**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»**

**КАФЕДРА БЕЗОПАСНОСТИ НАСЕЛЕНИЯ И ТЕРРИТОРИЙ
ОТ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ**

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ И ВОПРОСЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ РЕАЛЬНОЙ ЭКОНОМИКИ

Сборник научных трудов по итогам III Всероссийской научно-практической конференции «Инновационные технологии и вопросы обеспечения безопасности реальной экономики»

Санкт-Петербург

31 марта 2021 года

***Под редакцией
доктора технических наук, профессора Г.В. Лепеша,
кандидата физико-математических наук, доцента О.Д. Угольниковой
кандидата экономических наук, доцента С.Ю. Александровой***

**ИЗДАТЕЛЬСТВО
САНКТ-ПЕТЕРБУРГСКОГО ГОСУДАРСТВЕННОГО
ЭКОНОМИЧЕСКОГО УНИВЕРСИТЕТА
2021**

ББК 65.050
И66

И66 **Инновационные** технологии и вопросы обеспечения безопасности реальной экономики : сборник научных трудов по итогам III Всероссийской научно-практической конференции «Инновационные технологии и вопросы обеспечения безопасности реальной экономики». Санкт-Петербург. 31 марта 2021 года / под ред. д-ра техн. наук, проф. Г.В. Лепеша, канд. физ.-мат. наук, доц. О.Д. Угольниковой, канд. экон. наук., доц. С.Ю. Александровой. – СПб. : Изд-во СПбГЭУ, 2021. – 228 с.

ISBN 978-5-7310-5495-9

В сборнике опубликованы научные труды участников III Всероссийской научно-практической конференции «Инновационные технологии и вопросы обеспечения безопасности реальной экономики» ITES-2021, которая состоялась в Санкт-Петербургском государственном экономическом университете 31 марта 2021 года.

Сборник включает статьи Пленарной сессии (Часть 1, Часть 2). В них изложены результаты исследований по актуальным вопросам безопасности и устойчивости техногенных комплексов, цифровой трансформации промышленности, финансовой, экологической безопасности, обеспечению безопасности в информационной сфере, фармацевтической отрасли, здравоохранении, безопасности логистических систем, приграничных территорий, актуальные правовые аспекты безопасности жизнедеятельности.

Все материалы публикуются в авторской редакции. Точка зрения редакции может не совпадать с мнениями авторов статей.

Материалы могут быть использованы в учебной, научной и практической деятельности.

In the collection of papers published in the proceedings of the III All-Russian Scientific and Practical Conference «Innovative Technologies in the Economy for its Security» ITES-2021, held in Saint-Petersburg state University of Economics on 31 March 2021.

The collection includes articles of the participants of the Plenary Session, Part 1 and the Plenary Session, Part 2. It contains the research results on topical issues of security and sustainability of man-made complexes, digital transformation of industry, financial, environmental security, security in the information sphere, pharmaceutical industry, health care, security of logistic systems, border areas, current legal aspects of life safety.

All materials are published in the author's edition. The editorial Board's point of view can differ from the opinions of the authors' articles.

The materials can be used in education, research and practice.

ББК 65.050

Рецензенты: д-р техн. наук, проф. **В.Н. Ложкин**
д-р техн. наук, проф. **С.И. Корягин**

ISBN 978-5-7310-5495-9

© СПбГЭУ, 2021

ПРЕДИСЛОВИЕ

В настоящее время вектор стратегии национальной безопасности Российской Федерации направлен на новый уровень экономического развития и повышения качества жизни граждан. В стране «принимаются комплексные меры, направленные на преодоление негативных демографических тенденций и решение системных проблем в области здравоохранения, на снижение уровня бедности и расслоения общества по уровню доходов, на улучшение состояния окружающей среды. Развитие научного потенциала, повышение качества и доступности образования ускорят структурную перестройку российской экономики». Решению поставленных в стратегии задач препятствуют трансформации структуры мирового порядка, связанные со стремлением стран Запада сохранить свою гегемонию, с ростом числа чрезвычайных ситуаций, связанных с природными, техногенными и социальными опасностями, нарастающими на фоне наступления эпидемиологических угроз, в том числе – коронавирусной инфекции.

Большое значение в Стратегии национальной безопасности отводится трансформации российской экономики на новой технологической основе, обеспечивающей конкурентоспособность России на международной арене, выход ее на передовые позиции в ключевых областях, обеспечивающих дальнейшее укрепление обороноспособности страны и достижение национальных целей развития.

31 марта 2021 года в Санкт-Петербургском государственном экономическом университете состоялась III Всероссийская научно-практическая конференция «Инновационные технологии и вопросы обеспечения безопасности реальной экономики» ITES-2021. В рамках конференции проведена пленарная сессия, две научно-практические секции: «Безопасность в профессиональной деятельности» и «Серебряное ожерелье России: безопасность и новые стандарты туристского, гостиничного и ресторанного бизнеса в постковидный период», а также научный семинар на тему «Расширение сетевого взаимодействия индустриально развитых регионов России и Республики Беларусь».

Миссия конференции – содействие развитию инновационных процессов в области обеспечения комплексной безопасности реальной экономики, развития сферы сервиса, туризма и гостеприимства, межвузовского, межрегионального и международного научно-технического и делового сотрудничества, обеспечивающих социальное благополучие населения, национальную безопасность и повышения международного авторитета Российской Федерации с целью привлекательности сотрудничества с ней для других государств.

Участников конференции поддержали:

Комитет по науке и высшей школе Правительства Санкт-Петербурга, Комитет Санкт-Петербурга по делам Арктики, Комитет по промышленной политике, инновациям и торговле Санкт-Петербурга, Комитет по развитию туризма, Комитет по вопросам законности, правопорядка и безопасности, Главное управление МЧС России по г. Санкт-Петербургу.

В Конференции приняли участие научно-педагогические работники и обучающиеся отечественных вузов, Союзного государства Республики Беларусь, ученые и специалисты в области исследования и обеспечения безопасности промышленных предприятий Санкт-Петербурга и регионов Российской Федерации, атомной промышленности, транспорта, инженерных систем жизнеобеспечения, информационной и экономической безопасности, системы РСЧС, институтов туризма, природопользования и охраны окружающей среды. Всего 150 участников.

От сектора реальной экономики были представлены, в частности, ГУП «Водоканал Санкт-Петербург», предприятия металлургической, фармацевтической и др. отраслей.

Для участия в конференции было заявлено: от СПбГЭУ – 50 чел., от других вузов Санкт-Петербурга – 31 чел.; от вузов других регионов – 38 чел., от представителей органов государственной власти – 15 чел., от научных организаций – 3 чел., от предприятий и организаций реальной экономики –6 чел.

География конференции была представлена представителям следующих городов и регионов: г. Санкт-Петербург, г. Москва, г. Екатеринбург, г. Владивосток, г. Пермь, г. Снежинск (Челябинская область), г. Чусовой (Пермский край), г. Нижний Новгород, г. Пенза, г. Новосибирск, г. Тверь, г. Таганрог, г. Минск (Республика Беларусь), г. Караганда (Казахстан), всего 14 городов.

В докладах участников конференции представлены результаты исследований в области решения задач безопасности техногенных комплексов, цифровой трансформации промышленности, финансовой, экологической безопасности, обеспечению безопасности в информационной сфере, фармацевтической отрасли, здравоохранении, безопасности логистических систем, приграничных территорий, правовых аспектов безопасности жизнедеятельности.

Всероссийская научно-практическая конференция «Инновационные технологии и вопросы обеспечения безопасности реальной экономики (ITES)» стала ежегодной инновационной площадкой для представления

результатов научных исследований, профессионального обсуждения и экспертных заключений по вопросам безопасного развития самых различных секторов экономики, разработки и внедрения инновационных решений для обеспечения комплексной безопасности человека, окружающей его среды, общества, государства.

Организационный комитет ITES-2021 благодарит всех участников за проявленный интерес к проблемам безопасности, вынесенным в программу конференции, и надеется на дальнейшее плодотворное научное сотрудничество.

С уважением, Григорий Васильевич Лепеш,
д-р технических наук, профессор,
заведующий кафедрой безопасности населения и территорий от ЧС,
заместитель Председателя Оргкомитета III Всероссийской
научно-практической конференции «Инновационные технологии
и вопросы обеспечения безопасности реальной экономики» ITES-2021.

ПЛЕНАРНАЯ СЕССИЯ

УДК 332.122

Лепеш Григорий Васильевич
д-р техн. наук, профессор
Санкт-Петербургский государственный
экономический университет

ПРИГРАНИЧНОЕ И ТРАНСГРАНИЧНОЕ СОТРУДНИЧЕСТВО В КОНТЕКСТЕ БЕЗОПАСНОСТИ УСТОЙЧИВОГО РАЗВИТИЯ ТЕРРИТОРИЙ

Аннотация. Рассмотрены основные направления экономической политики РФ, направленной на устойчивое развитие приграничных регионов, в рамках которых предусматривается развитие транспортной инфраструктуры, туризма, приграничной и международной торговли. Оценены вызовы и угрозы приграничного сотрудничества отдельных сопредельных территорий в контексте нарастающего международного политического экстремизма со стороны стран Запада.

Ключевые слова: государственная граница, приграничное и трансграничное сотрудничество, безопасность, пересечение границ, угрозы, территориальные претензии.

CROSS-BORDER AND CROSS-BORDER COOPERA TION IN THE CONTEXT OF SECURITY AND SUSTAINABLE DEVELOPMENT OF TERRITORIES

Lepesh G.V.
St. Petersburg State Economic University

Annotation. The main directions of the economic policy of the Russian Federation aimed at the sustainable development of border regions, within which the development of transport infrastructure, tourism, cross-border and international trade is envisaged, are considered. The challenges and threats of cross-border cooperation of certain adjacent territories in the context of growing international political extremism on the part of Western countries are assessed.

Keywords: state border, cross-border and cross-border cooperation, security, border crossing, threats, territorial claims.

Общая протяженность российской государственной границы после присоединения Крыма оказалась почти равной границе бывшего СССР

(62 262 км и 62710 тыс. км, соответственно). Приграничная территория Российской Федерации (РФ) представляет собой непосредственно зону государственной границы, а также включает в себя территории административных районов и городов, санаторно-курортных зон, особо охраняемых объектов, природных и других территорий, прилегающих к государственной границе. Громадный пограничный периметр, с прилегающими территориями, различающимися, этносом, динамикой демографических процессов, погодными условиями, наличием природных ресурсов и др., вносит существенные проблемы в их социально-экономического развитие. Проблема усугубляется тем, что многие годы относительно обширные приграничные территории РФ были закрыты даже для собственного населения.

Безопасность границ РФ обеспечивается на всех участках границы, несмотря на их особенности, сложившиеся в историческом аспекте. Значительная часть государственной границы РФ (с Польшей, Финляндией, Норвегией, Китаем, Монголией, Северной Кореей, Японией и США) является частью государственной границы бывшего СССР. Государственные границы со странами Балтии: Литвой, Латвией, Эстонией образовались после их выхода из СССР. После распада СССР образовались также государственные границы с членами СНГ и с частично признанными Абхазией и Южной Осетией. Здесь особый статус имеет граница с Республикой Беларусь, входящей в состав Союзного государства России и Беларуси.

Приграничное сотрудничество является важной составляющей современной концепции внешней политики РФ [1] и осуществляется в трех основных направлениях (европейское, постсоветское и азиатское). Элементами правовой основы развития приграничного сотрудничества являются положения Федерального закона «О координации международных и внешнеэкономических связей субъектов Российской Федерации» от 04.01.1999 №4-ФЗ [2], Концепции приграничного сотрудничества в РФ [3], положения Европейской рамочной конвенции о приграничном сотрудничестве территориальных сообществ и властей от 1980 года [4]. В концепции [3] под приграничным сотрудничеством в РФ понимается «установление и развитие конструктивного диалога субъектов приграничного сотрудничества с субъектами приграничного сотрудничества сопредельных государств… в рамках которого государства, регионы и муниципальные образования осуществляют взаимодействие в экономической, научно-технической, гуманитарной и иных сферах» [стр. 2, 3]. В соответствии с законодательством РФ субъектами приграничного сотрудничества в пределах своей компетенции могут являться федеральные органы исполнительной власти, органы исполнительной власти субъектов РФ и органы местного самоуправления, а также юридические и физические лица.

Их основные полномочия, установленные законодательством РФ приведены на рисунке 1.

Приграничное сотрудничество, как согласованные действия, направленные на укрепление и поощрение добрососедских отношений между приграничными территориями, на развитие культурных связей, торговли, экономики, охрану окружающей среды, ликвидацию ЧС и др. в целях развития сопредельных территорий, содержатся в целом ряде других нормативных документов, например, ([4], [5]). Современная экономическая политика РФ направлена на устойчивое развитие приграничных регионов, в рамках которого предусматривается развитие транспортной инфраструктуры, туризма, приграничной и международной торговли. В качестве механизмов развития предполагается совместная реализация инвестиционных проектов, создание трансграничных производственных кластеров и упрощение пересечения границы.

Отмеченные различия в особенностях государственной границы с различными сопредельными странами привели к реализации практически всех известных форм пересечения границы, сложившихся в международной практике – от традиционного визового режима до свободного пересечения границ, устанавливаемых индивидуально для каждой из сопредельных стран [6]. Следует отметить, что в настоящее время действуют ограничения, вызванные введением мероприятий по предупреждению проникновения на территорию РФ коронавирусной инфекции Covid-19, которые отменяют практику пересечения границ, установленную правилами [6].

