы направлений и специальностей высшего образования 09.00.00 «Информатика и вычислительная техника».

Ключевые слова: линейная схема подготовки бакалавра, магистра и специалиста, информационные системы и технологии.

APPROACH TO MODERNIZATION OF MULTILEVEL SYSTEM OF THE HIGHER EDUCATION IN RUSSIA IN THE CONDITIONS OF MODERN INTERNAL AND EXTERNAL THREATS

Boris Sovetov¹, Victor Kasatkin²

¹ The St. Petersburg State Electrotechnical University «LETI»,
Russia, St. Petersburg, Professor Popov str., 5,

² St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,
Russia, St. Petersburg, 14 Line, 39,
emails: bysovetov@mail.ru, v.v.kasatkin@iias.spb.su

Abstract: Approach to modernization of multilevel system of the higher education in the conditions of modern threats and sanctions is discussed. The approach realizing the linear scheme of training of the bachelor, master and expert is offered. Options of implementation of the linear scheme of training on the example of the directions of training "Information systems and technologies" in structure of the integrated group of the directions and specialties of the higher education 09.00.00 "Informatics and computer facilities" are discussed.

Keywords: linear scheme of training of the bachelor, master and expert, information systems and technologies.

Начиная с 2003 года, последовательно реализуется политика реформирования Российского образования в соответствии с требованиями «Болонского процесса». Если изначально основной целью модернизации образовательной системы было вхождение в мировую систему образования, то в условиях санкций со стороны США и Европейских государств со всей очевидностью назрела необходимость быстрого восстановления и инновационного развития отечественного производства, требованиям которого, к сожалению, не отвечают в полной мере выпускники вузов, получающие квалификацию бакалавра и магистра [1]. Очевидно, что работодателям для развития современно высокотехнологичного производства требуются высококвалифицированные специалисты – инженеры, способные разрабатывать и производить отечественную продукцию, проектировать и эксплуатировать устройства и системы на основе использования отечественной элементной и технологической базы и отвечающие современным требованиям к качеству и конкурентноспособности продукции на мировых рынках.

С учетом естественной инерционности любой образовательной системы может быть предложен подход, реализующий линейную схему подготовки бакалавра, магистра и специалиста. Для этого потребуется разработка законодательных инициатив и нормативно-правовых актов, позволяющих совмещать разные образовательные траектории на отдельных стадиях подготовки кадров разной квалификации. Это означает переход к линейной схеме организации образовательного процесса, когда на младших курсах по единым совмещенным учебным планам и программам дисциплин обучаются

будущие бакалавры, магистры и специалисты. После двух - двух с половиной лет обучения в зависимости от направления подготовки целесообразно осуществлять конкурсный отбор студентов (с учетом их интересов, возможностей, индивидуальных особенностей) на дальнейшее обучение по образовательным траекториям бакалавра, магистра, специалиста соответственно. Без сомнения, такое решение позволит более рационально оценить возможности каждого студента, скорректировать ошибки выбора образовательной траектории, сэкономить государственные средства на подготовку и последующую переподготовку кадров [2]. Естественно, введение линейной схемы подготовки потребует также модернизации ФГОС и примерных образовательных программ, включающих примерные учебные планы и примерные программы дисциплин, практик, самостоятельной работы студентов и т.п. При ее реализации появляется реальная возможность корректировки числа выпускников при заданных контрольных цифрах приема студентов на разные уровни обучения в условиях меняющихся условий в Российской экономике, потребностей рынка труда и образовательных услуг.

В докладе приводятся конкретные варианты реализации линейной схемы подготовки кадров на примере направлений подготовки кадров «Информационные системы и технологии» в структуре укрупненной группы направлений и специальностей высшего образования 09.00.00 «Информатика и вычислительная техника».

СПИСОК ЛИТЕРАТУРЫ

1. Советов Б.Я. Тенденции развития высшего образования и подготовки кадров в области информационных технологий. // Региональная информатика (РИ-2016). Юбилейная XV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2016)». Санкт-Петербург, 26-28 октября 2016 г.: Материалы конференции. / СПОИСУ. – СПб., 2016. – 599 с.
2. Советов Б.Я., Касаткин В.В. Интеграция образования, науки и промышленности как основа профессиональной ориентации ИТ-специалистов при многоуровневой подготовке // Региональная информатика (РИ-2016). Юбилейная XV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2016)». Санкт-Петербург, 26-28 октября 2016 г.: Материалы конференции. / СПОИСУ. – СПб., 2016. – 599 с.

УДК 331.7

СОВРЕМЕННЫЕ УГРОЗЫ РАЗВИТИЮ РОССИЙСКОЙ ОБРАЗОВАТЕЛЬНОЙ СИСТЕМЫ

Советов Борис Яковлевич¹, Касаткин Виктор Викторович²

¹Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5,

²Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Россия, Санкт-Петербург, 14 линия, 39,
emails: bysovetov@mail.ru, v.v.kasatkin@iias.spb.su,

Аннотация: Продолжающееся реформирование Российского образования с целью вхождения его в мировую образовательную систему привело к отказу от достижений и традиций отечественного образования и перестройке его на основе Болонской конвенции. Результаты адаптации образования к западной системе, которые наряду с прогрессивными преобразованиями привели к ряду негативных моментов: утрате воспитательного значения образования, подходу к образованию как к услуге, частичному разрушению инженерного образования, снижению роли научно-педагогических школ, утрате статуса аспирантуры как научной организации, бюрократизации сферы управления образованием. На примере анализа содержания подготовки разработчиков информационных систем и технологий обсуждаются предложения о введении образовательных программ подготовки специалиста, ориентированного на решение задач кадрового обеспечения отечественного промышленного производства в условиях современных вызовов и санкций.

Ключевые слова: многоуровневая система высшего образования, бакалавриат, магистратура, специалитет, информационные системы и технологии.

MODERN THREATS TO DEVELOPMENT OF THE RUSSIAN EDUCATIONAL SYSTEM

Boris Sovetov¹, Victor Kasatkin²

¹ The St. Petersburg State Electrotechnical University «LETI»,
Russia, St. Petersburg, Professor Popov str., 5,

² St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science,
Russia, St. Petersburg, 14 Line, 39,
emails: bysovetov@mail.ru, v.v.kasatkin@iias.spb.su,

Abstract: The continuing reforming of Russian education for the purpose of occurrence into world educational system has led him to refusal of achievements and traditions of domestic education and his reorganization on the basis of the Bologna convention. Results of adaptation of education to the western system which along with progressive transformations have led to a number of the negative moments: to loss of educational value of education, approach to education as to service, partial destruction of engineering education, decrease in a role of scientific and pedagogical schools, loss of the status of a postgraduate study

as scientific organization, bureaucratization of the sphere of management of education. On the example of the analysis of content of training of developers of information systems and technologies offers on introduction of educational programs of training of the expert focused on the solution of tasks of staffing of domestic industrial production in the conditions of modern calls and sanctions are discussed.

Keywords: *multilevel system of the higher education, bachelor degree, magistracy, specialist programme, information systems and technologies.*

В информационном обществе, как было определено в резолюции конференции в Рио-де-Жанейро в 1992 году, лидирующее место должно занимать образование. На современном этапе завершения формирования информационного общества в условиях необходимости решения приоритетных задач цифровой трансформации государственного управления и экономики страны, поставленных Президентом Российской Федерации, реализации программы «Цифровая экономика Российской Федерации», приоритетных проектов «Вузы как центры создания пространства инноваций», «Современная цифровая образовательная среда в Российской Федерации», необходимо со всей ответственностью подойти к проблемам качества и перспективам развития российской системы образования [1].

Продолжающееся в течение более 10 лет реформирование Российского образования с целью вхождения его в мировую образовательную систему привело к отказу от достижений и традиций отечественного образования и перестройке его на основе Болонской конвенции. В итоге мы получили реальные результаты адаптации образования к западной системе, которые наряду с прогрессивными преобразованиями привели под лозунгами деологизации, вариативности, толерантности, либерализации и т.п. к ряду негативных моментов: утрате воспитательного значения образования, подходу к образованию как к услуге, частичному разрушению инженерного образования, снижению роли научно-педагогических школ, утрате статуса аспирантуры как научной организации, бюрократизации сферы управления образованием, в т.ч. отходу от профессиональной содержательной оценки эффективности и качества образования, необоснованным требованиям поголовного достижения высоких наукометрических показателей (в зарубежных системах цитирования, размещенных в иностранных базах данных), публикационной активности отечественных научно-педагогических работников, в т.ч. занятых исследованиями и разработками в сфере оборонно-промышленного комплекса, критических технологий, стратегических инициатив.

В настоящее время вполне очевидно, что переход на двухуровневую систему высшего образования противоречит потребностям отечественной промышленности: нередко бакалавр после окончания вуза оказывается невостребованным в промышленности, а магистр требует дополнительных бюджетных средств на адаптацию, зачастую рабочее место магистра не соответствует направленности его подготовки. Наиболее остро влияние указанных факторов проявилось в условиях действия санкционных ограничений, непосредственно затронувших высокотехнологические отрасли промышленности, включая ИТ-индустрию, а также сферу подготовки кадров, в частности, подготовки ИТ-специалистов-разработчиков информационных систем и технологий [2]. В условиях санкций США и европейских государств отечественной промышленности необходимы кадры, готовые после окончания вуза к быстрой адаптации на рабочих местах с целью организации отечественного промышленного производства, сохранения и воспроизводства кадрового потенциала высокотехнологичных отраслей промышленности. Необходимо признать, что переход российского высшего образования на многоуровневую систему оказался для России серьезной ошибкой, и только решительный отказ от нее может устранить угрозы для национальной безопасности в части зависимости страны от импорта и сворачивания отечественного промышленного производства.

На данном этапе должен быть предложен компромиссный вариант, предусматривающий разумное сочетание уровней подготовки кадров и специалитета, который необходимо ввести в укрупненные группы направлений и специальностей высшего образования, где он был исключен, рассматривая бакалавриат как прикладной, нацеленный на подготовку эксплуатационщиков.

В докладе в качестве примера решения указанной проблемы рассматриваются реализованные в настоящее время предложения разработчиков федеральных государственных образовательных стандартов (ФГОС) по включению в структуру укрупненной группы направлений и специальностей (УГСН) высшего образования 09.00.00 «Информатика и вычислительная техника» специалитета по направлению 09.05.01 «Применение и эксплуатация автоматизированных систем специального назначения» и новое предложение о ведении в указанную УГСН разработанного проекта ФГОС подготовки специалиста по направлению 09.05.02 «Информационные системы и технологии специального назначения», ориентированного на решение приоритетных задач кадрового обеспечения отечественного промышленного производства в условиях современных вызовов и санкций.

СПИСОК ЛИТЕРАТУРЫ

1. Советов Б.Я., Касаткин В.В. Фундаментализация и профессиональная ориентация подготовки кадров в области информационных технологий. // Региональная информатика (РИ-2016). Юбилейная XV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2016)». Санкт-Петербург, 26-28 октября 2016 г.: Материалы конференции. / СПОИСУ. – СПб., 2016. – 599 с.
2. Б.Я. Советов, В.В. Цехановский. Информационные технологии: теоретические основы. Учебное пособие. СПб: Лань, 2017 г. 444 с.

УДК 37.072

**МЕТОДЫ ПОВЫШЕНИЯ КАЧЕСТВА ПОДГОТОВКИ СПЕЦИАЛИСТОВ В СФЕРЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Соколов Сергей Сергеевич

Государственный университет морского и речного флота имени адмирала С.О. Макарова, Россия,
Санкт-Петербург, ул. Двинская, 5/7,
email:sokolovss@gumrf.ru

Аннотация: В статье рассмотрен опыт создания в Государственном университете морского и речного флота имени адмирала С.О. Макарова современной лаборатории «Технических средств и систем в защищенном исполнении» - целевой аудитории ПАО «Газпром», как пример эффективного взаимодействия с работодателем с целью повышения качества подготовки специалистов в области информационной безопасности.

Ключевые слова: *качество подготовки; современные технические средства; методы обучения.*

THE METHODS OF QUALITY IMPROVEMENT SPECIALIST OF INFORMATION SECURITY

Sokolov Sergey Sergeevich

Admiral Makarov SUMIS, Russia, St. Petersburg, Dvinskaya str, 5/7,
email:sokolovss@gumrf.ru

Abstract: In this article experience of creation in the Admiral Makarov SUMIS of modern "Technical means and systems in the protected execution" laboratory - target audience of Gazprom as an example of effective interaction with the employer for the purpose of quality improvement of specialists education in the field of information security is considered.

Keywords: *quality of education; modern technical means; training methods.*

Введение. Высшие учебные заведения все чаще сталкиваются с противоречием: с одной стороны – увеличивающиеся требования, закрепленные в соответствующих законодательных актах и касающиеся повышения качества образовательного процесса путем обновления лабораторной базы и использования инновационных методов организации и проведения образовательного процесса, с другой – недостаточность финансирования, устаревание материальной базы, на обновление которой собственных средств ВУЗа зачастую не хватает.

В соответствии с ФГОС ВО 10.03.01 «Информационная безопасность» (уровень бакалавриата): «7.3.1. ... минимально необходимый для реализации программ бакалавриата перечень материально-технического обеспечения должен включать в себя лаборатории в области: ...технической защиты информации, оснащенную специализированным оборудованием по защите информации от утечки по акустическому каналу...», аналогичные, на взгляд автора, более мягкие требования содержатся и по уровням: специалитет и магистратура. [1, 2, 3]

В виду большей ориентации современного контингента обучающихся в сторону Интернет-технологий, веяния времени и законодательные предпосылки все больше ставят перед нами задачи внедрения современных методов электронного (уже как обязательное) и дистанционного (пока лишь как рекомендуемое) обучения – это можно в явном виде прочесть в требованиях к функционированию электронной информационно-образовательной среды. [1, 2, 3, 4, 5, 6]

Эти две предпосылки мы имеем с одной стороны, с другой – мы понимаем, что имеющееся финансирование с учетом устаревания материальной базы, необходимостью выполнения дородных карт (в т.ч. показателей, влияющих на сокращение учебно-вспомогательного персонала) явно недостаточно для выполнения требований, и чтобы успеть или даже опередить время необходимы иные подходы. Такими подходами могут являться: выполнение НИР и НИОКР в рассматриваемой области с целью получения дополнительного финансирования для обновления материальной базы; взаимодействие с работодателями с целью получения спонсорской помощи. Первый подход не является предметом данной статьи и может быть рассмотрен отдельно. Второй подход тоже имеет свои особенности: спонсорские средства, выданные без целевого назначения быстро и «тонким слоем» можно распределить на массу нужд, в тоже время, финансирование конкретного проекта – видна большая, четко понятная цель, на которую средства возможно получить с большей долей вероятности (проектно-целевой подход – одна из основ современной экономики). По этому пути пошли в Государственном университете морского и речного флота имени адмирала С.О. Макарова и обратились в ПАО «Газпром» с предложением (на что и было полученное соответствующее финансирование) выделения средств для создания многофункциональной специализированной аудитории: Целевая аудитория ПАО «Газпром», Лаборатория «Технических средств и систем в защищенном исполнении».

Многофункциональность аудитории заключается в следующем назначении: специализированная аудитория для подготовки по УГС «Информационная безопасность», оснащенная современной

методической базой, компьютерной техникой и специализированным оборудованием для закладки и обнаружения закладных устройств с целью предотвращения утечки по основным рассматриваемым каналам передачи; площадка для проведения дистанционных занятий и консультаций как удаленно доступными преподавателями, так и со стороны головного ВУЗа для сети филиалов (на данный момент их у университета 10); проведение научных исследований; площадка для проведения семинаров, конференций и встреч с коллегами из учебных, научных заведений и с представителями ПАО «Газпром».

В ГУМРФ имени адмирала С.О. Макарова есть традиция по именованию таких крупных аудиторий в честь ученых, педагогов, вложивших наибольший вклад в развитие ВУЗа. Представленная аудитория решением руководства ВУЗа будет носить имя одного из основателей и первых участников северо-западного УМО по информационной безопасности, основателя диссертационного совета университета, заведующего кафедрой, научного руководителя множества докторов и десятков кандидатов наук – д.т.н., профессора Гаскарова Вагиза Дилляуровича.

Закключение. Очень часто мы стали вспоминать слова: «Новое – это хорошо забытое старое». Кооперация и совместные действия между ВУЗами и отраслевыми организациями – это успешно перенесенный в современную Россию опыт, который одно время не использовался, но сейчас, когда мы находимся в начале шестого технологического уклада, этот опыт важен и нужен, только совместно можно двигаться вперед.

СПИСОК ЛИТЕРАТУРЫ

1. ФГОС ВО 10.03.01 «Информационная безопасность» (уровень бакалавриата).
2. ФГОС ВО 10.03.01 «Информационная безопасность автоматизированных систем» (уровень специалитета).
3. ФГОС ВО 10.04.01 «Информационная безопасность» (уровень магистратуры).
4. Пастушак Т.Н. Приоритетные направления развития электронной информационно-образовательной среды отраслевого университетского комплекса / Пастушак Т.Н., Соколов С.С., Ковальногова Н.М., Маньковская А.В. // Информационные технологии. 2014. № 9. С. 40-46.
5. Соколов С.С. Электронная информационно-образовательная среда современного университетского комплекса / Соколов С.С., Ковальногова Н.М. // В сборнике: Морское образование: традиции, реалии и перспективы материалы научно-практической конференции. 2015. С. 157-163.
6. Пастушак Т.Н. Приоритетные направления применения электронного обучения и дистанционных образовательных технологий университетского комплекса / Пастушак Т.Н., Соколов С.С., Ковальногова Н.М., Маньковская А.В. // В сборнике: Актуальные проблемы экономики и управления на водном транспорте Материалы научно-практической конференции, посвященная 75-летию со дня рождения профессора А.С. Бутова. 2014. С. 214-224.

УДК 004.451

ИЗУЧЕНИЕ МЕТОДОВ УПРАВЛЕНИЯ ДОСТУПОМ В БАЗОВОЙ ДИСЦИПЛИНЕ «ОПЕРАЦИОННЫЕ СИСТЕМЫ» СПЕЦИАЛЬНОСТИ «КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ»

Широков Владимир Владимирович, Щиголева Марина Андреевна
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5,
email: vvshirokov@mail.ru, vvcehanovskiy@mail.ru

Аннотация: Рассматриваются методы управления доступом к данным, предлагаемые для изучения на специальности «Компьютерная безопасность» в базовой дисциплине «Операционные системы». Основное внимание уделено двум методам. Первый метод - классический дискреционный метод, включающий понятия «владелец», «пользователь», «группа». А также понятия прав доступа на «чтение», «запись», «выполнение». Второй - мандатный метод, включающий понятия «уровень допуска» и «мандатные метки». Представлены описания лабораторных и практических работ, в которых студенты программируют списки контроля доступа в Linux-подобных и в Windows-подобных операционных системах.

Ключевые слова: операционная система; права доступа к объектам операционных систем; методы мандатного управления доступом; дескрипторы безопасности; программирование прав доступа к объектам операционных систем.

THE STUDY OF ACCESS CONTROL METHODS IN BETVOYAGERCASINO "OPERATING SYSTEMS" SPECIALTY "COMPUTER SECURITY"

Shirokov Vladimir, Schigoleva Marina
The St. Petersburg State Electrotechnical University "LETI",
email: vvshirokov@mail.ru

Abstract: Deals with methods of access control to the data available for study on a speciality "Computer security" basic discipline "Operating systems". The focus is on two methods. The first method is the classic discretionary method, including the concepts of "owner", "user", "group". As well as the concept of access rights "read", "write", "execute." The second mandatory method that includes the concept of "level of tolerance" and "mandatory label". Presents descriptions of laboratory and practical work in which students programmed the access control lists in Linux-like and Windows-like operating systems.

Keywords: *operating system; access rights to objects the operating systems; methods mandatory access control; security descriptors; programming of access rights to objects operating systems.*

Современные операционные системы функционируют в агрессивной информационной среде. Поэтому знания о методах управления доступом к данным необходимо получать уже на начальном этапе обучения студентов направлений подготовки «Информатика и вычислительная техника», «Управление в технических системах», «Информационная безопасность». Получению таких знаний способствует базовая дисциплина «Операционные системы» [1,2,3], изучаемая на младших курсах обучения. При дальнейшем обучении, дисциплина «Операционные системы» является базовой в последующей профессиональной подготовке по теоретическому материалу и практическим программно-вычислительным средствам решения предметно-ориентированных прикладных задач.

Информационная системы представляется как совокупность взаимодействующих субъектов и объектов. Управления доступом регламентируют доступ субъектов к объектам. Среди наиболее распространённых и стратегически выстроенных в управлении, обслуживании, организации обмена данными и их хранении, представлена дискреционная (произвольная) модель, в которой обычные пользователи могут принимать участие в определении функций политики управления и обеспечения безопасности. Системы защиты распространяются на субъекты, объекты, уровни доступа, операции, наборы и структуры данных.

Организация взаимодействия элементов информационной системы описывается моделями управления доступом, которые регламентируют доступ субъектов к объектам из определенного множества субъектов и объектов, поведение системы, операций, выполняемых субъектом над объектом. Методы управления доступом изучаются в разделе «Файловые системы». Рассматриваются средства хранения данных в информационных системах.

При организации управления доступом студенты знакомятся с понятиями «владелец», «пользователь», «суперпользователь», «группа пользователей». А также с правами доступа на «чтение», «запись», «выполнение». В лабораторных работах и на практических занятиях студенты учатся программно устанавливать права доступа к таким объектам операционных систем, как каналы, разделяемая память, очереди сообщений. В качестве наглядного гибкого многовариантного решения для моделирования управления информационными системами был выбран класс Linux-подобных операционных систем [4]. На практических занятиях студенты также знакомятся с API (Application Programming Interface), предоставляемым операционными системами, для управления доступом. С целью расширения охвата операционных систем, API рассматривается на примере Windows.

Ограниченное число субъектов доступа (владелец, группа, остальные) при дискреционном методе ограничивает и возможности управления. Здесь на помощь приходят списки контроля доступа, позволяющие устанавливать права доступа к объекту любому конкретному пользователю.

С помощью API студенты создают программные объекты, создают для них дескрипторы безопасности, создают элементы списка, разрешающие и запрещающие определенные виды доступа определенным пользователям. Затем включают эти элементы в списки контроля доступа, привязывают эти списки к дескриптору безопасности и проверяют полученные правила доступа к объекту.

Известным недостатком дискреционного метода является возможность владельца самому устанавливать права другим пользователям на доступ к объекту. К подобному выводу студенты должны придти по результатам проводимых исследований и освоения предлагаемых вариантов заданий. В качестве разрешения выявленных недостатков студентам предлагается познакомиться с методом мандатного управления доступом, лишённого выявленного недостатка и широко используемого в отечественных операционных системах, например, МСВС и системах управления базами данных, например, СУБД Линтер.

После изучения представленного материала студенты приобретают базовые знания о широко используемых методах контроля доступа и приобретают умения и навыки программирования прав доступа к объектам операционных систем и приобретают компетенции, соответствующие видам последующей профессиональной деятельности:

- способностью анализировать результаты проведения экспериментов; осуществлять выбор оптимальных и эффективных решений;
- способностью проектировать и осуществлять целевые предметно-ориентированные исследования; готовность использовать современные методы и технологии;
- умение осуществлять управления в технических системах на базе стандартных и оригинальных программно-вычислительных средств автоматизированного проектирования и исследований.

СПИСОК ЛИТЕРАТУРЫ

1. Таненбаум Э., Бос Х. Современные операционные системы. - (Серия «Классика computer science»). 4-е изд. — СПб.: Питер, 2015. — 1120 с.
2. Столлингс В. Операционные системы. М.: Вильямс, 2004. - 848 с.
3. Олифер В.Г., Сетевые операционные системы: учебное пособие для вузов / В.Г. Олифер, Н.А. Олифер. - СПб.: Питер, 2005. - 539 с.
4. А.Стахов. Сетевое администрирование Linux. СПб BHV, 2014 [Электронный ресурс]. - Электрон. дан. - Режим доступа: <http://www.linux.ru/doc> (документация по ОС Linux).



МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПРОБЛЕМЫ УСТОЙЧИВОГО РАЗВИТИЯ»

УДК 004.9

СТРАТЕГИИ РАЗВИТИЯ УМНОГО ИНФОРМАЦИОННОГО ОБЩЕСТВА

Бариков Леонид Николаевич, Игнатьев Михаил Борисович
Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Россия, Санкт-Петербург, ул. Большая Морская 67
emails: lnbarikov@gmail.com, ignatmb@mail.ru

Аннотация: В статье рассматривается история развития информационного общества и определяются положительные и отрицательные аспекты этого развития

Ключевые слова: информационное общество, язык, сообщения, сеть

THE STRATEGY OF DEVELOPMENT OF THE SMART INFORMATION SOCIETY

Barikov Leonid, Ignatyev Mikhail
Saint-Petersburg state University of aerospace instrumentation,
Russia, Saint-Petersburg, Bolshaya Morskaya str. 67
emails: lnbarikov@gmail.com, ignatmb@mail.ru

Abstract: The article presents history of development of the information society and determines the positive and negative aspects of this development

Keywords: information society, language, communications, network

Опубликована «Стратегия развития информационного общества в РФ на 2017-2030 годы», утвержденная Указом Президента РФ. С самого начала появления человеческого общества оно было информационным, основанным на широком использовании естественного языка. По мере развития науки и техники к распространению информации подключались новые технологии – сначала это было книгопечатание, потом электрический телеграф, потом радио, потом телевидение, потом компьютерные сети и ИНТЕРНЕТ, причем появление новых видов информационного взаимодействия не исключало старых – они существовали и существуют параллельно. Но технология распространения и сохранения информации – это лишь форма, главное – содержание информации, которое может оказать либо положительное влияние на развитие общества, либо отрицательное, и возникает важная задача защита общества от разрушительной информации. Умное информационное общество имеет мощные механизмы защиты от разрушительной информации. Стратегии развития информационного общества во многом определяются глобальным социально - культурным циклом [1], [2], который складывается из частных циклов, таких как цикл распространения финансовой информации, изобразительной информации, музыкальной информации и др., которые определяются особенностями истории и культуры каждой из стран и степенью влияния глобальных тенденций на каждую из стран. В связи с опубликованием Стратегии развития информационного общества РФ нам предстоит колоссальная работа.

СПИСОК ЛИТЕРАТУРЫ

1. Моль А. «Социодинамика культуры» - М.: Мысль, 1973, 352с.
2. Игнатьев М.Б. Кибернетическая картина мира: Сложные киберфизические системы: Учебное пособие – СПб.: ГУАП, 2014, 472с.

УДК 004.8

МОДЕЛИРОВАНИЕ ОРГАНИЗМА ЧЕЛОВЕКА ДЛЯ ПОДДЕРЖКИ ВРАЧЕБНЫХ РЕШЕНИЙ

Губин Александр Вадимович, Игнатьев Михаил Борисович, Катермина Татьяна Сергеевна,
Красников Андрей Георгиевич
Россия, Курган, ФГБУ «РНЦ «Восстановительной травматологии и ортопедии» им. академика
Г.А.Илизарова, С-Петербургский государственный университет аэрокосмического приборостроения,
Нижевартовский государственный университет, Санкт-Петербург, Первый медицинский университет
им.И.П.Павлова.
emails: gubin_av@ilizarov.ru, ignatmb@mail.ru

Аннотация. Рассматривается проблема компьютерного моделирования организма человека и определяется его стратегия – от моделирования на уровне органов до моделирования на молекулярном уровне

Ключевые слова: лингво-комбинаторное моделирование, сложность, поддержка врачебных решений, моделирование живой клетки, молекулярный уровень.

SIMULATION OF THE HUMAN BODY TO SUPPORT MEDICAL DECISIONS

Gubin Alexander Vadimovich, Ignatiev Mikhail Borisovich, Katerina Tatiana Sergeevna,

Krasnikov Andrey Georgievich

Russia, Kurgan, 640014, "Russian Ilizarov Scientific Center "Restorative traumatology and Orthopaedics",

St. Petersburg state University of aerospace instrumentation, Nizhnevartovsk state University, Saint

Petersburg Pavlov First Medical University.

emails: gubin_av@ilizarov.ru, ignatmb@mail.ru

Abstract. Considers the problem of computer simulation of the human body and is defined by its strategy – from modeling at the level of the organs to the simulation at the molecular level

Keywords: *linguo-combinatorial simulation, complexity, support medical decisions, modeling of a living cell, the molecular level.*

В настоящее время для исследования и создания сложных систем и сооружений широко применяется компьютерное моделирование. По мнению всемирной организации здравоохранения (ВОЗ) необходимо развивать компьютерное моделирование и в медицине, прежде всего чтобы уменьшить количество врачебных ошибок. Но возникает вопрос – на каком уровне строить эти компьютерные модели? Это возможно и на молекулярном уровне. Например, в 2012 году ученым Стенфордского университета удалось создать полную модель живого организма, используя данные 900 научных работ для того, чтобы учесть все молекулярные взаимодействия, происходящие в жизненном цикле бактерии *Mycoplasma genitalium* – одного из самых маленьких организмов, способных существовать самостоятельно. Был создан весь живой организм *in silico* – на кремнии – с помощью компьютерной модели, что позволяет ставить различные эксперименты, проведение которых технически неосуществимо в случае живой клетки. А как быть с человеческим организмом, с многоклеточным организмом? Эта задача по сложности превосходит задачу моделирования бактерии в миллиарды раз, конечно со временем и она будет решена, а как быть сейчас? Еще в 2000 году мы предложили моделировать основные органы человека и их взаимодействие [1], для лечащего врача важно рассматривать организм прежде всего на уровне органов и мы предложили построить лингво-комбинаторную модель организма исходя из общепринятого набора органов: органы движения (кости, мышцы, связки), органы пищеварения, органы дыхания, мочеполовые органы, кроветворная и лимфатическая системы, центральная нервная система, периферическая нервная система, железы внутренней секреции, кожа и сенсорные системы, иммунная система, -такие модели были построены и уже применяются. В связи с разработкой электронного паспорта здоровья родилось предложение сделать его основой конкретную лингво-комбинаторную модель организма [2].

СПИСОК ЛИТЕРАТУРЫ

1. Ignatyev M.B. et al. Global model of organism for decision making support: Proc.of the high performance computing symp.HPC 2000/Ed. A. Tentner. Washington D.C., USA, 2000, P. 66-71.
2. Игнатев М.Б. Кибернетическая картина мира. Сложные киберфизические системы, СПб, 2014, 478 стр.

УДК 004.8

К ВОПРОСУ О СОЗДАНИИ НОВОГО ЗДАНИЯ МУЗЕЯ ОБОРОНЫ И БЛОКАДЫ ЛЕНИНГРАДА

Игнатев Михаил Борисович, Макин Алексей Иванович, Мамошин Михаил Александрович,

Никитин Александр Иванович, Фадеева Нина Владимировна

Россия, Санкт-Петербург, Региональная общественная организация воспитанников детских домов блокадного Ленинграда, Музыкальное училище им. М.П. Мусоргского, Архитектурная мастерская Мамошина, С-Петербургский государственный университет аэрокосмического приборостроения

Аннотация. Рассматривается проблема создания нового здания музея обороны и блокады Ленинграда с учетом прошлого опыта и перспектив применения новых технологий.

Ключевые слова: история обороны Ленинграда, старый музей, виртуальная и дополненная реальности.

THE QUESTION OF THE CREATION OF THE NEW BUILDING OF THE MUSEUM OF DEFENSE AND BLOCKADE OF LENINGRAD

Ignatyev Mikhail, Makin Alexey, Mimosin Michael, Nikitin Alexander, Fadeeva Nina

Russia, Saint-Petersburg *Regional public organization of orphanages of besieged Leningrad, Music school. Mussorgsky, Architectural Studio of Mamoshin, St.Petersburg state University of aerospace instrumentation

Abstract: Deals with development of a new building of the Museum of defense and blockade of Leningrad on the basis of past experience and prospects of application of new technologies.

Keywords: *history of the defense of Leningrad, the old Museum, virtual and augmented reality.*

Вопросы информационной безопасности тесно связаны с патриотической воспитательной работой в обществе, что определяет мотивацию людей. В настоящее время развернулась острая борьба за трактовку исторических событий и в этом ряду героическая оборона и блокада Ленинграда в период 1941 – 1944 годов занимает особое значительное определившее победу место в ряду событий Второй мировой войны [1]. Музей обороны и блокады Ленинграда был организован в 1944 году после полного снятия блокады города, ему было выделено здание Всероссийской выставки народного хозяйства, построенное еще в царское время напротив Летнего сада площадью 40 тыс. квадратных метров. Этот музей пользовался большой популярностью среди жителей и гостей города, но в 1949 году в связи с так называемым Ленинградским делом музей был закрыт, а его сотрудники репрессированы, и только в 1989 году по требованию общественности музей был вновь открыт, но в сильно урезанном виде, ему выделили лишь одну тысячу квадратных метров, что не соответствовало количеству накопленного материала и значению музея для города, страны и мира, и только в 2017 году было принято решение о строительстве нового здания музея в районе Смольного на берегу Невы. Это очень значимое место – ведь в Смольном помещался штаб обороны города. В сентябре 2017 года была открыта выставка проектов нового здания музея, было представлено девять проектов, среди которых выдающееся место занимал проект, подготовленный Архитектурной мастерской Мамошина, поэтому в нашем докладе он и рассматривается прежде всего.

По нашему мнению, проект Архитектурной мастерской Мамошина тоже нуждается в доработке. Это прежде всего создание лестницы памяти из 872 ступеней по числу дней блокады, для чего необходимо использовать подземное пространство. Преодоление лестницы памяти – лучшее средство для воспитания молодежи [1]. Во-вторых, создание светового конуса над зданием музей, для чего необходимо установить 12 прожекторов по кромке здания, лучи которых были бы направлены вверх под углом 75 градусов, управляя этими лучами можно было бы реализовать цветомузыку, соответствующую значимости тех событий. В-третьих, необходимо использовать технологии виртуальной и дополненной реальности для представления событий в действии. Разработка и реализация проекта нового здания музея обороны и блокады Ленинграда должна быть основана на предложениях ветеранов войны и жителей блокадного Ленинграда и явиться сама по себе важным актом патриотического воспитания.

СПИСОК ЛИТЕРАТУРЫ

1. Игнатьев М.Б. «Кибернетическая картина мира» СПб, изд. ГУАП, 2010.

УДК 005.33

ТИПОВЫЕ ИНФОРМАЦИОННЫЕ УГРОЗЫ БАЗАМ ДАННЫХ CRM-СИСТЕМ И МЕТОДЫ ЗАЩИТЫ ОТ НИХ

Репина Валерия Владимировна
Санкт-Петербургский государственный экономический университет
Россия, Санкт-Петербург, наб. кан. Грибоедова 30-32
email: valeriarepina@mail.ru

Аннотация: В статье рассмотрено понятие CRM-системы, как системы управления взаимоотношениями с клиентами, типовые информационные угрозы CRM-системам и методы защиты данных.

Ключевые слова: *CRM-системы, информационные угрозы*

MODEL INFORMATION OF THE THREAT DATABASES, CRM-SYSTEMS AND METHODS OF PROTECTION AGAINST THEM

Repina Valeria
Saint-Petersburg state University of Economics
Russia, Saint-Petersburg, nab.kan. Griboyedova 30-32
email: valeriarepina@mail.ru

Abstract: The article considers the concept of CRM as a system for customer relationship management, model of information threats CRM systems and data protection methods.

Keywords: *CRM system, the threat of information*

Введение. Часто в компаниях, предоставляющих услуги населению, самым уязвимым местом являются внедренные CRM-системы со всей клиентской базой данных. Как правило, это привлекает конкурирующие компании, которые не всегда ведут честную конкурентную борьбу.

Основные угрозы информационной безопасности CRM-системы:

1. Угроза конфиденциальности – несанкционированный доступ к базам данных с мотивом их хищения.
2. Угроза целостности – несанкционированная модификация, дополнение или уничтожение данных.
3. Угроза доступности – ограничение или блокирование доступа к базам данных.

Источники угроз могут быть внешними и внутренними. Внешние – несанкционированный доступ к информации со стороны заинтересованных организаций, компьютерные вирусы и другое вредоносное ПО. К внутренним источникам угроз будут относиться: ошибки пользователей и сисадминов, ошибки в работе ПО, сбой в работе компьютерного оборудования, нарушение регламентов компании по работе с информацией.

Способы защиты информации предполагают использование определённого набора средств, например, таких как:

Физические средства – решётки на окнах, прочные двери, надёжные замки/электронные ключи, строгий пропускной пункт в здание офиса, противопожарная система.

Технические и аппаратные средства – сигнализации; блоки бесперебойного питания для корректного завершения работы при отключении электричества.

Организационные средства – правила работы, регламенты, законодательные акты в сфере защиты информации, подготовка помещений с компьютерной техникой и прокладка сетевых кабелей с учетом требований по ограничению доступа к информации и пр. При эффективном использовании организационных средств работники предприятия должны быть хорошо осведомлены о технологии работы с охраняемыми сведениями, четко выполнять свои обязанности и нести ответственность за предоставление недостоверной информации, утечку или потерю данных. Должен быть подписан договор о неразглашении конфиденциальной информации каждым сотрудником, имеющим доступ к секретным данным компании. Если произойдёт нарушение договора, виновного привлекут либо к административной, либо к уголовной ответственности. В компании должны использоваться программные средства, отражающие хакерские атаки, проводящие резервное копирование данных примерно раз в неделю автоматически, а также рекомендуется использовать ПО по восстановлению баз данных. Приветствуется использование шифрования информации с помощью специальных алгоритмов (криптография). Но поскольку эти методы обеспечения безопасности информации недостаточны эффективны, потому что выяснить источник утечки информации в максимально быстрые сроки очень сложно и эти меры можно легко обойти, хотелось бы предложить пути их модификации.

Во-первых, для увеличения уровня безопасности доступа не только к базам данных, но и к компьютерам, необходимо производить вход в систему с помощью индивидуального логина и пароля, последний из которых нужно периодически менять. С помощью этой функции система будет ограничивать права пользователя согласно его роли в компании. Пароль администратора следует менять раз в неделю, смена всех паролей должна осуществляться после ухода кого-либо из сотрудников, имеющего доступ к системе.

Во-вторых, целесообразно использовать метод двухфакторной аутентификации пользователя в сети. Этот метод сейчас широко используется в интернете, так почему же не добавить это в авторизацию в корпоративных системах. Пользователь вводит логин и пароль, а ему на телефон приходит смс с кодом доступа. После его корректного ввода осуществляется вход в систему. Этот способ не обязательно использовать для каждого сотрудника, это нужно для авторизации пользователей, у кого открыты большие права в системе.

В-третьих, для более эффективной защиты информации отлично подойдут подавители сети. При обнаружении попытки взлома можно отключить сети на всём предприятии и не дать злоумышленникам повредить/скопировать оставшуюся часть информации.

В-четвертых, возможно использование программного обеспечения, которое будет отслеживать и фиксировать подключения к посторонним сетям, контролировать выгрузку данных в сеть Интернет или на внешние носители. Если система зафиксирует выгрузку данных, то она может автоматически отправить смс руководству компании и администраторам, которые в свою очередь активируют глушители сети и заблокируют все компьютеры в офисе до выявления виновников несанкционированного доступа к базам данных. Несмотря на то, что данные методы защиты повлекут за собой определённые финансовые затраты, как правило незначительные, эффективность защиты CRM-систем существенно возрастёт.

Заключение. Таким образом, предложенные методы модификации средств защиты информации помогут усилить степень безопасности конфиденциальной информации организации.

СПИСОК ЛИТЕРАТУРЫ

1. Галаяутдинов Р.Р. Информационная безопасность. Виды угроз и защита информации // Сайт преподавателя экономики. [2014]. URL: <http://galyautdinov.ru/post/informacionnaya-bezopasnost> (дата обращения: 25.09.2017).
2. Классификация методов защиты информации URL: <http://camafon.ru/informatsionnaya-bezopasnost/metodyi-zashchityi> (дата обращения: 25.09.2017).

УДК 332.1

**СТРАТЕГИИ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РЕГИОНАЛЬНЫХ
ЭКОНОМИЧЕСКИХ СИСТЕМАХ С УЧЕТОМ РАЗНЫХ ТИПОВ РЕАКЦИЙ НА ВЫЗОВЫ ВНЕШНЕЙ
СРЕДЫ**

Титовец Алиса Юрьевна
Уральский государственный экономический университет,
Россия, Екатеринбург, ул.8 Марта 62,
emails: Alisa-2007-al@mail.ru

Аннотация: В статье рассматриваются перспективы и стратегические ориентиры развития информационных технологий в региональных экономических системах. Определена проблематика реализации государственной политики в области информационной безопасности и развития информационных технологий. Доказано, что барьером для развития информационных технологий в различных региональных экономических системах является разнокачественная территориальная реакция на инструменты воздействия. Описываются качественные характеристики понятий «временной реакционный буфер» и «реакция территорий (регионов или муниципалитетов)» и подчеркивается необходимость определения уровня и типа реакций на развитие и внедрение информационных технологий.

Ключевые слова: *информационные технологии, региональная экономическая система, реакция, временной реакционный буфер, безопасность, государственная политика*

**STRATEGIES OF INFORMATION TECHNOLOGIES DEVELOPMENT IN REGIONAL ECONOMIC
SYSTEMS, BASED ON DIFFERENT TYPES OF REACTIONS TO THE CHALLENGES OF THE
EXTERNAL ENVIRONMENT**

Titovets Alisa
Ural State University of Economics
Russia, Yekaterinburg, 8 Marta 62
emails: Alisa-2007-al@mail.ru

Annotation: Prospects and strategic guidelines for information technologies development in regional economic systems have been discussed in the article. Problems of state policy implementing in the sphere of information security and information technologies development have been identified. It is proved that a barrier to the information technologies development in different regional economic systems is a territorial reaction to the tools of influence. Qualitative characteristics of such concepts like "timed reactionarybuffer" and "reaction of areas (regions or municipalities)" are described and need to identify the level and type of reactions for the development and implementation of information technology are emphasized.

Keywords: *information technologies, regional economical system, reaction, timed reactionarybuffer, security, state policy*

Введение. Каждая социально-экономическая трансформация общества осуществляется посредством новых технологий, которые существенно модифицируют производственные и экономические отношения. Экономика и общество современного мира находятся на стадии постиндустриального развития, который является этапом внедрения технических достижений второй половины XX века в экономические и общественные процессы. Интегрирование научных и технических достижений позволяет сформировать фундамент для перехода в новый технологический уклад.

Как отметил Президент РФ В.В. Путин «для выхода на новый уровень развития экономики, социальных отраслей нам нужны собственные передовые разработки и научные решения. Необходимо сосредоточиться на направлениях, где накапливается мощный технологический потенциал будущего, а это цифровые, другие, так называемые сквозные технологии, которые сегодня определяют облик всех сфер жизни» [15]. Прежде всего, это информационные технологии и компьютеризированные системы, высокие производственные технологии, являющиеся результатом новых открытий и изобретений.

Как отмечают В. Новиков и Е. Ткачёва «новые трансформации экономического пространства и информационные возможности вызывают к жизни новые информационные мотивы и потребности, развитие и удовлетворение которых приводит к модификации и в экономике, и в повседневной жизни» [14].

Поэтому устойчивое социально-экономическое развитие – это поиск и выбор среди имеющихся альтернатив такого способа развития, при котором достижение определённых целей в настоящем времени будет способствовать их достижению в будущем [11].

На территории РФ функционирует и реализуется несколько стратегических документов в области развития информационных технологий и информационного общества:

- 1) ФЗ О безопасности критической информационной инфраструктуры Российской Федерации
- 2) Доктрина информационной безопасности Российской Федерации

- 3) Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы
- 4) Стратегия Развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года
- 5) Программа "Цифровая экономика Российской Федерации"
- 6) План мероприятий ("дорожная карта") "Развитие отрасли информационных технологий"
- 7) Концепция региональной информатизации.

В рамках данных документов определено, что информационные технологии являются инструментом формирования информационного общества, цифровой экономики и эффективной системы взаимодействия всех уровней власти между собой, бизнесом и населением. Внедрение, развитие и создание информационных технологий позволит стране в целом сформировать конкурентоспособную экономику на мировом уровне, а самое главное, последние принятые документы нацелены на повышение уровня безопасности страны и населения от внешних угроз. Информационные технологии стали частью современных управленческих систем во всех отраслях экономики, сферах государственного управления, обороны страны, безопасности государства и обеспечения правопорядка, а повсеместное внедрение иностранных информационных технологий усложняет решение задачи по обеспечению защиты интересов граждан и государства в информационной сфере [3].

Анализ документов стратегического планирования, позволяет сделать вывод, что новый вектор развития информационных технологий в контексте территориального развития снова выстраивается по прошлому сценарию. С акцентом только на общих вопросах развития данной области, без учета специфики регионов или муниципалитетов, без понимания что одни и те же инструменты не могут сработать на разных территориях одинаково и без учета прошлых ошибок.

По мнению Гусакова М.А. «... в нашей стране в последние 10 и более лет реализовывался инерционный сценарий развития науки и технологии, не произошло принципиальных изменений в отношении динамики технологического и инновационного развития» [10]. И, по его мнению, единственной возможностью запустить нормальный процесс развития науки и технологий это « ... вовлечение максимального числа регионов ...» [10].

Для вовлечения максимального количества регионов и муниципалитетов в данный процесс, необходимо учитывать уровень экономико-технического развития территории, который определяет возможность субъекта или муниципалитета реализовать стратегические информационные мероприятия. Поэтому при формировании вектора развития информационных технологий в территориальном аспекте необходимо, на наш взгляд, в первую очередь оценить степень реагирования региональной или муниципальной системы на новые изменения и условия. Изучение данного вопроса, позволяет сделать вывод, что в современном мире для эффективного развития территориальных экономических и общественных систем необходимо учитывать реакцию данной системы, как живого организма и сложной системы, на угрозы и факторы развития.

Галазова С.С. отмечает что «исследования по соответствующей тематике находятся фактически на начальной стадии. Поэтому сегодня имеются все основания оценивать ситуацию как этап формирования методологической и теоретической базы изучения реакции региональных социально-экономических систем на изменения национальных макроэкономических параметров и институциональных условий. Тем не менее, уже сложилась фундаментальная основа для реализации выбранного направления исследования как особого фактора становления региональной экономики и того, что этим обусловлено – процесса формирования региональной экономической политики» [9].

