НБ

НАЦРАЗВИТИЕ

НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ РОССИИ: АКТУАЛЬНЫЕ АСПЕКТЫ

Материалы Всероссийской научно-практической конференции

NATSRAZVITIE
Saint Petersburg

ГУМАНИТАРНЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ИНСТИТУТ «НАЦРАЗВИТИЕ»

МАТЕРИАЛЫ
ВСЕРОССИЙСКОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ
«НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ РОССИИ:
АКТУАЛЬНЫЕ АСПЕКТЫ»

МАЙ 2020

Сборник избранных статей

Рекомендовано к публикации
редакционно-издательским советом
ГНИИ «НАЦРАЗВИТИЕ»
Протокол № 113 от 14.06.20

Санкт-Петербург
2020

ББК 72
М 34
DOI 10.37539/NB185.2020.78.94.001

Национальная безопасность России: актуальные аспекты: сборник избранных статей Всероссийской научно-практической конференции (Санкт-Петербург, Май 2020). – СПб.: ГНИИ «Нацразвитие», 2020. – 106 с.

ISBN 978-5-6044176-9-0

В материалах конференции публикуются избранные научные работы участников.

Материалы Всероссийской научно-практической конференции «Национальная безопасность России: актуальные аспекты» адресованы руководителям и специалистам государственных и негосударственных организаций, научным работникам и преподавателям, аспирантам, студентам.

В сборник вошли избранные статьи, рекомендованные к публикации редакционно-издательским советом ГНИИ «Нацразвитие».

Издание адресовано научным и педагогическим работникам научных и производственных организаций, учебных заведений.

Научное издание

Сборник издается без редакторских правок.
Ответственность за содержание статей возлагается на авторов.

МАТЕРИАЛЫ КОНФЕРЕНЦИЙ ГНИИ «НАЦРАЗВИТИЕ».
МАЙ 2020
Сборник избранных статей

Выпускающий редактор Ю.Ф. Эльзессер
Ответственный за выпуск Л.А. Павлов
Подписано в печать с оригинал-макета 20.06.2020.
Формат 60x84/16. Печать цифровая
Гарнитура Times New Roman. Усл. печ. л. 6,3.
Тираж 100 экз. Заказ № 42127.
Гуманитарный национальный исследовательский институт «Нацразвитие»
197348, Санкт-Петербург, Коломяжский пр., д. 18, лит. А, офис 5-114

Всероссийская научно-практическая конференция
"НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ РОССИИ:
АКТУАЛЬНЫЕ АСПЕКТЫ"

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ЗАЩИТА ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

КИБРБЕЗОПАСНОСТЬ И КИБЕРПРЕСТУПНОСТЬ

ВОПРОСЫ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ

ЭКОНОМИЧЕСКИЕ АСПЕКТЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

УДК 003.26
DOI 10.37539/NB185.2020.45.58.011

Губарева Елена Николаевна, ФГБОУ ВО «Самарский государственный экономический университет», г. Самара
Gubareva Elena Nikolaevna, Samara State University of Economics, Samara

Чуракова Екатерина Николаевна, кандидат юридических наук, доцент кафедры гражданского и арбитражного процесса, ФГБОУ ВО «Самарский государственный экономический университет», г. Самара
Churakova Ekaterina Nikolaevna, Samara State University of Economics, Samara

ЗАЩИТА ЭЛЕКТРОННОЙ ПОДПИСИ ОТ ФАЛЬСИФИКАЦИИ
ELECTRONIC SIGNATURE PROTECTION AGAINST FALSIFICATION

Аннотация: в данной статье авторы рассматривают преимущества и недостатки электронной подписи, её виды и их применение для различных задач документооборота. Особое внимание обращается на безопасность использования электронной подписи, рассмотрены виды мошенничества в электронном документообороте, а также названы способы, с помощью которых можно снизить к минимуму возможность фальсификации ЭЦП.

Abstract: in this article, the authors consider the advantages and disadvantages of electronic signatures, its types and their application for various workflow tasks. Particular attention is paid to the safety of using electronic signatures, the types of fraud in electronic document management are examined, and the ways by which you can minimize the possibility of falsification of digital signatures are described.

Ключевые слова: электронный документооборот, электронная цифровая подпись, криптографическая защита, квалифицированная электронная подпись, простая электронная подпись, фальсификация электронной подписи.

Keywords: electronic document management, electronic digital signature, cryptographic protection, qualified electronic signature, simple electronic signature, falsification of electronic signature.

В настоящее время в условиях активной глобализации все большее значение приобретает стремительное развитие информационных технологий, что неизбежно ведет к изменению экономических, правовых, общественных и других отношений, в которых появляются новые институты и явления такие, например, как электронный документооборот и цифровая подпись. Так электронный документооборот по сравнению с традиционным бумажным обладает несомненными преимуществами, такими как быстрота передачи информации, заключения сделок, внесения изменений в документ. Для того, чтобы идентифицировать личность, подписывающую документ и вносящую изменения, существует электронная подпись. Согласно Федеральному Закону

«об электронной подписи» от 06.04.2011 № 63-ФЗ [ниже0], электронная подпись - это информация в электронной форме, которая присоединена к документу в электронной форме или каким-либо иным образом связана с ним, предназна-ченная для криптографической защиты информации. Электронный документ, подписанный ЭЦП по юридической силе признаётся равным бумажному, подписанному рукописной подписью. Применение ЭЦП является необходимым для организации электронного документооборота, так как она обеспечивает подлинность документа.

Пользователю электронной цифровой подписью создаются оригинальные открытый и закрытый ключи. Закрытый ключ представляет собой набор информации, хранящийся в недоступном для других месте дискете, смарт-карте и работающий только в паре с открытым ключом, он должен быть известен лишь лицу, подписывающему документ. Открытый же создается для проверки, получаемых документов и передается вместе с ними. Сертификаты ключей ЭЦП выпускает удостоверяющий центр.

Существует два вида электронных подписей простая и усиленная. Усиленная же делится на квалифицированную и неквалифицированную.

Простая электронная подпись позволяет лишь идентифицировать личность лица, подписавшую документ, но не дает возможности увидеть изменения, которые были внесены в него, то естьона не предназначена для защиты документа от подделки.

Усиленная неквалифицированная подпись не только устанавливает автора документа, но и показывает,какие внесены в источник изменения.

Средства защиты усиленной квалифицированной подписи сертифицированы ФСБ РФ.

И так разберемся насколько безопасно использовать электронную цифровую подпись, для этого рассмотрим, каким образом происходит защита информации. Для генерации ЭП используют средства криптографической защиты с хэш-функциями, из-за чего взлом электронной подписи является, довольно, проблематичным, так как механизм усиленной криптозащиты слишком тяжелый, но это не спасает владельцев от физической утраты ключа или пароля к нему, а также от фальсификации ЭЦП через удостоверяющие центры.

За те годы, что в России действует ЭЦП, наблюдалось несколько способов мошенничества, такие как незаконные действия через центры сертификации ЭП, например, оформление документов без участия гражданина, так были зарегистрированы случаи массовой фальсификации ЭЦП путем повторного использования удостоверяющим центром электронной подписи клиента, например, случай, когда в 2019 году произошел отъем квартиры с помощью фальсификации электронной подписи [0] и дистанционный выпуск квалифицированного сертификата без личного контакта заявителя.

Цифровые подписи являются относительно безопасными, только в случаях, когда фальсификатору невозможно взломать криптографические функции, незаконно узнать ключ подписи лица, обмануть устройство в отношении поддельного документа, что он настоящий[0], а также подать заявление в удостоверяющий центр без участия владельца ЭЦП.

Для того, чтобы защититься от фальсификации, нужно хранить ключ ЭП только в безопасном месте, для чего лучше использовать специализированные программно-аппаратные хранилища, а также Росреестр рекомендует подать заявление о запрете проведения сделок какого-либо характера без личного участия заявителя, после чего Росреестр внесет специальную запись ЕГРН, о том, что даже лицо у которого есть нотариальная доверенность не сможет заключать сделки, без личного участия владельца подписи.

Предусмотренные законодательством виды электронных подписей позволяют дифференцированно подходить к их применению для различных задач документооборота. При этом использование УКЭП по сравнению с рукописной дает новые возможности, как установление его подлинности, ускорение самого процесса, так без ЭП современный документооборот уже не представляется возможным [0]. ЭЦП на данный момент не может гарантировать полную информационную безопасность, но законодательство, касающееся этого вопроса, продолжает совершенствоваться, так в Государственной Думе уже готовится законопроект, который бы ужесточил требования к удостоверяющим центрам, а также следует отметить, что в условиях активного развития компьютерных технологий,ЭЦП продолжает совершенствоваться, чтобы предоставить своим пользователям, как можно более высокий уровень защиты с технической стороны данного вопроса.

Список литературы:

1. Статья 2. Основные понятия, используемые в настоящем Федеральном законе / КонсультантПлюс [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_112701/c5051782233acca771e9adb35b47d3fb82c9ff1c/ (дата обращения: 12.03.2020).

2. Марина Бобылева Управленческий документооборот. От бумажного к электронному – PDF FreeDownload [Электронный ресурс]. URL: https://docplayer.ru/56738182-Marina-bobyleva-upravlencheskiy-dokumentooborot-ot-bumazhnogo-k-elektronnomu.html (дата обращения: 12.03.2020).

3. Квалифицированная ЭЦП: проблемы и риски в свете последних событий [Электронный ресурс]. URL: https://www.accountor.com/ru/russia/article/digital-signature-problems-and-risks (дата обращения: 12.03.2020).

4. Методы защиты от фальсификации электронной подписи КиберЛенинка [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/metody-zaschity-ot-falsifikatsii-elektronnoy-podpisi (дата обращения: 12.03.2020).

УДК 37.035.7

Касавцев Михаил Юрьевич, канд. техн. наук, кафедра Организации повседневной деятельности и боевой подготовки, Военно-космическая академия имени А.Ф.Можайского, г. Санкт-Петербург
Kasavtsev Mikhail Yurevich, Military space Academy named after A. F. Mozhaisky, St. Petersburg

МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ ВОЕННОСЛУЖАЩЕГО В ПРОЦЕССЕ ВОИНСКОГО ОБУЧЕНИЯ И ВОСПИТАНИЯ ПРИ ПОВСЕДНЕВНОЙ ДЕЯТЕЛЬНОСТИ
PERSONAL INFORMATION SECURITY MODEL MILITARY PERSONNEL IN THE PROCESS OF MILITARY TRAINING AND EDUCATION IN THEIR DAILY ACTIVITIES

Аннотация: рассматривается актуальный вопрос информационно безопасности личности военнослужащего в условиях цифровизации большинства сфер воинской деятельности. В результате анализа научных публикаций выявлено противоречие для разрешения, которого авторы разработали модель информационной безопасности личности военнослужащего.

Abstract: the article deals with the current issue of information security of the individual soldier in the conditions of digitalization of most areas of military activity. As a result of the analysis of scientific publications, a contradiction has been identified for the resolution of which the authors have developed a model of information security of the serviceman's personality.

Ключевые слова: информационно-психологическое воздействие, личность военнослужащего, информационно-психологическая безопасность.

Keywords: informational and psychological impact, military personnel's personality, informational and psychological security.

В настоящее время процессы цифровизации всех сфер жизни российского общества предъявляют определенные требования к готовности участников цифровой среды быть адекватным потребителем информационного контента, с учетом вопросов информационной безопасности личности в условиях перманентного информационно-психологического воздействия (ИПВ) на личность. Данные положения соответствуют решению задач, изложенных в соответствующих указах президента Российской Федерации [1, 2] и сформулированных им в послании Федеральному Собранию Российской Федерации [3], что подчеркивает актуальность тематики исследования.

Сфера военного образования не стала исключением из процесса цифровизации, поэтому в данной работе рассмотрим вопросы информационной безопасности личности военнослужащего (ИБЛВ). В научных публикациях процесс формирования ИБЛВ рассматривался авторами с различных точек зрения. Так, например, А.С. Кузин изучил ИБЛВ с точки зрения воспитания военнослужащих [4]. Авторы Р.В. Стрельцов, Т.А. Лавина и А.В. Черноземцев рассматривали ИБЛВ с позиции педагогических принципов и технологий [5].

Аспекты психологической безопасности, том числе в информационной среде, исследовали В.Д. Карандашов, А.А. Головинский и М.И. Нужа [6], а также М.Н. Горфина и В.Л. Горфин [7]. Вопросы противодействия ИПВ исследовались А.И. Макаренко [8], Н.И. Гомелем и М.В. Неверко [9], Е.Г. Барановым и Е.А. Каргиным [10]. Кроме того, в работе [11] А.Н. Дегтярев и М.З. Закиров представили модель информационной системы безопасной жизнедеятельности. Однако, почти все авторы рассматривают процесс ИБЛВ обособленно, в рамках одного конкретного аспекта. Кроме того, ни в одной работе нет предложений по систематизации процесса ИБЛВ.

Анализ научных публикаций по теме статьи выявил противоречие. С одной стороны, необходимость ИБЛВ – участника цифровой среды. С другой, отсутствие единого подхода к вопросам ИБЛВ. Для разрешения противоречия и систематизации процесса ИБЛВ существует необходимость разработки модели ИБЛВ в процессе воинского обучения и воспитания при повседневной деятельности, что является целью данной работы.

Представим процесс ИБЛВ в виде модели, изображенной на рисунке, где $\bar{I}$ – вектор ИПВ (управляющее воздействие) с учетом состояния векторов $\bar{N}$ – вектор ИБЛВ (корректируемых параметров) и $\bar{R}$ – вектор неконтролируемых командиром состояний военнослужащего (НКСВ) (некорректируемых параметров) воздействует на $\bar{\Psi}$ – вектор состояния объекта управления (компоненты личности военнослужащего) формируя при этом $\bar{H}$ – вектор защищаемых компонентов психологического здоровья (КЗПЗ) военнослужащих (управляемого воздействия). Данная модель позволяет объединить для совместного рассмотрения все воздействия на личность военнослужащего в процессе взаимодействия пользователя с цифровой средой.

Задачу ИБЛВ в формализованном виде запишем в виде выражения:

$$\bar{\Psi} f(\bar{I}, \bar{R}, \bar{N}) \to max\,. \qquad (1)$$

При решении данной задачи необходимо стремиться к максимизации уровня компонентов личности военнослужащего.

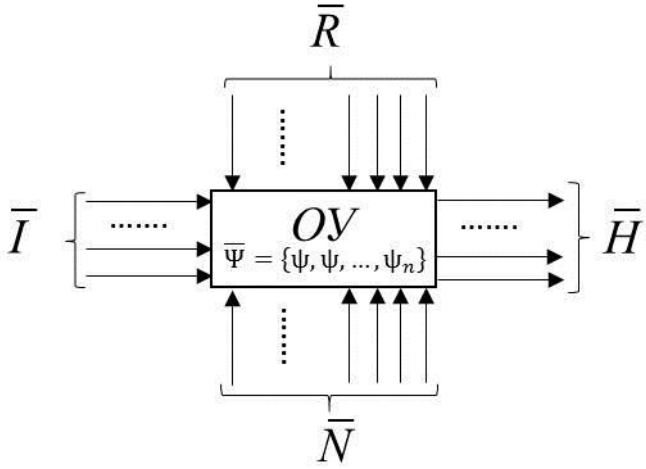

Рисунок – Модель ИБЛВ

Управление процессом ИБЛВ достигается варьированием величины составляющих векторов воздействий на объект управления. Ниже в таблице представлены компоненты данных векторов.

Таблица 1

Векторы модели ИБЛ военнослужащего

№ п/п	Составляющие векторов			
	$\bar{I}$ (вектор ИПВ)	$\bar{R}$ (вектор ИБЛВ)	$\bar{N}$ (вектор НКСВ)	$\bar{H}$ (вектор КЗПЗ)
1	убеждение и суггестивные методы	мероприятия по защите информации	темперамент	удовлетворенность
2	информационно-техногенные методы	мероприятия обучения военнослужащих	состояние здоровья	адекватность отражения окружающего мира
3	информационно-техногенные средства и методы ИПВ	методы воспитания военнослужащих	отсутствие обучающегося (наряд, командировка, госпиталь и т.п.)	адаптивность
4	психотропные средства ИПВ	способы и приемы психологической защиты личности	наличие психотравмирующей ситуации	психологическая устойчивость
5	«феноменологические» методы ИПВ	мероприятия правового воспитания		целостность личности
6	средства и методы манипуляции сознанием			внутренний локус контроля
7	комбинирование средств и методов ИПВ			личностная активность
8				автономность
9				мотивация
10				система личностных ценностей

Таким образом, в статье представлена модель ИБЛВ в процессе воинского обучения и воспитания при повседневной деятельности. Применение этой модели позволит с единых позиций рассматривать процесс информационной безопасности личности военнослужащего, а также использовать её при проведении дальнейших исследований эффективности безопасности личности военнослужащего при осуществлении на него ИПВ в повседневной деятельности.

Список литературы:

1. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». – URL: http://www.garant.ru/products/ipo/prime/doc/71456224/#1000 (дата обращения: 11.04.2020).

2. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы». – URL:http://www.garant.ru/products/ ipo/prime/doc/71570570/ #1000 (дата обращения: 14.04.2020).

3. Путин заявил о необходимости создания своих цифровых платформ. – URL.https://ria.ru/20180301/1515521860.html (дата обращения 25.04.2020)

4. Кузин А.С. Обучение будущих офицеров информационной безопасности // Материалы межвузовской студенческой научно-практической конференции, Новосибирск, 19 декабря 2017 г. – С. 91-94.

5. Стрельцов Р.В., Лавина Т.А., Черноземцев А.В. Методические основы подготовки военнослужащих войск национальной гвардии российской федерации в области информационной безопасности // Ученые записки университета им. П.Ф. Лесгафта. – № 4. – 2018. – С. 242-247.

6. Карандашов В.Д., Головинский А.А., Нужа М.И. Методологические аспекты исследования психологической безопасности военнослужащих // Вестник Ленинградского государственного университета им. А.С. Пушкина. – № 2. – 2017. – С. 1-10.

7. Горфина М.Н., Горфин В.Л. Психологическая характеристика механизмов психологической защиты военнослужащих // Материалы Международной научно-практической конференции «Современные условия взаимодействия науки и техники», г. Уфа, 11 ноября 2018. – С. 112-121.

8. Макаренко А.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века / Монография. – СПб.: Наукоемкие технологии, 2017. – 546 с.

9. Гомель Н.И., Неверко М.В. Управление сознанием военнослужащих в контексте решения задач обеспечения информационной безопасности государства // Гуманитарные проблемы военного дела. – №1 (6). – 2016. – С. 22-28.

10. Баранов Е.Г., Каргин Е.А. Информационная культура современного российского офицера // Вестник экспериментального образования. – № 2. – 2016. – С. 1-8.

11. Дегтярев А.Н., Закиров М.З. Разработка моделей информационных систем безопасной жизнедеятельности социально- экономических систем регионов российской федерации // Россия: тенденции и перспективы развития. – № 3. – 2018. – С. 12-20.

УДК 681.322.067
DOI 10.37539/NB185.2020.76.26.008

Левченков Александр Николаевич, к.т.н., доцент,
Донской государственный технический университет, г. Ростов-на-Дону
Levchenkov Alexandr Nikolaevic,
Don State Technical University, Rostov-on-Don

Абдуллаева Эльвира Наджаф кызы,
Донской государственный технический университет, г. Ростов-на-Дону
Abdullaeva Elvira Nadjaf, Don State Technical University, Rostov-on-Don

К ВОПРОСУ КЛАССИФИКАЦИИ АГРЕССИВНОСТИ ВЫЧИСЛИТЕЛЬНОЙ СРЕДЫ
ON THE CLASSIFICATION OF COMPUTING ENVIRONMENT AGGRESSIVENESS

Аннотация: в статье рассматривается подход к описанию вопросов безопасности за счет манипуляции информацией на основе принципов уникальности и обратимости информации. Рассмотрены два этапа описания: на основе классификации вычислительных сред и на основе ввода модели обработки информации с последующей формулировкой новой парадигмы безопасности информации.

Abstract: the article discusses the approach to describing security issues through the manipulation of information based on the principles of uniqueness and reversibility of information. Two stages of the description are considered: based on the classification of computing environments and based on the introduction of an information processing model with the subsequent formulation of a new information security paradigm.

Ключевые слова: безопасность информации, вычислительная среда, агрессивность вычислительной среды, ущерб безопасности, целостность ПО, достоверность, математическая верификация, модель агрессивности, приемо-сдаточные испытания, техническое задание.

Keywords: information security, computing environment, aggressive computing environment, security damage, software integrity, reliability, mathematical verification, aggressiveness model, acceptance tests, technical task.

Основным тезисом в решении задач безопасности информации в компьютерных системах является: – «Все вопросы безопасности информации описываются доступами субъектов к объектам». Мы можем обобщить этот тезис: – «Все вопросы безопасности информации описываются через принципы ***унификации*** и ***необратимости***». Основной тезис данной работы, который, по мнению авторов позволит выйти за рамки проблемы защиты информации, можно сформулировать следующим образом: – «Все вопросы безопасности информации решаются, за счет описания и манипуляции информацией на основе принципов **уникальности** и **обратимости** информации». Принятие соответствующего тезиса позволит снять практически все проблемы обеспечения безопасности информации вычислительных сред в корпоративных вычислительных сетях [1].

Реализацию описанного выше принципа предполагается провести в два этапа. На первом этапе осуществляется классификация открытых вычислительной сред, и определяется модель агрессивности открытых вычислительной сред. Это позволит решать задачи защиты информации от не легитимного доступа к информации в современных информационных технологиях. На втором этапе вводится новая модель обработки информации, и на ее основе формулируется новая парадигма безопасности информации. Основная цель новой парадигмы может быть сформулирована так: **– предел агрессивности любой открытой вычислительной среды стремится к нулю при стремлении времени ее существования к бесконечности, без административного вмешательства человека** (т.е. прозрачно для конечного пользователя).

Агрессивная вычислительная среда (АВСр) представляет собой такую вычислительную среду, в которой существуют экстравертные нелегитимные процессы [2].

Величину, характеризующую способность ВСр нанести ущерб безопасности и целостности ПО назовем уровнем агрессивности ВСр. Уровень агрессивности ВСр существенно влияет на уровень безопасности ПО и определяет в общем случае безопасность ВСр для исследуемого ПО, является составляющей уровня безопасности ПО. Воздействия ВСр, нарушающие безопасность и целостность ПО связываются с понятием агрессивного свойства ВСр прежде всего исходя из семантического сходства с понятием агрессии в области психологии. Таким образом, *задача исследования* состоит в определении качественных и количественных характеристик агрессивной ВСр (АВСр), оценке ее влияния на уровень безопасности ПО [3].

Цель исследований является проведение анализа свойств агрессивности вычислительной среды, выявить зависимость уровня безопасности программного средства от степени проявления свойства агрессивности ВСр.

С учетом классификации открытых вычислительных сред обработки информации выбраны классы ВСр как наиболее интересные, с токи зрения обеспечения безопасности объектов информатики, имеющих повышенные требования к сохранению конфиденциальности [1].

Классы вычислительных сред:

1. Вычислительная среда **реального времени:**

a) моделирование реального (физического) процесса;

b) класс ВСр РЕАЛЬНОГО ВРЕМЕНИ обычно реализуется на аппаратном, программно-аппаратном и операционных уровнях иерархии ВСр;

c) требует только эксплуатации.

2. Вычислительная среда **проектирования**:

a) моделирование объектов информатики;

b) реализуется на прикладном и пользовательском уровнях иерархии ВСр;

c) планирование.

3. Вычислительная среда **разработки:**

a) реализация информационного объекта (программной системы) в соответствии с моделью (спланированной в классе ВСр **проектирование**);

b) реализуется на инструментальном уровне иерархии ВСр;

c) реализация и тестирование.

4. **Прикладная** вычислительная среда:

a) обработка, хранение и передача, по каналам связи, информации;

b) реализуется на пользовательском и проблемном уровнях иерархии ВСр;

c) применение информационного объекта.

В качестве применения модели агрессивности вычислительных сред, при разработке показателей и метрик агрессивности ВСр, мы рассмотрим класс ВСр РЕАЛЬНОГО ВРЕМЕНИ. Этот выбор определяется важностью соответствующих средств при эксплуатации объектов информатики военного назначения. Классификация опирается на следующий критерии агрессивности ВСр:

a) уровень достоверности ВСр на присутствие закладок;

b) уровень достоверности ВСр на присутствие реимплицитных программ («компьютерные вирусы»);

c) уровень достоверности ВСр по доступу к информации и ресурсам компьютерной системы.

1. Полностью ДОВЕРИТЕЛЬНАЯ ВСр $\tau^{ПД}$:

a) при приемо-сдаточных испытаниях была проведена математическая верификация на полноту, непротиворечивость и соответствие техническому заданию (ТЗ), математическая верификация на избыточность ВСр реального времени (без погружение в ВСр ПО РЕАЛЬНОГО ВРЕМЕНИ);

b) в процессе эксплуатации ВСр реального времени нет никаких каналов по которым ВСр может быть модифицирована из вне объектами отличными от штатного ПО системы РЕАЛЬНОГО ВРЕМЕНИ;

c) ВСр РЕАЛЬНОГО ВРЕМЕНИ не обладает средствами отказа в доступе (исключения составляют ошибки или сбои аппратных средств).

2. Относительно ДОВЕРИТЕЛЬНАЯ ВСр $\tau^{ОД}$:

a) при приемо-сдаточных испытаниях была проведена математическая верификация на полноту, непротиворечивость и соответствие техническому заданию (ТЗ), математическая верификация на избыточность ВСр реального времени (без погружение в ВСр ПО РЕАЛЬНОГО ВРЕМЕНИ);

b) в процессе эксплуатации ВСр реального времени нет никаких каналов по которым ВСр может быть модифицирована из вне объектами отличными от штатного ПО системы РЕАЛЬНОГО ВРЕМЕНИ;

c) ВСр РЕАЛЬНОГО ВРЕМЕНИ обладает собственными программно-аппаратными средствами разделения доступа к информации, процессам и ресурсам.

3. Относительно АГРЕССИВНАЯ ВСр $\tau^{ОА}$:

a) при приемо-сдаточных испытаниях не была проведена математическая верификация на полноту, непротиворечивость и соответствие техническому заданию (ТЗ), математическая верификация на избыточность ВСр реального времени (без погружение в ВСр ПО РЕАЛЬНОГО ВРЕМЕНИ);

b) в процессе эксплуатации ВСр реального времени нет никаких каналов по которым ВСр может быть модифицирована из вне объектами отличными от штатного ПО системы РЕАЛЬНОГО ВРЕМЕНИ;

c) ВСр РЕАЛЬНОГО ВРЕМЕНИ обладает собственными программно-аппаратными средствами разделения доступа к информации, процессам и ресурсам.

4. Полностью АГРЕССИВНАЯ ВСр $\tau^{ПА}$:

a) при приемо-сдаточных испытаниях не была проведена математическая верификация на полноту, непротиворечивость и соответствие техническому заданию (ТЗ), математическая верификация на избыточность ВСр реального времени (без погружение в ВСр ПО РЕАЛЬНОГО ВРЕМЕНИ);

b) в процессе эксплуатации ВСр реального времени есть каналы по которым ВСр может быть модифицирована из вне объектами отличными от штатного ПО (выделенные каналы, удаленный доступ, устройства хранения информации и т.д.) системы РЕАЛЬНОГО ВРЕМЕНИ;

c) ВСр РЕАЛЬНОГО ВРЕМЕНИ обладает собственными, но не документированными, программно-аппаратными средствами разделения доступа к информации, процессам и ресурсам.

Приведенная классификация необходима для разработки модели агрессивной вычислительной среды и определения качественных и количественных характеристик агрессивности среды а также для определения зависимости уровня безопасности программного средства от уровня агрессивности ВСр.

Список литературы:

1. Запечников С.В., Милославская Н.Г. и др. Информационная безопасность открытых систем: Учебник для вузов. В 2-х томах. Том 1 – Угрозы, уязвимости, атаки и подходы к защите. – М.: Горячая линия-Телеком, 2016. – 536 с.

2. Климов В.С. Методы и модели противодействия компьютерным атакам. – Люберцы.: КАИАЛИТ, 2010. – 316 с.

3. Лобко В.Т. Инструментальное средство экспериментальной оценки метрик качества и безопасности программ. // Известия высших учебных заведений. Северо-Кавказский регион. Технические науки, № 2, 2017.

УДК 681.322.067
DOI 10.37539/NB185.2020.68.59.009

Левченков Александр Николаевич, к.т.н., доцент,
Донской государственный технический университет, г. Ростов-на-Дону
Levchenkov Alexandr Nikolaevic,
Don State Technical University, Rostov-on-Don

Абдуллаева Эльвира Наджаф кызы,
Донской государственный технический университет, г. Ростов-на-Дону
Abdullaeva Elvira Nadjaf, Don State Technical University, Rostov-on-Don

АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ НА ОСНОВЕ ГРАФОВОЙ МОДЕЛИ
GRAPH-BASED SECURITY RISK ANALYSIS

Аннотация: в статье описывается один из подходов к анализу угроз безопасности информации на основе использования графовой модели, которая описывает различные информационные потоки на основе учета политики безопасности, которая определяет правила взаимодействия информационных потоков с информационными объектами и узлами с целью выявления и перекрытия несанкционированных маршрутов.

Abstract: the article describes one of the approaches to the analysis of information security threats based on the use of a graph model that describes various information flows based on a security policy that defines the rules for the interaction of information flows with information objects and nodes in order to identify and block unauthorized routes.

Ключевые слова: информационные потоки, граф, узел, вершина, ребро, множества, информационные узлы, автоматизированная система, политика безопасности, угрозы, уязвимость программного обеспечения.

Keywords: information flows, graph, node, vertex, edge, sets, information nodes, automated system, security policy, threats, software vulnerability.

Рассмотрим совокупность информационных потоков в автоматизированной системе. Каждый информационный поток исходит из какого-либо узла и заканчивается в каком-либо узле. Представим эти потоки в виде графа

$$G=\{V,E\} \quad (1)$$

где V – множество вершин графа, соответствующих узлам,

E – множество ребер графа, соответствующих информационным потокам [1].

Поскольку каждый поток имеет определенное начало и конец, то граф G является ориентированным графом.

Среди множества информационных узлов выделим те узлы, которые принадлежат внешней среде автоматизированной системы. Назовем такие узлы внешними, а соответствующие им вершины графа G – внешними вершинами.

$$V = V_I \cup V_O, \quad (2)$$

где V_I – внутренние вершины графа,

V_O – внешние вершины.

Зададим функцию

$$I_V : V \to N, \tag{3}$$

которая ставит в соответствие каждой вершине некоторое натуральное число, являющееся ее идентификатором.

Зададим функцию

$$L_V : V \to N_L \subset N, \tag{4}$$

где N_L – подмножество натуральных чисел, обозначающих уровни доступа (или грифы секретности). Функция L_V ставит в соответствие каждой вершине ее уровень доступа.

Зададим функцию

$$I_E : E \to N, \tag{5}$$

которая ставит в соответствие каждому ребру некоторое натуральное число, являющееся идентификатором соответствующего информационного потока.

Зададим функцию

$$L_E : E \to N_L, \tag{6}$$

которая определяет для каждого ребра уровень доступа, определенный для соответствующего информационного потока. Уровень доступа информационного потока и его идентификатор равны уровню доступа и идентификатору обрабатываемого в этом потоке информационного объекта.