Граждане РФ совершают поездки в приграничные зарубежные страны по большей части с целью личного шопинга, туризма или отдыха. Такие поездки имеют характер краткосрочных приграничных перемещений. Наиболее часто россиянами, особенно проживающими в Северо-Западном регионе РФ, посещаются приграничные районы Финляндии и страны Балтии, а также Польши. Гражданами восточных регионов РФ наиболее посещаемы Китай и Монголия. В доковидном 2019 году перечисленные страны посетили совокупно 22,9% россиян, выезжавших в этом году за рубеж (на 6,8% больше, чем в прошлом 2018 году) [7]. Наибольший прирост в совокупном объеме выезжавших из РФ составил Китай (+13,5%). Обратный поток со стороны названных стран, за исключением Китая, незначителен и связан в основном с туристическими целями. Однако за последние годы обратный туристический поток несколько подрос в связи с девальвацией российской национальной валюты. Значительное количество туристов и коммерсантов (многие под видом туристов, примерно половина) приехало в 2019 г. в Россию из Китая.

Рисунок 1 – Основные полномочия федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ и органов местного самоуправления в области приграничного сотрудничества, установленные российским законодательством

Основу российско-китайского массового выездного туризма составляют поездки по безвизовому групповому обмену. В 2020 г. в связи с введенными ограничениями число пересечений границы составило лишь около 25% от уровня 2019 года (2,4 млн., по сравнению с 9,5 млн. годом ранее). При этом общее количество поездок российских граждан за рубеж по сравнению с 2019 годом упало на 70,6% [8].

Наиболее открытой для свободного пересечения является российско-белорусская граница. В других случаях пересечение российской границы производится только через установленные пункты пропуска и с соблюдением установленных законом процедур. Свободное пересечение при наличии национальных паспортов также предусмотрено через пункты пропуска на границе РФ с Казахстаном, Киргизией, Южной Осетией.

С некоторыми сопредельными странами и регионами РФ установила безвизовый режим, позволяющий временное пребывание в течение ограниченного срока. В этом случае пересечение границы производится при наличии документа, удостоверяющего личность (для граждан РФ – заграничного паспорта). Так безвизовый режим на основании межгосударственных соглашений установлен с Республикой Армения, Украиной, с Китайской Народной Республикой (КНР) в отношении приграничного района – города Суйфэньхэ (провинция Хэйлунцзян). Безвизовое пребывание иностранных граждан в течение восьми дней разрешено на территории свободного порта Владивосток.

Несмотря на безвизовый режим пересечения российско-украинской границы, попасть со стороны России на территорию Украины, можно только через межгосударственные/международные пограничные пункты. Обратно можно выезжать через местные пункты пропуска. Для российских граждан, наряду с другими иностранными гражданами, законно пребывающими на территории Украины действуют ограничения перемещения по территории зон отчуждения, закрытых после Чернобыльской катастрофы, а также по отношению к непризнанным Донецкой Народной Республикой и Луганской Народной Республикой, образованных на территории Донецкой и Луганской областей Украины после государственного переворота, состоявшегося в Украине в 2014 году. Подобные формальные ограничения установлены для Республики Крым, вошедшей в состав России. Кроме того, приграничная территория со стороны Украины закрыта для доступа приграничной полосой, составляющей несколько десятков километров, попасть в которую можно лишь при пересечении границы по разрешительным документам. Приграничная полоса распространяется также на приграничную территорию с Крымом, на Донецкую и Луганскую народные республики.

Для граждан РФ, проживающих в Республике Крым, посещение Украины запрещено. Посещение Крыма с украинской стороны возможно, однако действуют таможенные ограничения по провозу денежных сумм и кругу перемещаемых товаров. Кроме того, украинской стороной введен запрет на транспортное сообщение с Крымом, за исключением личных транспортных средств.

Визовый режим вводится странами в целях национальной безопасности, в том числе для ограничения миграционных потоков, пресечения контрабанды, незаконного оборота наркотических средств, оружия, международной преступности и пр. Как правило, визовый режим устанавливают в зависимости от степени взаимного доверия и уровня двухсторонних отношений. Процедура получения визы в некоторые страны достаточно продолжительная, иногда требуется приглашение от принимающей стороны, что затрудняет трансграничное взаимодействие.

По официальной статистике [9] в доковидном 2019 году россиянам было оформлено 4 054 685 шенгенских виз. При этом более трех миллионов граждан РФ получило мультивизы. Это принесло визовой индустрии около €200 млн. Основными целями российских туров в зону шенгена традиционно являются: бизнес, образование и культурно-познавательные цели. По отношению к приграничным регионам соседних стран до момента наступления санкционных ограничений на поставку продовольственных продуктов целями значительной части туристов являлось совершение покупок.

Практика показывает, что упрощение визового режима положительно сказывается на приграничной торговле и приграничном сотрудничестве. Так, например, облегченный порядок въезда, подобный установленному в странах ЕС по отношению к соседним странам, установлен для въезда в Китай российских граждан, проживающих в граничащих с КНР Амурской и Иркутской областях, а также в Забайкальском, Приморском и Хабаровском краях.

Основными объектами трансграничного сотрудничества стран являются: зоны приграничной торговли, туристические зоны, а также трансграничные промышленные зоны. В целях осуществления межрегионального сотрудничества с Северо-Восточным Китаем в 2015 г. российское правительство приняло Концепцию развития приграничных территорий субъектов РФ, входящих в состав Дальневосточного федерального округа. В документе указано, что приоритетом России является создание транспортной инфраструктуры в Северо-Восточной Азии, обеспечивающей расширение трансграничного транспортного сообщения и развитие инвестиционного климата в регионе. В целях координации межрегионального сотрудничества в 2017 г. Россия и Китай создали межправительственную

комиссию. По инициативе в основном китайской стороны в целях развития своих приграничных регионов, создания условий для экспорта продукции китайского производства, продвижения своей экономической политики на приграничные российские территории, сформированы совместные производственные площадки – так называемые зоны приграничного экономического сотрудничества (ЗПЭС). Нормативную основу российско-китайского приграничного взаимодействия сегодня составляет Программа развития российско-китайского сотрудничества в торгово-экономической и инвестиционных сферах на Дальнем Востоке РФ на 2018–2024 годы [10], являющаяся продолжением Программы сотрудничества между регионами Дальнего Востока и Восточной Сибири Российской Федерации и Северо-Востока Китайской Народной Республики (2009–2018 гг.). Программой предусмотрены крупные инвестиции Китая в дальневосточную экономику, а Российская сторона обеспечивает благоприятную инвестиционную политику и реализует меры для снятия барьеров, препятствующих инвестициям из КНР на Дальнем Востоке России. Инвестиции сегодня затрагивают практически все традиционные отрасли экономики: газо- и нефтехимическую промышленность, освоение месторождений твердых ископаемых, транспорт и логистику, сельское хозяйство, лесную промышленность, аквакультуру и туризм. В рамках трансграничного сотрудничества предлагается развитие инфраструктуры международных транспортных коридоров «Приморье-1» и «Приморье-2», строительство трансграничных мостовых переходов и др.

Основным механизмом координации развития российско-китайского торгово-экономического и инвестиционного сотрудничества на Дальнем Востоке РФ является Межправительственная Российско-Китайская комиссия по сотрудничеству и развитию Дальнего Востока и Байкальского региона РФ и Северо-Востока КНР. Однако происходящие на Дальнем Востоке масштабные преобразования в приграничных районах КНР увеличивают разрыв в экономическом развитии двух регионов. В трансграничном сотрудничестве все большую инициативу и координацию в данном процессе берет на себя Китай. В случае значительного отставания российских субъектов Дальнего Востока возникают потенциальные угрозы, связанные с замыканием российской экономики на китайский рынок, с захватом Китаем сырьевых и земельных ресурсов, недвижимости и установлением полного контроля над дальневосточным бизнесом, что грозит превращением Дальнего Востока в сырьевую и ресурсную базу и транспортно-логистический центр для китайских приграничных регионов и китайской экономики в целом.

Парирование угроз с российской стороны связано с ускорением социально-экономического развития восточных районов, с переходом от

модели развития транспортно-логистической инфраструктуры дальневосточных регионов и использования их как сырьевой периферии для международных экономик, к модели развития постиндустриальной экономики, сопровождающейся переходом к сверхиндустриальным укладам, цифровизацией и сетевизацией производств, с привлечением к этому переходу не только китайских, но и российских инвесторов. Важнейшим условием развития восточных регионов при этом является государственная политика, направленная на выравнивание демографического дисбаланса в приграничных регионах, а также на подготовку и закрепление высококвалифицированных кадров на Дальнем Востоке.

Другим ближайшим соседом восточных регионов России является Монголия, экономика которой в значительной степени отличается от Китая и традиционно основана на животноводстве (крупный рогатый скот, овцы и козы), в то время как на российской стороне в приграничных районах более развито растениеводство. Выравнивание дисбаланса диктует необходимость трансграничного взаимодействия между странами в производстве сельскохозяйственной продукции. В настоящее время существует ряд сдерживающих факторов, оказывающих влияние на развитие такого взаимодействия. Одним из них является то, что с российской стороны трансграничное взаимодействие с Монголией осуществляют жители приграничных районов Республики Бурятия, отличающиеся низким уровнем жизни по сравнению с жителями других регионов РФ. При этом, уже сейчас при небольшой плотности населения с обеих сторон, с российской стороны продолжается отток населения в более благополучные регионы РФ. Сдерживающими факторами являются также неразвитость транспортной и пограничной инфраструктуры, сложности таможенного оформления товаров вследствие недостатков гармонизации нормативной и законодательной базы обеих стран. Российско-монгольское трансграничное сотрудничество имеет большой взаимовыгодный потенциал, который заключен в реализации выгодного экономико-географического положения. Наличие обширных свободных территорий, пригодных для производства сельскохозяйственной продукции строительства жилья и объектов производственной, социальной и транспортно-логистической инфраструктуры могут стать объектами обоюдовыгодных трансграничных инвестиционных проектов. Развитию российско-монгольских отношений способствовала отмена виз в 2014 г. Эффект проявился в незамедлительном росте количества монгольских туристов, что привело к развитию торговли и сферы гостеприимства в Республике Бурятия, а также стимулировало развитие всей приграничной инфраструктуры.

В дальневосточных регионах РФ осуществляется также приграничное сотрудничество с Японией, особенностью которого является интерес

японской стороны к островам Южной Курильской гряды: Итуруп, Кунашир, Шикотан и Хабомаи. Посещение островов, японцами происходит по упрощенному безвизовому режиму. Между РФ и Японией подписана программа о совместной хозяйственной деятельности, в рамках которой японской стороной поддерживается строительство объектов инфраструктуры на этих островах.

РФ имеет морскую границу с расположенным на Аляске регионом Соединенных Штатов Америки (США). Трансграничное сотрудничество на данном участке границы отсутствует из-за того, что со стороны РФ здесь практически нет гражданского населения. Однако между РФ и США в данном регионе остаются общие интересы, в том числе необходимость сотрудничать в Арктике, договариваться о квотах на лов рыбы и правилах судоходства в Беринговом проливе, переданном Россией США во временное пользование. Кроме того, у США есть необоснованные претензии по использованию Северного морского пути, проходящего в территориальных водах России.

Самую большую протяженность (более 7500 км) составляет участок границы России с Казахстаном. Граница образовалась в 2005 году. Граница охраняется и контролируется. Допуск на сопредельные территории осуществляется через 50 пропускных пунктов по упрощенной схеме при наличии подтверждающих личность документов. В настоящее время действуют ограничения пересечения границы, связанные с нераспространением новой коронавирусной инфекции. Приграничное сотрудничество между Россией и Казахстаном осуществляется в соответствии с нормативно-правовыми соглашениями, установленными в рамках Евразийского экономического союза. В силу того, что экономики России и Казахстана исторически взаимосвязаны, сотрудничество осуществляется в различных отраслях промышленности, науке, культуре, здравоохранении. Эффективность сотрудничества обсуждается на ежегодных Форумах приграничных регионов с участием глав государств Республики Казахстан и РФ. Вызовы российско-казахскому приграничному сотрудничеству связаны с возможностью дополнительных ограничений в отношении пересечения границы, которые могут быть вызваны общей политической ситуацией в Республике Казахстан, проводящей многовекторную политику с ориентацией на страны Запада и Китай.

Россия и Беларусь интегрируются в конфедеративное Союзное Государство и имеют практически формальные границы, пересечение которых для граждан обеих стран не ограничено специальными требованиями. В настоящее время оно ограничено в связи с новой коронавирусной инфекцией. Имеющиеся на сегодня различия в экономической политике обоих государств легко нивелируются при совместной экономической де-

ятельности в приграничных регионах. Особенности российско-белорусского сотрудничества приводятся в обширных исследованиях, включая [11]. Угрозы сотрудничеству, вызванные внешним давлением на российско-белорусские отношения агрессивно настроенными странами ЕС, успешно нивелируются путем последовательного движения в сторону налоговой и гражданский интеграции общества, общего внешнеторгового режима, единого регулятора рынков нефти, газа и электроэнергии, объединенному банковскому надзору.