При этом данное направление исследования имеет огромное значение для России в целом и для конкретных регионов (муниципалитетов) - субъектов федерации, высокий уровень нестабильного и дифференцированного развития регионов страны приводит к неэффективному функционированию всей системы, которая по кругу задевает все регионы (не стабильность "проблемных регионов" - не стабильность страны - не стабильность "сильных" регионов).

Понимание сложности реакции и ее неравномерности по всей территории страны, приводит необходимости выделения такого явления как "временной реакционный буфер". Отталкиваясь от того, что регионы не просто по-разному реагируют на внешние факторы, но и в разное время, то есть наблюдается в действии теория "центр-периферия" и возникает ситуация отложенной во времени региональной реакции.

Это приводит к тому, что некоторые территории достаточно быстро показывают результат по внедрению информационных технологий и начинают получать информационные выгоды, а некоторые территории не в состоянии внедрить информационные технологии, так например, ОМСУ сельских территорий не могут создать свой сайт не потому что у них нет финансовых средств или специалистов, а потому что скорость Интернета на их территориях настолько низкая, что им просто не имеет смысла его делать, его никто не сможет загрузить и использовать.

То есть экономически сильные регионы, смогут эффективнее и быстрее перетягивать положительные факторы развития, так Зубаревич Н.В. отмечает, что «...процессы глобализации ранее всего проявились в крупнейших городских агломерациях...» [12]. Данный феномен приводит к

неравномерности развития территорий страны и под влиянием "положительных" факторов остается и даже усиливается.

На этот аспект обращают внимание Глушков А.И. и Цало И.М., отмечая, что «в городах федерального значения экономическая реакция на значительные изменения тенденций на мировых рынках происходит крайне быстро, тогда как в региональных городах экономическая реакция отложена во времени». Это связано с тем, что данные территории сильнее вовлечены и зависимы от мировых рынков.

Поэтому временной реакционный буфер для каждого региона будет свой, в зависимости от уровня развития территории, соответственно и деятельность органов власти на данных территориях должна быть разной. Соответственно, существует необходимость классификации видов реакций региональных экономических систем и типологизации регионов РФ с точки зрения реакций.

В работе Лымарева М.И. отмечено, что необходима особая «рефлексивная» типология российских регионов по степени, факторам и результатам их реакции на динамику макроэкономических параметров и разработка рекомендаций по выбору наиболее эффективных инструментов воздействия федеральных экономических индикаторов на развитие экономики того типа [13].

Формирование стратегических документов и федеральной политики с учетом "реакционности" территории на инструменты воздействия позволит эффективно и рационально использовать имеющиеся ресурсы необходимые для развития. Соответственно необходимо разработать классификацию реакций регионов (муниципалитетов) на внешние и внутренние изменения с учетом специфики территорий.

Можно отметить, что существует необходимость учета и повышения устойчивости экономики к воздействиям, в том числе и на региональном уровне, проскальзывает в стратегическом документе "Стратегия экономической безопасности Российской Федерации на период до 2030 года". В рамках данного документа четко выделяется задача по формированию «сбалансированного пространственного и регионального развития Российской Федерации, укрепления единства ее экономического пространства» от внешних и внутренних вызовов и угроз [2].

Но даже с учетом данного документа, можно четко определить, что перед всеми регионами и муниципалитетами ставятся одни те же цели и задачи по развитию информационной экономики, информационного общества и информационных технологий, без учета региональной или муниципальной специфики.

Таковыми основными задачами являются:

- повышение качества жизни
- увеличение вклада отрасли информационных технологий в ВРП и ВВП
- обеспечение конкурентоспособности экономики и технологического развития
- создание и развитие информационной структуры
- повышение эффективности государственного и муниципального управления
- создание и развитие ИТ- кластеров
- повышение уровня обеспеченности кадрами ИТ отрасли.

Из выше изложенных задач, можно сделать вывод, что успеха добьются в развитии информационных технологий, только те регионы и муниципалитеты, которые имеют базу и экономические возможности для этого. В принципе сейчас это и происходит в стране, так как позитивными результатами в данной области могут похвастаться только г. Москва, г. Санкт - Петербург и Республика Татарстан, остальные регионы не достигли и не сформировали нужный информационный уровень развития, а соответственно и уровень безопасности. Но здесь все намного сложнее, так одно не работающее звено в цепи информационной безопасности приводит к краху всей цепи. При этом, если проблематика регионального уровня хотя бы поднимается, то муниципальный уровень остается без внимания.

Заключение. Один из самых сложных аспектов функционирования регионов в современных реалиях – это реагирование на постоянные изменения во внешней и внутренней среде. Так как XXI век не только сформировал уникальные возможности для внедрений и развития информационных технологий, но усилил проблематику безопасности. Поэтому с учетом специфики территориального уровня развития России, при формировании стратегических документов информационного развития необходимо учитывать разные типы реакции территорий. Все это обуславливает сложность реализации принятых решений на региональном и муниципальном уровнях и невозможность реализации их традиционными методами и способами и приводит к необходимости определения типов, уровней и масштаба реакции регионов или муниципалитетов, формирования классификации реакций.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 5.12.2016 г. № 646
2. Стратегия экономической безопасности Российской Федерации на период до 2030 года: Указ Президента РФ от 13.05.2017 N 208
3. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы: Указом Президента РФ от 9.05.2017 г. № 203

4. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 N 187-ФЗ
5. Стратегия Развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года: Распоряжение Правительства РФ от 01.11.2013 N 2036-р
6. План мероприятий ("дорожная карта") "Развитие отрасли информационных технологий": Распоряжение Правительства РФ от 30.12.2013 N 2602-р
7. Концепция региональной информатизации: Распоряжение Правительства РФ от 29.12.2014 N 2769-р
8. Программа "Цифровая экономика Российской Федерации": Распоряжение Правительства РФ от 28.07.2017 N1632-р
9. Галазова С.С. Пространственный аспект современной экономической теории // Terra Economicus. 2014. Т. 12. № 2-2. С. 6-10.
10. Гусаков М.А. Выявление направлений и путей трансформации научно-инновационного пространства регионов разного типа // Экономические и социальные перемены: факты, тенденции, прогноз 2014. 3 (33). с. 151-168
11. Ефимова Е.Г. Развитие региональной социоэкономической системы как новая возможность экономического роста // Материалы II международной научно-практической конференции «Актуальные вопросы экономических наук» - Астана: Мастер По ЖШС, 2017. – 617 с.
12. Зубаревич Н.В. Крупнейшие города России как «агенты» глобализации // Россия и современный мир. 2002. № 4 (37). С. 97-101
13. Лымарев М.И. Макроэкономические приоритеты региональной динамики // Экономический вестник Ростовского государственного университета, 2008 г. Том 6 (№2). Часть 2
14. Новиков В.С., Ткачева Е.Н. Виртуальное экономическое пространство в глобализирующейся системе региональной экономики // Региональная экономика: теория и практика. 2012 г. № 7. С. 53–58.
15. Послание Президента Федеральному Собранию 01.12.2016 года // <http://kremlin.ru>

УДК 004.056.53

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ВЛОЖЕНИЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКА В БАЙТ-КОД ПУТЕМ ЗАМЕНЫ УЯЗВИМОГО БАЙТ-КОДА JAVA КЛАССА

Шариков Павел Иванович¹, Красов Андрей Владимирович²

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича,
Россия, Санкт-Петербург, пр. Большевиков 22 к.1,
emails: sharikov.pavel@ro.ru, krasov@inbox.ru

Аннотация: В статье данной статье исследована проблема уязвимости при сериализации и десериализации данных в Java. Дается общее представление о принципах работы сериализации в языке программирования. Рассмотрены реальные примеры, показывающие в какие моменты приложение, использующее сериализацию, уязвимо. Произведен разбор уязвимости, варианты в которых она возникает. Разработан алгоритм поиска уязвимых файлов в проекте, даны рекомендации по исправлению уязвимых мест приложения.

Ключевые слова: сериализация Java; десериализация Java; уязвимость; байт-код; исполняемые файл; защита авторских прав;

INVESTIGATION OF THE POSSIBILITY OF INVESTMENT OF THE DIGITAL WATER SIGN IN THE BYTE CODE BY REPLACING THE VARIABLE BYTE CODE JAVA CLASS

Sharikov Pavel¹, Krasov Andrey²

St. Petersburg State University of Telecommunications of the prof. M. A. Bonch-Bruyevich,
Russia, St. Petersburg, prosp. Bolshhevikov Street 22 building 1,
emails: sharikov.pavel@ro.ru, krasov@inbox.ru

Abstract: This article investigates the vulnerability in data serialization and deserialization in Java. We give a general idea of the principles of serialization in the programming language. Real examples are considered, showing at what moments the application using serialization is vulnerable. The vulnerability has been parsed, the variants in which it arises. The algorithm for searching for vulnerable files in the project is developed, recommendations for correcting vulnerabilities of the application are given.

Keywords: serilization Java; deserialization Java; vulnerability; bytecode; portable executable file; copyright protection;

Введение. В данный момент Java один из самых популярных языков программирования. На этом языке написано огромное количество приложений и крупных коммерческих проектов. Например, таких как: Jenkins, Web Sphere, Web Logic, JBoss и другие. Java используется в банках, кассовых терминалах и еще во многих сферах жизни и бизнеса.

Десериализованные (unserialize) уязвимости – это класс уязвимостей. Большинство языков программирования предоставляют пользователям встроенные возможности для вывода данных приложения на локальный диск или передавать их по сети. Процесс преобразования данных приложения в другой формат (чаще всего двоичный), подходящий для транспортировки, называется сериализацией. Процесс чтения данных после того, как они были сериализованы, называется десериализацией.

Уязвимости, которые мы далее будем исследовать, возникают, когда разработчики приложений на java пишут код, который принимает сериализованные данные от пользователей и производится

попытка десериализации этих данных для дальнейшего использования их в программном продукте. В зависимости от языка программирования, это может привести различного рода последствиям.

Когда java читает сериализованный объект, первое, что она делает после чтения в необработанный байтах, – это вызов пользовательского метода `readObject`, если он существует. В этом случае метод `readObject` добавляет восклицательный знак к имени, содержащемуся в строке.

Где используется сериализация. Java использует сериализацию практически повсеместно.

В запросах HTTP – Параметры, ViewState, Cookies.

RMI – широко используемый протокол java RMI на 100% основан на сериализации

RMI через HTTP. Многие веб-приложения с «толстым» клиентом используют это.

JMX – Полностью полагается на сериализованные объекты

Пользовательские протоколы. Отправка получаемых необработанных объектов Java является нормой, которую мы увидим в некоторых примерах.

Может ли приложение быть уязвимым.

Уязвимость была привнесена из-за того, что библиотека некорректно saniрует вводимые пользователем данные. Атакующий может добавить вредоносный код, и он будет принят и выполнен.

Приложение уже может быть в списке уязвимых, если оно или одна из подключаемых библиотек использует библиотеку `commons-collections.jar`. Для эксплуатации достаточно, чтобы библиотека была в `classpath`.

Поиск уязвимости. Защита. Итак, мы нашли приложение или сервер с приложениями, который поставляется в комплекте с уязвимой библиотекой.

Первое, что необходимо сделать – это найти ту часть приложения, в которой используется каким-либо образом сериализованный объект. Чтобы найти эту часть достаточно будет посмотреть на `hexdump` вашего приложения. Обычно существуют два отдельных объекта. Один из них шифруется `base64`, показывается в самом правом столбце и начинается с «`гO0AB`». Другой – это двоичный код, поэтому нам нужен шестнадцатеричный столбец. Он начинается с байтов «`ас ed 00 05 73 72`». Именно так выглядят сериализованные объекты java, они идентифицированы этими заголовками и всегда начинаются с «`ас ed 00 05 73 72`», а после того, как это шифруется `base64`, то выдается как «`гO0...`». Необходимо следить за данными двумя строками.

Первое, что необходимо сделать, если вы подозреваете, что ваше приложение уязвимо, необходимо развернуть его в тестовой среде, «песочнице».

Подход для устранения уязвимости заключается в удалении класса «`InvokerTransformer`». Если мы удалим этот `class`-файл везде, где есть любые попытки его использования, то попытки использования уязвимости должны завершиться неудачей.

Выводы. Необходимо крайне тщательно проверять использование сериализации и десериализации в вашем проекте.

Проверить ваше приложение на использование библиотеки `apache commons-collections`. Если вы все -аки используете сериализацию в проекте, достаточно проверить весь проект на использование или любое обращение к классу `InvokerTransformer.class`. После переписать весь проект без использования данного класса и удалить этот класс из `jar` файла: «`org/apache/commons/collections/functors/InvokerTransformer.class`».

СПИСОК ЛИТЕРАТУРЫ

1. Красов А.В., Верещагин А.С., Цветков А.Ю. Аутентификация программного обеспечения при помощи вложения цифровых водяных знаков в исполняемый код // Телекоммуникации. 2013, №57. С.27-29.
2. Shterenber S.I., Krasov A.V., Ushakov I.A. Analysis of using equivalent instructions at the hidden embedding of information into the executable files // Journal of Theoretical and Applied Information Technology. Т.80, 2015, №1. Р.28-34.
3. Коржик В.И., Небаева К.А., Герлинг Е.Ю., Догиль П.С., Федянин И.А. Под общей редакцией профессора В.И. Коржика. Цифровая стеганография и цифровые водяные знаки // Санкт-Петербург, Том Часть 1 Цифровая стеганография, 2016.
4. Шариков П.И., Красов А.В., Штеренберг С.И. Методика создания и вложения цифрового водяного знака в исполняемые java файлы на основе замен опкодов // Т-Comm: Телекоммуникации и транспорт. Т.11, 2017, №3. С. 66-70.
5. Красов А.В., Шариков П.И. Методика защиты байт-кода Java-программы от декомпиляции и хищения исходного кода злоумышленником // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. №1, 2017. С. 47-50.
6. Хомяков И.Н., Красов А.В. Возможность скрытого вложения информации в байт-код java // Информационные технологии моделирования и управления. №2(86), 2014. С. 185-191



МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

УДК 519.688

ПОСТРОЕНИЕ ИНФОРМАЦИОННО-МОНИТОРИНГОВОЙ СИСТЕМЫ АРОМОБЕЗОПАСНОСТИ НА АППАРАТНО-ПРОГРАММНЫХ СРЕДСТВАХ

Антонов Валерий Валентинович

Санкт-Петербургский государственный университет телекоммуникаций им.проф. М. А. Бонч-Бруевича
Россия, Санкт-Петербург, пр. Большевиков, 22
Email: antonler@rambler.ru

Аннотация: В статье рассмотрены вопросы построения и функционирования информационно-мониторинговой системы аромобезопасности на аппаратно-программных средствах Arduino. Получаемая информация передаётся на сервер событий, который обрабатывает событие в соответствии с заданным алгоритмом реагирования. В статье рассмотрено только использование газоанализаторных датчиков, однако открытая архитектура такой системы позволяет не только использовать большое количество существующих датчиков и модулей, но и проектировать новые устройства.

Ключевые слова: аромобезопасность; умный датчик запахов (терминал запахов); сервер событий.

CONSTRUCTION OF THE INFORMATION-MONITORING SYSTEM OF AROMA-SAFETY ON HARDWARE AND SOFTWARE

Antonov Valery

Federal State Budget-Financed Educational Institution of Higher Education
The Bonch-Bruевич Saint - Petersburg State University of Telecommunications,
Russia, St. Petersburg, Prospekt Bolshevikov str. 22,
email: antonler@rambler.ru

Abstract: In the article the questions of construction and functioning of the information-monitoring system of aroma-safety on hardware-software means Arduino are considered. The transmitted information is transmitted to the event server that processes the event in accordance with the specified response algorithm. The article considers only the use of gas analyzers, but the open architecture of such a system allows not only to use a large number of existing sensors and modules, but also to design new devices.

Keywords: aroma safet; smart odor sensor (odor terminal); event server

Введение. Современное развитие микроэлектроники позволяет создавать недорогие и миниатюрные аппаратные платформы контроля состояний различных датчиков и анализаторов. Это позволяет выделить в проблематике глобальной безопасности государства проблему «персональной безопасности личности». Одним из признаков, указывающим на возникновение угроз такого тиа, является запах.

Возможность датчика определять не только само присутствие конкретного вещества в воздухе, но и его концентрацию позволяет построить информационную систему адекватного реагирования на угрозу, то есть определить сценарий нейтрализации угрозы. Система аромобезопасности является принципиально новым объектом.

Система строится на трех уровнях. Это физический уровень реализуется датчиками (сенсорами) запахов, логический уровень реализуется сетью датчиков при помощи технологий мобильного доступа и интернета вещей, когнитивный уровень реализуется протоколами взаимодействия.

Основной задачей терминала запахов является информирование сервера событий о превышении концентрации отслеживаемого вещества в окружающем терминал пространстве. Основной задачей сервера событий является фиксация и обработка принятого от терминала запахов сообщения. Для каждого из сообщений, приходящих на сервер существует свой сценарий обработки. Всю информацию сервер передаёт для обработки в модуль внешнего реагирования.

Клиенты и сервер системы осуществляют взаимодействие посредством разработанного автором бинарного протокола. В основе протокола лежит широко применяемый в клиент серверной архитектур принцип разбиения сообщения на части заранее определённой размерности.

Наиболее нагруженной частью системы является сервер событий. Перебои в его работе могут привести к трагическим последствиям. Для программной реализации сервера событий была применена акторная модель [1]. Применение подобной модели зарекомендовала себя с лучшей стороны в системе распознавания образов.

Заключение. Система аромобезопасности должна стать начальной платформой, на которой в дальнейшем будет строиться система безопасной городской среды. Результатом разработки является аппаратный прототип терминала запахов с одним датчиком и прототип сервера событий.

СПИСОК ЛИТЕРАТУРЫ

1. Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. /Под. ред. С. В. Бачевского; сост. А. Г. Владыко, Е. А. Аникевич. СПб.: СПбГУТ, 2017. Т. 2. С. 87-90.
2. Шершнева И. Л. Национальная безопасность России как система // НАВИГУТ (приложение к журналу «Безопасность Евразии»). 2000. № 1. С. 45–54

УДК 004.85

ПРИМЕНЕНИЕ МАШИННОГО ОБУЧЕНИЯ В ГЛУБОКОМ АНАЛИЗЕ СЕТЕВОГО ТРАФИКА

Безверхняя Екатерина Александровна
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский проспект, 49,
email: kate.bezverkhnyaya@gmail.com

Аннотация: В статье рассмотрены пять алгоритмов машинного обучения, с помощью которых осуществляется фильтрация зашифрованного сетевого трафика отдельно взятой подсети: Naive Bayes, NBTree, LibSVM, J4.8, AdaBoost+J4.8. В результате сравнения скорости работы и необходимого количества пакетов потока для определения соответствия между потоком трафика и веб-службой для каждого из алгоритмов, определены два самых эффективных.

Ключевые слова: машинное обучение; анализ сетевого трафика; классификация; сетевое администрирование.

APPLICATION OF MACHINE LEARNING IN DEEP TRAFFIC ANALYSIS

Ekaterina Alexandrovna
St. Petersburg National Research University information technology, mechanics and optics,
Russia, St. Petersburg, Kronverkskiy prospect, 49,
email: kate.bezverkhnyaya@gmail.com

Abstract: Five machine learning algorithms are considered in the article, using which the encrypted network traffic of a single subnet is filtered. To achieve each of the algorithms, disassemble the two most effective.

Keywords: machine learning; analysis of network traffic; classification; network administration.

Введение. Сетевой анализ является полезным и иногда важным инструментом в области сетевого администрирования. Он используется провайдерами интернет-услуг (Internet Service Providers - ISP) для мониторинга трафика в своих сетях и обеспечения постоянного качества обслуживания (Quality of Service - QoS) для своих клиентов [3]. Сетевые администраторы могут использовать инструменты сетевого анализа, которые обнаруживают вторжение вредоносных программ и обеспечивают фильтрацию данных, что позволяет автоматически блокировать и сообщать о подобных сообщениях [2]. Однако шифрование служит препятствием для анализа таких сообщений [2]. Многие традиционные устройства сетевого анализа не могут эффективно анализировать зашифрованный сетевой трафик. Все больше приложений перемещается в облако и использует веб-сервисы [6], [7]. Эти веб-службы часто используют шифрование сетевых протоколов, таких как Transport Layer Security (TLS) [5], [9], [10]. По мере увеличения количества TLS трафика, возможность изучения потоков TLS для анализа рисков безопасности становится более важной.

Это исследование предоставляет способ быстрой классификации веб-службы в рамках зашифрованного сетевого трафика, построенный на основе анализа способности алгоритмов машинного обучения (Machine Learning - ML) классифицировать приложения и протоколы, оперируя их сетевым трафиком [8]: Naive Bayes, NBTree, LibSVM, J4.8, AdaBoost+J4.8/ Дальнейшие исследования показывают возможность использования алгоритмов ML для определения того, связано ли приложение с зашифрованным потоком [1]. ML-алгоритмы также полезны при классификации сетевого трафика в режиме реального времени [4]. Измеряя эффективность алгоритмов ML при классификации 16 типов

веб-сервисов в потоках TLS. Предполагается, что проверенные алгоритмы ML смогут успешно классифицировать веб-службы, связанные с зашифрованными сетевыми потоками. Кроме того, предполагается, что точность и время выполнения алгоритмов ML будут увеличиваться по мере увеличения количества анализируемого сетевого трафика. Целью этого исследования является повышение способности устройств сетевого анализа уменьшать вторжение вредоносных программ и фильтрацию данных через зашифрованные сетевые коммуникации. Хотя метод, проанализированный в этом исследовании, не пытается идентифицировать конкретные случаи вторжения или провести фильтрацию, он позволяет применять более широкие политики для смягчения этих рисков. Классифицируя зашифрованные веб-службы, сетевые администраторы могут обнаруживать и предотвращать использование несанкционированных веб-сервисов. Для достижения поставленной цели, нужно решить две задачи: - оценить, какие алгоритмы ML, вероятно, будут хорошо выполняться при классификации зашифрованного веб-трафика. Начальные эксперименты выполняются для проверки каждого из пяти алгоритмов ML над идентичным набором трафика. Алгоритмы, которые работают лучше всего с точки зрения точности и времени выполнения, используются для оставшейся части экспериментов. Вторая цель этого исследования - определить, сколько пакетов необходимо для достижения приемлемой точности классификации. Предполагается, что время выполнения и точность будут увеличиваться по мере увеличения количества анализируемых пакетов. Хотя решение, которое оптимизирует обе метрики, вероятно, не существует, это исследование количественно оценивает каждую метрику индивидуально для увеличения анализируемых потоков, начиная с начала потока.

Закключение. В этом исследовании представлены два алгоритма ML для использования при классификации веб-службы в зашифрованном потоке TLS и показывает, что алгоритмы ML могут достичь в этом контексте приемлемой точности. По мере того, как все больше приложений переходит на веб-услуги или облачные сервисы, это становится все более важным. В дополнение к внедрению способности алгоритмов ML классифицировать веб-сервисы, это исследование также расширяет число меток, используемых в исследованиях классификации трафика на основе ML. Он также непосредственно анализирует эффективность использования AdaBoost в сочетании с J4.8 в классификации веб-сервисов. Также анализируется время, необходимое для классификации зашифрованного потока трафика на современных системах. Используемый набор функций с выбранными двумя алгоритмами показывает отличные результаты возможностью алгоритма ML классифицировать недельный трафик уровня TLS менее чем за 5 секунд, используя медленные алгоритмы. Эта скорость классификации показывает возможность использования этого метода для предотвращения вторжений вредоносных программ и предотвращения фильтрации данных в устройствах анализа сети в режиме реального времени.

СПИСОК ЛИТЕРАТУРЫ

1. Альшаммари, Р. и А. Н. Цинсир-Хейвуд. «Обобщение подписей для идентификации шифрованного трафика SSH». Вычислительный интеллект в кибербезопасности, 2009. CICS '09. Симпозиум IEEE, 167-174. 2009.
2. Бордерс, К. и А. Пракаш. «Количественное определение утечек информации в исходящей веб-трафике». Безопасность и конфиденциальность, 2009 г. 30-й симпозиум IEEE, 129-140. 2009. ISBN 1081-6011.
3. Браун, Л., Г. Мунз и Г. Карл. «Пакетная выборка для обнаружения червя и ботнета в TCP-соединениях». Симпозиум по сетевым операциям и управлению (NOMS), 2010 IEEE, 264-271. ISBN 1542-1201.
4. Канини, Марко, Вэй Ли, Мартин Задник и Эндрю У. Мур. «Опыт высокоскоростной автоматической идентификации приложений для управления сетью». Материалы 5-го симпозиума ACM / IEEE по архитектуре сетей и систем связи, ANCS '09, 209-218. ACM, Нью-Йорк, Нью-Йорк, США, 2009. ISBN 978-1-60558-630-4. URL <http://doi.acm.org/10.1145/1882486.1882539>.
5. Констин, Джош. «Facebook может замедлить крошечный бит, когда он начнет переключать всех пользователей на безопасные HTTPS-соединения», 8 ноября 2012 года.
6. Кусумано, Майкл. «Облачные вычисления и SaaS - новые вычислительные платформы». Сообщения ACM, 53 (4): 27-29, 2010.
7. Кэмпбелл-Келли, Мартин. «Исторические размышления: подъем, падение и воскрешение программного обеспечения как службы». Сообщения ACM, 52 (5): 28-30, 05 2009. URL <http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=39363001&site=ehost-live>.
8. Мур, Эндрю У., Денис Зуев и Майкл Кроган. Дискриминаторы для использования в классификации, основанной на потоках. Технический отчет RR-05-13, факультет компьютерных наук, Королева Мэри, Лондонский университет, август 2005 года.
9. Райт, Чарльз В., Фабиан Монроуз и Джеральд М. Массон. Msgstr "Выполнение поведения протокола приложения в зашифрованном сетевом трафике". Журнал исследований машинного обучения, 7 (12): 2745-2769, 12 2006. URL <http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=23757985&site=ehost-live>.
10. Салливан, Дэнни. «Google начнет шифрование поисков и исходящих кликов по умолчанию с помощью SSL-поиска», 18 октября 2011 г. 2011 г.

УДК 004.056

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ

Бондарева Анастасия Дмитриевна, Гоман Елена Вячеславовна
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверский пр-т, 49,
emails: Bondareva.AD@yandex.ru, nen7995ka@mail.ru

Аннотация: Предложено определение автоматизированной системы управления технологическим процессом. Определено, что АСУ ТП является объектом информатизации, реализующим информационную технологию с использованием технических средств и систем. Предложен системный подход к обеспечению информационной безопасности АСУ ТП.

Ключевые слова: автоматизированные системы управления технологическим процессом; объект информатизации; системный подход; информационная безопасность.

ENSURING INFORMATION SAFETY OF AUTOMATED SYSTEMS OF TECHNOLOGICAL PROCESS CONTROL

Bondareva Anastasia, Goman Elena
ITMO University, Russia, Saint Petersburg, 49 Kronverksky Pr.
emails: Bondareva.AD@yandex.ru, nen7995ka@mail.ru

Abstract: This article proposes the definition of an automated process control system. It is determined that automated process control system is an informatization object, realizing information technology with the use of technical means and systems. A system approach to ensuring information security of the automated process control system is proposed.

Keywords: Automated process control system; informatization object; system approach; information security.

В настоящее время на предприятиях повсеместно используются автоматизированные системы управления технологическим процессом (АСУ ТП). Они предназначены для повышения эффективности производственного процесса, повышения безопасности в аварийных ситуациях и уменьшения затрат на производство.

Недостаточное понимание, что представляет собой данная система, какая информация подлежит защите и каким способом осуществлять ее защиту, создает проблематику обеспечения информационной безопасности АСУ ТП. В целях повышения эффективности обеспечения ИБ предприятий очевидна постановка задачи о разработке единого обобщенного подхода к обеспечению защиты информации (ЗИ) на АСУ ТП.

Для решения поставленной задачи было проведено исследование законодательной и нормативно-правовой базы РФ в области информационной безопасности, в процессе которого было выявлено, что отсутствует четкое и понятное определение АСУ ТП. Принимая во внимание определения «автоматизированная система» [1] и «технологический процесс» [2] представляется целесообразным сформулировать понятие АСУ ТП как «система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию управления частью производственного процесса, содержащей целенаправленные действия по изменению и (или) определению состояния предмета труда».

Так как в любой автоматизированной системе хранится и обрабатывается информация, то от защищенности данной информации зависит корректность и непрерывность функционирования АС, а соответственно и защищенность интересов организации.

При обеспечении информационной безопасности (ИБ) организации основополагающим понятием является «объект защиты информации». Исходя из [3], в автоматизированной системе управления объектами защиты является не только информация о параметрах управляемого объекта или процесса, но и программно-технический комплекс, включающий технические средства, программное обеспечение (ПО), а также средства защиты информации (СрЗИ). Это означает, что при обеспечении ИБ организации, использующей АСУ ТП, следует говорить не о самой АС, а об объекте АСУ ТП.

Таким образом, с одной стороны объектом защиты информации на предприятии будет являться объект АСУ ТП, включающий в себя защищаемую информацию и комплекс средств автоматизации, обеспечивающий технологию ее обработки. С другой стороны, в качестве «Объектов защиты информации» в соответствии с моделью объекта защиты информации [4] определены объекты информатизации предприятия (ОИ). ОИ подразделяются на объекты информатизации, реализующие ИТ с использованием технических средств и систем (ОИ_ТСС) и объекты информатизации, предназначенные для ведения конфиденциальных переговоров. Таким образом, если при обработке информации используются технические средства, то следует говорить о первом типе объекта информатизации.

При соотнесении структуры понятий объекта АСУ ТП и ОИ_ТСС, было выявлено, что понятие ОИ_ТСС шире и включает в себя объект АСУ ТП. Это позволяет сделать вывод, о том, что объект АСУ ТП является объектом информатизации, реализующим информационную технологию с использованием технических средств и систем.

Анализ законодательной и нормативно-правовой базы РФ в области информационной безопасности показал, что нет ни одного конкретного решения по обеспечению ИБ АСУ ТП кроме приказа ФСТЭК №31, который предназначен для обеспечения ЗИ в автоматизированных системах

управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Это означает, что защита информации на объектах АСУ ТП предприятий, не связанных с вышеперечисленными областями, не регулируется данным приказом и может быть обеспечена мерами защиты, в нем не описанными. С другой стороны, приказ содержит точные и понятные инструкции по защите АСУ ТП и не запрещает их использование на других объектах.

Так как объект АСУ ТП является ОИ_ТСС, то представляется возможным обеспечивать его информационную безопасность на основе системного подхода, являющегося обобщенным для всех ОИ и не противоречащим требованиям Приказа ФСТЭК №31. В качестве используемого в системном подходе методологического средства предлагается использование моделирования различных этапов разработки подсистемы технической защиты информации.

Важно помнить, что организация и функционирование СЗИ должны осуществляться в соответствии с циклической моделью Деминга и информационная безопасность ОИ должна обеспечиваться на всех этапах его жизненного цикла.

Заключение:

1. Предложено определение автоматизированной системы управления технологическим процессом.

2. Определен объект АСУ ТП как объект информатизации, реализующий информационную технологию с использованием технических средств и систем.

3. Предложен системный подход к обеспечению безопасности ИБ АСУ ТП являющийся универсальным и не противоречащим приказу ФСТЭК №31.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения // Каталог национальных стандартов – Росстандарт. 2017. URL: <http://protect.gost.ru/v.aspx?control=8&baseC=-1&page=0&month=-1&year=-1&search=&RegNum=1&DocOnPageCount=15&id=129578> (дата обращения 12.09.2017)
2. ГОСТ 3.1109-82 "Единая система технологической документации. Термины и определения основных понятий" URL: <http://gostexpert.ru/gost/gost-3.1109-82> (дата обращения 12.09.2017)
3. Приказ ФСТЭК от «14» марта 2014 г. №31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» URL: <http://fstec.ru/rss-lenta/110-tekhnicheskaya-zashchita-informatsii/dokumenty/prikazy/864-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31> (дата обращения 15.09.2017)
4. Загородников А.А., Козлов С.В. Модель объекта защиты информации // Конференция участников ГПО ТУСУР 2014. URL: <https://gpo-conference.tusur.ru/conference/2014/themes/99/projects/571/discourses/654> (дата обращения 16.09.2017)

УДК 004.056.55

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ЦИФРОВОЙ СТЕГАНОГРАФИИ

Галлямова Милляуша Равильевна

Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский пр., 49,
emails: Miljausha-18@mail.ru

Аннотация: В статье рассматривается метод защиты информации цифровой стеганографии. Стеганография - способ передачи или хранения информации с сохранением в тайне самого факта передачи (хранения) путем встраивания в компоненты мультимедиа: изображение, аудио, видео. Конечная цель: замаскировать само существование встроенных данных.

Ключевые слова: *стеганография, наименее значимый бит, цифровой водяной знак (ЦВЗ), несанкционированный доступ (НСД).*

METHOD OF PROTECTING INFORMATION AS DIGITAL STEGANOGRAPHY

GallyamovaMilyausha

Saint-Petersburg National research University of information technologies, mechanics and optics "ITMO",
Russia, St. Petersburg, Kronverskiy avn. 49,
emails: Miljausha-18@mail.ru

Abstract: In article the method of information security of a digital steganografiya is considered. Steganografiya - a way of transfer or storage of information with preservation in secret the fact of transfer (storage) by embedding in multimedia components: image, audio, video. Ultimate goal: to disguise existence of the built-in data.

Keywords: *steganography, least significant bit (LSB), digital watermark (DWM), unauthorized access.*

Введение. В современном мире информация является одним из важнейших аспектов жизни. В связи с этим, многие эксперты в области компьютерной безопасности, а также многие обычные пользователи компьютеров связаны с информационной безопасностью. В этой статье рассматривается метод защиты информации цифровой стеганографии. Цифровая стеганография — направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов. Данные объекты являются мультимедиа файлами (изображения, видео, аудио, текст) и внесение искажений. Сегодня стеганография позволяет не только успешно решать основную задачу – скрытно передавать информацию, но и целый ряд других актуальнейших задач, в том числе встраивание скрытой информации с целью защиты авторских прав на интеллектуальную собственность, представленную в цифровом виде.

Эта скрываемая информация называется цифровым водяным знаком (ЦВЗ), который представляет собой специальную метку, содержащую информацию, однозначно подтверждающую авторство или права на коммерческое использование защищаемого объекта. Она незаметно внедряется в изображение или другой сигнал с целью тем или иным образом контролировать его использование. ЦВЗ активно используются при размещении уникальных фотографий, видео, аудио в электронном виде в сети Интернет. Первые работы по встраиванию водяных знаков были сделаны в 90-х годах 20 века.

Типы ЦВЗ. Как правило, различают три разных типа ЦВЗ: робастные, хрупкие и полухрупкие. Под робастностью понимается устойчивость ЦВЗ к различного рода воздействиям на стегоконтейнер. Такие ЦВЗ применяются для защиты авторских прав на интеллектуальную собственность, выставляемую в публичных компьютерных сетях. Хрупкие ЦВЗ разрушаются при незначительной модификации заполненного контейнера. Они применяются для аутентификации сигналов. Полухрупкие ЦВЗ устойчивы по отношению к одним воздействиям и неустойчивы по отношению к другим. ЦВЗ называют незаметным, если исходный и помеченный сигналы по определённым критериям восприятия неотличимы. Обычно легко сделать надёжный или незаметный ЦВЗ. Но, как правило, тяжело сделать ЦВЗ незаметный и надёжный одновременно. ЦВЗ могут представляться в виде битовой последовательности, изображения или последовательности с плавающей точкой.

Области применения ЦВЗ. Встраивание ЦВЗ в медиафайлы может быть использовано для следующих целей:

1. Встраивание информации с целью ее скрытой передачи.
2. Встраивание ЦВЗ с целью защиты авторских прав на интеллектуальную собственность, представленную в цифровом формате.
3. Маркирование идентификационными номерами для отслеживания путей распространения нелегальных копий продукта, используя технику уникальной подписи для каждой легальной копии.
4. Встраивание с целью защиты от копирования медиафайла.
5. Мониторинг широкоэмитерных каналов.
6. Встраивание с целью проверки целостности переданных данных.
7. Встраивание с целью индексации частей файла.
8. Встраивание ЦВЗ для подписи медицинских снимков или нанесения легенды(картография) на карту.

Методы и алгоритмы цифровой стеганографии. Методы, использующие для скрытия данных частотную область, являются более стойкими к различным возможным внешним воздействиям на изображение-контейнер. В этой группе используются достаточно разнообразные трансформации:

- дискретное косинус-преобразование (ДКП);
- вейвлет-преобразование (ДВП);
- дискретное преобразование Фурье (ДПФ);
- преобразование Карунена-Лоева (ПКЛ);
- сингулярное разложение.

Заключение. Цифровая стеганография - динамичная и быстро развивающаяся наука, которая использует методы и достижения криптографии, цифровой обработки сигналов, теории коммуникации и информации. Наряду с обычным пользователем также заинтересованы крупные компании, работающие в области мультимедиа, стремясь защитить свой контент от незаконного использования. Это не привлекает внимания, в отличие от чистой криптографии. Анализ тенденций в цифровой стеганографии показывает, что в ближайшие несколько лет интерес к разработке своих методов будет расти все больше и больше.

СПИСОК ЛИТЕРАТУРЫ

1. Рибунин В.Г., Оконов И.Н., Туринцев И.В. Цифровая стеганография. – М.: Солон-Пресс, 2002. – 272 с.
2. Хорошко В.О., Азаров О.Д., Шелест М.Э., Основы компьютерной стеганографии: Учебное пособие для студентов и аспирантов. – Винница: ВДТУ, 2003. – 143 с.
3. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография: Теория и практика И: "МК-Пресс" 2006. с. 283.
4. Marks, W.B., Dobbela, W.H. & MacNichol, E.F. Visual pigments of single primate cones. Science (1964) 143:1181—1183.

УДК 004.056.53

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАЩИЩЕННОСТИ ОСУЩЕСТВЛЕНИЯ ФИНАНСОВЫХ ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ БЕСКОНТАКТНОЙ ОПЛАТЫ

Ганчикова Юлия Сергеевна, Курышева Алена Андреевна
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский пр., 49,
emails: yul7494582@yandex.ru, kuryшева.al@yandex.ru

Аннотация: В статье приведен анализ защищенности операций с использованием технологий бесконтактных платежей. Рассмотрены принципы работы технологий и обеспечения безопасности бесконтактных расчетов.

Ключевые слова: финансовая безопасность; бесконтактные платежи; NFC; транзакции; защита.

COMPARATIVE ANALYSIS OF FINANCIAL TRANSACTIONS SECURITY USING CONTACTLESS PAYMENT TECHNOLOGIES

Ganchikova Yulia, Kuryшева Alena
St. Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronverksky Pr. 49,
emails: yul7494582@yandex.ru, kuryшева.al@yandex.ru

Abstract: The article presents analysis of security transactions using contactless payment technologies. The article considered the principles of work of technologies and provision of security of contactless calculations.

Keywords: financial security; contactless payments; NFC; transaction; security.

Введение. В настоящее время технологии бесконтактной оплаты используются всё более широко. В связи с этим вопрос защищенности бесконтактных технологий является крайне актуальным. От уровня защищенности напрямую зависит сохранность денежных средств и персональных данных.

Бесконтактная оплата может быть произведена с помощью карты или с помощью смартфона. Для сравнения технологий бесконтактной оплаты были использованы «MasterCard PayPass», «Apple Pay», «Samsung Pay» и «Android Pay». Технологии сравнивались по стандартам, идентификации, аутентификации, инструментам и дополнительной защите. Сравнительный анализ показал, что в первую очередь различаются данные необходимые для аутентификации и идентификации пользователя.

Заключение. На основе сравнительного анализа можно сделать вывод, что каждая из рассмотренных технологий и систем проведения платежа имеет ряд особенностей. Введение дополнительного уровня безопасности обеспечивает более эффективную защиту транзакций. Для повышения уровня защищенности технологий бесконтактной оплаты и надежности хранения персональных данных следует уделить особое внимание использованию дополнительных системы защиты и повышенному уровню аутентификации.

СПИСОК ЛИТЕРАТУРЫ

1. Никонец О. Е., Гринь И. А., Марченко А. В. Бесконтактные платежи: история возникновения и безопасность // Научно-методический электронный журнал «Концепт». – 2016. – Т. 15. – С. 2726–2730. – URL: <http://e-koncept.ru/2016/96466.htm> (дата обращения: 16.09.2017).
2. О мерах безопасного использования банковских карт [Электронный ресурс] : Письмо ЦБР от 2 октября 2009 г. №120-Т. Доступ из справ.-правовой системы «Гарант».
3. О национальной платежной системе [Электронный ресурс] : федер. закон Рос. Федерации от 27 июня 2011 г. №161-ФЗ : принят Гос. Думой 14 июня 2011 г. : одобр. Советом Федерации 22 июня 2011 г. (ред. от 18.07.2017). Доступ из справ.-правовой системы «КонсультантПлюс».

УДК 4.056

МЕТОДЫ И СТРАТЕГИИ ОПОВЕЩЕНИЯ НАСЕЛЕНИЯ ОБ УГРОЗАХ ВОЗНИКНОВЕНИЯ КРИЗИСНЫХ СИТУАЦИЙ

Гераськина Вероника Сергеевна, Сахаров Дмитрий Владимирович, Пестов Игорь Евгеньевич, Виткова Лидия Андреевна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Россия, 193232, Санкт-Петербург, пр. Большевиков 22,
emails: geraskinaVeronika@yandex.ru, d.sakharov@rkn.gov.ru, pestovie@outlook.com, iskinlidia@gmail.com

Аннотация: Развитие проекта «умный город» и внедрение комплексных систем безопасности безусловно является положительной тенденцией. Одновременно с этим, действующие системы

оповещения населения об угрозах возникновения кризисных ситуаций целесообразны, решают вопросы оповещения. Авторы предполагают, что действующие способы оповещения все же требуют улучшения с учетом текущих требований информационной сферы государства. Возможно исследование информационной сферы объекта на примере города поможет выявить пути развития и обновления текущих систем оповещения.

Ключевые слова: *Безопасный город, система «Умный город», кризисные ситуации, информационная сфера, информационное поле*

TECHNIQUES AND STRATEGIES FOR ALERTING THE PUBLIC ABOUT THE THREATS OF CRISIS SITUATIONS

VeronikaGeraskina, Dmitry Saharov, Igor Pestov, LidiyaVitkova
Federal State Budget-Financed Educational Institution of Higher Education The Bonch-Bruевич Saint -
Petersburg State University of Telecommunications,
Russia, Saint-Petersburg, ProspektBolsheviko, 22 – 1,
emails: geraskinaVeronika@yandex.ru, d.saharov@rkn.gov.ru, pestovie@outlook.com,
iskinlidia@gmail.com

Abstract: The development of the project "smart city" and implementation of integrated security systems is certainly a positive trend. At the same time, the existing system of warning the population about the threats of crisis situations is appropriate, decide the issues of the alert. The authors suggest that current methods of notification are still in need of improvement based on the current requirements of the information domain of the state. It is possible to study the information sphere of the object on the example of the city will help to identify the development and updates of current warning systems.

Keywords: *Safe city, "Smart city", crisis, information field, information field*

Сегодня одним из актуальных вопросов в развитии государственных информационных систем становится развитие комплексных систем безопасности, в том числе развитие проекта "Безопасный город". В числе первых городов России, попавших под модернизацию, одновременно с Москвой и Казанью стал Санкт-Петербург.

Городская структура для корректного взаимодействия ее составляющих между собой требует создания специализированной информационной системы, в роли которой и выдвигается "Безопасный город". Таким образом, проект «Безопасный город» – это программный-аппаратный комплекс с применением видеоаналитических решений, созданный с целью помочь быстро определять и оперативно реагировать на всякого рода нештатные ситуации, а также вовремя предпринимать меры по устранению их последствий.

В Санкт-Петербурге реализуется масштабный проект по внедрению «умных систем» в области обеспечения безопасности и рационального управления городским коммунальным хозяйством. Представитель Комитета по информатизации и связи Санкт-Петербурга в своем интервью сообщал, что smart-подходы используются во многих сферах деятельности города, охвачены такие сферы, как комплексная безопасность, благоустройство города, инженерные энергетические сети, жилищно-коммунальное хозяйство, транспорт и др. Утверждается, что результатом применения данных систем должна стать интеллектуальная интегрированная система, позволяющая управлять городом как единым целым [1].

Сейчас в Санкт-Петербурге уже можно наблюдать реализованные проектные решения, такие как "умная остановка", система оповещения с учетом информации о человекопотоке у стадиона "Санкт-Петербург", охват Wi-Fi сетью метрополитена, а так же некоторого наземного общественного транспорта, мостов и некоторых зон, в которых находясь камеры наблюдения, системы отслеживания транспорта, различного вида информационные табло (в черте города и на ЗСД/КАД), интеллектуальная система подземных коллекторов «Водоканала», «умные светофоры», различные терминалы экстренной связи «Гражданин-Полиция» и многое другое.

Большинство из вышеуказанных объектов, входящих в систему "Безопасного города" возможно использовать для оповещения граждан о наступлении ЧС с помощью трансляции необходимой информации. При этом, к более привычным методам оповещения граждан мы можем отнести такие системы, как централизованное оповещение с использованием РАСЦО (электросирены, громкоговорители), цифровое и спутниковое теле- и радиовещание, оповещение с использованием таксофонов и оповещение в метрополитене. В обиход вошло использование ТФОП, а также SMS-рассылка (МЧС-Информер).

В своем исследовании на тему методы и стратегии оповещения населения об угрозах возникновения кризисных ситуаций обращаются к статистике.

Прежде всего, обращает на себя внимание тот факт, что более 70% населения имеют при себе постоянно свои мобильные устройства (смартфоны, планшеты и иные девайсы). По итогам исследований рейтинговых агентств выяснилось, что люди возрастной категории от 16 до 24 лет тратят более 3,5 часов в сутки на серфинг с мобильного телефона [2]. В свою очередь все активные

мобильные пользователи, по словам Главы PayPal в России Владимира Малюгина имеют контакт со своим устройством около 200 раз и более в день. При этом более 50% пользователей создают и оценивают посты в социальных сетях, и более 60% находятся в постоянной переписке [3].

Руководитель интернет-проектов TNS Russia ТНСС Ишункина презентовала данные о потреблении информации с различных устройств. Исследования показали, что количество интернет-пользователей, использующих смартфон для выхода в интернет, выросло на 44%, а пользователей планшета стало на 33% больше. Около 22% времени пользователи мобильных устройств тратят на те функции, ради которых они его приобрели, около 15% времени проводят в социальных сетях, 12% времени тратят на браузеры [4].