Функции I_V, L_V, I_E и L_E предназначены для идентификации вершин и ребер и назначения им уровней доступа. Эти идентификаторы и метки уровней доступа используются для отражения в модели различных методов разграничения полномочий (мандатного и дискреционного).

Принятая для автоматизированной системы политика безопасности определяет правила взаимодействия информационных потоков с информационными объектами и узлами.

Анализ различных угроз позволяет выявить некоторые общие черты. Во-первых любая угроза направлена на какое-то определенное множество информационных объектов. Это могут быть данные пользователей, служебная информация, данные операционной системы и т.д. Во-вторых, угроза всегда исходит от какого-либо источника. В различных случаях в качестве источника, от которого исходит угроза, может выступать злоумышленник, пользователь системы, нарушающий правила работы, случайные события, такие как сбой в сети электропитания и т.д. В-третьих, всякая угроза реализуется, используя некоторые недостатки или уязвимости автоматизированной системы или информационной технологии. Их еще можно назвать точками приложения угрозы. Это могут быть недостатки в организации вычислительного процесса, сбои и отказы аппаратных средств, ошибки и уязвимости программного обеспечения [2]. Таким образом, угрозу T можно представить в виде тройки множеств:

- множество объектов O;
- множество источников S;
- множество точек приложения P. Или

$$T=\{O, S, P\} \quad (7)$$

Рассмотрим структуру этих множеств более подробно.

Множество объектов O, на которые направлены угрозы безопасности, состоит из информационных объектов, представляющих собой порции информации и правила их обработки. Собственно, угроза безопасности информации состоит в доступе или модификации с нарушением этих правил. Правила обработки информации можно представить в виде логических выражений или предикатов, определяющих разрешенные действия над информационными объектами. Т.е. информационный процесс IP может выполнить операцию Op над информационным объектом O только в том случае, если предикаты $Preds \in O$ принимают значения ИСТИНА для Op и IP.

Кроме правил, определяющих разрешенные операции так же существуют предикаты, которые описывают внутренние свойства информации, например, ее целостность и непротиворечивость. Эти правила задаются при проектировании информационной технологии и отражаются в документации и спецификациях на информационные массивы и программное обеспечение. При информационных узлах все предикаты должны иметь значение «истина». Внутри потоков правила могут нарушаться, так как обработка информации выполняется последовательно и невозможно обеспечить целостность информации при выполнении программ ее обработки.

Контроль за выполнением правил обработки информации осуществляется выделенной группой информационных процессов, называемых ядром безопасности. Они работают с информационными объектами, называемыми дескрипторами защиты и представляющими собой предикаты других информационных объектов. Предикаты, описывающие правила работы с дескрипторами задаются при проектировании информационной технологии и остаются неизменными в течение всего времени ее использования. Таким образом, в модели выделяются две группы процессов – обычные и относящиеся к ядру безопасности. Первые выполняют функциональные задачи информационной системы, а вторые обеспечивают безопасность обрабатываемой информации.

Множество источников угроз S представляет собой причины нарушений безопасности информации. Такими источниками могут быть случайные факторы внешней среды или самой системы, а так же злоумышленники. В данном случае важен не их субъективный или объективный характер, а то, что эти источники инициируют процесс реализации угрозы.

Точки приложения P – это уязвимости, на использовании которых основана конкретная угроза безопасности информации. К их числу относятся недостатки организационного характера, ошибки, сбои и отказы аппаратуры, уязвимости программного обеспечения.

В предлагаемой модели информационной технологии объект O – это информация, источник – часть среды информационного потока, точка приложения – свойство информационного потока.

Рассмотрим, в чем проявляется реализация угрозы безопасности информации на графовой модели информационных потоков. Нарушение безопасности информации выражается в невыполнении предикатов информа-

ционного объекта при нахождении его в информационных узлах [3]. Кроме того, раскрытие может произойти при попадании информационного объекта в информационный поток, заканчивающийся на внешнем информационном узле, не имеющем требуемого уровня полномочий. Пусть информационный поток IP начинается в узле IN1 и заканчивается в узле IN2. В нашей модели ему соответствует дуга $e \in E$ и вершины $v_1, v_2 \in V$, соответствующие начальному и конечному узлам. Предположим, что в потоке находится информационный объект O, обозначим функцию, соответствующую логическому произведению его предикатов O.pred(). Тогда нарушение безопасности имеет место, когда

$$\text{O.pred}(v_2)=\text{false}. \quad (8)$$

Таким образом, для противодействия угрозам безопасности информации необходимо не допускать ситуаций, при которых выполняется (8). Такие ситуации могут возникнуть в следующих случаях:

- в результате преобразования информации в информационном потоке;
- в результате перемещения защищаемой информации информационным потоком.

Первый случай касается угроз нарушения целостности, модификации и отказа в доступе, второй случай охватывает угрозы, связанные с разглашением информации ограниченного доступа. Для противодействия угрозам, относящимся к первому случаю существует ряд методов, связанных с контролем в начальных и конечных узлах информационных потоков, который осуществляется ядром безопасности. Это методы контрольного суммирования, проверки полномочий доступа, управления списком разрешенных действий и т.д. Ситуации, возникающие во втором случае, связаны с наличием в автоматизированных системах внешних информационных узлов, которые имеют непосредственную связь с внешней средой. Важной особенностью внешних узлов является то, что на них начинаются информационные потоки во внешнюю среду, которые реализуются вне вычислительных машин и не подпадают под контроль ядра безопасности. Уровень доступа и идентификатор внешнего информационного узла определяются уровнем доступа и идентификатором носителя информации, используемого в нем и очень часто у ядра безопасности нет технической возможности проконтролировать его. Например, ядро безопасности ПЭВМ не может определить учтенная или не учтенная бумага используется в принтере.

Таким образом, необходимо контролировать внешние информационные узлы и маршруты информационных потоков, заканчивающиеся в них. Рассмотрим некоторый информационный объект O [4]. Разобьем множество внутренних вершин на два подмножества V_1 и V_2, такие, что

$$V_I = V_1 \cup V_2, \quad (9)$$

$$V_1 = \{v \mid v \in V_I, O.pred(v) = true\}, \quad (10)$$

$$V_2 = \{v \mid v \in V_I, O.pred(v) = false\}. \quad (11)$$

В первое множество входят вершины, которые соответствуют тем узлам, в которых, согласно политики безопасности, может находиться информационный объект O, а ко второму – те, которые соответствуют узлам, попадание

в которые объекта О означает нарушение безопасности информации. В соответствии с этим разобьем множество дуг.

$$E = E_1 \cup E_2, \tag{12}$$

$$E_1 = \{ e = (v_1, v_2) | (v_1 \in V_1 \vee v_1 \in V_0) \wedge (v_2 \in V_1 \vee v_2 \in V_0) \}, \tag{13}$$

$$E_2 = \{ e = (v_1, v_2) | v_1 \notin V_1 \vee v_2 \notin V_1 \}. \tag{14}$$

Такое разбиение приводит к тому, что граф информационных потоков (1) распадается на два подграфа

$$G = G_1 \cup G_2, \tag{15}$$

Где

$$G = G_1 \cup G_2, \tag{16}$$

$$G = G_1 \cup G_2, \tag{17}$$

$$G = G_1 \cup G_2, \tag{18}$$

Граф (17) представляет собой схему информационных потоков и узлов, которые являются для объекта О разрешенными политикой безопасности. За техническую реализацию разбиения (15) в информационной системе отвечает ядро безопасности.

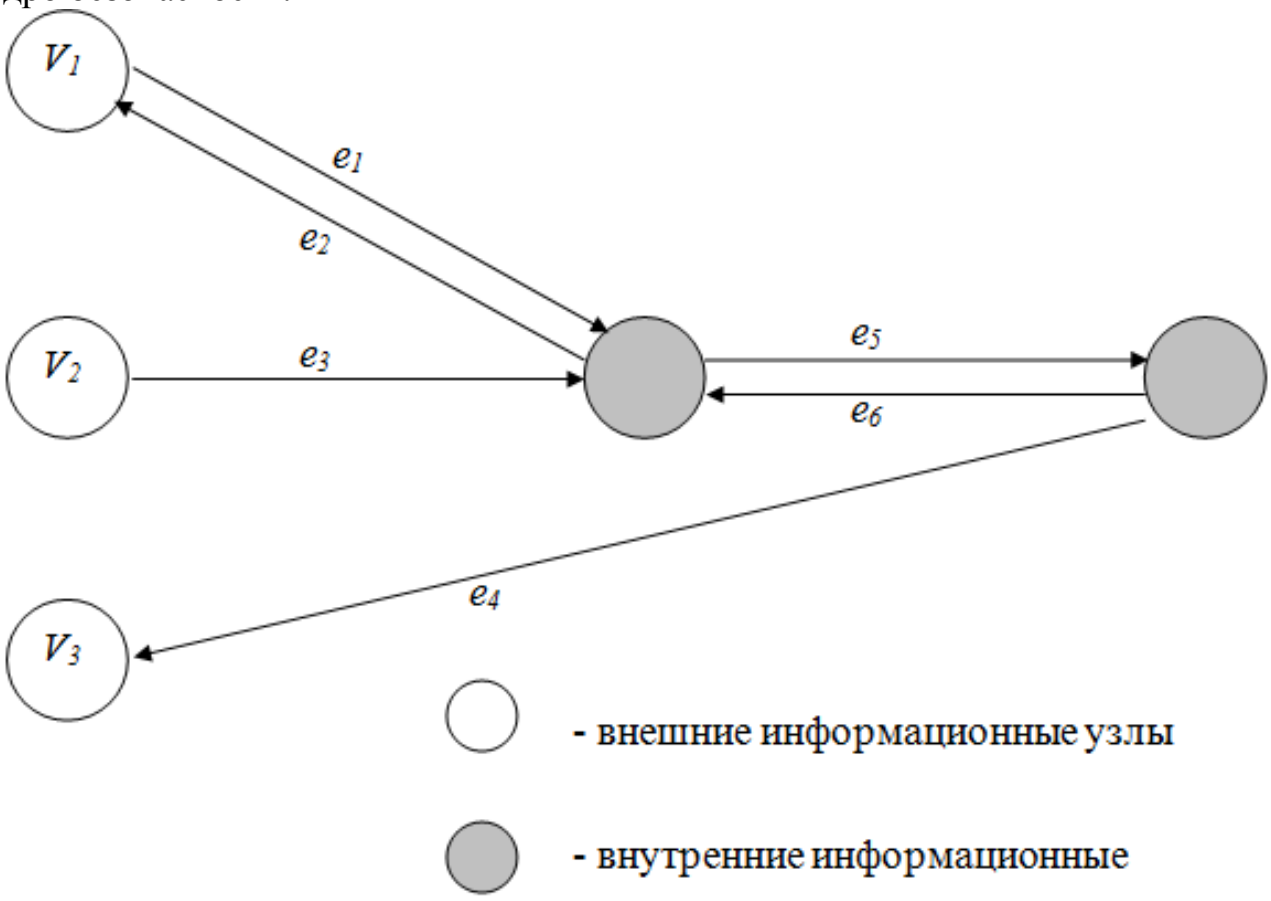

Рисунок 1 – Пример графовой модели информационных потоков

Пусть в некоторый момент времени информационный объект О находится в информационном узле, которому соответствует вершина $v \in G_1$. Рассмотрим вершину $v' \in V_O$. Если в графе G_1 существует ориентированный маршрут M, начальная вершина которого есть v, а конечная – v', то существует угроза

$$T = \{O, S, P\}, \quad (19)$$

где P – уязвимость, заключающаяся в возможности утечки информации через информационный узел, которому соответствует вершина v'.

Таким образом, в настоящее время одной из актуальных проблем является возможность раскрытия информации при записи ее на отчуждаемые носители. Для решения этой проблемы необходимо разработать и реализовать комплекс механизмов и средств, выявляющих и перекрывающих маршруты, по которым информационные объекты могут попадать на внешние информационные узлы и отчуждаемые носители информации.

Список литературы:

1. Оре О. Теория графов. – М.: Наука, 1980. – 352 с.
2. Запечников С.В., Милославская Н.Г. и др. Информационная безопасность открытых систем: Учебник для вузов. В 2-х томах. Том 1 – Угрозы, уязвимости, атаки и подходы к защите. – М.: Горячая линия-Телеком, 2016. – 536 с.
3. Аляев Ю.А., Тюрин С.Ф. Дискретная математика и математическая логика. – М.: Финансы и статистика, 2006. – 368 с.
4. Гуров С. И. Булевы алгебры, упорядоченные множества, решетки: Определения, свойства, примеры. Изд.2. М.: Книжный дом «ЛИБРОКОМ», 2013. – 352 с.

НБ ЗАЩИТА ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

УДК 006.63+658.62.018.012

Карганов Виталий Вячеславович,
Старший научный сотрудник к.т.н., доцент, Научно исследовательский центр Военная академия связи, г. Санкт-Петербург
Karganov Vitaly Viacheslavovich, Science Research Center Military Academy of telecommunications, Saint-Petersburg

ОСНОВНЫЕ ПОЛОЖЕНИЯ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ЧАСТИ АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ
THE BASIC PROVISIONS ON THE REQUIREMENTS INFORMATION SECURITY IN THE PART OF CERTIFICATION OF INFORMATIZATION OBJECTS

Аннотация: рассмотрены основные положения по аттестации объектов информатизации, как одного из элементов мероприятий по защите информации ограниченного доступа. Приведены мероприятия на этапе подготовки, функции

органов и заявителей, а также порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Материалы статьи изложены на основе общедоступных документов Российской Федерации.

Abstract: the main provisions on certification of informatization objects as one of the elements of measures to protect restricted access information are considered. Measures at the stage of preparation, functions of bodies and applicants, as well as the procedure of certification of informatization objects according to the requirements of information safety are presented. The materials of the article are presented on the basis of publicly available documents of the Russian Federation.

Ключевые слова: объект информатизации, аттестат соответствия, аттестация, требованиям по безопасности информации, защита информации.

Keywords: object of informatization, certificate of conformity, certification, information security requirements, information protection.

Под аттестацией объекта информатизации (ОИ) понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» («АС») подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК и/или ФСБ России [1].

Наличие на ОИ действующего «АС» дает право обработки информации с соответствующим грифом конфиденциальности на период времени, установленным в непосредственном документе.

Обязательной аттестации подлежат ОИ, предназначенные для обработки информации, составляющей государственную тайну (ГТ), управления экологически опасными объектами, ведения закрытых переговоров. В остальных случаях аттестация носит добровольный характер и может осуществляться по инициативе заказчика или владельца ОИ.

Аттестация по требованиям безопасности информации предшествует началу обработки, подлежащей защите информации (ЗИ), и вызвана, необходимостью официального подтверждения эффективности комплекса мер ЗИ. При аттестации ОИ подтверждает его соответствие требованиям по ЗИ от несанкционированного доступа (НСД), в том числе от компьютерных вирусов, от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на ОИ, от утечки или воздействия на нее за счет специальных устройств, встроенных в ОИ и других угроз безопасности информации [2].

Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого ОИ в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации. Она проводится органом по аттестации в установленном порядке в соответствии со схемой, выбираемой этим органом на этапе подготовки к аттестации (рис. 1).

Рисунок 1 – Основные мероприятия на этапе подготовки к аттестации

Органы по аттестации аккредитуются ФСТЭК и/или ФСБ России, где правила аккредитации определены в действующем документе [3]. Они несут ответственность за выполнение возложенных на них функций, обеспечение сохранности государственных и коммерческих секретов, а также за соблюдение авторских прав разработчиков, аттестуемых ОИ и их компонент. Ниже приведены функции органов по аттестации и непосредственно заявителей (табл. 1).

Таблица 1

Функции органов и заявителей по аттестации

Участник	Функции
Органы по аттестации	Аттестуют ОИ и выдают «АС».
	Осуществляют контроль над безопасностью информации, циркулирующей на аттестованных ОИ, и за их эксплуатацией.
	Отменяют и приостанавливают действие выданных этим органом «АС».
	Формируют фонд нормативной и методической документации, необходимой для аттестации конкретных типов ОИ, участвуют в их разработке.
	Ведут информационную базу аттестованных этим органом ОИ.
Заявители	Проводят подготовку ОИ для аттестации путем реализации необходимых организационно-технических мероприятий по ЗИ.
	Привлекают органы по аттестации для организации и проведения аттестации ОИ.
	Предоставляют органам по аттестации необходимые документы и условия для проведения аттестации.

Окончание таблицы 1

Участник	Функции
	Привлекают, в необходимых случаях, для проведения испытаний несертифицированных средств ЗИ, используемых на аттестуемом ОИ, ИЛ(Ц) по сертификации.
	Осуществляют эксплуатацию ОИ в соответствии с условиями и требованиями, установленными в «АС».
	Извещают орган по аттестации, выдавший «АС», обо всех изменениях в информационных технологиях, составе и размещении средств и систем информатики, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств ЗИ.
	Представляют необходимые документы, и условия для осуществления контроля и надзора за эксплуатацией ОИ, прошедшего обязательную аттестацию.

Дальнейшее изучение, исследуемого материала, приводит нас к графическому представлению, порядка проведения аттестации ОИ безопасности информации (рис. 2).

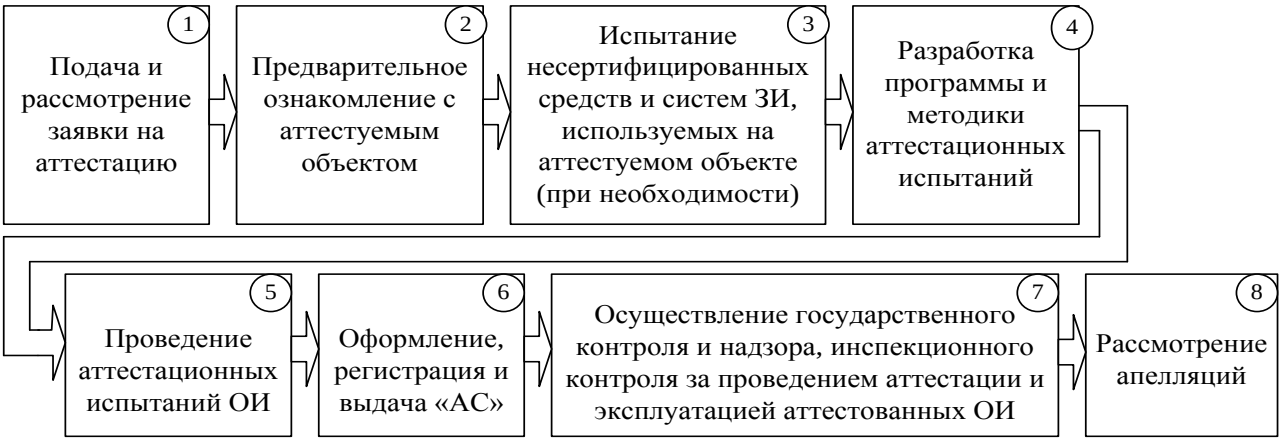

Рисунок 2 – Основные действия при проведении аттестации

Последующая детализация представленных выше действий (см. рис. 2) побуждает рассмотреть порядок необходимых работ на этапе аттестационных испытаний ОИ (табл. 2).

Таблица 2

Перечень необходимых работ

№ п/п	Наименование
1.	Осуществляется анализ организационной структуры ОИ, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы ЗИ на объекте, разработанной документации и ее соответствия требованиям нормативной документации по ЗИ.
2.	Определяется правильность категорирования объектов электронной вычислительной техники и классификации систем (при их аттестации), выбора и применения сертифицированных и несертифицированных средств и систем ЗИ.

Окончание таблицы 2

№ п/п	Наименование
3.	Проводятся испытания несертифицированных средств и систем ЗИ на аттестуемом объекте или анализ результатов их испытаний в ИЛ(Ц) по сертификации.
4.	Проверяется уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации.
5.	Проводятся комплексные аттестационные испытания ОИ в реальных условиях эксплуатации путем проверки фактического выполнения, установленных требований на различных этапах технологического процесса обработки защищаемой информации.
6.	Оформляются протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты ОИ в соответствие с установленными требованиями и совершенствованию этой системы, а также рекомендациями по контролю над функционированием ОИ.

Заключение по результатам аттестации с краткой оценкой соответствия ОИ требованиям по безопасности информации, выводом о возможности выдачи «АС» и необходимыми рекомендациями подписывается членами аттестационной комиссии и доводится до сведения заявителя. К заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод. Протоколы испытаний подписываются экспертами – членами аттестационной комиссии, проводившими испытания. Заключение и протоколы испытаний подлежат утверждению органом по аттестации. Документ в виде «АС» оформляется и выдается заявителю после утверждения заключения по результатам аттестации. Владелец аттестованного ОИ несет ответственность за выполнение установленных условий функционирования ОИ, технологии обработки защищаемой информации и требований по безопасности информации.

В случае изменения условий и технологии обработки защищаемой информации владельцы аттестованных объектов обязаны известить об этом орган по аттестации, который принимает решение о необходимости, проведения дополнительной проверки эффективности системы защиты ОИ. При несоответствии аттестуемого объекта требованиям по безопасности информации и невозможности оперативно устранить отмеченные аттестационной комиссией недостатки орган по аттестации принимает решение об отказе в выдаче «АС».

ФСТЭК России может передавать права на аккредитацию отраслевых (ведомственных) органов по аттестации другим органам государственной власти в том числе, Министерству обороны Российской Федерации.

Таким образом, выше представленный материал раскрывает наиболее основные положения предлагаемого вопроса, а именно – аттестация ОИ по требованиям безопасности информации. Стоит отметить, что представленные данные приведены в соответствии с нормами и требованиями, действующих на настоящее время руководящих документов Российской Федерации.

Констатация вышесказанного позволяет говорить о том, что выполнение приведенных выше мероприятий позволит установленным федеральным органам исполнительной власти в данной предметной области, удостоверить соответствие ОИ требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров. И как следствие, это свидетельствует о том, что рассматриваемое выше положение, по своей сути не что иное, как одно из звеньев, одной большой цепи в системе ЗИ.

Список литературы:

1. Приказ Федеральной службы по техническому и экспортному контролю России от 3 апреля 2018 г. № 55 «Об утверждении Положения о системе сертификации средств защиты информации».

2. Приказ Федеральной службы по техническому и экспортному контролю России от 20 марта 2012 г. № 28 «Об утверждении Требований в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требований к средствам антивирусной защиты)».

3. Приказ Министра обороны Российской Федерации от 7 августа 2015 г. № 465 «Об осуществлении в Министерстве обороны Российской Федерации аккредитации органов по сертификации и испытательных лабораторий, выполняющих работы по оценке (подтверждению) соответствия в отношении продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну».

НБ КИБРБЕЗОПАСНОСТЬ И КИБЕРПРЕСТУПНОСТЬ

УДК 343.3

Ващинников Артем Дмитриевич, Калистратова Алина Александровна,
Московский Государственный Технический Университет
им. Н.Э. Баумана, г. Москва
Vashchinnikov Artem Dmitrievich, Kalistratova Alina Aleksandrovna,
Bauman Moscow State Technical University, Moscow

ПРОБЛЕМЫ НАРУШЕНИЯ АВТОРСКИХ ПРАВ И КИБЕРБЕСОПАЗНОСТИ
PROBLEMS OF COPYRIGHT VIOLATION AND CYBERSECURITY

Аннотация: в статье освещаются существующие вопросы кибербезопасности, анализируется их современное состояние, проблемы и возможные их решения. Рассмотрено использование нелицензионного программного обеспечения в качестве одной из причин, приводящих к повышению уязвимости от кибератак. Даны рекомендации по повышению защищенности предприятия от киберпреступности.

Abstract: the article highlights the existing issues of cybersecurity, analyzes their current state, problems and possible solutions. The use of unlicensed software as one of the reasons leading to increased vulnerability from cyber attacks is considered. Recommendations are given to improve the company's security against cybercrime.

Ключевые слова: кибербезопасность, кибератаки, информационные технологии.

Keyword: cybersecurity, cyber attacks, information technology.

В эпоху информационного общества практически все сферы жизнедеятельности человека оказываются компьютеризованны. Информационные технологии оказывают значительное влияние на жизнь общества и работу государственных служб.

Экспертами по кибербезопасности было установлено, что в мире в 2019 году кибератаки совершались каждые 14 секунд. Убытки компаний различных секторов экономики уже исчисляется триллионами рублей и в дальнейшем эти цифры будут только расти.

Большинство инноваций в области компьютерной техники расширяют сферу киберпреступности и создают новые возможности для злоумышленников. Киберпреступления регулярно входят в пять основных видов экономических преступлений в мире, даже несмотря на то, что на настоящий момент не существует однозначных и общепринятых методов сбора данных о подобных преступлениях и некоторые из них остаются неучтенными. На настоящий момент многие российские компании недооценивают последствия кибератак, а потерпевшие граждане не знают, куда обращаться за помощью.

Чаще всего жертвами мошенников оказываются не крупные компании, имеющие квалифицированных специалистов и соответствующее программное обеспечение, а предприятия малого и среднего бизнеса. В связи с низким бюджетом подобных предприятий, им сложно предпринимать серьезные меры по повышению информационной безопасности и они зачастую не могут гарантировать конфиденциальность данных своих клиентов или защиту своей интеллектуальной собственности. Зачастую подобные фирмы, став жертвами мошенников, даже не обращаются в правоохранительные органы. Это связано с опасениями потерять репутацию среди клиентов, а так же с тем, что вероятность найти виновных и компенсировать убытки невелика. Отсутствие необходимости обязательно информировать правоохранительные органы о кибератаках позволяет преступникам чувствовать себя в безопасности и безнаказанно повторять свои действия.

По данным МВД, в 2019 году зарегистрированы 294,4 тысячи преступлений, совершенных с использованием информационно-телекоммуникационных технологий, или на 68,5% больше, чем за аналогичный период прошлого года [1].

Расследование киберпреступлений усложняется тем, что они носят международный характер. Преступники не ограничиваются каким-то конкретным городом или регионом и занимаются поиском уязвимостей во всех странах мира. Для противодействия киберпреступлениям в 2019 году председателем Следственного комитета России был подписан приказ о создании отдела по расследованию киберпреступлений и преступлений в сфере высоких технологий, но до полного решения проблемы киберпреступности пока еще далеко.

Для повышения уровня кибербезопасности в стране прежде всего необходимо оповестить сотрудников о распространённых методах сетевых атак, угрозах безопасности и их роли в соблюдении правил информационной безопасности. Большинство людей не знает, как распознавать и реагировать на различные атаки, какие предпринимать меры и к чему подобные действия злоумышленников могут привести.

В США опрос среди исполнительных директоров показал, что более 50% из них опасаются киберугроз и считают их значительной проблемой. В России большинство директоров компаний вообще не считают кибербезопасность угрозой и в лучшем случае согласны приобрести корпоративную версию антивирусной программы.

Отсутствие лицензионного программного обеспечения во многих компаниях так же помогает преступникам. В связи с высокой стоимостью программных продуктов (например, установка AutoCAD обойдется компании примерно в 100 тысяч рублей за компьютер) многие фирмы используют пиратские программные продукты и операционные системы. Такие программы часто содержат вирусы или шпионский код, сообщающий злоумышленнику результаты работы в этой программе. Бывают и случаи, когда директор компании просто не разбирается в данном вопросе, а системный администратор, получив средства на приобретение программного продукта, присваивает их себе и устанавливает на компьютеры пиратский продукт.

Ответственность за использование нелицензионного программного обеспечения наступает в соответствии со ст.7.12 КоАП РФ «Нарушение авторских и смежных прав, изобретательских и патентных прав». Размеры штрафа определяются следующим образом: для граждан – штраф в размере от 1 500 до 2 000 рублей; плюс конфискация оборудования, для должностных лиц – штраф в размере от 10 000 до 20 000 рублей; плюс конфискация оборудования, для юридических лиц – штраф в размере от 30 000 до 40 000 рублей; плюс конфискация оборудования [2].

При крупной сумме ущерба для правообладателя, превышающей 100 000 рублей, предусмотрено привлечение к уголовной ответственности за использование нелицензионного ПО осуществляется на основании ст. 146 УК РФ «Нарушение авторских и смежных прав». Незаконное использование объектов авторского права или смежных прав, а равно приобретение, хранение, перевозка контрафактных экземпляров произведений или фонограмм в целях сбыта, совершенное в крупном размере, влечет одно из следующих наказаний: штраф в размере до 200 000 рублей или в размере заработной платы/иного дохода осужденного за период до 18 месяцев; обязательные работы на срок до 480 часов; исправительные работы на срок до 2-х лет; принудительные работы на срок до 2-х лет; лишение свободы на срок до 2-х лет [3]

На сайте Ассоциации поставщиков программных продуктов [4] можно увидеть выборку судебных приговоров за нарушение авторских прав на программное обеспечение, причем некоторые штрафы достигают миллионов рублей. Среди нарушителей можно встретить как небольшие предприятия, так и крупные компании, заводы и даже образовательные учреждения.

Несмотря на активную борьбу с нелицензионным программным обеспечением, всё ещё существуют различные способы уйти от ответственности. На некоторых сайтах рекомендуется передача компьютерной техники в аренду или использование пароля на BIOS. На практике это не работает, так как для передачи компьютера в аренду требуется особое лицензионное соглашение с правообладателем, и если оно отсутствует, то избежать штрафа не получится. Так же считается, что факт нахождения программы на носителе является использованием программы, а в ходе проведения проверки придется сообщить государственным службам все пароли для доступа к информации на жестком диске.

В последнее время во многих предприятиях для сокрытия нелицензионных программ применяется переносной жёсткий диск. При проверке диск извлекается и комиссии показывается компьютер исключительно с официальными программами. Подробная проверка все равно покажет факт обращения операционной системы компьютера к программе со съёмного диска, но доказать вину в таком случае становится уже сложнее.

Тем не менее, обманывая правоохранительные органы с помощью подобных действий, владельцы предприятий прежде всего обманывают сами себя, так как нелицензионные программные продукты наиболее уязвимы для хакеров и кибератак. И это только одна из проблем, приводящих к недостаточной защищенности данных. Для уменьшения количества кибератак необходимо проводить регулярное тестирование оборудования, анализировать

инциденты, приводящие к нарушению безопасности работы, организовывать непрерывную защиту серверов и веб-приложений, а также постоянно повышать квалификацию сотрудников в области кибербезопасности.

Список литературы:

1. Официальный сайт МВД РФ, ссылка на электронный ресурс https://мвд.рф
2. Кодекс об административных правонарушениях, N 195-ФЗ|ст. 7.12 КОАП РФ
3. Уголовный кодекс, N 63-ФЗ | СТ. 146 УК РФ
4. Из судебной практики, http://www.appp.ru/nopirate/expirience.php
5. Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. В. С. Овчинский. – М. :Норма, 2017. – 528 с.

УДК 343.9

Саков Никита Андреевич,
Поварчук Анастасия Александровна, Шилков Михаил Михайлович,
Российский университет транспорта (МИИТ), г. Москва
Sakov Nikita Andreevich, Povarchuk Anastasia Alexandrovna,
Shilkov Mikhail Mikhailovich, Russian University of Transport (MIIT), Moscow

Королева Анна Михайловна, старший преподаватель,
Российский университет транспорта (МИИТ), г. Москва
Koroleva Anna Mikhailovna, Russian University of Transport (MIIT), Moscow

КИБЕРПРЕСТУПНОСТЬ: ПОНЯТИЕ, ВИДЫ
CYBER CRIME: CONCEPT, TYPES

Аннотация: в данной статье рассматривается тема киберпреступности. Актуальность заключается в том, что мы живем в эпоху информационного общества, когда компьютеры и телекоммуникационные системы охватывают все сферы жизнедеятельности человека и государства. Но человечество не предвидело какие возможности для злоупотребления создают эти технологии.