Приграничное сотрудничество Калининградской области РФ имеет свои особенности, обусловленные полуэксклавным положением среди стран ЕС – Польши и Литвы. В условиях действующих ограничений нераспространения вирусной инфекции пересечение границы со странами ЕС для жителей Калининградской области запрещено. С июля 2012 по июль 2016 года было возможно упрощенное (безвизовое) пересечение польской границы для жителей полуэксклава в рамках соглашения о порядке местного приграничного передвижения (МПП) между Калининградской областью РФ и Варминьско-Мазурском и Поморским воеводствами Польши [12]. В 2016 году режим МПП отменен Польшей в одностороннем порядке. Для всех граждан РФ включая жителей Калининградской области для пересечения границы ЕС необходимо предоставить шенгенскую визу. Для поездки в другие регионы России через Литву или Беларусь, граждане Калининградской области могут оформить один из двух предусмотренных упрощенных документов. Упрощенный транзитный документ выдается по загранпаспорту на 3 года и позволяет находиться на территории Литвы в течение 24 часов. Упрощенный транзитный железнодорожный документ оформляется при покупке железнодорожного билета и позволяет передвигаться по Литве в течение 6 часов и в течение 3 месяцев возвратиться обратно [12].

Международная правовая база приграничного сотрудничества в РФ основана на ратификации Европейской рамочной конвенции и еще двух дополнительных протоколов по созданию и деятельности еврорегионов, формировавшихся параллельно развитию ЕС. Основная цель, преследуемая ЕС, – это ликвидации внутриевропейских национальных границ, а также сохранение стабильности по периметру границ ЕС путем стимулирования преобразований в России на основе европейских моделей и стандартов.

В Калининградской области в середине 90-х было создано пять еврорегионов. Организация приграничного сотрудничества тогда рассматривалась как возможность компенсации негативных последствий эксклавного расположения Калининградской области. Однако результаты деятельности приграничного сотрудничества в рамках еврорегионов ограни-

чились поставками с сопредельных территорий потребительских товаров, а также переработкой на территории калининградской особой экономической зоны сырья и полуфабрикатов, которые отправляются далее на российский рынок.

На сегодняшний день по отношению приграничного сотрудничества в Калининградской области продвигаются две противоположные тенденции. Одна из низ связана с дальнейшей интеграцией в европейское сообщество имеющая деструктивный для российской государственности смысл, в том числе, и переименование Калининграда в Кёнигсберг. Наличие такой тенденции стало последствием открытости Калининградской области к сотрудничеству в рамках проектов еврорегионов с Польшей и Литвой, ставящих перед собой цель по формированию европейской идентичности в эксклаве, в том числе через представленную здесь католическую общину. Вторая учитывает реальное движение ЕС в сторону милитаризации, а, следовательно, невозможность углубления процессов интеграции, поскольку, по словам заместителя министра иностранных дел РФ Александр Грушко, «точка невозврата» в отношениях России и Запада пройдена и «окна возможностей» закрыты [13]. Следует отметить, что после усиления российского военного контингента в 2016 году на территории калининградского эксклава, Польша и Литва потеряли интерес к сотрудничеству в еврорегионах с РФ. Российская сторона, по словам Председателя СФ РФ В. Матвиенко, по-прежнему рассматривает еврорегион как «наиболее продвинутую форму международной интеграции», а сотрудничество в рамках еврорегионов как «один из ведущих и неизменных приоритетов России» [13], преследуя при этом цели повышения благосостояния населения приграничных районов, сохранения культурной идентичности, развития транспортной инфраструктуры, межуниверситетских научных контактов, сохранения экологии, проведения мероприятий по снятию языковых и культурных барьеров и др., способствующих стабильному социально-экономическому развитию региона.

Проблемы и перспективы приграничного сотрудничества еврорегионов с участием России подробно исследованы в работе Рустамовой Л.Р. [14], которая обоснованно отмечает, что поскольку Россия не входит в ЕС, то основной проблемой является то, что «в рамках еврорегионов европейского типа сложно говорить о какой-то территориальной идентичности, поскольку Россия не входит в Европейский Союз и ее не объединяют с европейскими странами общеевропейские ценности и стремление к регионализации... Еврорегионы постсоветского пространства имеют все основания к углублению сотрудничества на основе построения идентичности. Проблема заключается в том, что они становятся полем боя европейского и российского проектов» [14, стр.728]. Отрицательным примером является

потеря украинской идентичности через чрезмерное вовлечение украинских властей в еврорегионы с участием стран ЕС: «Буг», «Карпаты», «Нижний Дунай», «Верхний Прут» у западных границ, что явилось одной из причин развала государственности на Украине, отказа от развития отношений с Россией в пользу ассоциации с ЕС.

В процессе освоения северных частей России исторически складываются культурные и экономические взаимоотношения со странами Скандинавии. Специфика взаимоотношений основана на необходимости взаимной помощи при завозе необходимого продовольствия и оборудования для строительства инфраструктуры при добыче полезных ископаемых. Приграничное сотрудничество со скандинавскими странами базируется на соглашениях, заключенных между Данией, Финляндией, Норвегией и Швецией на уровне местных сообществ, а также о содействии приграничному сотрудничеству между РФ и Финляндией [15]. Сотрудничество между РФ и странами Скандинавии происходит в различных областях: рыбном хозяйстве, лесоперерабатывающей и целлюлозно-бумажной промышленности, строительстве, туризме и природоохранной деятельности. Однако в настоящее время большинство соглашений на правительственном уровне заморожено из-за введенных западных санкций. Несмотря на санкции взаимодействие на региональном уровне по программам приграничного сотрудничества (ППС) продолжается. Так на российско-норвежской границе было организовано МПП по правилам, установленным ЕС для стран не членов ЕС (безвизовое пребывание до 15 дней в тридцатикилометровой приграничной зоне), которым пользовались десятки тысяч жителей в год, как норвежцев, так и россиян [16].

Наиболее значимую эффективность в российско-скандинавских проектах приграничного сотрудничества имеет ППС «Колартик», направленная на развитие доступности северных территорий, развитие бизнеса и охрану окружающей среды, финансирование которой осуществляется всеми странами участниками (Россией, Финляндией, Швецией и Норвегией) на паритетных условиях. Доля вложения России в проект в совокупности составила более €12 млн. [16]. Наиболее активна в отношении приграничного сотрудничества Республика Карелия, которая имеет наиболее протяжённую границу с Финляндией, являющейся членом ЕС. Сотрудничество осуществляется в рамках ППС «Карелия». Особенностью этого сотрудничества является совместная реализация трансграничных мероприятий, взаимовыгодных экономических проектов, а также культурное взаимодействие, причем в условиях, когда по обе стороны границы имеются проблемы, связанные со старением и сокращением населения, высоким уровнем безработицы, особенно среди молодежи. На первом этапе (2007–2013 гг.) большую часть финансирования ППС осуществлялась со сторо-

ны ЕС. Однако начиная с 2012 г. в связи с изменениями международной ситуации было принято новое российско-финляндское межправительственное соглашение о приграничном сотрудничестве, основанное уже на симметричном взаимодействии в реализации трансграничных региональных мероприятий [13].

Несмотря на то, что между РФ и ЕС установлено визовое пересечение границы, обычно российско-финскую границу в год пересекают около 9 млн. человек (в 2019 г. около 8 млн. человек; снижение обусловлено падением покупательной способности российского рубля), в то время как за 2020 г. – только около 2 млн. человек (резкое снижение следствие ограничений из-за пандемии). Ограничения на въезд в страну для большинства стран, не входящих в ЕС, в том числе для России, непрерывно продлеваются. Ограничения привели к падению товарооборота между РФ и Финляндией за 2020 год почти на 30%.

Как российская, так и финская стороны, надеясь на восстановление показателей взаимовыгодного сотрудничества после снятия ограничений, развивают приграничную инфраструктуру: ведут реконструкцию пограничного пункта пропуска Светогорск–Иматра, создают трансграничные велосипедные маршруты, обсуждают возобновление к 2025 году движения электричек Петербург–Светогорск–Иматра, с пассажиропотоком около 1 млн. человек. Финская сторона крайне заинтересована в возобновлении объема российского турпотока с целью шопинга и отдыха на природе, который приносил Финляндии в предшествовавшие годы доходы около €1 млрд. В настоящее время Финляндия, хотя и является членом ЕС, но не является членом Северо-Атлантического блока НАТО, а в отношении России ведет взвешенную политику, направленную на добрососедские отношения, что позволяет и в дальнейшем успешно реализовывать совместные проекты в рамках ППС.

К изложенным правовым и социально-экономическим экономическим проблемам приграничного сотрудничества в последнее время добавляются угрозы, создаваемые и поддерживаемые США и недружелюбно настроенными странами ЕС, направленные на ослабление международного влияния РФ. Из них следует выделить следующие основные, дестабилизирующие социально-экономическую обстановку в приграничных районах:

1. Наращивание группировок войск вблизи границ РФ, проведение учений и демонстрация военной силы с провокационными целями, ведущие к нарушению сложившегося баланса сил;

2. Наличие вблизи границ РФ вооруженных конфликтов и угроз их возникновения;

3. Территориальные претензии к РФ и угрозы политического или силового отторжения от РФ отдельных территорий.

Нарастающими угрозами дестабилизации приграничных территорий и трансграничных взаимоотношений являются также:

1. Нестабильность, слабость государственных институтов в приграничных странах, особенно с антироссийскими фобиями бывших прибалтийских республиках СССР и на Украине, являющихся сателлитами США, а также слабость местных органов самоуправления на приграничных территориях.

2. Деятельность международных исламских радикальных группировок в приграничных районах.

3. Трансграничная преступность, включающая транспортировку наркотиков на территорию РФ и другие виды контрабандной деятельности в масштабах, угрожающих военно-политической безопасности РФ, а также стабильности на территории союзников РФ.

Из официальных правительственных документов следует, что РФ завершила демаркацию своих границ, однако на сегодняшний день имеется «незавершенность международно-правового оформления отдельных участков государственной границы, также имеются попытки ряда иностранных государств оспорить правомерность ранее заключенных межгосударственных соглашений о ее прохождении». Территориальные претензии к России имеют следующие страны:

1. Эстония, согласно конституции которой сухопутная государственная граница проходит по территории нынешних Ленинградской и Псковской областей РФ, что обосновывается ссылкой на Тартуский мирный договор, заключенный с РСФСР в 1920 году, утративший силу в 1940 году в связи с вхождением Эстонии в состав СССР. Подписанный в феврале 2014 года новый договор о границе до сих пор не ратифицирован обеими сторонами.

2. Южная Корея, не имеющая общих границ с РФ, претендует на остров Ноктундо, находящийся в Приморском крае в устье реки Туманной на границе КНДР и РФ. Территория острова перешла к Российской империи по Пекинскому договору. В 1990 году КНДР признала юрисдикцию СССР над островом Ноктундо, однако Южная Корея – не признала.

3. Китайская Республика в лице государства на острове Тайвань претендует на остров Кутузов на реке Уссури. Остров находился под контролем СССР со времен правления образованного Японией марионеточного государства Маньчжоу-Го. Юрисдикция СССР за островом закреплена в 1991 году на основании советско-китайского договора о границе. Тайвань также претендует на территорию Республики Тыва, которая после Монгольской национальной революции в 1911 году вышла из Китая в составе Внешней Монголии, а в 1914 году эта территория перешла под протекторат Российской империи по просьбе местной знати. В 1921 году там была

провозглашена народная республика, которая в 1944 году вошла в состав РСФСР. Тайвань высказывает претензии и к переданным Российской империи в 1858 г. территории бывших 64-х деревень, расположенных к востоку от реки Амур. Китай еще раз отказался от них в 1991 году после того, как наши войска выдворили жителей деревень на другой берег Амура. Претензии Тайваня распространяются также и на восточную половину Большого Уссурийского острова, который в 1929 году был занят войсками Красной Армии во время освобождения от захватчиков Китайско-Восточной железной дороги. После попыток Китая возвращения острова под свой контроль Россия передала его западную часть вместе с островом Тарабаровым по договору 2004 года. Восточная осталась у России. В 2016 году было опубликовано совместное российско-китайское заявление об окончании демаркации границы, которое исключает взаимные территориальные претензии.

4. Абхазия, признанная лишь пятью странами – членами ООН, являющаяся экономическим партнером и военным союзником РФ, претендует на часть села Аибга и его окрестности, принадлежащие РФ. Ранее территория всего села с обширными окрестностями входила в состав РСФСР. С началом грузино-абхазского конфликта только половина села, отделенная от Абхазии рекой Псоу, принадлежит РФ в составе г. Сочи. С момента Сочинской Олимпиады российские пограничники усиленно контролируют границы с Абхазией и пресекают свободное перемещение через нее.

5. Украина, согласно административно-территориальному делению, по-прежнему считает весь полуостров Крым в своем составе. Однако большая часть территории полуострова Крым (исключением является северная часть Арабатской стрелки) на основании результатов общекрымского референдума, проведенного 16 марта 2014 года, воссоединена с Россией на правах субъектов федерации (Республики Крым и города федерального значения Севастополя).

6. Норвегия, являясь членом НАТО, все же признает права РФ на архипелаг Шпицберген, однако протестует против увеличения присутствия российских граждан в регионе, в то время как в соответствии с новой стратегией РФ предполагается развитие российского присутствия на Шпицбергене, в том числе предполагает строительство нескольких объектов в городе Баренцбург.