Далее перечислим наиболее популярные по посещаемости сайты на смартфонах и планшетах:

1. ВКонтакте,
2. Google,
3. YouTube,
4. Яндекс,
5. И соответственно мобильные приложения:
6. 2Gis,
7. Google,
8. YouTube;
9. ВКонтакте,
10. Viber,
11. Яндекс,
12. Instagram,
13. Mail.ru,
14. WhatsApp,
15. Skype.

В связи с этим авторы предполагают, что современное общество находится в несколько ином информационном поле, данные в котором потребляются в основном из сети "Интернет" или различных мессенджеров, чем используют современные средства оповещения. Следовательно, развитие систем оповещения граждан нужно направить именно на данную сферу, определив несколько корректных способов.

Большое количество Интернет браузеров размещает важную новостную информацию на своих страницах, но достаточно ли этого для оповещения граждан, вопрос остается открытым. Необходимо правильно подавать информацию и учитывать воздействие психологических факторов на население, и в таких случаях можно использовать социальные сети для размещения информации о ЧС или о предупреждении, создавать различные программы вредоносного типа (баннеры), позволяющие донести информацию до пользователей.

Одновременно с этим стоит обратить внимание на то, что аудио пространство сети "Интернет" также можно задействовать. Уже сейчас различные музыкальные сайты, а также социальные сети периодически вставляют рекламные аудио записи в треки и фильмы. Таким образом, наравне с этим можно заполнять так называемый эфир при необходимости важными сообщениями [5]. Однако, не стоит забывать, что данный способ можно использовать и как элемент пагубного воздействия, вводя пользователей в панику и, тем самым, создавая еще худшую ситуацию.

Выводы.

Внедрение комплексных систем безопасности и развитие проекта «умный город» очень положительная тенденция. При этом системы оповещения населения об угрозах возникновения кризисных ситуаций, действующие в населенных пунктах, целесообразны, решают вопросы оповещения, но способы оповещения все же требуют улучшения с учетом текущих требований информационной сферы государства [6]. Авторы предполагают, что исследование информационной сферы объекта на примере города поможет выявить пути развития и обновления текущих систем оповещения.

СПИСОК ЛИТЕРАТУРЫ

1. Основные тенденции развития ИТ в России обсудили на форуме «IT Диалог 2016»// Режим электронного доступа: <http://kis.gov.spb.ru/news/2016-06/27--osnovnye-tendencii-razvitiya-it-v-rossii-obsudili/> (дата обращения 22.09.2017);
2. Медиапотребление в России выросло до 8,5 часа // Режим электронного доступа: <https://iz.ru/news/587641> (дата обращения 22.09.2017);
3. Владимир Малюгин, PayPalRussia: Российский пользователь — продвинутый, разницы с Европой и США мы не видим// Режим электронного доступа: http://json.tv/ict_video_watch/paypal_russia-vladimir_malyugin-e-commerce--20150824061338 (дата обращения 22.09.2017);
4. Сахаров Д.В. Проблема автоматизированного мониторинга графических изображений в сети интернет/ Сахаров Д.В., Жувикин А.Г., Виткова Л.А.// Защита информации. Инсайд. 2017. № 2 (74). С. 64-67;
5. Технические аспекты управления с использованием сети интернет /Алейников А.А., Билятдинов К.З., Красов А.В., Кривчун Е.А., Крысанов А.В. Монография / Санкт-Петербург, 2016;
7. Инновационное управление рисками информационной безопасности /Андрианов В.И., Красов А.В., Липатников В.А. / учебное пособие / Федеральное агентство связи, Федеральное гос. образовательное бюджетное учреждение высш. проф. образования "Санкт-Петербургский гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича". Санкт-Петербург, 2012.

УДК 4.056

КОНВЕРГЕНЦИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМ ПРОСТРАНСТВОМ САНКТ-ПЕТЕРБУРГА

Головлёва Юлия Андреевна, Виткова Лидия Андреевна, Ковцур Максим Михайлович, Дмитриева Екатерина Викторовна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Россия, 193232, Санкт-Петербург, пр. Большевиков 22,
emails: golovlyova96@mail.ru, iskinlidia@gmail.com, maxkovzur@mail.ru,
dmitrieva.ekaterina94@gmail.com

Аннотация: Система «Умный город Санкт-Петербург» в перспективе безусловно может повысить качество жизни горожан, сделать её более комфортной и безопасной. Однако такой сложной и всеобъемлющей системе необходима комплексная и актуальная защита информации. Авторы статьи предполагают, что в процессе конвергенции информационных технологий с точки зрения эффективного управления городом необходимо учитывать вопросы информационной безопасности. Требуется построить имитационную модель нарушителя в системе «Умный город» и с учетом полученных данных планировать развитие и внедрение новых инновационных решений.

Ключевые слова: Система комплексной безопасности, система «Умный город», киберпреступление, кибератака, взлом, сети, модель нарушителя

THE CONVERGENCE OF INFORMATION TECHNOLOGIES FOR INCREASE OF EFFICIENCY OF MANAGEMENT OF THE INFORMATION SPACE OF ST. PETERSBURG

Ulia Golovleva, Lidiya Vitkova, Maksim Kovcur, Ekaterina Dmitrieva

Federal State Budget-Financed Educational Institution of Higher Education The Bonch-Bruевич Saint-Petersburg State University of Telecommunications, Russia, Saint-Petersburg, Prospekt Bolshheviko, 22
emails: golovlyova96@mail.ru, iskinlidia@gmail.com, maxkovzur@mail.ru,
dmitrieva.ekaterina94@gmail.com

Abstract: The "Smart city of Saint-Petersburg" in the future will definitely enhance the quality of life of citizens, to make it more comfortable and safe. However, such a complex and comprehensive system requires a comprehensive and up to date. The authors suggest that the process of convergence of information technology with effective management of the city must consider the information security issues. It is necessary to construct a simulation model of the intruder in the system "Smart city" and taking into account the obtained data to plan the development and implementation of innovative solutions.

Keywords: System integrated security system "Smart city", cybercrime, cyber attack, hacking, network, model of the offender

Введение. Постановлением Правительства Санкт-Петербурга от 26.01.2016 № 52 в Санкт-Петербурге создана Межведомственная комиссия по разработке и реализации проекта «Умный город Санкт-Петербург» [1]. Сама система «Умный город» создана с целью повышение качества жизни петербуржцев, а также обеспечения интенсивного взаимодействия горожан с органами власти. Поэтому основной функционал в системе направлен на современное качественное управление городским хозяйством. Основной задачей проекта «Умный город» является повышение связанности между существующими системами города, повышение их надежности и интеллектуальности. Согласно требованиям Постановления безопасность, комфорт и оперативность становятся отправными точками, с которых и начинается «Умный город». И конечно, же в первую очередь «Умный город» должен обеспечить безопасность и комфорт жизни горожан, именно поэтому авторы рассматривают его со стороны информационной безопасности.

Анализ.

Сейчас в рамках системы «Умный город Санкт-Петербург» создаётся открытая сеть Wi-Fi, которая сегодня уже охватывает историческую часть города, где особенно велик туристический трафик: весь Невский проспект, большую часть Центрального района, практически весь Петроградский остров, восточную часть Васильевского острова, часть Аптекарского острова. К настоящему моменту установлено более 400 точек доступа со средним радиусом зоны обслуживания 120 метров, которые покрывают более 3,5 квадратных километра. В будущем зона свободного Wi-Fi в городе будет расширена до 10 квадратных километров. В метрополитене также продолжаются работы по созданию свободной Wi-Fi сети [2].

Одновременно с этим стоит отметить, что свободные Wi-Fi сети могут использоваться и злоумышленниками. Взломав сеть или, например, используя метод атаки посредника (создаётся «двойник» точки доступа в сеть, и жертва сама подключается к ней), злоумышленник может украсть конфиденциальную информацию, заразить устройство вредоносным ПО или использовать публичную точку для пропаганды в рамках информационных войн. Так, в марте 2016 пассажиры московского метрополитена сообщили о появлении изображения флага «Исламского государства» (запрещенная в

России организация) при попытке пройти авторизацию во время подключения к Wi-Fi сети. Таким образом внедряя современные технологии, повышая уровень взаимосвязи между городом и его жителями мы сами создаем новые уязвимости с точки зрения информационной безопасности.

Конечно же, эффективное управление транспортной инфраструктурой – одно из основных направлений деятельности при создании «умного города». Сегодня спутниковые навигационные технологии – это ключевая часть построения интеллектуальных транспортных систем городов, они позволяют решать проблему автомобильных заторов, управлять важнейшими транспортными узлами, обеспечивать профилактику ДТП, оптимизировать транспортные потоки, намечать пути развития транспортной инфраструктуры. В настоящее время создается государственная информационная система Санкт-Петербурга «Центр навигационно-информационного обеспечения» ИОГВ с применением спутниковых навигационных технологий ГЛОНАСС, ГЛОНАСС/ГНСС, геоинформационных и веб-технологий. Особое внимание уделяется созданию и развитию Единого навигационного центра Санкт-Петербурга как составной части ЦНИО. Дальнейшее развитие Единого навигационного центра Санкт-Петербурга предусматривает, в частности, работы по созданию и внедрению информационно-навигационных систем на основе технологий ГЛОНАСС, реализующих функции мониторинга и диспетчеризации автотранспортных средств городских и районных ИОГВ, мониторинга и предоставления сведений о состоянии и местоположении транспортных средств.

Вопросы информационной безопасности по-прежнему остаются открытыми, так 5 декабря 2016 года Указом Президента Российской Федерации была утверждена новая Доктрина информационной безопасности Российской Федерации, согласно которой состояние информационной безопасности характеризуется тем, что постоянно повышается сложность, увеличивается масштаб и скоординированность компьютерных атак на объекты критической информационной инфраструктуры. [3]. Транспортная инфраструктура города безусловно является критически важным объектом, и информатизация системы повышает количество возможных угроз информационной безопасности.

Ещё одним новшеством «Умного города» является Единый центр управления транспортом и объектами транспортной инфраструктуры, который должен появиться на месте нынешнего наземного вестибюля станции «Фрунзенская». Из Единого центра будет в режиме реального времени производиться мониторинг работы всего транспортного комплекса Петербурга, обеспечиваться взаимодействие и координация разных видов общественного транспорта. Специалисты смогут получать прогнозы транспортной ситуации в разных районах города, а также оперативно реагировать на возникновение нештатных ситуаций. Система «умного светофора» со встроенными видеодетекторами будет управлять транспортными потоками, увеличивая или уменьшая длительность зелёного сигнала для автомобилей.

С точки зрения безопасности, специалистам важно, прежде всего, защитить центр мониторинга и систему от возможных кибератак. Так отключение даже одного светофора грозит пробками и возникновением опасной ситуации на дороге. Взлом подобной системы может привести к транспортному коллапсу во всём городе: не только на земле, но и в метрополитене. Система оповещения может быть использована для пропаганды или создания паники негативными новостями. Теоретически возможно сокрытие информации об авариях или ремонтных работах на информационных табло, что также может привести к крупным пробкам или транспортному коллапсу.

Сейчас в городе установлено более 20 тысяч камер видеонаблюдения. Система городского видеонаблюдения также является одним из главных направлений в проекте «Умный город». Благодаря единой системе видеонаблюдения ни одно дорожно-транспортное происшествие или противоправное действие, совершаемое в Санкт-Петербурге и попавшее в зону охвата видеокамеры, не останется незамеченным. Событие попадает в объектив видеокамеры, после чего информация в режиме реального времени поступает на монитор оператора, который фиксирует событие, а также на серверы-видеорегистраторы для последующего хранения. По запросу, в случае необходимости, информация с городских видеокамер может быть предоставлена сотрудникам полиции, МЧС, ФСО или представителям органов власти. В случае происшествия любой петербуржец может оставить заявку на сохранение видеоархива и течение 7 дней и обратиться в полицию для его выдачи. При этом несанкционированный доступ к системе видеонаблюдения предоставляет возможность следить за всем городом, например, для установления времени и места крупного скопления людей. А также взлом системы может вывести из строя все видеокамеры.

Выводы. Система «Умный город Санкт-Петербург» в перспективе безусловно может повысить качество жизни горожан, сделать её более комфортной и безопасной. Однако такой сложной и всеобъемлющей системе необходима комплексная и актуальная защита информации. С развитием городских технологий развиваются также и технологии злоумышленников, которые могут быть направлены на взлом и перехват управления системой «Умный город». Поэтому безопасность системы должна постоянно повышаться, закрывая возможные уязвимости и не оставляя возможности её взломать. И в случае успешного взлома необходимо максимально быстро восстановить штатный режим работы системы. Конвергенция в телекоммуникациях сейчас используется как понятие раскрывающее процесс объединения услуг (в сетях), авторы данной статьи предполагают, что в процессе конвергенции информационных технологий с точки зрения эффективного управления

городом необходимо учитывать вопросы информационной безопасности. Требуется построить имитационную модель нарушителя в системе «Умный город» и с учетом полученных данных планировать развитие и внедрение новых инновационных решений [4, 5].

СПИСОК ЛИТЕРАТУРЫ

1. Постановление Правительства Санкт-Петербурга от 26 января 2016 г. N 52 "О Межведомственной комиссии по разработке и реализации проекта "Умный город Санкт-Петербург" при Правительстве Санкт-Петербурга" // Система ГАРАНТ: URL: <http://base.garant.ru/43401594/#ixzz4t8GS8uBq>
2. Бесплатный Wi-Fi в Петербурге подрос на три квадратных километра // URL: <http://www.iksmedia.ru/news/5375824-Besplatnyj-WiFi-v-Peterburge-podros.html#ixzz4t8GzGt7M>
3. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895) // Система ГАРАНТ. URL: <http://base.garant.ru/182535/#ixzz4t8HQ14Wu>
4. Герлинг Е.Ю. Модели нарушителей информационной безопасности / Герлинг Е.Ю., Кулишкина Е.И., Бирих Э.В., Виткова Л.А. // Известия высших учебных заведений. Технология легкой промышленности. 2017. Т. 1. С. 27-30.
5. Донской Д.М. Некоторые аспекты модели нарушителя информационной безопасности в интернете вещей / Донской Д.М., Рябова О.Н., Сахаров Д.В., Виткова Л.А. // В сборнике: Интернет вещей и 5G 2016. С. 47-50.

УДК 004.42

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ВЕБ-СЕРВЕРА PYTHON-ПРИЛОЖЕНИЙ ДЛЯ РАЗМЕЩЕНИЯ НА КЛИЕНТСКИХ МАШИНАХ

Грибачев Виталий Петрович, Харитонов Георгий Дмитриевич
Санкт-Петербургский государственный университет телекоммуникаций «СПбГУТ»,
Россия, Санкт-Петербург, наб.р. Мойки, 23,
emails: y270166@yandex.ru, haritonov67273@gmail.com

Аннотация: В статье рассмотрены некоторые особенности защиты информации при разработке веб-приложения с распределенной структурой и серверной частью, так же выполняющейся на клиентских машинах

Ключевые слова: *распределенные вычисления; P2P-сети; защита веб-серверов; Python-приложения*

SECURING THE PYTHON APPLICATION WEB SERVER FOR DEPLOYMENT ON CLIENT MACHINES

Gribachev Vitaliy, Kharitonov Georgiy
The St. Petersburg State University of Telecommunications "SPbGUT",
Russia, St. Petersburg, Moyki str. 23,
emails: y270166@yandex.ru, haritonov67273@gmail.com

Abstract: The article presents some features of information protection are considered when developing a web application with distributed structure and server part running on client machines

Keywords: *distributed computing; P2P networks; protection of web servers; Python applications*

Введение. Программная защита веб-серверов всегда беспокоила системных администраторов и разработчиков. Однако, универсального решения, которое смогло бы защитить любую систему от атак злоумышленников, до сих пор нет, поэтому это является актуальной задачей и в сегодняшний день.

При построении веб-сервера, который смог бы обеспечить достаточную защиту для распространения данного ПО на пользовательских машинах, к выбору сервера для Python-приложений необходимо подойти с особым вниманием. Анализ предоставляемых свободных решений для размещения приложений показал необходимость использования стандарта WSGI, который обеспечивает совместимость веб-сервера и приложения на Python. Данный стандарт так же определяет возможность наличия middleware-сервиса, который может являться промежуточным звеном в данной цепи. Таким образом, возможно, настраивать и разворачивать веб-сервера, которые будут отвечать пользовательским запросам производительности и быстродействия.

Выбор веб-сервера для приложения в данном случае является не тривиальной задачей. Исходя из специфики структуры сервиса, складываются следующие технологические требования: легковесность, простота в настройке и управлении, малое потребление ресурсов компьютера, масштабируемость, возможность выдерживать высокие нагрузки и своевременно обрабатывать запросы пользователей. Под данные критерии был выбран веб-сервер CherryPy. Данное решение является минималистичным, поставляемым без большого числа готовых компонентов, сервером приложений Python, а также удобным фреймворком, предоставляющим интерфейс для взаимодействия приложения и сервера. И хотя веб-сервер CherryPy может обслуживать статические файлы вместе с ответами от приложений, для балансировки нагрузок лучше установить инвертированный прокси-сервер Nginx, который будет обслуживать эти файлы и управлять соединениями (запросами). Обработывая запросы от клиентов, это существенно снизит нагрузку на сервер приложений, и тем самым улучшит общую производительность, увеличив число возможных

одновременных соединений. Nginx так же является нетребовательным к ресурсам машины клиента и не занимает много места на жестком диске. Таким образом, была подобрана оптимальная связка из двух серверов, где Nginx будет обрабатывать запросы пользователей и обслуживать статические файлы, вроде JavaScript, CSS, изображений, и CherryPy для обработки ответов от приложения Python.

С учетом распределенной архитектуры приложения многие типы атак на веб-сервера будут иметь меньшие масштабы, нежели у приложений с клиент-серверной архитектурой, однако при этом не теряют значимости, к тому же, добавляются и новые факторы риска и угрозы безопасности. Например, пользователь, не знакомый с администрированием веб-сервера и имеющий небольшой опыт, может по случайности или за незнанием нарушить работу сервиса и/или повредить пользовательские данные. Поэтому, безопасности следует уделить особое внимание. Так же, в связи с увеличением сложности поставляемого ПО, следует учесть и возможный рост количества уязвимостей системы. Одними из наиболее распространенных типов угроз безопасности веб-сервера на сегодняшний день являются атака типа обратный путь в директориях или «Path Traversal», которая направлена на получение доступа к файлам, директориям и командам, находящимся вне основной директории веб-сервера и внедрение операторов SQL («SQL-инъекции»), направленная на хищение и/или уничтожение пользовательской информации. Некоторых типов атак можно избежать при правильной настройке веб-сервера. Тогда, задача разработчика будет состоять в том, чтобы максимально автоматизировать конфигурацию сервера и предоставить наиболее удобный и простой интерфейс для пользователя.

Однако, не смотря на количество возросших угроз безопасности веб-сервера, так же открываются и новые возможности по его защите, которые были бы невозможны при клиент-серверной архитектуре. Например, для того чтобы ограничить доступ к веб-серверу, тем самым значительно сократив вероятность атаки типа отказ в обслуживании («DOS-атаки»), в некоторых случаях имеет смысл предоставлять доступ к веб-серверу только внутри локальной сети, в которой он находится.

При внедрении веб-сервера на клиентские машины необходимо использовать уже известные методы сокрытия информации и пресечения несанкционированного доступа, принимая во внимание, что помимо стандартных угроз безопасности, появляются специфичные, связанные с распределенной структурой приложений, когда владелец сервера является одновременно и пользователем. В данном случае, надо предоставить пользователю готовый для развертывания набор возможностей, который уже будет включать в себя необходимые средства для обеспечения безопасности, при этом, не заставляя его самостоятельно конфигурировать веб-сервер и устанавливать стороннее ПО. Так, например, с данным веб-сервером можно поставлять: встроенные возможности аутентификации и авторизации пользователей, контроль сессий пользователей, защиту СУБД, возможности аудита системы, шифрования трафика и хранящихся данных на сервере, а также предоставлять автоматизированную конфигурацию веб-сервера или предоставлять пользователю простой интерфейс, при невозможности полностью автоматизировать процесс.

Заключение. Говоря о правильном, с нашей точки зрения, построении защиты разрабатываемой системы, необходимо придерживаться такого подхода, который бы равнозначно распределял внимание на каждом уровне безопасности. Потенциальная угроза может возникнуть даже от самого пользователя, который не слишком аккуратен или не имеет достаточного опыта работы с серверами. Учитывая специфику разрабатываемого ПО, а также большое разнообразие пользовательских требований к его возможностям, стоит обеспечить такую защиту от атак различного рода, которая будет отвечать современным критериям безопасности для веб-серверов, но при этом не потребует от пользователя знаний разработки или устройства системы.

СПИСОК ЛИТЕРАТУРЫ

1. Грибачев В.П., Харитонов Г.Д. Распределенные сети P2P нового поколения. - АПИНО 2017, 2017, 5с.
2. Positive Technologies Как хакеры атакуют веб-приложения: боты и простые уязвимости // SECURITYLAB.RU: информационный портал. 2017. URL: <http://www.securitylab.ru/analytics/485977.php>

УДК 004.056

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ОДНОРАЗОВОГО БЛОКНОТА ДЛЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ ПОТОКОВ БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА

Грозов Владимир Андреевич

Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский пр., 49,
email: vladimirgrozov@mail.ru

Аннотация: В докладе рассмотрены особенности и возможности использования шифрования методом одноразового блокнота применительно к защите информационных потоков, возникающих в процессе эксплуатации беспилотного летательного аппарата. Обсуждаются риски, возможные при

использовании широко распространенных алгоритмов шифрования. Приведены перспективные направления развития схемы одноразового блокнота.

Ключевые слова: беспилотный летательный аппарат; одноразовый блокнот; псевдослучайная последовательность; шифрование

PROSPECTS OF ONE-TIME PAD USAGE FOR PROTECTION OF UNMANNED AERIAL VEHICLE DATA STREAMS

Grozov Vladimir

ITMO University,

Russia, St. Petersburg, Kronverksky Pr. 49,

e-mail: vladimirgrozov@mail.ru

Abstract: The article presents the features and capabilities of the encryption method based on one-time pads for protection of information flows that occur in the process of operation of unmanned aerial vehicle. The risks that are possible when using common cryptographic algorithms are discussed. The promising directions of a one-time pad scheme development are represented.

Keywords: one-time pad; unmanned aerial vehicle; pseudorandom sequence; encryption

Введение. Защита информационных потоков, возникающих при эксплуатации беспилотного летательного аппарата (БЛА), является сегодня очень актуальной задачей, поскольку несанкционированное вмешательство в его систему управления может привести к серьезному ущербу, вплоть до потери аппарата. Особенностями БЛА является передача по слабо защищенному от перехвата радиоканалу, а также ограниченные вычислительные ресурсы.

Ценность любой содержательной информации в современных условиях очевидна, и так же очевидны все возрастающие усилия заинтересованных сторон, направленные на завладение ею. Риск несанкционированного доступа усугубляется серьезной поддержкой нелегального сбора информации со стороны определенных структур, в том числе и государственных. На разработчиков программного обеспечения и соответствующего оборудования оказывают давление с тем, чтобы уже на этапе разработки предусматривались уязвимости в программных продуктах и устройствах [1]. В результате многие широко распространенные алгоритмы шифрования уже скомпрометированы, и, вполне возможно, что и остальные шифры ждет та же участь. Кроме того, приближается эра квантовых компьютеров, имеющих несопоставимо более высокую, по сравнению с обычными, скорость обработки данных. Это может сделать уязвимыми классические алгоритмы шифрования, построенные на принципе невозможности дешифрования за приемлемое время. В настоящее время стоимость действующих моделей квантовых компьютеров крайне высока из-за технических трудностей при обеспечении их нормальной эксплуатации. В результате может сложиться определенный дисбаланс: мощности, используемые для дешифрования, могут оказаться намного большими, чем мощности шифрования. По названным причинам растет интерес к совершенным шифрам, в том числе к одноразовому блокноту (шифру Вернама).

Одноразовый блокнот (ОБ) представляет собой набор однократно используемых ключевых последовательностей (страниц) размером не меньшим, чем длина шифруемого сообщения. Шифрование заключается в наложении ключа на открытый текст с помощью операции XOR. Шифр Вернама обладает двумя важными особенностями: абсолютной криптостойкостью (теоретически доказанной для истинно случайной ключевой последовательности) [2] и более высокой по сравнению с другими шифрами скоростью работы.

Последнее свойство ОБ достигается за счет предельной простоты алгоритма шифрования и разделения во времени подготовки шифроблокнота и самого процесса шифрования. Это является серьезным преимуществом при работе в системах реального времени, к которым относится БЛА. При практической реализации такого шифрования наиболее сложной задачей является создания ключа (шифроблокнота), который должен представлять собой последовательность равновероятных, не зависящих друг от друга символов. В настоящее время активно используются и развиваются как подходы, основанные на классических генераторах псевдослучайных последовательностей, так и новые варианты генерации с применением квантовых, фрактальных, нейросетевых, генетических и других биоинспирированных алгоритмов [3–6]. Проводятся также теоретические исследования, расширяющие в определенных условиях область доказательной абсолютной стойкости ОБ [7].

Технические вопросы, связанные с быстрой генерацией качественного шифроблокнота большого объема, его хранения и передачи на БЛА, в настоящее время успешно разрешаются за счет использования мощных и доступных графических процессоров (распараллеливание процессов), современных быстрых флэш-накопителей.

Заключение. Анализ текущего состояния в области исследований и применения ОБ показывает, что такая система шифрования жизнеспособна, активно развивается и имеет хорошие перспективы применения в будущем.

СПИСОК ЛИТЕРАТУРЫ

1. Bernstein D.J., Lange T., Niederhagen R. Dual EC: A Standardized Back Door. / In: Ryan P., Naccache D., Quisquater J.J. (eds) The New Codebreakers. Lecture Notes in Computer Science. – Berlin: Springer, 2016. Vol. 9100. P. 256-281.
2. Shannon C.E. Communication theory of secrecy systems // Bell Syst. Tech. J. 1949. Vol. 28. P. 656–715.
3. Бурлов С.А., Горохов А.В. О возможности защиты квантового канала связи на состояниях орбитального углового момента фотонов // Сб. тр. конф. «Актуальные проблемы обеспечения информационной безопасности». 2017. С. 69-73.
4. Кулешов С.В. Фрактальное шифрование // ТРУДЫ СПИИРАН. 2004. Том 1. №2. С. 231-235.
5. Юрьев Р.А. Обзор моделей нейрокриптографии // Вестник научных конференций. 2015. № 4-2 (4). С. 160-164.
6. Сергеев А.С. Применение бионических информационных технологий для решения задач классического, асимметричного и блочного криптоанализа // Сб. материалов XI Международной конф. по неравновесным процессам в соплах и струях (NPNJ'2016). 2016. С. 457-459.
7. Ryabko B. The Vernam cipher is robust to small deviations from randomness // Problems of Information Transmission. 2015. Vol. 51. No. 1. P. 82-86.

УДК 621.392

АНАЛИЗ ПРОТОКОЛОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИОТ-СРЕДЕ

Долгун Владислав Олегович, Литвинов Владислав Леонидович
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
Россия, Санкт-Петербург, пр. Большевиков, 22/1
emails: dolgun.vlad@mail.ru, vlad.litvinov61@gmail.com

Аннотация: В статье рассматривается задача в развитии концепции Интернет вещей (IoT), а также обеспечение информационной безопасности в обширном спектре защиты от угроз злоумышленников. Рассмотрены основные протоколы обеспечения безопасного соединения на прикладном, транспортном, сетевом уровнях с проведением сравнительного анализа между ними. В статье приведен пример развития интеллектуальных устройств и рассмотрена проблема обеспечения безопасности, подчеркнута востребованность и необходимость изучения направления защиты Интернет вещей (IoT).

Ключевые слова: информационная безопасность; интернет вещей; TCP/IP; прикладной уровень; сетевой уровень; транспортный уровень

ANALYSIS OF INFORMATION SECURITY PROTOCOLS IN IOT-ENVIRONMENT

Dolgun Vladislav, Litvinov Vladislav
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
Russia, St. Petersburg, Bolshevikov pr. 22 \ 1
emails: dolgun.vlad@mail.ru, vlad.litvinov61@gmail.com

Abstract: The article deals with the problem in the development of the concept of Internet Things (IoT) are the provision of information security in a wide range of protection against the threats of intruders. The main protocols for providing secure connections at applied, transport, network levels are analyzed with a comparative analysis between them. The article gives an example of the development of intelligent devices and the problem of ensuring security, the need for and the need to study the direction of the protection of the Internet of things (IoT) is underlined.

Keywords: information security; Internet of Things (IoT); TCP / IP; application layer; network layer; transport layer

Введение. IoT – это концепция вычислительной сети физических предметов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей как явление, способное перестроить экономические и общественные процессы, исключаяющее из части действий и операций необходимость участия человека [1]. Таким образом, IoT – это среда, где объект может представлять себя, увеличиваться благодаря подключению к окружающим объектам и безграничным данным, которые протекают вокруг него. По словам 95 % опрошенных руководителей, их компании планируют запустить проекты, связанные с Интернетом вещей, в течение ближайших трех лет [2].

Основная проблема IoT устройств заключается в том, что идея сетевых устройств и других объектов относительно новая, безопасность не всегда учитывается при разработке продуктов. Продукты IoT продаются со старыми операционными системами и программным обеспечением. Зачастую покупатели не могут изменять пароли по умолчанию на IoT устройствах. Чтобы повысить безопасность устройства, которое имеет выход в интернет, необходимо его сегментировать в собственную сеть и ограничить выход из сети для каждого устройства. После чего сегмент сети должен отслеживаться для выявления аномального трафика и, при возникновении проблемы, необходимо вовремя принимать нужные решения.

Вопрос безопасности в IoT системе является важным и основополагающим аспектом, поскольку он направлен на взаимосвязь большого числа различных устройств между собой и Интернетом.

Устройства Интернет вещей генерируют и передают большой объем информации при значительном удалении друг от друга, что является угрозой для безопасности системы. Устройства могут иметь различные технологические и конструктивные исполнения, что может быть недостатком, так и достоинством. Так как, имея свою конструктивную и технологическую особенность, они могут быть адаптированы к одной области применения и вызвать проблему совместимости с другой системой. Для взаимодействия всех устройств требуется единая стандартизация. В качестве стандарта для взаимодействия умных объектов было предусмотрено использование протокола IP. Архитектура Интернет вещей должна придерживаться архитектуры IP, так как многие аспекты безопасности уже определены и используются для Интернета.

Использование всех протоколов не целесообразно и не является обязательным решением для обеспечения безопасности, поскольку нагрузка на устройство возрастает от количества используемых функций. Протокол прикладного уровня CoAP предназначен для использования в условиях ограниченных ресурсов в таких устройствах, как датчики, узлы беспроводных сетей, переключатели и компоненты, которые контролируются или отслеживаются через Интернет. Сам протокол построен по принципу «клиент-сервер» и не обеспечивает аутентификации и защиты персональных данных, в связи с этим защита должна быть обеспечена на прикладном или на нижних уровнях. Проверка данных и их целостность может быть обеспечена и на низких уровнях, таких как PHY и MAC, но никакая непрерывная безопасность не может быть гарантирована без высокого уровня доверия. Создание безопасности на основе PHY или MAC невозможно, так как между удаленными устройствами будет использоваться беспроводная коммуникация (multihop-routing), для обеспечения безопасности которой требуется использовать механизм безопасности на прикладном, транспортном и сетевом уровне.

IoT узел может осуществлять обмен данными на сетевом уровне, используя протокол IPSec, который обеспечивает конфиденциальность и целостность данных, проверку подлинности данных и предотвращает атаки повторного воспроизведения. Не стоит забывать, что безопасное соединение можно реализовать на транспортном уровне посредством протоколов TLS и DTLS. Протокол TLS работает поверх TCP. TLS обеспечивает полную безопасность, используя асимметричное и симметричное шифрование. В свою очередь IPSec и DTLS исполняют схожие функции безопасности своими собственными средствами, только на разных уровнях стека протоколов. Кроме того, соглашение о ключе Internet Key Exchange (IPSec IKE) показывает точно такую функцию взаимосвязи, как и DTLS.

Главное преимущество обеспечения безопасного соединения на транспортном уровне с использованием DTLS заключается в предоставлении более детального контроля доступа.

С точки зрения безопасности, одной из главных проблем DTLS и IPSec является то, что соединение на передачу данных от узла к узлу через промежуточные узлы не будет гарантировано, так как они не могут обеспечить целостность передачи. В связи с этим требуется рассматривать направление на обеспечение безопасности на уровне самого приложения.

Самый доступный и эффективный способ обеспечить защиту Интернет вещей для обычного пользователя – предоставить пользователю возможность изменять учетные данные своих интеллектуальных устройств. Чтобы направить пользователей к изменению учетных данных своих устройств Интернет вещей, производителям необходимо сделать создание уникального и надежного пароля обязательным во время первого подключения устройства к сети. Это не выход, но даже простая смена логина и пароля с заданных по умолчанию может серьезно снизить шанс взлома устройства. Другая возможность – это создание производителем на заводе уникальных и случайных паролей, содержащих буквы, цифры и символы для каждого устройства. Не менее важной задачей является выпуск обновления программного обеспечения устройства или прошивки, которые помогут устранить уязвимости, найденные в ходе эксплуатации. Зачастую производители используют устаревшие версии библиотек, для взлома которых существуют множество инструментов, что делает устройства беззащитным перед DDoS-атакой (Distributed Denial of Service). Защита IoT устройств позволяет обеспечить не только конфиденциальность пользователя, но и помогает избежать DDoS-атаки, а также предотвратить более серьезные последствия. Заразив одно устройство, можно заразить целую сеть устройств, с которым контактирует зараженное устройство.

Заключение. Если верить прогнозу развития устройств IoT, то само развитие экспоненциально, и, согласно оценкам, к 2020 году будет насчитываться свыше 50 миллиардов устройств, подключенных к Интернету [3]. При таком быстром росте встает вопрос безопасности устройств в случае отсутствия процессов, которые обеспечивают целостность и шифрование передаваемых данных. Все сведения, которые хранят устройства IoT, являются востребованными, так как могут показать последовательность событий и привычки пользователя. Наличие баз данных такого содержания является полезным для различных компаний, которые могут направить свои ресурсы на изготовление нужных товаров и услуг под конкретного пользователя, не говоря уже о том, что будет, если такие данные попадут в руки киберпреступников. Единственное, что может помочь свести к минимуму проблемы – это использование сертифицированного оборудования и специальные системы защиты, которые шифруют загружаемые и сохраненные данные в облачном хранилище.

СПИСОК ЛИТЕРАТУРЫ

1. Леонид Черняк. Платформа Интернета вещей . Открытые системы. СУБД, №7, 2012. URL: <https://www.osp.ru/os/2012/07/13017643/>.
2. https://www.cisco.com/c/ru_ru/solutions/internet-of-things/overview.html#~stickynav=1.
3. Степанова М.В. Концепция Интернета вещей на базе платформы IBM Bluemix. Современные тенденции развития науки и технологий. 2016. №3-2. С. 138-141.

УДК 004.8

ОСОБЕННОСТИ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ НАЗЕМНОГО ГОРОДСКОГО ПАССАЖИРСКОГО ТРАНСПОРТА

Ильченко Лидия Михайловна, Зайцев Святослав Игоревич

¹ Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Российская Федерация, 197101, Санкт-Петербург, Кронверкский пр., 49

² Государственный университет морского и речного флота имени адмирала С.О. Макарова

Российская Федерация, 198035, г. Санкт-Петербург, ул. Двинская, 5/7

email: Lidiya9510@yandex.ru, Sunilink@yandex.ru

Аннотация: В данной работе рассматриваются особенности построения системы защиты информации в автоматизированных системах управления наземного городского пассажирского транспорта.

Ключевые слова: информационная безопасность, интеллектуальная дорожно-транспортная система, угрозы безопасности, средства защиты информации, автоматизированная система управления наземным городским пассажирским транспортом.

PARTICULAR QUALITIES OF CONSTRUCTION OF INFORMATION PROTECTION SYSTEM IN INTELLECTUAL SYSTEMS OF GROUND CITY PASSENGER TRANSPORT

Ilchenko Lydia, Zaytsev Svyatoslav

¹ Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics 197101, Russia, St. Petersburg, 49 Kronverksky Pr.² Admiral Makarov State University of Maritime and Inland Shipping

198035, Russia, St. Petersburg, Dvinskaya st., 5/7

email: Lidiya9510@yandex.ru, Sunilink@yandex.ru

Abstract: In this paper we consider the construction of a system for protecting information in the intellectual systems of ground city passenger transport.

Keywords: information security, intellectual road and transport system, security threats, data protection facilities, intellectual systems of ground city passenger transport.

Введение. На сегодняшний день транспортная система является неотъемлемой частью инфраструктуры любого развитого государства. На территории России насчитывается более 1 396 000 км сети автодорог общего пользования. В связи с чем возникает ряд потребностей, основной из которых является максимизация качества функционирования дорожно-транспортной системы, которая особенно остро ощущающихся в больших городах, где поток транспортных средств намного превышает пропускную способность дорожной инфраструктуры.

Существует два направления решения этой задачи: использование технологий автоматизированного управления транспортной системой путем использования информационных технологий; и модернизация участков дороги.

Во время проектирования автономных систем наземного транспорта, решающих отдельные задачи, появилась обоснованная необходимость в создании общей государственной стратегии развития, контроля и регламентации единого программного комплекса, объединяющего деятельность всех органов власти, действующих в сфере транспортной инфраструктуры государства. [6]

Система, основной функцией которой стало объединение в единый технологический и технический комплекс множество отдельных подсистем дорожного движения, получила название «Интеллектуальная дорожно-транспортная система» (далее – ИТС). [5]

Одной из ведущих подсистем ИТС является система автоматизированного управления наземным городским пассажирским транспортом (АСУ НГПТ).

Стратегическую цель создания АСУ НГПТ составляет удовлетворение спроса на пассажирский транспорт. Результатом функционирования АСУ НГПТ является описание целевых направлений построения интеллектуальной дорожно-транспортной системы:

- мониторинг дорожной ситуации;
- организация транспортного потока и пр.

В рамках управления системой городского наземного транспорта рассматривается:

- управление непосредственно самим транспортом (автобусы, трамваи, и пр), частью пригородных перевозок (связь города с вокзалами и аэропортами);
- определение местоположения транспортных средств в режиме реального времени на базе технологий ГЛОНАСС/GPS;

- система информирования пассажиров на остановочных пунктах и в транспортных средствах;
- система учета пассажиров;
- система диспетчерского управления;
- система безопасности;
- дуальный канал связи транспортных средств с диспетчерскими центрами;

Основными функциями автоматизированной системы управления наземным городским дорожным транспортом являются:

1. Диспетчеризация (журналирование выполненных работ, управление движением в режиме реального времени, контроль за соблюдением расписания).[3]

2. Планирование (составление паспорта маршрута, мониторинг пассажиропотока, журналирование и аудит работы перевозчиков).

3. Безопасность (видеоконтроль, реагирование в случае поступления сигналов бедствия, информирование о чрезвычайных происшествиях). [2] [4]

Для автоматизированной системы управления главными векторами обеспечения защиты является доступность и целостность. Конфиденциальность данных обеспечивается по необходимости. [9]

В качестве источников внутренних отказов автоматизированной системы управления выступают:

- непреднамеренные ошибки эксплуатации системы;
- системные ошибки из-за превышения допустимых объемов обрабатываемых данных;
- отказ программного и (или) аппаратного обеспечения;
- потеря информации и (или) физических носителей информации. [1]

Для рассматриваемой системы класс защищенности определяется в соответствии с приказом ФСТЭК России от 14 марта 2014 г. № 31, и напрямую зависит от уровня значимости обрабатываемых данных, который прямо пропорционален возможному ущербу для каждого из свойств безопасности информации (целостности, доступности, конфиденциальности).

Степень возможного ущерба для АСУ наземного городского пассажирского транспорта: для целостности, доступности и конфиденциальности – низкая.

Исходя из вышеуказанных данных уровень значимости системы соответствует третьему (УЗ-3), а класс защищенности, в соответствии с таблицей в п.3 Приложения №1 приказа ФСТЭК России от 14 марта 2014 г. № 31, соответствует третьему классу (К3).

Обеспечение защиты информации в АСУ наземного городского пассажирского транспорта достигается за счет комплексного подхода к организации системы защиты данных. Базовый набор мер представлен в приложении №2 приказа ФСТЭК России от 14 марта 2014 г. №31. Адаптивный набор мер формируется в результате оценки угроз информационной безопасности на базе составленной модели угроз.

Как минимум, меры защиты должны обеспечивать минимизацию, либо полную ликвидацию угроз безопасности информации, источником которых является нарушитель с низким потенциалом.

В системе защиты должны быть реализованы следующие группы мер:

- идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ);
- управление доступом субъектов доступа к объектам доступа (УПД);
- ограничение программной среды (ОПС);
- защита машинных носителей информации (ЗНИ);
- регистрация событий безопасности (РСБ);
- антивирусная защита (АВЗ);
- обнаружение (предотвращение) вторжений (СОВ);
- контроль (анализ) защищенности информации (АНЗ);
- целостность автоматизированной системы управления и информации (ОЦЛ);
- доступность технических средств и информации (ОДТ);
- защита среды виртуализации (ЗСВ);
- защита технических средств и оборудования (ЗТС);
- защита автоматизированной системы и ее компонентов (ЗИС);
- безопасная разработка прикладного и специального программного обеспечения (ОБР);
- управление обновлениями программного обеспечения (ОПО);
- планирование мероприятий по обеспечению защиты информации (ПЛН);
- обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС);
- информирование и обучение персонала (ИПО);
- анализ угроз безопасности информации и рисков от их реализации (УБИ);
- выявление инцидентов и реагирование на них (управление инцидентами) (ИНЦ);

– управление конфигурацией автоматизированной системы управления и ее системы защиты (УКФ).

Исходя из анализа Реестра сертифицированных ФСТЭК России средств защиты информации и практики их применения, можно составить перечень необходимых и достаточных средств защиты:

– СЗИ от несанкционированного доступа (СЗИ от НСД) применимы для следующих групп мер: ИАФ, УПД, ОПС, РСБ, АНЗ, ОЦЛ, ЗИС, ОПО, ИНЦ;

– средств индивидуального межсетевое экранирования (МЭ) применимы для следующих групп мер: ИАФ, УПД, ОПС, РСБ, ЗСВ, ОЦЛ, ИНЦ;

– средств обнаружения вторжений применимы для следующих групп мер: УПД, РСБ, СОВ, АНЗ, ЗИС, ИНЦ;

– средств резервирования применимы для следующих групп мер: ОЦЛ, ОДТ, ЗИС, ДНС;

– средств антивирусной защиты информации (АВЗ) применимы для следующих групп мер: РСБ, АВЗ, ОЦЛ, ЗИС, ОПО, ИНЦ.

А также средства криптографической защиты информации (СКЗИ), сертифицированные Федеральной службой безопасности РФ (ФСБ России) применимы для следующих групп мер: РСБ, ОЦЛ, ЗИС, ИНЦ.

Кроме этого, необходимо применять ряд организационных мер.

Третий класс защищенности предъявляет следующие требования:

– средства вычислительной техники не ниже 5 класса;

– СЗИ не ниже 6 класса. [7]

Выводы. При проектировании системы защиты необходимо учитывать все особенности АСУ НГПТ, а также необходимо учитывать актуальные угрозы безопасности и специфику обрабатываемых данных, акцентируя внимание на доступности и целостности обрабатываемой информации, и лишь по необходимости на конфиденциальности. Кроме этого, необходимо учитывать требования нормативно-правовых актов, регламентирующих данную категорию автоматизированных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. – М.: Горячая линия – Телеком, 2014. – 594 с.
2. Жанказиев. С.В. Интеллектуальные транспортные системы: учеб. пособие / – М.: МАДИ, 2016. – 120 с.
3. Ивченко Б.П., Мартыщенко Л.А., Монастырский М.Л. Теоретические основы информационно-статистического анализа сложных систем. – СПб.: Лань, 1997. – 320 с.
4. Конопляно, В.И. Организация и безопасность дорожного движения / В.И. Конопляно. – М.: Транспорт, 1991. – 183 с.
5. Косолапов, А.В. Повышение эффективности информационного обеспечения участников дорожного движения в городах: дис. ...канд. техн. наук. – М., 1992.
6. Опыт создания и эксплуатации интеллектуальных транспортных систем: Информационный сборник / Федеральное дорожное агентство Министерства транспорта Российской Федерации. – М.: ООО «Принт Форс Пабблишинг», 2009. – 287 с.
7. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». – 42 с.
8. Руководящий документ «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры», от 18 мая 2007 года, ФСТЭК России.
9. Руководящий документ «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры», от 18 мая 2007 года, ФСТЭК России.

УДК 001.812

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ОБУЧЕНИИ ХИМИИ

Колоколов Даниил Сергеевич

Санкт-Петербургский государственный университет,

Россия, Санкт-Петербург, Университетская наб., 7/9,

email: kolokolov.d@gmail.com

Аннотация: В статье рассмотрены, как пример повышения эффективности обучения химии.

Ключевые слова: компьютер, преподавание химии

USE OF INFORMATION TECHNOLOGIES IN TRAINING CHEMISTRY

Daniil Kolokolov

St. Petersburg State Institute,

Russia, St. Petersburg, Universitetskaya Embankment, 7/9,

email: kolokolov.d@gmail.com

Abstract: The article is considered as an example of increasing the effectiveness of teaching chemistry.