Abstract: this article addresses the topic of cybercrime. The relevance lies in the fact that we live in the era of the information society, when computers and telecommunication systems cover all spheres of human and state life. But mankind did not foresee what opportunities for abuse these technologies create.

Ключевые слова: киберпреступность, информационное оружие, сеть.

Keywords: cybercrime, information weapons, the Internet.

За последние время число киберпреступлений в мире существенно увеличилось, мотивы и цели киберпреступников менялись с течением времени, а опасность совершаемых преступлений возрастает с каждым годом. Этому свидетельствуют огромные финансовые потери юридических лиц и структур, а также участившиеся случаи киберпреступлений и против физических лиц.

Эту стремительно возрастающую по своим масштабам проблему необходимо как можно быстрее начать эффективно решать, потому что уровень киберпреступности и сложности преступлений растет, а раскрываемость дел и эффективность работы против преступников в киберпространстве падает.

Понятие «киберпреступности» на сегодняшний получило большое распространение в связи с информационно-телекоммуникационным прорывом, произошедшим в XXI в.

Киберпреступность – совокупность преступлений, совершаемых в «киберпространстве» с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, а также против компьютерных систем, компьютерных сетей и компьютерных данных. К «киберпреступлению» относится любое преступление, совершенное с применением различных способов и средств создания, обработки, передачи компьютерной информации [1].

Термин «киберпреступность» более расширенный, чем «компьютерная преступность», хотя иногда они употребляются вместе или как синонимы, так как «киберпреступность» – это преступность, связанная как с использованием компьютеров, так и с использованием информационных технологий и глобальных сетей, а «компьютерная преступность» относится только преступлениям, совершаемым против компьютеров или компьютерных данных [3].

Большинство преступлений, которые совершаются в глобальных компьютерных сетях, характеризуются следующими особенностями [3]:

1. Повышенная скрытность совершения преступления.
2. Трансграничный характер сетевых преступлений, при котором преступник, объект преступного посягательства и потерпевший могут находиться на территориях разных государств.
3. Особая подготовленность преступников, интеллектуальных характер преступной деятельности.
4. Возможность совершения преступления в автоматизированном режиме в нескольких местах одновременно.
5. Неосведомленность потерпевших о том, то они подверглись преступному воздействию.
6. Дистанционный характер преступных действий в условиях отсутствия физического контакта преступника и потерпевшего.
7. Невозможность предотвращения и пресечения преступлений данного вида традиционными средствами.

Сегодня киберпреступность содержит в себе обширный диапазон противоправных действий – от неразрешенного вторжения в компьютерные сети, краж индивидуальной данных до финансового шпионажа и отмывания наличных средств. Как отмечают некоторые авторы, в последние годы интернет-ресурсы используются во всех циклах торговли людьми и запрещенными предметами, а также в последующей легализации преступных доходов [2].

Субъектами преступлений, активно использующими высокие технологии, наряду с лицами, выполняющими профессиональные функции в организациях и на предприятиях, становятся практически любые лица. При этом преследуемые ими цели, используемые методы и располагаемые ими возможности практически не отличаются от тех, которые присущи преступникам по роду занятости.

Киберпреступники используют свой арсенал информационного оружия, представляющий собой совокупность средств, предназначенных для нарушения (копирования, искажения или уничтожения) информационных ресурсов на стадии их создания, обработки, распространения и хранения.

К основным видам информационного оружия относят следующие [1]:

1. Бэкдор – данный инструмент предполагает скрытый метод в системе, который позволяет получить доступ к защищенной области.

2. Компьютерные вирусы – специальные программы, которые внедряются в программное обеспечение компьютеров, уничтожают, искажают или дезорганизуют его функционирование. Они способны передаваться по линиям связи, сетям передачи данных, выводить из строя системы управления и т.п. Кроме того, “вирусы” способны самостоятельно размножаться.

3. «Логические бомбы» – программные закладные устройства, которые заранее внедряют в информационно-управляющие центры инфраструктуры, чтобы по сигналу или в установленное время привести их в действие.

4. Программное вредоносное обеспечение – программы или утилиты, которые после установки выполняет незаявленные функции в фоновом режиме.

5. Нейтрализаторы тестовых программ, обеспечивающие сохранение естественных и искусственных недостатков программного обеспечения.

6. Анализаторы трафика (sniffer) – программы или устройства, которые контролируют данные, передаваемые по сети. Традиционно используемые для законных функций сетевого управления, они могут применяться и во время кибератак с целью кражи информации.

7. DDos-атаки – предназначены для нарушения доступа к сети, как правило, при помощи выполнения миллионов запросов каждую секунду в результате чего доступ к сети затрудняется или нарушается.

8. Киберпреступления, совершаемые с помощью e-mail – это метод отправки электронной почты с подменой источника, используется для того, чтобы заставить получателя предоставить конфиденциальную информацию.

9. Keylogger – представляет собой программное или аппаратное средство, предназначенное для контроля нажатия клавиш на клавиатуре компьютера, для получения пароля, пин-кода или другой информации.

Виды киберпреступности можно классифицировать таким образом:

- Электронное и компьютерное мошенничество, кража денег с банковских счетов и карточек. Финансовая сфера является одной из самых незащищенных от киберпреступности: с развитием современных сфер коммуникации подавляющая часть денежных потоков стала носить безналичный характер, что существенно упростило преступникам совершать хищения со счетов банков и со счетов пластиковых карт обычных граждан.

- Взлом и хищение баз данный, хакерские атаки, распространение вирусов. Касаясь проблемы взлома, хищения баз данных, а также хакерских атак и распространения вирусов, следует отметить, что проблемами предотвращения данных видов угроз является невозможность прогнозирования потенциальных проблем, использование идентичного ПО в различных устройствах, что увеличивает эффективность эксплуатации технических уязвимостей, а также нехватка кадров в области киберзащиты.

- Незаконная слежка и прослушивание телефонов, вторжение в частную жизнь. Незаконное вторжение в частную жизнь получает наибольшее распространение с каждым годом: люди по всему миру пользуются современными гаджетами, а они в свою очередь могут рассказать преступнику, как местоположения пользователя, так и более личную и конфиденциальную информацию. Таким видом преступления пользуются не только вымогатели, но отделы маркетинга компаний, которые отслеживая личную информацию потенциального потребителя, строят анализ его предпочтений, таким образом выстраивая целевую рекламу и занося информацию о нем в свои базы данных.

- Присвоение интеллектуальной собственности. Незаконное присвоение интеллектуальной собственности также является распространенным видом киберпреступности, так как с развитием IT технологий (как следствие и развития киберпреступности), создатели интеллектуальной собственности, которая подвергается опасности со стороны киберпреступлений, как правило, не могут воспользоваться экономическими плодами своей собственной работы, тем самым подрывая стимулы к осуществлению необходимых инвестиций в развитие своего продукта, а также создатель интеллектуальной собственности будет находиться в невыгодном положении по отношению к тому, кто просто скопировал его наработки, так как создатель вкладывал в разработку идеи финансы и время.

В связи со стремительным развитием информационных технологий, киберпреступность расширилась и включает в себя на сегодня новые серьезные угрозы, такие как: [4]

- Кибертерроризм;
- сетецентрическая война;
- кибервойн.

Угроза кибертерроризма может исходить от террористических и экстремистских организаций, отличается большой масштабностью, интенсивностью и огромными последствиями.

Сетецентрическая война и кибервойна, в тактике и искусстве войны за последнее время произошли принципиальные перемены, требующие от правительств государств пересмотра прежних военных доктрина, переоценки области военного искусства, эти войны принципиально новые виды ведения войн против государств, которые требуют особого подхода и противодействия.

Переходя к развитию киберпреступности, можно сделать вывод: преступления в Сети наиболее новая и динамично развивающая сфера деятельности для злоумышленников. Формы киберпреступности видоизменяются и распространяются на все новые достижения научно-технического прогресса. Повышенное внимание направлено на социальные сети и мобильные устрой-

ства – область, в которой пользователи менее информированы о киберугрозах. Хакерские атаки стали более сложными и профессиональными, направленными не только на отдельных пользователей, но и промышленные системы.

Список литературы:

1. Глотина И.М. Киберпреступность: Основные проявления и экономические последствия // Вопросы экономики и права. – 2014. – №8. – 12 с.
2. Морозов Н.А. Борьба с компьютерной преступностью в Японии // Общество и право. – 2014. – № 2 (48). – 141 с.
3. Сериева М. М. Киберпреступность как новая криминальная угроза // Новый юридический вестник. – 2017. – №1. – 104-106 с.
4. Головинов О. Киберпреступность в современной экономике: состояние и тенедеции развития // Вопросы инновационной экономики – 2016. – Т. 6. – №1– 79 с.

НБ ВОПРОСЫ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ

УДК 159.9.07

Медовикова Евгения Александровна, к.психол.н.
ФГБОУ ВО «Кемеровский государственный университет» г. Кемерово
Medovikova Evgenia Alexandrovna,
Kemerovo State University, Kemerovo

РОЛЬ ЛИЧНОСТИ В РАМКАХ РЕШЕНИЯ ПРОБЛЕМЫ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ТРУДА И ОХРАНЫ ЗДОРОВЬЯ НА ПРЕДПРИЯТИЯХ УГОЛЬНОЙ ПРОМЫШЛЕННОСТИ *

THE ROLE OF PERSONALITY IN THE FRAMEWORK OF SOLVING THE PROBLEM OF INCREASING LABOR SAFETY AND HEALTH PROTECTION AT THE ENTERPRISES OF THE COAL INDUSTRY

***Работа выполнена при финансовой поддержке РФФИ, в рамках научно-исследовательского проекта 20-413-420003/20 р_а «Обеспечение безопасности труда и охраны здоровья сотрудников предприятий угольной промышленности Кузбасса: социально-психологические факторы, превентивные меры снижения рисков травматизма»**

Аннотация: безопасность жизнедеятельности имеет важное значение в современном мире. В основе производственной деятельности лежит человеческий фактор, который раскрывает суть индивидуально-типологических особенностей личности. На предприятиях угольной промышленности всегда был высок риск производственной деятельности, но если раньше его напрямую связывали с работой машин и механизмов, то сейчас особое значение уделяется личностному компоненту.

Abstract: life safety is important in the modern world. The basis of production is the human factor, which reveals the essence of the individual typological characteristics of the individual. At the enterprises of the coal industry there has always been a high risk of production activity, but if earlier it was directly associated with the operation of machines and mechanisms, now special importance is given to the personal component.

Ключевые слова: психологическая безопасность, субъект труда, психологическое состояние, сознание, потенциальные опасности.

Keywords: psychological safety, subject of labor, psychological state, consciousness, potential dangers.

Предприятия угольной промышленности на региональном уровне сталкиваются с рядом проблем, одной из которых является вопрос реализации программ сопровождения психологической безопасности. Вопрос в том, что программы должны иметь комплексный характер, включая вопросы медицинской, социальной, психологической и информационной помощи. Те программы, которые имеют определенную степень реализации в рамках регионального аспекта не обеспечивают в полной мере нейтрализацию объективных и субъективных рисков в производственном процессе. Чрезмерная высокая нагрузка производственных мощностей в угольной промышленности отрицательно сказывается на состоянии условий труда, охраны труда и промышленной безопасности. В связи с чем угольная отрасль характеризуется одним из самых высоких уровней травматизма в мире. Целью обзора данной проблематики, является необходимость осветить проблемы психологии безопасности, связанные с личностным фактором, в связи с чем можно будет прогнозировать сложные ситуации на рабочем месте и в рамках социального пространства, что позволит снизить уровень травматизма на предприятиях.

Если рассматривать само понятие «безопасность», то оно чаще трактуется через ряд признаков, которые отражают состояние стабильности личности. Это состояние характеризуется степенью защищенности от различного рода угроз и опасностей, которые оказывают разрушающее воздействие на структурную (изменение сознания) и функциональную целостность (психофизиологический аспект) субъекта производственной деятельности [1]. Развитие личностных качеств, обеспечивающих сопротивление деструктивным факторам среды, и учет их значения в производственной сфере имеет важное значение. Однако, вопрос изучения и диагностики личностных характеристик, которые определяют успешность преодоления субъектом ситуаций неопределенности в профессиональной деятельности, до сих пор окончательно не решен в психологической науке и практике. Например, Г. В. Грачев определяет важную роль такого компонента психологической защиты личности, как психологическая самозащита. С. Мадди особое внимание уделяет такой черте личности, как жизнестойкость, которая взаимосвязана с личностным ростом и позволяет справляться с дистрессом в рамках производственных отношений. В. И. Кабрин рассматривал личностные изменения со стороны транскоммуникативного потенциала, включающего в себя особенности личностного роста и борьбу с коммуникативным стрессом. В связи с чем можно сказать, что в основе

психологической безопасности личности совокупность психических свойств и состояний, а также способов реагирования на внешние обстоятельства, что имеет динамическую тенденцию и обеспечивает в итоге эффективное взаимодействие личности с окружающей средой, в основе которой лежит производственная деятельность [2].

Вопрос решения проблемы психологической безопасности в рамках трудовой деятельности включает в себя моменты минимизации отрицательного воздействия факторов, которые несут угрозу психологическому состоянию личности, со стороны профессиональной среды, а также повышению уровня эффективности коммуникации в организационной структуре и выработке механизмов личностной защиты от негативного влияния совокупности факторов. Таким образом, психологическая безопасность личности и безопасность среды представляют собой два взаимосвязанных компонента. Производственные процессы в организационной структуре оказывают влияние на психологическое благополучие личности. Важными показателями психологической безопасности среды являются степень удовлетворенности условиями взаимодействия внутри коллектива, наличие профессионально-важных качеств личности, что определяет ее субъективное благополучие в рамках производственного процесса.

На основе анализа научных источников можно выделить основные деструктивные факторы социальной среды организации, влияющие на психологическую безопасность субъекта труда.

Первая группа факторов взаимосвязана с нарушениями в сфере охраны труда. К данной группе относятся такие компоненты, как напряженность трудовой деятельности, нарушение норм и условий труда, низкий уровень или полное отсутствие внимания к вопросам безопасности труда на предприятиях, индивидуально-типологические особенности личности (темперамент, характер). При этом необходимо отметить, что работники угольных предприятий стоят перед сложным выбором: с одной стороны, беспрекословное выполнение плана, с другой, четкое соблюдение правил техники безопасности в рамках производственного процесса [3]. Необходимо отметить, что в рамках анализа данного фактора имеет значение определение особенностей нервной системы сотрудников угольных предприятий. Согласно проведенному анализу личностных особенностей работников угольных предприятий Юга Кузбасса получены следующие данные по тесту темперамента В. М. Русалова: в общей выборке 100 человек большую часть представляют собой личности с сильным типом нервной системы (сангвиник (45%) и холерик (35%)), что обусловлено сложностью работы в условиях неопределенности, риска.

Вторая группа факторов связана с нарушениями межличностного взаимодействия в процессе осуществления трудовой деятельности. В данную группу относятся такие компоненты, как неблагоприятный психологический климат в микрогруппах, затяжные или бурнопротекающие конфликты в коллективе, низкий уровень доверия и эмпатии членов коллектива друг к другу, отсутствие взаимовыручки, чрезмерная конкуренция, моббинг и буллинг, стиль руководства коллективом, наличие психологически сложного контингента, с которым необходимо контактировать при осуществлении профессиональной

деятельности [4]. По данным анкеты, предложенной работникам угольной отрасли из общего числа работников (100 человек) выявлено, что большинство опрашиваемых 62 % оценивают атмосферу в трудовом коллективе как дружескую. Этот момент логичен так как в работе в сложных условиях важен дух коллективизма и формирование команды.

Третья группа факторов, определяется веянием современных тенденций на весь производственный процесс и связанна с информационным стрессом во время осуществления профессиональной деятельности, высоким уровнем тревожности личности в производственных условиях. Излишний или недостаточный объем информации оказывает напрямую деструктивное воздействие на личность, провоцируя стрессовые состояния, чувство тревожности субъекта труда, снижение степени адаптированности в производственных условиях [5]. По результатам методики «Оценка уровня реактивной и личностной тревожности» (Ч. Д. Спилберг, Ю. Л. Ханин) получены следующие данные: *70%* респондентов, отметили умеренный уровень реактивной тревожности, что характеризуется субъективно переживаемыми эмоциями: напряжением, беспокойством, озабоченностью, нервозностью связанной с данной конкретной ситуацией. *68 %* рабочих отметили умеренный уровень личностной тревожности. Личная тревожность активизируется при восприятии определенных стимулов, расцениваемых работником как опасные для самооценки, самоуважения. Личности, относимые к категории умеренно – тревожных, не склонны воспринимать угрозу своей жизнедеятельности в обширном диапазоне ситуаций и реагировать весьма выраженным состоянием тревожности. Тем не менее личностная тревожность является важным аспектом для изучения, т.к. она снижает степень эффективности личности в сложных условиях жизнедеятельности.

Если говорить об общих причинах травматизма на предприятиях угольной промышленности, то в результате исследования можно отметить следующие. В качестве основной причины нарушений правил техники безопасности на производстве респонденты отметили, что в процессе работы забывают о необходимости соблюдения правил техники безопасности и невнимательны в процессе выполнения производственных заданий – 56%, причем это не связано ни с возрастом, ни со стажем, ни с уровнем образования работников. Другая часть респондентов видит причины нарушения техники безопасности в нарушении дисциплины в бригаде и постоянного увеличения темпа выполнения деятельности – 18 %. 8 % отмечают, что они не усвоили правила техники безопасности и всего лишь 6% работников угольной сферы заявляют о соблюдении правил техники безопасности на рабочем месте в процессе трудовой деятельности.

Таким образом, определяя личностный компонент психологии безопасности труда, важно учитывать индивидуально-типологические особенности личности, проявляющиеся в профессиональной сфере и оказывающие влияние на поведение личности в ситуации опасности. Поведение определяется, с одной стороны, личными качествами члена производственного коллектива, с другой стороны – факторами среды, влияющими на его состояние. Выявление взаимосвязи между личностными качествами и психологией безопасности

труда способствует выстраиванию эффективной системы отбора персонала, подготовке человека к работе в условиях повышенного риска и неопределенности. Факторы, влияющие на психику человека в процессе профессиональной деятельности, должны учитываться при разработке мероприятий по психокоррекции и психогигиене. Психосоциальный аспект безопасности необходимо принимать во внимание при организации и управлении всем производственным процессом.

Список литературы:

1. Коропец, О. А. Психологическая безопасность личности в профессиональной деятельности / О. А. Коропец // Современное общество и власть. – 2017. – 2(12). – С. 21-24.

2. Лазарева, А. Ю. Психологическая безопасность личности / Ю.А. Лазарева // Форум молодых ученых. – ООО «Институт управления и социально-экономического развития» (Саратов), 2019. – 4 (32). – С. 646-649.

3. Медовикова, Е. А., Мороденко Е. В. Значение психологии безопасности в рамках профессиональной деятельности на угольных предприятиях Кузбасса / Е. А. Медовикова, Е. В. Мороденко // Горный информационно-аналитический бюллетень. –2018. – № 10. – С. 219–226. DOI: 10.25018/0236-1493-2018-10-0-219-226

4. Мороденко, Е. В. Анализ социально-психологического климата трудового коллектива на предприятиях угольной промышленности Кемеровской области / Е. В. Мороденко, Е. А. Медовикова // Вестник КемГУ. – 2015. – № 2 (62), Т. 1. – С. 135-137.

5. Уваров, В. И. Социально-психологическая безопасность личности: влияние внешних и внутренних факторов // Современная психология: материалы V Междунар. науч. конф. (г. Казань, октябрь 2017 г.). – Казань: Бук, 2017. – С. 19-25. – URL https://moluch.ru/conf/psy/archive/254/12925/ (дата обращения: 16.03.2020)

УДК 622.44
DOI 10.37539/NB185.2020.21.76.014

Серегин Александр Сергеевич, к.т.н., доцент кафедры безопасности производств, Санкт-Петербургский горный университет, г. Санкт-Петербург
Seregin Alexandr Sergeevich, Saint Petersburg Mining University, Saint-Petersburg

Фещенко Екатерина Андреевна, к.т.н., ассистент кафедры безопасности производств, Санкт-Петербургский горный университет, г. Санкт-Петербург
Feshchenko Ekaterina Andreevna,
Saint Petersburg Mining University, Saint-Petersburg

Иконников Дмитрий Андреевич, к.т.н., доцент кафедры безопасности производств, Санкт-Петербургский горный университет, г. Санкт-Петербург
Ikonnikov Dmitry Andreevich, Saint Petersburg Mining University, Saint-Petersburg

НОРМАТИВНО-ПРАВОВЫЕ АСПЕКТЫ УСТАНОВЛЕНИЯ НОРМЫ РАСХОДА ВОЗДУХА ДЛЯ ПРОВЕТРИВАНИЯ ГОРНЫХ ВЫРАБОТОК ПРИ ИСПОЛЬЗОВАНИИ МАШИН С ДИЗЕЛЬНЫМ ДВИГАТЕЛЕМ
REGULATORTORY AND LEGAL ASPECTS OF SETTING AIR FLOW IN MINE WORKINGS WITH OPERATION OF DIESEL ENGINES

Аннотация: рассмотрен аспект обязательного характера применения отдельных нормативных правовых актов в вопросах проветривания горных выработок угольных шахт России при эксплуатации машин с дизельными двигателями.

Abstract: the article discusses the aspect of obligatory usage of some normative legal acts in the ventilation of coal mine workings in Russia during the operation diesel engines.

Ключевые слова: нормативные правовые акты, вентиляция, угольные шахты, дизельный двигатель.

Keywords: regulations, ventilation, coal mines, diesel engine.

Бурное развитие технологий и техники для добычи полезных ископаемых, в частности каменного угля, в последние десятилетия обуславливают необходимость актуализации нормативной документации, касающейся, в том числе, требований безопасности. Так, за последние 20 лет Правила безопасности в угольных шахтах были полностью пересмотрены дважды.

Тем не менее, не вся нормативная база подвергалась пересмотру. Так, Технические требования по безопасной эксплуатации транспортных машин с дизельным приводом в угольных шахтах. РД 05-312-99 (вместе с «Инструкцией по расчету вентиляции выработок, обслуживаемых транспортными машинами с дизельным приводом»), утв. Постановлением Госгортехнадзора РФ от 30.09.1999 N 71 (далее – РД 05-312-99) [1] в части вопросов вентиляции полностью повторяют заменные ими «Временные нормы и технические требования для безопасной эксплуатации дизельных локомотивов (машин) в угольных шахтах (МакНИИ, 1975)».

Таким образом, требования к проветриванию горных выработок при эксплуатации машин с дизельными двигателями не меняются с 70-х годов прошлого столетия. В тоже время новые технические решения позволили сделать работу дизельных двигателей более экологичной за счет применения более чистого топлива, более точного смесеобразования (аккумуляторных систем впрыска топлива), повсеместного использования устройств каталитической нейтрализации выхлопных газов и др. К современным горным машинам с дизельным приводом предъявляются строгие стандарты по количеству и качеству выхлопных газов такие как Stage V/ Tier 5 [2]. Согласно стандарту Tier 5 выхлопные газы дизель-гидравлических машин должны содержать не более 5 г/(кВт□ч) угарного газа, в то время как машины стандарта Tier 1, принятого в 1996 году могли выбрасывать 11,4 г/(кВт ч). Снижение удельного содержания вредных веществ, выделяющихся в составе выхлопных газов, позволяет уменьшить расход воздуха, подаваемого в горную выработку для проветривания.

Однако, пунктом 3.2 РД 05-312-99, закреплен минимальный расход свежего воздуха, подаваемого в выработки и на участки, по которым проходят маршруты движения транспортных машин с дизельным приводом, который составляет 5 $м^3$/мин на каждую л.с. номинальной мощности дизельных двигателей. С учетом того, что применяемые дизельные двигатели становятся не только экологичнее, но и мощнее, угольные шахты вынуждены затрачивать дополнительные средства для проветривания поддерживаемых горных выработок, а в некоторых ситуациях ограничивать доступ монорельсовых локомотивов в проходческие забои.

Сложившаяся ситуация в долгосрочной перспективе может привести не только к снижению конкурентоспособности российских угольных шахт, но и составлять угрозу энергетической безопасности, а значит и национальной безопасности.

Для решения вопроса уменьшения установленной нормы расхода воздуха в первую очередь необходимо убедиться, что рассматриваемое требование носит обязательный характер.

В соответствии с ч. 3 ст. 15 Конституции РФ все законы, а также любые нормативные акты, затрагивающие права, свободы и обязанности человека и гражданина, должны быть официально опубликованы для всеобщего сведения. Этот принцип послужил основой для принятия актов, определивших порядок опубликования и вступления в силу нормативных правовых актов (далее – НПА). Указом Президента РФ от 23.05.1996 N 763 «О порядке опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти» [3] установлено, что нормативные правовые акты федеральных органов исполнительной власти, затрагивающие права, свободы и обязанности человека и гражданина, устанавливающие правовой статус организаций или имеющие межведомственный характер, прошедшие государственную регистрацию в Министерстве юстиции Российской Федерации, подлежат обязательному официальному опубликованию, кроме актов или отдельных их положений, содержащих сведения, составляющие государственную тайну, или сведения конфиденциального характера. Пункт 10 того же

указа говорит о том, что вышеупомянутые НПА, не прошедшие государственную регистрацию, а также зарегистрированные, но не опубликованные в установленном порядке, не влекут правовых последствий, как не вступившие в силу, и не могут служить основанием для регулирования соответствующих правоотношений, применения санкций к гражданам, должностным лицам и организациям за невыполнение содержащихся в них предписаний.

В соответствии с Указом Президента РФ от 23.05.1996 N 763 в редакции от 13.08.1998, действовавшей на момент выхода РД 05-312-99, источниками официального опубликования НПА являлись «Российская газета» и Бюллетень нормативных актов федеральных органов исполнительной власти издательства «Юридическая литература» Администрации Президента Российской Федерации.

РД 05-312-99 утверждены Постановлением Госгортехнадзора РФ от 30.09.1999 N 71 и введены в действие постановлением Госгортехнадзора России от 19.06.2000 N 35. Источник публикации: «Безопасность горнотранспортного оборудования угольных шахт» (сборник документов), выпуск 10 (часть 2), М., ГП «НТЦ по безопасности в промышленности Госгортехнадзора РФ», 2000. Государственную регистрацию не проходили.

Приказом Ростехнадзора от 10.07.2017 N 254 [4] утвержден перечень нормативных правовых актов и нормативных документов, относящихся к сфере деятельности Федеральной службы по экологическому, технологическому и атомному надзору. Данный документ представляет собой информационно-справочный сборник, предназначенный для информирования должностных лиц Ростехнадзора, других федеральных органов исполнительной власти, юридических лиц и индивидуальных предпринимателей о нормативных правовых актах и нормативных документах, действующих в установленной сфере деятельности Ростехнадзора по указанным выше вопросам. В п.6 приказа указано: «при проведении проверки должностные лица Ростехнадзора не вправе проверять выполнение в том числе и обязательных требований и требований, установленных муниципальными правовыми актами, не опубликованными в установленном законодательством Российской Федерации порядке».

Помимо всего вышесказанного, приказом Ростехнадзора от 17.10.2016 N 421 [5] рассматриваемый РД 05-312-99 не отнесен к перечню документов, обязательных к исполнению, и не оценивается при проведении контроля со стороны надзорных органов.

Вывод:

Таким образом, РД 05-312-99 в данный момент носит рекомендательный характер и, если в локальных нормативных актах предприятия не приводится ссылка на рассматриваемый документ, его исполнение не оценивается при проведении контроля со стороны Ростехнадзора. В таком случае, увеличение мощности дизельных двигателей в эксплуатируемых машинах при соблюдении установленных норм по удельному содержанию вредных веществ в выхлопных газах позволяет сохранить на том же уровне или даже снизить расход свежего воздуха, подаваемого для проветривания горных выработок угольных шахт без нарушения требований безопасности.

Список литературы:

1. «Технические требования по безопасной эксплуатации транспортных машин с дизельным приводом в угольных шахтах. РД 05-312-99» (утв. Постановлением Госгортехнадзора РФ от 30.09.1999 N 71) (вместе с «Инструкцией по расчету вентиляции выработок, обслуживаемых транспортными машинами с дизельным приводом»).

2. Регламент N 2016/1628 Европейского парламента и Совета Европейского Союза «О требованиях в отношении пределов выбросов газообразных и твердых загрязняющих веществ, об одобрении типа для двигателей внутреннего сгорания, установленных на недорожной технике, а также об изменении Регламентов (ЕС) 1024/2012 и (ЕС) 167/2013, и об изменении и отмене Директивы 97/68/ЕС» [рус., англ.] (вместе с «Определением подкатегорий двигателей...», «Пределами выбросов выхлопных газов...», «Сроками применения настоящего Регламента...», «Периодами устойчивости характеристик выбросов (EDP)...», «Значениями пределов выбросов двигателей для специальных целей (SPE)...»).

3. Указ Президента РФ от 23.05.1996 N 763 «О порядке опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти».

4. Приказ Ростехнадзора от 10.07.2017 N 254 «Об утверждении Перечня нормативных правовых актов и нормативных документов, относящихся к сфере деятельности Федеральной службы по экологическому, технологическому и атомному надзору (раздел I «Технологический, строительный, энергетический надзор») П-01-01-2017».

5. Приказ Ростехнадзора от 17.10.2016 N 421 «Об утверждении перечней правовых актов, содержащих обязательные требования, соблюдение которых оценивается при проведении мероприятий по контролю в рамках осуществления видов государственного контроля (надзора), отнесенных к компетенции Федеральной службы по экологическому, технологическому и атомному надзору» (вместе с «Порядком ведения перечней правовых актов и их отдельных частей (положений), содержащих обязательные требования, соблюдение которых оценивается при проведении мероприятий по контролю в рамках осуществления видов государственного контроля (надзора), отнесенных к компетенции Федеральной службы по экологическому, технологическому и атомному надзору»).

НБ ЭКОНОМИЧЕСКИЕ АСПЕКТЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

УДК 334.723

Митяшин Глеб Юрьевич, Санкт-Петербургский политехнический университет Петра Великого, г. Санкт-Петербург
Mityashin Gleb Yurievich,
Peter the Great St. Petersburg Polytechnic University, Saint-Petersburg

КОНТРАКТ ЖИЗНЕННОГО ЦИКЛА: ДОСТОИНСТВА И РИСКИ
LIFE CYCLE CONTRACT: ADVANTAGES AND RISKS

Аннотация: в данной работе автором описывается правовое поле и финансовое взаимодействие стейкхолдеров при реализации КЖЦ, приводятся преимущества и недостатки данной формы взаимодействия, а также предлагаются возможные способы модернизации КЖЦ.

Abstract: in this paper the author describes the legal field and financial interaction of stakeholders in the implementation of the LCC, provides advantages and disadvantages of this form of interaction, and suggests possible ways to modernize the LCC.

Ключевые слова: контракт жизненного цикла, КЖЦ, контрактная система государственных закупок, совокупная стоимость владения, ТСО, ГЧП.

Keywords: life cycle contract, LCC, the contract system of public procurement, total cost of ownership, TCO, PPP.