7. Япония претендует на управляемые Россией острова Южно-Курильской гряды (острова Итуруп, Кунашир, Шикотан, группу островов Хабомаи), общей площадью 5175 км^2.

Помимо перечисленных официальных претензий все чаще на неофициальном уровне (как правило, с участием официальных лиц), со сто-

роны Литвы выдвигаются претензии на российские территории Калининградской области. Географическое положение Польши, исторически имеющей претензии к российской стороне, лежащей на пути между Россией и Западной Европой, составляет угрозу торговым отношениям с западными странами и доступу российским ресурсов в Калининградскую область. Начиная с прошлого 2020 года почти на официальном уровне (депутат Госдумы РФ, председатель Республиканского Союза и др.) выдвигают взаимные претензии о государственной границе между Россией и Казахстаном. Особенно в связи с наметившимся процессом деинтеграции из-за многовекторной политики Казахстана, направленной в сторону Запада, противоречащей отчасти экономической интеграции постсоветского пространства в рамках ЕАЭС. Обсуждается также вопрос о законности оставления северной части Арабатской стрелки в составе Украины.

Подытоживая изложенный материал, по отношению к приграничному сотрудничеству, можно констатировать следующее:

1. Границы привносят как позитивные, так и негативные факторы в социально-экономические процессы, происходящие в приграничных регионах, что обусловливает необходимость проведения дифференцированной политики России, как в отношении границ, так и в отношении развития приграничных территорий и регулирования приграничного сотрудничества. Развитие приграничных территорий наиболее эффективно производить сочетанием специальных мер поддержки и федеральных программ развития территорий с международными соглашениями.

2. Многие российские приграничные территории до сих пор отстают в области экономики, развития транспортной и пограничной инфраструктуры. Отставание обусловлено, как ограниченностью доступа к ним в советское время, так и географическими причинами – расположением их по периферии страны.

3. На границе ЕС с РФ с находятся проблемные периферийные ареалы, к которым относятся страны Балтии, создающие двойную или даже тройную окраину ЕС, препятствующие трансграничному взаимодействию.

4. На приграничной территории РФ существуют предпосылки к дестабилизации обстановки, вызванные неразрешенностью социально-экономических проблем, религиозно-этническими противоречиями и сепаратистскими проявлениями среди населения, а также рисками экономической и демографической экспансии из-за низкой заселенности и высокой дифференциации уровня социально-экономического развития при транспортной изоляции этих территорий.

5. Деструктивная политика США по отношению к РФ реализуется через дестабилизацию приграничных к РФ территорий Украины и Бело-

руссии, а также путем милитаризации русофобских стран Балтии и усиление роли Польши в Восточной Европе как стратегического союзника и проводника американских политических и экономических интересов в противовес российским.

6. Развитие сотрудничества сопредельных приграничных территорий во всех аспектах (культуры, науки, экономики) в большой степени зависит от преодоления современных внешних угроз, а также ограничено падением курса российской национальной валюты, страхом заболеть коронавирусом за рубежом и действующими при этом ограничениями пересечения границ.

Литература

1. Концепция внешней политики Российской Федерации: утверждена указом Президента РФ от 30.11.2016 г. №640. [Электронный ресурс] – URL: https://www.garant.ru/products/ipo/prime/doc/71452062/ (дата обращения: 10.03.2021).

2. О координации международных и внешнеэкономических связей субъектов Российской Федерации: федеральный закон от 04.01.1999 №4-ФЗ. [Электронный ресурс]. – URL: https://base.garant.ru/179963/ (дата обращения: 10.03.2021).

3. Концепция приграничного сотрудничества в Российской Федерации: утверждена распоряжением Правительства РФ от 7 октября 2020 г. №2577-р. [Электронный ресурс]. – URL: https://www.garant.ru/products/ipo/prime/doc/74639793/ (дата обращения: 10.03.2021).

4. Конвенция о приграничном сотрудничестве государств-участников Содружества Независимых Государств: заключена в г. Бишкеке 10.10.2008 г. // Бюллетень международных договоров. 2010. №1.

5. Европейская рамочная конвенция о приграничном сотрудничестве территориальных сообществ и властей: заключена в г. Мадриде 21.05.1980 г. (Вместе с «Типовыми и рамочными соглашениями, уставами и контрактами о приграничном сотрудничестве между территориальными сообществами и властями») // СЗ РФ. 2003. №31. Ст. 3103.

6. О порядке выезда из Российской Федерации и въезда в Российскую Федерацию: федеральный закон от 15.08.1996 №114-ФЗ. [Электронный ресурс]. – URL: https://base.garant.ru/10135803/ (дата обращения: 10.03.2021).

7. Статистика выезда россиян за рубеж в 2019 году. Официальные данные. [Электронный ресурс]. – URL: https://www.atorus.ru/news/press-centre/new/50475.html (дата обращения: 10.01.2021).

8. Официальная статистика выезда российских граждан за границу в 2020 году. [Электронный ресурс]. – URL: https://www.atorus.ru/news/press-centre/new/54297.html (дата обращения: 10.01.2021).

9. Ассоциация туроператоров. Официальный сайт. [Электронный ресурс]. – URL: https://www.atorus.ru/news/press-centre/new/51416.html (дата обращения: 10.01.2021).

10. Программа развития российско-китайского сотрудничества в торгово-экономической и инвестиционных сферах на Дальнем Востоке РФ на 2018–2024 годы. [Электронный ресурс]. – URL: https://minvr.gov.ru/upload/iblock/369/programma-itogovyy-variant.doc/ (дата обращения: 10.01.2021).

11. Лепеш Г.В. Формирование промышленной политики территорий России и Беларуси, ориентированной на расширение сетевого взаимодействия. // Технико-технологические проблемы сервиса. №3(53), 2020 г. - С. 3–11.

12. Соглашение между правительством Российской Федерации и правительством республики Польша о порядке местного приграничного передвижения (Москва, 14 декабря 2011 года). [Электронный ресурс]. – URL: https://kaliningrad.mid.ru/localbordertraffic/agreement (дата обращения: 10.01.2021).

13. Замглавы МИД РФ: интеграция РФ и ЕС не состоялась из-за неготовности Европы. ИА Красная Весна. [Электронный ресурс]. – URL: ttps://rossaprimavera.ru/news/e245a75f/(дата обращения: 10.01.2021).

14. Рустамова Л.Р. Проблемы и перспективы приграничного сотрудничества еврорегионов с участием России // Регионология. 2019. №4 (109). [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/problemy-i-perspektivy-prigranichnogo-sotrudnichestva-evroregionov-s-uchastiem-rossii (дата обращения: 05.05.2021).

15. Соглашение между Правительством Российской Федерации и Правительством Финляндской Республики о содействии приграничному сотрудничеству между Российской Федерацией и Финляндской Республикой. [Электронный ресурс]. – URL: www.pravo.gov.ru, 11.06.2013 (дата обращения: 10.01.2021).

16. Лепеш Г.В. Современные угрозы безопасности границ и устойчивому развитию приграничных территорий // Технико-технологические проблемы сервиса. №4(46) 2018. - С. 45-63.

17. Основы государственной пограничной политики Российской Федерации. Проект указа Президента РФ. [Электронный ресурс]. – URL: http://www.fsb.ru/fsb/npd/pva/more.htm%21id%3D10438241%40fsbNpa.html, 17.01.2018 (дата обращения: 10.01.2021).

УДК 004.056.5

Васильева Ирина Николаевна
доцент, канд. физ.- матем. наук
Санкт-Петербургский государственный
экономический университет,
Санкт-Петербургский университет
Министерства внутренних дел России

СОВРЕМЕННЫЙ ПОДХОД К МОНИТОРИНГУ БЕЗОПАСНОСТИ СЕТЕВЫХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР

Аннотация. В статье рассматриваются современные концепции обеспечения безопасности корпоративных компьютерных сетей, исследуются особенности такого класса решений защиты информации, как системы анализа сетевого трафика (NTA) и оценивается их роль в системе защиты корпоративной информационной инфраструктуры.

Ключевые слова: информационная безопасность, средства защиты информации, безопасность компьютерной сети, кибератака, мониторинг сетевой безопасности, анализ сетевого трафика.

Vasilyeva I.N.
St. Petersburg State Economic University,
The St. Petersburg University of the Ministry of Internal Affairs of Russia

A MODERN APPROACH TO MONITORING THE SECURITY OF NETWORK INFORMATION INFRASTRUCTURES

Annotation. The article discusses modern concepts of corporate computer network security, examines the features of such a class of information security solutions as network traffic analysis systems (NTA) and assesses their role in the protection of corporate information infrastructure.

Keywords: information security, information security tools, computer network security, cyber-attack, network security monitoring, network traffic analysis.

В последнее время концепция обеспечения безопасности корпоративной сетевой инфраструктуры претерпевает значительное изменение. Традиционный подход, разделяющий сетевое окружение на внешнюю недоверенную среду и внутреннюю доверенную сеть предприятия и базирующийся на защите внешнего сетевого периметра, уже не эффективен. Этому способствует как размытие границ сетевого периметра, так и

развитие техники и тактики проведения атак, все чаще способных обходить традиционные средства защиты информации, работающие на границе сети.

Широкое использование для доступа к корпоративным приложениям и данным мобильных устройств, в том числе, используемых и для личных целей, развитие внешних облачных сервисов, необходимость обеспечения регулярной и полноценной дистанционной работы пользователей во время пандемии приводят к увеличению числа точек входа в корпоративную сеть, и фактическому перемещению ее периметра в то место, где в настоящее время работает пользователь.

Еще одна проблема – увеличение числа сложных целенаправленных APT- атак, широко использующих техники социальной инженерии для проникновения в корпоративную инфраструктуру. До начала активных действий инфраструктура компании тщательно изучается злоумышленниками, а используемые вредоносные инструменты зачастую специально разрабатываются или модифицируются для обхода используемых средств защиты. Так, по данным компании Positive Technologies, более 90% компаний не защищены от внешних угроз, при этом процесс компрометации всей информационной инфраструктуры для них занимает менее суток ([1], [2]). В целом в 2020 году заметен существенный рост числа фиксируемых атак, что объясняется массовым переводом сотрудников на удаленный режим работы и ростом числа открытых сервисов, доступных извне компании.

Как только злоумышленник попадает на какой-либо узел внутренней сети, модель безопасности, доверяющая внутренним узлам, перестает действовать. Поэтому последнее время все большую популярность приобретает модель «нулевого доверия» (Zero Trust), разработанная еще в 2010 году. В отличие от традиционной модели сетевой безопасности, в которой пользователи, устройства и приложения, находящиеся в зоне доверия, обладают определенной свободой действий без дополнительных проверок, модель Zero Trust предполагает отсутствие какого-либо доверия по умолчанию. Каждый раз, когда пользователю, устройству или приложению потребуется доступ к какому-либо корпоративному ресурсу, они должны быть надлежащим образом аутентифицированы.

По сути, Zero Trust – это не какое-то защитное решение, а набор требований к организации системы защиты сетевой инфраструктуры организации. Кроме аутентификации и авторизации всех действий в корпоративной сети, она включает такие компоненты, как реализация принципа минимальных привилегий на уровне политики управления доступом, а также сегментация (или даже микросегментация) сети, что позволяет выделять отдельные зоны со своими политиками безопасности и правами доступа.

Периметр безопасности сужается до уровня отдельных узлов, которые могут состоять даже из одного-единственного устройства или приложения. Таким образом, обеспечивается контроль непосредственно на этапе доступа к данным (Рис. 1).

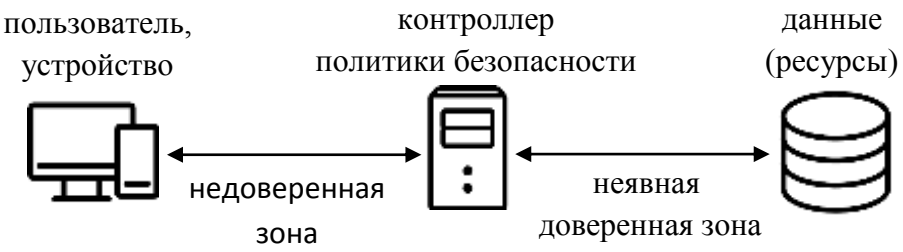


Рисунок 1 – Сужение контролируемого периметра до уровня данных

Идея нулевого уровня доверия применительно к сетевому доступу (Zero Trust Network Access) означает, что прежде чем предоставить доступ к данным, необходимо проверить надежность источника, из которого поступил запрос. При сетевом доступе каждый пользователь проходит проверку до и во время подключения, и каждое подключение регулируется политикой, которая контролирует, к каким ресурсам можно получить доступ. Идентификация происходит не просто по IP-адресу или имени устройства, как в традиционной модели, а производится аутентификация пользователя, устройства (компьютера), с которого осуществляется подключение, и используемого приложения (процесса), которое пытается получить доступ к данным. С технической точки зрения контролируемый доступ к корпоративным данным (ресурсам) реализуется с помощью контроллера политик безопасности, управляющего политиками доступа на уровне пользователей, устройств и приложений, а также сервисного шлюза, который осуществляет фильтрацию подключений на основе политик безопасности.

Все эти мероприятия нацелены на усиление контроля доступа и затруднение горизонтального перемещения злоумышленника внутри корпоративной сети. Еще один немаловажный компонент – мониторинг состояния сети.