Keywords: computer, teaching chemistry

В настоящее время в Российском образовании идет процесс перехода к стандартам нового поколения, при этом определяется роль информатизации и подтверждается факт вхождения

человечества в эпоху глобализации информационных процессов. Только за последнее десятилетие повсеместно стали использоваться новые информационные технологии: Интернет, мобильная связь, цифровые технологии. При этом разрабатываемый образовательный стандарт должен стать ответом на вызов современного глобального непрерывно меняющегося мира. Все новинки технологического прогресса с особым восторгом встречают именно дети. Поэтому очень важно использовать любознательность и высокую познавательную активность учащихся для целенаправленного развития их личности. Именно на уроках под руководством педагога школьники могут научиться использовать компьютерные технологии в образовательных целях, овладеть способами получения информации для решения учебных, а впоследствии и более широкого круга задач, приобрести навыки, обеспечивающие возможность продолжать образование в течение всей жизни. Однако использование в настоящее время компьютерных технологий в процессе обучения, в том числе химии, скорее исключение, чем правило. Кроме того, надо признать, что за последние годы наблюдается снижение интереса учащихся к естествознанию вообще и к химии в частности, что представляет собой одну из проблем школьного образования. Причины негативных изменений, появившихся в обучении химии за последние годы, связаны с нарастанием сложности программного материала и сокращением учебного времени на его усвоение, а также недостаточным обеспечением учебного процесса специальным оборудованием. На современном этапе развития страны осуществляется модернизация среднего образования, в рамках которой и педагогами нашей школы активно ведутся поиски новых подходов, средств и методов обучения. Цель педагогической деятельности ориентирована на повышение качества образования через внедрение и интеграцию современных образовательных технологий, при этом информационным отводится ведущее место.

Для достижения поставленной цели в области преподавания химии определены следующие задачи: рассмотреть основные принципы и методические приемы построения компьютеризированных методик обучения химии; адаптировать применение информационных компьютерных технологий к условиям лечебно-образовательного процесса; создать условия для формирования ключевых компетенций обучающихся с акцентом на информационные; содействовать созданию здоровьесберегающей среды обучения. Реализация обозначенных цели и задач в нашем образовательном учреждении возможна благодаря наличию соответствующей материальной базы, созданной в рамках программы компьютеризации общеобразовательных учреждений. Для реализации нового подхода к преподаванию с применением информационных технологий необходимо знать возможности, предоставляемые компьютером для усовершенствования учебного процесса на каждом этапе урока. Так, на этапе подготовки к уроку компьютер предоставляет возможности: создавать компьютерные модели конспекта урока, темы, курса в целом; максимально целесообразно располагать материал; обеспечивать основной материал дополнительной информацией; подбирать и систематизировать материал с учетом особенностей класса и отдельных учащихся. На этапе проведения уроков компьютер позволяет: экономить время; красочно оформлять материал; повышать эмоциональную, эстетическую, научную убедительность преподавания; оптимизировать процесс усвоения знаний, воздействуя на различные анализаторы; индивидуализировать обучение; концентрировать внимание на важнейшей проблеме урока; в любой момент возвращаться к уже знакомому материалу; самостоятельно использовать учебный материал обучающимися.

СПИСОК ЛИТЕРАТУРЫ

1. Курдюмова Т. Н. Компьютерная технология обучения химии: достоинства и недостатки. // Химия в школе, 2002. - №8, с. 35 – 37.
2. Курдюмова Т. Н., Курдюмов Г. М. Компьютерные обучающие игры. // Химия. Методика преподавания, 2004. - №1, с. 75 – 77.

УДК 004.056

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Красов Андрей Владимирович, Левин Марк Вадимович, Фостач Елена Сергеевна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича,

Россия, Санкт-Петербург, ул. Проспект Большевиков, 22,
emails: krasov@inbox.ru, m.va.levin@gmail.com, elena.fostach@gmail.com

Аннотация: Проблема обеспечения безопасности данных, размещенных в облачных средах, является уязвимым местом эксплуатации модели виртуализации. В данной статье рассматриваются особенности безопасности облачной архитектуры, а также проводится анализ перспективы развития модели предоставления облачных услуг. Результаты проведенного анализа позволяют сформировать требования к обеспечению информационной безопасности, а также определить ключевые функции, которые должны быть поддержаны как поставщиком, так и потребителем услуг. Такой подход способствует обеспечению высокой скорости развертывания, оперативности и эффективности, обеспечивая по требованию пользователя доступ к общим источникам вычислительных ресурсов в автономном, динамично масштабируемом и выверенном режиме.

Ключевые слова: облачные технологии; облачные вычисления; SaaS, PaaS, IaaS; виртуализация; информационная безопасность.

SAFETY PROBLEMS OF CLOUD COMPUTING

Krasov Andrey, Levin Mark, Fostach Elena

The St. Petersburg State University of Telecommunications,
Russia, St. Petersburg, Prospekt Bol'shevikov street 22,

emails: krasov@inbox.ru, m.va.levin@gmail.com, elena.fostach@gmail.com

Abstract: Cloud computing is a new computational paradigm that offers a distributed infrastructure. Despite the potential gains achieved from the cloud computing, the model security is still questionable which impacts the cloud model adoption. The security problem becomes more complicated under the cloud model as new dimensions have entered into the problem scope related to the model architecture, multi-tenancy and elasticity. Cloud computing security concerns, especially data security and privacy protection issues, remain the first problem of cloud computing services. In the actual article we introduce a detailed analysis of the cloud security problem. We investigated the problem from the cloud architecture. Based on this analysis we offers a detailed specification of the cloud security problem and key features that should be covered by any proposed security solution

Keywords: cloud technologies; cloud computing; virtualization; SaaS, PaaS, IaaS; information security.

Введение. Облачные вычисления являются следующим шагом развития Интернет-технологий, где вычислительные ресурсы предоставляются пользователю в качестве услуги «as-a-service». У модели предоставления облачных услуг имеется ряд проблем, которые влияют на ее эксплуатацию. Для поставщиков облачных услуг обеспечение безопасности требует значительных финансовых затрат и ресурсов (т.к. обеспечение безопасности является задачей потребления ресурсов). Тем не менее, ответственность за обеспечение безопасности должна возлагаться как на поставщика, так и на потребителя облачных услуг в зависимости от используемой сервисной модели.

Архитектура облачных технологий.

Согласно стандарту NIST, модель облачных вычислений описывает три модели предоставления услуг: инфраструктура как услуга (IaaS), платформа как услуга (PaaS), программное обеспечение как услуга (SaaS). Архитектура облачных вычислений представляет собой упорядоченный набор уровней объектов виртуализации, где функциональность и безопасность более высокого уровня зависит от обеспечения и контроля безопасности на нижних уровнях. Для поддержания трех базовых свойств информационной безопасности – конфиденциальности, целостности и доступности данных пользователей, были обозначены ключевые проблемы, которые необходимо решить в первую очередь:

1. Исследование механизмов аутентификации пользователей и использования защищенного канала связи на пути между клиентом и сервером.

2. Исследование способов хранения информации в зашифрованном виде, ее обработки и поиска в облачном хранилище.

Решение данных проблем позволит повысить уровень конфиденциальности, целостности и доступности данных в облачных средах.

Определение способов конфиденциальной передачи данных.

За основу была взята схема функциональной архитектуры облачной среды, на базе которой построено исследование. Схема демонстрирует способ развертывания баз данных и приложений на ресурсах облачной инфраструктуры вместе с сетевой схемой взаимодействия, показывает уровни коммутации (L2) и маршрутизации (L3) данных между объектами облачной инфраструктуры.

В соответствии с решаемой проблемой, ключевыми аспектами информационной безопасности, которые должны лежать в основе каждого надежного облачного сервиса, являются - определение способов конфиденциальной передачи данных, организация доступа авторизованных пользователей к данным.

Решение первой задачи, определение способов конфиденциальной передачи данных, требует использования криптографических механизмов, позволяющих обеспечить надежное шифрование данных. С целью снижения вероятности перехвата в открытом виде передаваемого сообщения, шифрование данных должно происходить до того момента, как информация покинет браузер пользователя (т.е. до момента отправки сообщения на сервер).

Использование протокола TLS v1.2 позволяет создать канал конфиденциальной передачи данных. Механизмы работы данного протокола не обеспечивают контроль времени жизни каждой пользовательской сессии и повторную аутентификацию клиента для возобновления сессии в случае разрыва установленного соединения. Протокол TLS v1.2 не позволяет аутентифицировать самого пользователя, в связи с этим, рассмотрим механизм аутентификации пользователей в рамках протокола OAuth2.0.

Организация доступа авторизованных пользователей к данным.

Чтобы решить задачу, связанную с упрощением авторизации пользователя при работе с большим количеством приложений и онлайн сервисов, был рассмотрен протокол OAuth. При

использовании OAuth-авторизации к основным преимуществам принято относить отсутствие передачи логина и пароля в приложение, с которым работает пользователь. Таким образом, приложение может выполнить только то, что явно разрешил пользователь. Так же, отпадает необходимость решения вопроса обеспечения защищенного хранения пароля и логина приложением.

Снижение риска несанкционированного доступа к ресурсам и обеспечение доступности информации можно добиться за счет внедрения механизма аутентификации.

Суммируя описанные ранее подходы, была представлена концептуальная схема, которая отражает ключевые элементы облачной архитектуры (клиентскую часть приложения, сервер аутентификации, сервер приложения (который включает в себя механизмы обработки информации), а также хранилище данных). Дополнительно, на схеме отмечено, на каких сегментах сети применимы рассмотренные ранее протоколы OAuth 2.0, TLSv1.2 для обеспечения надежного соединения.

Заключение. В результате исследования показано, что для создания надежного TLS соединения важно иметь возможность аутентификации именно клиентской части приложения, а не самого пользователя. Так же стоит отметить, что в основе протокола TLS v1.2 отсутствуют механизмы контроля времени жизни пользовательской сессии и механизмы повторной аутентификации для возобновления сессии в случае разрыва соединения. Вследствие чего необходимо внедрение средств аутентификации пользователей за счет протокола OAuth2.0.

СПИСОК ЛИТЕРАТУРЫ

1. Wayne Jansen, Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing, NIST, Draft Special Publication 800-144, January 2011.
2. T. Dierks, E. Rescorla. The Transport Layer Security (TLS) Protocol, Version 1.2 (RFC5246).
3. Красов А.В., Левин М.В., Цветков А.Ю. Управление сетями передачи данных с изменяющейся нагрузкой // Всероссийская научная конференция по проблемам управления в технических системах. 2015. № 1. С. 141-146.
4. Security issues in OAuth 2.0 SSO implementations. Li, W. & Mitchell, C. J. 2014 Information Security - 17th International Conference, ISC 2014, Hong Kong, China, October 12-14, 2014. Proceedings. Chow, S., Camenisch, J., Hui, L. & Yiu, S-M. (eds.). Springer-Verlag, p. 529-541 13 p.
5. Красов А.В. Возможности управления трафиком в рамках концепции SDN : Монография / А.В. Красов, М.В. Левин. - Актуальные проблемы инфотелекоммуникаций в науке и образовании IV Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 томах, 2015. - 350-354 с.
6. Алейников А.А. Контроль, измерение и интеллектуальное управление трафиком : Монография / А.А. Алейников, К.З. Билядинов, А.В. Красов, М.В. Левин. Санкт-Петербург, 2016.
7. Красов А.В., Левин М.В., Штеренберг С.И., Исаченков П.А. Модель управления потоками трафика в программно-определяемой сети с изменяющейся нагрузкой // Научно-технические аспекты в космических исследованиях Земли. 2016. Т. 8. № 4. С. 70-74.
8. Алейников А.А. Технические аспекты управления с использованием сети интернет : Монография / А.А. Алейников, К.З. Билядинов, А.В. Красов, Е.А. Кривчун, А.В. Крысанов. Санкт-Петербург, 2016.

УДК 004.056.53

АНАЛИЗ ЗАЩИЩЕННОСТИ ERP-СИСТЕМ. ОБЩИЙ ПОДХОД К АНАЛИЗУ

Кривдюк Надежда Михайловна

Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский пр., 49,
email: krivdyuk.nadezhda@gmail.com

Аннотация: В статье рассмотрены наиболее известные проблемы безопасности ERP-систем, ранжированные по степени важности и влияния на корпоративные приложения в целом. В ходе исследования был предложен подход анализа защищенности корпоративных приложений, покрывающие все критичные области любой ERP-системы.

Ключевые слова: ERP-системы; анализ защищенности; Top-9 ERP Issues; настройки безопасности; критичность проблем; EAS-SEC.

ANALYSIS OF ERP-SYSTEMS SECURITY. GENERAL APPROACH TO ANALYSIS

Krivdyuk Nadezhda

The St. Petersburg National Research University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, 49 Kronverksky Pr.,
email: krivdyuk.nadezhda@gmail.com

Abstract: The article discusses the most known security problems of ERP-systems, ranked by the degree of importance and influence on corporate applications in general. In the course of the study, an approach was proposed to analyze the security of enterprise applications, covering all critical areas of any ERP-system.

Keywords: ERP-systems; security analysis; Top-9 ERP Issues; security settings; criticality of problems; EAS-SEC.

Современное общество характеризуется стремительным развитием новейших информационных технологий, где постоянно циркулирует информация. Вместе с чем значительно возрастают угрозы

безопасности информации, что может привести к нарушению непрерывности бизнеса. В связи с этим очевидна необходимость обеспечения безопасности организаций.

В крупных компаниях и не только вся критичная информация хранится и обрабатывается в корпоративных приложениях и системах: веб-приложения, СУБД, системах управления ресурсами предприятия (ERP-системы) и других. Такая информация может содержать финансовые данные, коммерческую тайну, персональные данные и иную специфическую информацию, которой заинтересованы злоумышленники [1].

Объектом исследования выбраны ERP-системы, так как в них обрабатываются наиболее критичная информация. В ходе исследования проанализированы существующие рекомендации по безопасности от Oracle, ISACA [2], OWASP [3], PCIDSS и BIZEC и других, а также доклады крупных конференций по информационной безопасности. Задачей исследования стояло захватить вниманием как можно больше проблемных областей в ERP-системах, для которых необходимо проведение анализа защищенности. В процессе исследования были выбраны и описаны самые критичные проблемы, оказывающие негативное воздействие на системы, и определить приоритеты решения данных проблем. Были определены области, внутри которых необходимо осуществить безопасность. При этом, важно было выделить те области, которые являются наиболее распространенными в Корпоративных Приложениях. Кроме высокой частоты обнаружения этих проблем, необходимо было понять еще несколько фактов о каждой из них. В результате среди многообразия проблем ERP-систем были выбраны девять самых критичных, ранжированы по степени важности и влияния на корпоративные приложения в целом, и безопасность EAS в частности. Для этого было утверждены критерии: уровень авторотационного доступа, критичность проблемы, сложность использования проблемы и частота встречаемости проблемы.

Заключение. В результате анализа появился окончательный вариант ранжированного по критичности списка девяти наиболее распространенных проблем ERP-систем Top-9 ERP Issues:

1. Недостатки управления обновлениями.
2. Учетные записи по умолчанию для доступа к приложению.
3. Дополнительный функционал.
4. Открытые удаленные интерфейсы управления.
5. Небезопасные настройки.
6. Незашифрованные соединения.
7. Контроль доступа и SOD конфликты.
8. Небезопасные доверенные соединения.
9. Протоколирование событий безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. «Система планирования ресурсов предприятий ERP», RBC group – Решения по управлению предприятиями на основе систем ERP и BI, [Электронный ресурс], URL: <http://www.rbcgrp.com/erp-planing.html>, режим доступа: свободный, дата обращения: 19.09.2017.
2. Information Technology - Information Security – Information Assurance | ISACA [Электронный ресурс] / Режим доступа: <https://www.isaca.org> (19.09.2017)
3. OWASP, Top 10 Application Security Risks [Электронный ресурс] / Режим доступа: https://www.owasp.org/index.php/Top_10_2017-A2-Broken_Authentication_and_Session_Management (19.09.2017)

УДК 004.056.53

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАЩИЩЕННОСТИ ОСУЩЕСТВЛЕНИЯ ФИНАНСОВЫХ ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ

Курышева Алена Андреевна, Ганчикова Юлия Сергеевна
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский пр., 49,
emails: kurysheva.al@yandex.ru, yul7494582@yandex.ru

Аннотация: Статья посвящена сравнительному анализу защищенности финансовых операций с использованием электронных платежных систем. Рассмотрены уровни защищенности нескольких платежных систем предназначенных для оплаты товаров и услуг в сети Интернет.

Ключевые слова: финансовая безопасность; платежные системы; транзакции; защита; 3D-secure.

COMPARATIVE ANALYSIS OF FINANCIAL TRANSACTIONS SECURITY USING ELECTRONIC PAYMENT SYSTEMS

Kurysheva Alena, Ganchikova Yulia
University of Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronverksky Pr. 49,
emails: kurysheva.al@yandex.ru, yul7494582@yandex.ru

Abstract: The article presents analysis of security transactions using electronic payment systems. The article considered levels of security of several payment systems designed to pay for goods and services on the Internet.

Keywords: *financial security; payment system; transactions; security; 3d-secure.*

Введение. На сегодняшний день электронные платежные системы используются миллионами пользователей ежедневно. Сохранность персональных данных и денежных средств зависит от безопасности проведения транзакций в платежных системах.

Рассматриваемые электронные платежные системы предназначены для упрощения проведения финансовых операций при помощи сети Интернет. Для сравнительного анализа использованы следующие платежные сервисы: «QIWI», «WebMoney», «PayPal», «Яндекс.Деньги». Проведено сравнение электронных платежных систем по следующим критериям: шифрование, аутентификация, идентификация, дополнительное подтверждение операции, дополнительная защита.

Заключение. Сравнительный анализ позволяет сделать вывод, что каждая рассмотренная электронная платежная система имеет несколько уровней защиты. Процесс подтверждения операций у каждой из платежных систем имеет свой алгоритм и от этого напрямую зависит безопасность транзакций. Часть рассмотренных платежных систем имеет более низкий уровень безопасности. Для повышения уровня следует уделить более пристальное внимание аутентификации, идентификации и алгоритму подтверждения финансовых операций.

СПИСОК ЛИТЕРАТУРЫ

1. Никонец О. Е., Гринь И. А., Марченко А. В. Бесконтактные платежи: история возникновения и безопасность // Научно-методический электронный журнал «Концепт». – 2016. – Т. 15. – С. 2726–2730. – URL: <http://e-koncept.ru/2016/96466.htm> (дата обращения: 16.09.2017).
2. О национальной платежной системе [Электронный ресурс] : федер. закон Рос. Федерации от 27 июня 2011 г. №161-ФЗ : принят Гос. Думой 14 июня 2011 г. : одобрен Советом Федерации 22 июня 2011 г. (ред. от 18.07.2017). Доступ из справ.-правовой системы «КонсультантПлюс».

УДК 004.056.53

АНАЛИЗ СУЩЕСТВУЮЩИХ ДАТЧИКОВ ДЛЯ ВЫЯВЛЕНИЯ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

Лисецкая Кристина Валерьевна

Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский пр., 49,
email: kristinasev62@gmail.com

Аннотация: В статье рассмотрены наиболее эффективные датчики для создания комплексной системы защиты, которые помогают предотвратить несанкционированный доступ к информации. Определены и проанализированы их главные достоинства и недостатки. Описан принцип работы каждого компонента комбинированного датчика.

Ключевые слова: *системы контроля доступа; датчик; несанкционированный доступ; комбинированный датчик.*

ANALYSIS OF EXISTING SENSORS FOR DETECTING THE ATTEMPTS OF UNAUTHORIZED ACCESS TO PROTECTED INFORMATION

Lisetskaya Kristina

The St. Petersburg National Research University Information Technologies, Mechanics and Optics,
Russia, St. Petersburg, Kronverksky Pr. 49,
email: kristinasev62@gmail.com

Abstract: The article deals with the most effective sensors for creating an integrated security system that prevents unauthorized access to information. The main advantages and disadvantages are determined and analyzed. The principle of operation of each component of the combined sensor is described.

Keywords: *access control systems; sensor; unauthorized access; combined sensor.*

Введение. На сегодняшний день остро стоит проблема безопасности, а именно, охраны предприятия от несанкционированного доступа к защищаемой информации. Системы контроля доступа прогрессируют и их значимость увеличивается. Нередко на предприятиях используют для надёжной защиты своих данных такие устройства, как датчики. Однако, при выборе необходимо помнить о следующих важных факторах: цена, качество и надёжность.

Основная часть. Рассматриваются датчики, которые чаще всего применяют в системе контроля доступа, их достоинства и недостатки. Проведя сравнительный анализ датчиков, используемых в системе защиты были выбраны наиболее эффективные. Для достижения максимального результата

их следует использовать в комплексе, так как каждый извещатель имеет свою уязвимость. Описаны принцип работы каждого составляющего устройства.

Заключение. В результате проведенного анализа, выявлено, что каждый из датчиков склонен к уязвимостям, поэтому необходимо их использовать в комплексе. Используя комбинированный датчик повысится надёжность всей системы. Данное устройство обеспечит предотвращение нарушения охраняемого периметра, а также несанкционированного доступа к защищаемой информации.

СПИСОК ЛИТЕРАТУРЫ

1. Умные датчики для интеллектуальных систем безопасности. [электронный ресурс], режим доступа: http://www.vashdom.ru/articles/st_16.htm
2. Электротехническая энциклопедия №16. Датчики. [электронный ресурс], режим доступа: http://electrolibrary.info/subscribe/sub_16_datchiki.htm
3. Основные характеристики датчиков. [электронный ресурс], режим доступа: http://studopedia.ru/2_66109_osnovnie-harakteristiki-datchikov.html
4. Датчики охранной сигнализации. [электронный ресурс], режим доступа: <http://sec4all.net/datchik.html>
5. Извещатели комбинированные и совмещенные. [электронный ресурс], режим доступа: <http://specautomatik.ru/index.php/article/211-kombinirovannye>

УДК 004.056.53

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Орлов Иван Алексеевич

Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский пр., 49,

Аннотация: Статья посвящена применению искусственных нейронных сетей и вариантам их обучения для решения проблем информационной безопасности. Приведены примеры использования и выведены основные направления развития нейронных сетей в области информационной безопасности.

Ключевые слова: нейронная сеть, криптография, искусственный интеллект

APPLICATION OF NEURAL NETWORKS IN THE FIELD OF INFORMATION SECURITY

Orlov Ivan

Federal State Autonomous Educational Institution of Higher Education
“Saint-Petersburg State University of Aerospace Instrumentation”
Russia, Saint-Petersburg, st. Bolshaya Morskaya, 67, lit. A

Abstract: The article is devoted to application of neural networks and their training options for solving problems of information security. Examples of the use was given and main directions of development of neural networks in the field of information security was inferred.

Keywords: neural network, cryptography, artificial intelligence

Введение. На ряду с ростом проблем в области информационной безопасности развивается область искусственного интеллекта и компьютерного обучения. Если до недавнего времени еще вставал вопрос об использовании искусственных нейронных сетей для решения проблем защиты информации, то в настоящее время стало ясно, что они переводят области криптографии и криптологии на новую ступень развития.

Варианты построения нейронных сетей варьируются в зависимости от поставленных целей, что позволяет подстроить сеть под требуемую задачу информационной безопасности. Для построения нейронной сети используется набор параметров, который в будущем может быть изменен для получения более точных результатов и уменьшения вероятности ошибки сети при получении конечного результата. Функциональные возможности искусственных нейронных сетей определяются их топологией, алгоритмами обучения и характеристиками нейронов. Основным преимуществом в использовании нейронных сетей является массовый параллелизм и способность к сохранению знаний, основанных на полученном опыте, адаптируясь под задачу сети с увеличением количества проведенных экспериментов. Приведенные характеристики позволяют решать искусственным нейронным сетям задачи криптографии.

Заключение. Нейронные сети являются перспективным направлением и интерес к их применению стремительно растет. Области использования меняются от обнаружения скрытой информации до шифрования данных, а возможности и способы применения в силу развития технологий будут увеличиваться. Данные представляют интерес для сотрудников, работающих в областях защиты информации и позволяют оценить целесообразность использования нейросетевых систем, являющихся относительно новым и подающим надежды методом работы с информацией в области информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Червяков Н.И., Галушкин А.И., Евдокимов А.А., Лавриненко А.В., Лавриненко И.Н. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. — М. Издательство: Физмалит, 2012 — 280с.
2. Евдокимов А.А., Тихонов Э.Е. Интеллектуальные информационные системы защиты информации. — Невинномысск. Издательство: НИЭУП, 2012 — 120с.
3. Писаренко И. Нейросетевые технологии в безопасности. // Information Security/ Информационная безопасность. 2009. №4 [Электронный ресурс]. URL: <http://www.itsec.ru/articles2/Oborandteh/neyrosetevye-tehnologii-v-biznese> (дата обращения: 03.09.2017).

УДК 004.7

**ИННОВАЦИИ ЖИЗНЕННОГО ЦИКЛА ЗАЩИЩЁННЫХ СЕРВИС-ОРИЕНТИРОВАННЫХ СИСТЕМ
ДЛЯ ЦИФРОВОЙ ЭКОНОМИКИ**

Птицына Лариса Константиновна, Нежинский Виталий Владимирович
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
Россия, Санкт-Петербург, наб. р. Мойки 61,
emails: ptitsina_lk@inbox.ru, seekerofconfessor@gmail.com

Аннотация: В статье актуализировано развитие методологических основ жизненного цикла защищённых сервис-ориентированных систем для цифровой экономики. Представлены системообразующие формализации жизненного цикла защищённых сервис-ориентированных систем. Показана объективная необходимость расширения формализмов для описания защищённых сервис-ориентированных систем с темпоральной логикой. Описаны ключевые этапы формирования описаний защищённых сервис-ориентированных систем с темпоральной логикой и их основные операции. Рассмотрены отличительные особенности приводимых операций. Акцентировано внимание на преимуществах предлагаемых инноваций в жизненном цикле защищённых сервис-ориентированных систем для цифровой экономики.

Ключевые слова: *жизненный цикл; сервис; сервис-ориентированная система; защита информации; темпоральная логика; спецификация; модель, верификация.*

**INNOVATION OF THE LIFE CYCLE OF PROTECTED SERVICE-ORIENTED SYSTEMS FOR THE
DIGITAL ECONOMY**

Ptitsyna Larisa, Nezhinsky Vitaliy
Federal State Educational Budget-Financed Institution of Higher Education the Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
Russia, St. Petersburg, Moika River emb. 61,
emails: ptitsina_lk@inbox.ru, seekerofconfessor@gmail.com

Abstract: The report actualizes the development of the methodological foundations of the life cycle of secure service-oriented systems for the digital economy. The system-forming formalizations of the life cycle of the protected service-oriented systems are presented. The objective necessity of expanding formalisms for the description of protected service-oriented systems with temporal logic is shown. The key stages of the formation of the descriptions of the protected service-oriented systems with temporal logic and their basic operations are described. The distinctive features of these operations are considered. Attention is focused on the benefits of proposed innovations in the life cycle of secure service-oriented systems for the digital economy.

Keywords: *life cycle; service; service-oriented system; data protection; temporal logic; specification; model; verification.*

На современном этапе жизни информационного общества магистральное направление его развития ассоциируется с цифровой экономикой. При реализации этого направления предусматривается значительное повышение производительности труда и образование новых высокоэффективных областей профессиональной деятельности на основе непрерывного увеличения объёмов и ускорения темпов погружения взаимно-согласованных видов профессиональной деятельности в высокопроизводительные информационные инфраструктуры. В подобных условиях возрастает значимость обеспечения повышенного уровня информационной безопасности при обширных масштабах априорной неопределённости, касающейся всевозможных ситуаций в профессиональной деятельности. Один из перспективных путей такого обеспечения может основываться на интеграции в информационных инфраструктурах комплексных систем защиты информации, распределённых по ресурсам инфраструктуры, и защищённых сервис-ориентированных систем. Благодаря подобной интеграции, предоставляется возможность воспользоваться представительным комплексом технологий их жизненного цикла, имеющих индустриальный характер, и арсеналом преимуществ сервис-ориентированных систем. К неоспоримым преимуществам относится поддержка масштабируемой распределённости систем, независимость от технологий разработки и платформ, управляемое распределение нагрузки между сервисами, сжатые до

обоснованной целесообразности сроки вывода на IT-рынок, высокая степень гибкости функциональной спецификации, согласуемая с современными запросами науки, образования промышленности, транспорта, медицины и социальной сферы, а также управляемое качество их функционирования.

Расширение многообразия комплексизируемых сегментов профессиональной деятельности, погружаемых в информационные инфраструктуры цифровой экономики, сопровождается повышением востребованности защищённых сервис-ориентированных систем, жизненный цикл которых наполняется технологической поддержкой многокомпонентного программного обеспечения. Определение и оценивание качества функционирования многокомпонентного программного обеспечения, образуемого посредством интеграции сервисов, обеспечивается методологическим базисом, ключевые компоненты которого раскрываются в [1, 2, 3, 4, 5, 6, 7]. Задачи соблюдения требуемого уровня информационной защищённости возлагаются на подсистему сервисов защиты информации от потенциальных угроз, соответствующих комплексизируемым сегментам профессиональной деятельности и сопровождающим информационным инфраструктурам. Определение и оценивание показателей различных профилей информационной защищённости обеспечивается методологическим базисом, основные составляющие которого представляются в [8].

При обширном объёме тематики научных исследований, связанных с жизненным циклом сервис-ориентированных систем, методологические аспекты их формальной верификации остаются открытыми. Отмеченная особенность может являться одной из причин несогласованности составляющих жизненного цикла сложных многокомпонентных программных систем, обеспечивающих технологическое сопровождение цифровой экономики. К примеру, при создании систем с первым классом информационной защищённости позиционируется обязательность проведения верификации. В силу представленных оснований предлагается развитие системы формализаций методологии проектирования защищённых сервис-ориентированных систем посредством введения процедур их формальной верификации.

Согласно традиционным канонам [8] верификация модели осуществляется за три этапа: построение математической модели; представление проверяемых свойств в виде спецификации; формальное доказательство наличия или отсутствия проверяемого свойства и всех свойств в совокупности. Математическая модель системы для верификации строится в виде графа. При этом состояниям системы (ситуациям или классам ситуаций, в которых может находиться система в различные моменты времени) ставятся в соответствие вершины графа, а действиям, выполняемым системой, – ребра графа.

Спецификация определяется как описание свойств системы в виде формального текста. Она представляется в формальном виде, зависящем от характера логики. В случае применения одной из самых известных логик CTL (Computational Tree Logic), соответствующей реальным условиям организации и функционирования распределённого программного обеспечения в гетерогенных активных инфокоммуникационных средах, спецификация записывается в терминах предикатов с использованием темпоральной логики.

В случае доказательства наличия всех проверяемых свойств защищённая сервис-ориентированная система признаётся пригодной для дальнейшего исследования и реализации, в процессе которых определяются и оцениваются показатели качества её функционирования. Посредством формальной верификации расширяется методологический базис проектирования защищённых сервис-ориентированных систем с требуемыми свойствами и качеством их функционирования для технологического сопровождения различных секторов цифровой экономики.

СПИСОК ЛИТЕРАТУРЫ

1. Птицына Л.К., Смирнов Н.Г. Разработка и анализ моделей интеграции сервис-ориентированных средств в гетерогенных сетях // Научно-технические ведомости СПбГПУ 6.1 (138). 2011. С. 71-80.
2. Птицына Л.К. Программное обеспечение компьютерных сетей. Управление крупно-гранулярными процессами на основе языка BPEL: учеб. пособие / Л.К. Птицына, Н.Г. Смирнов. – СПб.: Изд-во Политехн. ун-та, 2011. 105 с.
3. Птицына Л.К., Смирнов Н.Г. Системно-аналитическая основа интеграции сервис-ориентированных средств // Промышленные АСУ и контроллеры. 2011. № 5. С. 31-36.
4. Птицына Л.К., Веселов В.О. Анализ интеграции сервис-ориентированных средств в активных инфокоммуникационных средах // Научные технологии в космических исследованиях Земли. 2015. Т. 7. № 2. С. 42-47.
5. Веселов В.О., Птицына Л.К. Моделирование интеграции сервис-ориентированных средств в активных инфокоммуникационных средах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2 т.; Т.1 / под ред. К.В. Дукельского, сост. А.Г. Владыко, Е.А. Аникевич, Л.М. Минаков. – СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2015. С. 465 – 470.
6. Птицына Л.К., Кондратьев Д.А., Эльсабаяр Шевченко Н. Моделирование интеллектуальных сервис-ориентированных систем // Информационные системы и технологии в моделировании и управлении: материалы всероссийской научно-практической конференции. Гуманитарно-педагогическая академия (филиал) ФГАОУ ВО «КФУ им. В.И. Вернадского» в г. Ялте; Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», 2016. С. 57-60.
7. Кондратьев Д.А., Птицына Л.К., Эльсабаяр Шевченко Н. Концептуальные модели интеллектуализации сервис-ориентированных архитектур // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3 т.; Т.2 / под ред. С.В. Бачевского, сост. А.Г. Владыко, Е.А. Аникевич, Л.М. Минаков. – СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2016. С. 108 – 113.

8. Птицын, А.В., Птицына, Л.К. Аналитическое моделирование комплексных систем защиты информации. Гамбург. Saarbrücken: LAP LAMBERT Academic Publishing, 2012. 293 с.
9. Миронов А.М. Верификация программ методом Model Checking [Электронный ресурс]. URL: <http://intsys.msu.ru/staff/mironov/modelchk.pdf> (дата обращения 10.02.2017).

УДК 004.7

РАСПРЕДЕЛЁННЫЙ МОДЕЛЬНО-АНАЛИТИЧЕСКИЙ ИНТЕЛЛЕКТ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Птицына Лариса Константиновна, Гусев Дмитрий Сергеевич
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
Россия, Санкт-Петербург, наб. р. Мойки 61,
emails: ptitsina_lk@inbox.ru, gusev999dima@gmail.com

Аннотация: В статье показана обусловленность интеллектуализации комплексных систем защиты информации. Представлены возможные подходы к интеллектуализации комплексных систем защиты информации. Рассмотрены дидактические элементы возможных подходов к интеллектуализации. Приведены предпосылки для формирования модельно-аналитического интеллекта комплексных систем защиты информации. Выделены методологические разработки модельно-аналитического интеллекта. Описаны предлагаемые принципы распределения модельно-аналитического интеллекта в архитектурах комплексных систем защиты информации.

Ключевые слова: информационная безопасность; система защиты информации; интеллектуализация; модельно-аналитический интеллект; распределение; архитектура.

DISTRIBUTED MODEL ANALYTICAL INTELLIGENCE OF INTEGRATED SYSTEMS OF INFORMATION PROTECTION

Ptitsyna Larisa, Gusev Dmitriy
Federal State Educational Budget-Financed Institution of Higher Education the Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
Russia, St. Petersburg, Moika River emb. 61,
emails: ptitsina_lk@inbox.ru, gusev999dima@gmail.com

Abstract: The article shows the conditionality of intellectualization of complex information security systems. Possible approaches to the intellectualization of complex information security systems are presented. The didactic elements of possible approaches to intellectualization are considered. The prerequisites for the formation of the model-analytical intelligence of complex information security systems are given. Methodological development of model-analytical intelligence is singled out. The proposed principles for the distribution of model-analytic intelligence in the architectures of complex information security systems are described.

Keywords: information security; system of information protection; intellectualization; model-analytical intelligence; distribution; architecture.

В развитии информационных инфраструктур за последние десятилетия выделяются такие закономерности, как высочайшие темпы разработки новых технологий, формирования гипертехнологических кластеров, обновления высокопроизводительных систем, объединения вычислительных систем в крупномасштабные вычислительные сети, роста количества и ценности передаваемой и обрабатываемой информации, расширения клиентской базы, унификации архитектур вычислительных сетей и хранилищ данных.

В условиях экономики знаний информационные инфраструктуры становятся неотъемлемой составляющей индустрии информации, обеспечивающей формирование и развитие наукоёмких отраслей профессиональной деятельности.

С ростом масштабов профессиональной деятельности, погружаемой в информационные инфраструктуры, расширяются пространства полей возможных угроз и повышается степень априорной неопределённости относительно их описания и последствий воздействия на техногенные системы, результаты труда и состояние социума в целом. Указанные особенности сопровождаются возникновением новых проблем в информационной безопасности.

В описанных условиях проявляется острейшая необходимость в обеспечении информационной безопасности с сохранением доступности услуг сетей для непрерывно расширяющейся базы их клиентов, разработке технологий, регламентирующих создание систем информационной безопасности с многообразием профилей качества.

Непрерывно расширяющимися границами областей применения крупномасштабных информационных инфраструктур и жесткими условиями конкурентной борьбы за потребителя

обуславливается устойчивое развитие программного обеспечения комплексных систем защиты информации.

Одним из перспективных направлений развития программного обеспечения комплексных систем защиты информации является его интеллектуализация.

Согласно современным представлениям о развитии искусственного интеллекта, описанным в [1], интеллектуализация программного обеспечения комплексных систем защиты информации может основываться на когнитивном моделировании, автоматизации процесса проведения рассуждений и использовании рациональных агентов.

В парадигме, предусматривающей когнитивное моделирование, формальные подходы к интеллектуализации комплексных систем защиты информации могут опираться на сочетание математических моделей, разрабатываемых в теории искусственного интеллекта, и экспериментальных методов, исследуемых в психологии.

В парадигме, предусматривающей автоматизацию процесса проведения рассуждений, формальные подходы к интеллектуализации комплексных систем защиты информации могут базироваться на моделях и методах теорий логик и формальной теории убеждений. В этом случае главный акцент делается на автоматическом формировании правильных логических выводов.

В парадигме, предусматривающей использование рациональных агентов, главная роль отводится таким действиям, при которых удаётся достичь наилучшего результата в условиях неопределённости либо наилучшего ожидаемого результата.

Парадигмы, выделенные согласно теории искусственного интеллекта, могут дополняться за счёт отображения знаний, аккумулирующих результаты исследований в области информационной безопасности. Один из путей формирования дополнительной парадигмы связывается с формированием модельно-аналитического интеллекта комплексных систем защиты информации, учитывающим обширные возможности комплексирования систем.

Современные методы комплексирования различаются по задействованным формам избыточности, присущей системам защиты информации. Среди задействованных форм выделяются: структурная избыточность аппаратных средств; структурная избыточность программных средств; структурная избыточность аппаратно-программных средств; функциональная избыточность аппаратных средств; функциональная избыточность программных средств; функциональная избыточность аппаратно-программных средств; временная избыточность; протокольная избыточность; модельная избыточность.

Методы генерации модельно-аналитического интеллекта комплексных систем защиты информации при различных формах избыточности раскрываются в [2]. Помимо представленных различий, наблюдаются альтернативные тенденции в организации и распределении функциональных задач по комплексируемым системам защиты информации в соответствии с определёнными классами защищённости.

В [3] представляются методы формирования модельно-аналитического интеллекта комплексных систем защиты информации, которые базируются на агентных технологиях.

Наряду с выделенными методологическими разработками, проводятся исследования по выявлению новых возможностей при сочетании парадигмы, основанной на рациональных агентах, и парадигмы, предусматривающей введение модельно-аналитического интеллекта в их архитектуру. В [4] описывается методология формирования модельно-аналитического интеллекта агентов при достижении целей по обеспечению информационной безопасности, включающая расширенное объектно-ориентированное моделирование и аналитический вывод показателей качества программных агентов.

Предлагаемые альтернативные варианты функциональных спецификаций модельно-аналитического интеллекта основываются на планируемой распределённости его компонентов по тем системам защиты информации, которые комплексированы в целях соблюдения требований, соответствующих определённому классу защищённости.

Основные идеи предлагаемой концепции распределения модельно-аналитического интеллекта по компонентам комплексных систем защиты информации заключаются в следующих положениях:

- условия соответствия определённому классу защищённости остаются неизменными для всего жизненного цикла модельно-аналитического интеллекта;
- функциональные модели комплексных систем защиты информации соответствуют методологии расширенного объектно-ориентированного моделирования;
- в описаниях моделей присутствуют априорно неопределённые параметрические пространства и спецификации;
- комплексные системы защиты информации разворачиваются в распределённой инфраструктуре;
- каждая система защиты информации ориентируется на обнаружение, идентификацию и отражение профильных типов угроз.

Реализация изложенной концепции может осуществляться на множестве альтернативных архитектур комплексных систем защиты информации с распределённым по мультиагентной системе модельно-аналитическим интеллектом.

СПИСОК ЛИТЕРАТУРЫ

1. Искусственный интеллект: современный подход, 2-е изд. : Пер. с англ. – М. : Издательский дом «Вильямс», 2007. 1408 с.
2. Птицын, А.В., Птицына, Л.К. Аналитическое моделирование комплексных систем защиты информации. Гамбург. Saarbrücken: LAP LAMBERT Academic Publishing, 2012. 293 с.
3. Птицын А. В. Методологический базис агентных технологий для обеспечения информационной защищённости // Научные технологии в космических исследованиях Земли. 2015. Т.7. № 1. С. 50-55.
4. Птицына Л.К., Птицын А.В. Обеспечение информационной безопасности на основе методологического базиса агентных технологий // Вестник Брянского государственного технического университета. 2017. № 2 (55). С. 146 -154.

УДК 004.056.53

АНАЛИЗ СОВРЕМЕННЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДОВ ПРОНИКНОВЕНИЯ В КОМПЬЮТЕРНУЮ СИСТЕМУ

Лукин Евгений Игоревич¹, Прокопович Максим Сергеевич², Федоров Дмитрий Юрьевич

¹ Санкт-Петербургский государственный экономический университет,
Россия, Санкт-Петербург, ул. Садовая, 21,

² Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, Санкт-Петербург, ул. Профессора Попова, 5.

emails: genya.lukin@yandex.ru, mxm.prokopovich@gmail.com, dmitriy.fedoroff@gmail.com

Аннотация: В статье был проведен анализ современных угроз информационной безопасности, методов проведения компьютерных атак. В результате были предложены способы защиты информационных системы от злоумышленников. Для сбора статистики был выбран метод моделирования уязвимой машины (honeypot).

Ключевые слова: моделирование; вирусы; сети; проникновение; обратная разработка; программирование; уязвимости.

ANALYSIS OF MODERN THREATS OF INFORMATION SECURITY AND METHODS OF PENETRATION IN THE COMPUTER SYSTEM

Lukin Evgeny¹, Prokopovich Maxim², Fedorov Dmitry

¹ The St. Petersburg State University of Economics",
Russia, St. Petersburg, Sadovaya str. 21,

² The St. Petersburg State Electrotechnical University "LETI",
Russia, St. Petersburg, Professor Popov str. 5.

emails: genya.lukin@yandex.ru, mxm.prokopovich@gmail.com, dmitriy.fedoroff@gmail.com

Abstract: The article analyzes the current threats, attack methods, the structure of some of them, ways to protect the system from intruders. For the collection of statistics was the chosen method for modeling a vulnerable machine (honeypot).

Keywords: modeling; viruses; network penetration; reverse engineering; programming; vulnerability.

Введение. В современных реалиях злоумышленники все больше и больше времени уделяют компьютерным технологиям. Развитие компьютерных технологий и увеличение числа злоумышленников ведет к появлению угроз информационной безопасности. В представленной работе был проведен анализ современных сетевых угроз, способов их реализации на примере удаленного проникновения в компьютерную систему.

Целью работы является повышение уровня безопасности компьютерных систем через выявление наиболее уязвимых мест в системе, которые могут привести к несанкционированному доступу злоумышленника в сеть и похищению конфиденциальных данных.

Задачи работы: исследование активности злоумышленников в сетевом пространстве и последующее изучение результатов для выведения статистической картины угроз на текущий момент времени. Формирования рекомендаций для усиления защиты персональных компьютеров, мобильных телефонов и различных устройств, которые относятся к интернету вещей [1].

Для исследования несанкционированных методов проникновения в компьютерную систему были рассмотрены различные вредоносные типы программ: трояны (бекдоры, банкеры, дропперы) и ботнеты.

В качестве инструментария исследования были использованы три сервера, сконфигурированные в виде приманок - honeypot. Данные серверы представляют собой эмуляцию машин, уязвимых к различным типам атак, но попытка их эксплуатации приведет лишь к записи в лог-файл. На основе полученной информации была собрана статистика по наиболее часто используемым уязвимостям и методам проникновения в компьютерную систему, а также предложены способы защиты от

вредоносных атак, что позволит предотвратить выход их строя системы и потерю важной информации [2].

В современных реалиях очень важно быть готовым к атакам в информационной среде, поэтому следует следить за вирусной и пользовательской активностью, защищать свои системы от современных уязвимостей.

СПИСОК ЛИТЕРАТУРЫ

1. Актуальные вопросы безопасности современных информационных технологий: Монография / [Р.Р. Бежан и др.]; Под ред. д-ра экон. наук, проф. Е.В. Стельмашонок. – СПб : Изд-во СПбГЭУ, 2015. – 164 с.
2. Федоров, Ю. Программирование на языке высокого уровня Python : учеб. пособие для прикладного бакалавриата / Д. Ю. Федоров. – М. : Издательство Юрайт, 2017. – 126 с.

УДК 004.8

СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА ПРИМЕРЕ ВЫСШЕГО УЧЕБНОГО ЗАВЕДЕНИЯ

Сазонов Антон Борисович, Немченко Алексей Алексеевич
Федеральное государственное автономное образовательное учреждение высшего образования
«Санкт-Петербургский государственный университет аэрокосмического приборостроения»
Россия, Санкт-Петербург, ул. Большая Морская, 67, лит. А
emails: sazonov-anton@mail.ru, nemchenko_aleks@mail.ru

Аннотация: Статья посвящена системам контроля и управления доступом, развернутых в учебных заведениях высшего образования. Рассмотрены основные проблемы, которые помогают решить установка СКУД.

Ключевые слова: Системы контроля и управления доступом.

ACCESS CONTROL AND MONITORING SYSTEM, FOR EXAMPLE, A HIGHER EDUCATION INSTITUTION

Sazonov Anton ,Nemchenko Aleksey
Federal State Autonomous Educational Institution of Higher Education " Saint-Petersburg State University of
Aerospace Instrumentation"
Russia, St. Petersburg, st. Bolshaya Morskaya, 67, lit. A
emails: sazonov-anton@mail.ru, nemchenko_aleks@mail.ru

Abstract: The article is devoted to access control systems and administrations deployed in educational institutions of higher education. The main problems that solve the installation of ACS

Key words: Access control system.

Система контроля и управления доступом – это комплекс программно-аппаратных средств безопасности нацеленных на ограничение и регистрацию объектов (человек, машина), на вход и выход из заданной территории через точки прохода, такие, как КПП, двери и ворота. Основную роль, которую выполняет СКУД - управление доступом на заданную территорию. СКУД позволяет разграничивать доступ на заданную территорию и идентифицировать лицо, имеющую к ней доступ. СКУД состоит из считывателя, контроллера, конвертера среды и магнитного замка, а для идентификации объекта использует идентификатор – ключ, карта или брелок [1].