В настоящее время существует большое количество разновидностей государственно-частного партнерства (ГЧП), адаптированных для решения разного рода задач и соответствующих различным потребностям государства и частного оператора [2-4, 6, 8, 11, 14]. Одной из таких разновидностей является контракт жизненного цикла (КЖЦ) [7]. В рамках такого контракта частная компания не только создает необходимый для государства продукт (чаще всего – сложное транспортное оборудование или объекты транспортной инфраструктуры), но и обеспечивает его надлежащее функционирование в течение всего жизненного цикла.

Мы выполним обзор преимуществ и недостатков применения КЖЦ с точки зрения ключевых стейкхолдеров (государства и частного оператора) и предложим пути решения некоторых проблем КЖЦ.

Ффинансовое взаимодействия между стейкхолдерами реализуется посредством аннуитетных платежей. Государство выплачивает оператору равные суммы денег на протяжении всего контракта, с периодичностью, установленной договором. Такой подход является удобным для обеих сторон. Для государства (муниципалитета) облегчается бюджетное планирование, так как инфраструктурные объекты всегда дорогостоящие, а распределение их стоимости на

длительный период снижает нагрузку на бюджет, позволяя избежать больших единовременных выплат. Для частного партнера данный механизм решает две важные задачи. Во-первых, он, в соответствии с природой аннуитетных платежей, позволяет частному оператору гарантированно получить возмещение своих инвестиций с определенной нормой доходности. Во-вторых, поскольку объект, создаваемый и управляемый в рамках КЖЦ, создается под заказ государства (муниципалитета), частный оператор не привязан к колеблющемуся спросу, а получает гарантированный регулярный доход. То есть, он может сконцентрироваться исключительно на качественном предоставлении услуги, так как поток доходов определен договором заранее [11].

Следующим важным критерием реализации КЖЦ является актуальность и доступность нормативной базы. Применение КЖЦ в России регламентируется следующими нормативными актами: №44-ФЗ «О контрактной системе...» [12] и постановление правительства РФ № 1087 [10]. 44-ФЗ описывает суть контрактов жизненного цикла, определяет область их применения, механизмы реализации, подчеркивает равенство обоих стейкхолдеров и достаточно полно описывает то, что связано с КЖЦ. С момента выхода постановления правительства РФ №1087 (28.11.2013) было внесено порядка 7 дополнений, которые значительно расширили сферу заключения КЖЦ. В настоящее время их можно применять не только к транспорту, но и к объектам здравоохранения, памятникам и объектам культурного наследия, модернизации военно-промышленного комплекса. Таким образом, правительство модернизирует и расширяет нормативную базу, что говорит о привлекательности системы КЖЦ для государства [1, 10, 12].

Для наглядности нами предлагается таблица 1, отражающая основные преимущества КЖЦ для каждого из стейкхолдеров.

Таблица 1

Преимущества КЖЦ

Для государства	Для частного партнера
1. Облегчение бюджетного планирования 2. Экономия средств на организации тендеров 3. Экономия средств на управлении объектом 4. Получение инфраструктуры высокого качества	1. Независимость дохода от спроса на услуги 2. Долгосрочное финансирование

Несмотря на удобное для обоих стейкхолдеров финансовое взаимодействие и на актуализацию нормативной базы, КЖЦ также имеют ряд рисков:

1. Риск неправильного определения стоимости объекта;
2. Риски некорректного формирования экономической модели;
3. Риски некорректного прогнозирования потока расходов.

Ключевым риском является неправильное построение экономической модели. Это обусловлено сложностью прогнозирования потока расходов для объекта длительного пользования. Так как все операционные доходы должен нести представитель бизнеса, то при построении экономической модели будет целесообразно использовать разные подходы к управлению жизненным циклом

объекта [12, 13]. Одним из таких подходов является совокупная стоимость владения (Total Cost of Ownership, TCO) – сумма затрат, которые владелец вынужден нести с момента начала разработки проекта, во время его строительства, эксплуатации и ликвидации. В рамках этой концепции происходит перераспределение затрат за счет увеличения инвестиций на начальном этапе (что позволяет повысить качество объекта) и снижения операционных затрат на стадии эксплуатации. Основным тезисом данной концепции является увеличение финансирования на этапе проектирования и строительства объекта, что приведет к снижению затрат на этапе его эксплуатации. Затраты на строительство объекта составляют лишь 25% от его полной стоимости, а 75% приходится на операционные затраты (заработная плата сотрудников, электроэнергия, ремонт и замена оборудования и т.д.) [5, 13].

TCO позволяет строить более точную экономическую модель проекта. Это позволяет рекомендовать TCO в качестве инструмента управления финансовыми отношениями участников ГЧП.

Список литературы:

1. Егоров Е.С. Минина И.С. Правовое регулирование государственно-частного партнерства в России и за рубежом // Государственное управление. Электронный вестник. – 2018. – № 3. – С. 294-311.

2. Котляров И. Д. Применение аутсорсинга в государственной деятельности в Российской Федерации // Вопросы государственного и муниципального управления. – 2012. – № 2. – С. 112-120.

3. Котляров И. Д. Организация эффективного военно-гражданского сотрудничества // Ресурсное обеспечение силовых министерств и ведомств: вчера, сегодня, завтра. Сборник статей II Международной научно-практической конференции. Пермь: Пермский военный институт войск Национальной гвардии Российской Федерации, 2016. – С. 177-181.

4. Курбанов А. Х., Плотников В. А. Государственно-частное партнерство и аутсорсинг: сравнительный анализ структуры и характера отношений // В мире научных открытий. – 2013. – № 4. – С. 33-47.

5. Митяшин Г. Ю., Стельмашонок Е. В. Применение концепции совокупной стоимости владения к анализу жизненного цикла спортивного сооружения // Экономика и предпринимательство. – 2020. – № 4. – С. 747-751.

6. Мочальников В. Государственно-частное партнерство в стратегии социально-экономического развития России // Вестник Института экономики РАН. – 2010. – № 1. – С. 55-76.

7. Никитин Ю. А., Васильев Н. И., Детков Г.Б. Особенности контракта жизненного цикла // Теория и практика сервиса: экономика, социальная сфера, технологии. – 2019. – № 2 (40). – С. 33-41.

8. Плотников В. А., Вертакова Ю. В. Частно-государственное партнерство в организации профессионального образования в интересах российской промышленности // Экономика и управление. – 2012. – № 11. – С. 36-40.

9. Плотников В. А., Федотова Г. В., Пролубников А. В. Государственно-частное партнерство и специфика его реализации в регионах России // Экономика и управление. – 2015. – № 1. – С. 38-43.

10. Постановление 1087 // www.consultant.ru [Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_155054/ (дата обращения: 27.05.2020).
11. Ракута Н. В. Использование контрактов жизненного цикла при госзакупках. Опыт развитых стран // Вопросы государственного и муниципального управления. – 2015. – № 2. – С. 53-78.
12. ФЗ-44 // www.consultant.ru [Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_144624/ (дата обращения: 27.05.2020).
13. Эрнст энд Янг // https://www.ey.com/ru [Электронный ресурс] URL: https://www.ey.com/ru_ru (дата обращения: 27.05.2020).

УДК 330

Осмонова Айнур Анваровна,
доктор экономических наук, профессор Кыргызско-Российского Славянского университета, г. Бишкек, Кыргызская Республика
Osmonova Ainur Anvarovna, Russian Slavic University, Bishkek, Kyrgyzstan

Эмирова Алтынай Эмировна, Американский университет стран Центральной Азии, г. Бишкек, Кыргызская Республика
Emirova Altynai Emirovna,
American University of Central Asia, Bishkek, Kyrgyzstan

Сепетерова Алина Андреевна, Кыргызско-Российский Славянский университет им. Б.Н. Ельцина, г. Бишкек, Кыргызская Республика
Sepeterova Alina Andreevna,
Kyrgyz-Russian Slavic University n.a. B.N. Yeltsin, Bishkek, Kyrgyzstan

АНАЛИЗ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ КОМПАНИИ КАК ГАРАНТИЯ ЕЕ ФИНАНСОВОЙ ЗАЩИЩЕННОСТИ
ANALYSIS OF THE ECONOMIC SECURITY OF THE COMPANY AS A WARRANTY OF ITS FINANCIAL SECURITY

Аннотация: в статье проанализированы подходы в определению термина «экономическая безопасность компании», рассмотрены факторы и условия обеспечения экономической безопасности компании в условиях современного рынка, а также выделены наиболее оптимальные методы анализа экономической безопасности.

Abstract: the article shows the analysis of the approaches to define the “economic security of a company” term, factors and conditions for ensuring the economic security of a company in a modern market are considered, the most optimal methods of analyzing economic security are identified.

Ключевые слова: экономическая безопасность, анализ рисков, информационно-учетное обеспечение, анализ.

Keywords: economic security, risk analysis, information and accounting support, analysis.

Необходимость анализа экономической безопасности компании обусловлена тем, что в условиях современной экономики компания на протяжении всего своего жизненного цикла подвергается различным внешним и внутренним рискам, а конкурентная рыночная среда только усиливает многочисленные угрозы. Проблема экономической безопасности компании касается не только ее собственников и сотрудников, а также её клиентов, партнеров и акционеров. Поэтому перед управленческими структурами компании все более актуализируется необходимость построения целостной системы по обеспечению охраны финансовых ресурсов, защиты коммерческой информации и имущества компании. Нынешняя ситуация на внутреннем и мировом рынках характеризуется сложностью коммерческих схем, использованием интегрированных продуктов, усилением конкуренции между компаниями. Управление денежными и финансовыми потоками, а также ресурсами и персоналом компании становятся все более трудной задачей, которая напрямую связана с увеличением документооборота и повышением стремительности информационных потоков. Эти факторы увеличивают экономические риски, остающиеся на довольно высоком уровне. Причиной создания такой ситуации может являться плохой менеджмент, а вследствие чего слабая кадровая политика.

В экономической литературе единого мнения относительно значения термина «экономическая безопасность» нет. Однако принято выделять два наиболее распространенных подхода к определению экономической безопасности. Первый подход рассматривает экономическую безопасность компании как определенное состояние экономической системы без ссылок на какие-либо угрозы. Данного мнения придерживаются такие ученые, как О. Грунин, А. Кашин, В. Пономарев и другие. Второй подход заключается в понятии экономической безопасности как обеспечения сохранения коммерческой тайны и защиты информации. Данный подход характерен для российских ученых 90-х годов, среди которых можно выделить А. Шаваева и В. Ярочкина. На мой взгляд, наиболее точное определение экономической безопасности дает Меламедов С. Л.: «под экономической безопасностью предпринимательской структуры будем понимать защищенность ее жизненно важных интересов от внутренних и внешних угроз, т. е. защита предпринимательской структуры, ее кадрового и интеллектуального потенциала, информации, технологий, капитала и прибыли, которая обеспечивается системой мер специального правового, экономического, организационного, информационно-технического и социального характера» [0].

Понятие «экономической безопасности» в Кыргызской Республике является сравнительным новым. В законодательстве Кыргызской Республики не давалось определения понятию «безопасность» до 2001 года, и только с принятием «Концепции национальной безопасности Кыргызской Республики» появилось нормативное определение этому термину. Принятие данной Концепции заложило основы в рамках национальной безопасности, а также затронуло проблемы обеспечения экономической безопасности.

Если рассматривать отношение к экономической безопасности в мире, то значительное количество стран сосредоточено на разработке теоретических и

прикладных основ повышения экономической безопасности компании и формировании основ для благоприятной бизнес-среды. Наибольших результатов в этом направлении добились предприниматели из Германии, США и Японии. В таблице 1 приведены отличительные черты обеспечения экономической безопасности компаний в разных странах.

Таблица 1

Особенности обеспечения экономической безопасности компаний в развитых странах [2]

Страна	Меры по обеспечению экономической безопасности предприятий	
	На макроуровне	На микроуровне
Германия	- правительством созданы национальные спецслужбы для контроля за ситуацией на экономически важных объектах страны; - население своим гражданским долгом считает необходимым проинформировать соответствующие органы о правонарушениях и получить за это должное вознаграждение.	- частные агентства помогают в получении оперативно-значащей информации о совершенных или планируемых правонарушениях; - сотрудники спецслужб и детективных агентств осуществляют постоянный мониторинг ситуации на совместных предприятиях и изучают поведение иностранных граждан по соблюдению ими требований закона и интересов бизнеса.
Япония	- государство учитывает интересы бизнеса и пытается предусмотреть вероятные ответные меры руководства конкурентов, а также реакцию внутренних и зарубежных ТНК, на те или иные решения; - экономическая разведка основана на эффективном распределении ролей между большим числом организаций ориентированных на экспорт.	- отсутствие законов, предусматривающих ответственность за разглашение коммерческой тайны, что связано с воспитанием у сотрудников чувства патернализма, они считают себя членами одной семьи; - на отдел кадров, имеющихся в каждой японской фирме, возлагается контроль за неукоснительным соблюдением режима секретности, основанном на Кодексе поведения служащих.
США	- при поддержке государства более 500 корпораций регулярно обмениваются информацией по наиболее актуальным вопросам национальной и экономической безопасности; - государство обеспечивает защиту секретной информации на базе жестких стандартов, требований и процедур по защите ценной научно-технической, технологической и коммерческой информации частного сектора.	- бесконфликтное решение проблем в сфере экономической безопасности; - если фирма имеет месячный доход более 10 тыс. долларов, а штат фирмы превышает три человека, то один из сотрудников обязан заниматься, вопросами безопасности; - будущие сотрудники службы безопасности, обычно получают 8-часовой тренинг до начала выполнения своих обязанностей и 40-часовой тренинг в течение 9 первых дней работы.

Изучив международный опыт развитых стран в отношении организации экономической безопасности компаний, можно сделать выводы, что для обеспечения экономической безопасности компаний необходим комплекс мер и инструментов. Исходя из международной практики, наиболее эффективными являются усовершенствование законодательной основы, внедрение и применение на постоянной основе инструментов для предупреждения и

профилактики угроз, а также формирование грамотной политики управления персоналом. Также, как показывает международный опыт, необходимо внедрять инновационные продукты и технологии во все направления деятельности компании. Защита конфиденциальной информации, в том числе коммерческой тайны, на правовой основе является неотъемлемым условием для обеспечения благоприятного климата предпринимательской среды, что приводит к повышению экономической безопасности в целом.

Для повышения экономической безопасности компаниям необходима поддержка и содействие государства в вопросах ведения бизнеса и его безопасного существования. Именно поэтому государству важно организовать эффективную систему взаимодействия между компаниями, государственными правоохранительными органами и частными охранными организациями. Принимая во внимание тот факт, что службы безопасности компаний в основном состоят из бывших сотрудников спецслужб, вышедших в отставку, то государство должно беспокоиться об их будущем устройстве на работу. Такая практика сложилась в госструктурах развитых государств, где бывшие работники спецслужб работают в частных структурах, но в интересах государства. То есть, на опыте развитых стран видно, что для экономической безопасности компаний необходимо, прежде всего, создание благоприятных условий. Комплексное взаимодействие государства и компаний на макроуровне и взаимодействие компании и всех её подразделений на микроуровне позволяют достичь экономической безопасности в полном понимании этого термина.

Говоря о целях достижения экономической безопасности компании главной из них можно считать обеспечение длительного и наиболее эффективного функционирования текущей деятельности и развитие будущего потенциала компании. Из данной цели выделяют функциональные цели экономической безопасности компании, а именно:

• достижение компанией наивысшего финансового результата исходя из её плана развития;

• достижение компанией полной независимости и стойкости к постоянно изменяющимся рыночным условиям;

• полная конкурентоспособность компании и повышение её технического оснащения;

• построение высокоэффективной системы менеджмента;

• надежная защита информации, относящейся к коммерческой тайне, а также её безопасное хранение;

• подбор высококвалифицированного персонала и создание системы по его эффективному управлению.

В соответствии с вышеуказанными функциональными целями экономической безопасности компании необходимо рассмотреть её функциональные составляющие. Понятие функциональной составляющей экономической безопасности компании очень многогранно, так как это совокупность её направлений, противоположных по своему содержанию. Среди функциональных составляющих экономической безопасности компании можно выделить главные:

• финансовая составляющая – ее смысл заключается в эффективном и рациональном использовании ресурсов компании;

• информационная составляющая – активное применение информационно-аналитических методов в управлении компанией;

• интеллектуальная составляющая – формирование интеллектуальных возможностей компании;

• правовая составляющая – правовое обеспечение деятельности компании;

• рыночная составляющая – соответствие компании конкурентной среде;

• технологическая составляющая – соответствие технологий компании рыночным требованиям;

• кадровая составляющая – эффективное управление кадрами компании.

Рассматривать факторы экономической безопасности компании, необходимо исходя из её целей и задач, а также от вида её хозяйственной деятельности. Основные факторы экономической безопасности можно разделить на два вида – эндогенные и экзогенные. К эндогенным принято относить такие составляющие, как кадры компании и её политика в этой области, маркетинговая политика, внедрение инноваций в деятельность компании, её конкурентоспособность и выживаемость на рынке. К экзогенным относят все факторы макроуровня, то есть политическая обстановка страны, её экономическая ситуация, фискальная политика государства, рынки сбыта и т.д. Также факторы экономической безопасности можно рассмотреть в иной классификации – это организационно-управленческая структура компании, её менеджмент, кадры, всё имущество и финансы, а также технологии. Любые перечисленные факторы с одной стороны выступают элементами обеспечения экономической безопасности, а с другой – источниками вероятных угроз безопасности компании. Именно поэтому при принятии управленческих решений очень важно принимать во внимание две стороны перечисленных факторов. При проведении анализа необходимо высчитать удельный вес каждого фактора в общей совокупности. Это позволит проанализировать долю каждого фактора в процессе обеспечения экономической безопасности компании.

Рассматривая экономическую безопасность необходимо выделить её основные показатели и критерии. В мировой практике выделяют четыре группы показателей экономической безопасности компании: производственные, финансовые, социальные и показатели взаимоотношений с клиентами и партнерами. Производственные показатели отражают показатели динамики производства (стагнации, роста), производительности производственного капитала, объема инвестиций в инновации, фонда производительности труда, темпов роста основных фондов, коэффициента выбытия, а также анализируют структуру и соотношение оборудования, рабочего времени, средств, темпов, уровня загруженности, рентабельности производства и т. д. К социальным показателям относятся текучесть кадров, уровень сложности работы квалифицированных работников, движение персонала, потерянное рабочее время, просроченная заработная плата и т. п.

Критерий является признаком, который оценивает угрозы и ущерб от их воздействия. Критерии экономической безопасности, в отличие от показателей, могут быть как количественными, так и качественными. Они выражены показателями экономической безопасности. Пороги используются для оценки

того или иного критерия, то есть порогов, которые соответствуют нормальному уровню экономической безопасности компании. Чтобы проанализировать уровень экономической безопасности организации, необходимо отслеживать деятельность компании и сравнивать полученные показатели с пороговыми значениями.

Одним из основных инструментов диагностики экономической безопасности является SWOT-анализ. Основная идея этого метода заключается в том, что угрозы компании могут быть компенсированы сильными сторонами внешней среды. В процессе SWOT-анализа факторы внутренней и внешней среды сравниваются попарно. Последовательность анализа следующая:

• построить основную матрицу, суммирующую значительные сильные и слабые стороны организации, угрозы и возможности внешней среды;

• построение вспомогательной матрицы – выбор когерентных и конфликтующих пар;

• анализ пар соответствия и разработка стратегических альтернатив;

• выбор вероятной реакции компании на изменения.

В основной матрице SWOT-анализа угрозы и возможности внешней среды, а также сильные и слабые стороны организации классифицируются в порядке убывания важности для компании.

Также часто используемым инструментом диагностики экономической безопасности является BCG-матрица – это механизм для стратегического планирования, имеющий две отличительные особенности: жизненный цикл товара и эффект масштаба производства. Совокупность этих особенностей делает возможным группировку товара по его возможным четырем ролям для производящей или продающей его компании. Такое группирование товара позволяет определить его конкурентоспособность по принципу наличия большинства товаров в приоритетных группах.

Для анализа привлекательности отрасли с точки зрения характера конкуренции применяется такой интересный инструмент, как пятифакторная модель конкуренции Портера. Данная модель предполагает существование пяти позиций, которые определяют уровень конкуренции, а значит, и привлекательность ведения бизнеса в данной стране или регионе. Привлекательность отрасли в понимании модели Портера означает её необходимую рентабельность, а неконкурентная отрасль признается отраслью, в которой совокупность этих позиций существенно снижает рентабельность бизнеса.

Подводя итоги, следует заметить, что надежность системы управления экономической безопасностью определяется как инструментами, так и технологиями управления. Т.е к ним можно отнести создание ответственной группы, постоянный мониторинг и анализ существующих и выявление будущих экономических угроз с целью определения количественных и других параметров, а также создание плана по минимизации отрицательных последствий экономических угроз, оценка полученных результатов по реализации мер по предупреждению экономических угроз. Эффективная система управления экономической безопасностью компании гарантирует финансовую защищенность и стабильность компании, повышение её рентабельности и конкурентоспособности.

Список литературы:

1. Меламедов С.Л. Формирование стратегии экономической безопасности предпринимательских структур. СПБ, 2002

2. Савенко М. М. Международный опыт организации экономической безопасности предприятий / М. М. Савенко / инвестиции: практика и опыт. – 2011. – № 4. – С. 60-63.

3. Гизатуллина О.М. Сравнительная характеристика методик оценки вероятности банкротства // Наука и образование транспорту. 2013. №1. с.139.

4. Денисов М.В., Молдован А.А. Бенчмаркинговый подход к стратегическому планированию деятельности туристских компаний//Известия Санкт-Петербургского государственного аграрного университета. 2012. № 28. С. 275-279.

5. Воронов С.А., Зубарева Л.В. Систематизация методов оценки кадровых рисков при формировании стратегии развития организации в условиях ее реструктуризации/ С.А. Воронов. – Управление экономическими системами: электронный научный журнал. – 2012. – №38. с.24.

6. Деревяшкин С.А. Об анализе экономических рисков и их влияния на капитал организации // Экономические науки. 2015. №127. с.134.

УДК 323.1

Попова Софья Ростиславовна,
Шадыев Рустам Русланович, Лях Анна Викторовна,
Российский университет транспорта (МИИТ), г. Москва
Popova Sofya Rostislavovna,
Shadyev Rustam Ruslanovich, Lyakh Anna Viktorovna,
Russian University of Transport (MIIT), Moscow

Королева Анна Михайловна, старший преподаватель,
Российский университет транспорта (МИИТ), г. Москва
Koroleva Anna Mikhailovna,
Russian University of Transport (MIIT), Moscow

ПРАВОВЫЕ НЮАНСЫ В СФЕРЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ
LEGAL NUES IN THE FIELD OF NATIONAL SECURITY

Аннотация: в статье рассматриваются правовые аспекты обеспечения безопасности российского государства и общества, которые дают возможность выявить ряд факторов, активно влияющих на резервы государства в решении задач обеспечения национальных интересов. Проводится анализ основных понятий и составляющих, которые в свою очередь раскрывают и поясняют проблематику такой темы как национальная безопасность.

Abstract: the article discusses the legal aspects of ensuring the security of the Russian state and society, which make it possible to identify a number of factors that actively influence the state’s reserves in solving problems of ensuring national interests. The analysis of the basic concepts and components, which in turn reveal and explain the problems of such topics as national security.

Ключевые слова: национальная безопасность, правовые аспекты, обеспечение безопасности, российское государство.

Keywords: national security, legal and political aspects, security, Russian state.

В настоящее время, как в научной, так и в юридической литературе, существует огромное количество различных подходов к определению понятия безопасности. Причем безопасность – это не, только в общем смысле, но и в понятии национальной безопасности. Так, первый российский закон «О безопасности» 1992 года дает первое определение национальной безопасности. Согласно этому нормативному правовому акту, национальная безопасность – это защита национальных интересов от внутренних и внешних угроз [1]. Безопасность российского государства тесно связана с историческими тенденциями различных эпох, в каждую из которых существовали свои особенности, выразившиеся в законодательных и иных правовых нормах. Началу государственной безопасности положило формирование государственной тайны, являвшейся существенным элементом в механизме осуществления власти. В настоящее время в зарубежной и отечественной научной литературе говорится о функционирующей системе обеспечения национальной безопасности, которая складывалась на протяжении всего исторического периода существования государств. В нашей стране понятие «национальная безопасность» прошло различные этапы своего становления и развития. Главными составными частями национальной безопасности как социально-политического явления сегодня выступают безопасность личности, безопасность общества и безопасность государства в таких сферах как оборона, общественная жизнь, международная жизнь, экология, экономика и информация.

Национальная безопасность государства – это сложное и многомерное явление, которое связано практически со всеми аспектами существования человека, государства и общества. Неудивительно, что правовая сторона обеспечения национальной безопасности не закреплена в каком-то одном законодательном акте, а распределена по нескольким основным документам и различным нормативно-правовым актам.

Правовая безопасность основывается на Конституции Российской Федерации [1].

Также правовой основой обеспечения безопасности являются общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, Федеральный закон «О безопасности», иные федеральные законы и нормативные правовые акты Российской Федерации и ее субъектов, органы местного самоуправления, принятые в пределах их компетенции в области безопасности.

Основные правовые акты, связанные с обеспечением национальной безопасности России:

1. Правовой механизм обеспечения безопасности отражен в Федеральном законе № 390-ФЗ «О безопасности». (Этому предшествовала редакция закона Российской Федерации от 05.03.1992 № 2446-1 «о безопасности» 1992 года) [2]. Этот документ определяет основные принципы обеспечения безопасности в

России. Речь идет об обеспечении «государственной безопасности, общественной безопасности, экологической безопасности, личной безопасности и иных видов безопасности, предусмотренных законодательством Российской Федерации». Таким образом, данный документ определяет принципы обеспечения национальной безопасности только в общих чертах, говоря о безопасности в целом и не делая различий между этими терминами.

Более подробно вопрос обеспечения национальной безопасности прописан в разделе закона о функциях Совета Безопасности. Вопросы национальной безопасности непосредственно связаны с:

- рассмотрением вопросов безопасности, организации обороны, военного строительства, оборонного производства, военно-технического сотрудничества Российской Федерации с иностранными государствами, иных вопросов, связанных с защитой конституционного строя, суверенитета, независимости и территориальной целостности Российской Федерации, а также вопросов международного сотрудничества в области безопасности;
- анализом информации о реализации Основных направлений государственной политики в области безопасности, о социально-политической и экономической ситуации в стране, о соблюдении прав и свобод человека и гражданина;
- разработка и уточнение Стратегии национальной безопасности Российской Федерации, иных концептуальных и доктринальных документов, а также критериев и показателей обеспечения национальной безопасности. Федеральный закон от 29 декабря 2010 года «О безопасности» определяет такие важные правовые аспекты обеспечения национальной безопасности, как основные принципы этого процесса, содержание деятельности по обеспечению национальной безопасности, государственная политика в этой сфере, вопросы международного сотрудничества.

Также стоит отметить, что закон явился важным шагом на пути расширения понятия безопасности: безопасность рассматривается не только как защита и безопасность государственной системы от внешних и внутренних угроз, но и как обеспечение гражданских свобод, безопасности и защиты интересов общества и личности.

Проработка этих вопросов и правовых норм была разработана в другом документе, одном из важнейших с этой точки зрения, – стратегии обеспечения национальной безопасности Российской Федерации до 2020 года. Так, в документе отмечается, что в целях предотвращения угроз национальной безопасности необходимо обеспечить социальную стабильность, межнациональное и межконфессиональное согласие, повысить мобилизационный потенциал и рост национальной экономики, повысить качество работы органов государственной власти и создать эффективные механизмы их взаимодействия с гражданским обществом в целях реализации права граждан РФ на жизнь, безопасность, труд, жилище, здоровье и здоровый образ жизни, доступное образование и культурное развитие [2].

Задачи защиты информации были определены в Концепции национальной безопасности России и подтверждены в Стратегии обеспечения национальной безопасности РФ до 2020 года [3]. Таким образом, подтверждается

важность баланса между обеспечением свободного доступа к информации и реализацией конституционного права граждан на информацию и необходимостью ограничения доступа к определенным видам информации в целях обеспечения безопасности.

Следующий «этап» – это уровень законодательства Российской Федерации. Здесь, прежде всего, следует выделить закон «Об информации, информатизации и защите информации», Закон «О средствах массовой информации», Закон «О государственной тайне», закон «О рекламе» и др. Универсальность понятия информационной безопасности определяет широкий круг нормативных актов и официальных документов, которые так или иначе касаются безопасности в данной сфере.

Помимо обеспечения права на получение информации, законодательство в этой сфере также решает проблему защиты прав организаций и физических лиц на тайну информации и недопущения разглашения государственной и иной тайны.

Кроме того, Гражданский кодекс РФ также регулирует стандарты информационной безопасности.

Нормы, призванные обеспечить информационную безопасность, содержатся также в законодательстве, которое, как представляется, не имеет прямого отношения к этой сфере. Например, Федеральный закон «О противодействии терроризму» косвенно указывает на важность средств массовой информации для основных принципов противодействия терроризму. Закон предусматривает «систематическое и всестороннее использование политических, информационно-пропагандистских, социально-экономических, правовых, специальных и иных мер противодействия терроризму».

В современной России национальная безопасность выступает как интегрирующая идея, для чего есть объективные предпосылки. Так, комплексный кризис, который переживала наша страна в 1990-е гг., создавал ощущение небезопасности и выдвигал безопасность в качестве одной из главных и актуальных ценностей. Другой предпосылкой развития такой идеологии является потребность в объединяющей общество основе, и распространение идей, связанных с национальной безопасностью, в какой-то мере удовлетворяет эту потребность [4]. Недаром наибольшую поддержку российские политические лидеры имели после победы в пятидневной войне на Кавказе – общество почувствовало себя в безопасности, что свидетельствует о ее значимости в жизни каждого человека.

Существуют различные подходы к пониманию национальной безопасности. Так, сторонники традиционного подхода склонны подчинять интересы личности и общества интересам государства. Приверженцы либерально-демократического подхода к национальной безопасности трактуют ее более широко – как безопасность индивидуума, общества и государства, в основе, которой лежит приоритет безопасности личности и обеспечение ее прав и свобод.

Подводя итог, можно сказать, что законодательство в области национальной безопасности является столь же обширным и всеобъемлющим, как и содержание самого понятия. В этой связи нормы, регулирующие защиту национальных интересов государства, общества и личности, можно найти в

официальных документах и законодательных актах практически любого уровня. Это в равной степени относится и к информационной безопасности как составляющей национальной безопасности Российской Федерации.

То внимание, которое в последние годы уделяется вопросам безопасности в мире, свидетельствует о современных приоритетах в мировосприятии и ценностных ориентациях, складывающихся под влиянием глобальных перемен. Жизнь в безопасности выходит для общества на первый план даже посредством ограничения прав и свобод человека, которыми невозможно эффективно воспользоваться при реальных угрозах жизни и здоровью людей. В данном контексте интересы государства и общества совпадают: усиление влияния государственных институтов на общественную жизнь не вызывает резкого противодействия со стороны граждан при условии гарантии их безопасности. Однако чрезмерное усиление государства приводит к политической инфантильности общества, снижению востребованности в демократических нормах и правилах и формированию авторитарного режима. Поэтому повышение влияния государства должно сочетаться с усилением гражданского общества, которое может ограничить монопольное государственное притязание на управление всеми сферами жизнедеятельности через призму исключительно государственных интересов.