Контроль доступа к данным может осуществляться на уровне хостов сети, кроме того, может контролироваться доступ на уровне периметра, однако то, что происходит между этими двумя уровнями, то есть события внутренней сети, остается вне поля зрения средств защиты информации. В большинстве случаев это дает внутренним нарушителям или проникнувшим во внутреннюю сеть атакующим получить контроль над сетью.

Получив первоначальный доступ к какому-либо узлу сети, и попав таким образом вовнутрь сетевого периметра, злоумышленник осуществляет различную деятельность – исполнение вредоносных программ, закрепление на узлах сети, повышение полномочий, исследование сетевой инфраструктуры и горизонтальное перемещение внутри сети [3]. Эту активность необходимо своевременно выявлять для блокирования атаки на ранних стадиях. При этом традиционные средства мониторинга трафика, работающие на периметре сети, с такой задачей справиться не могут, поскольку:

– проводят анализ внешнего трафика, в то время как нарушитель действует внутри сети;

– не имеют необходимых технологий для выявления угроз внутренней сети;

– работают в режиме реального времени, не записывают и не хранят трафик, что не позволяет обнаруживать сложные целенаправленные атаки, реализация которых, как правило, разнесена во времени;

– а также не дают достаточной информации для ретроспективного анализа и проведения криминалистического расследования в случае обнаружения инцидентов безопасности.

Даже если использовать традиционную систему обнаружения вторжений для анализа внутреннего трафика, это не позволит выявить скрытые каналы передачи данных, перемещения злоумышленника по сети, атаки на Active Directory и другие виды угроз.

Положение усугубляется тем, что для осуществления атак зачастую применяется техника «выполнение пользователем», когда в результате фишинга введенный в заблуждение пользователь сам выполняет требуемые злоумышленникам действия, а также используются данные легальных учетных записей и традиционные средства сетевого администрирования [4]. Отличить такие действия от обычной сетевой активности традиционными сигнатурными методами практически невозможно. Все это существенно затрудняет детектирование внутренних атак, делая действия злоумышленников «невидимыми» для традиционных средств защиты информации. По оценкам специалистов компании Positive Technologies, среднее время скрытного присутствия злоумышленников в сети с момента первоначального доступа составляет более полугода [2].

Для решения этих проблем требуется сформировать принципиально новый подход к мониторингу корпоративной сети. Такой подход реализуется новым классом средств защиты – NTA (Network Traffic Analysis), предназначенным, прежде всего, для анализа внутреннего трафика и детектирования подозрительных действий в сети, которые могут свидетельствовать о реализации атак на корпоративную инфраструктуру.

Применение средств класса NTA для пилотного мониторинга корпоративных сетей позволило выявить следующие типовые проблемы [5]:

– нарушение регламентов информационной безопасности;
– наличие подозрительной активности в сети;
– активность вредоносного программного обеспечения;
– попытки эксплуатации уязвимостей;
– попытки подбора паролей.

При этом среди основных факторов риска исследователи отмечают использование незащищенных сетевых протоколов (LLMNR, NetBios), и особенно протокола удаленного рабочего стола (Remote Desktop Protocol, RDP), нескольких утилит удаленного администрирования, многие из которых являются уязвимыми. Использование слабых паролей позволяет злоумышленникам успешно получать доступ к учетным записям зарегистрированных пользователей и повышать привилегии.

Работа средств защиты информации класса NTA во многом схожа с действием систем обнаружения вторжений, однако NTA-системы позволяют сканировать не только внешний (входящий и исходящий), но и внутренний сетевой трафик, не выходящий за рамки корпоративной сети. Их настройка производится исходя из специфики внутрисегментных атак, поэтому NTA могут обнаруживать такие злоупотребления как:

– внутреннее сканирование сети;
– получение данных с контроллера домена (например, выгрузка сведений о пользователях домена, входящих в группу администраторов);
– попытки удаленного запуска процессов и инструмента командной строки;
– запуск инструментов администрирования (таких, как PowerShell, WMI);
– подключения, использующие сокрытие трафика (проксирование, туннелирование);
– подключения по протоколу RDP;
– появление новых DHCP-серверов и др.

Большинство из этих действий могут быть легитимными, в частности, выполняться сетевыми администраторами в целях диагностики, однако такие действия требуют внимания и проведения анализа контекста, поскольку в равной степени такая деятельность может свидетельствовать об активности нарушителей в сети.

Кроме того, диагностируются действия, традиционно рассматриваемые в качестве свидетельств проведения атак:

– подключения к подозрительным внешним адресам;
– множественные неудачные попытки аутентификации;
– запуск известных инструментов проведения атак.

Поскольку системы анализа внутреннего трафика (в частности, NTA) должны отслеживать весь объем сети, одной точки сбора данных здесь недостаточно. Архитектурно такие системы состоят из ядра, проводящего общий анализ и детектирование угроз, и сенсоров. Сенсоры – это программное обеспечение, осуществляющее захват сырого сетевого трафика и его разбор по протоколам (SMB, DCE/RPC, Kerberos, LDAP и др.), а также первичный анализ трафика по заданным правилам. Также сенсоры позволяют, кроме того, хранить сырой трафик (файлы PCAP).

Сенсоры устанавливаются там, где есть возможность наиболее полного охвата передаваемого трафика, например, подключаются к коммутаторам, с которых на сенсоры зеркалируется весь трафик соответствующих сегментов. Таким образом средство мониторинга (NTA) может контролировать весь трафик сети или трафик произвольного набора сетевых сегментов (Рис. 2).

Системы анализа сетевого трафика NTA проверяют метаданные в реальном времени из всех сетевых сообщений, включая зашифрованные, со второго по седьмой уровни модели сетевой архитектуры OSI. Кроме того, для анализа контекста могут дополнительно привлекаться различные логи и журналы регистрации событий.

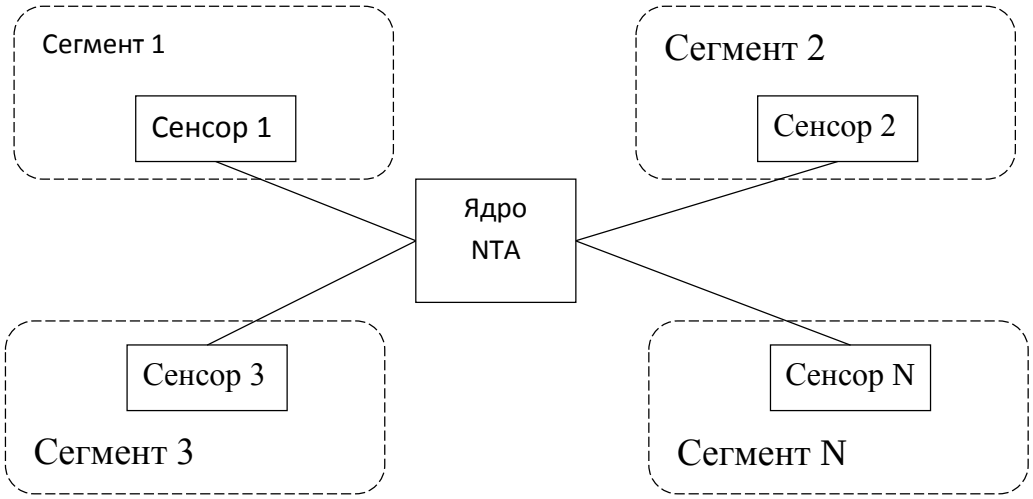


Рисунок 2 – Схема встраивания системы NTA
в инфраструктуру организации

Следует отметить, что NTA являются не единственными средствами контроля состояния внутренней сети. К таким средствам можно отнести прежде всего, SIEM системы (Security Information and Event Management). SIEM позволяет централизованно собирать, накапливать и проводить анализ данных от других средств защиты информации и протоколирования событий (журналы регистрации событий, логи). Эти данные часто отра-

жают разные аспекты деятельности в компьютерных системах и представлены в различных форматах. SIEM позволяет работать с разными форматами логов из разных источников и представлять информацию о событиях в единообразном виде. Кроме того, она позволяет проводить анализ полученных данных – осуществляет таксономию (распределяет поступающие данные по типам и категориям) и корреляцию данных (связывает разрозненные события между собой) и другие виды статистического анализа, что позволяет выявлять различные аномалии. На основе корреляции событий могут быть выявлены угрозы безопасности.

В структуре SIEM системы можно выделить агентов, осуществляющих сбор информации о событиях безопасности, централизованное хранилище данных и сервер обработки, реализующий функции анализа получаемой информации и управления инцидентами, включая выдачу уведомлений безопасности и генерации отчетов.

Информацию о злоупотреблениях внутри корпоративной сети отчасти могут предоставить и средства защиты отдельных узлов – средства антивирусной защиты, межсетевые экраны и средства обнаружения вторжений уровня хоста. В последнее время развитие получают комплексные средства защиты, позволяющие обеспечить активную реакцию на обнаруживаемые угрозы – EDR (Endpoint Detection and Response). Идея, лежащая в основе EDR, – не только обнаружение и блокирование атак, нацеленных на конечные точки, но и рассмотрение их в более широком контексте – как возможную составную часть реализацию более опасного и сложного сценария атаки, нацеленной на организацию в целом. EDR-система состоит из сервера и агентов, устанавливаемых на конечные точки.

Как видно, все эти три типа систем мониторинга имеют сходную распределенную архитектуру и нацелены на выявление всесторонней информации и формирование как можно более полного представления о проблемах безопасности на уровне корпоративной инфраструктуры в целом. Поэтому, наряду с привычными SIEM системами, системы NTA и EDR рассматриваются в настоящее время как неотъемлемые части корпоративного центра безопасности SOC (Security Operation Center). Назначение SOC выходит за рамки только лишь реагирования на инциденты безопасности и понимается более широко – как постоянный мониторинг и поддержание безопасности информационной инфраструктуры компании.

В чем же заключается специфика именно NTA систем? Очевидно, они имеют большую сферу охвата по сравнению с EDR системами, и могут действовать проактивно, то есть, в отличие от SIEM, нацелены не только на выявление уже случившихся инцидентов безопасности, но на блокирование и предотвращение дальнейшего развития обнаруженных атак. Если SIEM системы предназначены, прежде всего, для сбора, агре-

гирования и анализа данных разнородных журналов, то NTA производит захват, разбор и анализ сетевых потоков в режиме реального времени. С этой точки зрения NTA системы больше похожи на средства обнаружения/предотвращения вторжений, и также, как и они, могут использовать для детектирования угроз как правила, так и методы поведенческого анализа, анализа аномалий, технологии машинного обучения и другие средства интеллектуализации.

Кроме того, большинство NTA систем могут сохранять перехваченный трафик, что позволяет в случае необходимости провести его более глубокий ретроспективный анализ и иные криминалистические исследования. Необходимость быстрой активной реакции в случае обнаружения атак для блокирования их дальнейшего развития (например, изоляция скомпрометированных узлов сети или учетных записей пользователей), требует высокой оперативности такого дополнительного анализа. Для проведения же самих исследований необходимо наличие высокой квалификации и достаточного опыта у оператора NTA системы. Компания может и не располагать подобными специалистами в своем штате.

Поэтому услуги центра безопасности SOC, и, в частности, мониторинг с использованием NTA систем зачастую предлагается на рынке в качестве услуги. Наиболее известными поставщиками услуг мониторинга внутренней сети на российском рынке являются компании Positive Technologies, Group IB, «Лаборатория Касперского», «Гарда Технологии».

Вместе с тем следует отметить еще одну современную тенденцию, которая порождает ряд проблем для всех систем сетевого мониторинга – шифрование трафика. Современные средства защиты информации все чаще используют защищенные туннели и шифрование для защиты передаваемой информации и противодействию атакам на традиционно открытые сетевые протоколы. Речь идет не только о VPN и практически полном шифровании веб-трафика за счет использования протокола HTTPS, но и, например, об использовании DOH – DNS over HTTPS для защиты от подмены DNS при «проксировании» трафика, шифровании трафика мобильными и облачными приложениями. Это приводит к тому, что объем зашифрованного трафика в корпоративной сети растет, а ее прозрачность для средств мониторинга снижается [6]. Выявление признаков вредоносной активности в зашифрованном трафике затруднено.

Технологии шифрования активно берутся на вооружение и злоумышленниками, как для деструктивных действий (например, вирусы-шифровальщики), так и для сокрытия передаваемой информации от систем защиты. При этом само по себе наличие зашифрованного туннеля уже не выглядит аномальным событием. Это значит, что средства мониторинга, в том числе, NTA системы, должны использовать методы выявле-

ния аномалий в зашифрованном трафике, не поддающемся традиционному анализу. Такой анализ может проводиться на основе метаданных внутри потока (внутрипотоковой телеметрии) ([7], [8]).

Подводя итог, можно заключить, что системы анализа внутреннего трафика, такие как NTA, становятся важным инструментом обеспечения безопасности корпоративных сетей. Применение таких систем особенно актуально для крупных информационных инфраструктур. Совместное применение SIEM, NTA и EDR систем позволяет оперативно выявлять злонамеренную активность в корпоративной сети и значительно снижают шансы нарушителей на достижение целей атак. Очевидно, эти средства ожидает совершенствование в направлении повышения интеллектуализации анализа, а также развития услуг мониторинга.