Рассматривая проекты системы контроля и управления доступом (далее – СКУД), можно сделать вывод, что на сегодняшний день возможности СКУД остаются недооценёнными. СКУД позволяет устранить несколько проблем крупных организаций. Одна из таких проблем многопользовательский доступ к лекционным аудиториям учебных заведений высшего образования. Для того, чтобы начать проводить лекцию преподавателю необходимо взять ключ от аудитории в бюро пропусков и вернуться в аудиторию. В данном случае это может занимать дополнительное время, так как если у другого преподавателя была пара в этой же аудитории раньше, то сначала придется дождаться ключа, а уже после этого начинать проведение пары. СКУД решает данную проблему тем, что преподаватель сможет использовать свой личный пропуск как ключ к магнитному замку. В данном случае СКУД позволяет сформировать базу для контроллера в соответствии с расписанием преподавателя.

Следующую проблема, которую поможет решить СКУД – это возможность отслеживания посещения пар студентами. Для реализации такой возможности предлагается поставить либо промышленный считыватель с мощной антенной, либо считыватель большего радиуса действия. В данном случае преподаватель всегда будет иметь возможность просмотреть электронный журнал и проверить посещаемость конкретного студента. Так же СКУД может помочь реализовать возможность для временного доступа по индивидуальной ключ-карте к аудитории, в которой преподаватель не ведет пары, но ему нужно заменить его коллегу [2].

Закключение. СКУД предоставляет широкие возможности по настройке и оптимизации рабочего процесса. На примере системы, разрабатываемой для вуза, можно убедиться, что СКУД позволяет

интегрировать себя в любую систему. Благодаря установке СКУД снижаются эксплуатационные расходы на поддержания в работе механических замков. Подобная система сэкономит значительное время и позволит преподавателям начинать пары во-время. Это улучшит как качество рабочей среды, так и производительность труда, следовательно, повысит качество усвоения учебного материала у студентов.

СПИСОК ЛИТЕРАТУРЫ

1. Национальный стандарт РФ ГОСТ Р 51241-2008 "Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 17 декабря 2008 г.) - 430 - с
2. Примеры проектов СКУД [Электронный ресурс]. – URL: <http://www.cleper.ru/project/category/kontrol-dostupa.php>. – (Дата обращения: 20.09.2017)

УДК 003.26

ФОРМАЛИЗОВАННЫЙ ПОДХОД К АНАЛИЗУ ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ

Уткина Алена Алексеевна, Юркин Дмитрий Валерьевич

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Россия, Санкт-Петербург, пр. Большевиков, 22-1,
emails: alena_utkina_95@mail.ru, dvyrurkin@yandex.ru

Аннотация: В статье рассмотрено применение аппарата логики формализованного анализа протоколов аутентификации – BAN-логики. На основе предикатов и постулатов формализованной логики проведен анализ протокола аутентификации Никитина-Юркина с использованием бесключевых хэш-функций. В результате проведенного анализа были выявлены недостатки протокола, которые ограничивают область его применения. Проведена модификация исходного протокола, в результате чего были устранены выявленные в ходе анализа недостатки.

Ключевые слова: аутентификация; уязвимости протоколов аутентификации; BAN-логика; формализованный анализ; логика аутентификации, бесключевые хэш-функции

FORMALIZED APPROACH TO THE ANALYSIS OF AUTHENTICATION PROTOCOLS

Utkina Alena, Yurkin Dmitriy

The Bonch-Bruevich St. Petersburg State University of Telecommunications,
Russia, St. Petersburg, Prospekt Bolshevikov, 22-1,
emails: alena_utkina_95@mail.ru, dvyrurkin@yandex.ru

Abstract: The article considers the application of the logic device for formalized analysis of authentication protocols - BAN-logic. Based on the predicates and postulates of formalized logic, an analysis of the authentication protocol of Nikitin-Yurkin using keyless hash functions was performed. As a result of the analysis, there were revealed the disadvantages of the protocol, which limit the scope of its application. The original protocol was modified, as a result of which the shortcomings identified during the analysis were eliminated.

Keywords: authentication; the vulnerability of authentication protocols; BAN-logic; formalized analysis; authentication logic, keyless hash functions

Введение. В настоящее время, в зависимости от различных требований к автоматизированным системам в защищенном исполнении, существует множество различных криптографических протоколов аутентификации [1-3]. Поиск уязвимостей в системах управления доступом к защищаемым информационным ресурсам является актуальным, вследствие чего возникает необходимость формализованного анализа самой модели работы протокола. В статье рассмотрен аппарат логики формализованного анализа протоколов аутентификации, проведен анализ протокола аутентификации, использующего бесключевые хэш-функции, с целью выявления уязвимостей.

Аппарат BAN-логики. BAN-логика – это метод формализованного анализа криптографических протоколов, по результатам применения которого можно получить ответ на ряд вопросов, таких как:

– Какие фактические задачи выполняет этот протокол.

– Присутствуют ли в этом протоколе избыточные действия, от которых можно избавиться без ослабления работы протокола.

– Обеспечивает ли должную конфиденциальность передаваемых данных этот протокол, и могут ли скомпрометировать отправленные в открытом явном виде данные ход его работы [4-8].

Основной целью разработки метода является объяснение основных концепций при проверке подлинности, так как BAN-логика большей частью построена на парадигме доверия [9-11].

Протокол аутентификации с использованием бесключевых хэш-функций. В данной статье рассмотрен протокол аутентификации Никитина-Юркина. Данный протокол предусматривает двухстороннюю аутентификацию корреспондентов путем передачи всего двух сообщений. Для однонаправленного преобразования информации используются бесключевые хэш-функции, а общий секрет используется в качестве входной переменной хэш-функции [12, 13]. Данный протокол был

проанализирован с помощью механизма BAN-логики. В результате проведенного анализа было выявлено два недостатка в работе протокола:

1. при получении общего ключа от центра распределения ключей оба корреспондента не могут точно знать, в какое время было отправлено сообщение, содержащее ключ; знание о свежести сообщения является необходимым условием для дальнейшей работы протокола аутентификации;

2. данный протокол аутентификации не может быть использован для того, чтобы уникально идентифицировать трех и более корреспондентов, среди которых распределен общий секрет, так как невозможно однозначно определить, кем именно был послан сгенерированный хэш, поскольку каждый из участников мог его сгенерировать.

Исследуемый протокол был модифицирован, а именно, было принято решение дополнить первое сообщение от центра распределения ключей, в котором содержится общий ключ для корреспондентов, временной меткой. В результате данного преобразования исключается первый из выявленных недостатков.

Закключение. Использование механизма BAN-логики является надежным способом описания протоколов. При использовании формализованного анализа можно определить, какие действия выполняет тот или иной протокол, а также выявить его типовые недостатки. Необходимо отметить что, по причине работы изложенных методов на абстрактном уровне, не рассматриваются такие аспекты специфики реализации протоколов как, например, корректность использования криптосистем. Также, было отмечено, что, несмотря на то, что допускается возможность существования злоумышленников, данный метод концентрируется исключительно на доверии надежных сторон, которые участвуют в процессе аутентификации.

В работе был произведен анализ протокола аутентификации с использованием бесключевых хэш-функций с использованием механизма BAN-логики. При анализе не было выявлено избыточных шагов, без которых процесс аутентификации выполнялся бы успешно. Однако, было выявлено два существенных недостатка, один из которых был успешно устранён.

Рассмотренный протокол предоставляет достаточно быструю и надежную аутентификацию субъектов информационного обмена, поскольку в нем используется передача только двух сообщений при определении доступа субъектов к информационным ресурсам, а также в нем используются бесключевые хэш-функции для преобразования информации, что не требует периодической смены ключа, как в случае использования ключевой хэш-функции. Однако, данный способ аутентификации требует доработки для того, чтобы при его использовании стала возможна аутентификация трех и более корреспондентов.

СПИСОК ЛИТЕРАТУРЫ

1. Burrows M., Abadi M., Needham R. M. A logic of authentication // Rep. 39, Digital Equipment Corporation Systems Research Center, Palo Alto, Calif. 1989. P.3-13.
2. Burrows M., Abadi M., Needham R. M. A logic of authentication // ACM Transactions on Computer Systems. 1990. Vol. 8. N 1. P. 18-36.
3. Chatzieleftheriou, G., Bonakdarpour, B., Katsaros, P., Smolka, S. Abstract Model Repair. Logical Methods in Computer Science. 2015.
4. Watkins L., Robinson W.H., Beyah, R.A. A Passive Approach to Rogue Access Point Detection // Global Telecommunications Conference, Washington. 2007. P. 355-360.
5. Chong E., Loo M., Christopher L., Marimuthu P. Intrusion Detection for Routing Attacks In Sensor Networks // International Journal of Distributed Sensor Networks. 2006. Vol 2. N 1. P. 313-332.
6. Chung-Hsin L., Po-Cheng T., Chun-Lin L., Kuo-Hao L. The Study of the Wireless Network Dos Attack // Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human, New York. 2009. P. 418-421.
7. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model, Version 3.1 // Common Criteria Portal. 2006. <http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf> (дата обращения: 20.10.2013).
8. Common Criteria for Information Technology Security Evaluation. Part 2: Security functional requirements, Version 3.1. // Common Criteria Portal. 2006. <http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R3.pdf> (дата обращения: 20.10.2013).
9. Wagatsuma K., Anze S., Goto Y., Cheng J. Formalization for Formal Analysis of Cryptographic Protocols with Reasoning Approach // Future Information Technology. 2014. P. 211-218.
10. Косачев А.С., Пономаренко В.Н. Анализ подходов к верификации функций безопасности и мобильности. – М.: Триумф, 2004. – 101 с.
11. Могилевская Н.С., Новиков А.М. Формализация и анализ протоколов аутентификации // Информационное противодействие угрозам терроризма. Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования "Южный федеральный университет" в г. Таганроге (Таганрог). 2009. №12. С.99-102. ISSN: 2219-8792
12. Юркин Д. В., Никитин В. Н. Анализ протоколов шифрования. Журнал радиоэлектроники. №4. 2009. <http://jre.cplire.ru/jre/apr09/5/text.html> (дата обращения: 14.10.2013).
13. Юркин Д. В., Никитин В. Н. Улучшение способов аутентификации для каналов связи с ошибками. // Информационно-управляющие системы. №6. 2010. С. 42-46.

УДК 004.056

**ПРЕДВАРИТЕЛЬНАЯ ОБРАБОТКА ГРАФИЧЕСКИХ ОБЪЕКТОВ ДЛЯ ЗАДАЧИ ИДЕНТИФИКАЦИИ
В ВИДЕОПОТОКЕ**

Шевченко Денис Алексеевич

Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики,
Россия, Санкт-Петербург, Кронверкский проспект, 49,
email: dashevchenko@corp.ifmo.ru

Аннотация: В статье рассматривается задача подготовки исходных данных для последующей идентификации в видеопотоке, проведено исследование взаимодействия различных методов цифровой обработки изображений между собой. В результате работы сформирован определенный порядок операций, применяемых к видеоизображению, позволяющий добиться наилучшего результата.

Ключевые слова: обработка изображений; идентификация объектов

**PRELIMINARY PROCESSING OF GRAPHIC OBJECTS FOR IDENTIFICATION IN THE VIDEO
SEQUENCE**

Shevchenko Denis

St. Petersburg National Research University of Information Technologies, Mechanics and Optics, Russia,
Saint Petersburg, Kronverkskiy Prospekt, 49,
email: dashevchenko@corp.ifmo.ru

Abstract: The article deals with the problem of preparing the initial data for the subsequent identification in a video stream, conducting studies of the interaction of various methods of digital image processing. As a result of the work, the order of operations is formed which allows to achieve the best result.

Keywords: image processing; object identification

Введение. Постоянно набирающий темпы технический прогресс приводит к повсеместному распространению устройств видеофиксации. Наряду с портативными цифровыми камерами увеличивается количество систем видеонаблюдения, цифровых видеорегистраторов, телефонов с камерами. Все это способствует повышению качества цифровых изображений и видеоматериалов. Несмотря на то, что качество технологии цифровых камер постоянно улучшается, цифровые изображения, используемые в криминалистических исследованиях, часто не являются релевантными. Такие проблемы, как плохое разрешение, низкая контрастность, неточное воспроизведение цвета, размытие и шум, являются типичными при использовании цифровых изображений. Методы улучшения качества изображения могут быть использованы для решения многих из этих проблем.

Производители программного обеспечения для информационных систем предоставляют решения подобного рода, однако предлагаемые ими алгоритмы разрознены и требуют детальной настройки. Исследователи не ставят своей целью создать всеобъемлющую и универсальную технологию обработки фото- и видеоизображений с целью улучшения их визуального качества, а решают узкие конкретные задачи. Произвольное объединение множества разнородных алгоритмов в рамках единой технологии приводит к падению качества обработки изображений из-за слабой согласованности отдельных алгоритмов. В связи с этим актуальной является проблема разработки и согласования алгоритмов улучшения качества фото- и видеоматериалов.

В работе произведены формирование обобщенного подхода к улучшению качества видеоизображения, разработка метода обработки видеоданных, разрешающего проблему несогласованности существующих методов повышения визуального качества видеоизображений, на основе методов дискретной обработки сигналов, цифровой обработки изображений. Практическая значимость исследования состоит в применимости разработанной методики при проведении расследований инцидентов, требующих исследования видеоматериалов.

Большинство методов улучшения визуального качества изображений, могут применяться последовательно для достижения наилучшего эффекта. Однако процессы шумоподавления и тональной компрессии тесно связаны между собой и в некоторых случаях не могут выполняться последовательно. Одним из самых сложных случаев при улучшении визуального качества видеоизображения является низкий динамический диапазон яркостей изображения. В этом случае значения интенсивности шумов могут быть сопоставимы со значениями интенсивности сцены изображения. Такая ситуация возникает, например, при видеосъемке в обстановке с низкой освещенностью. Прямое растяжение динамического диапазона видео с низким освещением провоцирует появление различных нежелательных эффектов, таких как усиление шума, насыщенность интенсивности и снижение разрешения. Таким образом, перед тем, как сжать динамический диапазон, необходимо выполнить подходящую процедуру шумоподавления. Однако, несмотря на то, что перед шагом тональной компрессии удалится значительное количество шума, шум, усиленный на этапе

тональной компрессии, должен быть удален с помощью подходящего метода шумоподавления. Предлагаемый метод улучшения видеоизображения основан на алгоритмах улучшения изображений. Видео с низким динамическим диапазоном сначала подвергается временной фильтрации, затем тональной компрессии, и в завершение фильтруется в пространственной области. Несмотря на то, что значительное количество шума ослабляется после временного шумоподавления, оставшийся шум усиливается на этапе тональной компрессии. Для пространственного шумоподавления в работе используется алгоритм нелокальных средних, который измеряет сходство между соседним и опорным блоком. Алгоритм нелокальных средних вычисляет средневзвешенное значение пикселей в пространстве, рассматривая сходство между пикселями для понижения шумов изображения.

В результате исследований, проведенных в данной работе, было обнаружено, что порядок применения определенных методов улучшения изображений может повлиять на визуальную точность обрабатываемого изображения. Проводя тестирование различных комбинаций методов обработки изображений, было определено следующее: чересстрочное видео не может быть точно приведено в соответствие с прогрессивной разверткой после применения таких операций, как интерполяция, корректировка размытия и корректировка искажения. Шум может негативно повлиять на алгоритмы устранения размытости, регулировки контрастности и увеличения резкости. Корректировка размытости негативно влияет на видимость после увеличения резкости и корректировки цвета. Корректировка размытости не может быть корректно выполнена после корректировки искажения. Наконец, устранение размытости и корректировка цвета могут помочь определить области, которые могут быть улучшены путем увеличения резкости. В результате исследования был разработан такой порядок операций для обработки графических данных, при котором увеличивается эффективность каждого метода улучшения изображений. Основной целью установления порядка операций является обеспечение качества обработки видеоданных. Порядок операций устанавливает правила, которые уменьшают вероятность появления ошибки вследствие человеческого фактора и способствуют проведению надежного анализа. Если порядок является обоснованным, может быть повышена уверенность в том, что эксперты будут создавать визуально сопоставимые результаты и что эти результаты с меньшей вероятностью искажают исходные данные.

Заключение. Предлагаемый порядок операций по улучшению изображений направлен на нахождение оптимального баланса между повышением информативности изображения и уменьшением артефактов посредством исследования свойств изображений и взаимодействия методов обработки изображений между собой.

СПИСОК ЛИТЕРАТУРЫ

1. Гонсалес Р., Вудс Р. Цифровая обработка изображений: Учебное пособие – М.: Техносфера, 2012, 1104 с.
2. Опленгейм А., Шафер Р. Цифровая обработка сигналов: Учебное пособие – М.: Техносфера, 2012, 1048 с.

УДК 4.056

ИССЛЕДОВАНИЕ ДЕЙСТВУЮЩЕЙ ИТ-ИНФРАСТРУКТУРЫ ОРГАНИЗАЦИИ ДЛЯ ПОСЛЕДУЮЩЕГО ПЕРЕХОДА К ОБЛАЧНОЙ АРХИТЕКТУРЕ

Чмутов Михаил Валериевич, Ковцур Максим Михайлович, Ушаков Игорь Александрович,
Пестов Игорь Евгеньевич

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Россия, 193232, Санкт-Петербург, пр. Большевиков 22,
emails: frost32.ru@yandex.ru, maxkovzur@mail.ru, ushakovia@gmail.com, pestovie@outlook.com

Аннотация: Переход к облачной ит-архитектуре стал для многих организаций реальностью. То, что еще не так давно обсуждалось на перспективу, сегодня требует скорейшего внедрения и реализации. В данной статье авторы рассматривают начальный этап управления процессами миграции с традиционной ит - инфраструктурой на облачную

Ключевые слова: Облачная архитектура, OpenStack, единая информационная система, открытое ПО

A STUDY OF THE EXISTING IT INFRASTRUCTURE FOR FUTURE TRANSITION TO CLOUD ARCHITECTURE

Mihail Chmutov, Maksim Kovcur, Igor Ushakov, Igor Pestov

Federal State Budget-Financed Educational Institution of Higher Education The Bonch-Bruевич Saint - Petersburg State University of Telecommunications, Russia, Saint-Petersburg, ProspektBolsheviko, 22
emails: frost32.ru@yandex.ru, maxkovzur@mail.ru, ushakovia@gmail.com, pestovie@outlook.com

Abstract: The transition to cloud-based it architecture has become for many organizations a reality. What else has discussed on the future, today calls for a speedy adoption and implementation. In this article, the authors consider the initial stage of management of processes of migration from traditional it to cloud infrastruclu

Keywords: *Cloud architecture OpenStack, a unified information system, open source*

Переход к облачной ит-архитектуре стал для многих организаций реальностью. То, что еще не так давно обсуждалось на перспективу, сегодня требует скорейшего внедрения и реализации. В данной статье авторы рассматривают начальный этап управления процессами миграции с традиционной ит-инфраструктуры на облачную. Стоит отметить, что облачные вычисления меняют наше представление об информационных технологиях, и это не просто очередное веяние моды. Потребители используют облако для хранения музыкальных записей. Молодые предприятия обращаются к облаку, чтобы встать на ноги и начать работать без непомерных инвестиций. Крупные фирмы и госучреждения опираются на облако, чтобы сделать доступными больше данных. Облачные вычисления меняют характер функционирования бизнеса и общества, открывая широкие возможности для инноваций. Мы видим, как разработчики объединяют информационные системы с системами общения, создавая облачные приложения нового типа. Это системы взаимодействия [1].

Анализ. Прежде всего рассмотрим назначение, состав и общее описание логической структуры ИТ-инфраструктуры предприятия. ИТ инфраструктура имеет общее название Единая информационная система предприятия (далее – ЕИС предприятия) и реализуется на базе локальной вычислительной сети, в своем составе имеет:

- программно-аппаратный комплекс
- аппаратную платформу – сервер;
- системное и прикладное программное обеспечение - операционную систему «Серверная операционная система с интегрированными серверными службами».
- активное сетевое оборудование – коммутатор Cisco Catalyst;
- пассивное сетевое оборудование;
- сетевое устройство хранения данных;
- автоматизированное рабочее место (далее – АРМ) пользователя (на базе ПЭВМ).

ЕИС предприятия осуществляет обмен данными с внешними автоматизированными системами через Корпоративную мультисервисную сеть передачи данных (КМСПД) предприятия [2].

Каналы передачи данных (основной и резервный) используют телекоммуникационные сети (магистральные IP-сети) оператора связи, предоставляющего услуги с использованием технологии IP MPLS. Подключение к магистральным IP-сетям оператора связи осуществляется через PE-маршрутизаторы расположенные на границе сети IP MPLS. В качестве поставщиков услуг линии доступа к магистральной IP-сети оператора связи выступают региональные операторы связи [3].

Система защиты информации КМСПД обеспечивает безопасность передаваемой информации между подключенными к ней автоматизированными системами.

Далее рассмотрим назначение состав и общее описание физической структуры ЕИС.

Компонент обработки персональных данных ЕИС включает следующие функциональные составные части:

1. Центр обработки данных, в котором расположена серверная платформа, которая непосредственно обеспечивает обработку персональных данных.

2. Серверная платформа включает:

- средства вычислительной техники (аппаратные ресурсы);
- системное серверное программное обеспечение;
- прикладное серверное программное обеспечение.

Автоматизированные рабочие места пользователей, которые обеспечивают доступ сотрудников предприятия к персональным данным. Автоматизированные рабочие места пользователей включают

- средства вычислительной техники (аппаратные ресурсы);
- системное клиентское программное обеспечение;
- прикладное клиентское программное обеспечение.

Функциональная составная часть Центра обработки данных (ЦОД) компонента реализована на базе локальной вычислительной сети, развернутой в арендованном помещении. Центр обработки данных построен по принципу горячего резервирования основных средств вычислительной техники. Всё оборудование ЦОД располагается в 9 арендованных стойках, размещенном в здании узла междугородней, международной связи ММТС [4].

Функциональные составные части Автоматизированных рабочих мест пользователей, реализованы на базе локальных вычислительных сетей, развернутых в пределах контролируемой зоны центрального офиса предприятия и территориальных офисов.

Компонент обработки персональных данных ЕИС обеспечивает обработку персональных данных только в части прикладных программных средствах.

«Прикладные программные средства имеют в своем составе серверную часть, на базе OracleApplicationServer (на сервере приложений) и системы управления базами данных OracleDatabaseServer (на сервере баз данных) и клиентские части (на автоматизированных рабочих местах).

Сервер приложений и сервер баз данных функционируют на двух аппаратных платформах. Сервер приложений, на SunFire (платформа RISC). Сервер баз данных, на SunEnterprise (платформа RISC). Оба сервера функционируют под управлением операционной системы Solaris.

Клиентская часть прикладных программных средств функционирует на Автоматизированных рабочих местах пользователей под управлением операционной системы MicrosoftWindows на аппаратной платформе Intel x86 и представляет собой стандартный браузер для просмотра HTML страниц.

Модель организации построена на базе доменных серверов в локальной вычислительной сети, сеть объединяет компьютеры под одной общей политикой безопасности и управляется централизованно. Это необходимо так как:

- локальная сеть постоянно развивается и количество пользователей растет;
- видоизменяется топология и география сети;
- необходимо разграничить доступ к ресурсам для каждого пользователя или группы;
- необходим контроль за использованием ресурсов сети интернет.

В данный момент организация переходит на уровень выше, а именно, от соединения офисов оптикой к использованию облачных вычислений. Так как локальная сеть постоянно развивается и растет, то при последующем разделении на офисы придется соединить между собой каждую сеть офиса, гораздо удобнее и логичнее использовать облачные системы, а защищенность соединения гарантировать каналами VPN. При этом по требованиям предприятия облачная архитектура должна строиться на базе ПО с открытым исходным кодом и открытых стандартов.

Базовым решением для построения нового типа архитектуры был выбран OpenStack. Это комплекс проектов свободного программного обеспечения, который может быть использован для создания инфраструктурных облачных сервисов и облачных хранилищ, при том как публичных, так и частных. Все проекты комплекса распространяются под лицензией ApacheLicense [5].

Выводы.

В рамках данной работы авторы рассматривают текущую архитектуру предприятия для проведения исследования методов развертывания и миграции ит-инфраструктуры в облачной среде Openstack. Планируется использование открытого и свободного программного решения для автоматизации создания виртуальных кластеров Apache в облачной среде Openstack. В рамках моделирования процесса миграции авторы планируют провести анализ частного случая атаки на облачную инфраструктуру, вычислить условия устойчивости системы, провести расчеты бифуркационного рождения предельного цикла. Для решения данной задачи потребуется: провести анализ методик оценки рисков нарушения информационной безопасности. Рекомендации по управлению и оценкам содержатся во многих международных и отечественных регламентирующих документах и обоснованы существующей практикой развития информационных технологий, служб, регуляторов в разных странах [6].

СПИСОК ЛИТЕРАТУРЫ

1. Открытая облачная архитектура IBM // Режим электронного доступа: <https://www.ibm.com/developerworks/ru/library/cl-open-architecture/index.html> (дата обращения 22.09.2017)
2. КОНТРОЛЬ, ИЗМЕРЕНИЕ И ИНТЕЛЛЕКТУАЛЬНОЕ УПРАВЛЕНИЕ ТРАФИКОМ /Алейников А.А., Билятдинов К.З., Красов А.В., Левин М.В. //монография / Санкт-Петербург, 2016;
3. Возможности управления трафиком в рамках концепции SDN /Красов А.В., Левин М.В. /В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании IV Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 томах. 2015. С. 350-354;
4. Технические аспекты управления с использованием сети интернет /Алейников А.А., Билятдинов К.З., Красов А.В., Кривчун Е.А., Крысанов А.В. //Монография / Санкт-Петербург, 2016;
5. OpenStack® Ocata Strengthens Core Infrastructure Services and Container Integration with 15th Release of Cloud Computing Software // Режим электронного доступа: <https://www.openstack.org/news/view/302/openstack-ocata-strengthens-core-infrastructure-services-and-container-integration-with-15th-release-of-cloud-computing-software> (дата обращения 22.09.2017);
6. Виткова Л.А. Исследование и разработка адаптивных систем информационной безопасности на основе теории бифуркации / Виткова Л.А., Андрианов В.И.// В сборнике: АПИНО II МНТНМК 2013. С. 813-815.

УДК 004.056

ЗАКОН СОХРАНЕНИЯ ЦЕЛОСТНОСТИ ОБЪЕКТА В УСЛОВИЯХ РАЗРУШЕНИЯ ПРОГРАММНО-АППАРАТНОЙ СРЕДЫ

Мокеева Татьяна Олеговна, Долгирева Елена Сергеевна, профессор Бурлов Вячеслав Георгиевич
Государственный университет морского и речного флота имени адмирала С.О.Макарова
Россия, Санкт-Петербург, ул.Двинская 5/7
emails: mokeeva-t-o@yandex.ru, lenin91@mail.ru, burlovvg@mail.ru

Аннотация: в статье рассмотрена эффективность применения закона сохранения целостности при разработке компьютерных технологий.

Ключевые слова: модель; объект; управление; защита; программно-аппаратная среда.

THE LAW OF PRESERVING THE INTEGRITY OF THE OBJECT IN THE CONDITIONS OF DESTRUCTION OF SOFTWARE HARDWARE

Mokeyeva Tatiana, Dolgireva Elena, professor Burlov Viacheslav
Admiral Makarov State University of maritime and inland shipping
Russia, Saint-Petersburg, Dvinskaya st., 5/7
emails: mokeyeva-t-o@yandex.ru, lenin91@mail.ru, burlovvg@mail.ru

Annotation: The article examines the effectiveness of the application of the law of conservation of integrity in the development of computer technology.

Keywords: *model; object; control; protection; software - hardware environment.*

Безопасность программно-аппаратной среды может быть достигнута, если система устойчива к внешним разрушающим воздействиям и к внутренним сбоям вычислительных процессов, и способна гарантированно решать поставленную задачу в условиях разрушения среды функционирования. Такое выполнение возможно в случае адекватности модели функционирования вычислительной системы в программно-аппаратной среде. Показателем адекватности является полнота учёта закономерностей изучаемой предметной области.

В качестве этой закономерности целесообразно рассмотреть закон сохранения целостности, сформулированный в работах профессора Бурлова В.Г. Основная составляющая этого закона определяется неразрывной связью объекта и его движения и характеризуется как взаимная трансформация свойств объекта и свойств его движения при заданном, чётко фиксированном предназначении [1, 2]. Модель объекта – процессор. Модель действия – программа в действии. Заданное предназначение – требуемое количество требуемых символов, преобразованных в памяти вычислительной системы.

На практике данный закон не реализован в полной мере при разработке той или иной программно-аппаратной системы, что не позволяет корректно реагировать как на сбои аппаратной составляющей, так и на несанкционированные внешние программные воздействия. Основная часть современных ЭВМ придерживается «модели фон Неймана». Главной отличительной чертой этой модели остаётся принцип единой «линейной памяти», что адресуется последовательными номерами ячеек и в которой команды неотличимы от данных.

Игнорируя на практике закон сохранения целостности объекта, мы сталкиваемся с проблемой того, что результат производимых действий не соответствует ожидаемому. Особенность данного подхода заключается в принципиально ином рассмотрении внешних и внутренних факторов, имеющих место при работе программно-аппаратной среды. То есть, в функционирование программно-аппаратной системы вводится понятие объективной реальности, которое ранее находило ничтожно малое отражение при реализации алгоритмической части программы и, в конечном итоге, подменялось понятием «целевое назначение». Если же объективной реальности уделить должное внимание и так же, как и требования к программному обеспечению и атрибутам информации, провести через методологический, методический и технологический уровни, то получится, по сути, та же модель информационной системы, но с дополнительным очень важным компонентом.

Учитывая объективную реальность при работе программно-аппаратной среды, уже на методологическом уровне появляется понятие мироустройства. Современная наука уже давно рассматривает и изучает объекты и их движение (статика и динамика), но еще нигде не предложен физико-математический аппарат о том, когда законы статики и динамики начинают действовать. Именно на этой грани и находится мироустройство, которое при переходе на методический уровень, превращается в более осязаемое свойство целостности. Именно эта целостность позволяет связать в единую модель структурность и изменчивость, как промежуточные абстракции. Это позволяет при переходе на технологический уровень вывести условие замыкания между моделью объекта и моделью действия.

Для распространения в компьютерных технологиях закона сохранения целостности необходимо перейти от схемы «машины фон Неймана» к ЭВМ с многомерно организованной памятью и соответственно многомерными командами. Предлагаемая модель позволяет понизить роль администратора до функций контроля работоспособности, подняв проблему коррекции программно-аппаратных ошибок, на автоматический уровень.

СПИСОК ЛИТЕРАТУРЫ

1. Бурлов В.Г. Основа гарантированного управления риском – структурно - функциональный синтез модели потенциально опасного объекта. В кн. «Фундаментальные исследования в технических университетах». Том 2. Национальная безопасность, стр. 137-150, – СПб. С-ПбГТУ, 2002.
2. Гуд Г.Х., Макол Р.Э. Системотехника, - М.: Сов. радио, 1962. – 427 с.
3. Бурлов В.Г. Разработка модели борьбы за рынки сбыта информационных услуг на основе закона сохранения целостности. В кн. «Фундаментальные исследования в технических университетах». Том 2. Национальная безопасность, стр. 137-150, – СПб. С-ПбГТУ, 2002.

ОГЛАВЛЕНИЕ

ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ	15
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СЕВЕРО-ЗАПАДНОМ ФЕДЕРАЛЬНОМ ОКРУГЕ КАК ПРИМЕР РЕАЛИЗАЦИИ РЕГИОНАЛЬНОЙ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ Кучерявый Михаил Михайлович, Вовенда Юлия Владимировна	15
КОНЦЕПЦИЯ СЕКЬЮРИТИЗАЦИИ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ ПОЛИТИКИ РОССИИ Баранов Николай Алексеевич	17
УПРАВЛЕНИЕ БЕЗОПАСНОЙ ИНТЕЛЛЕКТУАЛЬНОЙ СРЕДОЙ ОБИТАНИЯ НА ПРИМЕРЕ ЖИЛИЩНО-КОММУНАЛЬНОЙ СФЕРЫ САНКТ-ПЕТЕРБУРГА Груздева Мария Николаевна, Шарипов Роман Радикович	19
АКТУАЛЬНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОСУЩЕСТВЛЕНИИ ГОСУДАРСТВЕННОЙ МИГРАЦИОННОЙ ПОЛИТИКИ В РОССИЙСКОЙ ФЕДЕРАЦИИ Клечиков Александр Владимирович	21
ИСПОЛЬЗОВАНИЕ ПОЧТОВЫХ АКТИВОВ В СОЗДАНИИ ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА УМНОГО ГОРОДА Павловская Мария Александровна, Кононова Ольга Витальевна	22
ИНФОРМАЦИОННАЯ ПОЛИТИКА РОССИИ В КОНТЕКСТЕ СТРАТЕГИИ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА Попов Павел Валентинович	24
ИМПОРТОЗАМЕЩЕНИЕ КАК ПУТЬ ОБЕСПЕЧЕНИЯ ТЕХНОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИИ Советов Борис Яковлевич, Касаткин Виктор Викторович	26
МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ФОРМИРОВАНИЯ СИСТЕМЫ РАСПРЕДЕЛЕННЫХ СИТУАЦИОННЫХ ЦЕНТРОВ Соколов Борис Владимирович, Салухов Владимир Иванович	27
ОСОБЕННОСТИ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕВЕРО-ЗАПАДНОМ ФЕДЕРАЛЬНОМ ОКРУГЕ Сторожик Виктор Сергеевич	30
ИНФОРМАЦИЯ КАК ВАЖНЕЙШИЙ РЕСУРС ДЛЯ ПРИНЯТИЯ ЭФФЕКТИВНЫХ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ Тарашнина Светлана Ивановна	32
ПРОГРАММА «ЦИФРОВАЯ ЭКОНОМИКА» В КОНТЕКСТЕ РАЗВИТИЯ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ИНФОРМАТИЗАЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ Чугунов Андрей Владимирович	34
ДОВЕРИЕ МЕЖДУ КОНТРАГЕНТАМИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ Шугай Антон Андреевич	36
ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	38
ПРИНЦИПЫ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ СЕТЕЙ ПОДВИЖНОЙ РАДИОСВЯЗИ ПРАВООХРАНИТЕЛЬНОЙ СФЕРЫ НА ОСНОВЕ СОВЕРШЕНСТВОВАНИЯ ЧАСТОТНО-ТЕРРИТОРИАЛЬНОГО ПЛАНИРОВАНИЯ Бабкин Александр Николаевич	38
ЗАДАЧА ВИЗУАЛИЗАЦИИ МАРШРУТОВ ВЫПОЛНЕНИЯ КОМПЬЮТЕРНЫХ ПРОГРАММ Безруков Вячеслав Алексеевич, Синещук Юрий Иванович, Синещук Максим Юрьевич	40

АЛГОРИТМ СИНТЕЗА ЭФФЕКТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ Вилков Валерий Борисович, Сычев Сергей Евгеньевич, Черных Андрей Климентьевич	41
НЕКОТОРЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РЕАЛИЗАЦИИ ПОЛИЦИЕЙ ФУНКЦИИ ГОСУДАРСТВЕННОЙ ЗАЩИТЫ Галушко Валерий Анатольевич, Воронов Анатолий Федорович, Малахов Александр Сергеевич.....	43
ПОДХОД К РАЗРАБОТКЕ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА ДЕЖУРНОГО ПО УНИВЕРСИТЕТУ Иванов Николай Николаевич, Потехин Владимир Семенович	44
ПОДХОД К АДАПТАЦИИ ТИПОВЫХ РЕШЕНИЙ ПРИ РАЗРАБОТКЕ СИСТЕМЫ КОНТРОЛЯ УПРАВЛЕНИЯ ДОСТУПОМ НА ОБЪЕКТЫ ОСОБОЙ ВАЖНОСТИ Калачев Максим Сергеевич, Потехин Владимир Семенович, Саратов Дмитрий Николаевич.....	46
О ПРАВОВЫХ АСПЕКТАХ ЭЛЕКТРОННОЙ БИБЛИОТЕКИ Кононов Олег Александрович, Кононова Ольга Васильевна	47
ОБ ЭТИКЕ ЭЛЕКТРОННОЙ ПЕРЕПИСКИ Кононов Олег Александрович, Кононова Ольга Васильевна	49
ПОДХОДЫ К ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТ Костюк Анатолий Владимирович.....	50
ОРГАНИЗАЦИОННЫЕ СТРУКТУРЫ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ Костюк Анатолий Владимирович, Бобонец Сергей Алексеевич	54
РАЗРАБОТКА ТРЕБОВАНИЙ К ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В СРЕДСТВАХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ Куватов Валерий Ильич, Примакин Алексей Иванович	56
ПРЕСТУПЛЕНИЯ В ОБЛАСТИ ИТ-ИНФОРМАТИЗАЦИИ В РОССИИ И МИРЕ Лядов Алексей Олегович, Евсеев Алексей Викторович.....	57
КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ В СОВРЕМЕННЫХ УСЛОВИЯХ Парфенов Николай Петрович, Алексеев Сергей Алексеевич	62
ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ ОВД ПОСРЕДСТВОМ СПЕЦИАЛЬНОЙ ОБРАБОТКИ Парфенов Николай Петрович, Алексеев Сергей Алексеевич	64
О НЕКОТОРЫХ АСПЕКТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ШКОЛЬНИКОВ Поправко Анна Сергеевна	66
ОБ АПРОБАЦИИ ТЕХНОЛОГИИ ГИПЕРССЫЛОК ПРИ РАБОТЕ С ДОКУМЕНТАМИ, РАЗМЕЩЕННЫМИ В ХРАНИЛИЩЕ ПОДРАЗДЕЛЕНИЯ Гореленко Константин Евгеньевич, Потехин Владимир Семенович	67
ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ Редковников Владислав Александрович	68
ПОДХОД К РАЗРАБОТКЕ СРЕДСТВ ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ ПРИ САМОСТОЯТЕЛЬНОЙ ПОДГОТОВКЕ ОБУЧАЕМЫХ К ЗАЧЕТУ И ЭКЗАМЕНУ НА ПРИМЕРЕ ОДНОЙ ИЗ ДИСЦИПЛИН, СВЯЗАННЫХ С ОБЕСПЕЧЕНИЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Рыжова Валентина Сергеевна, Потехин Владимир Семенович	70

УЧЕБНО – ТРЕНИРОВОЧНЫЙ КОНТРОЛЬНО – ПРОПУСКНОЙ ПУНКТ, КАК ЭЛЕМЕНТ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ «БОЕВОЙ СИСТЕМЫ» МВД Саликов Александр Васильевич, Синешук Юрий Иванович	72
КОМПЛЕКСНАЯ ОЦЕНКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ САНКТ-ПЕТЕРБУРГСКОГО УНИВЕРСИТЕТА МВД РОССИИ ПОСРЕДСТВОМ ПРИМЕНЕНИЯ МЕТОДОВ МНОГОМЕРНОГО АНАЛИЗА (НА ПРИМЕРЕ КЛАСТЕРНОГО И ДИСКРИМИНАНТНОГО АНАЛИЗА) Саратов Дмитрий Николаевич, Козлов Михаил, Хухха Кристина	74
СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ МЧС РОССИИ Саратов Дмитрий Николаевич, Подружкина Татьяна Александровна	76
ОБЛАЧНЫЕ ТЕХНОЛОГИИ, КАК СРЕДСТВО ПРЕДУПРЕЖДЕНИЯ ПОТЕРИ ДАННЫХ Синешук Юрий Иванович, Трубин Игорь Романович	79
ОБ АВТОМАТИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ ДВИЖЕНИЕМ СПЕЦТРАНСПОРТА НА ПЕРЕКРЕСТКЕ С ИСПОЛЬЗОВАНИЕМ РАДИОМЕТОК Смоленцева Линда Александровна, Потехин Владимир Семенович	81
ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ ЗАЩИТА СОТРУДНИКОВ СИЛОВЫХ СТРУКТУР Ярмоленко Наталия Владимировна	82
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ	85
БЕЗОПАСНОСТЬ ДОСТУПА К ОБРАЗОВАТЕЛЬНЫМ РЕСУРСАМ ПРИ ИСПОЛЬЗОВАНИИ УДАЛЕННОГО ДОСТУПА Анисимов Андрей Владимирович	85
ОРГАНИЗАЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ Барышникова Надежда Юрьевна, Егоров Александр Николаевич, Крупенина Наталия Викторовна	86
НЕБЕЗОПАСНОСТЬ МОБИЛЬНЫХ УСТРОЙСТВ Башмаков Алексей Васильевич	88
ПРИМЕНЕНИЕ АЛГОРИТМА РЕШЕНИЯ КУБИЧЕСКИХ УРАВНЕНИЙ В КОНЕЧНОМ БИНАРНОМ ПОЛЕ В ОТРИЦАЕМОМ ШИФРОВАНИИ Будчан Дарья Сергеевна	90
РАЗРАБОТКА ТЕХНОЛОГИИ УПРАВЛЕНИЯ ПРОЦЕССОМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ WEB – ПРИЛОЖЕНИЯ Бурлов Вячеслав Георгиевич, Петров Сергей Вадимович, Грозмани Елена Сергеевна	91
МОДЕЛИРОВАНИЕ СИСТЕМЫ НА ОСНОВЕ ЗАКОНА СОХРАНЕНИЯ ЦЕЛОСТНОСТИ Бурлов Вячеслав Георгиевич, Долгирева Елена Сергеевна, Мокеева Татьяна Олеговна	93
СТАТИЧЕСКИЙ АНАЛИЗ БЕЗОПАСНОСТИ ANDROID-ПРИЛОЖЕНИЙ Дремов Андрей Сергеевич, Павленко Евгений Юрьевич	95
ОБОСНОВАНИЕ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ОПАСНОГО ВЗРЫВООБРАЗНОГО РАЗВИТИЯ ПОПУЛЯЦИОННОГО ПРОЦЕССА ДЛЯ ИНВАЗИОННОГО ТАКСОНА Дубровская Виктория Андреевна, Переварюха Андрей Юрьевич	96
РАЗРАБОТКА ЗАЩИЩЕННОГО ПРОТОКОЛА ТАЙНОГО ГОЛОСОВАНИЯ В ТВОРЧЕСКОМ КОНКУРСЕ Дмитриева Лариса Михайловна, Макарова Таисья Васильевна	98
ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ КЛАССА ДВУХМОДУЛЬНЫХ КОДОВ С СУММИРОВАНИЕМ ПРИ СИНТЕЗЕ ДИСКРЕТНЫХ СИСТЕМ С ОБНАРУЖЕНИЕМ ОТКАЗОВ Ефанов Дмитрий Викторович, Щагина Владислава Александровна	99

ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ВЫЯВЛЕНИЯ ВРЕДОНОСНЫХ ANDROID-ПРИЛОЖЕНИЙ Игнатьев Глеб Юрьевич, Павленко Евгений Юрьевич.....	101
ПОСТАНОВКА ЗАДАЧИ О РАЗРАБОТКЕ СИСТЕМЫ МЕТРИК ЗАЩИЩЕННОСТИ БАЗ ДАННЫХ Мария Феликсовна Исаева, Михаил Леонидович Глухарев	103
ЗАЩИТА ИНФОРМАЦИИ ОТ СКРЫТЫХ УГРОЗ В СРЕДЕ ОБЛАЧНЫХ ТЕХНОЛОГИЙ Марков Вячеслав Сергеевич, Сидоренко Татьяна Владимировна	104
СПОСОБ УМЕНЬШЕНИЯ СЛУЖЕБНОГО ТРАФИКА В СЕТИ ПЕРЕДАЧИ ДАННЫХ С КОММУТАЦИЕЙ ПАКЕТОВ Курашев Заур Валерьевич.....	106
ЗАЩИТА ИНФОРМАЦИИ И ЧЕЛОВЕЧЕСКИЙ ФАКТОР Карташов Павел Николаевич	107
ИНФОРМАЦИОННО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИН ЛИНГВИСТИЧЕСКОГО ЦИКЛА Колоколова Лидия Петровна	109
РЕШЕНИЕ БАЗОВОЙ ВЫЧИСЛИТЕЛЬНОЙ ЗАДАЧИ МЕТОДАМИ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ Мельников Александр Владимирович, Нарушев Илья Романович.....	110
ИЕРАРХИЧЕСКИЙ ПОДХОД К ВЫЯВЛЕНИЮ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ Москвин Дмитрий Андреевич, Павленко Евгений Юрьевич, Ярмач Анастасия Викторовна.....	112
ИССЛЕДОВАНИЕ МЕХАНИЗМОВ БЕЗОПАСНОСТИ В ДЕЦЕНТРАЛИЗОВАННЫХ СИСТЕМАХ ОБЛАЧНОГО ХРАНЕНИЯ ДАННЫХ Мясников Алексей Владимирович, Москвин Дмитрий Андреевич	113
ИСПОЛЬЗОВАНИЕ КАРТ КОХОНЕНА В СРЕДЕ МАТЛАВ ДЛЯ КЛАСТЕРИЗАЦИИ АНОМАЛЬНОГО ПОВЕДЕНИЯ Нарушев Илья Романович	114
НЕ СТРУКТУРИРОВАННЫЕ ДАННЫЕ В ЗАДАЧАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Полтавцева Мария Анатольевна, Печенкин Александр Игоревич	116
ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В ГРАФИЧЕСКОМ КОНТЕНТЕ МОБИЛЬНЫХ УСТРОЙСТВ Попов Борис Николаевич	118
ОЦЕНКА НАДЕЖНОСТИ СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ СИСТЕМ Свеженцев Игорь Иванович.....	118
ASSESSMENT OF RELIABILITY OF SOCIO-ECONOMIC SYSTEMS Svezhentsev Igor Ivanovich.....	119
ЗАЩИТА ОТ АТАК МЕТОДАМИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ Солодяников Александр Владимирович, Сухостат Валентина Васильевна, Антонова Любовь Сергеевна	120
ОСОБЕННОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ПРОЦЕССЕ ФУНКЦИОНИРОВАНИЯ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ Солодяников Александр Владимирович , ...	122
ФАКТОРЫ НАСЛЕДОВАНИЯ И ПРОАКТИВНОСТИ В ЖИЗНЕННОМ ЦИКЛЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ Соколов Борис Владимирович, Мустафин Николай Габдрахманович, Миллер Владимир Евгеньевич, Савосин Сергей Валентинович.....	126