Список литературы:

1. Буркин А.И., Национальная безопасность России в контексте современных политических процессов/ Буркин А.И., Возженников А.В., Синеок Н.В. Москва: Издательство Юрайт, 2020. – 332с.– (Высшее образование). – ISBN 978-5-534-12725-6. – Текст : электронный // ЭБС Юрайт [сайт]. – URL: https://urait.ru/bcode/448188

2. Закон РФ от 5 марта 1992 г. № 2446-1 «О безопасности» (с изменениями и дополнениями).

3. Стратегия национальной безопасности Российской Федерации до 2020 года // Официальный сайт Президента России. URL: http://news.kremlin.ru/ref_notes/424

4. Кардашова, И.Б. Основы теории национальной безопасности: учебник для вузов/ И.Б. Кардашова. – 2-е изд., перераб. и доп. – Москва: Издательство Юрайт, 2020. – 332 с. – (Высшее образование). – ISBN 978-5-534-12725-6. – Текст: электронный // ЭБС Юрайт [сайт]. – URL: https://urait.ru/bcode/448188

УДК 338.24

Пролубников Андрей Викторович, к.э.н., докторант,
Военная академия материально-технического обеспечения
имени генерала армии А. В. Хрулева, г. Санкт-Петербург
Prolubnikov Andrey Viktorovich, General of Army A. V. Khrulev Military
Academy of Procurement and Logistics, Saint-Petersburg

УРОВНИ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ ПОЛИТИКИ
LEVELS OF THE STATE ECONOMIC POLICY

Аннотация: в статье описаны проблемы, связанные со структурированием национальной экономики в целях реализации государственной экономической политики. Сформулированы рекомендации по решению этих проблем.

Abstract: the paper contains a description of problems linked to the structuring of the national economy for the implementation of the state economic policy. Recommendations for solving these problems are formulated.

Ключевые слова: государственная экономическая политика, национальная экономика, вертикальные связи, горизонтальные связи.

Keywords: state economic policy, national economy, vertical ties, horizontal ties.

Государственная экономическая политика (ГЭП) по определению является многоуровневой, поскольку многоуровневыми являются как ее объект (национальная экономика), так и субъект (система государственного управления) [6, 13]. Из этого следуют две ключевые задачи разработки ГЭП: во-первых, как корректно разделить объект и субъект ГЭП на уровни, и, во-вторых, как обеспечить правильное соответствие между уровнями. Отметим, что решение первой задачи не равнозначно решению второй: для системы государственного управления реализация ГЭП является лишь одной из множества задач, и поэтому ее структурирование на уровни исходя исключительно из целей ГЭП может помешать эффективному достижению других целей этой системы.

Аналогично, национальная экономика представляет собой совокупность хозяйствующих субъектов, действующих не только (и в ряде случаев – не столько) для достижения целей ГЭП, но и в своих собственных интересах, и поэтому структурировать ее исключительно в соответствии со структурой системы государственного управления может привести к снижению эффективности народного хозяйства. Такое структурирование оправдано только в случае полного государственного контроля над экономикой, но в условиях рыночной экономики оно может стать источником проблем.

Ситуация осложняется тем, что если система государственного управления носит в некотором смысле искусственный характер, поскольку создается целенаправленно и отличается более или менее строгой и фиксированной структурой, то национальная экономика по своей природе представляет собой естественный объект с размытыми границами между уровнями. Если система государственного управления дискретна, то национальная экономика непре-

рывна. Таким образом, структурировать ее необходимо так, чтобы, с одной стороны, обеспечить возможность управления ею в рамках ГЭП, но, с другой стороны, в максимальной степени учесть ее сложный, непрерывный характер.

Хотя в данном исследовании задача разработки математической модели ГЭП не ставится, можно утверждать, что соответствие между уровнями системы государственного управления и уровнями национальной экономики будет нечетким. Это означает, что, хотя у каждого уровня государственного управления будет приоритетный для него с точки зрения ГЭП уровень национальной экономики, ему будет необходимо учитывать и другие уровни народного хозяйства и участвовать в мероприятиях, связанных с реализацией ГЭП для этих уровней.

Ниже мы опишем те проблемы, которые связаны с разделением национальной экономики на уровни.

В национальной экономике традиционно выделяются три уровня: национальный (применительно к России – федеральный), региональный и локальный (муниципальный) [4]. Теоретически такая модель соответствует и структуре государственного управления. Однако на практике с использованием такой трехуровневой системы возникают проблемы.

Прежде всего, в силу больших размеров нашей страны, непосредственный переход от федерального уровня управления к региональному затруднителен [2, 11] (это справедливо и для национальной экономики, в которой выделяются экономические районы или макрорегионы [3]). Для частичного устранения этой проблемы в России существует институт федеральных округов – не предусмотренных Конституцией РФ укрупненных образований, представляющих, по сути дела, уровень управления, занимающий промежуточное положение между региональным и федеральным уровнями. Он позволяет координировать мероприятия по реализации ГЭП на надрегиональном уровне. В отличие от предусмотренного Конституцией административного деления нашей страны, федеральные округа официальными единицами не являются, что делает их использование гораздо более гибким.

В частности, для повышения эффективности ГЭП на региональном и надрегиональном уровнях отдельные субъекты федерации могут передаваться из одного федерального округа в другой по указу Президента РФ. Именно это произошло с Забайкальским краем и Республикой Бурятия, которые в 2018 г. были переданы из Сибирского федерального округа в состав Дальневосточного федерального округа (что упростило администрирование федеральной целевой программы «Финансово-экономическое развитие Дальнего Востока и Байкальского региона»). Интересно, что после этой передачи Дальневосточный федеральный округ совпал по составу с Дальневосточным экономическим районом (это единственное совпадение среди всех федеральных округов и экономических районов нашей страны).

Кроме того, по мере необходимости федеральные округа могут укрупняться (вхождение Крымского федерального округа в состав Южного) или, наоборот, дробиться (выделение Северо-Кавказского федерального округа из Южного). Проведение таких изменений с субъектами федерации сталкивается с гораздо большими административными и регуляторными трудностями.

Еще одной важной особенностью федеральных округов является то, что они представляют собой не иерархические (в частности, главы субъектов федерации не находятся в подчинении у полномочного представителя президента в соответствующем федеральном округе), а координационные структуры [10].

По сути дела, использование федеральных округов позволяет сделать реализацию ГЭП более гибкой за счет как формирования надрегиональных структур, так и управления составом этих структур. Фактически речь идет о реализации сетевого подхода (гибкость состава и координационный, а не иерархический, механизм регулирования) на надрегиональном уровне. Распространение сетевых структур является отличительной тенденцией современного менеджмента [5, 9], и по этой причине ее отражение в системе государственного управления нашей страны абсолютно оправдано. Именно поэтому мы считаем, что институционализировать статус федеральных округов в Конституции не следуем – после этого они утратят свою гибкость.

Таким образом, наряду с официальной трехуровневой структурой государственного управления в нашей стране можно говорить о фактически четырехуровневой структуре: федеральный уровень – окружной (надрегиональный) уровень – региональный уровень – муниципальный уровень. При этом надрегиональный уровень придает гибкость и целостность трехуровневой вертикали. Это позволяет говорить о необходимости выделения надрегионального уровня и в национальной экономике. Формально таким уровнем являются экономические районы, однако они практически не институционализированы в российской экономической политике.

Мы полагаем, что необходимо устранить эту проблему и осуществлять регулирование экономики на надрегиональном (макрорегиональном) уровне, передав соответствующие полномочия на окружной уровень системы государственного управления (неадминистративный статус экономических районов хорошо соответствует неадминистративному статусу федеральных округов). Хотя экономических районов в нашей стране больше, чем федеральных округов, это проблему можно решить за счет того, что в федеральный округ будет входить более одного района.

Также следует указать, что трехуровневая структура построена на вертикальных связях, из-за чего системе государственного управления не хватает горизонтальных связей. Этот недостаток она унаследовала от советских времен. Попыткой – к сожалению, провалившейся – его устранить во времена СССР было внедрение системы совнархозов при Н. С. Хрущева [7]. Причинами провала этой реформы управления экономикой стало тотальное замещение системы вертикальных связей (при отсутствующих горизонтальных) системой горизонтальных связей (при отказе от вертикальных). Это позволяет сделать очевидное предположение, что оптимальная система государственного регулирования экономики должна основываться на балансе вертикальных и горизонтальных связей, при этом вертикальные связи должны охватывать все горизонтальные уровне, а горизонтальные связи должны быть представлены на всех вертикальных уровнях.

Частично эта проблема компенсируется в наши дни за счет института федеральных округов, однако очевидно, что потенциал горизонтальных связей отдельных регионов не ограничивается теми связями, которые существуют в пределах федеральных округов. Один и тот же регион может принимать участие в разных системах горизонтальных связей. Более того, эти системы связей могут быть разными для разных частей одного и того же региона (как показывает пример Арктической зоны Российской Федерации [12]).

Еще одним решением этой проблемы является кластерная политика [1, 8], однако она подходит не для всех регионов и отраслей.

Таким образом, мы можем констатировать следующее:

- наличие в системе государственного управления надрегионального (окружного) уровня делает эту систему более гибкой и эффективной за счет применения сетевого инструментария, который частично компенсирует недостатки, присущие жесткой вертикальной трехуровневой системе;
- представляется целесообразным закрепить наличие в национальной экономике надрегионального (макрорегионального) уровня, передав реализацию ГЭП на этом уровне федеральным округам;
- соответствие между уровнями системы государственного управления и уровнями национальной экономики не должно быть жестким, так как это приведет к изоляции уровней друг от друга и к недостаточной координации мероприятий, проводимых на разных уровнях. Хотя за каждым уровнем системы государственного управления должен быть закреплен приоритетный для нее уровень национальной экономики (и наоборот), границы между уровнями должны быть проницаемыми. Органы управления, расположенные на определенном уровне системы государственного управления, должны иметь возможность влиять на мероприятия ГЭП, проводимые за пределами закрепленного за ними уровня национальной экономики;
- необходимо развивать и внедрять инструментарий формирования и управления горизонтальными связями в национальной экономике и стимулировать развитие таких связей.

Список источников:

1. Вертакова Ю. В., Прокопенко О. С. Использование кластерного подхода в реализации структурной политики // Вестник Академии знаний. – 2019. – № 3. – С. 61-68.

2. Вертакова Ю. В., Плотников В. А. Теоретические аспекты учета динамических характеристик социально-экономических систем в управлении региональным развитием // Известия Русского географического общества. – 2011. – Т. 143. – № 6. – С. 42-50.

3. Вертакова Ю. В., Пролубников А. В., Прокопенко О. С. Трансформация хозяйственных комплексов макрорегионов мерами структурной и кластерной политики // Вестник Академии знаний. – 2019. – № 4. – С. 70-79.

4. Коростышевская Е. М., Плотников В. А., Пролубников А. В., Рукинов М. В. Социальная компонента государственной региональной политики и ее роль в обеспечении устойчивого развития и экономической безопасности // Известия Санкт-Петербургского государственного экономического университета. – 2018. – № 6. – С. 120-126.

5. Котляров И. Д. Формы ведения предпринимательской деятельности в виртуальном пространстве: попытка классификации // Экономическая наука современной России. – 2011. – № 2. – С. 89-100.

6. Курбанов А. Х., Смуров А. М., Плотников В. А. Сущность и эволюция государственной экономической политики в современной России // Известия Юго-Западного государственного университета. – 2016. – № 5. – С. 131-142.

7. Миндлин Ю. Б. Сравнительная характеристика кластеров и совнархозов // Экономика и управление: проблемы, решения. – 2020. – Т. 1. – № 5. – С. 124-129.

8. Миндлин Ю. Б. Особенности применения кластеров в региональном управлении // Менеджмент и бизнес-администрирование. – 2014. – № 2. – С. 70-80.

9. Орехова С. В., Заруцкая В. С. Интеграция бизнеса: эволюция подходов и новая методология // Журнал экономической теории. – 2019. – Т. 16. – № 3. – С. 554-574.

10. Плещенко В. И. Об институциональной среде российского общества и о перспективе формирования новых структур координационного типа // Общество и экономика. – 2017. – № 7. – С. 41-45.

11. Плотников В. А. Управление социально-экономическим развитием регионов в посткризисных условиях // Известия Курского государственного технического университета. – 2010. – № 3. – С. 93-100.

12. Целыковских А. А., Курбанов А. Х. Логистические проблемы организации материально-технического обеспечения войск (сил) в Арктической зоне Российской Федерации и способы их решения // Военная мысль. – 2018. – № 7. – С. 40-49.

13. Чепель С. В. Как повысить эффективность экономической политики: экономический анализ роли государственных институтов // Вопросы экономики. – 2009. – № 7. – С. 62-74.

УДК 316.614
DOI 10.37539/NB185.2020.32.23.006

Хмелева Галина Анатольевна, д.э.н., доцент,
Самарский государственный экономический университет, г. Самара
Khmeleva Galina Anatolyevna, Samara State University of Economics, Samara

Домрачева Алина Александровна,
Самарский государственный экономический университет, г. Самара
Domracheva Alina Aleksandrovna, Samara State University of Economics, Samara

COVID 19: ВРЕМЯ ДЛЯ ПЕРЕЗАГРУЗКИ СТРАТЕГИИ И ПРОЕКТОВ РЕГИОНА
COVID 19: TIME TO RESET THE REGION'S STRATEGY AND PROJECTS

Аннотация: в статье проведена оценка влияния кризиса COVID-19 и снижения мировых цен на нефть на региональную экономику, представлены рекомендации авторов по повышению устойчивости экономики в регионах, одной из которых является перезагрузка стратегий социально-экономического развития.

Abstract: the article assesses impact of the COVID-19 crisis and decline in world oil prices on the regional economy, presents the authors' recommendations to improve sustainability of regional economy, one of which is a reload of socio-economic development strategies.

Ключевые слова: стратегия региона, COVID-19, кризис, пандемия, коронавирус, меры поддержки, экономика, регион.

Keywords: strategy, region, COVID-19, crisis, epidemic, coronavirus, measures to support, the economy.

В настоящее время мировая экономика столкнулась с огромными проблемами, связанными с пандемией вируса. Пандемия коронавируса (COVID-19) вызвала значительные гуманитарные и экономические издержки, поскольку массовая изоляция и приостановка деятельности предприятий во многих странах мира оказала влияние на спрос и предложение сырьевых товаров, а также услуг. Последствия будут значительными. По прогнозам Международного валютного фонда в 2020 году падение мировой экономики составит 3%, в России – 5,5% [5]. Чтобы в 2021 году выйти на положительные значения экономического роста необходимо в российских регионах оценить последствия для экономики и, возможно, пересмотреть стратегии социально-экономического развития.

На наш взгляд, у многих регионов возникла потребность в трансформации действующей стратегии с учётом кризисных явлений, так как изменяется их вектор развития, появляются новые вопросы, требующие незамедлительного государственного вмешательства, становится невозможным достижение ожидаемых результатов.

В настоящее время регионами самостоятельно разрабатываются стратегии социально-экономического развития, содержащие приоритеты, основные цели и задачи, а также показатели государственного управления субъектов Российской Федерации [4]. В первую очередь, данный документ отражает основные направления развития региональной экономики и риски, которые могут возникнуть во время его реализации.

Так, к ключевым направлениям Стратегии развития Самарской области на этапе реструктуризации и создания условий относятся привлечение инвестиций, в том числе иностранных, импортозамещение, развитие малого и среднего бизнеса и другие [2].

Но в связи с угрозой коронавирусной инфекции во всех городах и муниципальных образованиях Президентом Российской Федерации было предпринято решение о введении режима всеобщей самоизоляции. С принятием Указа оказалась запрещена любая деятельность, не связанная с продажей или производством товаров первой необходимости, работой экстренных служб, непрерывно действующих предприятий [3]. Это привело к негативным последствиям для развития малого и среднего предпринимательства в регионе, к остановке целых секторов бизнеса. Эпидемия коронавируса несет финансовый ущерб ещё и потому, что большая часть предприятий ориентирована на экспорт продукции на территории многих стран мира, где сейчас также очаг массового распространения заболевания.

С появлением новых проблем появилась необходимость в перераспределении внимания со стороны органов государственной власти с одних сфер деятельности на другие. Под угрозу влияния экономической нестабильности в Самарской области особенно попали такие сферы, как автоперевозки, общественное питание, гостиничный бизнес, деятельность в области культуры, спорта, организации досуга и развлечений, бытовые услуги, непродовольственный ритейл, стоматологические услуги, в которых занято порядка 300 тыс. человек, включая малый бизнес. В последние годы малый бизнес активно развивался в регионе. В 2018 г. оборот малых предприятий составил 554 млрд. руб., показав третье место в Приволжском федеральном округе. Нефтяной кризис и обвал цен на нефть угрожает снизить экономические результаты предприятий нефтехимического комплекса, расположенных в регионе и входящих в нефтехимический кластер региона с якорными предприятиями – представителями ПО «Роснефть». Доля сектора добычи полезных ископаемых в ВРП региона в 2018 году составляла 15,3%, доля экспорта минеральных продуктов 38% (1922,5 млн.долл). Снижение спроса вследствие падения доходов населения дестабилизирует работу предприятий по производству автомобилей. Вместе с тем в Самарской области базируется межрегиональный автомобилестроительный кластер. В 2019 году география участников значительно расширилась и в настоящее время охватывает 109 предприятий из 18 регионов страны с численностью занятых более 60 тыс. человек. Негативный эффект распространяется также на 250 предприятий-поставщиков и более 100 компаний из 39 регионов России.

Для стабилизации ситуации перед органами власти встала следующая задача – заранее определить мероприятия, которые будут «работать на опережение» в борьбе с вирусом и помогут восстановить региональную экономику, пересмотреть региональный бюджет, возможно, увеличить резервный фонд. В результате были предприняты следующие меры поддержки бизнеса: временный мораторий на проверки компаний надзорными органами, уменьшение ставки налогообложения для гостиничной сферы, почти нулевая ставка транспортного налога, льготы по земельному налогу, отсрочка платежей ЖКХ [1].

Следующей основной целью реализации стратегии развития является стабилизация демографической ситуации, повышение ожидаемой продолжительности и качества жизни населения, что противоречит сущности пандемии. Уже на сегодняшний день коэффициент смертности от коронавирусной инфекции в мире составляет 4,49%, а в России – 0,93%. Такое низкое значение показателя удалось достичь с помощью эффективных действий со стороны государства, например, карантина прибывших из-за рубежа, остановки большого количества авиасообщений, дифференцированный подход к мерам самоизоляции в регионах.

Также немаловажное значение имеет образование, которое, исходя из стратегического документа, будет ориентировано на повышение доступности и качества предоставляемых услуг. Так как в связи с коронавирусом организации всех уровней обучения были переведены на длительное время на дистанционный режим, показатели в данной сфере остались независимыми от «корона-кризиса».

Таким образом, коронавирус – это бедствие, которое внесёт свой след в развитие общества. И именно от степени реализации стратегии социально-экономического развития региона зависит, насколько успешна будет экономика страны в постэпидемический период и каковы будут убытки для различных отраслей.

Как и любой кризис, случившаяся пандемия является временем переосмысления и поиска «окон возможностей» в «новой реальности». Необходимо критически еще раз взглянуть на стратегические приоритеты региона, соотнести с мировыми секторами экономики и компаниями, которые лучшим образом показывают себя к сложившихся условиях.

В отношении наиболее конкурентных секторов необходимо проводить политику форсированного развития и поиска точек опережающего роста на основе всемерного использования конкурентных преимуществ и научного потенциала. В Самарской области ведется активная работа по созданию научно-образовательного центра «Инженерия будущего», выделены ключевые направления в создании технологий, материалов и цифровых решений в аэрокосмических системах, передовых транспортных системах и медицине. В рамках указанных направлений могут быть выделены проекты различного типа: создание новых технологий мирового уровня, а также технологий наверстывания технологического отставания. Такие проекты требуют различных подходов в привлечении средств и управления. В условиях, когда на внешние инвестиции рассчитывать не приходится, важно еще большее внимание уделить созданию благоприятных условий для привлечения внутренних инвесторов. В области создана развитая инфраструктура поддержки инвестиционной и предпринимательской деятельности, что позволило Самарской области в 2019 году подняться в рейтинге инвестиционного климата с 48 на 24 место. Важно проводить дальнейшую «тонкую настройку» для повышения уровня комфорта бизнеса, вести адресную работу с инвесторами. Объективные предпосылки для активизации инвестиционной деятельности в период после пандемии формируются уже сегодня. Снижена учетная ставка до 5,5%, предложен перезапуск механизма специального инвестиционного контракта как соглашения между инвестором и государством в лице Российской Федерации, субъекта Российской Федерации и муниципального образования, что создает возможности привлечения «длинных денег» с горизонтом 15-20 лет в зависимости от объема финансирования проекта.

Особую актуальность приобретает всемерное стимулирование инновационной активности, особенно среди молодежи. В Самарской области вузы хорошо дополняют друг друга, образуя мощный образовательный кластер для экономики региона. Настоящий кризис выступил триггером перехода в цифровое пространство образования, которое по-настоящему перестало иметь границы. Важно, чтобы знания студентов могли быть трансформированы в реальные бизнес-проекты для целей опережающего развития региона. Для этого, на наш взгляд, целесообразно разработать региональную грантовую программу поддержки молодых предпринимателей-выпускников вузов региона.

Как показывает опыт стран, приступивших к послаблению карантинных мер, предпринимательская деятельность восстанавливается постепенно. Возможно, уже сейчас следует подумать о том, чтобы продлить налоговые послабления (например, снижение страховых выплат вплоть до введения нулевой ставки) в восстановительный период экономики. Необходимо расширять меры, направленные на поддержку лиц, потерявших работу, и рост спроса в экономике. В период Великой депрессии были запущены инфраструктурные программы, которые позволили дать работу, увеличить спрос и обновить инфраструктуру в стране. Хорошей мерой поддержки являются выплаты семьям с детьми.

Таким образом, триада запускающего механизма стратегического планирования, налогов и мер по увеличению спроса в экономике позволит сформировать импульс опережающего социально-экономического развития региона.

Список литературы:

1. Постановление Губернатора Самарской области от 08.04.2020г. № 77 «О первоочередных мерах поддержки субъектов предпринимательства в Самарской области, оказавшихся в зоне риска в связи с угрозой распространения новой коронавирусной инфекции (COVID-19) в Самарской области» [Электронный ресурс]. – Режим доступа: https://pravo.samregion.ru (дата обращения 08.04.20).

2. Постановление Правительства Самарской области № 441 от 12.07.2017г. «Стратегия социально-экономического развития Самарской области на период до 2030 года» [Электронный ресурс]. – Режим доступа: https://economy.samregion.ru (дата обращения 08.04.20).

3. Указ Президента РФ от 25.03.2020г. № 206 «Об объявлении в Российской Федерации нерабочих дней» [Электронный ресурс]. – Режим доступа: https://base.garant.ru (дата обращения 08.04.20).

4. Федеральный закон от 28.06.2014г. № 172-ФЗ «О стратегическом планировании в Российской Федерации» (ред. от 18.07.2019) [Электронный ресурс]. – Режим доступа: https://base.garant.ru (дата обращения 08.04.20).

5. World Economic Outlook, April 2020: The Great Lockdown. URL: https://www.imf.org/en/Publications/WEO/Issues/2020/04/14/weo-april-2020

НБ ПРАВОВЫЕ И ПОЛИТИЧЕСКИЕ АСПЕКТЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

УДК 34
DOI 10.37539/NB185.2020.69.43.013

Лескова Юлия Геннадьевна, доктор юридических наук, доцент,
Кубанский государственный аграрный университет
им. И.Т. Трубилина, г. Краснодар
Leskova Julia Gennad'evna, KUBSAU, Krasnodar

Машталенко Данил Сергеевич, Кубанский государственный аграрный
университет им. И.Т. Трубилина, г. Краснодар
Mashtalenko Danil Sergeevich, KUBSAU, Krasnodar

СПОСОБЫ ЗАЩИТЫ В СОВРЕМЕННОЙ ЮРИДИЧЕСКОЙ НАУКЕ
METHODS OF PROTECTION IN MODERN LEGAL SCIENCE

Аннотация: в данной статье автор затрагивает проблемы, связанные с ограниченным выбором способов защиты, описывая и раскрывая их виды. Также в данной работе приведены возможные пути разрешения поднятых проблем.

Abstract: in this article, the author addresses the problems associated with a limited selection of protection methods, describing and revealing their types. Also in this paper, possible solutions to the problems raised are given.

Ключевые слова: право, гражданское законодательство, юридическая наука.

Keywords: law, civil law, legal science.

С развитием экономических отношений в любом государстве для обеспечения социальной составляющей, стабильности и порядка необходимы правовые механизмы.

С появлением системы права жизнь людей значительно изменилась, но не обязательно в хорошую сторону. Именно о правовых пробелах в защите прав граждан и их способах в юридической науке будет идти речь в данной статье.

Положения Конституции России 1993 г. о признании Российской Федерации демократическим правовым государством (п. 1 ст. 1), о том, что человек, его права и свободы являются высшей ценностью, а признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства (ст. 2) наглядно показывают значимость правого государства и гарантируют защиту всем его субъектам деятельности.

На законодательном уровне существуют судебная, внесудебная и административная формы защиты прав субъектов различных областей. Однако

доктрина выделяет дополнительные способы, которые не нашли отражение в правовых актах. Ограниченность способов защиты понуждает лиц действовать в строго определенных рамках не просто для достижения результата в виде доказательства своей правоты, но и для законности принятого по спору решения, которое подкрепляется меры государственного воздействия.

Следует отметить, что российское законодательство не содержит определения понятия «способы защиты субъективных гражданских прав» [1]. В связи с этим представляется необходимым выяснить мнения ученых на этот счет. Так, по мнению М.И. Брагинского и В.В. Витрянского способы защиты гражданских прав есть средства, «с помощью которых могут быть достигнуты пресечение, предотвращение, устранение нарушений права, его восстановление и (или) компенсация потерь, вызванных нарушением права» [2].

По мнению Суханова Е.А. под способами защиты прав понимаются меры принудительного характера, посредством применения которых производится восстановление нарушенных прав. Также он утверждает, что такая мера обязательно должна быть законодательно закреплена [3].

Одним из способов защиты прав является самозащита. Правовая самозащита, конечно же, является формой проявления правовой активности, поскольку осуществляется лицом на основе собственного волеизъявления. «Самозащита как деятельность самостоятельна, совершается по инициативе тех субъектов или групп субъектов, которые нуждаются в защите» [4].

Право на защиту следует рассматривать в нескольких аспектах: в материально-правовом смысле, как элемент механизма правового регулирования, и как способ воздействия на участников правоотношений. Но наиболее целесообразным и значимым нам представляется определение способов защиты как особого способа правового воздействия на участников различных правоотношений.

Стоит подробнее рассмотреть виды защиты, поименованные в ГК РФ. К ним относятся взыскание убытков, наложение штрафов (пеней), понуждение к совершению какого-либо действия, пресечение действий, нарушающих правоотношения и другие.

Требования о признании права, пресечении действий, нарушающих право или создающих угрозу его нарушения и возмещении убытков можно отнести к общим способам защиты.

При учете, что каждый из вышеуказанных способов подкрепляется нормами специальной части ГК РФ, нельзя также не отметить особую категорию защиты – интеллектуальные права. Их относят к специальным способам защиты прав [5]. Но нельзя также не упомянуть про защиту чести, достоинства и деловой репутации.

Резюмируя изложенное выше, можно прийти к выводу о том, что восстановление нарушенного права следует рассматривать в трех аспектах: как принцип защиты гражданских прав, означающий кроме прочего необходимость, обязательность восстановления нарушенного права; как одну из целей защиты гражданских прав, наряду с пресечением, предотвращением, устранением нарушений права и др., а также в качестве одного из способов защиты гражданских прав.

Способов защиты есть множество, они классифицируются по различным признакам, трактуются различными учеными и юристами по-разному. Но неизменным остается их правозащитный характер. Не всегда имеет значение являются они юрисдикционными или же носят характер самозащиты, главное, чтобы они выполняли свою функцию, при этом не нарушая права других субъектов.

В современной юридической литературе не так много целесообразных способов защиты ввиду того, что многие, в основном, цитируют уже существующие, а новое пока не достигло той пользы, чтобы кардинально изменить то, что имеется. В своих трудах ученые сейчас описывают и раскрывают содержание того, что закреплено на законодательно уровне, в частности в ГК РФ, что заставляет прийти к выводу об исчерпываемости существующих способов защиты и их правовом закреплении. Отсюда и вытекают гарантии любого субъекта на защиту их прав.

Список литературы:

1. Гринь Е.А. Способы защиты прав при изъятии земельного участка для государственных и муниципальных нужд. // Современная научная мысль. 2015. № 5. С. 138-145

2. Брагинский М.И., Витрянский В.В. Договорное право. Книга первая: Общие положения. М., 2001. С. 776.

3. Гражданское право: учебник: в 4 т. / отв. ред. Е.А. Суханов. Т. 1: Общая часть. М., 2005. С. 557; Гражданское право / под ред. Б.М. Гонгало, Т.И. Илларионовой, В.А. Плетнева. М., 2001. С. 54.

4. Гаранин М.Ю. Самозащита как социально-философская проблема: дис. канд. филос. наук. – Н. Новгород, 2004. – 181 с.

5. Гринь Е.А. Процедура медиации в спорах, связанных с интеллектуальной собственностью: проблемы и перспективы. // Аграрное и земельное право. 2019. № 8 (176). С. 106-107

НБ ВНЕШНЕПОЛИТИЧЕСКИЕ И ВНЕШНЕЭКОНОМИЧЕСКИЕ АСПЕКТЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

УДК 339.9(470+476)
DOI 10.37539/NB185.2020.42.82.002

Балашова Мария Александровна, кандидат экономических наук, доцент, Байкальский государственный университет, г. Иркутск
Balashova Mariia Alexandrovna, Baikal State University, Irkutsk

Балашова Анастасия Михайловна, Кравченко Владимир Александрович, Байкальский государственный университет, г. Иркутск
Balashova Anastasiia Mikhailovna, Kravchenko Vladimir Alexandrovich, Baikal State University, Irkutsk

О НЕОБХОДИМОСТИ УГЛУБЛЕНИЯ СОТРУДНИЧЕСТВА РОССИИ И БЕЛОРУССИИ С ПОЗИЦИИ ПОВЫШЕНИЯ ГАРАНТИИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ДВУХ СТРАН
ON THE NECESSITY OF DEEPENING THE COOPERATION BETWEEN RUSSIA AND BELARUS FROM THE STANDPOINT OF STRENGTHENING THE GUARANTEE OF NATIONAL SECURITY FOR THE TWO COUNTRIES

Аннотация: современные тенденции развития мировой экономики приводят к возникновению новых угроз в обеспечении национальной безопасности, в первую очередь, развивающихся стран мира, правительства которых вынуждены искать новые инструменты, способные гарантировать защищенность отечественным экономическим субъектам. Не являются исключением в данном случае Россия и Белоруссия, которые могут и должны решить соответствующие проблемы путем углубления взаимного сотрудничества.

Abstract: current trends of the global economic development lead to the emergence of new threats to national security. This is especially true for the developing countries, whose governments are forced to seek new tools of guaranteeing security to domestic economic entities. Russia and Belarus are no exception, so they could and should solve the corresponding problems by deepening their mutual cooperation.

Ключевые слова: международные экономические отношения, национальная безопасность, внешнеэкономическое сотрудничество России и Белоруссии.

Keywords: international economic relations, national security, foreign economic cooperation between the Russian Federation and Belarus.