Литература

1. Непрерывный анализ защищенности бизнеса. [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/services/security-services/ (дата обращения: 20.03.2021).
2. Результаты анализа трафика в 41 компании и новые возможности PT NAD. [Электронный ресурс]. - URL: https://www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/PT_NAD_18_03.pdf (дата обращения: 20.03.2021).
3. ATT&CK Matrix for Enterprise. [Электронный ресурс]. - URL: https://attack.mitre.org/ (дата обращения: 20.03.2021).
4. Программы-вымогатели 2020/2021. // Group-IB. [Электронный ресурс]. - URL: https://www.group-ib.ru/resources/threat-research/ransomware-2021.html (дата обращения: 20.03.2021).
5. Топ угроз ИБ в корпоративных сетях. Результаты мониторинга сетевого трафика в 2020 году. // Positive Technologies. [Электронный ресурс]. - URL: https://www.ptsecurity.com/ru-ru/research/analytics/top-ugroz-ib-v-korporativnyh-setyah-2021/ (дата обращения: 20.03.2021).
6. Прозрачность корпоративных сетей в России, 2020 // Positive Technologies. [Электронный ресурс]. - URL: https://www.ptsecurity.com/ru-ru/research/analytics/prozrachnost-korporativnyh-setej-v-rossii-2020/ (дата обращения: 20.03.2021).
7. Как выявлять активность злоумышленников в зашифрованном трафике // Positive Technologies. [Электронный ресурс]. - URL: https://www.ptsecurity.com/ru-ru/research/webinar/298091/ (дата обращения: 20.03.2021).
8. Аналитика зашифрованного трафика // Cisco. [Электронный ресурс]. - URL: https://www.cisco.com/c/dam/m/ru_ru/campaigns/security/pdf/security_eta.pdf (дата обращения: 20.03.2021).

УДК 614

Воротков Павел Александрович
аналитик
Автономная некоммерческая организация
«Агентство по привлечению инвестиций Свердловской области»
г. Екатеринбург

ЧАСТНАЯ МЕДИЦИНА КАК КОМПЕНСАЦИОННЫЙ МЕХАНИЗМ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗДОРОВЬЯ НАСЕЛЕНИЯ (НА ПРИМЕРЕ СВЕРДЛОВСКОЙ ОБЛАСТИ)

Аннотация. В статье рассмотрены проблемы обеспечения инфраструктуры оказания медицинской помощи как системы обеспечения безопасности здоровья населения в заданных объемах, по видам и формам, без дополнительного бюджетного финансирования. Указаны пути решения, в частности - развитие в регионе частных лечебно-диагностических организаций.

Ключевые слова: здравоохранение, безопасность здоровья, лечебно-диагностические организации, частная медицина.

PRIVATE MEDICINE AS A COMPENSATORY MECHANISM IN THE SYSTEM OF ENSURING THE SAFETY OF PUBLIC HEALTH (ON THE EXAMPLE OF THE SVERDLOVSK REGION)

Vorotkov P.A.
Autonomous Nonprofit Organization
«Investment Promotion Agency of the Sverdlovsk regional»
Yekaterinburg

Annotation. The article considers the problems of providing the infrastructure of medical care as a system of ensuring the safety of public health in the specified volumes, by types and forms, without additional budget funding. Solutions are indicated, in particular, the development of private medical and diagnostic organizations in the region.

Keywords: healthcare, health safety, medical and diagnostic organizations, private medicine.

Медицина – важнейшая составляющая уровня жизни населения. В Свердловской области, территория которой насыщена множеством экологически вредных объектов, а тяжелые природно-климатические условия

больше способствуют потере, чем сохранению здоровья людей, современная и эффективная система здравоохранения – необходимое условие для обеспечения безопасности здоровья жителей региона.

Современные подходы к управлению здоровьем требуют не только перераспределения объемов медицинской помощи, но и пересмотра инфраструктуры здравоохранения. Она должна соответствовать потребностям населения, обеспечивать оказание медицинской помощи в заданных объемах по видам и формам, но при этом не быть избыточной и оставаться эффективной. Одним из наиболее эффективных способов обеспечения таких требований является развитие в регионе частных лечебно-диагностических организаций.

Как утверждает Евгений Рабцун, генеральный директор медицинского объединения «ЦСМ-Санталь», «По данным ФНС, в России 16,7 тысячи частных организаций, имеющих лицензию на медицинскую деятельность. Ежегодный прирост этой категории, по приблизительным подсчетам, составляет 1,7 тысячи. При стартовом объеме инвестиций в 50 млн рублей – это 80 млрд. рублей в год. Основной стимул для частников – оголенный спрос на доступную медицинскую помощь» [5].

Нужно отметить, что в Свердловской области частные медицинские учреждения занимают достаточно большое место. Так, из 2389 выданных региональным Минздравом медицинских лицензий – 1413 выданы частным медучреждениям [9], из 226 медицинских организаций, участвующих в реализации Территориальной программы государственных гарантий бесплатного оказания гражданам медицинской помощи в Свердловской области на 2019 год – 54 частных [8]. Впрочем, оговоримся, что из этих 54 медучреждений 19 составляют медсанчасти предприятий, выведенные в отдельные юридические лица, среди которых 7 больниц РЖД. По понятным причинам, основная функция этих предприятий – обслуживание своих сотрудников и совсем рыночными их считать нельзя, т.к. только свободные от основной задачи мощности направлены на реализацию коммерческих задач, что роднит эту категорию медучреждений с государственными.

Впрочем, немало и независимых медицинских учреждений, чувствующих себя вполне прилично в рамках взаимодействия с государственно системой здравоохранения. Наиболее ярким в этом формате является пример ООО «Уральский медицинский центр» (УМЦ). Этот проект — хороший пример симбиоза государственных больниц и частных медицинских организаций. Диализный центр «встраивается» в существующую и привычную для населения медицинскую инфраструктуру — городскую больницу. На текущий момент УМЦ имеет 12 подразделений диализных центров, в которые и приходят пациенты. Четыре отделения расположены

в Екатеринбурге, два в Нижнем Тагиле. Также есть отделения в Первоуральске, Среднеуральске, Каменске-Уральском, Красноуфимске, Асбесте и Краснотурьинске. В его клиниках обслуживается 1217 человек — это более 60% всех диализных пациентов области. До 2022 г. еще в пяти населенных пунктах Свердловской области появятся собственные диализные клиники. Проект реализуется в рамках концессионного соглашения с правительством Свердловской области. Общие инвестиции в открытие клиник в Уральском медицинском центре оценивают в 250 млн. рублей. В сентябре 2020 года проект получил статус стратегического для Свердловской области, что гарантирует поддержку на всех уровнях.

Здесь следует отметить, что Свердловская область – одна из наиболее продвинутых в части интеграции частных клиник в систему оказания высокотехнологичной медицинской помощи (ВМП). Из 29 медицинских организаций Свердловской области, оказывающих высокотехнологичную медицинскую помощь в рамках Территориальной программы государственных гарантий бесплатного оказания гражданам медицинской помощи – 7 частных [7]. Высокотехнологичной медицинской помощью в регионе занимаются семь частных клиник – «Здоровье 365», АО «Екатеринбургский центр МНТК «Микрохирургия глаза», ООО «Городская больница №41», «Новая больница», «Наш медицинский центр «Парацельс», Уральский клинический лечебно-реабилитационный центр (УКЛРЦ) и «УГМК - Здоровье». Максимальный объем ВМП частные клиники выполняют по профилям «офтальмология» (МНТК «Микрохирургия глаза»), «травматология и ортопедия» (УКЛРЦ) и «сердечно-сосудистая хирургия» (ООО «Новая больница»). В интервью директора ТФОМС Свердловской области Валерия Шелякина журналу «Вадемекум», отмечено, что «та же «Новая больница» в своем роде уникальное медучреждение – будучи полностью частным, оно так давно встроено в систему оказания медицинской помощи на территории Екатеринбурга (в том числе в программу маршрутизации пациентов), что сами местные жители зачастую принимают его за обычную муниципальную больницу» [17].

Следует отметить, что население региона достаточно активно пользуется медицинскими услугами и помимо системы ОМС. По данным Росстата, расходы населения области на медицинские услуги в последние годы стабильно составляют около 2% от общих, что в сумме составляет более 17 млрд. руб./год [11]. По объему добровольного медицинского страхования (ДМС) Свердловская область занимает 5 место в РФ (после Москвы, Московской области, Санкт-Петербурга и Республики Татарстан). В абсолютных цифрах сборы по ДМС в 2018 году составили 456 182 тыс. руб., увеличившись более, чем на четверть (+26.8%) к 2010 году [3].

В тоже время следует отметить, что из 200 частных медицинских учреждений, действующих в РФ и вошедших в рейтинг АЦ «Вадемекум» в 2020 году (по результатам 2019 года) в регионе присутствует 11, из них федеральных сетей – 4 (на текущий момент 3 - «Альфа-Центр здоровья» ушел из региона) [12].

Наиболее успешной из федеральных структур в этом списке выглядит «Национальная медицинская сеть», вошедшая в регион через приобретение уже существовавших клиник «Здоровье 365». На текущий момент это одна из крупнейших сетей многопрофильных медицинских клиник, оказывающая медицинскую помощь в Екатеринбурге. По данным самой клиники, за прошедший год в ней зарегистрировано более 175 тыс. посещений. Сегодня сеть «Здоровье 365» входит в тройку самых известных и посещаемых клиник Екатеринбурга. В ближайших планах – строительство многопрофильного медицинского центра со стационаром и операционным блоком.

В начале пути ГК «МедИнвестГрупп», которая открыла в июле 2020 года центр лучевой терапии в Свердловском областном онкологическом диспансере, реализованный на принципах государственно-частного партнерства (ГЧП) Объем инвестиций в проект составил более 700 млн. руб., комплекс станет частью реализуемого группой проекта по созданию центра ядерной медицины в регионе. Ожидается, что в ходе реализации проекта «МедИвестГрупп» запустит еще два новых проекта: центр лекарственной терапии в Екатеринбурге, клинико-диагностический центр и центр лекарственной терапии в Нижнем Тагиле. Кроме того, к концу 2023 года в Свердловском онкодиспансере начнет принимать пациентов по системе ОМС центр радионуклидной терапии.

Федеральная сеть клиник «Будь здоров» была создана «Ингосстрахом» в 2005 году и ориентирована на обслуживание клиентов, прикрепленных по программе добровольного медицинского страхования (ДМС). На текущий момент медучреждение в Екатеринбурге закрыто, но остается достаточно большая клиника в Каменске-Уральском.

В число 7 вошедших в рейтинг местных негосударственных медицинских учреждений входят сети медучреждений «УГМК-Здоровье», «Городская больница №41», «Гармония», «Доктор плюс», «Парацельс», «Эдельвейс», «СМТ-Клиника», насчитывающих суммарно 41 точку, из которых 14 приходится на «Доктор плюс». Их суммарная выручка в 2019 году составляет около 4 млрд. руб., из которых более 40% приходится на «УГМК-Здоровье». Прирост результатов по сравнению с предыдущим годом составил более 12%, причем объемы выручки выросли у всех участников списка. Лидером роста стал «Эдельвейс» - более, чем в 1,5 раза, крупнейшая клиника - «УГМК-Здоровье» - выросла на 16%. Здесь нужно

учесть, что в рейтинг почему-то не попал один из крупнейших операторов регионального рынка медицинских услуг – «Новая больница» (которая уже упоминалась выше) с выручкой около 1.5 млрд. руб. Это вполне сопоставимо с клиникой УГМК.

Таким образом, мы видим 2 противоположных тенденции – федеральные сети медицинских учреждений снижают свою активность в Свердловской области, тогда как местные операторы медицинских услуг вполне заметно наращивают обороты.

Рискнем предположить, что решающим фактором в данном процессе выступает нехватка медицинских кадров. Важность этого фактора отмечают, например, EY в своем «Исследовании рынка коммерческой медицины в России 2018-2019 годы» и BusinesStat в своем «Анализе рынка медицинских услуг в России в 2015-2019 гг., оценка влияния коронавируса и прогнозе на 2020-2024 гг.». Так, в отчете EY говорится, что «Участники исследования отмечали возросшую избирательность пациентов в отношении репутации врачей, в том числе тщательное изучение информации и отзывов о конкретных специалистах на ресурсах лечебных учреждений, сайтах отзывов и медицинских агрегаторов. Также респонденты упоминали о том, что у пациентов есть любимые врачи в разных клиниках, особенно в тех направлениях, где необходимо постоянное наблюдение у одного специалиста (например, в гинекологии, педиатрии или в случае хронических заболеваний)» [6, с.16]. По данным исследования BusinesStat главными факторами лояльности коммерческим клиникам в Москве пациенты называли высокую квалификацию врачей и эффективное лечение, а в целом по России – полноценность приема, эффективность лечения, хорошее соотношение между ценой и качеством и высокую квалификацию врачей [2]. Более того, EY отмечает, что «подавляющее количество опрошенных в качестве ключевой проблемы обозначили нарастающую конкуренцию со стороны государственных учреждений за врачебный персонал, что может в дальнейшем привести к оттоку части пациентов из частных клиник» [6, с.16].