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СЕТИ ИНТЕРНЕТА ВЕЩЕЙ СРЕДСТВАМИ НИЗКОРЕСУРСНОЙ КРИПТОГРАФИИ Супрун Александр Федорович, Царьков Игорь Сергеевич	127
ПРОТОКОЛ ВЗАИМОДЕЙСТВИЯ ВНУТРИ СЕТИ ИНТЕРНЕТА ВЕЩЕЙ Супрун Александр Федорович, Царьков Игорь Сергеевич	128
ВЫЧИСЛЯЕМЫЙ ВОПРОС КАК ПЕДАГОГИЧЕСКАЯ ТЕХНОЛОГИЯ В ЭЛЕКТРОННОМ ОБУЧЕНИИ Титова Юлияна Францевна.....	129
УГРОЗЫ И МЕРЫ ЗАЩИТЫ ПРИ ИСПОЛЬЗОВАНИИ КОНЦЕПЦИИ BYOD Усатых Ксения Сергеевна	130
СТРУКТУРА ДАННЫХ ДВУХМАСШТАБНОЙ ДИХОТОМИЧЕСКОЙ ИЕРАРХИИ ОБЪЕКТОВ НА ЦВЕТОВОМ ИЗОБРАЖЕНИИ Харинов Михаил Вячеславович.....	132
МОДЕЛИРОВАНИЕ УЯЗВИМОСТЕЙ В СИСТЕМЕ БЕЗОПАСНОСТИ Шипилева Алла Владимировна.....	134
СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ	136
СПЕЦИФИЧЕСКИЕ УГРОЗЫ СИСТЕМ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ Бориева Анна Андреевна.....	136
ТЕСТИРОВАНИЕ СОВРЕМЕННЫХ СРЕДСТВ ЗАЩИТЫ ВИРТУАЛЬНЫХ ИНФРАСТРУКТУР Бородин Михаил Константинович, Бородина Полина Юрьевна	137
СЛОЖНОСТЬ ЗАДАЧ УПРАВЛЕНИЯ И СЕТЕЦЕНТРИЗМ Верзун Наталья Аркадьевна, Колбанев Михаил Олегович	138
ВЛИЯНИЕ ПАРАМЕТРОВ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ НА ПОТРЕБЛЕНИЕ ЭНЕРГИИ АВТОНОМНОЙ СИСТЕМОЙ МОНИТОРИНГА ЭКОСИСТЕМ Верзун Наталья Аркадьевна, Колбанев Михаил Олегович, Колбанев Алексей Михайлович	140
БЕЗОПАСНАЯ ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ ПРОЕКТИРОВАНИЯ КОРПОРАТИВНЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ УНИФИЦИРОВАННОГО ЯЗЫКА МОДЕЛИРОВАНИЯ UML Дубенецкий Владислав Алексеевич, Кузнецов Александр Григорьевич, Цехановский Владислав Владимирович	141
СТРАТЕГИЯ И КУЛЬТУРА БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ СОБСТВЕННОГО АВТОРСКОГО ИНФОРМАЦИОННОГО РЕСУРСА Виноградов Алексей Борисович, Щиголева Марина Андреевна.....	143
ПОСТРОЕНИЕ ПРОГРАММНОГО ШЛЮЗА ДЛЯ СЕТЕВОЙ ИЗОЛЯЦИИ ВИРТУАЛЬНЫХ МАШИН Зегжда Петр Дмитриевич, Никольский Алексей Валерьевич, Алексеев Илья Вадимович.....	144
АНАЛИЗАТОРЫ ПРОТОКОЛОВ ДЛЯ КОНТРОЛЯ НАД ПАКЕТАМИ ДАННЫХ МЕЖДУ УСТРОЙСТВАМИ СЕТИ Зорин Кирилл Михайлович, Гурьянов Денис Юрьевич, Щиголева Марина Андреевна.....	145
МОДЕЛИ КОРРЕКЦИИ ФУНКЦИОНАЛЬНОГО СОСТОЯНИЯ, ОСНОВАННЫЕ НА ТИПОЛОГИЧЕСКИХ ОСОБЕННОСТЯХ ЧЕЛОВЕКА-ОПЕРАТОРА В РАМКАХ УЛУЧШЕНИЯ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ИНДИВИДА Колмаков Сергей Александрович.....	147
ТЕОРИЯ СОЗДАНИЯ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ АВТОМАТИЗИРОВАННОГО ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ Кривоногов Сергей Вячеславович.....	148

КОМПРОМИСС БЕЗОПАСНОСТИ И ЮЗАБИЛИТИ СОВРЕМЕННЫХ ПОЛЬЗОВАТЕЛЬСКИХ ИНТЕРФЕЙСОВ Леонов Антон Викторович	150
О ЗАДАЧЕ ПОИСКА НОВЫХ КОНЕЧНЫХ АССОЦИАТИВНЫХ АЛГЕБР ДЛЯ ПОСТРОЕНИЯ КРИПТОСХЕМ С ОТКРЫТЫМ КЛЮЧОМ Молдовян Николай Андреевич, Ковалева Ирина Владиславовна	152
ПОСТРОЕНИЕ КОНЕЧНЫХ АЛГЕБР ДЛЯ РЕАЛИЗАЦИИ ПОСТКВАНТОВЫХ ПРОТОКОЛОВ ЗАЩИТНЫХ ПРЕОБРАЗОВАНИЙ ИНФОРМАЦИИ Молдовян Николай Андреевич, Абросимов Иван Константинович	154
ПРОГРАММНО-ТЕХНИЧЕСКИЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ЗАДАЧ ЭКСПЛУАТАЦИИ РБД Нечитайленко Роман Александрович, Новопашин Владимир Сергеевич, Белько Роман Вячеславич	155
ИСПОЛЬЗОВАНИЕ АЛГОРИТМА ПОИСКА МИНИМАЛЬНОГО ОСТОВНОГО ДЕРЕВА ДЛЯ СРЕДСТВ ВИЗУАЛИЗАЦИИ ИЗОБРАЖЕНИЙ ЗАЩИЩЕННОЙ ОТКАЗОУСТОЙЧИВОЙ КОРПОРАТИВНОЙ ИНФРАСТРУКТУРЫ Пелевин Максим Сергеевич	157
АЛГОРИТМ ВЫБОРА ОПТИМАЛЬНОГО ВАРИАНТА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ Попова Елена Владимировна	158
ЭЛЕКТРОННЫЕ ПОДПИСИ СТРУКТУРИРОВАННЫХ ХРАНИЛИЩ ДАННЫХ Романова Юлия Николаевна, Янюшкин Константин Александрович	159
БЛОКЧЕЙН ДЛЯ ГЕОТЕГИРОВАНИЯ ПЕРИМЕТРА БЕЗОПАСНОСТИ Рыжков Сергей Романович	160
АУДИТ СЕТЕВОЙ БЕЗОПАСНОСТИ Садикова Анастасия Александровна, Титова Юлия Алексеевна, Савков Сергей Витальевич	162
СТЕГАНОГРАФИЯ КАК АЛЬТЕРНАТИВА КРИПТОГРАФИИ Соколов Сергей Сергеевич, Ревера Галина	163
КОМПЛЕКСНАЯ СИСТЕМА ИНЖЕНЕРНО ТЕХНИЧЕСКОЙ ЗАЩИТЫ КАБИНЕТА РУКОВОДИТЕЛЯ. ЭФФЕКТИВНОСТЬ РАБОТЫ ПРИБОРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ КОМПЛЕКСНОЙ СИСТЕМЫ ИНЖЕНЕРНО ТЕХНИЧЕСКОЙ ЗАЩИТЫ КАБИНЕТА РУКОВОДИТЕЛЯ Фаязов Кобилджон Абдукаюмович	165
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ	167
АНАЛИЗ ОСНОВНЫХ ВИДОВ ТРАФИКА В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ И ОЦЕНКА ЕГО ЧУВСТВИТЕЛЬНОСТИ К ПОКАЗАТЕЛЯМ КАЧЕСТВА ОБСЛУЖИВАНИЯ Власова Дарья Николаевна, Баглай Валерия Витальевна, Апарина Елена Юрьевна	167
АНАЛИЗ ПРОБЛЕМ РАЗВИТИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ Борисов Александр Иванович, Логинов Вячеслав Алексеевич, Пименов Алексей Сергеевич	168
СХЕМА И ИНФРАСТРУКТУРА ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОСТИ КОММУНИКАЦИЙ В СЕТИ ИНТЕРНЕТ ОТ АТАКИ ТИПА «ЧЕЛОВЕК ПОСЕРЕДИНЕ», ОСНОВАННОЙ НА ИСПОЛЬЗОВАНИИ ОТОЗВАННЫХ СЕРТИФИКАТОВ Бусыгин Алексей Геннадьевич, Коноплев Артем Станиславович, Зегжда Дмитрий Петрович	170
ПОДХОД К ПРОТИВОДЕЙСТВИЮ КОМПЬЮТЕРНЫМ АТАКАМ НА КРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННЫХ СЕГМЕНТАХ СЕТИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ Васюков Дмитрий Юрьевич, Смыгин Александр Михайлович Митрофанов Михаил Валерьевич	171
ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ ПЕРЕДАЧИ, ХРАНЕНИЯ И ОБРАБОТКИ ИНФОРМАЦИИ Волостных Виктор Анатольевич, Рогов Руслан Александрович, Митрофанов Михаил Валерьевич	173

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ Дахнович Андрей Дмитриевич, Москвин Дмитрий Андреевич	174
СПОСОБ ЗАЩИТЫ РЕСУРСОВ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ Журавель Евгений Павлович.....	175
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ УПРАВЛЕНИЯ РОБОТИЗИРОВАННЫХ СИСТЕМ С ПРИМЕНЕНИЕМ НЕЙРОННЫХ СЕТЕЙ Захаров Руслан Владимирович, Лаута Олег Сергеевич, Крибель Александр Михайлович, Соловьев Дмитрий Владимирович.....	178
РОЛЕВАЯ МОДЕЛЬ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ ДЛЯ СЕТЕЙ ТРАНСПОРТНЫХ СРЕДСТВ Калинин Максим Олегович, Резединова Евгения Юрьевна	179
СИСТЕМАТИЧЕСКАЯ ПРОЦЕДУРА ПРИМЕНЕНИЯ МЕТОДА ДВУХМОМЕНТНОЙ АППРОКСИМАЦИИ ДЛЯ ОПРЕДЕЛЕНИЯ ФУНКЦИИ РАСПРЕДЕЛЕНИЯ ВРЕМЕНИ РЕАЛИЗАЦИИ СТОХАСТИЧЕСКОЙ СЕТИ Канаев Андрей Константинович, Карабанов Юрий Сергеевич, Привалов Андрей Андреевич.....	180
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА КАНАЛА УПРАВЛЕНИЯ РОБОТИЗИРОВАННЫХ СИСТЕМ Коцыняк Михаил Антонович, Гудков Михаил Александрович, Сафонов Алексей Александрович, Арутюнян Борис Артурович	182
МЕТОДИКА ОЦЕНКИ КОМПЛЕКСНОГО ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ НА ИТКС СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ Коцыняк Михаил Антонович, Ястребов Владимир Васильевич, Клишов Илья Андреевич, Гулевич Антон Владимирович	184
МЕТОДИКА ПРОГНОЗИРОВАНИЯ ПРОТОКОЛЬНЫХ ВОЗДЕЙСТВИЙ НА РОБОТИЗИРОВАННЫЕ СИСТЕМЫ Коцыняк Михаил Антонович, Дементьев Владислав Евгеньевич, Тесля Сергей Петрович, Лаута Олег Сергеевич	185
ВЕРОЯТНОСТНО-ВРЕМЕННЫЕ ХАРАКТЕРИСТИКИ АТАК НА РОБОТИЗИРОВАННЫЕ СИСТЕМЫ Кузнецов Сергей Иванович, Иванов Денис Александрович, Власенко Максим Андреевич, Латушко Николай Александрович	186
ПОДХОД К ОЦЕНКЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ОТ ТЕХНИЧЕСКОЙ КОМПЬЮТЕРНОЙ РАЗВЕДКИ Лаута Олег Сергеевич, Клишов Илья Андреевич, Ястребов Владимир Васильевич, Русаков Егор Владимирович, ...	187
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ НА ОСНОВЕ ВЫБОРА ЗАЩИЩЕННЫХ ИНТЕРВАЛОВ СВЯЗИ ОТ РАДИОПОДАВЛЕНИЯ Митрофанов Михаил Валерьевич., Ракицкий Станислав Николаевич, Чиков Дмитрий Викторович	189
ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ РФ ОТ КИБЕРАТАК Мошак Николай Николаевич, Евсейко Константин Владиславович	190
ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МОБИЛЬНЫХ УСТРОЙСТВАХ И ВОЗМОЖНЫЕ ПУТИ ИХ РЕШЕНИЯ Неижмак Алексей Владимирович.....	192
МОДЕЛИ ИНТЕЛЛЕКТУАЛЬНЫХ ВОЗДЕЙСТВИЙ Нечепуренко Александр Петрович, Суетин Артем Игоревич, Муртазин Ильдар Робертович, Лаута Олег Сергеевич	193
КОНТРОЛЬ МНОГОВЫХОДНЫХ ЛОГИЧЕСКИХ СХЕМ АВТОМАТИКИ НА ОСНОВЕ МЕТОДА ЛОГИЧЕСКОГО ДОПОЛНЕНИЯ ПО РАВНОВЕСНЫМ КОДАМ Пивоваров Дмитрий Вячеславович, Ефанов Дмитрий Викторович, Сапожников Валерий Владимирович, Сапожников Владимир Владимирович.....	195

ПРОТИВОДЕЙСТВИЕ НЕСАНКЦИОНИРОВАННОМУ ДОСТУПУ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ НА ОБЪЕКТЫ УЧРЕЖДЕНИЙ Остроумов Олег Александрович, Атигов Умар Умарович, Сотникова Дарья Ивановна.....	196
ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ АКТИВНОГО ОБОРУДОВАНИЯ КОРПОРАТИВНЫХ СЕТЕЙ Серёгин Сергей Сергеевич, Гвоздков Игорь Вячеславович	197
МЕТОДИКА ПРОЕКТИРОВАНИЯ СИСТЕМЫ РАЗГРАНИЧЕНИЯ ДОСТУПА АВТОМАТЕЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ Фиалкин Илья Александрович	199
АНСАМБЛИ ДИСКРЕТНЫХ ОРТОГОНАЛЬНЫХ СИГНАЛОВ СЛОЖНОЙ СТРУКТУРЫ Сазонов Виктор Викторович, Беззубов Олег Владимирович, Мосягин Дмитрий Евгеньевич	200
ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ОБМЕНА ЭЛЕКТРОННОЙ КОРРЕСПОНДЕНЦИИ ВЕДОМСТВЕННОГО НАЗНАЧЕНИЯ Сазонов Виктор Викторович, Салыхова Алия Маратовна.....	202
МОДЕЛЬ ДЛЯ ОПРЕДЕЛЕНИЯ СКРЫТНОСТИ СИСТЕМЫ СВЯЗИ Худайназаров Юрий Кахрамонович, Маслов Олег Николаевич, Барауля Игорь Геннадьевич	203
ВНЕДРЕНИЕ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В ДЕЯТЕЛЬНОСТЬ ПОЛИЦИИ Шалагинова Ольга Борисовна	205
ПОДХОД К ЗАЩИТЕ ИНФОРМАЦИИ В СЕТЯХ С ВЫСОКИМ УРОВНЕМ КОНФИДЕНЦИАЛЬНОСТИ Штаненко Василий Иванович, Барауля Игорь Геннадьевич, Маслов Олег Николаевич	205
ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ	207
ТЕХНОЛОГИИ БЕЗОПАСНОСТИ В БАНКОВСКОЙ СФЕРЕ ОТ КИБЕРАТАК Абрамова Кристина Владимировна, Голубева Мария Геннадьевна	207
ОБЛАСТИ ПРИМЕНЕНИЯ АРОМОСЕНСОРНЫХ СИСТЕМ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ Афанасьев Дмитрий Сергеевич, Бардакова Елена Андреевна, Быстрыков Денис Сергеевич	208
ОСОБЕННОСТИ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ Володина Анастасия Андреевна, Левкин Игорь Михайлович	210
ОБ АЛГОРИТМЕ ОБРАБОТКИ СИТУАЦИОННЫХ МОДЕЛЕЙ Головкин Юрий Борисович	211
АЛГОРИТМ РАЗМЕЩЕНИЯ СЕНСОРОВ СИСТЕМЫ ИНТЕРНЕТА ВЕЩЕЙ Дзюбенко Иван Николаевич.....	213
SOC КАК ИНСТРУМЕНТ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ Демидова Наталья Дмитриевна, Колоколов Даниил Сергеевич.....	214
ИМИТАЦИОННАЯ МОДЕЛЬ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ В СЕТИ ИНТЕРНЕТА ВЕЩЕЙ Елизаров Максим Андреевич	215
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ В ОБЛАЧНЫХ СЕРВИСАХ Емельянов Александр Александрович	216
МЕХАНИЗМЫ ПОВЫШЕНИЯ УРОВНЯ БЕЗОПАСНОСТИ ПРИ ПЕРЕДАЧЕ СЕТЕВЫХ ДАННЫХ Емельянов Александр Александрович	218
НЕКОТОРЫЕ АСПЕКТЫ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ КРИПТОВАЛЮТ Кадырова Асия	220

ОЦЕНКА И ПРОГНОЗИРОВАНИЯ РИСКОВ ДЛЯ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Капанов Алексей Александрович, Мещеряков Евгений Евгеньевич, Косолапов Владимир Викторович, Астахова Татьяна Николаевна	221
МЕТАДАННЫЕ В СИСТЕМАХ ДОЛГОВРЕМЕННОГО ХРАНЕНИЯ Колбанёв Михаил Олегович, Пойманова Екатерина Дмитриевна, Татарникова Татьяна Михайловна.....	222
ПОДУРОВЕНЬ БЕЗОПАСНОСТИ АРХИТЕКТУРНОЙ МОДЕЛИ СОХРАНЕНИЯ ДАННЫХ Колбанёв Михаил Олегович, Ипатов Олег Сергеевич, Пойманова Екатерина Дмитриевна.....	223
ЭНЕРГЕТИЧЕСКИЕ АСПЕКТЫ БЕЗОПАСНОСТИ ДОЛГОВРЕМЕННОГО ХРАНЕНИЯ ДАННЫХ Колбанёв Михаил Олегович, Касаткин Виктор Викторович, Пойманова Екатерина Дмитриевна.....	225
ОБ УЧАСТИИ ЭКОНОМИЧЕСКОГО УНИВЕРСИТЕТА В ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ДЛЯ ЦЕНТРОВ КОМПЕТЕНЦИЙ РЕГИОНОВ Коршунов Игорь Львович, Левкин Игорь Михайлович, Микадзе Сергей Юрьевич.....	226
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРИ ПЕРЕНОСЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ ПРЕДПРИЯТИЯ В ОБЛАЧНУЮ СТРУКТУРУ Кузнецова Маргарита Александровна	227
ОСНОВНЫЕ ВИДЫ НАРУШИТЕЛЕЙ, СПОСОБНЫЕ ВЕСТИ КОНКУРЕНТНУЮ РАЗВЕДКУ ИЛИ ОКАЗАТЬ ВОЗДЕЙСТВИЯ НА ИНФОРМАЦИЮ Кулишкин Виталий Александрович, Чуйков Игорь Олегович	228
ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКИЕ УГРОЗЫ В ЦИФРОВОЙ ЭКОНОМИКЕ Левкин Игорь Михайлович, Левкина Светлана Вячеславовна	229
ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ ПРОЕКТИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ Лобанов Вячеслав Игоревич, Соколов Роман Владимирович	231
ТРЕБОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАЗРАБОТКЕ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ Маслов Никита Сергеевич, Астахова Татьяна Николаевна.....	232
ИРРАЦИОНАЛЬНОЕ ВЛИЯНИЕ ИНФОРМАЦИОННЫХ ПОТОКОВ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ В ЦИФРОВОЙ ЭКОНОМИКЕ Минаков Владимир Федорович, Лобанов Олег Сергеевич, Сотавов Абакар Капланович	233
СТРАТЕГИЯ РАЗВИТИЯ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ Михайлов Николай Семёнович.....	235
МОТИВАЦИЯ ПЕРСОНАЛА НА ОСНОВЕ КРІ Михайлова Анна Сергеевна.....	235
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЦИФРОВОЙ ЭКОНОМИКЕ Романова Анна Александровна, Астахова Татьяна Николаевна, Колбанев Михаил Олегович	236
МЕТОДЫ МОДЕЛИРОВАНИЯ САМОПОДОБНОГО ТРАФИКА Татарникова Татьяна Михайловна, Яковлев Сергей Алексеевич.....	238
ЗАЩИЩЕННАЯ СИСТЕМА УДАЛЕННОГО МОНИТОРИНГА ПАЦИЕНТОВ Татарникова Анна Александровна	240
МЕТОДИКА ПРОЕКТИРОВАНИЯ ИНФРАСТРУКТУРЫ ГИС ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЯ ПРИ УПРАВЛЕНИИ КОРАБЛЕМ Яготинцева Наталья Владимировна	241
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ИМПОРТОЗАМЕЩЕНИЕ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ	243

МОДЕЛИ СОТРУДНИЧЕСТВА ВУЗОВ И ИТ-КОМПАНИЙ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ В УСЛОВИЯХ ИМПОРТОЗАМЕЩЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ Абрамян Геннадий Владимирович.....	243
ПАРАМЕТРИЧЕСКИЙ СИНТЕЗ СИСТЕМЫ РАДИОМОНИТОРИНГА НА ОСНОВЕ ФОРМАЛЬНОГО ПОДХОДА Гудков Алексей Александрович, Малышев Сергей Романович	246
ПОРТИРОВАНИЕ ОПЕРАЦИОННОЙ СИСТЕМЫ РЕАЛЬНОГО ВРЕМЕНИ «FREERTOS» НА АППАРАТНЫЕ МОДУЛИ, ПОСТРОЕННЫЕ НА БАЗЕ ПРОЦЕССОРОВ РОССИЙСКОЙ КОМПАНИИ «ЭЛВИС» Гук Игорь Иосифович, Павлов Федор Андреевич.....	248
СЕЛЕКТИРОВАНИЕ В ИЕРАРХИЧЕСКИХ СИСТЕМАХ ОБЪЕКТОВ НАБЛЮДЕНИЯ И УСТАНОВЛЕНИЕ ИХ ПРИНАДЛЕЖНОСТИ С ПРИМЕНЕНИЕМ АЛГОРИТМА ОЦЕНКИ ХАРАКТЕРИСТИК ВЗАИМОСВЯЗАННОСТИ Кузьмин Виталий Владимирович, Удальцов Николай Петрович.....	249
АНАЛИЗ ТРЕБОВАНИЙ К СИСТЕМЕ УПРАВЛЕНИЯ ИБ ДЛЯ КРИТИЧНЫХ ОБЪЕКТОВ Лившиц Илья Иосифович, Маликов Владимир Викторович	250
АНАЛИЗ ТРЕБОВАНИЙ К ОЦЕНКЕ ДОВЕРИЯ КРИТИЧНЫХ ОБЪЕКТОВ НА БАЗЕ СОВРЕМЕННЫХ СТАНДАРТОВ ISO Лившиц Илья Иосифович, Маликов Владимир Викторович.....	252
АНАЛИЗ ВЛИЯНИЯ РИСК-ОРИЕНТИРОВАННЫХ СТАНДАРТОВ НА ОБЕСПЕЧЕНИЕ ИБ ОБЪЕКТОВ КРИТИЧНОЙ ИНФРАСТРУКТУРЫ Лившиц Илья Иосифович, Маликов Владимир Викторович	254
ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ, ИХ РАЗВИТИЕ Михайленко Евгений Иванович	256
ПРОТОКОЛ МАРШРУТИЗАЦИИ В БЕСПРОВОДНОЙ СЕТИ Молокович Игорь Аркадьевич.....	257
АЛГОРИТМ УПРАВЛЕНИЯ РЕЖИМАМИ ОБМЕНА ДАННЫМИ В САМООРГАНИЗУЮЩЕЙСЯ СЕТИ ДЕКАМЕТРОВОЙ РАДИОСВЯЗИ Путилин Алексей Николаевич.....	259
МЕТОД МОДЕРНИЗАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ ЭКОЛОГИЧЕСКОГО МОНИТОРИНГА Рябовая Валентина Олеговна	260
ПРОГРАММНАЯ МОДЕЛЬ ЦИФРОВОЙ СИСТЕМЫ СВЯЗИ В КВ ДИАПАЗОНЕ С ПСЕВДОСЛУЧАЙНОЙ ПЕРЕСТРОЙКОЙ РАБОЧЕЙ ЧАСТОТЫ Шаптала Василий Сергеевич, Секунов Николай Юрьевич.....	261
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТРАНСПОРТНЫХ СИСТЕМ.....	263
ТЕХНОЛОГИИ СЕТЕЙ НОВОГО ПОКОЛЕНИЯ (NGN) И ИХ ПРИМЕНЕНИЕ НА ВОДНОМ ТРАНСПОРТЕ Алексеев Андрей Дмитриевич, Ерисова Анастасия Дмитриевна, Малов Сергей Сергеевич	263
ИСПОЛЬЗОВАНИЕ ЦВЕТНЫХ СЕТЕЙ ПЕТРИ ПРИ МОДЕЛИРОВАНИИ ПОДСИСТЕМ ПРЕДПРИЯТИЯ Барашков Александр Валерьевич, Петровский Дмитрий Валерьевич	265
МОДЕЛЬ ТРАНСПОРТНОГО ПОТОКА Бариков Леонид Николаевич, Галанина Валентина Александровна.....	266

СКРЫТАЯ ПЕРЕДАЧА ДАННЫХ ЧЕРЕЗ ВОЗДУШНЫЙ АУДИОКАНАЛ С ПОМОЩЬЮ АУДИОСИГНАЛОВ, ПОДВЕРГНУТЫХ ЦИФРОВОМУ МАРКИРОВАНИЮ Гофман Максим Викторович, Корниенко Анатолий Адамович, Кустов Владимир Николаевич, Мирончиков Евгений Тимофеевич, Никитин Александр Борисович	267
МЕТОД ВОССТАНОВЛЕНИЯ ПРОФИЛЯ ВЕТРА ПО ОЦЕНКАМ ШИРИНЫ СПЕКТРА РАДИОЛОКАЦИОННОГО СИГНАЛА Денисенков Дмитрий Анатольевич, Жуков Владимир Юрьевич, Щукин Георгий Георгиевич	269
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ ПОДСИСТЕМ СИСТЕМЫ ДИНАМИЧЕСКОГО ПОЗИЦИОНИРОВАНИЯ СУДНА ПОСРЕДСТВОМ АЛГОРИТМА ОПТИМАЛЬНОГО РАСПРЕДЕЛЕНИЯ УПОРОВ ДВИЖИТЕЛЬНО-РУЛЕВОГО КОМПЛЕКСА Зайцев Алексей Николаевич, Азаров Михаил Михайлович	270
ОСОБЕННОСТИ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ УПРАВЛЕНИЯ ЕДИНЫМ ПАРКОВОЧНЫМ ПРОСТРАНСТВОМ Зайцев Святослав Игоревич, Ильченко Лидия Михайловна	272
ЗАЩИТА КОРПОРАТИВНОЙ ИНФОРМАЦИИ В ТРАНСПОРТНО-ЛОГИСТИЧЕСКИХ СЕТЯХ Искандеров Юрий Марсович, Паутов Михаил Дмитриевич	275
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЦЕССА ПЕРЕВОЗКИ НЕГАБАРИТНЫХ ГРУЗОВ Искандеров Юрий Марсович, Чумак Александр Сергеевич	276
ФОРМИРОВАНИЕ БЕЗОПАСНОЙ БАЗЫ ЗНАНИЙ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ПРОЕКТИРОВАНИЯ АСУ НА ТРАСПОРТЕ Искандеров Юрий Марсович, Ершов Александр Александрович	277
МЕТОД ЗАЩИТЫ ОТ УГРОЗ ДОСТУПНОСТИ УЗЛОВ МЕЖМАШИННЫХ СЕТЕЙ ПУТЕМ ДИНАМИЧЕСКОЙ МАРШРУТИЗАЦИИ СЕТЕВЫХ ПОТОКОВ С ПОМОЩЬЮ МУРАВЬИНОГО АЛГОРИТМА Калинин Максим Олегович	278
КИБЕРБЕЗОПАСНОСТЬ, КАК НЕОТЪЕМЛЕМАЯ ЧАСТЬ СИСТЕМЫ БЕЗОПАСНОСТИ СУДНА Кардакова Мария Владимировна	279
МОДЕЛИРОВАНИЕ И ИССЛЕДОВАНИЕ СВОЙСТВ БЕЗОПАСНОСТИ ПЕРЕМЕЩАЮЩИХСЯ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ VANET/MANET С ИСПОЛЬЗОВАНИЕМ ВИРТУАЛЬНОЙ СРЕДЫ СУПЕРКОМПЬЮТЕРА Крундышев Василий Михайлович, Калинин Максим Олегович, Зегжда Дмитрий Петрович	280
СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ В СЕТЯХ ТРАНСПОРТНЫХ СРЕДСТВ НА БАЗЕ ТЕХНОЛОГИИ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ Крундышев Василий Михайлович, Калинин Максим Олегович	282
МЕТОДЫ РЕИНЖИНИРИНГА САЙТОВ В ЗАДАЧЕ ОПТИМИЗАЦИИ ИТ-АРХИТЕКТУРЫ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ ОРГАНИЗАЦИИ Москалева Валерия Дмитриевна, Кривцов Александр Николаевич	284
ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПОЛЕТОВ БЕСПИЛОТНЫХ ВОЗДУШНЫХ СУДОВ Рубцов Евгений Андреевич	286
АЛГОРИТМЫ РЕШЕНИЯ ЗАДАЧ МАРШРУТИЗАЦИИ КАК ОПРЕДЕЛЯЮЩАЯ ЗАДАЧА ОНЛАЙН-РИТЕЙЛА Котляр Софья Денисовна, Кривцов Александр Николаевич	288
ФОРМИРОВАНИЕ ЭЛЕКТРОННОЙ ОБРАЗОВАТЕЛЬНОЙ ТРАЕКТОРИИ ПРИ ОБУЧЕНИИ КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Митрофанова Анастасия Витальевна, Соколов Сергей Сергеевич, Новоселов Роман Юрьевич	289

СПОСОБЫ ОПТИМИЗАЦИИ БАЗ ДАННЫХ В ВЫСОКОНАГРУЖЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ НА ТРАНСПОРТЕ Новоселов Роман Юрьевич, Соколов Сергей Сергеевич, Митрофанова Анастасия Витальевна.....	290
УЯЗВИМОСТИ VOIP Полугина Юлия Константиновна	292
БЕЗОПАСНАЯ VOIP АТС Полугина Юлия Константиновна	293
ПРИМЕНЕНИЕ МЕТОДОВ СТАТИСТИЧЕСКОГО АНАЛИЗА ДЛЯ ИДЕНТИФИКАЦИЙ ВЕРСИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ УДАЛЕННЫХ АВТОНОМНЫХ ОБЪЕКТОВ ТРАНСПОРТНЫХ СИСТЕМ Салахутдинова Ксения Иркиновна, Лебедев Илья Сергеевич.....	294
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ	296
ЭКСПЕРИМЕНТАЛЬНАЯ ОТРАБОТКА ТЕХНОЛОГИИ ОТМУ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ ПРОГРАММОЙ РАЗВИТИЯ ОМТИ Александров Владимир Леонидович, Алексеев Анатолий Владимирович, Поляничко Виктор Викторович, Ходан Сергей Владимирович.....	296
АДАПТИВНЫЙ АЛГОРИТМ ПРОГНОЗИРОВАНИЯ РАЗВИТИЯ IS-ОБСТАНОВКИ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И ИНФРАСТРУКТУРЫ Алексеев Анатолий Владимирович, Мусатенко Роман Иванович, Киселев Валерий Михайлович.....	298
ПРОБЛЕМА КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ОМТИ И ЕЁ РАЗРЕШЕНИЕ НА ОСНОВЕ ОПТИМАЛЬНЫХ ИНТЕГРАЦИОННЫХ РЕШЕНИЙ Алексеев Анатолий Владимирович.....	300
ПРОБЛЕМА СИСТЕМАТИЗАЦИИ ЛУЧШИХ ПРАКТИК И ФОРМИРОВАНИЯ ТРЕБОВАНИЙ К РАЗВИТИЮ СИСТЕМ АВТОМАТИЗАЦИИ И УПРАВЛЕНИЯ ЖИЗНЕННЫМ ЦИКЛОМ ОМТИ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ Алексеев Анатолий Владимирович, Тычинин Игорь Юрьевич, Мусатенко Роман Иванович	302
КОНЦЕПЦИЯ ПОЛИГОНА СЕТЕВОЙ МЕЖОБЪЕКТОвой ОТРАБОТКИ ТЕХНОЛОГИЙ УПРАВЛЕНИЯ И ОБЕСПЕЧЕНИЯ ПРЕВОСХОДСТВА В ИНФОСФЕРЕ Алексеев Анатолий Владимирович, Барабаш Павел Александрович, Жигадло Валентин Эдуардович, Зикратов Игорь Алексеевич, Нырков Анатолий Павлович.....	304
СИСТЕМА БОРЬБЫ ЗА ИНФОРМАЦИОННУЮ ЖИВУЧЕСТЬ СУДНА ПО ТРЕБОВАНИЯМ НБЖС Алексеев Анатолий Владимирович, Петров Александр Акимович	306
ВОПРОСЫ ИБ В ТРЕТЬЕЙ РЕДАКЦИИ МОНОГРАФИИ «АВТОМАТИЗАЦИЯ ПРОЦЕССОВ БОРЬБЫ ЗА ЖИВУЧЕСТЬ КОРАБЛЯ, СУДНА»: ПРЕЗЕНТАЦИЯ ИЗДАНИЯ Алексеев Анатолий Владимирович, Поленин Владимир Иванович, Москаленко Василий, Александрович, Мусатенко Роман Иванович.....	308
ПРОБЛЕМЫ СОЗДАНИЯ ИТ УПРАВЛЕНИЯ БОРЬБОЙ ЗА ЖИВУЧЕСТЬ ОМТ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ И ПЕРСПЕКТИВНЫЕ ПУТИ ИХ РЕШЕНИЯ Алексеев Анатолий Владимирович, Соловьев Сергей Николаевич, Бороненков Иван Михайлович, Туркин Игорь Иванович, Москаленко Василий Александрович, Мусатенко Роман Иванович	310
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПРОБЛЕМЫ СИСТЕМЫ УПРАВЛЕНИЯ КАЧЕСТВОМ ПРАКТИЧЕСКОЙ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ОБЪЕКТОВ ВМФ Алексеева Елена Кирилловна, Алексеев Сергей Алексеевич, Парфенов Николай Петрович	313
БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ПРОГНОЗЕ И ДИАГНОСТИКЕ КАЧЕСТВА ПРАКТИЧЕСКОЙ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ОБЪЕКТОВ ВМФ Алексеева Елена Кирилловна, Алексеев Сергей Алексеевич, Парфенов Николай Петрович	315

К ВОПРОСУ ПОДГОТОВКИ СИЛ ОБЕСПЕЧЕНИЯ ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ Алимов Олег Михайлович	317
РЕГРЕССИОННЫЙ АНАЛИЗ ДИНАМИКИ 10 ЛЕТ ХАКЕРСКИХ АТАК И ИНФОРМАЦИОННЫХ ИНЦИДЕНТОВ Анциферов Александр Владимирович	319
ВОЗМОЖНОСТИ ДИСТАНЦИОННОЙ ДИАГНОСТИКИ НА СУДАХ Баркова Наталия Александровна, Барков Алексей Васильевич, Грищенко Дмитрий Вячеславович, Федорищев Владимир Валерьевич	320
АНАЛИЗ УЯЗВИМОСТЕЙ СЕРВИСОВ АВТОРИЗАЦИИ И ВОЗМОЖНОСТИ ИХ СОВЕРШЕНСТВОВАНИЯ Бирюкова Александра Валерьевна	322
АНАЛИЗ МОДЕЛЕЙ ОЦЕНКИ КОНКУРЕНТНОЙ СПОСОБНОСТИ ОМТИ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ Бобрович Владимир Юрьевич, Алексеев Анатолий Владимирович, Антипов Василий Васильевич, Смольников Александр Васильевич	323
СОВРЕМЕННЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДАННЫХ КЛИНИЧЕСКИХ ИССЛЕДОВАНИЙ ЛЕКАРСТВЕННЫХ ПРЕПАРАТОВ Галимов Тимур, Сухов Родион, Шавинская Сания	324
АРХИТЕКТУРА, СОСТАВ И ТРЕБОВАНИЯ К СИСТЕМЕ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ ОМТИ Доминова Татьяна	326
ВЕРБАЛЬНАЯ СТРУКТУРНО-ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ АДАПТАЦИИ ТЕХНОЛОГИИ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ И УПРАВЛЕНИЯ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ ДЛЯ РЕШЕНИЯ КРИТИЧЕСКИ ВАЖНЫХ ЗАДАЧ ВМФ Каганский Михаил Александрович	327
ПРЕДЛОЖЕНИЯ В ОБОБЩЕННУЮ МОДЕЛЬ ИНТЕГРИРОВАННОЙ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ВМФ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ Каганский Михаил Александрович	329
ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНОГО КОМПЬЮТЕРНОГО АНАЛИТИЧЕСКОГО ТРЕНАЖЕРА (СКАТ) «БАРС» ДЛЯ ОТРАБОТКИ ПРАКТИЧЕСКИХ НАВЫКОВ ПО ОБЕСПЕЧЕНИЮ ЯДЕРНОЙ И РАДИАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ЭКСПЛУАТАЦИИ ЯЭУ ЭКИПАЖАМИ КОРАБЛЕЙ И ПОДВОДНЫХ ЛОДОК Каленихин Владимир Альбертович, Леберянский Александр Павлович, Салашенко Александр Иванович, ...	331
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МОРСКОМ СЕКТОРЕ ЕВРОПЕЙСКОГО СОЮЗА Колесникова Марина Львовна	333
К ВОПРОСУ О ПОВЫШЕНИИ ИНФОРМАЦИОННОГО КАЧЕСТВА МОРСКОГО ОБЪЕКТА Кружилин Роман Вячеславович	335
СЕРВИСЫ, ТЕХНОЛОГИИ, УЯЗВИМОСТИ, УГРОЗЫ И ЗАЩИТА BLUETOOTH Кузнецова Нина Александровна	336
ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ Лавренова Анна Алексеевна	336
ОСОБЕННОСТИ РАЗРАБОТКИ СИСТЕМ ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ БОРЬБЫ ЗА ЖИВУЧЕСТЬ ПОДВОДНОЙ ЛОДКИ С УЧЕТОМ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Левоева Инга Валерьевна, Мудрова Алёна Александровна	337

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЭКСПЛУАТАЦИИ ТЕХНИЧЕСКИХ СРЕДСТВ КОРАБЛЕЙ ВМФ Москаленко Василий Александрович, Коваленко Дмитрий Игоревич, Калюта Николай Георгиевич	339
МОНИТОРИНГ И УПРАВЛЕНИЕ КОМПЛЕКСНОЙ БЕЗОПАСНОСТЬЮ МОРСКОГО ПОРТА Пантелейкин Сергей Викторович	341
СОЦИАЛЬНЫЕ СЕТИ В ИНТЕРНЕТЕ Пархатский Дмитрий Дмитриевич	342
ОСНОВЫ МЕТОДИКИ ПОСТРОЕНИЯ ВИЗУАЛИЗИРОВАННЫХ ЛОГИКО-ВЕРОЯТНОСТНЫХ МОДЕЛЕЙ СТРУКТУРНО-СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ Поленин Владимир Иванович, Суценок Дмитрий Андреевич	343
ПРОБЛЕМЫ КОМПЛЕКСИРОВАНИЯ И ИНТЕГРАЦИИ АСУ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ Согонов Сергей Александрович, Алексеев Анатолий Владимирович, Хруцкий Олег Валентинович, Равин Александр Александрович.....	345
СИСТЕМА ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ ОПЕРАТОРА ЭНЕРГЕТИЧЕСКОЙ УСТАНОВКИ Хруцкий Олег Валентинович, Алексеев Анатолий Владимирович, Согонов Сергей Александрович	347
ИНТЕЛЛЕКТУАЛЬНАЯ ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ АДМИНИСТРАТОРА ИБ ТИПОВЫХ ОМТИ Стрельцов Егор Сергеевич	349
ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЕ ПОЛОЖЕНИЯ ФОРМИРОВАНИЯ И РАЗВИТИЯ ПСМВ КАК ЛАБОРАТОРИИ И ЦЕНТРА ФОРМИРОВАНИЯ СОВРЕМЕННЫХ IS-КОМПЕТЕНЦИЙ Тюрин Иван Сергеевич, Разживин Никита Сергеевич, Жуланова Дарья Николаевна	350
СОСТАВ И ТРЕБОВАНИЯ К СИСТЕМЕ МОНИТОРИНГА И УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ОМТИ Тюрина Виктория Викторовна, Тюрин Иван Сергеевич	352
ИНТЕЛЛЕКТУАЛЬНАЯ ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ АДМИНИСТРАТОРА ИБ ТИПОВЫХ ОМТИ Тюрин Иван Сергеевич.....	354
АНАЛИЗ УЯЗВИМОСТЕЙ И СРАВНЕНИЕ МЕТОДОВ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ Узбекова Юлия Шамильевна.....	355
ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ.....	357
МУЛЬТИМЕДИЙНЫЕ ТЕХНОЛОГИИ В СОХРАНЕНИИ КУЛЬТУРНОГО НАСЛЕДИЯ Барабаш Павел Александрович, Ляшенко Татьяна Васильевна	357
МАНИПУЛИРОВАНИЕ СОЗНАНИЕМ В ХОДЕ ПРОЦЕССОВ «ЦВЕТНЫХ РЕВОЛЮЦИЙ»: СИСТЕМНЫЙ ПОДХОД Борейко Андрей Андреевич	360
ПРИМЕНЕНИЕ СЕТЕЦЕНТРИЧЕСКОЙ КОНЦЕПЦИИ УПРАВЛЕНИЯ В ЦИФРОВОМ ОБЩЕСТВЕ Верзун Наталья Аркадьевна, Колбанев Михаил Олегович, Яковлев Сергей Алексеевич	362
ЗАЩИТА ИНФОРМАЦИИ И ЧЕЛОВЕЧЕСКИЙ ФАКТОР Карташов Павел Николаевич	363
ОСОБЕННОСТИ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ В ИНТЕРНЕТЕ Левкин Игорь Михайлович Науменко Ксения Андреевна, Виткова Лидия Андреевна.....	365
ИНФОРМАЦИОННЫЙ ПОТЕНЦИАЛ СУБЪЕКТА РОССИЙСКОЙ ФЕДЕРАЦИИ И СИТУАЦИОННЫЙ ЦЕНТР КАК ИНСТРУМЕНТ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМ ПОТЕНЦИАЛОМ Мальмберг Сергей Александрович	367
ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛА ОТ НАПАДЕНИЙ, ИСПОЛЬЗУЮЩИХ ТЕХНОЛОГИИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ Солодяников Александр Владимирович, Сухостат Валентина Васильевна, Антонова Любовь Сергеевна	369

ЧТО ТАКОЕ СОЦИАЛЬНЫЙ ИНЖИНИРИНГ Хайруллов Артем Вадимович, Галлямова Миляуша Равильевна	371
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АРКТИЧЕСКОГО РЕГИОНА	373
ПРИМЕНЕНИЕ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ РАБОТЫ ДОБЫВАЮЩИХ СКВАЖИН Вирстюк Анастасия Юрьевна, Микшина Виктория Степановна	373
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АРКТИЧЕСКОГО РЕГИОНА Голубева Мария Геннадьевна, Абрамова Кристина Владимировна	374
АЛЬТЕРНАТИВНАЯ КОНЦЕПЦИЯ СОЗДАНИЯ ИНТЕГРАЛЬНОЙ СИСТЕМЫ МОНИТОРИНГА ОБСТАНОВКИ В АРКТИКЕ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ Зимин Николай Семенович, Митько Арсений Валерьевич	376
ОЦЕНКА ВНУТРИСИСТЕМНОЙ ЭЛЕКТРОМАГНИТНОЙ СОВМЕСТИМОСТИ СЕТИ РАДИОСВЯЗИ С КОДОВЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ Крячко Александр Федотович, Антонов Кирилл Валерьевич	378
ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АРКТИКЕ Митько Валерий Брониславович	379
МОДЕЛЬ ОЦЕНКИ СТРАТЕГИЧЕСКОЙ УСТОЙЧИВОСТИ ГОСУДАРСТВА В АРКТИКЕ Поленин Владимир Иванович, Митько Валерий Брониславович	381
ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ И ЦЕЛОСТНОСТИ ДАННЫХ, ПЕРЕДАВАЕМЫХ БЕСПИЛОТНЫМИ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ В АРКТИЧЕСКОМ РЕГИОНЕ Шкоркина Елена Николаевна, Александрова Елена Борисовна	383
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭКОЛОГИИ.....	386
СОСТАВЛЕНИЕ ПРОСТРАНСТВЕННОЙ МОДЕЛИ И ПРОГНОЗНОЙ КАРТЫ УЧАСТКА ГУБА ДОЛГАЯ – ОЗЕРО БОЛЬШОЕ ТОРФЯНОЕ Ахметшина Анастасия Борисовна	386
ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ АКВАТОРИИ РЕКИ НЕВЫ, СВЯЗАННАЯ С РАЗЛИВАМИ НЕФТЕПРОДУКТОВ Биненко Виктор Иванович, Родионов Владимир Зенонович	387
ВКЛАД МЕТАНА В ЗАГРЯЗНЕНИЕ АТМОСФЕРНОГО ВОЗДУХА НАД Г. САНКТ-ПЕТЕРБУРГОМ Биненко Виктор Иванович, Северюхина Анастасия Сергеевна	387
ОЦЕНКА ЭКОЛОГИЧЕСКИХ РИСКОВ ПРИ РЕКОНСТРУКЦИИ МЕСТОРОЖДЕНИЯ В АРКТИЧЕСКОЙ ЗОНЕ РФ Быковская Елена Александровна, Кустикова Марина Александровна, Саусярис Эдгарас Стасевич, Макурова Александра Сергеевна	388
АВТОМАЗИРОВАННАЯ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНАЯ СИСТЕМА ДЛЯ КОНТРОЛЯ СОСТАВА ДЕЗИНФИЦИРУЮЩИХ РАСТВОРОВ СОДЕРЖАЩИХ ПОЛИГЕКСАМЕТИЛЕНГУАНИДИН Василевский Александр Михайлович, Герасимов Владимир Александрович, Коноплев Георгий Асадович, Кострин Дмитрий Константинович, Степанова Оксана Сергеевна, Ухов Андрей Александрович	390
ПРОСТРАНСТВЕННАЯ ДИНАМИЧЕСКАЯ МОДЕЛЬ РЕГИОНАЛЬНОГО УРОВНЯ ОКРЕСТНОСТИ ОЗЕРА КРАСНОЕ Воронцова Екатерина Николаевна	392
РАЗРАБОТКА ПРОСТРАНСТВЕННОЙ ДИНАМИЧЕСКОЙ МОДЕЛИ: ЭКОЛОГО-ЭКОНОМИЧЕСКАЯ МОДЕЛЬ КАРТЫ ДРЕВЕСНЫХ ЗАПАСОВ Герасимов Константин Романович, Хворостовский Артемий, Кравцов Илья	393