Ключевой особенностью построения международных экономических отношений в XXI в. является резкая интенсификация сотрудничества на всех уровнях экономического анализа. Ее предпосылками выступают как расширение количества субъектов мировой экономики, к числу которых в настоящее время принято относить не только страны, но и международные экономические организации (МЭО), интеграционные объединения, транснациональные компании (ТНК); так и изменения "правил игры". Речь, прежде всего, идет о необходимости выстраивания отношений в условиях повышения открытости, как самих экономических субъектов, так и пространства, в котором они осуществляют свое взаимодействие.

Нарастающие процессы внутри- и внешнеэкономической либерализации, глобализации, интеграции, регионализации, как никогда ранее обостряют угрозы гарантии национальной безопасности.

Государствам в XXI в. все сложнее становится защищать себя от внутренних и внешних опасностей. С одной стороны, у них появляется возможность объединять свои усилия в решении соответствующих проблем и сообща их нивелировать, с другой, они становятся подверженными давлению со стороны других участников международных экономических отношений. Не случайно в Указах Президента РФ от 17.12.97 № 1300 "Об утверждении концепции национальной безопасности Российской Федерации", от 31.12.2015 № 683 "О стратегии национальной безопасности Российской Федерации", наряду с огромным перечнем актуальных внутренних угроз, к числу ведущих внешних рисков отнесены: "целенаправленное сознательное вмешательство иностранных государств и международных организаций во внутреннюю жизнь народов России", "попытки других государств противодействовать укреплению России как одного из влиятельных центров формирующегося многополярного мира".

Эти и другие, напрямую связанные с ними угрозы, подробнейшим образом исследованы как зарубежными, так и отечественными учеными. Особый интерес, с наших позиций, представляют идеи таких отечественных специалистов как:

- Кривохижа В.И., подчеркивающий в своих работах изменившийся характер построения международных экономических отношений, в которых роль лидера закрепляется уже не за отдельными государствами, а "центрами силы", "полюсами", "цивилизациями" [3];
- Евстафьев Д.Г., обосновывающий факт повышения актуализации цивилизационных противоречий, развития цивилизационных разломов изменившимся характером социальных институтов и социальных связей, что является архиважным для безопасности России и развития Евразии [1];
- Урсул А.Д., предполагающий, что в уже ближайшем глобальном будущем безопасность его субъектов будет зависеть от их устойчивого развития [14];
- Тонких В.А. и Лытнева Н.А., доказывающие факт сохранения актуальности в XXI в. феномена «имперское сознание», который активно проводят в своем внешнеполитическом курсе США [12];
- Маркина С.В, акцентирующая внимание на концепциях "управляемого хаоса", "мягкой силы" и "гибридной войны" [4] и др.

Мы согласны с мнением специалистов о том, что по "шкале приоритетов национальной безопасности" из всех возможных видов ее угроз, пристальное внимание в XXI в., в первую очередь, необходимо уделить внешним составляющим. Именно они, вынуждая страны мира следовать в фарватере "интересов западного сообщества", могут полностью блокировать возможность гарантии системой (во главе с государством) защищенности субъектам своей национальной экономики [10, 13], а также стать причиной нанесения небезразличного ущерба национальным ценностям (геополитическим, политическим, правовым, экономическим, научно-техническим, социальным, культурным, информационным, экономическим, военным и др.) [5].

Особо актуальной проблема способности самостоятельной защиты государства от внешних и внутренних угроз является для развивающихся стран. За установлением контроля над спросом местного населения в них, за их национальной ресурсной и производственной базами в XXI в. продолжается активная борьба.

Постсоветское пространство в данном случае не представляет собой исключение. Даже его ведущие экономики – Российской Федерации и Белоруссии, руководство которых старается активно противостоять внешней "атаке", оказываются в настоящее время критически зависимыми от иностранного "партнерства". Несмотря на разный уровень экономического развития этих стран и достигнутые макроэкономические показатели (табл. 1), оба государства, фактически в одинаковой степени испытывают на себе внешнее давление.

В частности, известно, что рынки товаров и услуг, как РФ, так и Белоруссии, в большей своей части находятся в настоящее время под контролем иностранных производителей. Например, такие машиностроительные гиганты, как Volkswagen Group, Toyota Motor, Renault, Nissan Manufacturing и др., занимают доминирующее положение, как на Российском, так и на Белорусском автомобильном рынке: автомобили, производимые вышеназванными компаниями, на 2019 г. являются наиболее продаваемыми в обеих странах. Подобная ситуация отмечается и в других отраслях соответствующих национальных экономик: пищевая промышленность, бытовая техника, электроника, товары массового спроса, одежда, где на рынке доминируют иностранные фирмы-производители. Даже платежные системы, которыми пользуется почти всё население рассматриваемых стран, принадлежат американским компаниям VISA и Mastercard, которые последовательно и безальтернативно вытесняют Белорусскую национальную платежную систему «Белкарт» и Российскую – «МИР» с их национальных рынков. Учитывая эти новые тренды, «выживающие» отечественные компании вынуждены серьезнейшим образом пересматривать систему своего корпоративного управления для сохранения некогда занятых сегментов национальных рынков [11].

Таблица 1

Динамика ключевых макроэкономических показателей развития России и Республики Беларусь

Показатель	1995 г.		2000 г.		2010 г.		2018 г.	
	РФ	Бела-русь	РФ	Бела-русь	РФ	Бела-русь	РФ	Бела-русь
ВВП (трлн. долл.)	0,396	0,014	0,26	0,013	1,525	0,59	1,658	0,6
ВВП ППС (трлн. долл.)	0,833	0,41	1,001	0,60	2,927	0,159	4,051	0,190
ВВП на душу Населения (долл.)	2 666	2 309	1 772	2 709	10 765	6 181	11 289	6 745
ВВП на душу населения ППС (долл.)	5 613	3 999	6 825	6 027	20 490	15 928	27 588	19 995
Инфляция (%)	197,4	709,35	20,799	168,6	6,849	7,736	2,878	4,87
Безработица (%)	9,45	2,9	10,58	2,1	7,369	2,1	4,846	4,76
ИЧР	0,702	0,656	0,782	0,682	0,782	0,792	0,824	0,817

Примечание: составлено авторами на основе обобщения источников [Официальный сайт Всемирного Банка [Электронный ресурс]. – Режим доступа: https://data.worldbank.org/indicator/ (дата обращения (19.04.2020); Официальный сайт Программы ООН по Человеческому развитию [Электронный ресурс]. – Режим доступа: http://hdr.undp.org/en/countries/profiles/ (дата обращения (19.04.2020)]

Особую тревогу вызывает в настоящее время тот факт, что ключевые предприятия, как РФ, так и республики Беларусь все глубже погружаются в зависимость от иностранных комплектующих.

В России это, например,

- предприятия судостроительной отрасли, которые в огромных объёмах импортируют судовое комплектующее оборудование (по словам ген. директора АО Центрального научно-исследовательского института (ЦНИИ) «Курс» В.Ханычева, судовые двигатели и радионавигационное оборудование, которое могло бы конкурировать с импортным, найти в России сложно);

- автомобилестроительные компании (например, в связи с тем, что руководство и инженеры компании АО «АВТОВАЗ» являются представителями Альянса Renault–Nissan–Mitsubishi, материалы и комплектующие для производства таких автомобилей, как LADA, импортируются из-за рубежа);

- компании, занимающиеся производством спутников, которые почти на 70% зависят от электронно-компонентной базы иностранного производства (даже такая ведущая российская спутниковая система как ГЛОНАСС на 40% состоит из зарубежных комплектующих) и др.

В свою очередь, в Белоруссии на импортном оборудовании сегодня работают:

- одно из крупнейших нефтехимических предприятий страны – ОАО «Нафтан» (импортируют нефтехимическое, резервуарное, насосное, сварочное, компрессорное оборудование, арматуру и пр.);

- Минский автомобильный завод (МАЗ), являющийся управляющей компанией холдинга Белавтомаз (для производства выпускаемой им большегрузной автомобильной, а также автобусной, троллейбусной и прицепной техники, использует импортные комплектующие, поставляемые такими странами, как Германия и США) и др.

Национальные ресурсы соответствующих стран осваиваются совместно с иностранными партнерами. Например, одной из причин медленных темпов реализации нефте- и газодобывающей кампании по освоению российского шельфа Арктики является ее высокая зависимость от поставок зарубежных технологий и оборудования. Проблемы еще более усугубились после 2014 г., когда в следствии применения санкционной политики, иностранные партнеры просто ушли из арктических проектов в России.

Огромные проблемы имеются у стран в сфере производства сложной наукоемкой продукции. Зачастую ни провести стадию научно-исследовательских и опытно-конструкторских разработок (НИОКР), ни начать производство оказывается для экономических субъектов соответствующих стран невозможным без помощи иностранных инвестиций.

Например, Российский фонд прямых инвестиций (РФПИ) инвестирует сегодня в реализацию отечественного металлургического проекта на базе горно-металлургической компании М. Прохорова «Интергео» совместно с Российско-китайским инвестиционным фондом и Ближневосточным суверенным фондом. Эти инвестиции направлены на проект «Кингаш» в Красноярском крае, являющемся вторым в России по запасам никеля, и «Ак-Суг» в Республике Тыва, входящем в пятерку крупнейших в России по запасам меди.

Понимаю всю сложность ситуации, еще в 1997 г. Россия и Белоруссия заключили договор о создании Союзного Государства (СГРБ), что было обусловлено необходимостью политической и экономической интеграции двух стран в области материального и интеллектуального потенциалов для подъема экономик, повышения уровня жизни граждан, а также духовного развития личности[1]. Параллельно с этим продолжилась интенсификация интеграционных процессов между рассматриваемыми странами и другими государствами постсоветского пространства в рамках Содружества Независимых Государств (СНГ), Таможенного Союза (ТС), созданного еще в 1995 г. и переросшего в последующем сначала в Евразийское экономическое сообщество (ЕврАзЭс), а потом и в Евразийский экономический союз (ЕАЭС).

За минувшие 20 с лишним лет были получены, действительно, значимые результаты. В частности,

[1] Всего в «Договоре о создании Союзного государства» было прописано восемь основных целей создания СГРБ, направленных на «обеспечение мирного и демократического развития братских народов государств-участников», «создание единого экономического пространства», а также «проведение согласованной внешней политики и политики в области обороны».

- между предприятиями двух стран активно осуществляется производственное сотрудничество. Так, еще в 2006 г. российский "Лукойл" и белорусский "Нафтан" организовали совместное предприятие по производству присадок к маслам;

- продолжается реализация совместных, в том числе инвестиционных и научно-технических проектов. В частности, в настоящее время в Белоруссии заканчивается строительство атомной электростанции (АЭС), запуск первого блока которой запланирован на июль 2020 г. Основным партнером Белоруссии в этом проекте является Россия;

- активно поддерживается военно-техническое сотрудничество (в 2011 г. вступило в силу Соглашение об обеспечении взаимных поставок продукции военного назначения в период нарастания угрозы агрессии и в военное время; в 2016 г. было подписано Соглашение о совместном техническом обеспечении региональной группировки войск и создана Восточно-европейская объединённая региональная система противовоздушной обороны (ПВО);

- сохраняется взаимодополняемость в насыщении рынков производственных товаров и услуг двух стран (табл. 2). Ведь не случайно в начале XXI в. их руководителями был предложена концепция "две страны – один рынок", реализация которой позволяет странам сохранять друг для друга статус «одного из ключевых внешнеторговых партнеров» (табл. 3).

Таблица 2

Обзор ключевых потребителей продукции, производимой ведущими предприятиями России и республики Беларусь (2019 г.)

Компания	**Сектор**	**Прибыль (млрд. долл.)**	**Потребители**
Российские компании			
Газпром	Нефть, газ	18,9	Германия, Турция, Италия, Белоруссия
Лукойл	Нефть, газ	9,9	Белоруссия, Мексика, США, Египет
Novatek	Газ	2,6	Испания, Китай, страны АТР
КамАЗ	Автомобили	2,17	Казахстан, Белоруссия, Алжир
Компании республики Беларусь			
Беларуськалий	Калийные удобрения	1,73	Россия, Турция, страны ЕС
БЕЛАЗ	Автомобили	0,106	Россия, Украина, Казахстан
ОАО “НАФТАН”	Нефтепереработка	0,104	Страны СНГ, Европы
Белшина	Автомобильные шины	0,009	Россия, Украина, Казахстан

Примечание: составлено авторами на основе обобщения источников [Официальный сайт Журнала Forbes [Электронный ресурс]. – Режим доступа: https://www.forbes.com/global2000/list/24/#header:country (дата обращения (21.04.2020); Официальный сайт телеканала РБК [Электронный ресурс]. – Режим доступа: https://www.rbc.ru/rbc500/ (дата обращения (21.04.2020); Официальный сайт нефтяной компании ЛУКОЙЛ [Электронный ресурс]. – Режим доступа: https://lukoil.ru/Company/BusinessOperation/GeographicReach (дата обращения (21.04.2020); Официальный сайт компании ОАО Беларусь-калий [Электронный ресурс]. – Режим доступа: https://kali.by/company/ (дата обращения (21.04.2020)]

Вместе с тем, нельзя не отметить и тот факт, что между рассматриваемыми странами были и периоды явного обострения отношений. Например,

- в 1998 г., когда в результате изменений системы тарифного и нетарифного регулирования во внешней торговле с третьими странами, а также в связи с введением дополнительной импортной пошлины на многие категории товаров, принятыми Россией в одностороннем порядке, между странами фактически разгорелся таможенный конфликт, который ощутимо ударил по экономике Белоруссии;
- в 2007 г. на фоне резкого повышения цен на газ, что стало шоком для белорусской экономики [6];
- в 2009 г. в ходе реализации "молочной войны", которая привела не только к негативным последствиям в развитии соответствующей отрасли двух стран, но и к периоду политической конфронтации;

Вместе с тем, нельзя не отметить и тот факт, что между рассматриваемыми странами были и периоды явного обострения отношений. Например,

- в 1998 г., когда в результате изменений системы тарифного и нетарифного регулирования во внешней торговле с третьими странами, а также в связи с введением дополнительной импортной пошлины на многие категории товаров, принятыми Россией в одностороннем порядке, между странами фактически разгорелся таможенный конфликт, который ощутимо ударил по экономике Белоруссии;
- в 2007 г. на фоне резкого повышения цен на газ, что стало шоком для белорусской экономики [6];
- в 2009 г. в ходе реализации "молочной войны", которая привела не только к негативным последствиям в развитии соответствующей отрасли двух стран, но и к периоду политической конфронтации;
- в 2014 г., когда разгорелся торговый конфликт, обусловленный неспособностью белорусской стороной выполнить обещание по недопущению поставок в Россию западных продуктов, подпадающих под эмбарго; объективными проблемами с качеством продукции ряда белорусских предприятий; а также раздраженностью российской стороной в плане неприсоединения Белоруссии к российским санкциям в отношении западных товаров;
- с 2019 г. по настоящее время в связи с экономическими потерями республики Беларусь от повышения цен на импортируемую из России нефть, в связи с введением в последней налога на добычу полезных ископаемых.

Таблица 3

Основные внешнеторговые партнеры России
(февраль 2019 г. – февраль 2020 г.) и Белоруссии (2019 г.)

Страны – покупатели			**Страны – поставщики**		
Страна	**Сумма, млрд. долл.**	**Доля, %**	**Страна**	**Сумма, млрд. долл.**	**Доля, %**
Основные внешнеторговые партнеры России					
Китай	59,6	13,4	Китай	58,1	22,3
Нидерланды	46,6	10,4	Германия	27	10,4
Германия	28,9	6,5	США	14,3	5,5
Турция	22,4	5	**Белоруссия**	**13,3**	**5,1**
Белоруссия	**20,8**	**4,7**	Италия	11,7	4,5
Южная Корея	17	3,8	Франция	9,65	3,7
Казахстан	15	3,4	Япония	9,41	3,6
Англия	15	3,4	Южная Корея	8,15	3,1
Италия	15	3,4	Казахстан	5,68	2,2
США	14,4	3,2	Польша	5,44	2,1
Основные внешнеторговые партнеры Белоруссии					
Россия	**13,67**	**41,2**	**Россия**	**22,0**	**55,9**
Украина	4,1	12,6	Китай	3,8	9,7
Великобритания и Северная Ирландия	2,3	7,0	Германия	1,7	4,4
Германия	1,3	4,0	Украина	1,7	4,3
Польша	1,3	3,9	Польша	1,3	3,4
Литва	1,1	3,2	Италия	0,8	2,0
Казахстан	0,8	2,5	Турция	0,8	1,9

Примечание: составлено авторами на основе обобщения источников [Официальный сайт Ru-Stat [Электронный ресурс]. – Режим доступа: https://ru-stat.com/ (дата обращения 26.04.2020); Официальный сайт Национального статистического комитета республики Беларусь [Электронный ресурс]. – Режим доступа: https://www.belstat.gov.by/ofitsialnaya-statistika/realny-sector-ekonomiki/vneshnyaya-torgovlya/ (дата обращения (26.04.2020)]

Мы полагаем, что в складывающихся в мировой экономике условиях, странам просто необходимо попытаться уйти от данных проблем и стать союзниками, а не соперниками. В XXI в. быть самостоятельным это – привилегия лидеров глобализации. Для РФ и Белоруссии максимально надежный вариант достижения желаемого уровня защищенности это – сотрудничество, в том числе в реализации оборонительной тактики при парировании внешних угроз. В качестве его возможных и перспективных направлений, ориентированных на защиту собственной национальной безопасности, мы предлагаем:

- сделать, в первую очередь, ставку на экономическое сотрудничество, поскольку именно экономическая безопасность выступает самым важным интересом национальной безопасности [9]. Достижению этой цели может способствовать последующее углубление процессов кооперирования на уровне

производства товаров и услуг обоих государств (например, уже сегодня ОАО "Белшина" закупает каучук в России и поставляет к нам порядка 70% своего экспорта);

- активизировать научно-техническое сотрудничество, что должно поспособствовать развитию национальных инновационных систем [7] и повысить, тем самым, уровень национальной конкурентоспособности (а, с ней и национальной безопасности). Данный шаг представляется одним из самых важных в XXI в. Его осуществление укладывается в концепцию формирования в скором времени фактически единой (на уровне мировой экономики) научной системы, за исключением разработок в военной сфере [2];

- продолжить углублять интеграционные связи, стремясь достигнуть действительно глубокой формы интеграции, при которой страны становятся способными развивать конкурентные преимущества друг друга, а не нивелировать сравнительные. Для этого, имеет смысл попробовать попытаться провести реиндустриализацию внутри ЕАЭС, которая позволит его участникам выйти на устойчивый экономический рост, стать более независимыми от политики стран-лидеров глобализации и отстоять собственную экономическую независимость [8];

- интенсифицировать приграничное сотрудничество, в том числе и в более широком формате, а не только Россия – Белоруссия (его базис официально был заложен еще в 1980 г. в рамках подписания Европейской рамочной конвенции о приграничном сотрудничестве; сегодня это – реально функционирующий Еврорегион "Неман"). Практика дает немало примеров того, что эффективное приграничное сотрудничество стран, находящихся на разных уровнях экономического развития, может способствовать не только решению локальных проблем, таких как, например, насыщение региональных рынков товаров и услуг, но и снимать напряженность в сфере национальной безопасности;

- консолидировать совместные усилия в решении глобальных проблем. Осуществляя сотрудничество в процессе противодействия общим угрозам, страны становятся сильнее в отражении внешних опасностей, носящих субъективный характер. В частности, следует попробовать использовать последствия мирового кризиса, связанного с пандемией COVID-19, в качестве триггера в активизации непосредственно российско-белорусских внешне-экономических связей, которые согласно всей предыдущей логике нашего исследования, должны способствовать повышению защищенности национальных интересов обеих стран от внешних угроз. В частности, известно, что уже в настоящее время между странами достигнута договоренность о поддержке продовольственных рынков друг друга (Россия будет поставлять в Белоруссию продовольствие – гречку и рис). Кроме того, возможно, руководству республики Беларусь следует пересмотреть свое недавнее решение о получении материальной помощи для борьбы с последствиями пандемии COVID-19 от международных структур и иностранных государств (в настоящее время Минск ведёт переговоры с правительствами ряда государств, со Всемирным банком, Международным валютным фондом (МВФ), банком развития Китая, Европейским инвестиционным банком и другими структурами и получении помощи в размере 2 – 2,5 млрд. долл.) в пользу России.

Понимая, что пределы национального суверенитета во внешнеэкономических и внешнеполитических решениях должны не просто существовать, но быть признаны страной–партнером, мы еще раз подчеркиваем, что в современном мире только объединив усилия, РФ и республика Беларусь смогут если и не в полной мере защитить свои национальные ценности от небезразличного для их народов и экономик ущерба, то попытаться сдержать своих соперников от активного вмешательства в вопросы национального развития.

Список литературы:

1. Евстафьев Д. Г. Глобализация и новые цивилизационные разломы: риски и перспективы для России и Евразии / Д. Г. Евстафьев // Геополитика и экогеодинамика регионов. – 2019. – Т. 5 (15). – № 1. – С. 22-33.

2. Козырская И. Е. Новые тенденции деглобализации в современной международной экономике: 2014 – 2016 гг. / И. Е. Козырская, Ю. В. Кузьмин, Т. П. Добровольская, Н. Р. Эпова // Восьмые востоковедные чтения БГУ: сб. науч. трудов. – Иркутск, 2017. – С. 65-72.

3. Кривохижа В. И. Россия в новой структуре международных отношений (Наброски к концепции национальной безопасности) / В. И. Кривохижа // Полис. Политические исследования. – 1995. – № 3. – С. 9

4. Маркина С. В. От стратегии "невоенных угроз" до стратегии "гибридной войны" вызовы национальной безопасности России / С. В. Маркина // Человеческий капитал – 2016. – № 11 (95). – С. 79-82.

5. Поздняков А. И. Основы теории национальной безопасности. Курс лекций / А. И. Поздняков // Альманах Пространство и время – 2013. – Т 2, №1. [Электронный ресурс].– Режим доступа: https://cyberleninka.ru/article/n/osnovy-teorii-natsionalnoy-bezopasnosti-kurs-lektsiy-lektsiya-1-kontseptualnye-osnovy-natsionalnoy-bezopasnosti-rossii/viewer (дата обращения (18.04.2020)

6. Ракова Е. Рост цен на газ: новые вызовы для белорусской экономики / Ракова Е., Точицкая И., Шиманович Г. // Рабочий материал Исследовательского центра ИПМ WP/07/03. [Электронный ресурс]. – Режим доступа: http://www.research.by/webroot/delivery/files/wp2007r03.pdf (дата обращения (26.04.2020)

7. Самаруха А. В. Развитие национальной инновационной системы / А. В. Самаруха, Г. И. Краснов // Известия Иркутской государственной экономической академии (БГУЭП). – 2011. – N 1. – С. 49-53.

8. Самаруха В. И. К вопросу об экономическом развитии ЕАЭС / В. И. Самаруха // Актуальные проблемы развития ЕАЭС в условиях современных глобальных изменений: материалы 1-й Всероссийской (национальной) научно-практической конференции. Иркутск, 13 декабря 2018 г. – Иркутск, 2019. – С. 189-195.

9. Санина Л. В. Экономическая безопасность на уровне регионов: трансформация подходов к определению / Л. В. Санина // Активизация интеллектуального и ресурсного потенциала регионов: материалы 4-й Всерос. науч.-практ. конф., г. Иркутск, 17 мая 2018 г.: в 2 ч. – Иркутск, 2018. – Ч. 1. – С. 353-362.

10. Сачек А. Г. Теоретический анализ элементов системы обеспечения экономической безопасности Республики Беларусь и Российской Федерации / А. Г. Сачек // Юридическая наука и практика: Вестник Нижегородской академии МВД России – 2015. [Электронный ресурс].– Режим доступа: https://cyberleninka.ru/article/n/teoreticheskiy-analiz-elementov-sistemy-obespecheniya-ekonomicheskoy-bezopasnosti-respubliki-belarus-i-rossiyskoy-federatsii/viewer (дата обращения (18.04.2020)

11. Светник Т. В. Российские корпорации в глобальном мире: новые тренды / Т. В. Светник // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права. – 2011. – № 6.

12. Тонких В. А. Национальная безопасность России в условиях современных вызовов и угроз / В. А. Тонких, Н. А. Лытнева. // Молодой ученый. – 2017. – № 11 (145). – С. 404-408. [Электронный ресурс]. – Режим доступа: https://moluch.ru/archive/145/40753/ (дата обращения: 22.04.2020)

13. Трусов Н. А. Методологические акценты понимания феномена национальной безопасности России / Н. А. Трусов // Марийский юридический вестник – 2016. – № 3 (18). [Электронный ресурс].– Режим доступа: https://cyberleninka.ru/article/n/metodologicheskie-aktsenty-ponimaniya-fenomena-natsionalnoy-bezopasnosti-rossii/viewer (дата обращения (15.04.2020)

14. Урсул А. Д. Безопасность в контексте глобальной устойчивости / А. Д. Урсул // Информационные войны. – 2018. – № 2. – С. 64–68.

НБ ГУМАНИТАРНЫЕ И ИНФОРМАЦИОННЫЕ АСПЕКТЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

УДК 159.9

Виноградов Олег Станиславович, доцент, к. т. н.,
ФГБОУ ВО «Московский государственный университет технологий и управления им. К.Г. Разумовского (ПКУ)», г. Пенза
Vinogradov Oleg Stanislavovich, «K.G. Razumovsky Moscow State University of technologies and management (the First Cossack University)», Penza

Виноградова Наталья Александровна, доцент, к. т. н.,
ФГБОУ ВО «Московский государственный университет технологий и управления им. К.Г. Разумовского (ПКУ)», г. Пенза
Vinogradova Natalya Aleksandrovna, «K.G. Razumovsky Moscow State University of technologies and management (the First Cossack University)», Penza

Бочкарева Людмила Петровна, доцент, к.пс.н,
ФГБОУ ВО «Московский государственный университет технологий и управления им. К.Г. Разумовского (ПКУ)», г. Пенза
Bochkareva Lyudmila Petrovna, «K.G. Razumovsky Moscow State University of technologies and management (the First Cossack University)», Penza

Чернышев Алексей Андреевич,
ФГБОУ ВО «Московский государственный университет технологий и управления им. К.Г. Разумовского (ПКУ)», г. Пенза
Chernyshev Alexey Andreevich,
«K.G. Razumovsky Moscow State University of technologies and management (the First Cossack University)», Penza

НЕКОТОРЫЕ АСПЕКТЫ ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ СОТРУДНИКОВ СЛУЖБ СПАСЕНИЯ
SOME ASPECTS OF PSYCHOLOGICAL SAFETY OF EMPLOYEES OF EMPLOYEES

Аннотация: в статье описан выбор поведенческой стратегии у сотрудников помогающих профессий в кризисном взаимодействии. Рассмотрены особенности реагирования на кризисную ситуацию. На примере спасателей, показана зависимость поведения сотрудников от акцентуаций их характера.

Abstract: the article describes the choice of a behavioral strategy for employees of assisting professions in crisis interaction. The features of responding to a crisis situation are considered. On the example of rescuers, the dependence of employee behavior on accentuations of their nature is shown.

Ключевые слова: поведение, взаимодействие, психология, спасатели, кризисная ситуация.

Keywords: behavior, interaction, psychology, rescuers, crisis.

Говоря о выборе поведенческой стратегии в рамках кризисного поведения необходимо отметить, что тщательность ее выбора будет зависеть от личностной значимости исхода конфликтной ситуации, насколько это связано и совпадает с интересами конфликтующих сторон.

Для того, чтобы профессиональная реализация представителей помогающих профессий была наиболее гармоничной, важным будет изучение взаимосвязи особенностей кризисного взаимодействия и акцентуаций характера у сотрудников. Для сотрудников это актуально, т.к. им приходиться вступать во взаимоотношения с конфликтными личностями и быть участниками разнородных кризисных ситуаций [1-3].

Первым шагом в диагностике этих показателей у спасателей МЧС стало тестирование с помощью опросника Леонгарда – Шмишека.

На рисунке 1 графически представлены полученные данные, где четко видно преобладание определенных типов акцентуированности характеров у испытуемых – спасателей.

Далее был произведен расчет среднегрупповых показателей, относительно акцентуированности характера лиц, принимавших участие в исследовании.

Вторым шагом в рамках проведения психодиагностических процедур стало проведение опроса с помощью методики описания поведения в конфликте К. Томаса для выявления поведенческих особенностей спасателей в рамках кризисного взаимодействия и определения поведенческой стратегии по его разрешению.

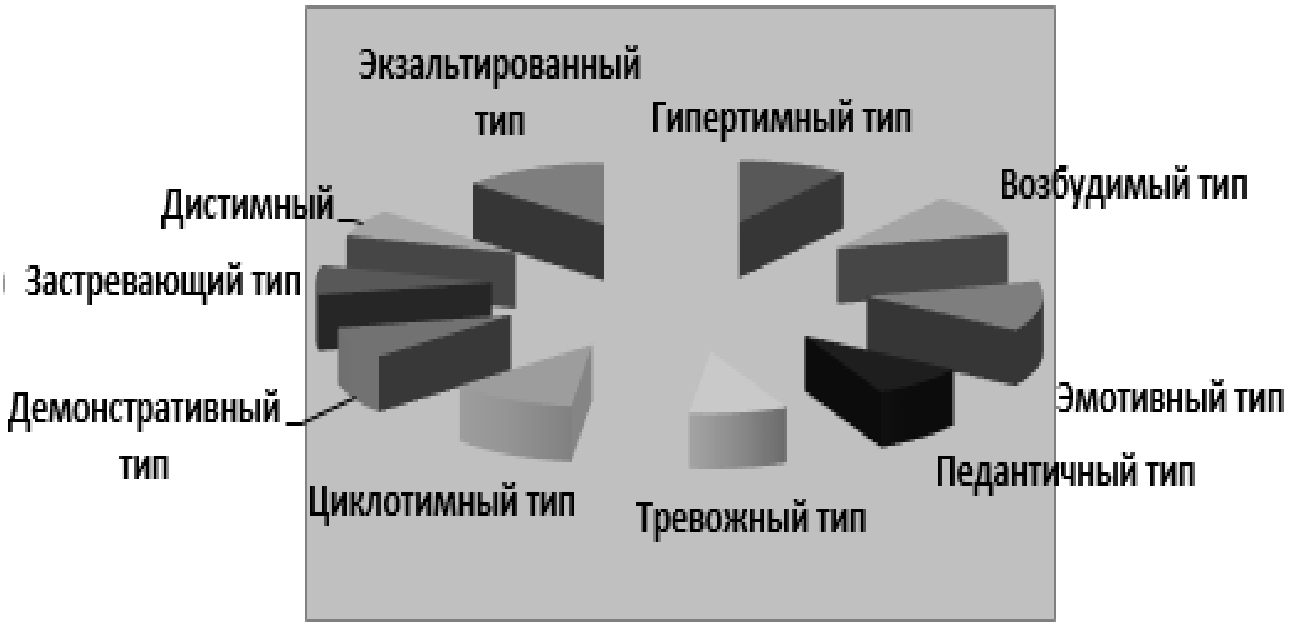

Рисунок 1 – Средние показатели диагностики акцентуированности характера спасателей

В ходе тестирования были получены определенные данные, усреднив которые была получена общая картина относительно выбора сотрудниками тех или иных поведенческих стратегий в кризисном взаимодействии.