В свете вышесказанного нужно учесть кадровую ситуацию в медицине региона. Свердловская область занимает, по данным Росстата, 58 место по количеству врачей и 41 место по количеству среднего медицинского персонала на 10000 населения среди субъектов РФ ([14], [15]). Это говорит о том, что регион испытывает вполне серьезную нехватку врачебных кадров (по данным Правительства области, на начало 2020 года – около 700 специалистов [16]). Для инорегиональных частных медицинских учреждений такая ситуация обозначает необходимость конкурировать за персонал еще и с местными частными игроками, укорененными в

медицинскую среду региона (наиболее яркий пример - «УГМК-Здоровье», генеральный директор которого – М.С. Скляр, 8 лет занимал пост министра здравоохранения Свердловской области), а так же с ведомственными больницами, которые, не будучи ограниченными тарифными рамками в государственных медучреждениях и экономической эффективностью в частных, составляют серьезную конкуренцию в привлечении необходимых им специалистов (наиболее яркий пример – сеть клиник РЖД). Таким образом, тесная интеграция в региональное медицинское сообщество, обусловливающая возможность привлечения «знаковых» персоналий во врачебной среде, очевидно, является, как минимум, существенным фактором для успеха медицинского учреждения вне зависимости от его принадлежности. Собственно, это мы и наблюдаем – из 4 серьезных федеральных сетей, заходивших на медицинский рынок Свердловской области, комфортно себя чувствуют «Национальная медицинская сеть», сохранившая инфраструктуру и местный бренд «Здоровье 365» и «МедИнвестГрупп», действующая в формате симбиоза с Свердловским областным онкологическим диспансером. Клиники федеральных страховщиков, зашедшие в Екатеринбург самостоятельно, уже закрылись.

В целом, можно отметить, что, в целом, рынок многопрофильных частных медицинских учреждений в Свердловской области, несмотря на потенциал развития (см. темпы роста местных частных медучреждений), не особенно расположен к инорегиональным участникам. Их вхождение в регион без наличия уникального для территории и интересного для региональных органов власти предложения достаточно затруднительно. Скорее всего, в перспективе, с учетом ограничений с позиции ограничений в части покупательной способности населения, повышения качества государственной медицины и ограниченного кадрового ресурса, возможности для прихода новых частных медицинских учреждений будут сильно ограничены.

В то же время, в секторе частной медицины есть ниша, ситуация в которой заметно отличается от вышеприведенной. Это рынок лабораторной диагностики. В большинстве случаев лабораторные исследования необходимы для правильной постановки диагноза, поэтому востребованность данных услуг прямо коррелирует с востребованностью медицинских. В государственных медучреждениях данная сфера обычно интегрирована в общую систему оказания медицинских услуг, хотя технологически и организационно медицинские лаборатории и там отделены от клинических учреждений. В частной медицине предприятия лабораторной диагностики организационно зачастую никак не связаны с собственно медицинскими учреждениями, что, в общем, не мешает им взаимодействовать к взаимной выгоде.

По оценкам BusinesStat, за 2016-2019 гг. в России объем рынка лабораторной диагностики относительно стабилен (увеличение за 4 года на 2,8%: с 272,2 млн. исследований до 279,7 млн. исследований). Число проводимых лабораторных исследований ежегодно росло как в государственных медицинских учреждениях, так и в коммерческих лабораториях [1].

В 2020 г объем российского рынка услуг медицинских лабораторий резко вырос и достиг 330,6 млн. исследований, что на 18,2% превысило значение 2019 г. Впрочем, причина понятна - масштабное проведение исследований на выявление коронавируса. Объем прочих исследований сократился в связи со снижением доступности медпомощи по направлениям, не связанным с лечением коронавируса.

Дальнейшее развитие рынка будет зависеть от стабилизации эпидемической ситуации в стране. В 2021 г. ожидается, что тестирование на коронавирус будет по-прежнему актуальным, при этом восстановятся объемы исследований, не связанных с коронавирусом. В результате, численность проведенных лабораторных исследований в России ориентировочно составит 373,7 млн., что на 13,0% превысит значение 2020 г.

В 2022-2023 гг. BusinesStat прогнозирует сокращение объема российского рынка лабораторной диагностики до 336,7 млн. исследований за счет уменьшения числа проводимых тестов на коронавирус. Дальнейший рост рынка будет поддерживаться в основном за счет наращивания объемов исследований, не связанных с коронавирусом. В результате, к 2025 г. ожидаемая численность проведенных лабораторных исследований в России достигнет 342,7 млн., что на 22,5% превысит значение 2019 г., т.е. в течение ближайших 4-5 лет объем исследований вырастет приблизительно на четверть по сравнению с допандемическим периодом.

Что касается Свердловской области, то по данным регионального Минздрава, количество лабораторных исследований достаточно стабильно растет. Причем, если с 2005 г. по 2014 г. рост составлял 3% - 4%, то после спада в 2015 г. – 2016 г., начиная с 2016 года темпы прироста составляют около 10% - 11% в год. В результате их количество с 2010 года выросло приблизительно на треть [4, с.150-152]. Понятно, что эти цифры не полностью отражают ситуацию, т.к. фиксируют только количество исследований, выполненных в подведомственных региональному министерству учреждениях, однако сама по себе тенденция вполне очевидна.

Более того, учитывая, что в соответствии со Стратегией развития здравоохранения Свердловской области до 2035 года, «в ближайшие 10–15 лет в сохранении здоровья населения будет увеличиваться роль широкомасштабной диспансеризации различных групп населения, построенной на основе алгоритма, предусматривающего проведение ежегодных профилактических осмотров детей всех возрастных категорий и

ежегодную диспансеризацию не менее 23% взрослого населения» [10, с.15], количество лабораторных исследований будет продолжать увеличиваться. Основными направлениями роста, скорее всего, станут исследования в сфере онкологии, сердечно-сосудистых болезней, а также диагностики врожденных наследственных заболеваний у новорожденных детей. Именно эти направления прописаны в качестве приоритетных в региональной составляющей федерального проекта «Здравоохранение».

Если говорить о частных организациях, осуществляющих на территории области лабораторную диагностику, то следует отметить, что в регионе присутствуют 5 крупнейших частных сетевых клинико-диагностических лабораторий РФ - «ИНВИТРО», «Гемотест», «Хеликс», «СИТИЛАБ», KDL [13]. Их лаборатории берут на себя основную нагрузку в части клинических исследований населения, выходящих за пределы государственных клинико-диагностические лабораторий. Роль местных самостоятельных диагностических лабораторий невелика, что, в общем, легко объяснимо – в данной сфере доступ к высокотехнологичному (а, соответственно, и дорогостоящему) оборудованию заметно важнее уровня персонала и, вследствие этого, финансовые возможности федеральных игроков на этом рынке позволяют им не только сохранять, но и расширять свою сферу присутствия в регионе. Более того, в некоторых случаях сами медицинские учреждения интегрируют лабораторные сети в свою инфраструктуру. Примером может служить региональная сеть частных клиник «Эдельвейс», которая передала все клинические исследования «Ситилаб». В данной ситуации клиника сэкономила на оборудовании для исследований, а лаборатория получила целевой доступ к базе пациентов клиники.

Соответственно, перспектива для вхождения на рынок лабораторной диагностики Свердловской области существует, особенно если учесть рост объемов при параллельном уменьшении количества клинико-диагностических лабораторий в Свердловской области со 171 в 2010 г. до 150 в 2017 г. (более свежих данных нет, но вряд ли тенденция изменилась при сохранении общих подходов) [4, с.150-152]. Государственные действующие лаборатории становятся крупнее, но доступность все равно уменьшается. Но при вхождении на рынок Свердловской области обязательно нужно учитывать приоритеты региональной системы здравоохранения. В данном случае можно рассчитывать на содействие региональных властей с точки зрения поддержки размещения медицинских объектов, организации взаимодействия с местным медицинским сообществом, включения в систему ОМС, а также маршрутизации пациентов в сторону новой инфраструктуры.

Таким образом, частные медицинские организации четко реагируют на изменение спроса на медицинские услуги населения, как с точки зрения насыщения рынка, так и с позиций избыточного предложения, позволяя тем самым государству решать проблему обеспечения инфраструктуры оказания медицинской помощи. Тем самым обеспечивается безопасность здоровья населения в заданных объемах по видам и формам без дополнительного бюджетного финансирования.

Литература

1. Анализ рынка лабораторной диагностики в России в 2016-2020 гг., оценка влияния коронавируса и прогноз на 2021-2025 гг. [Электронный ресурс]. – URL: https://businesstat.ru/images/demo/laboratory_services_russia_demo_businesstat.pdf
2. Анализ рынка медицинских услуг в России в 2015-2019 гг, оценке влияния коронавируса и прогнозе на 2020-2024 гг. [Электронный ресурс]. – URL: https://businesstat.ru/images/demo/medicine_russia_demo_businesstat.pdf
3. Выплаты по договорам страхования, осуществленные страховыми организациями, по добровольному медицинскому страхованию по субъектам Российской Федерации // Т.7.4. Росстат 2020. [Электронный ресурс]. – URL: https://gks.ru/bgd/regl/b19_34/IssWWW.exe/Stg/r_7.xls
4. Доклад «О состоянии здоровья граждан, проживающих в Свердловской области в 2017 году» // Официальный интернет-портал правовой информации Свердловской области. [Электронный ресурс]. – URL: http://www.pravo.gov66.ru/media/pravo/736-ПП_cmOhYGK.pdf
5. Зачем Минздрав предложил ввести двойное лицензирование медицинских проектов. [Электронный ресурс]. – URL: http://www.np-med.ru/article/1011/
6. Исследование рынка коммерческой медицины в России 2018-2019 годы. [Электронный ресурс]. – URL: https://assets.ey.com/content/dam/ey-sites/ey-com/ru_ru/news/2020/03/ey_health-care_research_2018-2019_24032020.pdf
7. Перечень медицинских организаций Свердловской области, оказывающих высокотехнологичную медицинскую помощь в рамках Территориальной программы государственных гарантий бесплатного оказания гражданам медицинской помощи. [Электронный ресурс]. – URL: https://minzdrav.midural.ru/article/show/id/1072
8. Перечень медицинских организаций, участвующих в реализации территориальной программы государственных гарантий бесплатного ока-

зания гражданам медицинской помощи в Свердловской области на 2019 год и на плановый период 2020 и 2021 годов. [Электронный ресурс]. – URL: https://minzdrav.midural.ru/uploads/Перечень%20медицинских%20организаций%20Свердл_обл_%20по%20запросу%20МЗРФ.xlsx

9. Реестр организаций, имеющих лицензию на осуществление медицинской деятельности на территории Свердловской области. [Электронный ресурс]. – URL: http://open.midural.ru/opendata/6660010415-reestr_mo_licenzuya_na_med_dey

10. Стратегия развития здравоохранения Свердловской области до 2035 года // Официальный интернет-портал правовой информации Свердловской области. [Электронный ресурс]. – URL: http://www.pravo.gov66.ru/media/pravo/574-ПП_vtQeNqN.pdf

11. Структура потребительских расходов домашних хозяйств по КИПЦ-ДХ (Классификатор индивидуального потребления домашних хозяйств) // Росстат 2020. [Электронный ресурс]. – URL: https://rosstat.gov.ru/bgd/regl/b19_102/IssWWW.exe/Stg/god/pril1.xls

12. Топ 200 частных многопрофильных клиник России. // «Вадемекум» Деловой журнал об индустрии здравоохранения. [Электронный ресурс]. – URL: https://vademec.ru/download/Таблица_ТОП200_5_2020.pdf

13. Топ-20 крупнейших клинико-диагностических лабораторий РФ // Журнал «Здравоохранение России». [Электронный ресурс]. – URL: https://zdorovayarossia.ru/ratings/top-20-krupneyshikh-kliniko-diagnosticheskikh-laboratoriy-rf/

14. Численность врачей на 10 000 человек населения по субъектам Российской Федерации // Т.4.4. Росстат 2020. [Электронный ресурс]. – URL: https://gks.ru/bgd/regl/b19_34/IssWWW.exe/Stg/r_4.xls

15. Численность среднего медицинского персонала по субъектам Российской Федерации. // т.4.6. Росстат 2020. [Электронный ресурс]. – URL: https://gks.ru/bgd/regl/b19_34/IssWWW.exe/Stg/r_4.xls т.

16. Чукреев И. Свердловское правительство пообещало закрыть проблему нехватки врачей в области к 2022 году. [Электронный ресурс]. – URL: https://eanews.ru/news/sverdlovskoye-pravitelstvo-poobeshchalo-zakryt-problemu-nekhvatki-vrachey-v-oblasti-k-2022-godu_05-03-2020

17. Шубина Д., Добровольский Т., Юрасов Ф. Как операторы высокотехнологичной медпомощи борются за пациентов и деньги. // «Вадемекум» Деловой журнал об индустрии здравоохранения. [Электронный ресурс]. – URL: https://vademec.ru/article/glubinnaya_pompa/

УДК 004.056:621.391

Ильина Ольга Павловна
канд. экон. наук, профессор
Санкт-Петербургский государственный
экономический университет

МОДЕЛИРОВАНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЦИФРОВОГО ПРЕДПРИЯТИЯ

Аннотация. Система информационной безопасности цифрового предприятия имеет архитектуру, компонентами которой являются ИТ-решения по реализации требований к защите цифровых активов (программ, информации, технологических процессов, исполнителей), риски информационной безопасности и средства управления защитой от кибер-угроз.

Ключевые слова: архитектура системы, информационная безопасность, модель, система, цифровая платформа, цифровое предприятие, экосистема.