КОГНИТИВНЫЙ МОНИТОРИНГ ЭКСТРЕМАЛЬНЫХ СОСТОЯНИЙ В МНОГОМЕРНЫХ ВРЕМЕННЫХ РЯДАХ ДАННЫХ О ПРИРОДНЫХ СИСТЕМАХ Горохов Владимир Леонидович, Бузников Анатолий Алексеевич, Витковский Владимир Валентинович.....	394
КОГНИТИВНОЕ ОБНАРУЖЕНИЕ АНОМАЛИЙ И ВТОРЖЕНИЙ В МНОГОМЕРНЫХ ВРЕМЕННЫХ РЯДА ДАННЫХ ГИДРОЛОГИЧЕСКОГО МОНИТОРИНГА СКВАЖИН Горохов Владимир Леонидович, Бузников Анатолий Алексеевич	395
СТРУКТУРА ЭКОСИСТЕМ МЕЖОЗЕРЬЯ ДОЛГОЕ-ПОДСЕКИРНОЕ НА ТОПОЛОГИЧЕСКОМ УРОВНЕ Кувардина Мария Юрьевна	396
ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ МЕТОДОВ ОБРАБОТКИ СИГНАЛОВ И ИЗОБРАЖЕНИЙ В ЗАДАЧАХ ЭКСПРЕСС ВИБРОДИАГНОСТИКИ НА ОБЪЕКТАХ ТЭК Малышев Григорий Сергеевич, Гришканич Александр Сергеевич, Локтаев Кирилл Виленинович	397
ПРЕДСТАВЛЕНИЕ ОТКРЫТЫХ ДАННЫХ МОНИТОРИНГА АТМОСФЕРЫ ДЛЯ ПОВЫШЕНИЯ ИНФОРМИРОВАННОСТИ НАСЕЛЕНИЯ О СОСТОЯНИИ ОКРУЖАЮЩЕЙ СРЕДЫ Мателенок Игорь Владимирович, Мелентьев Владимир Владимирович.....	398
СОЗДАНИЕ СТРУКТУРНО-ДИНАМИЧЕСКОЙ МОДЕЛИ ТИПОВ ВЫДЕЛОВ ТЕРРИТОРИИ И ПРОГНОЗНОЙ ТЕМАТИЧЕСКОЙ КАРТЫ РАСПРЕДЕЛЕНИЯ ЛЕСОВ ПО КЛАССАМ ВЛАЖНОСТИ ПОЧВ НА ПРИМЕРЕ ЦЕНТРАЛЬНО-ЮГО-ЗАПАДНОЙ ЧАСТИ О. СОЛОВЕЦКОГО Носова Анастасия Олеговна.....	400
ИНФОРМАЦИОННАЯ И ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ПРИРОДНОЙ СРЕДЫ Павлова Светлана Михайловна	401
СТРУКТУРНАЯ МОДЕЛЬ ЮЖНОЙ ЧАСТИ БОЛЬШОГО СОЛОВЕЦКОГО ОСТРОВА Позднякова Виктория Владимировна	403
МОДЕЛЬ ФОРМИРОВАНИЯ ОЦЕНКИ АДДИТИВНОГО ЭКОЛОГИЧЕСКОГО УЩЕРБА ОТ ОБЪЕКТОВ ПРОШЛОГО ЭКОЛОГИЧЕСКОГО УЩЕРБА Романюк Людмила Павловна, Петухов Валерий Васильевич.....	404
ПРИМЕНЕНИЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ В ЦЕЛЯХ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ, ДЕЯТЕЛЬНОСТИ СИЛОВЫХ СТРУКТУР И ОТРАСЛЕЙ ЭКОНОМИКИ РОССИИ Тимошук Александр Сергеевич, Доронин Александр Павлович, Калустов Ярослав Игоревич.....	405
ЭКОЛОГИЧЕСКАЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕПЛОВОГО АВИАЦИОННОГО МОНИТОРИНГА САНКТ-ПЕТЕРБУРГА Шилин Борис Владимирович	406
МОДЕРН УМЕРЕННОГО ПЛАНА Ярошевич Людмила Ивановна	407
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИОКОМПЬЮТИНГЕ	409
ПОДХОД К ПОСТРОЕНИЮ СИСТЕМЫ УПРЕЖДАЮЩЕЙ ДИАГНОСТИКИ УЯЗВИМОСТЕЙ ПЕРСОНАЛА К СОЦИОИНЖЕНЕРНЫМ АТАКАМ Абрамов Максим Викторович	409
ПОСТРОЕНИЕ СТРАТЕГИИ ЗАЩИТЫ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ СОЦИОИНЖЕНЕРНЫХ АТАКУЮЩИХ ВОЗДЕЙСТВИЙ ЗЛОУМЫШЛЕННИКА Азаров Артур Александрович, Хлобыстова Анастасия Олеговна	410
АНАЛИЗ ПРОФИЛЕЙ СОЦИАЛЬНОЙ СЕТИ В КОНТЕКСТЕ СОЦИОИНЖЕНЕРНЫХ АТАК Багрецов Георгий Игоревич	411
УСЛОВИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КЛИНИЧЕСКОЙ СФЕРЕ СИСТЕМЫ ЗДРАВООХРАНЕНИЯ Блюм Владислав Станиславович.....	412

ПОДХОД К ПОСТРОЕНИЮ ПРОФИЛЯ КОМПЕТЕНЦИЙ ЗЛОУМЫШЛЕННИКА В ЗАДАЧЕ АНАЛИЗА ЗАЩИЩЁННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОТ СОЦИОИНЖЕНЕРНЫХ АТАК Бушмелев Федор Витальевич, Абрамов Максим Викторович	413
ПРИМЕНЕНИЕ МЕТОДОВ DATA MINING ДЛЯ ПОЛУЧЕНИЯ ИНФОРМАЦИИ О ПОЛЬЗОВАТЕЛЯХ СОЦИАЛЬНЫХ СЕТЕЙ Зегжда Дмитрий Петрович, Лемец Андрей Александрович, Павленко Евгений Юрьевич	414
СИНТЕЗ ТРЕТИЧНОЙ СТРУКТУРЫ АЛГЕБРАИЧЕСКОЙ БАЙЕСОВСКОЙ СЕТИ НА БАЗЕ ОРИЕНТИРОВАННОГО ГРАФА ВТОРИЧНОЙ СТРУКТУРЫ Золотин Андрей Алексеевич	416
МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ РЕЗОНАТОРОВ, ОБЕСПЕЧИВАЮЩИХ ЗАЩИТУ ОТ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ Копыльцов Александр Васильевич	418
АЛГОРИТМ ОЦЕНИВАНИЯ БЕЗОПАСНОСТИ ПОСТУПАЮЩЕЙ СЛАБО ФОРМАЛИЗОВАННОЙ ИНФОРМАЦИИ Копыльцов Антон Александрович	420
ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОПРЕДЕЛЕНИЯ АВТОМАТИЧЕСКИ УПРАВЛЯЕМЫХ УЧЕТНЫХ ЗАПИСЕЙ В СОЦИАЛЬНЫХ СЕТЯХ Малышев Егор Валерьевич, Павленко Евгений Юрьевич, Зегжда Петр Дмитриевич	422
АНАЛИЗ ЧУВСТВИТЕЛЬНОСТИ ЛОКАЛЬНОГО ЛОГИКО-ВЕРОЯТНОСТНОГО ВЫВОДА В МАТЕМАТИЧЕСКОЙ БИБЛИОТЕКЕ ALGBN MATH LIBRARY Мальчевская Екатерина Андреевна	423
ЯЗЫКОВЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Микони Станислав Витальевич	424
ВОССТАНОВЛЕНИЕ ПРОФИЛЯ УЯЗВИМОСТЕЙ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВАНИИ ИНФОРМАЦИИ, КОТОРАЯ МОЖЕТ БЫТЬ ПОЛУЧЕНА ИЗ СОЦИАЛЬНЫХ СЕТЕЙ Слѣзкин Никита Евгеньевич, Азаров Артур Александрович	426
АВТОМАТИЧЕСКОЕ ИЗВЛЕЧЕНИЕ ДАННЫХ О ДЛИНАХ ИНТЕРВАЛОВ МЕЖДУ ПОСЛЕДОВАТЕЛЬНЫМИ ЭПИЗОДАМИ ИЗ ОПРОСНИКА О ПОСЛЕДНИХ ЭПИЗОДАХ ПОВЕДЕНИЯ Столярова Валерия Фуатовна	427
МОДЕЛИРОВАНИЕ НЕТОЧНОСТИ ОТВЕТОВ В БАЙЕСОВСКОЙ СЕТИ ДОВЕРИЯ ДЛЯ ОЦЕНИВАНИЯ СОЦИАЛЬНО-ЗНАЧИМОГО ПОВЕДЕНИЯ РЕСПОНДЕНТОВ Суворова Алена Владимировна, Акульшина Ольга Дмитриевна	429
АНАЛИЗ ТЕКСТОВОЙ ИНФОРМАЦИИ ПОСТОВ В СОЦИАЛЬНОЙ СЕТИ КАК ОСНОВА ПСИХОЛОГИЧЕСКОГО ПРОФИЛЯ ПОЛЬЗОВАТЕЛЯ Суворова Алѐна Владимировна, Тулупьева Татьяна Валентиновна	430
ПОСТРОЕНИЕ СОЦИАЛЬНОГО ГРАФА СОТРУДНИКОВ КОМПАНИИ НА ОСНОВАНИИ ИНФОРМАЦИИ, ПОЛУЧАЕМОЙ ИЗ СОЦИАЛЬНЫХ СЕТЕЙ, ДЛЯ РАСЧѐТА ВЕРОЯТНОСТИ УСПЕХА СОЦИОИНЖЕНЕРНОЙ АТАКИ Сулейманов Алексей Александрович, Тулупьева Татьяна Валентиновна, Тулупьев Александр Львович	431
СИНТЕЗ МОДЕЛИ СОЦИАЛЬНО-ЗНАЧИМОГО ПОВЕДЕНИЯ КАК БАЙЕСОВСКОЙ СЕТИ ДОВЕРИЯ СО СКРЫТЫМИ ПЕРЕМЕННЫМИ Торопова Александра Витальевна	433
АЛГЕБРАИЧЕСКИЕ БАЙЕСОВСКИЕ СЕТИ КАК ИНСТРУМЕНТ АГРЕГИРОВАНИЯ СТАТИСТИЧЕСКОЙ И ЭКСПЕРТНОЙ ИНФОРМАЦИИ В ЗАДАЧАХ СОЦИАЛЬНОГО КОМПЬЮТИНГА Тулупьев Александр Львович	433

ЭКСПРЕСС-ДИАГНОСТИКА ОСОБЕННОСТЕЙ ЛИЧНОСТИ ПО ЦИФРОВЫМ СЛЕДАМ Тулупьева Татьяна Валентиновна	435
АЛГОРИТМЫ ПОДДЕРЖАНИЯ НЕПРОИВОРЕЧИВОСТИ В АЛГЕБРАИЧЕСКИХ БАЙЕСОВСКИХ СЕТЯХ В РАМКАХ БИБЛИОТЕКИ ALGBN MATH LIBRARY Харитонов Никита Алексеевич	436
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КИБЕРФИЗИЧЕСКИХ СИСТЕМ	438
ИССЛЕДОВАНИЕ СОЗДАНИЯ БЕЗОПАСНЫХ ПРОГРАММ ДЛЯ ВЫСОКОПРОИЗВОДИТЕЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ ПЛАТФОРМЫ Бежан Роман Романович, Медведев Михаил Сергеевич, Арустамов Сергей Аркадьевич	438
УСЛОВИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КЛИНИЧЕСКОЙ СФЕРЕ СИСТЕМЫ ЗДРАВООХРАНЕНИЯ Блюм Владислав Станиславович.....	439
ЗАЩИТА ИНФОРМАЦИИ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА В МНОГОУРОВНЕВЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ Бондаренко Игорь Борисович, Шиманчук Сергей Николаевич	440
ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ НСД С ИСПОЛЬЗОВАНИЕМ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ Брагина Елизавета Константиновна, Егоров Илья Эдуардович	442
РАЗРАБОТКА АППАРАТНО-ПРОГРАММНОГО КОМПЛЕКСА ИДЕНТИФИКАЦИИ СОСТОЯНИЯ ОБЪЕКТОВ И СУБЪЕКТОВ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИЙ ИНТЕРНЕТ ВЕЩЕЙ Дикий Дмитрий Игоревич, Артемьева Виктория Денисовна	444
УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ КИБЕРФИЗИЧЕСКИХ СИСТЕМ НА ОСНОВЕ ГОМЕОСТАТА Зегжда Петр Дмитриевич, Зегжда Дмитрий Петрович, Павленко Евгений Юрьевич.....	445
СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. ФИШИНГ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ ЕМУ Ильченко Лидия Михайловна, Уваров Роман Валерьевич, Зайцев Святослав Игоревич.....	446
СОВРЕМЕННЫЕ НЕЙРОСЕТЕВЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ КИБЕРУГРОЗ В СЕТЯХ VANET/FANET/MARINET Калинин Максим Олегович, Зегжда Петр Дмитриевич.....	449
АСИММЕТРИЯ ВРЕМЕНИ В ТЕОРИИ ПРОГНОЗИРОВАНИЯ СОСТОЯНИЯ СЛОЖНЫХ ДИНАМИЧЕСКИХ СИСТЕМ Острейковский Владислав Алексеевич, Денисова Татьяна Юрьевна, Шевченко Елена Николаевна.....	450
ИМПОРТОЗАМЕЩАЮЩЕЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ В ПРАКТИКЕ ПРОИЗВОДСТВЕННЫХ ИСПЫТАНИЙ МАШИНОСТРОИТЕЛЬНЫХ ИЗДЕЛИЙ Первухина Елена Львовна, Осипов Константин Николаевич, Тимофеев Илья Сергеевич.....	451
МЕТОДЫ ИЗВЛЕЧЕНИЯ ДАННЫХ С ИЗОЛИРОВАННЫХ МАШИН Романов Александр Алексеевич	452
МЕТОДИКИ И ИНСТРУМЕНТЫ АУДИТА СЕТЕВОЙ БЕЗОПАСНОСТИ Садикова Анастасия Александровна, Титова Юлия Алексеевна, Савков Сергей Витальевич	453
ПОВЫШЕНИЕ ТОЧНОСТИ МЕТОДОВ СТЕГАНОАНАЛИЗА ПУТЕМ ОПТИМИЗАЦИИ ПАРАМЕТРОВ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ Сивачев Алексей Вячеславович, Михайличенко Ольга Викторовна	455
ПРОБЛЕМА АНОНИМНОСТИ В СЕТИ ИНТЕРНЕТ СРАВНЕНИЕ МЕТОДОВ АНОНИМИЗАЦИИ ПОЛЬЗОВАТЕЛЯ Титова Юлия Алексеевна, Садикова Анастасия Александровна, Савков Сергей Витальевич	456

АНАЛИЗ ПРОТОКОЛА X-RACE Шенец Николай Николаевич, Трухина Екатерина Евгеньевна.....	458
ПРИМЕНЕНИЕ ИЗОГЕНИЙ ЭЛЛИПТИЧЕСКИХ КРИВЫХ ДЛЯ ПОСТРОЕНИЯ СХЕМЫ ГРУППОВОЙ ПОДПИСИ Штыркина Анна Александровна, Ярмач Анастасия Викторовна, Александрова Елена Борисовна	459
ПОДГОТОВКА И ПЕРЕПОДГОТОВКА КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	462
МУЛЬТИМЕДИЙНЫЕ ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ: ПРОБЛЕМЫ СОЗДАНИЯ И ИСПОЛЬЗОВАНИЯ Барабаш Павел Александрович, Ляшенко Татьяна Васильевна	462
ЛАБОРАТОРНЫЙ ПРАКТИКУМ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ» Барабаш Павел Александрович, Панасенко Михаил Александрович	466
МОДЕЛИРУЮЩИЙ УЧЕБНО-ТРЕНИРОВОЧНЫЙ ТРЕНАЖЕР ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОГО ФУНКЦИОНИРОВАНИЯ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ Богданов Тимур Рушанович, Яшин Александр Иванович.....	467
ИССЛЕДОВАНИЕ КАЧЕСТВА ОБРАЗОВАНИЯ ПРИ ПОДГОТОВКЕ СОТРУДНИКОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ Большакова Людмила Валентиновна, Кузьмина Кристина Александровна, Яковлева Наталья Александровна	469
О НЕОБХОДИМОСТИ ПОДГОТОВКИ И ПЕРЕПОДГОТОВКИ КВАЛИФИЦИРОВАННЫХ КАДРОВ В СФЕРЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ Бурлов Вячеслав Георгиевич, Грачев Михаил Иванович, Примакин Алексей Иванович	470
СЕТЕЦЕНТРИЗМ – ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКАЯ ОСНОВА ЦИФРОВОГО ОБЩЕСТВА Верзун Наталья Аркадьевна, Колбанев Михаил Олегович, Касаткин Виктор Викторович	472
РАЗВИТИЕ ПРИНЦИПОВ ПОСТРОЕНИЯ СЕТЕЙ ЭЛЕКТРОСВЯЗИ Верзун Наталья Аркадьевна, Колбанев Михаил Олегович, Ипатов Олег Сергеевич	474
ОБОБЩЕННАЯ МОДЕЛЬ ДЕЯТЕЛЬНОСТИ В ЦИФРОВОМ ОБЩЕСТВЕ Верзун Наталья Аркадьевна, Колбанев Михаил Олегович, Цехановский Владислав Владимирович.....	475
ОСОБЕННОСТИ ПЕРЕДАЧИ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ В МОДУЛЬНОЙ УЧЕБНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ Журавлев Антон Евгеньевич	476
ФОРМИРОВАНИЕ И ИСПОЛЬЗОВАНИЕ В УЧЕБНОМ ПРОЦЕССЕ СИТУАЦИОННОГО ЦЕНТРА ДЕЛОВОЙ РАЗВЕДКИ Левкин Игорь Михайлович, Микадзе Сергей Юрьевич	478
К ВОПРОСУ ПОДГОТОВКИ РАЗРАБОТЧИКОВ ПЕРСПЕКТИВНОГО ОТЕЧЕСТВЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ Первухина Елена Львовна, Шалимова Елена Михайловна.....	480
К ВОПРОСУ ПОДГОТОВКИ КАДРОВ ДЛЯ ЦИФРОВОЙ ЭКОНОМИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ Резунков Димитрий Андреевич, Иманов Гейдар Мамедович, Резункова Ольга Петровна	481
ПОДХОД К МОДЕРНИЗАЦИИ МНОГОУРОВНЕВОЙ СИСТЕМЫ ВЫСШЕГО ОБРАЗОВАНИЯ В РОССИИ В УСЛОВИЯХ СОВРЕМЕННЫХ ВНУТРЕННИХ И ВНЕШНИХ УГРОЗ Советов Борис Яковлевич, Касаткин Виктор Викторович.....	486
СОВРЕМЕННЫЕ УГРОЗЫ РАЗВИТИЮ РОССИЙСКОЙ ОБРАЗОВАТЕЛЬНОЙ СИСТЕМЫ Советов Борис Яковлевич, Касаткин Виктор Викторович.....	487

МЕТОДЫ ПОВЫШЕНИЯ КАЧЕСТВА ПОДГОТОВКИ СПЕЦИАЛИСТОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Соколов Сергей Сергеевич	489
ИЗУЧЕНИЕ МЕТОДОВ УПРАВЛЕНИЯ ДОСТУПОМ В БАЗОВОЙ ДИСЦИПЛИНЕ «ОПЕРАЦИОННЫЕ СИСТЕМЫ» СПЕЦИАЛЬНОСТИ «КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ» Широков Владимир Владимирович, Щиголева Марина Андреевна	490
МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПРОБЛЕМЫ УСТОЙЧИВОГО РАЗВИТИЯ»	492
СТРАТЕГИИ РАЗВИТИЯ УМНОГО ИНФОРМАЦИОННОГО ОБЩЕСТВА Бариков Леонид Николаевич, Игнатьев Михаил Борисович	492
МОДЕЛИРОВАНИЕ ОРГАНИЗМА ЧЕЛОВЕКА ДЛЯ ПОДДЕРЖКИ ВРАЧЕБНЫХ РЕШЕНИЙ Губин Александр Вадимович, Игнатьев Михаил Борисович, Катермина Татьяна Сергеевна, Красников Андрей Георгиевич	492
К ВОПРОСУ О СОЗДАНИИ НОВОГО ЗДАНИЯ МУЗЕЯ ОБОРОНЫ И БЛОКАДЫ ЛЕНИНГРАДА Игнатьев Михаил Борисович, Макин Алексей Иванович, Мамошин Михаил Александрович, Никитин Александр Иванович, Фадеева Нина Владимировна	493
ТИПОВЫЕ ИНФОРМАЦИОННЫЕ УГРОЗЫ БАЗАМ ДАННЫХ CRM-СИСТЕМ И МЕТОДЫ ЗАЩИТЫ ОТ НИХ Репина Валерия Владимировна	494
СТРАТЕГИИ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РЕГИОНАЛЬНЫХ ЭКОНОМИЧЕСКИХ СИСТЕМАХ С УЧЕТОМ РАЗНЫХ ТИПОВ РЕАКЦИЙ НА ВЫЗОВЫ ВНЕШНЕЙ СРЕДЫ Титовец Алиса Юрьевна	496
ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ВЛОЖЕНИЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКА В БАЙТ-КОД ПУТЕМ ЗАМЕНЫ УЯЗВИМОГО БАЙТ-КОДА JAVA КЛАССА Шариков Павел Иванович, Красов Андрей Владимирович	499
МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»	501
ПОСТРОЕНИЕ ИНФОРМАЦИОННО-МОНИТОРИНГОВОЙ СИСТЕМЫ АРОМОБЕЗОПАСНОСТИ НА АППАРАТНО-ПРОГРАММНЫХ СРЕДСТВАХ Антонов Валерий Валентинович	501
ПРИМЕНЕНИЕ МАШИННОГО ОБУЧЕНИЯ В ГЛУБОКОМ АНАЛИЗЕ СЕТЕВОГО ТРАФИКА Безверхняя Екатерина Александровна	502
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ Бондарева Анастасия Дмитриевна, Гоман Елена Вячеславовна	503
МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ЦИФРОВОЙ СТЕГАНОГРАФИИ Галлямова Миляуша Равильевна	505
СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАЩИЩЕННОСТИ ОСУЩЕСТВЛЕНИЯ ФИНАНСОВЫХ ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ БЕСКОНТАКТНОЙ ОПЛАТЫ Ганчикова Юлия Сергеевна, Курышева Алена Андреевна	507
МЕТОДЫ И СТРАТЕГИИ ОПОВЕЩЕНИЯ НАСЕЛЕНИЯ ОБ УГРОЗАХ ВОЗНИКНОВЕНИЯ КРИЗИСНЫХ СИТУАЦИЙ Гераськина Вероника Сергеевна, Сахаров Дмитрий Владимирович, Пестов Игорь Евгеньевич, Виткова Лидия Андреевна	507

КОНВЕРГЕНЦИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМ ПРОСТРАНСТВОМ САНКТ-ПЕТЕРБУРГА Головлёва Юлия Андреевна, Виткова Лидия Андреевна, Ковцур Максим Михайлович, Дмитриева Екатерина Викторовна.....	510
ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ВЕБ-СЕРВЕРА PYTHON-ПРИЛОЖЕНИЙ ДЛЯ РАЗМЕЩЕНИЯ НА КЛИЕНТСКИХ МАШИНАХ Грибачев Виталий Петрович, Харитонов Георгий Дмитриевич.....	512
ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ОДНОРАЗОВОГО БЛОКНОТА ДЛЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ ПОТОКОВ БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА Грозов Владимир Андреевич.....	513
АНАЛИЗ ПРОТОКОЛОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИОТ-СРЕДЕ Долгун Владислав Олегович, Литвинов Владислав Леонидович.....	515
ОСОБЕННОСТИ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ НАЗЕМНОГО ГОРОДСКОГО ПАССАЖИРСКОГО ТРАНСПОРТА Ильченко Лидия Михайловна, Зайцев Святослав Игоревич.....	517
ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ОБУЧЕНИИ ХИМИИ Колоколов Даниил Сергеевич.....	519
ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ Красов Андрей Владимирович, Левин Марк Вадимович, Фостач Елена Сергеевна.....	520
АНАЛИЗ ЗАЩИЩЕННОСТИ ERP-СИСТЕМ. ОБЩИЙ ПОДХОД К АНАЛИЗУ Кривдюк Надежда Михайловна.....	522
СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАЩИЩЕННОСТИ ОСУЩЕСТВЛЕНИЯ ФИНАНСОВЫХ ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ Курышева Алена Андреевна, Ганчикова Юлия Сергеевна.....	523
АНАЛИЗ СУЩЕСТВУЮЩИХ ДАТЧИКОВ ДЛЯ ВЫЯВЛЕНИЯ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ Лисецкая Кристина Валерьевна.....	524
ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Орлов Иван Алексеевич.....	525
РАСПРЕДЕЛЁННЫЙ МОДЕЛЬНО-АНАЛИТИЧЕСКИЙ ИНТЕЛЛЕКТ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ Птицына Лариса Константиновна, Гусев Дмитрий Сергеевич.....	528
АНАЛИЗ СОВРЕМЕННЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДОВ ПРОНИКНОВЕНИЯ В КОМПЬЮТЕРНУЮ СИСТЕМУ Лукин Евгений Игоревич, Прокопович Максим Сергеевич, Федоров Дмитрий Юрьевич.....	530
СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА ПРИМЕРЕ ВЫШЕГО УЧЕБНОГО ЗАВЕДЕНИЯ Сазонов Антон Борисович, Немченко Алексей Алексеевич.....	531
ФОРМАЛИЗОВАННЫЙ ПОДХОД К АНАЛИЗУ ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ Уткина Алена Алексеевна, Юркин Дмитрий Валерьевич.....	532
ПРЕДВАРИТЕЛЬНАЯ ОБРАБОТКА ГРАФИЧЕСКИХ ОБЪЕКТОВ ДЛЯ ЗАДАЧИ ИДЕНТИФИКАЦИИ В ВИДЕОПОТОКЕ Шевченко Денис Алексеевич.....	534
ИССЛЕДОВАНИЕ ДЕЙСТВУЮЩЕЙ ИТ-ИНФРАСТРУКТУРЫ ОРГАНИЗАЦИИ ДЛЯ ПОСЛЕДУЮЩЕГО ПЕРЕХОДА К ОБЛАЧНОЙ АРХИТЕКТУРЕ Чмутов Михаил Валериевич, Ковцур Максим Михайлович, Ушаков Игорь Александрович, Пестов Игорь Евгеньевич.....	535

ЗАКОН СОХРАНЕНИЯ ЦЕЛОСТНОСТИ ОБЪЕКТА В УСЛОВИЯХ РАЗРУШЕНИЯ ПРОГРАММНО-
АППАРАТНОЙ СРЕДЫ

Мокеева Татьяна Олеговна, Долгирева Елена Сергеевна, профессор Бурлов Вячеслав Георгиевич.....537

ОГЛАВЛЕНИЕ..... 539

CONTENTS..... 561

CONTENTS

INFORMATION SECURITY IN THE NORTH-WEST FEDERAL DISTRICT AS AN EXAMPLE OF IMPLEMENTATION OF REGIONAL STATE POLICY Kucheryavyi Mikhail, Vovenda Julia	15
THE CONCEPT OF SECURITIZATION IN THE CONTEXT OF INFORMATION POLICY OF RUSSIA Baranov Nikolai	17
MANAGEMENT OF THE INTELLECTUAL ENVIRONMENT AMONG THE EXAMPLE OF THE HOUSING AND MUNICIPAL SPHERE OF SAINT PETERSBURG Gruzdeva Maria ¹ , Sharipov Roman ²	19
ACTUAL ASPECTS OF INFORMATION INFRASTRUCTURE IN THE IMPLEMENTATION OF STATE MIGRATION POLICY IN THE RUSSIAN FEDERATION Klechikov Aleksandr	21
THE POSTAL ASSETS IN THE CREATION OF A SMART CITY PROTECTED INFORMATION SPACE Pavlovskaya Maria, Kononova Olga	22
RUSSIAN INFORMATION POLICY IN THE CONTEXT OF THE INFORMATION SOCIETY DEVELOPMENT STRATEGY Popov Pavel Valentinovich	24
METHODOLOGICAL ASPECTS OF FORMATION OF SYSTEM OF DISTRIBUTED SITUATIONAL CENTERS Sokolov Boris, Salukhov Vladimir	27
FEATURES OF TRAINING IN THE FIELD OF INFORMATION SECURITY IN THE NORTH-WEST FEDERAL DISTRICT Victor Storozhik	30
INFORMATION AS THE MOST IMPORTANT RESOURCE FOR MAKING EFFECTIVE MANAGERIAL DECISIONS Tarashnina Svetlana	32
DIGITAL ECONOMY PROGRAM: RUSSIAN FEDERATION INFORMATIZATION POLICY CONTEXT Chugunov Andrei	34
TRUST BETWEEN COUNTERPARTIES IN INFORMATION SYSTEMS Shugay Anton	36
PRINCIPLES OF INCREASE IN SECURITY OF INFORMATION OF NETWORKS MOBILE RADIO COMMUNICATION OF THE LAW-ENFORCEMENT SPHERE ON THE BASIS OF ENHANCEMENTS OF FREQUENCY AND TERRITORIAL PLANNING Babkin Alexander Nikolaevich	38
THE PROBLEM OF VISUALIZING ROUTES RUN COMPUTER PROGRAMS Bezrukov Vjacheslav, Sineshchuk Yuri Sineshchuk Maxim	40
SYNTHESIS ALGORITHM OF EFFECTIVE INFORMATION SYSTEMS Vilkov Valeriy ¹ , Sychev Sergey ² , Chernykh Andrey ²	41
SOME ASPECTS OF ENSURING INFORMATION SECURITY DURING THE IMPLEMENTATION OF THE POLICE FUNCTIONS OF THE STATE PROTECTION Galushko Valery, Voronov Anatoly, Malakhov Alexander	43
THE APPROACH TO THE DEVELOPMENT WORKSTATION ON DUTY AT THE UNIVERSITY Ivanov Nikolay, Potekhin Vladimir	44

APPROACH TO ADAPTATION OF TYPICAL SOLUTIONS AT THE DEVELOPMENT OF THE ACCESS MANAGEMENT CONTROL SYSTEM FOR SPECIAL IMPORTANCE OBJECTS Kalachev Maksim, Potekhin Vladimir, Saratov Dmitriy	46
ABOUT LEGAL ASPECTS OF ELECTRONIC LIBRARY Oleg Kononov, Olga Kononova	47
ABOUT ETHICS OF ELECTRONIC CORRESPONDENCE Oleg Kononov, Olga Kononova	49
APPROACHES TO INFORMATION-PSYCHOLOGICAL SECURITY OF THE PERSON Kostyuk Anatoliy	50
PECULIARITIES OF PEDAGOGICAL COMMUNICATIONS IN THE CONDITIONS OF EDUCATION INFORMATIZATION Kostyuk Anatoliy, Bobonets Sergey	52
ORGANIZATIONAL STRUCTURES AND INFORMATION SECURITY Kostyuk Anatoliy, Bobonets Sergey	54
MODEL FOR FORMATION OF REQUIREMENTS FOR CONFIDENTIALITY OF INTEGRITY AND ACCESSIBILITY OF DATA IN THE SYSTEM OF INFORMATION PROTECTION OF MEANS OF COMPUTER ENGINEERING AND AUTOMATED SYSTEMS Kuvatov Valery Ilyich, Primakin Alexey Ivanovich	56
ABOUT THE THEORETICAL UNDERSTANDING OF LEGAL REGULATION IN THE FIELD OF IT INFORMATIZATION Lyadov Aleksey, Evseyev Aleksey	58
PROBLEMS OF THE MODERN OPERATIVE-INVESTIGATIVE TECHNOLOGIES USING IN THE TERRORISM COUNTERACTION Nigmatov Nikolay	60
COMPLEX DEFENCE OF INFORMATION IN ORGANS OF INTERNAL AFFAIRS IN MODERN TERMS Nikolay Parfenov, Sergey Alekseev	62
PERSONAL DATA PROTECTION EMPLOYEES ATS BY SPECIAL TREATMENT Nikolay Parfenov, Sergey Alekseev	64
SOME ASPECTS OF INFORMATION SECURITY OF THE SCHOOLCHILDREN Popravko Anna	66
ON APPROBATION OF HYPERLINKS TECHNOLOGY AT WORK WITH DOCUMENTS, LOCATED IN THE SUBDIVISION DEPARTMENT Gorelenko Konstantin, Potekhin Vladimir	67
ISSUES OF ENSURING THE INFORMATION SECURITY OF INSORMATION SYSTEMS OF LAW-ENFORCEMENT BODIES OF RUSSIAN FEDERATION Redkovnikov Vladislav	69
AN APPROACH TO DEVELOPMENT OF INFORMATION SUPPORT TOOLS AT THE INDEPENDENT TRAINING OF TRAINED TO EXERCISE AND EXAMINATION ON THE EXAMPLE OF ONE OF THE DISCIPLINES RELATED TO SECURING INFORMATION SECURITY Ryzhova Valentina, Potekhin Vladimir	70
TRAINING CHECKPOINT, AS PART OF THE INFORMATION SECURITY SYSTEM "BATTLE SYSTEM" OF THE MINISTRY OF INTERIOR Salikov Alexander, Sineshchuk Yuri	72

COMPREHENSIVE ASSESSMENT OF SECURITY ASSURANCE INFORMATION SYSTEMS OF THE ST. PETERSBURG UNIVERSITY OF THE MOI OF RUSSIA THROUGH THE APPLICATION OF METHODS OF MULTIDIMENSIONAL ANALYSIS (ON THE EXAMPLE OF CLUSTER AND DISCRIMINANT ANALYSIS) Saratov Dmitry, Mikhail Kozlov, Huhkha Christina	74
MODERN CONDITION AND PROSPECTS FOR DEVELOPMENT OF THE TRAINING SYSTEM OF SPECIALISTS IN FIELDS OF INFORMATION SECURITY FOR EMERGENCY RUSSIA Saratov Dmitry, Podrzhkina Tatyana	76
CLOUD TECHNOLOGY AS A MEANS OF PREVENTING THE LOSS OF DATA Sineshchuk Yuri, Trubin Igor.....	79
ON AUTOMATION OF THE MOVEMENT MANAGEMENT PROCESS OF THE SPECIAL VEHICLES AT THE CROSSROADS WITH THE RFID USE Smolentseva Linda, Potekhin Vladimir	81
INFORMATION-PSYCHOLOGICAL PROTECTION OF EMPLOYEES OF POWER STRUCTURES Yarmolenko Natalia.....	82
SECURITY OF ACCESS TO EDUCATIONAL RESOURCES BY REMOTE ACCESS Anisimov Andrey Vladimirovich.....	85
ORGANIZATION OF INFORMATION SECURITY IN THE INFORMATION SYSTEM Baryshnikova Nadezhda, Egorov Aleksandr, Krupenina Nataliya.....	87
INSECURITY OF MOBILE DEVICES Bashmakov Alexey	88
ADAPTATION OF THE ALGORITHM FOR SOLVING CUBIC EQUATIONS IN A FINITE BINARY FIELD FOR DENIED ENCRYPTION Budchan Darya	90
DEVELOPMENT OF TECHNOLOGY MANAGING THE PROCESS SECURING INFORMATION ON THE EXAMPLE WEB – APPLICATIONS Burlov Viacheslav, Petrov Sergey, Grozmani Elena	92
MODELING OF SYSTEM BASED ON THE INTEGRITY CONSERVATION LAW Burlov Vyacheslav, Dolgireva Elena, Mokeeva Tatyana.....	93
STATIC ANALYSIS OF ANDROID-APPLICATIONS SECURITY Dremov Andrei, Pavlenko Evgeny	95
IMITATIVE MODELING OF HAZARDOUS EXPLOSIVE PROJECTION OF THE POPULATION PROCESS FOR THE INVASION TAXON Dubrovskaya Victoria, Perevaryukha Andrey, ...	96
DEVELOPMENT OF SECURE PROTOCOL FOR SECRET E-VOTING IN CREATIVITY COMPETITION Larisa Dmitrieva, Taisya Makarova	98
PROSPECTS OF USING THE CLASS OF TWO-MODULUS CODES WITH SUMMATION SYNTHESIS OF DISCRETE SYSTEMS WITH ERROR DETECTION Efanov Dmitry, Schagina Vladislava.....	100
USING MACHINE LEARNING FOR DETECTION OF MALICIOUS ANDROID-APPLICATION Ignatiev Gleb, Pavlenko Evgeny.....	101
PROBLEM STATEMENT OF DEVELOPING OF DATABASE SAFETY METRICS SYSTEM Maria Isaeva, Michael Gluharev	103

PROTECTION OF INFORMATION FROM HIDDEN THREATS IN THE ENVIRONMENT OF CLOUD COMPUTING Markov Vyacheslav, Sidorenko Tatiana	105
A METHOD FOR REDUCING THE OVERHEAD IN A PACKET DATA NETWORK Zaur Kurashev	106
DATA PROTECTION AND THE HUMAN FACTOR Kartashov Pavel	107
INFORMATION-TECHNICAL SUPPORT DISCIPLINES OF LINGUISTIC CYCLE Lidia Kolokolova	109
THE SOLUTION OF THE BASIC COMPUTATIONAL PROBLEM BY METHODS OF INTELLECTUAL DATA ANALYSIS Melnikov Aleksander, Narushev Ilya	111
HIERARCHICAL APPROACH TO DETECTING MALICIOUS SOFTWARE Moskvin Dmitry, Pavlenko Evgeny, Yarmak Anastasiya	112
ANALYSIS OF INFORMATION SECURITY MECHANISMS IN DECENTRALIZED SYSTEMS OF CLOUD DATA STORAGE Miasnikov Alexei, Moskvin Dmitrii	113
APPLICATION OF ALGORITHMS OF NEURAL NETWORKS AND MACHINE LEARNING TO THE DETECTION OF ANOMALOUS BEHAVIOR Narushev Ilya	115
SEMISTRUCTURED DATA IN INFORMATION SECURITY CHALLENGES Poltavtseva Maria Anatolevna, Pechenkin Alexander Igorevich	116
USING DIGITAL WATER MARKS IN THE GRAPHIC CONTENT OF MOBILE DEVICES Popov Boris	118
PROTECTION FROM ATTACKS BY METHODS OF SOCIAL ENGINEERING Solodyannikov Alexander, Sukhostat Valentina, Antonova Liubov	120
SPECIAL ASPECTS OF PROCESSING PERSONAL DATA IN THE PROCESS OF FUNCTIONING OF INDUSTRIAL COMPANY Solodyannikov Alexander	122
THE FACTORS OF INHERITANCE AND PROACTIVITY IN THE LIFE CYCLE OF THE INFORMATION SYSTEM Sokolov Boris Vladimirovich, Mustafin Nikolay Gabdrakhmanovich, Miller Vladimir Evgenjevich, Savosin Sergey Valentinovich	126
THE NETWORK SECURITY OF THE INTERNET OF THINGS MEANS OF LOW-RESOURCE CRYPTOGRAPHY Suprun Aleksandr, Tsarkov Igor	127
THE COMMUNICATION PROTOCOL WITHIN THE NETWORK OF THE INTERNET OF THINGS Suprun Aleksandr, Tsarkov Igor	128
CALCULATED THE QUESTION OF HOW EDUCATIONAL TECHNOLOGY IN E-LEARNING Titova Yuliayna Frantseva	129
THREATS AND PROTECTION MEASURES OF USING THE BYOD CONCEPT Usatykh Kseniia	130
DATA STRUCTURE OF TWO-SCALE DICHOTOMIC HIERARCHY FOR OBJECTS IN A COLOR IMAGE Kharinov Mikhail	132

MODELING OF FLAWS WITHIN A SECURITY SYSTEM Shipileva Alla	134
A SYSTEM APPROACH TO THE THEORY OF ART Yaroshevich Ludmila Ivanovna.....	135
SPECIFIC THREATS OF DATA BASE CONTROL SYSTEMS Borieva Anna	136
TESTING OF MODERN VIRTUAL DATA PROTECTION SOFTWARE Borodin Mihail, Borodina Polina.....	138
THE COMPLEXITY OF THE MANAGEMENT TASK AND NETWORK-CENTRIC Verzun Natalya, Kolbanev Mikhail	139
INFLUENCE OF PARAMETERS OF WIRELESS SENSOR NETWORK FOR ENERGY CONSUMPTION AUTONOMOUS SYSTEM OF ECOSYSTEM MONITORING Verzun Natalya, Kolbanev Mikhail, Kolbanev Aleksey	140
SECURE INFORMATION TECHNOLOGY FOR DESIGNING CORPORATE INFORMATION- MANAGEMENT SYSTEMS BASED ON THE USE OF THE UNIFIED MODELING LANGUAGE UML Dubenetsky Vladislav, Kuznetsov, Aleksandr, Tsehanovsky Vladislav.....	142
THE STRATEGY AND CULTURE OF THE SAFE USE OF AN ORIGINAL INFORMATION RESOURCE Shirokov Vladimir, Schigoleva Marina	143
BUILDING A PROGRAM GATEWAY FOR NETWORK INSULATION OF VIRTUAL MACHINES Zegzhda Petr, Nikolskiy Aleksey, Alekseev Iliia	144
PROTOCOL ANALYZERS FOR MONITORING DATA PACKETS BETWEEN NETWORK DEVICES Zorin Kirill, Guryanov Denis, Shigoleva Marina	146
MODEL OF CORRECTION FUNCTION STATE BASED ON THE TYPOLOGICAL FEATURES OF THE HUMAN OPERATOR IN THE FRAMEWORK OF IMPROVING THE INFORMATION-PSYCHO LOGICAL SECURITY OF THE INDIVIDUAL Sergey Kolmakov	147
THE THEORY OF THE CREATION OF A DISTRIBUTED SYSTEM FOR AUTOMATED DETECTION OF SOFTWARE VULNERABILITIES Krivonogov Sergey.....	149
COMPROMISE BETWEEN SECURITY AND USABILITY OF THE MODERN USER INTERFACES Leonov Anton.....	151
ABOUT THE PROBLEM OF FINDING NEW FINITE ASSOCIATIVE ALGEBRAS FOR CONSTRUCTING PUBLIC KEY CRYPTOSCHEMES Moldovyan Nikolay, Kovaleva Irina	152
CONSTRUCTION OF FINITE ALGEBRAS FOR IMPLEMENTATION OF POST-QUANTUM PROTOCOLS OF PROTECTIVE TRANSFORMATIONS OF INFORMATION Moldovyan Nikolay, Abrosimov Ivan.....	154
PROGRAM AND TECHNICAL ISSUES OF INFORMATION SECURITY FOR THE OPERATION PROBLEMS OF DDB Nechitailenko Roman, Novopashin Vladimir, Belyko Roman	156
USING THE ALGORITHM FIND A MINIMUM SPANNING TREE FOR VISUALIZATION THE IMAGES ARE PROTECTED FAULT-TOLERANT ENTERPRISE INFRASTRUCTURE Pelevin Maksym.....	157

ALGORITHM OF SELECTING THE OPTIMAL VARIANT OF THE INFORMATION SECURITY SYSTEM Popova Elena.....	158
DIGITAL SIGNATURES OF STRUCTURED DATA STORAGES Romanova Yuliya Nikolaevna, Yanyushkin Konstantin Aleksandrovich	159
THE BLOCKCHAIN FOR SECURITY PERIMETER GEOTAGGING Ryzhkov Sergey	161
NETWORK SECURITY AUDIT Sadikova Anastasia, Titova Yulia, Savkov Sergei	162
STEGANOGRAPHY AS AN ALTERNATIVE TO CRYPTOGRAPHY Sokolov Sergey Sergeevich, Revera Galina.....	164
INTEGRATED SYSTEM OF ENGINEERING AND TECHNICAL PROTECTION OF THE MANAGER'S OFFICE. THE EFFECTIVENESS OF THE WORK OF INFORMATION SECURITY DEVICES ON THE EXAMPLE OF AN INTEGRATED SYSTEM OF ENGINEERING AND TECHNICAL PROTECTION OF THE MANAGER'S OFFICE Fayazov Kobiljon Abdukayumovich	165
ANALYSIS OF THE MAIN TYPES OF TRAFFIC IN INFORMATIONTELECOMMUNICATION NETWORKS AND TO EVALUATE IT IS SENSITIVITY TO THE QUALITY OF SERVICE INDICATORS Vlasova Darya Nikolaevna, Baglay Valeria Vitalievna, Aparina Elena Yurievna.....	167
ANALYSIS OF PROBLEMS OF DEVELOPMENT OF ASU OF A SPECIAL PURPOSE Alexander Borisov, Vyacheslav Loginov, Aleksey Pimenov	169
PROTOCOL AND INFRASTRUCTURE OF THE INTERNET COMMUNICATIONS PROTECTION AGAINST MAN-IN-THE-MIDDLE ATTACK BASED ON THE REVOKED CERTIFICATES Alexey Busygin, Artem Konoplev, Dmitry Zegzhda	170
APPROACH TO COUNTERING COMPUTER ATTACKS ON CRITICAL INFORMATION SEGMENTS OF A SPECIAL PURPOSE NETWORK Vasyukov Dmitry Yuryevich, Smygin Alexander Mikhailovich Mitrofanov Mikhail Valerievich	171
PROTECTION OF INFORMATION IN THE SYSTEMS OF TRANSMISSION, STORAGE AND PROCESSING OF INFORMATION Volostnykh Viktor, Rogov Ruslan, Mitrofanov Mikhail	173
ENSURING INFORMATION SECURITY IN INDUSTRIAL INTERNET OF THINGS NETWORKS Dakhnovich Andrei, Dmitrii Moskvina	174
THE WAY OF PROTECTION OF RESOURCES OF A MULTISERVICE COMMUNICATION NETWORK Evgeny Zhuravel	176
SAFETY OF MANAGEMENT OF ROBOTIC SYSTEMS ON THE BASIS OF ARTIFICIAL INTELLIGENCE WITH APPLICATION OF NEURAL NETWORKS Ruslan Zakharov, Oleg Laut, Aleksandr Kribel, Dmitriy Soloviov.....	178
ROLE-BASED ACCESS CONTROL FOR VEHICULAR NETWORKS Kalinin Maxim, Evgenia Rezedinova	179
TWO-MOMENT APPROXIMATION METHOD APPLICATION SYSTEMATIC PROCEDURE FOR THE FUNCTION DETERMINATION OF STOCHASTIC NETWORK TIME DISTRIBUTION IMPLEMENTATION Kanaev Andrey., Karabanov Yuriy., Privalov Andrey	180
CRYPTOGRAPHIC PROTECTION OF A CONTROL PATH OF ROBOTIC SYSTEMS Mikhail Kocinyak, Mikhail Gudkov, Alexey Safonov, Boris Arutunyan.....	183