Относительно количества выборов той или иной поведенческой стратегии информация представлена в процентном соотношении (см. рис. 2).

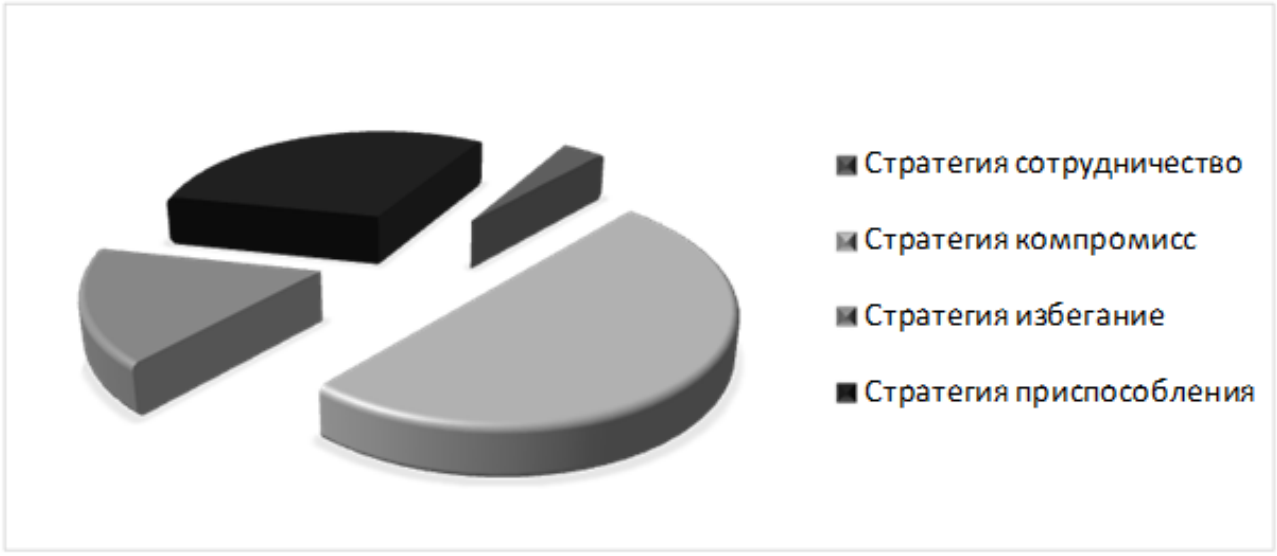

Рисунок 2 – Соотношение выборов сотрудниками МЧС поведенческих стратегий в кризисном взаимодействии

У испытуемых сотрудников МЧС преобладающими стали экзальтированный тип акцентуации характера у 33% и гипертимный тип у 23,1%. Это значит, что спасатели люди эмоциональные, не замкнутые и способные на оперативное реагирование в экстремальных ситуациях. То есть, такого рода результаты говорят о том, что при осознанном выборе профессиональной деятельности типа «Человек – Человек» [4-5], сотрудникам характерен высокий уровень чувствительности, эмпатии и эмоциональности.

С помощью критерия Спирмена были произведены расчеты, позволившие выявить корреляционно – значимые связи между выбором поведенческой стратегии сотрудников МЧС с характерными им акцентуациями характера.

Таким образом, результатом исследования явился тот факт, что представителям помогающих профессий, в нашем случае сотрудникам МЧС, в большей степени свойственны экзальтированный и гипертимный типы акцентуаций характера, что говорит о эмоциональности и чувственности личности. А математико – статистический анализ полученных результатов позволил доказать сформулированную в начале исследования гипотезу: выбор поведенческой стратегии у сотрудников помогающих профессий в кризисном взаимодействии зависим от акцентуаций их характера.

Список литературы:

1. Назарова О.М., Аверьянова А.В. Психологические особенности служебной деятельности женщин-сотрудников МЧС//В сборнике: Воспитание в современных условиях: региональный аспект Сборник научных статей по материалам Всероссийской научно-практической конференции. Под редакцией М А. Лыгиной, О.А. Логиновой, Л.Ю. Боликовой. 2018. С. 156-162.

2. Казаков В.А., Бареева Р.З., Сайфетдинова М.К. Роль производственной практики в формировании профессиональных навыков спасателей Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Экономические науки. 2010. № 3. С. 231.

3. Виноградов О.С., Виноградова Н.А., Кадакина Н.А., Малюкова И.О. Подготовка специалистов в области «Техносферной безопасности» в высшей школе//В сборнике: Актуальные проблемы физики и технологии в образовании, науке и производстве Материалах Всероссийской научно-практической конференции. 2019. С. 176-179.

4. Назарова О.М., Попова О.А., Сабурова Н.А. Коммуникативная компетентность и социальный интеллект как профессионально важные качества сотрудника МЧС /Вестник Саратовского областного института развития образования. 2019. № 4 (20). С. 72-77.

5. Гуляева Э.Ю. Психологическая и военно-патриотическая подготовка студентов «Техносферная безопасность»// В сборнике: Великая победа советского народа: история и вызовы современной России сборник статей Всероссийской научно-практической конференции. 2019. С. 20-24.

НБ ЭКОЛОГИЧЕСКИЕ АСПЕКТЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

УДК 632.983
DOI 10.37539/NB185.2020.33.51.005

Лазебный Михаил Юрьевич, Санкт-Петербургский государственный лесотехнический университет, г. Санкт-Петербург
Lazebnyiy Mikhail Yurievich,
Saint-Petersburg State Forest Technical University, Saint-Petersburg

Самсонова Ирина Дмитриевна, д. б. н., профессор,
Санкт-Петербургский государственный лесотехнический университет,
г. Санкт-Петербург
Samsonova Irina Dmitrievna,
Saint-Petersburg State Forest Technical University, Saint-Petersburg

ОЦЕНКА СОСТОЯНИЯ ИЛЬМОВЫХ И ОСОБЕННОСТИ РУБКИ ИХ В ЗЕЛЕНЫХ НАСАЖДЕНИЯХ ОБЩЕГО ПОЛЬЗОВАНИЯ САНКТ-ПЕТЕРБУРГА
EVALUATION OF THE STATE OF ILMOVS AND THE FEATURES OF THEIR HANDS IN GREEN PLANTS OF THE GENERAL USES OF ST. PETERSBURG

Аннотация: в настоящее время вязы, пораженные голландской болезнью, выявлены во всех 18 районах Санкт-Петербурга. Проведена оценка состояния ильмовых в зеленых насаждениях общего пользования, выявлена роль факторов их усыхания и проанализированы мероприятия по уходу за ними.

Abstract: currently, elms affected by the Dutch disease have been identified in all 18 districts of St. Petersburg. The state of elm trees in public green spaces was assessed, the role of their drying factors was revealed, and measures to care for them were analyzed.

Ключевые слова: ильмовые, графиоз, рубка, факторы.

Keywords: ilmovye, graphiosis, cutting, factors.

Городские насаждения страдают от множества факторов: сильная загазованность, уплотнение, иссушение, низкое плодородие и каменистость почвы, пониженная влажность воздуха, загрязнение строительным мусором и химическими отходами, своеобразный ветровой режим и резкий перепад температур, а также реагенты, используемые в зимний период. Санкт-Петербург в 2013 году признан одним из самых загрязнённых городов России, выбросы в воздух составляют 488 тыс. тонн в год. Основным источником загрязнения являются автомобили, на их долю приходится 85,9 % выбросов.

Основной ассортимент посадок на территории г, Санкт-Петербурга составляют такие виды деревьев и кустарников, которые могут длительное время произрастать в городских условиях, при этом не теряя своих декоративных качеств. В Санкт-Петербурге до эпидемии были наиболее распространены два вида вязов вяз гладкий (*Ulmus laevis Pall.)* и вяз голый *(Ulmus glabra Huds).* Вязы произрастали во всех видах городского озеленения. Именно так было до пандемии графиоза. Сейчас общее количество вязов в городе уже может исчисляться сотней деревьев, так как активная вырубка все время вносит коррективы в данные.

Цель работы – обследование зеленых насаждений общего пользования Санкт-Петербурга для оценки лесопатологического состояния ильмовых и проанализировать мероприятия по уходу за ними.

Исследования проводились на бульваре по улице Кораблестроителей, от Наличной улицы до Улицы Нахимова в г. Санкт-Петербурге, который относится к ведомству Василеостровского района. Бульвар – линейное насаждение, представляющую собой аллею, произрастающую с двух сторон от пешеходной части бульвара. Болезнь распространялась по корням деревьев.

Для подсчета индекса состояния древостоя использовались данные перечетов деревьев по категориям состояния и ступеням толщины на участке и коэффициенты облиственности деревьев разных категорий состояния.

В Санкт-Петербурге болезнь впервые была обнаружена в 1995 в пригороде г. Пушкина. В некоторых местах потеря вязов составила до 70%. На 2015 год зарегистрировано около 700 очагов голландской болезни [1].

Для контролирующего органа визуальный вид дерева является первым признаком для своевременного мониторинга за насаждением. При хроническом течении заболевания, весной пораженные графиозом вязы распускаются позже, чем здоровые, листовые пластинки уменьшаются, отчего крона приобретает ажурный вид. Усыхание ветвей начинается с верхушки и движется вниз. Дерево погибает в течение нескольких лет.

Информация об очагах болезни и здоровых деревьях доступна на следующей карте-схеме на срезовом участке «Бульвар ул. Кораблестроителей» по данным 2019 года (рис. 1).

Рисунок 1 – Схема поражения деревьев

К сожалению, даже самая современная мониторинговая станция не смогла бы предотвратить эту пандемию. Кубометры вязовой древесины, пораженной плодовыми телами, мицелием и продуктами жизнедеятельности грибов, утилизируются на свалке бытовых отходов за счет налогоплательщиков.

С 2009 году в рамках государственного мониторинга экологического состояния зеленых насаждений общего пользования идет сбор данных об очагах голландской болезни и здоровых насаждений вязов на территории всего города. Обновление электронной карты проводится ежегодно. В настоящее время вязы, пораженные голландской болезнью, выявлены во всех 18 районах Санкт-Петербурга. С 2016 года эти данные публикуются онлайн. С данными можно ознакомиться на сайте: http://grafioz2.myopencity.org/.

Оперируя данными, полученными в ходе наблюдений и исследований, согласно расчетам индекс состояния данного вяза равен 0,76 – в связи с чем можно отнести дерево к 3 категории состояния, что говорит о его повреждениях, по внешнему виду. Можно сделать заключение, что это вызвано нарушением обмена веществ в организме растения, разрушением хлорофилла в листьях, закупоркой сосудов и как следствие нарушением поступления воды и минеральных веществ. Что безусловно является первостепенными признаками Графиоза.

По нашим наблюдениям одним из негативных факторов является посадка некачественных саженцев, который впоследствии плохо приживается. Другим отрицательным действием является несоответствующий уход за посадочным материалом. Отдельным фактором негативного воздействия на зеленые насаждения хотелось бы выделить роль правильной подвязки молодого саженца [2].

Рубка деревьев производится на основании специального разрешения – порубочного билета, выдаваемого Комитетом по благоустройству Санкт-Петербурга. Производится разметка пораженных деревьев. Затем на участок

выезжает бригада рабочих под руководством мастера. Порубочные остатки вяза необходимо немедленно вывозить из насаждения и утилизировать. В технологическом процессе используют специальные технические средства, например, автогидроподъемники, бензопилы, щеподробильные машины и т.д. [3]. А также привлекаются специалисты самой квалификации, способные работать, как в кроне дерева, так и за ее пределами.

После рубки порубочные остатки, как правило, неэффективно утилизируются. Возможности переработки инфицированных порубочных остатков обширны. В острую стадию дерево усыхает за пару месяцев, от ствола отслаивается кора и оно приобретает мистический вид мертвого дерева. Подобные деревья использовать в качестве объектов современного искусства, а также в качестве декора в культурных местах или могут выполнять роль опор для освещения. Деревья, отобранные для такой роли, должны пройти обработку фунгицидом, и покрыты водоотталкивающим покрытием, например водостойким лаком для яхт. Это довольно хороший лак, качественный и он может применятся как средство защиты от влаги.

Еще одним вариантом монетизации сносимых вязов, должна быть деревообработка. За счет средств городского бюджета организовать деревообрабатывающее производство, куда принимал бы спиленные стволы, на безвозмездной основе. Это позволит сэкономить на плате за утилизацию порубочных остатков на свалке ТБО. Часть продукции реализовывать населению по доступной цене, равной себестоимости продукции. Изделия высших сортов реализовывать населению со средним доходом. Выделять из сортимента изделия сорта Люкс и Экстра. Возможно использовать спилы как сувенирную продукцию.

В ходе запланированной рубки приходится сталкиваться с разъяснением местному населению о выполняемых работах, что замедляет процесс сноса и уничтожения порубочных остатков. Это необходимо учитывать при расчете количества человеко-часов и трудозатрат в целом. Для эффективности производственного процесса необходимо ввести должность «Пресс-конферансье», который бы решал эту проблему и отвечал на интересующие вопросы граждан.

Список литературы:

1. Щербакова Л.Н. Мониторинг состояния вязов в г. Санкт- Петербурге в связи с распространением голландской болезни // Проблемы озеленения крупных городов: сб. матер. XX Междунар. практ. форума. М.: Перо, 2018. С. 129–132.

2. Лазебный М.Ю., Самсонова И.Д. Факторы негативного воздействия на зеленые насаждения общего пользования Санкт-Петербурга / «Лес-2020». 2020. № 56. С. 86-89

3. Лазебный М.Ю., Самсонова И.Д. Мониторинг состояния ильмовых в зеленых насаждениях общего пользования Санкт-Петербурга / В сборнике: Леса России: политика, промышленность, наука, образование Материалы пятой междун. науч.-техн. конф. Под ред. В.М. Гедьо. 2020. С. 363-366.

УДК 614.7+612.799.1(571.151-25)
DOI 10.37539/NB185.2020.23.63.004

Чанчаева Елена Анатольевна, д-р биол. наук, доцент,
Горно-Алтайский государственный университет, г. Горно-Алтайск
Chanchaeva Elena Anatolyevna, Gorno-Altaisk State University, Gorno-Altaisk

Лапин Виталий Сергеевич,
Горно-Алтайский государственный университет, г. Горно-Алтайск
Lapin Vitalij Sergeevich, Gorno-Altaisk State University, Gorno-Altaisk

Кузнецова Ольга Викторовна,
Горно-Алтайский государственный университет, г. Горно-Алтайск
Kuznecova Ol'ga Viktorovna, Gorno-Altaisk State University, Gorno-Altaisk

Куриленко Татьяна Калауиденовна, канд. биол. наук, доцент,
Горно-Алтайский государственный университет, г. Горно-Алтайск
Kurilenko Tat'yana Kalauidenovna,
Gorno-Altaisk State University, Gorno-Altaisk

Сидоров Сергей Сергеевич,
Горно-Алтайский государственный университет, г. Горно-Алтайск
Sidorov Sergey Sergeevich, Gorno-Altaisk State University, Gorno-Altaisk

К ВОПРОСУ ОБ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ АТМОСФЕРНОГО ВОЗДУХА ГОРОДСКОЙ АГЛОМЕРАЦИИ РЕСПУБЛИКИ АЛТАЙ
ON THE ISSUE OF ENVIRONMENTAL SAFETY ATMOSPHERIC AIR OF THE URBAN AGGLOMERATION OF THE ALTAI REPUBLIC

Аннотация: оценивали степень накопления тяжелых металлов в волосах домашних животных (*Canis lupus familiaris*) уличного содержания в условиях г. Горно-Алтайска. Оценку металлов (Cd, Pb, Cr, Cu, Mn) в волосах животных проводили атомно-абсорбционным методом. Установили, что концентрация Pb, Cr, Cu, Mn не превышает допустимые показатели. У большей части животных содержание Cd в волосах в 3.4 раза выше нормированного значения.

Abstract: the degree of accumulation of heavy metals in the hair of domestic animals (*Canis lupus familiaris*) of street care in Gorno-Altaisk was assessed. The content of metals (Cd, Pb, Cr, Cu, Mn) in animal hair was evaluated by atomic absorption method. It was found that the concentration of Pb, Cr, Cu and Mn does not exceed acceptable values. In most animals, the Cd content in the hair is 3.4 times higher than the limit value.

Ключевые слова: тяжелые металлы, животные, Горно-Алтайск.

Keywords: heavy metals, animals, Gorno-Altaisk.

Экологическое состояние атмосферного воздуха определяется промышленной, транспортной, теплоэнергетической и радиационной нагрузкой. Не маловажной значение имеет и рельеф местности, условия для выветривания поллютантов [1]. В связи с этим особого внимания в отношении экологической безопасности заслуживают регионы, которые в силу географических особенностей местности, входят в группу риска.

Загрязнение атмосферы техногенными выбросами связано со стратификацией атмосферы, величиной слоя перемешивания, скоростью ветра в слое 1,5 км. Сочетание метеорологических факторов, обуславливающих загрязнение атмосферы, представляет собой потенциал загрязнения. Известно, что очищение атмосферы от загрязняющих веществ, поступающих от различных источников, обусловлены мезо- и макромасштабными процессами – турбулентным обменом, высотой слоя перемешивания воздуха, режимом ветра т.д. Повторяемость и мощность инверсий связана с крупномасштабными атмосферными процессами. Наибольший уровень концентрации примесей в атмосфере отмечается в малоподвижных антициклонах и гребнях, на западной периферии антициклона или гребня, при адвекции тепла в малоподвижном небольшом по площади циклоне, в котором циркулирует одна и также воздушная масса. Концентрация вредных примесей увеличивается при туманах и дымках, которые аккумулируют вещества повышенной токсичности. Рассеиванию вредных примесей способствует быстро движущиеся циклоны, сильные фронтальные ветры, интенсивные осадки. Очищение атмосферы происходит при вторжении воздушных масс из Арктики, несущих чистый воздух [2].

Котловинообразное расширение долины, где расположен административный центр Республики Алтай (г. Горно-Алтайск) и незначительные перепады высот при существенной повторяемости антициклональной погоды обуславливают слабое самоочищение воздушного бассейна от загрязнителей. Метеорологические процессы в г. Горно-Алтайске, способствующие накоплению примесей в атмосфере, преобладают в течение всего года [3].

Среди наиболее токсичных веществ, формирующих загрязнение атмосферного воздуха, выделяют тяжелые металлы, при этом в первый класс токсичности относят Cd, Pb, Hg, As [4]. Для оценки экологического состояния атмосферного воздуха используют биоиндикационный метод. Животные ткани способны кумулировать тяжелые металлы, тем самым отражая экологическое состояние среды обитания. Волос – один из видов тканей, обладающий повышенной кумулятивной способностью, а сбор его образцов представляется удобным и нетравматичным. Цель исследования: оценить степень накопления тяжелых металлов в волосах домашних животных (*Canis lupus familiaris*) уличного содержания в условиях г. Горно-Алтайска.

Оценку тяжелых металлов в волосах животных (*Canis lupus familiaris*) проводили атомно-абсорбционным методом, при подготовке образцов для анализа использовали метод мокрого озоления.

В результате исследования установили, что модальные значения концентрации Pb, Cr, Cu, Mn не превышали предельно допустимые показатели (табл. 1).

Таблица 1

Концентрация тяжелых металлов
в волосах животных уличного содержания г. Горно-Алтайска (мг/кг)

показатели	Cd	Pb	Cr	Cu	Mn
ПДК	0.05	3.00	3.96	20.00	20.00
модальное значение	0.17	1.50	3.70	7.00	7.0
max	0.23	8.39	9.00	18.10	29.44
min	0.001	0.001	0.50	0.63	2.40

Лишь у 10% обследованных животных содержание Pb в волосах превышало предельные значения. Концентрация Cd в эктодермальной ткани животных в 3.4 раза выше допустимого показателя, при этом высокие концентрации экотоксиканта выявлены у большей части животных. По данным литературы [5], содержание тяжелых металлов в водопроводной, речной и грунтовой воде г. Горно-Алтайска не превышает допустимых значений. Следовательно, одним из наиболее вероятных путей поступления токсиканта в организм животных является вдыхание мелкодисперсных твердых частиц от выбросов твердотопливных отопительных систем и выхлопов двигателей внутреннего сгорания. Кроме этого, поверхность волоса способна абсорбировать химические вещества из внешней среды, поэтому оседание на шерсти собак пыли, твердых частиц с примесями Cd также является вероятным путем накопления микроэлемента. Учитывая условия слабого самоочищения воздушного бассейна города, высока вероятность накопление загрязнителей в приземной части, а значит и аккумуляция в животной ткани. Из всех оцениваемых нами микроэлементов Cd обладает крайне низкой экскреторной способностью (0.001% в сутки), этим обусловлено регламентированное значение (0.05 мг/кг) в животной ткани, которое в 60-400 раз ниже других элементов. Таким образом, микроэлементный состав волос животных г. Горно-Алтайска позволяет предположить о вероятном пролонгированном воздействии Cd на животное звено биоценоза.

Список литературы:

1. Щербатюк А. В. Стратегия оптимизации управления экологической безопасностью воздушной среды городов в условиях внутриконтинентальных межгорных котловин // Экологическая безопасность строительства и городского хозяйства. 2018. № 1. С. 29-34.

2. Исаев А. А. Экологическая климатология. М. : Научный мир, 2003. 470 с.

3. Chanchaeva E.A., Sukhova M.G., Sidorov S.S. Problems of the health status of children and atmospheric air of Gorno-Altaisk under the conditions of increasing transport load // IOP Conference Series: Earth and Environmental Science. 2019. Vol. 395. pp. 1-5. DOI: 10.1088/1755-1315/395/1/012004

4. Olumayede E. G., Ediagbonya T. F., Ojiodu C., Oguntimehin I. Particle-Size Distribution and Bioaccessibility of Metals-Loaded in Street Dust of Urban Center in Southwest Nigeria // Preprints. 2017. DOI: 10.20944/preprints201710.0109.v1

5. Робертус Ю.В. Индикация компонентами природной среды трансграничного переноса загрязняющих веществ на территорию Горного Алтая // Известия Томского политехнического университета. Инжиниринг георесурсов. 2016. № 9. С. 39-48.

УДК 332
DOI 10.37539/NB185.2020.63.91.003

Болгова Елена Владимировна, к.э.н., доцент,
Самарский государственный экономический университет, г. Самара
Bolgova Elena Vladimirovna, Samara State University of Economics, Samara

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ПАНДЕМИИ КОРОНАВИРУСА: РЕГИОНАЛЬНЫЙ АСПЕКТ
ECONOMIC SECURITY IN THE CONDITIONS OF THE CORONAVIRUS PANDEMIC: REGIONAL ASPECT

Аннотация: выполнен анализ факторов обеспечения экономической безопасности регионов в условиях пандемии коронавируса, исследованы возможности региональных институтов и мер поддержки экономики, предложено создание инициативных экспертных институтов.

Abstract: the analysis of factors ensuring the economic security of the regions in the context of the coronavirus pandemic is carried out, the possibilities of regional institutions and measures to support the economy are investigated, the creation of initiative expert institutions.

Ключевые слова: регион, экономическая безопасность, инициативные институты.

Keywords: region, economic security, initiative institutions.

Территориальный аспект экономической безопасности традиционно определяют как уязвимость перед другими государствами [1, 2]. Пандемия коронавируса привела к пересмотру определения экономической безопасности в свете рисков, создаваемых распространением заболевания в отдельных странах мира, в российских регионах. В этих условиях взаимосвязь между пандемией коронавируса и экономической безопасностью должна быть четко определена, а суждения о региональном аспекте экономической безопасности должны содержать тщательную оценку последствий распространения пандемии, возросшей нестабильности улучшения показателей социально-экономического развития субъекта РФ в долгосрочной перспективе [3, 4, 5].

Созданные для преодоления последствий пандемии институты могут компенсировать экономическую незащищенность российских регионов посредством предоставления мер поддержки. В составе институтов национальные играют центральную роль в обеспечении экономической безопасности, а региональные дополняют возможности национальных институтов, смягчая экономическую нестабильность. Несмотря на то, что некоторые региональные институты повторяют меры поддержки национального уровня, их роль в

преодолении последствий пандемии очень высока, а региональные инициативы могут создавать новые формы экономической безопасности. Перечень новых форм экономической безопасности определен угрозами, вывить которые позволяет проведение в регионе социологического исследования состояния экономики. Анализ финансово-экономических показателей предприятий (учреждений) субъекта РФ, пострадавших от пандемии коронавируса, в разрезе общероссийского классификатора видов экономической деятельности (ОКВЭД), форм собственности, организационно-правовых форм (ОПФ), а также разработка экспресс-прогноза развития сфер экономики, пострадавших от коронавируса, создает количественные оценки угроз. Оценка эффективности мер поддержки и разработка цифровых платформ и технологий оперативного мониторинга являются инструментами обеспечения экономической безопасности, эффективным способом «перезапуска» экономики регионов.

В ходе реализации региональных инициатив проведение социологического опроса представителей организаций наиболее пострадавших сфер деятельности, преследует цель изучить предложения по преодолению текущей негативной ситуации, оценить актуальность мерам государственной поддержки. Опрос в формате сплошного онлайн-анкетирования субъектов экономики с рассылкой анкет через созданную специально для целей исследования электронную почту, онлайн- и явочного опроса фокус-групп через СМИ и официальные сайты профильных министерств, институтов развития, администраций муниципальных образований, профессиональных онлайн-сообщества, посредством контактов в социальных сетях реализует задачу сохранения устойчивости экономики.

Проведение мониторинга финансово-экономического состояния системообразующий предприятий и отдельных сфер деятельности решает задачу выявления наиболее уязвимых сфер экономики, пострадавших от коронавируса, и локальных групп организаций, нуждающихся в дополнительных (регионального уровня) мерах поддержки. Мониторинг параметров занятости, среднемесячной заработной платы, выручки и основных статей расходов (на оплату труда, арендные платежи, проценты по кредитам, амортизацию), позволяет проводить анализ суммы выпадающих доходов, планировать объем компенсационных выплат за счет бюджетных источников. Экспресс-прогноз влияния пандемии коронавируса на экономику регионов является результатом обобщения итогов анкетирования, количественной оценкой масштабов экономических потерь. Статистические методы прогнозирования, основанные на методиках мировых аналитических агентств, создают информационную базу для оценки потерь экономики, корректировки действующих прогнозов ВРП, ВРП на душу населения, ВДС по отраслям экономики, численности занятых, утвержденных в стратегических документах социально-экономического развития.

Цифровые платформы состояния экономики являются инструментами мониторинга финансово-экономических показателей системообразующих предприятий региона, оказавшихся в зоне риска, позволяют профильным министерствам и хозяйствующим субъектам в режиме реального времени формировать, агрегировать и анализировать условия и риски развития.

Опыт европейских стран, а также лучшие региональные практики РФ показывают, что организационным фактором обеспечения экономической безопасности являются институты, созданные в субъектах страны для преодоления последствий пандемии. Институты регионального управления (оперативные штабы), институты в сфере здравоохранения (региональные управления Роспотребнадзора), финансовые институты (региональные отделения ЦБ РФ) действуя оперативно, помогают свести к минимуму экономическую незащищенность российских регионов. Вместе с тем, высокая информационная неопределенность ситуации, когда 100% решений приходится принимать в условиях 50% нужной и достоверной информации, требует создания инициативных институтов в составе научного экспертного сообщества, общественных институтов мониторинга, экспертизы, поддержки. Высокая роль научного экспертного сообщества в создании новых форм экономической безопасности определяется тем, что указанный институт является формой диалога, интерфейсом между органами власти и обществом, а его функция сводится к минимизации информационной неопределенности, установлению связей и контактов, необходимых в решении оперативных задач. Слаженность работы официальных и инициативных институтов формирует многосторонние действия, закладывает основы долгосрочных стратегий предотвращения угроз экономической безопасности в условиях вероятного распространения пандемии любого типа.

Список литературы:

1. Kay L. Gibson, Glyn M. Rimmington, Marjorie Landwehr-Brown. (2008) Developing Global Awareness and Responsible World Citizenship With Global Learning. Roeper Review 30:1, pp. 11-23.

2. Miles Kahler (2006) Economic security in an era of globalization: definition and provision. The Pacific Review, Volume 17, pp. 485-502

3. Irene Chan. (2019) Reversing China’s Belt-and-Road Initiative–Singapore’s Response to the BRI and Its Quest for Relevance. East Asia 36:3, pp 185-204.

4. V. Levchenko, A. Boyko, T. Savchenko, V. Bozhenko, Yu. Humenna, R. Pilin. (2019) State Regulation of the Economic Security by Applying the Innovative Approach to its Assessment. Marketing and Management of Innovations: 4, pp. 364-372.

5. Oleksandr Cherevko, Serhiy Nazarenko, Nataliia Zachosova, Nataliia Nosan, S. Semerikov, V. Soloviev, L. Kibalnyk, O. Chernyak, H. Danylchuk. (2019) Financial and economic security system strategic management as an independent direction of management. SHS Web of Conferences 65, pp. 03001.

УДК 614.8.084
DOI 10.37539/NB185.2020.69.99.007

Ильин Алексей Павлович, кандидат технических наук, доцент,
Вологодский государственный университет, г. Вологда
Ilyin Alexei Pavlovitch, Vologda State University, Vologda

Чернышов Олег Александрович, начальник технической группы, Центр обеспечения региональной безопасности Вологодской области, г. Вологда
Tchernychov Oleg Alexandrovitch,
Regional Security Center of the Vologda Region, Vologda

СИСТЕМА-112: ОПЫТ ВНЕДРЕНИЯ НА ТЕРРИТОРИИ ВОЛОГОДСКОЙ ОБЛАСТИ
SYSTEM-112: EXPERIENCE OF IMPLEMENTATION IN THE VOLOGDA REGION

Аннотация: в статье комментируется опыт внедрения системы-112 в Вологодской области, называется нормативная база, определяющая использование данной системы, характеризуются её структура и факторы, обеспечивающие эффективное функционирование системы-112 на территории региона.

Abstract: the article comments on the experience of implementing the system-112 in the Vologda region, describes the regulatory framework that determines the use of this system, describes its structure and factors that ensure the effective functioning of the system-112 in the region.

Ключевые слова: защита в чрезвычайных ситуациях, система связи и оповещения населения, система-112.

Keywords: emergency protection, communication and public notification system, system-112.

Основополагающими качествами коммуникационных систем в практике обеспечения защиты и безопасности являются системность, оперативность, универсальность и общедоступность. Поэтому переход регионов к единому номеру вызова экстренных служб (система-112) относится к числу актуальных технических задач. Решение этой задачи осуществляется силами регионов и с привлечением региональных бюджетных средств, поэтому анализ практики внедрения системы-112 даёт возможность обеспечить её максимально эффективную работу при оптимальных затратах. Это определяет актуальность темы нашего исследования. Его цель – изучение нормативно-правовой базы внедрения системы-112, истории её создания, а также разработка рекомендаций по достижению оптимального качества обслуживания населения ресурсами данной системы в указанном регионе.