SSESSMENT METHODOLOGY OF INTEGRATED INFORMATION IMPACT OF INFORMATION AND TELECOMMUNICATION SYSTEMS SPECIAL PURPOSE Kocinac Michael, Yastrebov Vladimir, Klinshov Ilya, Gulevich Anton	184
TECHNIQUE OF FORECASTING OF LEGAL IMPACTS ON ROBOTIC SYSTEMS Mikhail Kocinyak, Vladislav Dementiev, Sergei Teslya, Oleg Lauts	185
PROBABILISTIC AND TIME CHARACTERISTICS OF THE ATTACKS TO ROBOTIC SYSTEMS Sergey Kuznetsov, Denis Ivanov, Maxim Vlasenko, Nikolay Latushko	186
THE APPROACH TO THE SECURITY ASSESSMENT OF INFORMATION-TELECOMMUNICATION NETWORKS OF SPECIAL PURPOSE FROM TECHNICAL COMPUTER INTELLIGENCE Lauts Oleg, Klinshov Ilya, Yastrebov Vladimir, Rusakov Yegor	187
SECURITY OF TELECOMMUNICATION NETWORKS BASED ON THE SELECTION OF PROTECTED INTERVALS WHEN JAMMING Mitrofanov Michael, Rakitskiy Stanislav, Chikov Dmitry	189
PROBLEMS OF PROTECTION OF INFORMATION AND TELECOMMUNICATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION AGAINST CYBER ATTACKS Moshak Nikolay Nikolaevich, Evseiko Konstantin Vladyslavovich	190
PROBLEMS OF INFORMATION SECURITY IN MOBILE DEVICES AND POSSIBLE WAYS OF THEIR SOLUTIONS Alexey Neizhnik	192
MODELS OF INTELLECTUAL INFLUENCES Aleksandr Nechepurenko, Artem Suetin, Ildar Murtazin, Oleg Lauts	193
CONTROL OF MULTI-OUTPUT LOGIC AUTOMATIC SCHEMES BASED ON THE METHOD OF A BOOLEAN COMPLEMENT ON CONSTANT WEIGHTS CODES Pivovarov Dmitry, Efanov Dmitry, Sapozhnikov Valery, Sapozhnikov Vladimir	195
COUNTERMEASURES TO UNAPPROVED UNMANNED DRONES ACCESS ON INSTITUTES Oleg Ostroumov, Umar Atigov, Daria Sotnikova	196
ENSURING INTEGRATED SAFETY OF ACTIVE EQUIPMENT OF CORPORATE NETWORKS Seregin Sergey Sergeevich, Gvozdkov Igor Vyacheslavovich	198
THE DESIGN METHOD OF SYSTEM ACCESS SECURITY AUTOMATIC INFORMATION SYSTEMS Fialkin Ilya	199
ENSEMBLES OF DISCRETE ORTHOGONAL SIGNALS OF COMPLEX STRUCTURE Sazonov Viktor, Bezubov Oleg, Mosyagin Dmitry	201
FEATURES OF FUNCTIONING OF SYSTEMS OF EXCHANGE OF ELECTRONIC CORRESPONDENCE VEDOMSTVENNAJA PURPOSE Sazonov Viktor, Salyahova Alia	202
A MODEL FOR DETERMINATION OF SECRECY COMMUNICATION SYSTEM Hudaynazarov Yuri, Maslov Oleg, Baraulya Igor	203
IMPLEMENTATION OF TELECOMMUNICATION SYSTEMS IN THE WORK OF THE POLICE Shalaginova Olga Borisovna	205
THE DESIGN METHOD OF SYSTEM ACCESS SECURITY Shtanenko Vasily, Baraulya Igor, Maslov Oleg	205
TECHNOLOGIES OF SAFETY IN THE BANK SPHERE FROM CYBER ATTACKS Abramova Kristina, Golubeva Maria	207

APPLICATIONS AROMOSENSOR SYSTEMS FOR SAFETY Dmitry Afanasiev, Elena Bardakova, Denis Bystryakov	209
FEATURES OF CONSTRUCTION OF SYSTEMS OF INFORMATION SECURITY OF STATE INFORMATION SYSTEMS.....	210
Volodin Anastasiya Andreevna, Levkin Igor Mikhailovich	210
ABOUT ALGORITHM PROCESSING SITUATION MODELS Golovkin Yury.....	212
ALGORITHM OF IOT SYSTEM SENSORS PLACEMENT Ivan Dzubenko	213
SOC AS INSTRUMENT OF MANAGEMENT OF INFORMATION SECURITY OF THE ENTERPRISE Natalia Demidova, Daniil Kolokolov	214
IMITATION MODEL OF INFORMATIONAL INTERACTION IN THE IOT NETWORK Elizarov Maksim	215
SECURITY IN CLOUD SERVICES Emelyanov Alexandr	217
SECURITY IN NETWORKS Emelyanov Alexandr	218
SOME ASPECTS OF SECURITY AT USING CRYPTOCURRENCY Kadyrova Assiya	220
ESTIMATION AND FORECASTING OF RISKS FOR INFORMATION SECURITY SYSTEMS Alexey Kapanov, Evgeny Meshcheryakov, Vladimir Kosolapov, Tatyana Astakhova	221
METADATA IN THE LONG-TERM STORAGE SYSTEMS Kolbanov Mikhail, Poimanova Ekaterina, Tatarnikova Tatiana	222
SECURITY SUBLEVEL OF ARCHITECTURAL MODEL OF DATA STORAGE Kolbanov Mikhail, Ipatov Oleg, Poimanova Ekaterina	224
ENERGY ASPECTS OF LONG-TERM DATA STORAGE SECURITY Kolbanov Mikhail, Kasatkin Viktor, Poimanova Ekaterina	225
ABOUT THE PARTICIPATION OF THE ECONOMIC UNIVERSITY IN THE TRAINING OF SPECIALISTS FOR THE CENTERS OF THE COMPETITIONS OF THE REGIONS Korshunov Igor, Levkin Igor, Mikadze Sergey	226
SECURITY OF THE ENTERPRISE IN CLOUD SYSTEM Kuznetsova Margarita	227
THE MAIN TYPES OF INTRUDERS WHO ARE ABLE TO CARRY OUT COMPETITIVE INTELLIGENCE AND HAVE IMPACTS ON THE INFORMATION Kulishkin Vitaliy, Chuikov Igor.....	228
INFORMATION AND ECONOMIC THREATS IN THE DIGITAL ECONOMY Levkin Igor Mikhailovich, Levkin Svetlana Vyacheslavovna.....	229
INFORMATION AND ECONOMIC SECURITY OF INFORMATION SYSTEMS DESIGN Lobanov Viacheslav, Sokolov Roman	231
INFORMATION SAFETY REQUIREMENTS FOR THE DEVELOPMENT OF GRADUATION WORK Maslov Nikita, Astakhova Tatyana.....	232

IRRATIONAL INFLUENCE OF INFORMATION FLOWS ON THE ECONOMIC SAFETY IN DIGITAL ECONOMY Minakov Vladimir, Lobanov Oleg, Sotavov Abakar	233
STRATEGY OF DEVELOPMENT OF INDUSTRIAL ENTERPRISE Mikhailov Nikolay	235
KPI-BASED MOTIVATION OF PERSONNEL Mikhailova Anna	236
INFORMATION SECURITY IN THE DIGITAL ECONOMY Romanova Anna, Astakhova Tatyana, Kolbanev Mikhail	236
METHODS OF SIMULATION OF THE SELF-SIMULATED TRAFFIC Tatiana Tatarnikova, Yakovlev Sergey	238
PROTECTED SYSTEM OF REMOTE PATIENTS MONITORING Anna Tatarnikova	240
THE METHOD OF DESIGNING GIS INFRASTRUCTURE SUPPORTING DECISION-MAKING AT THE MANAGEMENT OF SHIPS Natalia Yagotinceva	241
MODELS OF COOPERATION OF HIGH SCHOOLS AND IT COMPANIES IN THE FIELD OF SECURING INFORMATION SECURITY OF THE REGIONS OF RUSSIA IN THE CONDITIONS OF IMPORT REPLACEMENT OF THE SOFTWARE Abrahamyan Gennady	243
PARAMETRIC SYNTHESIS OF THE RADIOMONITORING SYSTEM BASED ON THE FORMAL APPROACH Alexey Gudkov, Sergey Malishev	246
THE PORTING OF THE OPERATING SYSTEM REAL-TIME «FREERTOS» IN THE HARDWARE MODULES, ARE BUILT ON THE BASIS OF PROCESSORS OF THE RUSSIAN COMPANY "ELVIS" Guk Igor, Pavlov Fedor	248
SELECTION IN THE HIERARCHICAL SYSTEMS OF SUBJECTS TO OBSERVATION AND ESTABLISHMENT OF THEIR ACCESSORY WITH APPLICATION OF THE ALGORITHM OF ASSESSMENT OF CHARACTERISTICS OF COHERENCE Kuzmin Vitaly, Udaltsov Nikolai	249
THE DEVELOPMENT OF IT-SECURITY MANAGEMENT SYSTEM FOR CRITICAL INDUSTRIAL OBJECT Livshitz Ilya, Malikov Vladimir	251
THE ANALYSIS OF REQUIREMENTS FOR ASSESSMENT OF CRITICAL OBJECTS BASED ON MODERN ISO STANDARDS Livshitz Ilya , Malikov Vladimir	253
ANALYSIS OF THE IMPACT OF RISK-BASED STANDARDS FOR IT-SECURITY PROVISION FOR AN CRITICAL INFRASTRUCTURE OBJECTS Livshitz Ilya, Malikov Vladimir	254
TELECOMMUNICATION TECHNOLOGIES IN CRITICAL INFRASTRUCTURES, THEIR DEVELOPMENT Mihailenko Evgeny	256
PROTOCOL ROUTING IN WIRELESS NETWORK Molokovich Igor	258
DATA EXCHANGE PROCEDURE CONTROL ALGORITHM INTO SELF-ORGANIZING HF RADIO NET Putilin Aleksey	259

MODERNIZATION METHOD INFORMATION SYSTEMS OF ENVIRONMENTAL MONITORING Ryabovaya Valentina	260
SOFTWARE MODEL OF DIGITAL COMMUNICATION IN SHORT WAVES RANGE WITH FREQUENCY-HOPPING SPREAD SPECTRUM Shaptala Vasily	261
NEXT GENERATION NETWORK TECHNOLOGIES AND THEIR APPLICATION FOR THE WATER TRANSPORT Andrey Alexeev, Anastasiya Erisova, Malov Sergey	263
USING OF COLOURED PETRI NETS AT THE MODELING OF THE ENTERPRISE SUBSYSTEMS Barashkov Alexander, Petrovskii Dmitrii	265
MODEL OF TRAFFIC FLOW Barikov Leonid, Galanina Valentina	266
COVERT AIR AUDIO DATA TRANSMISSION VIA DIGITAL WATERMARKED AUDIO SIGNALS Gofman Maksim, Kornienko Anatolij, Kustov Vladimir, Mironchikov Evgenij, Nikitin Aleksandr	267
METHOD OF RESTORING THE WIND PROFILE DUE TO SPECTER WIDTH ESTIMATION OF THE RADAR SIGNAL Denisenkov Dmitriy, Zhukov Vladimir, Shukin Georgiy	269
OPTIMAL THRUST ALLOCATION ALGORITHM FOR PROVIDING OF SAFETY DATA INTERACTION BETWEEN SUBSYSTEMS OF DYNAMICAL POSITIONING SYSTEM Zaitsev Aleksey, Azarov Michael	271
PARTICULAR QUALITIES OF CONSTRUCTION OF INFORMATION PROTECTION SYSTEM IN INTELLECTUAL THE CONTROL SYSTEM OF THE UNIFIED PARKING SPACE Zaytsev Svyatoslav, Ilchenko Lydia	272
THE PROTECTION OF CORPORATE INFORMATION IN THE TRANSPORT AND LOGISTICS NETWORKS Iskanderov Yury, Pautov Mikhail	275
THE PROVISION OF INFORMATION SECURITY OF OVERSIZE CARGO TRANSPORTATION Iskanderov Yury, Chumak Alexander	276
THE FORMATION OF THE SAFE KNOWLEDGE BASE OF THE INTELLIGENT SYSTEM OF DESIGNING ACS ON TRANSPORT Iskanderov Yury, Ershov Alexander	277
THE METHOD OF PROTECTION OF M2M NETWORKS AGAINST UNAVAILABILITY THREATS BY DYNAMIC ROUTING WITH ANT ALGORITHM Kalinin Maxim	278
CYBERSECURITY, AS AN INTEGRAL PART OF THE SECURITY SYSTEM OF THE SHIP Kardakova Mariia	279
MODELING AND INVESTIGATION OF SECURITY FEATURES OF MOVING SOFTWARE-DEFINED VANET/MANET NETWORKS IN SUPERCOMPUTER-BASED VIRTUAL ENVIRONMENT Krudyshev Vasily, Kalinin Maxim, Zegzhda Dmitry	280
SECURITY CONTROL AND MANAGEMENT SYSTEM IN INTER-CAR NETWORKS WITH TECHNOLOGY OF SOFTWARE-DEFINED NETWORKS Krudyshev Vasily, Kalinin Maxim	282
METHODS OF REENGINEERING WEBSITES IN THE PROBLEM OF OPTIMIZATION OF THE IT- ARCHITECTURE OF THE SCIENTIFIC RESEARCH ORGANIZATION Moskaleva Valeriia, Krivtsov Alexander	284

PROBLEMS OF FLIGHT SAFETY OF UNMANNED AIRCRAFT Rubtsov Evgeny	286
VEHICLE ROUTING FOR E-FULFILLMENT Kotliar Sofia, Krivtsov Aleksandr	288
FORMATION OF ELECTRONIC EDUCATIONAL TRAJECTORY AT TRAINING OF STAFF IN THE FIELD OF SECURITY OF INFORMATION SECURITY Anastasya Mitrofanova, Sergey Sokolov, Roman Novoselov	289
METHODS DATABASES OPTIMIZATION IN HIGHLOAD INFORMATION SYSTEMS ON TRANSPORT Roman Novoselov, Sergey Sokolov, Anastasya Mitrofanova	290
VULNERABILITY VOIP Polugina Julia	292
SAFE VOIP ATX Polugina Julia	293
THE APPLICATION OF STATISTICAL ANALYSIS METHODS FOR IDENTIFYING VERSIONS OF REMOTE AUTONOMOUS TRANSPORTATION SYSTEM OBJECTS Salakhutdinova Kseniya, Lebedev Ilya	294
DEVELOPMENT TEST OF TECHNOLOGY OF OTMA IN A SECURE EXECUTION PROGRAM FOR THE DEVELOPMENT OF OMTI Vladimir Aleksandrov, Anatoly Aleksee, Viktor Polyanichko, Sergei Khodan	296
ADAPTIVE PREDICTION ALGORITHM DEVELOPMENT IS-ENVIRONMENT, MARINE FACILITIES AND INFRASTRUCTURE Anatoly Alekseev, Roman, Musatenko, Valery Kiselyov	298
THE PROBLEM OF INTEGRATED SECURITY, OMTI AND ITS RESOLUTION BASED ON THE OPTIMAL INTEGRATION SOLUTIONS Anatoly Alekseev	300
THE PROBLEM OF SYSTEMATIZATION OF BEST PRACTICES AND BUILDING REQUIREMENTS FOR DEVELOPMENT OF SYSTEMS OF AUTOMATION AND LIFECYCLE MANAGEMENT OMTI IN A SECURE EXECUTION Anatoly Alekseev, Igor Tychinin, Roman Musatenko	302
THE CONCEPT OF INTER-OBJECT POLYGON NETWORK TECHNOLOGY MANAGEMENT AND SUPPORT EXCELLENCE IN THE INFOSPHERE Anatoly Alekseev, Paul Barabash, Valentine Zhigadlo, Igor Zikratov, Anatoly Dives	304
CONTROL SYSTEM FOR INFORMATION SURVIVABILITY OF A VESSEL ACCORDING TO THE REQUIREMENTS NBIS Anatoly Alekseev, Alexander Petrov	307
THE ISSUES OF INFORMATION SECURITY THIRD EDITION OF THE MONOGRAPH "AUTOMATION OF PROCESSES THE STRUGGLE FOR THE SURVIVAL OF THE SHIP, THE SHIP": A PRESENTATION OF THE PUBLICATION Anatoly Alekseev, Vladimir Polenin, Vasily Moskalenko, Roman Musatenko	309
THE PROBLEM OF CREATING AN IT MANAGEMENT STRUGGLE FOR SURVIVABILITY OF OMT IN A SECURE EXECUTION AND PROMISING WAYS OF THEIR SOLUTION Anatoly Alekseev, Sergei Solovyov, Ivan Boronenkov, Igor Turkin, Vasily Moskalenko, Roman Musatenko	311
INFORMATION SECURITY AND PROBLEMS OF QUALITY MANAGEMENT SYSTEM PRACTICAL TRAINING FACILITIES OF THE NAVY Elena Alekseeva, Alekseev, Sergei, Parfyonov, Nikolai	313

THE SECURITY OF PERSONAL DATA IN THE PROGNOSIS AND DIAGNOSIS OF THE QUALITY OF PRACTICAL TRAINING FACILITIES OF THE NAVY Elena Alekseeva, Alekseev, Sergei, Parfyonov, Nikolai	315
QUESTIONS OF TRAINING TRANSPORT SECURITIES Alimov Oleg Mihailovich.....	317
REGRESSION ANALYSIS OF THE DYNAMICS OF 10 YEARS OF HACKING AND INFORMATION INCIDENTS Antsiferov Alexander	319
POSSIBILITIES OF REMOTE DIAGNOSTICS ON BOARD A SHIP Nataliya Barkova, Alexey Barkov, Dmitriy Grishchenko, Vladimir Fedorishchev	320
ANALYSIS OF VULNERABILITY OF SERVICES AUTHORIZATION AND POSSIBILITIES OF THEIR IMPROVEMENT Aleksandra Biryukova	322
ANALYSIS OF MODELS ASSESSING THE COMPETITIVE ABILITY OF OMTI IN A SECURE EXECUTION Vladimir Bobrovych, Anatoly Alekseev, Vasily Antipov, Alexander Smolnikov	323
MODERN APPROACH TO ENSURING INFORMATION SECURITY OF DATA OF CLINICAL TRIALS OF MEDICINAL DRUGS Timur Galimov, Rodion Sukhov, Sania Shavinskaya	325
ARCHITECTURE, COMPOSITION AND REQUIREMENTS FOR THE INTEGRATED INFORMATION SECURITY SYSTEM OF THE OMTI Dominova Tatyana	326
VERBAL STRUCTURAL-FUNCTIONAL MODEL OF ADAPTATION SYSTEM TECHNOLOGY DECISION SUPPORT AND MANAGEMENT IN THE PROTECTED EXECUTION FOR MISSION-CRITICAL NAVY Kagansky Mikhail	327
PROPOSALS IN A GENERALIZED MODEL OF THE INTEGRATED SYSTEM THE DECISION SUPPORT OF THE NAVY IN A SECURE EXECUTION Kagansky Mikhail	330
USE OF A SPECIAL COMPUTER ANALYTICAL SIMULATOR (SCAS) "BARS" FOR PRACTICAL SKILLS TO ENSURE NUCLEAR AND RADIATION SAFETY DURING OPERATION OF NUCLEAR POWER PLANT BY CREWS OF SHIPS AND SUMARINES Vladimir Kalenikhin, Alexandr Leberyanskiy, Alexandr Salazhenk.....	332
INFORMATION SECURITY IN THE MARITIME SECTOR OF THE EUROPEAN UNION Kolesnikova Marina.....	333
QUESTION OF THE INCREASE INFORMATION THE QUALITY OF THE MARINE FACILITY Kruzhilin Roman Vyacheslavovich.....	335
SERVICES, TECHNOLOGIES, VULNERABILITIES, THREATS AND PROTECTION OF BLUETOOTH Kuznetsova Nina	336
DIGITAL SIGNATURE Lavrenova Anna	337
THE FEATURES OF THE DEVELOPMENT OF INFORMATION SUPPORT SYSTEMS OF FIGHT FOR SURVIVABILITY OF SUBMARINE WITH THE INFORMATION SECURITY REQUIREMENTS Levoeva Inga, Mudrova Alena	338
SECURITY MAINTANANCE OF OPERATION OF TECHNICAL EQUIPMENT OF THE NAVAL SHIPS Vasily Moskalenko, Dmitriy Kovalenko, Nikolay Kalyuta	339

MONITORING AND MANAGEMENT OF INTEGRATED MARITIME SECURITY Panteleikin Sergey	341
SOCIAL NETWORK ON THE INTERNET Parkhatskiy Dmitriy	342
BASES OF THE TECHNIQUE OF CREATION OF THE MODELS OF STRUCTURAL AND DIFFICULT TECHNICAL SYSTEMS VISUALIZED BY LOGIKO-VEROYATNOSTNYH Vladimir Polunin, Sushchenkov Dmitry Andreevich	343
PROBLEMS OF AGGREGATION AND INTEGRATION OF ACS IN A SECURE EXECUTION Sergey Sogonov, Anatoly Alekseev, Oleg Khrutsky, Alexander Ravin	345
SYSTEM OF INFORMATION SUPPORT OF THE OPERATOR OF THE POWER PLANT Oleg Khrutsky, Anatoly Alekseev, Sogonov Sergey	347
INTELLIGENT DECISION SUPPORT ADMINISTRATOR IB MODEL FRTO Egor Archers	349
ORGANIZATIONAL-METHODICAL PROVISION OF FORMATION AND DEVELOPMENT OF PSPS AS A LABORATORY AND CENTER OF FORMATION OF THE MODERN IS-COMPETENCES Ivan Tyurin, Nikita Razzhivin, Daria Zhulanova	350
COMPOSITION AND REQUIREMENTS TO THE MONITORING AND SAFETY MANAGEMENT SYSTEM OMTI Victoria Tiurina, Ivan Tiurin	352
INTELLECTUAL SUPPORT FOR ADMINISTRATOR'S ACCEPTANCE OF TYPICAL OMS Tiurin Ivan	354
VULNERABILITY ASSESSMENT AND COMPARISON OF METHODS OF PROTECTION OF WEB APPLICATIONS Usbekova Julia	355
MULTIMEDIA TECHNOLOGIES IN PRESERVATION OF CULTURAL HERITAGE Pavel Barabash, Tatiana Lashenko	357
MANIPULATION WITH CONSCIOUSNESS IN THE "COLORED REVOLUTIONS": SYSTEM ANALYSIS APPROACH Andrey Boreiko	360
THE APPLICATION OF NETWORK-CENTRIC MANAGEMENT CONCEPT IN A DIGITAL SOCIETY Verzun Natalya, Kolbanev Mikhail, Yakovlev Sergey	362
DATA PROTECTION AND THE HUMAN FACTOR Kartashov Pavel	364
THE FEATURES OF INFORMATION-PSYCHOLOGICAL INFLUENCE ON THE INTERNET Levkin Igor, Ksenia Naumenko, Lidia Vitkova	366
INFORMATION POTENTIAL OF THE FEDERAL SUBJECT OF RUSSIA AND THE SITUATION CENTER AS A TOOL FOR MANAGING INFORMATION POTENTIAL Malmberg Sergei	367
ORGANIZATION OF EMPLOYEE PROTECTION FROM SOCIAL ENGINEERING ATTACKS Solodyannikov Alexander, Sukhostat Valentina, Antonova Liubov	369
WHAT IS SOCIAL ENGINEERING Khairullov Artem, Gallyamova Milyausha	371

USING MATHEMATICAL MODELS IN THE ASSESMENT OF THE EFFICIENCY WORK OF OIL WELLS Anastasiya Virstyuk, Viktoria Mikshina	373
INFORMATION SECURITY IN THE ARCTIC REGION Golubeva Maria. Abramova Kristina	375
ALTERNATIVE CONCEPTION OF INTEGRAL SYSTEM OF SITUATION MONITORING IN ARCTIC FOR SECURITY LIFE-SUPPORT PROVIDING Zimin Nikolay, Mitko Arseniy	377
EVALUATION OF THE INTERNAL SYSTEM ELECTROMAGNETIC COMPATIBILITY OF THE RADIOCOMMUNICATION WITH CODE DIVISION MULTIPLE ACCESS Kryachko Alexander, Antonov Kirill	379
PROBLEMS OF INFORMATION SECURITY IN ARCTIC PROVIDING Mitko Valery	380
MODEL OF STRATEGIC STATE SUSTAINABILITY IN ARCTIC EVALUATION Polenin Vladimir , Mitko Valery	382
ENSURING THE PRIVACY AND INTEGRITY OF DATA TRANSMITTED BY UNMANNED AERIAL VEHICLES IN ARCTIC REGION Shkorkina Elena, Alexandrova Elena	383
COMPILATION OF THE SPATIAL MODEL AND THE FORECAST MAP OF THE SITE DOLGAYA – LAKE GREAT PEAT Akhmetshina Anastasia	386
ECOLOGICAL SAFETY OF WATER AREA OF THE NEVA RIVER ASSOCIATED WITH OIL SPILLS Binenko Victor, Rodionov Vladimir	387
THE CONTRIBUTION OF METHANE IN AIR POLLUTION OVER THE CITY OF ST. PETERSBURG Binenko, Victor, Severyukhina Anastasia	388
ASSESSMENT OF ENVIRONMENTAL RISKS AT THE RECONSTRUCTION OF THE FIELD IN THE ARCTIC ZONE OF THE RUSSIAN FEDERATION Bykovskaia Elena, Kustikova Marina, Sausiaris Edgaras, Maiurova Aleksnadra	389
AUTOMATED INFORMATION-MEASURING SYSTEM FOR CONTROL OF THE COMPOSITION OF DISINFECTANTS CONTAINING POLYGEXAMETHYLENGUANIDINE Vasilevsky Aleksandr, Gerasimov Vladimir, Konoplev Georgii, Kostrin Dmitrii, Stepanova Oksana, Ukhov Andrey	390
SPATIAL DYNAMIC MODEL OF THE REGIONAL LEVEL OF THE LAKE KRASNOYE SURROUNDINGS Vorontsova Ekaterina	392
DEVELOPMENT OF THE SPATIAL DYNAMIC MODEL: ECOLOGO-ECONOMIC MODEL OF THE CARD OF WOOD RESERVES Gerasimov Konstantin Romanovich, Khvorostovskiy Artemiy, Kravtsov Ilya	393
COGNITIVE MONITORING OF EXTREME STATES IN MULTIDIMENSIONAL TIME DATA RANGES ON NATURAL SYSTEMS Gorokhov Vladimir, Buznikov Anatoli, Vitkovskiy Vladimir	394
COGNITIVE DETECTION OF ANOMALIES AND INVASIONS IN MULTIDIMENSIONAL TIME RANGE OF HYDROLOGICAL MONITORING DATA OF WELLS Gorokhov Vladimir, Buznikov Anatoli	395

STRUCTURE OF DOLGOE-PODSEKIRNOE INTER-LAKES ECOSYSTEMS AS THE TOPOLOGICAL LEVEL Kuvardina Mariya	396
USING DIGITAL SIGNAL AND IMAGE PROCESSING METHODS IN VIBRODIAGNOSTIC EXPRESS OBJECTS ON FACILITIES Malyshev Gregory, Grishkanich Alexander, Loktaev Kirill	397
REPRESENTATION OF AIR MONITORING OPEN DATA FOR RAISING PUBLIC AWARENESS OF ENVIRONMENTAL STATE ISSUES Matelenok Igor, Melentyev Vladimir	399
CREATION OF THE STRUCTURAL-DYNAMIC MODEL OF TYPES OF AREAS OF TERRITORY AND PREDICTIVE THEMATIC MAP OF DISTRIBUTION OF FORESTS BY CLASSES OF SOIL MOISTURE ON THE EXAMPLE OF THE CENTRAL-SOUTHWEST PART OF SOLOVETSKY ISLAND Nosova Anastasiia	400
INFORMATION AND ECOLOGICAL SECURITY OF ENVIRONMENT Pavlova Svetlana Michailovna	401
STRUCTURAL MODEL OF THE SOUTHERN PART OF THE GREAT SOLOVETSKY ISLAND Pozdniakova Viktoriia	403
MODEL FOR COMPLEX ASSESSMENT OF ENVIRONMENTAL DAMAGE FROM BRAWNFIELDS Romanjuk Ludmila, Petukhov Valery	404
THE USE OF DRONES FOR INFORMATION SUPPLY OF ECOLOGICAL SAFETY ACTIVITIES, LAW ENFORCEMENT AGENCIES AND BRANCHES OF THE RUSSIAN ECONOMY Timoshchuk Aleksandr, Doronin Aleksandr, Kalustov Yaroslav	405
ECOLOGICAL AND INFORMATION SECURITY OF THERMAL AERIAL MONITORING OF SAINT PETERSBURG Shilin Boris	406
MODERN OF MEDIUM PLAN Yaroshevich Ludmila Ivanovna	407
APPROACH TO THE CONSTRUCTION OF THE DETERMINING DIAGNOSTIC SYSTEM OF PERSONNEL VULNERABILITY TO SOCIAL ENGINEERING ATTACKS Abramov Maksim	409
CONSTRUCTION OF THE STRATEGY FOR THE PROTECTION OF USERS OF INFORMATION SYSTEMS FROM THE SOCIAL ENGINEERING ATTACKS Artur Azarov, Khlobystova Anastasia	410
SOCIAL NETWORK PROFILES ANALYSIS IN THE CONTEXT OF SOCIO-ENGINEERING ATTACKS Bagretsov Georgiy	411
CONDITIONS OF INFORMATION SECURITY IN THE CLINICAL SPHERE HEALTH SYSTEMS Blum Vladislav	412
APPROACH TO THE BUILDING OF THE ATTACKER COMPETENCIES PROFILE IN THE PROBLEM OF THE PROTECTION OF THE INFORMATION SYSTEM FROM SOCIAL ENGINEERING ATTACKS Bushmelev Fedor, Abramov Maksim	413
USING DATA MINING METHODS FOR OBTAINING INFORMATION ABOUT USERS IN SOCIAL NETWORKS Zegzhda Dmitry, Lemets Andrey, Pavlenko Evgeny	415

SYNTHESIS OF ALGEBRAIC BAYESIAN NETWORK TERTIARY STRUCTURE BASED ON SECONDARY STRUCTURE DIRECTED GRAPH Zolotin Andrey	417
MATHEMATICAL MODELING OF RESONATORS PROVIDING PROTECTION AGAINST ELECTROMAGNETIC RADIATION Alexander Kopyltsov	418
SAFETY ESTIMATION ALGORITHM THE ARRIVING WEAKLY FORMALIZED INFORMATION Anton Kopyltsov	420
USE OF NEURAL NETWORK FOR DETECTION AUTOMATICALLY CONTROLLED ACCOUNTS IN SOCIAL NETWORKS Malyshev Egor, Pavlenko Evgeniy, Zegzhda Peter	422
LOCAL PROBABILISTIC-LOGIC INFERENCE SENSITIVITY ANALYSIS IN MATHEMATICAL LIBRARY ALGBN MATH LIBRARY Malchevskaya Ekaterina	423
LANGUAGE PROBLEMS OF INFORMATION SECURITY Mikoni Stanislav	424
CONSTRUCTING USER'S VULNERABILITIES PROFILE ON THE BASIS OF INFORMATION EXTRACTED FROM SOCIAL NETWORKS Slezkin Nikita, Artur Azarov	426
AUTOMATED INTER-EPISEDE INTERVAL LENGTH DATA RETRIEVAL FROM DATABASE FOR LAST EPISEDES QUESTIONNAIRE Stoliarova Valeriia	428
IMPERCISION OF RESPONSES MODELING IN THE BAYESIAN BELIEF NETWORK FOR RESPONDENT'S SOCIALLY SIGNIFICANT BEHAVIOR ESTIMATION Suvorova Alena, Akulshina Olga	429
TEXT ANALYSIS OF PUBLICATIONS ON SOCIAL NETWORKING SITE AS THE BASIS FOR USER'S PSYCHOLOGICAL PROFILE Suvorova Alena, Tulupyeva Tatiana	430
CONSTRUCTION OF THE SOCIAL GRAPH OF THE COMPANY'S EMPLOYEES ON THE BASIS OF INFORMATION RECEIVED FROM SOCIAL NETWORKS TO CALCULATE THE PROBABILITY OF SUCCESS OF THE SOCIAL-ENGINEERING ATTACK Suleimanov Aleksei, Tulupyeva Tatiana, Tulupyevev Alexander	432
SYNTHESIS OF A SOCIALLY SIGNIFICANT BEHAVIOR MODEL AS A BAYESIAN BELIEF NETWORK WITH HIDDEN VARIABLES Toropova Aleksandra	433
ALGEBRAICAL BAYESIAN NETWORKS AS A TOOL FOR STATISTICAL AND EXPERT INFORMATION AGGREGATION FOR SOCIAL COMPUTING APPLICATIONS Tulupyevev Alexander	434
EXPRESS DIAGNOSTICS OF PERSONAL TRAITS BY DIGITAL TRACKS Ivanov Oleg, Petrov Sergey	435
ALGORITHMS FOR CHECKING CONSISTENCY IN ALGEBRAIC BAYESIAN NETWORKS IN LIBRARY ALGBN MATH LIBRARY Kharitonov Nikita	436
RESEARCH OF ERP SECURE PROGRAMS CREATION Bezhan Roman, Medvedev Mikhail, Sergey Arustamov	438

CONDITIONS OF INFORMATION SECURITY IN THE CLINICAL SPHERE HEALTH SYSTEMS Blum Vladislav	439
PROTECTION OF CONFIDENTIAL INFORMATION IN AUTOMATED MULTI-LEVEL SYSTEM Bondarenko Igor, Shimanchuk Sergey	440
INCREASING THE PROTECTION OF INFORMATION FROM UNAUTHORIZED ACCESS USING BIOMETRIC AUTHENTICATION Bragina Elizaveta, Egorov Ilia	442
DEVELOPMENT OF HARDWARE AND SOFTWARE IDENTIFY THE STATE OF OBJECTS AND SUBJECTS WITH APPLICATION OF TECHNOLOGIES OF INTERNET OF THINGS Dikii Dmitrii, Artemeva Viktoriia	444
SECURITY MANAGEMENT OF CYBER-PHYSICAL SYSTEMS BASED ON HOMEOSTAT Zegzhda Petr, Zegzhda Dmitry, Pavlenko Evgeny	445
SOCIAL ENGINEERING. PHISHING AND METHODS OF COUNTERING IT Ilchenko Lydia, Uvarov Roman, Zaytsev Svyatoslav	446
MODERN NEURAL NETWORK METHODS OF INTRUSION DETECTION IN VANET/FANET/MARINET Kalinin Maxim, Zegzhda Peter	449
ASYMMETRY OF TIME IN THE THEORY OF FORECASTING THE STATE OF COMPLEX DYNAMICAL SYSTEMS Vladislav Ostreykovsky, Tatyana Denisova, Elena Shevchenko, Surgut State University	450
IMPORT-SUBSTITUTION SOFTWARE IN THE PRACTICE OF ACCEPTING TESTING FOR MACHINE-BUILDING PRODUCTS Pervukhina Elena, Osipov Konstantin, Timofeev Iliya	451
METHODS OF DATA EXTRACTION FROM ISOLATED MACHINES Romanov Alexander	452
METHODS AND TOOLS OF THE AUDIT OF NETWORK SECURITY Sadikova Anastasia, Titova Yulia, Savkov Sergei	454
INCREASE OF ACCURACY OF STEGOANALYSIS METHODS BY OPTIMIZING PARAMETERS OF WAVELET-TRANSFORMATION Sivachev Alexey, Mikhailichenko Olga	455
THE PROBLEM OF ANONYMITY IN THE INTERNET NETWORK COMPARISON OF METHODS OF USER ANONYMIZATION Titova Yulia, Sadikova Anastasia, Savkov Sergei	457
STUDY OF THE X-PACE PROTOCOL Shenets N, Trukhina E	458
ISOGENY-BASED GROUP SIGNATURE Shtyrkina Anna, Yarmak Anastasiya, Aleksandrovna Elena	459
MULTIMEDIA EDUCATIONAL TECHNOLOGIES: PROBLEMS OF CREATION AND USE Pavel Barabash, Tatiana Lashenko	462
LABORATORY PRACTICUM ON EDUCATIONAL DISCIPLINE "SECURITY OF INFORMATION SYSTEMS" Barabash Pavel, Panasenko Mikhail	466

SIMULATION TRAINING SIMULATOR TO ENSURE THE SAFE OPERATION OF GEOGRAPHIC INFORMATION SYSTEMS Bogdanov Timur, Yashin Alexander	467
A STUDY OF THE QUALITY OF EDUCATION IN THE TRAINING OF PERSONNEL IN THE FIELD OF ENSURING INFORMATION AND ECONOMIC SECURITY Bolshakova Lyudmila, Kuzmina Kristina, Yakovleva Natalia	469
ABOUT NECESSITY OF PREPARATION AND RETRAINING OF QUALIFIED PERSONS IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY Burlov Vyacheslav, Grachev Mikhail, Primakin Alexey	470
NETWORK-CENTRIC – INFORMATION-TECHNOLOGY-BASED DIGITAL SOCIETY Verzun Natalya, Kolbanev Mikhail, Kasatkin Victor	472
DEVELOPMENT OF THE PRINCIPLES OF BUILDING TELECOMMUNICATION NETWORKS Verzun Natalya, Kolbanev Mikhail, Ipatov Oleg.....	474
A GENERALIZED MODEL OF ACTIVITIES IN A DIGITAL SOCIETY Verzun Natalya, Kolbanev Mikhail, Cehanovsky Vladislav.....	476
PERSONAL INFORMATION TRANSMISSION SPECIFIC IN THE MODULAR E-LEARNING INFORMATION SYSTEM Zhuravlev Anton	477
FORMATION AND USE IN THE EDUCATIONAL PROCESS OF THE SITUATIONAL CENTER FOR BUSINESS INTELLIGENCE Levkin Igor, Mikadze Sergey.....	479
TO THE QUESTION OF Training OF DEVELOPERS for THE Advanced National SOFTWARE Pervukhia Elena, Shalimova Elena.....	481
TO THE QUESTION OF TRAINING FOR THE DIGITAL ECONOMY OF THE RUSSIAN FEDERATION Rezunkov Dimitry, Imanov Geidar, Rezunkova Olga	482
APPROACH TO MODERNIZATION OF MULTILEVEL SYSTEM OF THE HIGHER EDUCATION IN RUSSIA IN THE CONDITIONS OF MODERN INTERNAL AND EXTERNAL THREATS Boris Sovetov, Victor Kasatkin.....	486
MODERN THREATS TO DEVELOPMENT OF THE RUSSIAN EDUCATIONAL SYSTEM Boris Sovetov, Victor Kasatkin.....	487
THE METHODS OF QUALITY IMPROVEMENT SPECIALIST OF INFORMATION SECURITY Sokolov Sergey Sergeevich.....	489
THE STUDY OF ACCESS CONTROL METHODS IN BETVOYAGERCASINO "OPERATING SYSTEMS" SPECIALTY "COMPUTER SECURITY" Shirokov Vladimir, Schigoleva Marina	490
THE STRATEGY OF DEVELOPMENT OF THE SMART INFORMATION SOCIETY Barikov Leonid, Ignatyev Mikhail	492
SIMULATION OF THE HUMAN BODY TO SUPPORT MEDICAL DECISIONS Gubin Alexander, Ignatiev Mikhail, Katerina Tatiana , Krasnikov Andrey	493
THE QUESTION OF THE CREATION OF THE NEW BUILDING OF THE MUSEUM OF DEFENSE AND BLOCKADE OF LENINGRAD Ignatyev Mikhail , Makin Alexey,Mimosin Michael, Nikitin Alexander, Fadeeva Nina	493

MODEL INFORMATION OF THE THREAT DATABASES, CRM-SYSTEMS AND METHODS OF PROTECTION AGAINST THEM Repina Valeria	494
STRATEGIES OF INFORMATION TECHNOLOGIES DEVELOPMENT IN REGIONAL ECONOMIC SYSTEMS, BASED ON DIFFERENT TYPES OF REACTIONS TO THE CHALLENGES OF THE EXTERNAL ENVIRONMENT Titovets Alisa.....	496
INVESTIGATION OF THE POSSIBILITY OF INVESTMENT OF THE DIGITAL WATER SIGN IN THE BYTE CODE BY REPLACING THE VARIABLE BYTE CODE JAVA CLASS Sharikov Pavel, Krasov Andrey	499
CONSTRUCTION OF THE INFORMATION-MONITORING SYSTEM OF AROMA-SAFETY ON HARDWARE AND SOFTWARE Antonov Valery.....	501
APPLICATION OF MACHINE LEARNING IN DEEP TRAFFIC ANALYSIS Ekaterina Alexandrovna.....	502
ENSURING INFORMATION SAFETY OF AUTOMATED SYSTEMS OF TECHNOLOGICAL PROCESS CONTROL Bondareva Anastasia, Goman Elena.....	504
METHOD OF PROTECTING INFORMATION AS DIGITAL STEGANOGRAPHY GallyamovaMilyausha.....	505
COMPARATIVE ANALYSIS OF FINANCIAL TRANSACTIONS SECURITY USING CONTACTLESS PAYMENT TECHNOLOGIES Ganchikova Yulia, Kuryshcheva Alena.....	507
TECHNIQUES AND STRATEGIES FOR ALERTING THE PUBLIC ABOUT THE THREATS OF CRISIS SITUATIONS Veronika Geraskina, Dmitry Saharov, Igor Pestov, Lidiya Vitkova.....	508
THE CONVERGENCE OF INFORMATION TECHNOLOGIES FOR INCREASE OF EFFICIENCY OF MANAGEMENT OF THE INFORMATION SPACE OF ST. PETERSBURG Ul'ia Golovleva, Lidiya Vitkova, Maksim Kovcur, Ekaterina Dmitrieva	510
SECURING THE PYTHON APPLICATION WEB SERVER FOR DEPLOYMENT ON CLIENT MACHINES Gribachev Vitaliy, Kharitonov Georgiy	512
PROSPECTS OF ONE-TIME PAD USAGE FOR PROTECTION OF UNMANNED AERIAL VEHICLE DATA STREAMS Grozov Vladimir	514
ANALYSIS OF INFORMATION SECURITY PROTOCOLS IN IOT-ENVIRONMENT Dolgun Vladislav, Litvinov Vladislav	515
PARTICULAR QUALITIES OF CONSTRUCTION OF INFORMATION PROTECTION SYSTEM IN INTELLECTUAL SYSTEMS OF GROUND CITY PASSENGER TRANSPORT Ilchenko Lydia, Zaytsev Svyatoslav	517
USE OF INFORMATION TECHNOLOGIES IN TRAINING CHEMISTRY Daniil Kolokolov	519
SAFETY PROBLEMS OF CLOUD COMPUTING Krasov Andrey, Levin Mark, Fostach Elena.....	521
ANALYSIS OF ERP-SYSTEMS SECURITY. GENERAL APPROACH TO ANALYSIS Krivdyuk Nadezhda.....	522

ANALYSIS OF EXISTING SENSORS FOR DETECTING THE ATTEMPTS OF UNAUTHORIZED ACCESS TO PROTECTED INFORMATION Lisetskaya Kristina	524
APPLICATION OF NEURAL NETWORKS IN THE FIELD OF INFORMATION SECURITY Orlov Ivan	525
INNOVATION OF THE LIFE CYCLE OF PROTECTED SERVICE-ORIENTED SYSTEMS FOR THE DIGITAL ECONOMY Ptitsyna Larisa, Nezhinsky Vitaliy	526
DISTRIBUTED MODEL ANALYTICAL INTELLIGENCE OF INTEGRATED SYSTEMS OF INFORMATION PROTECTION Ptitsyna Larisa, Gusev Dmitry	528
ANALYSIS OF MODERN THREATS OF INFORMATION SECURITY AND METHODS OF PENETRATION IN THE COMPUTER SYSTEM Lukin Evgeny, Prokopovich Maxim, Fedorov Dmitry	530
ACCESS CONTROL AND MONITORING SYSTEM, FOR EXAMPLE, A HIGHER EDUCATION INSTITUTION Sazonov Anton ,Nemchenko Aleksey	531
FORMALIZED APPROACH TO THE ANALYSIS OF AUTHENTICATION PROTOCOLS Utkina Alena, Yurkin Dmitry	532
PRELIMINARY PROCESSING OF GRAPHIC OBJECTS FOR IDENTIFICATION IN THE VIDEO SEQUENCE Shevchenko Denis	534
A STUDY OF THE EXISTING IT INFRASTRUCTURE FOR FUTURE TRANSITION TO CLOUD ARCHITECTURE Mihail Chmutov, Maksim Kovcur, Igor Ushakov, Igor Pestov	535
THE LAW OF PRESERVING THE INTEGRITY OF THE OBJECT IN THE CONDITIONS OF DESTRUCTION OF SOFTWARE HARDWARE Mokeyeva Tatiana, Dolgireva Elena, professor Burlov Viacheslav	538