Система-112 – это система обеспечения вызова экстренных оперативных служб по единому номеру «112» на территории Российской Федерации. Данная система призвана обеспечивать оказание экстренной помощи населению, а также функционирование единых дежурно-диспетчерских служб (ЕДДС)

муниципальных образований. Деятельность системы-112 регламентирована Федеральными законами «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» (№ 68-ФЗ от 21 декабря 1994 г.), «О пожарной безопасности» (№ 69-ФЗ от 21 декабря 1994 г.); «О средствах массовой информации» (№ 2124-1 от 27 декабря 1991 г.); «О связи» (№ 126-ФЗ от 7 июля 2003 г.), а также Постановлениями Правительства Российской Федерации и Указами Президента Российской Федерации, утверждающих перечень экстренных оперативных служб, определяющих единый номер вызова экстренных оперативных служб, инициирующих создание локальных систем оповещения, а также комплексной системы экстренного оповещения населения об угрозе возникновения или о возникновении чрезвычайных ситуаций. На региональном уровне эту деятельность регламентируют Постановления Губернатора Вологодской области, инициировавшие развертывание на территории Вологодской области системы обеспечения вызова экстренных оперативных служб по единому номеру «112» (№ 87 от 01.03.2012) и обеспечивающие постоянную готовность использования системы оповещения и информирования населения Вологодской области об угрозе возникновения или возникновении чрезвычайных ситуаций природного и техногенного характера, а также об опасностях, возникающих при военных конфликтах или вследствие этих конфликтов (№ 614 от 17.06.2013).

Предпосылками разработки и внедрения системы-112 является, во-первых, наличие высокого уровня рисков техногенного и природного характера, негативных последствий чрезвычайных ситуаций для устойчивого социально-экономического развития страны, во-вторых, значительный уровень количества пострадавших в чрезвычайных ситуациях, а также высокие показатели прямого и косвенного ущерба от происшествий и чрезвычайных ситуаций; в-третьих, необходимость защиты жизни и здоровья граждан, сохранности имущества, обеспечение личной и общественной безопасности; наконец, учёт опыта зарубежных стран и международных организаций [1]. Внедрение системы-112 в регионах осложнялось организационной и технической разрозненностью аварийных дежурно-диспетчерских служб, что влекло за собой отсутствие своевременного оповещения и информирования о чрезвычайных происшествиях и ситуациях всех заинтересованных служб города (района), искажение и дублирование информации, затрудняло управление аварийными службами и обеспечение их взаимодействия, получение объективной статистической информации об их работе.

В соответствии с Постановлением Правительства РФ № 894 от 31 декабря 2004 система-112 формируется на основе объединения единых дежурно-диспетчерских служб муниципальных образований (ЕДДС) и дежурно-диспетчерских служб (ДДС) следующих экстренных оперативных служб: а) служба пожарной охраны; б) служба реагирования в чрезвычайных ситуациях; в) служба полиции; г) служба скорой медицинской помощи; д) аварийная служба газовой сети; е) служба «Антитеррор». В 2013 году была принята Федеральная целевая программа «Создание системы обеспечения вызова экстренных оперативных служб по единому номеру «112» в Российской Федерации на 2013-2017 годы», государственным заказчиком, координатором и разработчиком которой

является Министерство по чрезвычайным ситуациям Российской Федерации. С этого же времени создание системы-112 разворачивается и в Вологодской области. Эта система осуществляет прием и обработку обращений граждан по вопросам экстренного характера; передачу данных о происшествии в службы экстренного реагирования; привлечение специалистов служб лингвистической или психологической поддержки к обслуживанию заявителей; консультацию граждан по вопросам, не требующим реагирования; получение информации о принимаемых мерах по реагированию и о завершении отработки сообщения о происшествии; подготовку и выгрузку отчетов для анализа работы системы-112; технический мониторинг работоспособности системы-112 на территории Вологодской области. Внутри системы выделяют шесть подсистем: *телекоммуникационную* (она обеспечивает прохождение сообщений от пользователей (абонентов) сетей фиксированной или подвижной радиотелефонной связи), *информационно-коммуникационную* (хранит и актуализирует базы данных, осуществляет обработку информации, а также информационно-аналитическую поддержку принятия решений по экстренному реагированию на принятые вызовы), *геоинформационную* (отображает характеристики территории и местонахождение лица, обратившегося по номеру "112", а также местонахождение транспортных средств экстренных оперативных служб), *мониторинговую* (предназначена для приёма и обработки информации и сигналов, поступающих от датчиков, установленных на контролируемых стационарных и подвижных объектах), *консультационную* (служит для оказания информационно-справочной помощи по вопросам обеспечения безопасности жизнедеятельности), а также подсистему, обеспечивающую *информационную безопасность* данных, хранящихся в системе-112. Все перечисленные виды деятельности осуществляются в Вологодской области силами следующих подразделений: а) Центр обработки вызовов (ЦОВ); б) Резервный центр обработки вызовов (РЦОВ); в) Единые дежурно-диспетчерские службы (ЕДДС); г) Дежурно-диспетчерские службы экстренных оперативных служб (ДДС). Система-112 взаимодействует со многими внешними автоматизированными информационными системами: это система «ЭРА-ГЛОНАСС»; АПК «Безопасный город»; системы обеспечения вызова экстренных оперативных служб по единому номеру «112» сопредельных субъектов Российской Федерации: Архангельская область, Ленинградская область (ООО «СВЕТЕЦ Интегро»), Новгородская область (НТЛ «НЭКСТ ТЕХНИКА»), Тверская область (ЗАО «Сфера»), Ярославская область (АО «ИскраУралТЕЛ»), Костромская область (ГК «ТЕЛЕКОР»), Кировская область, Республика Карелия (АО «ИскраУралТЕЛ»); система мониторинга подвижных объектов «АвтоТрекер» (ОАО «Русские Навигационные Технологии»); система мониторинга стационарных объектов на базе АС ОСОДУ (ЦИЭКС, ЗАО «ИНСИСТЕМ–Инженерные системы»); службы скорой медицинской помощи – система «АДИС» («Новые системы и технологии»), функционирующей в Вологде, Череповце, Великом Устюге и Соколе). Система-112 в Вологодской области является территориально-распределенной автоматизированной информационно-управляющей системой, она создаётся в административных границах Вологодской области, предусматривает создание ЦОВ-112 и РЦОВ-

112 в административном центре субъекта Российской Федерации – городе Вологде, а также установку в муниципальных образованиях оборудования СПД для обеспечения взаимодействия автоматизированных рабочих мест ЦОВ-112/РЦОВ-112, ЕДДС и ДДС. Система-112 создается с централизованным приемом и обработкой вызовов в ЦОВ-112/РЦОВ-112, с централизованным предоставлением комплекса инфокоммуникационных услуг, обеспечивающих необходимую функциональность системы-112 (в том числе хранение информации). Обмен голосовой информацией и данными внутри системы-112 возможно осуществлять по выделенной сети передачи данных, организованной по технологии IP/MPLS L3VPN на каналах связи операторов связи ПАО «Ростелеком» и ПАО «МегаФон».

Помимо оптимизации технических характеристик системы-112 определяющее значение для совершенствования её функционирования имеет обучение персонала. В Вологодской области создается инфраструктура обучения, которая предназначена для подготовки, аттестации и переподготовки штатного персонала ЦОВ и ЕДДС, а также для подготовки диспетчеров ДДС.

Обучение реализуется в специально оборудованных классах и организовано на базе бюджетного образовательного учреждения Вологодской области «Учебно-методический центр по гражданской обороне и чрезвычайным ситуациям». Оно проводится в форме дополнительного профессионального образования посредством реализации дополнительных профессиональных программ. Персонал, привлекаемый к выполнению задач системы-112, допускается к исполнению служебных обязанностей при наличии удостоверения или диплома об успешном освоении соответственно программы повышения квалификации или программы профессиональной переподготовки [2].

Анализ опыта внедрения системы 112 на территории Вологодской области показывает, что организация единого центра приёма сообщений граждан о чрезвычайных ситуациях, позволяет оптимизировать и повысить эффективность функционирования экстренных служб по оказанию помощи населению и ведению аварийно-спасательных и других неотложных работ.

Список литературы:

1. Маурин, И.Ф. Опыт создания службы «112» в Европе, гармонизация отечественной и зарубежных систем в соответствии с законодательством Европейского союза [Текст] / И.Ф. Маурин // Пожарная безопасность: проблемы и перспективы. – Воронеж : Воронежский институт Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, 2013. – № 1 (4). – С. 35-39.

2. Методические рекомендации по организации обучения персонала, привлекаемого к выполнению задач системы-112 от 02.09.2014 г. [Электронный ресурс]. – URL: http://112.mchs.ru/metod_rekomend

УДК 338.47
DOI 10.37539/NB185.2020.55.61.010

Копкова Елена Сергеевна, Трушин Сергей Николаевич,
Национальный Исследовательский Ядерный Университет «МИФИ», г. Москва
Kopckova Elena, Trushin Sergey Nikolaevich,
National Research Nuclear Unuversity «MEPHI», Moscow

РОЛЬ СЕВЕРНОГО МОРСКОГО ПУТИ КАК ФАКТОРА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ
THE ROLE OF THE NORTHERN SEA ROUTE AS A FACTOR OF NATIONAL SECURITY

Аннотация: Северный морской путь (СМП) становится все более актуальной сферой интересом для многих стран. Большая часть арктических территорий принадлежит России. Это стратегические запасы природных ресурсов, а также водные акватории, транспортная артерия – СМП. Развитие СМП, а также международное сотрудничество в области его использования является вопросом национальной безопасности.

Abstract: The Northern sea route (NSR) is becoming an increasingly relevant area of interest for many countries. Most of the Arctic territories belong to Russia. These are strategic reserves of natural resources, as well as water areas, and the transport artery – the NSR. The development of the NSR, as well as international cooperation in its use, is a matter of national security.

Ключевые слова: Северный морской путь (СМП), Арктическая зона РФ, северные территории, национальная безопасность.

Keywords: Northern Sea Rout (NSR), Arctic zone of the Russian Federation (RF), Northern territories, national security.

Введение. В последние годы становится актуальной тема Северного морского пути (далее СМП). СМП – морская артерия, кратчайшим образом соединяющая европейскую часть России с Дальним востоком. Он проходит через Карское море, море Лаптевых, Восточно-сибирское и Чукотское моря. Соединяя порты северного побережья России, он также объединяет между собой и бассейны сибирских рек. Длина пути составляет около 5600 км от Карских ворот до бухты Провидения, на протяжении которых Россия устанавливает режим прохода судов в соответствии с Конвенцией ООН по морскому праву [4]. Его освоение, сохранение суверенитета, а также международное сотрудничество тесно сопряжено с вопросом национальной безопасности нашей страны.

Основные проблемы обеспечения национальной безопасности в Арктической зоне РФ рассмотрены в трудах таких исследователей как Васильева А.М., Васильева В.В., Вышинской Ю.В., Гасниковой А.А., Зерщиковой Н.И., Козьменко С.Ю., Котомина А.Б., Николаевой А.Б., Победоносцевой Г.М., Селина В.С., Туиновой С.С., Ульченко М.В., Щегольковой А.А. В частности аспекты взаимосвязи СМП и национальной безопасности – Семченков А.С., Несоленая А.К., Пирцхалава Н.Р., Лагуткин А.В., Стороженко О.М.

Особенности развития СМП, его роль как фактора осуществления национальной безопасности СМП является альтернативным маршрутом для так называемого Южного маршрута, соединяющего Европу с Азией через

Суэцкий и Панамский каналы, длина которого короче практически вдвое. Сокращение протяженности маршрута не только позволяет снизить временные затраты в пути, но затраты на топливо, оплату труда, фрахт судна. Развитие СМП способствует укреплению национальной безопасности Российской Федерации, развитию масштабных проектов по добыче и реализации природных ресурсов, развитию альтернативной Суэцкому маршруту независимой транспортной системы, росту уровня жизни на северных территориях нашей страны.

СМП позволяет доставлять грузы из отдаленных северных территорий, таких как: Норильск, Ямал и др. Поддержание сообщения с этими отдаленными районами трудоемко и ресурсозатратно. В таких условиях СМП становится доступной альтернативой для доставки потребительских товаров, промышленных грузов и топлива в районы, отрезанные от большой части стратегических районов России. Таким образом, СМП поддерживает территории и население Арктической зоны РФ, способствуя их экономическому развитию.

Следует отметить, что в сумме ресурсы Арктики оцениваются примерно в 30 триллионов долларов. Это 40 % общероссийских запасов золота и нефти, а также стратегические запасы – 80 % природного газа, 90 % запасов хрома и марганца. Обширными запасами углеводородного сырья обладают Баренцево, Карское и Восточно-Сибирское моря. Разработки нефтяных месторождений ведутся наиболее активно в Баренцевом и в Карском морях. Это обусловлено климатическими и природными условиями, а также близостью шельфов зон этих морей к европейской части России, а, следовательно, и основным потребителям.

Отсюда вытекает актуальность основной проблемы арктического региона – плохой транспортной системы. Как раз решением этой проблемы в первую очередь является СМП. Он способен удовлетворить растущий спрос на арктические грузоперевозки. Это транспортировка полезных ископаемых, добываемых в регионе, продовольствия, техники, стройматериалов для создания инфраструктуры. Значительную часть спроса способен покрыть СМП, обеспечив дешевые грузоперевозки в районы нового освоения.

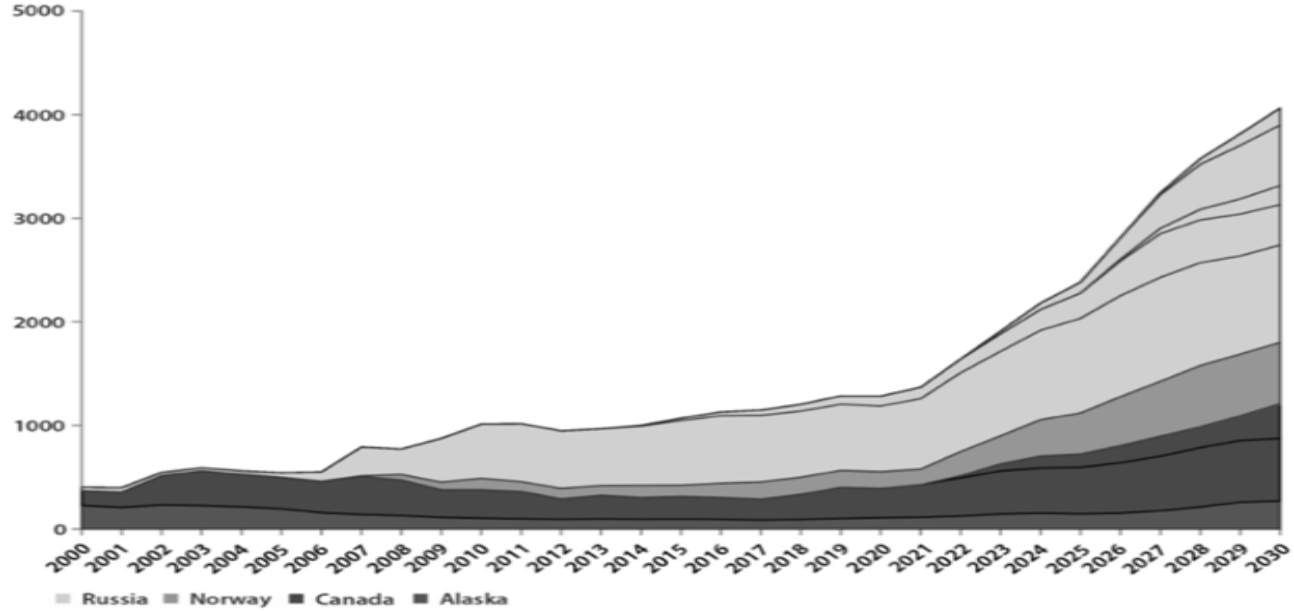

Рисунок 1 – Прогноз добычи шельфовых ресурсов до 2030[3]

Как видно из графика (рис. 1) в последние годы наблюдается рост добычи полезных ископаемых на арктическом шельфе. И, как уже говорилось ранее, это, безусловно, спровоцирует рост спроса на арктические перевозки. Но также необходимо рассмотреть, ряд особенностей, усложняющих развитие СМП. Так, на маршруте СМП малые глубины, что препятствует прохождению крупных судов с большой осадкой. Кроме того, гидрография этого района изучена слабо, что еще больше осложняет построение маршрутов для судов. Статистика аварийности мирового флота показывает, что аварийность увеличивается при возрастании интенсивности судоходства, при росте тоннажа судов, в мелководных районах с недостаточной гидрографической изученностью, при несоответствии конструкции судов ледовым условиям, при нарушении правил маневрирования в сложных гидрометеорологических условиях, при буксировках, движении в караванах и при других обстоятельствах. Для успешного развития СМП необходимо проведение гидрографических исследований на протяжении всего маршрута. Также необходимо модернизировать портовую инфраструктуру, обновить арктический флот.

Если рассматривать вопрос национальной безопасности, то следует изучить геополитическое положение Арктической зоны РФ. Непосредственное отношение к Арктике имеют 20 стран, 5 из которых имеют арктическую границу: Россия, США, Норвегия, Канада и Дания. Среди государств Арктического совета – Россия, Исландия, Финляндия, Дания, Норвегия, Швеция. На арктических территориях возрастает европейское влияние. Польша, Испания, Италия, Франция, Великобритания, ФРГ и Нидерланды – являются странами наблюдателями [1]. Возрастает интерес Японии, Индии, Сингапура и Республики Корея. Сферы интереса: проведение арктических научных исследований, создание судов готовых работать в сложной ледовой обстановке, разработка технологий добычи углеводородов. Кроме того – транспортная и торгово-экономическая интеграция Евразии – «Один пояс, один путь», в рамках которой этот СМП позволит обеспечить сообщения между КНР и ЕС [2].

Говоря о росте спроса на арктические перевозки, стоит сказать о том, что китайские инвесторы все больше интересуются темой северных перевозок. В СМП привлекает его небольшая по сравнению с Суэцким маршрутом протяженность. Желание Китая использовать СМП может благоприятно сказаться на развитии Арктической зоны РФ, как источник привлечения инвестиционного капитала других стран. Принятие китайские инвестиции и допущение Китая в российскую Арктику позволит получить доступ к новым инвестиционным ресурсам, что в свою очередь позволит более эффективно развивать российскую Арктику и повысит уровень жизни в Арктической зоне РФ. Фактором, наиболее сильно тормозящих развитие СМП в сотрудничестве с Китаем, является устаревшая инфраструктура.

И еще один факт в пользу СМП. Говоря о рисках и безопасности, необходимо упомянуть риски пиратства. В морских перевозках, особенно через Суэцкий канал, риски пиратства очень велики. Для того, чтобы избежать грабежа грузов, выкупа членов экипажа, корабли ускоряются при проходе возле побережья Сомали. Расход топлива при этом увеличивается, на корабли также приходится нанимать команды охраны. Суммарно на каждый проход мимо

Сомали, стоит для корабля 70000 долларов в среднем. При проходе по СМП такие риски попросту отсутствуют, что положительно сказывается на рисках для транспортных компаний, занимающихся перевозками по СМП.

Заключение. СМП на сегодняшний день является фактором снижения угроз национальной безопасности. Его развитие позволит укрепить существующие партнерские отношения России с другими странами, заинтересованными в эксплуатации СМП, снизить геополитические риски. Кроме того подобное сотрудничество со странами оппонентами, например Японией, также внесет положительный вклад. Однако не стоит забывать про сохранение национального суверенитета, усиление которого потребует значительного вклада в освоение СМП и модернизацию инфраструктуры.

Список литературы:

1. Лагуткин А.В. Северный морской путь – стратегическая составляющая экономического развития и национальной безопасности России // Образование и право. 2017. № 8. С. – 42-44.

2. Семченков А.С., Несоленая А.К. Северный морской путь как инструмент снижения угроз национальной безопасности России // Проблемы современных процессов 2019. №1. С. 79-87.

3. Издательство «Известия» «Прогноз добычи шельфовых ресурсов до 2030» [электронный ресурс]. Режим доступа URL: https://iz.ru/news/588397

4. Организация Объединенных Наций «Конвенция ООН по морскому праву» [электронный ресурс]. Режим доступа URL: https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_r.pdf

УДК 378.147.88
DOI 10.37539/NB185.2020.15.59.012

Курникова Марина Викторовна,
кандидат экономических наук, ФГБОУ ВО «Самарский государственный экономический университет», г. Самара
Marina Viktorovna Kurnikova, Samara State University of Economics, Samara

ОСНОВНЫЕ ИТОГИ И НАУЧНЫЕ РЕЗУЛЬТАТЫ СТУДЕНЧЕСКОЙ НАУЧНОЙ ЭКСПЕДИЦИИ В МУНИЦИПАЛЬНЫЙ РАЙОН
MAIN RESULTS AND SCIENTIFIC OUTCOMES OF THE STUDENT SCIENTIFIC EXPEDITION TO THE MUNICIPAL AREA

Аннотация: в статье приводится программа, структура и результаты студенческой научной экспедиции в муниципальный район Безенчукский Самарской области, проведенной летом 2019 г. Целью экспедиции явилось исследование процессов формирования экосистемы цифровой экономики в сельском муниципальном районе и уровня использования имеющихся информационных и цифровых технологий его организациями и населением.

Abstract: the paper presents the program, structure and outcomes of the student scientific expedition to the Bezenchuksky municipal area in 2019. The expedition was aimed at the research into the development of digital economy ecosystem in the rural municipal area and the level of ICT and digital technologies used by its businesses and citizens.

Ключевые слова: студенческая научная экспедиция, муниципальный район, цифровые технологии, цифровые компетенции.

Keywords: student scientific expedition, municipal area, digital technologies, digital competencies.

В Стратегия национальной безопасности Российской Федерации до 2020 г. в качестве одного из приоритетов устойчивого развития обозначено повышение качества жизни российских граждан путём гарантирования личной безопасности, а также высоких стандартов жизнеобеспечения (п. 24), достигаемое через обеспечение доступности информационных технологий (п. 52) для всех категорий граждан. Однако, практическая реализация данной меры (например, при исполнении задач и мероприятий, предусмотренных национальным проектом «Цифровая экономика») ограничивается сокращением цифрового неравенства первого уровня, когда сокращается неравный доступ к технологиям, существующий вследствие разного уровня развития инфраструктуры телекоммуникаций и связи в городах и сельских территориях. И если инфраструктурная часть «цифрового неравенства» постепенно сходит на нет – даже в селах уровень проникновения интернета в домашних хозяйствах превышает 70% [1], – то вопрос использования современных цифровых технологий не теряет своей остроты, поскольку в России все еще велико цифровое неравенство второго уровня, связанное с различиями между людьми по уровню владения цифровыми компетенциями.

Данный факт следует считать обусловленным персональными факторами (возрастом, образованием, доходом) и экономико-географическими факторами (уровнем социально-экономического развития территории, урбанизацией). Недостаточность навыков грамотного использования цифровых технологий – цифровых компетенций населения – признается экспертами как препятствие получению ожидаемых эффектов от цифровизации и формирования цифровой экономики в стране [2].

Несмотря на ряд имеющихся методик, позволяющих измерить цифровые компетенции населения по странам (Индекс развития ИКТ (Международный союз электросвязи), Национальный индекс развития цифровой экономики (Госкорпорация РОСАТОМ); субъектам РФ (Индекс цифровой грамотности (РОЦИТ); городам (Цифровая жизнь российских мегаполисов (Сколково), Цифровизация в малых и средних городах России (ВШЭ и Яндекс Такси)), отметим отсутствие исследований, посвященных измерению и анализу цифровых компетенций жителей слабо урбанизованных сельских территорий. Восполнить этот пробел была призвана студенческая научная экспедиция

«Уровень развития и использования информационных и цифровых технологий в муниципальном районе Безенчукский Самарской области», организованная кафедрой региональной экономики и управления Самарского государственного экономического университета летом 2019 г.

Следует отметить, что в Самарском государственном экономическом университете с 2003 года накоплен достаточно большой опыт организации и проведения студенческих научных экспедиций, включающих как масштабные экспедиции комплексного характера, так и экспедиции специального назначения. Достаточно подробно этот опыт обобщен в работе [3], где представлен перечень формируемых компетенций, рассмотрена тематика, выполнена оценка результатов, дана краткая характеристика методического обеспечения студенческих научных экспедиций.

Цель экспедиции «Уровень развития и использования информационных и цифровых технологий в муниципальном районе Безенчукский Самарской области» заключалась в исследовании формирования экосистемы цифровой экономики в муниципальном районе и уровня использования имеющихся цифровых технологий организациями и населением.

Задачи исследования включали:

1) оценку и описание наличия, качества и доступности инфраструктуры доступа к цифровым технологиям;

2) описание характера использования цифровых технологий в организациях (на примере 4-5 организаций): доступность и направления использования интернета в организациях; использование цифровых технологий; оценка затрат организаций на ИКТ;

3) изучение наличие «цифровых компетенций» у населения муниципального района.

Методами исследования стали сбор и анализ имеющейся статистической информации, наблюдение и экспертный опрос (исследование организаций), социологическое исследование в формате анкетирования (исследование «цифровых компетенций» у населения).

Выбор территории для проведения экспедиции был обусловлен тем, что муниципальный район Безенчукский среди других муниципальных районов Самарской области входит в ТОП-10 районов по ряду ключевых показателей в рейтинге Министерства экономического развития, инвестиций и торговли Самарской области: на 2 месте по уровню официально зарегистрированной безработицы; на 3 месте по отгрузке товаров собственного производства (В,С, Д, Е); на 6 месте по объему производства молока на 100 га с/х угодий; на 7 месте по уровню среднемесячной заработной платы; на 8 месте по инвестициям в основной капитал; на 9 месте по индексу промышленного производства по крупным и средним предприятиям, на 7 месте по сводному рейтингу.

В муниципальном районе было обследовано 10 предприятий, завершивших процессы цифровой трансформации: на них были организованы ознакомительные экскурсии для студентов, проведены интервью с руководителями высшего звена.

Особую научную ценность представляют результаты данные социологического опроса «Цифровые компетенции» жителей Безенчукского района, в ходе которого были опрошены 521 житель муниципального района в возрасте от 12 до 89 лет, из них 271 женщина (52%) и 232 мужчины (44,5%). Полученные данные были обработаны при помощи пакета SPSS Statistics (программы для статистической обработки данных, проведения прикладных исследований в общественных науках), результаты презентованы научной общественности на проведенной в СГЭУ международной научной конференции «Проблемы развития предприятий: теория и практика» (см. [4]).

В заключение отметим, что практическая ценность полученных результатов экспедиции связана с возможностью их использования при подготовке программ и проектов, направленных на развитие цифровых компетенций у населения, а также в качестве лучших практик цифровой трансформации предприятий.

Список литературы:

1. Цифровизация в малых и средних городах России / Аналитический отчет. URL: https://roscongress.org/materials/tsifrovizatsiya-v-malykh-i-srednikh-gorodakh-rossii/ (дата обращения: 01.05.2020).

2. Королева Е.Н., Курникова М.В. Работа с населением в органах местного самоуправления: учеб.-метод. пособие по программе курсов повышения квалификации / Самар. гос. экон. ун-т. Самара, 2018. 68 с.

3. Королева Е.Н., Гранкина А.А. Опыт организации студенческих научных экспедиций в муниципальные районы самарской области // Приоритетные направления развития науки и образования сборник статей Международной научно-практической конференции. В 2 частях. 2018. С. 170-173.

4. Курникова М.В., Королева Е.Н. Оценка цифровых компетенций населения сельского муниципального района // Проблемы развития предприятий: теория и практика. 2019. № 1-1. С. 65-69.

Ближайшие конференции
ГНИИ "НАЦРАЗВИТИЕ" (РИНЦ)

Шифр	Наименование конференции	Дата
ВТ 186	Международная научная конференция **"Высокие технологии и инновации в науке"**	28 июля 2020 года
КО 186	Международная научно-методическая конференция **"Проблемы управления качеством образования"**	29 июля 2020 года
НБ 186	Всероссийская научно-практическая конференция **"Национальная безопасность России: актуальные аспекты"**	30 июля 2020 года
ПБ 186	Международная студенческая научная конференция **"Поколение будущего"**	31 июля 2020 года
SRP 292	International Scientific Conference "**Science**.**Research**.**Practice**" (Международная конференция "**Наука. Исследования. Практика**"	26 августа 2020 года
TNS 292	International Scientific Conference "**Technical and Natural Sciences**". (Международная научная конференция "**Технические и естественные науки",**	27 августа 2020 года
SEH 292	International Scientific Conference "**Socio-Economic Sciences & Humanities**". (Международная научная конференция "**Социально-экономические и гуманитарные науки**"	28 августа 2020 года
ECS 292	International Scientific Conference "**Education, Culture and Society**". (Международная научная конференция **"Образование. Культура. Общество"**	29 августа 2020 года
PSM 292	International Scientific Conference **"Psychology, Sports Science and Medicine**" (Международная научная конференция **"Психология. Спорт. Здравоохранение"**	30 августа 2020 года
SITB 292	International Scientific Conference "**Security: Information, Technology, Behavior**". (Международная научная конференция **"Безопасность: Информация, Техника, Управление**"	31 августа 2020 года

Приглашаем к участию в конференциях научных и практических работников, преподавателей образовательных учреждений, докторантов, аспирантов, соискателей и студентов

Подробнее о конференциях Вы можете узнать
на официальном сайте ГНИИ «Нацразвитие»:
WWW.NATSRAZVITIE.RU
Интересующие вопросы можно задать по телефону:
8 (812) 905-29-09
или написать нам по адресу:
NATSRAZVITIE@GMAIL.COM

ТРЕБОВАНИЯ
К МАТЕРИАЛАМ УЧАСТНИКОВ КОНФЕРЕНЦИЙ

ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ТЕКСТА

Формат текста	Microsoft Word (*.doc, *.docx)
Формат страницы	А4 (210х297 мм)
Ориентация страницы	книжная
Поля (верхнее, нижнее, левое, правое)	20 мм
Размер шрифта (кегль)	14
Тип шрифта	Times New Roman
Межстрочный интервал	полуторный
Абзацный отступ	1,25 см
Выравнивание	по ширине
Переносы	автоматические (не вручную)

СТРУКТУРА СТАТЬИ

Структура статьи	**Требования**
УДК	В верхнем левом углу проставляется индекс УДК. Справочник по УДК: http://teacode.com/online/udc/
Сведения об авторе (авторах)	Выравнивание текста по правому краю. Если авторов несколько, то сведения о следующем авторе располагаются через пустую строчку.
Название	Строчные, полужирные буквы, выравнивание – по центру, на русском и на английском языках
Пустая строка	Пропустить строку
Аннотация	Аннотация на русском языке (не более 6 строк). Начинается со слов: "**Аннотация:**". Далее аннотация на английском языке (не более 6 строк). Начинается со слов: "**Abstract:**"
Пустая строка	Пропустить строку
Ключевые слова	Ключевые слова на русском языке. Начинаются со слов: "**Ключевые слова:**". Не более 6 слов или словосочетаний. Далее Ключевые слова на английском языке. Начинаются со слов: "**Keywords:**". Не более 6 слов или словосочетаний.
Пустая строка	Пропустить строку
Текст статьи	Расположить текст статьи
Пустая строка	Пропустить строку
Список литературы	Расположить список литературы

СВЕДЕНИЯ ОБ АВТОРЕ (строчными буквами)

№	**Перечень сведений об авторе**	**На каком языке приводится**
1	Фамилия, имя, отчество автора полностью	на русском языке
2	Ученая степень (если есть), звание (если есть), для студентов –"студент", для аспирантов – "аспирант"	на русском языке
3	Место работы автора	на русском языке
	Место жительства автора (город)	на русском языке
	Фамилия, имя, отчество автора полностью	в английской транслитерации
	Место работы автора	на английском языке
	e-mail автора	

Подробную информацию о требованиях к материалам участников конференций с примерами вы можете посмотреть здесь – http://natsrazvitie.ru/trebovaniya_k_materialam_uchastnikov/