Ilyina O.P.
St. Petersburg State Economic University

MODELING OF THE INFORMATION SECURITY SYSTEM OF A DIGITAL ENTERPRISE

Annotation. The information security system of a digital enterprise has an architecture, the components of which are IT solutions for the implementation of requirements for the protection of digital assets (programs, information, technological processes, performers), information security risks and cyber threat protection controls.

Keywords: system architecture, information security, model, system, digital platform, digital enterprise, ecosystem.

Федеральный проект «Информационная безопасность» национальной программы «Цифровая экономика» определяет информационную безопасность как «достижение состояния защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет и устойчивое социально-экономическое развитие Российской Федерации». Ключевые направления мероприятий федерального проекта «Информационная безопасность» на период до 2024 года [1]:

- рост уровня защищенности личности, информационной безопасности и устойчивости сетей связи общего пользования,

- создание новых сервисов (услуг) для граждан, гарантирующих защиту их персональных данных,

- профилактика и выявление правонарушений с использованием информационных технологий против общества и бизнеса,

- разработка новых механизмов поддержки отечественных разработчиков программного обеспечения и компьютерного оборудования в сфере информационной безопасности.

Цифровое предприятие - Digital Enterprise (DE) является основным субъектом цифровой экономики, для которого характерно наличие развитой ИТ-инфраструктуры, позволяющей применять цифровые технологии во всех сферах: в производстве продукции, выполнении работ и оказании услуг, так и в системе управления. Современные предприятия обладают и интенсивно используют цифровые активы, к которым относятся информационные, программные и технологические ресурсы, вычислительные устройства и сетевое оборудование. Неуклонно растет цифровая компетентность людей, вовлеченных в производственные процессы, обеспечивающие обслуживание и управление цифровыми активами и информационными системами предприятия. Благодаря цифровым технологиям предприятия получают конкурентные преимущества в бизнесе, переход на бизнес-модель, в которой цифровые технологии играют исключительно важную роль.

Цифровизация предприятий базируется на концепции программы «Индустрия 4.0», согласно которой происходит смена промышленного уклада экономики и процессов производства продукции. Федеральный проект «Цифровые технологии РФ» [2] предусматривает приоритетное внедрение следующих прорывных технологий:

1. Big Data – для обеспечения сбор, хранения и обработки огромных объёмов неструктурированных данных с целью извлечения из них новых знаний для принятия эффективных решений.

2. Различного вида нейротехнологии, имитирующие мыслительные процессы и высшую нервную деятельность человека (компьютерное зрение; обработка естественного языка; распознавание и синтез речи; интеллектуальные системы поддержки принятия решений; перспективные методы и технологии искусственного интеллекта и др.).

3. Надежное хранение данных и контроль их изменений в распределенной сети – «блокчейн», которая позволит организовать хранение цепочки блоков данных в сети, поддерживать распределенные бизнес-процессы, логистические и финансовые потоки, в которых множество участников.

4. Квантовые технологии, изменяющие основы передачи и обработки данных с помощью квантовых компьютеров.

5. Новые производственные технологии в ряде сегментов экономики.

6. Промышленный интернет вещей - Industrial Internet of Things (IIoT), когда различного рода датчики, контроллеры подключаются к узлам и агрегатам промышленного объекта, обеспечивают сбор и передачу данных для контроля за состоянием объектов, принятия оперативных управленческих решений.

7. Робототехника и сенсорика для взаимодействия технических систем между собой без участия и с участием человека.

8. Технологии беспроводной связи на основе радиоволн различных диапазонов, инфракрасного оптического или лазерного излучения. В частности, глобальная сеть связи, 5-е поколение мобильной связи; энергоэффективные сети дальнего радиуса действия для устройств IIoT; беспроводные сети связи для доступа в рамках локальных пространств; сети связи «вокруг» человека, спутниковые технологии связи.

9. Технологии виртуальной реальности (Virtual Reality, VR) для погружения человека в виртуальный мир, воспринимаемой человеком через ощущения, дополненной реальности (Augmented Reality, AR) для интеграции информации с объектами реального мира, расширения взаимодействия человека с окружающей средой.

Проект цифровой трансформации предприятия – сложный, как с точки зрения технической реализации, так и с точки зрения организационного и финансового обеспечения, сопряжен со многими рисками для социально-экономической и технологической систем. Большинству предприятий РФ требуется обновление материальной части – технологического оборудования, инженерных сетей, ИТ-инфраструктуры для реализации цифровых технологий более, чем на 50%. Процесс трансформации затрагивает организационную и экономическую основу предприятия, влечет существенные изменения состава и подчиненности структурных подразделений, штатного расписание (название должностей, профессий рабочих, численность, требования к компетенции кандидатов на занятие вакантных мест) и др. Для большинства бизнес-процессов проводится реинжиниринг.

Процесс цифровой трансформации подчинен тренду гибкости бизнеса - Business Agility, это быстрая, непрерывная и систематическая адаптация, предпринимательские инновации, направленные на получение и поддержание конкурентного преимущества с помощью цифровых технологий. Изменяются требования к информационным системам цифрового предприятия, которые должны обеспечить многоуровневую интеграцию распределенной системы управления.

Для успешного выполнения национального проекта цифровой трансформации предприятий необходимо применить архитектурный подход, рассматривая предприятие как большую и сложную систему. Под термином «архитектура системы (Architecture)» понимают представление базовых свойств системы в окружающей среде, воплощенное в ее элементах, отношениях и конкретных принципах развития [5]. Термин архитектура системы применительно к предприятию появился более 40 лет назад, трактовка термина: «архитектура предприятия (Enterprise Architecture)» рассматривается как область знаний об организованности систем, процессов, людей, инфраструктуры, данных, целей, задач, требований и др. ([5], [6]).

Архитектура предприятия употребляется в различных смыслах:

- как статическое описание всех аспектов функционирования предприятия;
- как метод изучения, анализа, основу принятия бизнес-, ИТ- и технических решений;
- как методология и дисциплина действий архитекторов предприятия, специалистов в области интеграции бизнес-систем и ИТ-систем.

Для создания архитектуры предприятия разработаны архитектурные фреймворки (TOGAF 9.2, Zachman, DoDAF и др.), которые содержат концепцию и принципы архитектурного описания, требований к архитектурным моделям, методы разработки и рекомендация по управлению архитектурой предприятия. Созданы разнообразные языки для описания моделей архитектуры предприятия (UML, IDEF, BPMN, ARIS и др.), среди которых выделяют язык ArchiMate - открытый стандарт архитектурного моделирования.

Архитектура предприятия согласно TOGAF 9.2 [7] представляется с помощью моделей:

- бизнес-архитектуры, описывающей основные характеристики предприятия как бизнес-системы;
- архитектуры ИТ-системы, включая:
- архитектуру данных предприятия;
- архитектуру приложений – прикладные программы и сервисы для поддержки бизнес-процессов и бизнес-функций;
- архитектуру ИТ-инфраструктуры – вычислительная система и системное программное обеспечение, среда реализации информационных технологий.

Бизнес-архитектура предприятия представляется с помощью моделей:

1) бизнес-канва – описывает формируемые ценности для потребителей (бизнес-сервисы - продукция и услуги); ключевые бизнес-процессы,

производственные процессы, ключевые ресурсы; рынки сбыта, каналы товародвижения, характер взаимоотношений с клиентами, структуру затрат и потоки доходов предприятия;

2) оргструктура предприятия – состав структурных подразделений, распределение ответственности и полномочий среди ролей;

3) функциональная структура - состав функциональных подсистем и зада управления;

4) процессная структура – состав и взаимосвязи бизнес-процессов, характеристики: владелец процесса, конечный продукт как результат выполнения процесса, показатели результативности/эффективности процесса, состав и последовательность операций, входные и выходные материальные и информационные потоки, трудовые ресурсы, технологическое оборудование, характеристики операций (длительность, трудоемкость, стоимость и др.);

5) информационная структура – состав форм документов, схема документопотоков, системы классификации и кодирования технико-экономической информации, источники входной и потребители выходной информации в привязке к операциям бизнес-процессов и функциям системы управления;

6) мотивационная модель для стейкхолдеров содержит набор драйверов для цифровой трансформации, согласованные с ними цели и задачи и их результаты, бизнес-требования по отношению к ИТ-системе;

7) стратегическая модель цифрового предприятия определяет план реализации стратегических целей, соответствующие цифровые компетенции и возможности, а также предполагаемые для этого ресурсы различного вида.

На предприятии может быть несколько ИТ-систем, которые могут обслуживать определенный уровень управления, структурное подразделение, бизнес-сферу, комплекс бизнес-процессов и т.п. Для каждой ИТ-системы должен быть установлен состав и характеристики функциональных и обеспечивающих подсистем, требуемые информационные ресурсы (во внемашинном и внутримашинном представлении), прикладное и системное программное обеспечение, необходимая ИТ-инфраструктура, объединяющая в себе вычислительную систему для реализации процессов обработки данных, хранилища информационных ресурсов, стек сервисов для поддержки приложений и данных, для взаимодействия с внешними информационными системами. Архитектура ИТ-системы раскрывается с помощью модели инфо-канвы, в которой представлены интегрированные ИТ-системы предприятия, интерфейсы для взаимодействия с внешним информационным окружением.

Архитектура цифрового предприятия имеет сервис-ориентированный тип - Service Oriented Architecture (SOA), обеспечивает поддержку требования гибкости бизнеса, необходимую скорость внесения изменений в бизнес-систему и ИТ-систему. Модель сервисов в составе архитектуры цифрового предприятия представлена на языке Archimate 3.0 (Рис. 1).

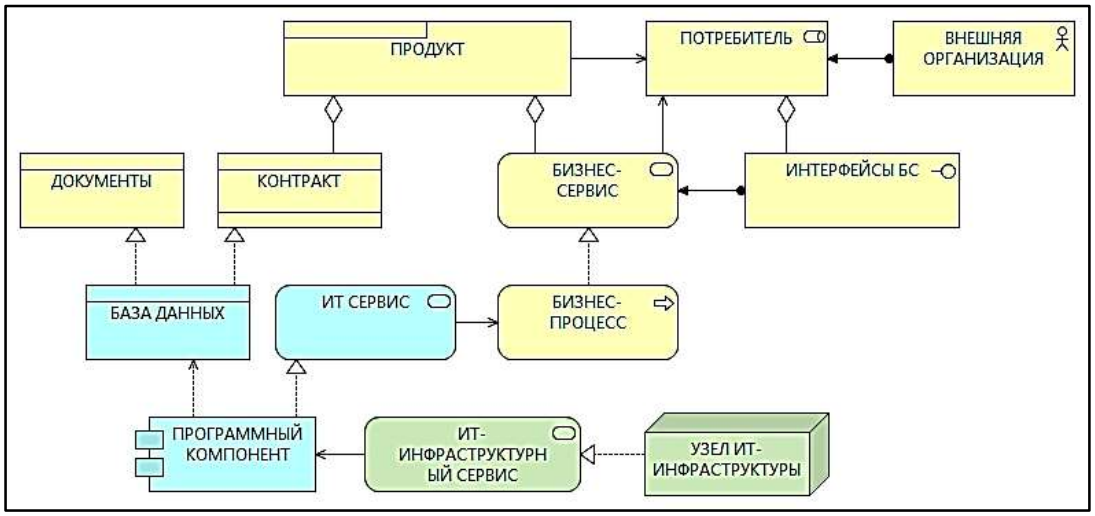


Рисунок 1 - Сервисы архитектуры предприятия

БИЗНЕС-СЕРВИСЫ – конечный результат деятельности предприятия путем выполнения БИЗНЕС-ПРОЦЕССОВ, ориентированы на потребности конечных потребителей (ВНЕШНЯЯ ОРГАНИЗАЦИЯ, которой назначена роль ПОТРЕБИТЕЛЯ бизнес-сервисов).

Совокупность бизнес-сервисов и обязательств предприятия перед клиентами, зафиксированных в документе типа КОНТРАКТ, представляет собой линейку ПРОДУКТОВ, с которыми предприятие выходит на рынок.

Успешная реализация бизнес-процессов требует поддержки со стороны ИТ-СЕРВИСОВ, которые создают ПРОГРАММНЫЕ КОМПОНЕНТЫ, обрабатывающие БАЗУ ДАННЫХ.

Информация ДОКУМЕНТОВ, КОНТРАКТОВ и т.п. содержится в базе данных.

ИТ-инфраструктура предприятия состоит из множества УЗЛОВ, включенных в компьютерные сети. УЗЛЫ создают ИТ-ИНФРАСТРУКТУРНЫЕ СЕРВИСОВ для поддержки программных компонентов и базы данных.

Для цифрового предприятия формируется динамический по составу и регламенту функционирования стек сервисов:

БИЗНЕС-СЕРВИС - > ИТ-СЕРВИС – ИТ ИНФРАСТРУКТУРНЫЙ СЕРВИС.

Переход к сервисной архитектуре несет определенные выгоды, а именно: динамичный набор сервисов, синхронное и асинхронное их взаимодействие компонентов ИТ-систем осуществляется на основе стандартов - XML, WSDL, BPEL и т. д.

Для разработки SOA цифрового предприятия используется эталонная сервис-ориентированная архитектура предприятия – Reference Model SOA (RM SOA) -Рис. 2, которая является многоуровневой структурой. Каждый слой содержит набор атрибутов, обязанностей и правил. Слои обычно имеют типичные механизмы взаимодействия друг с другом.

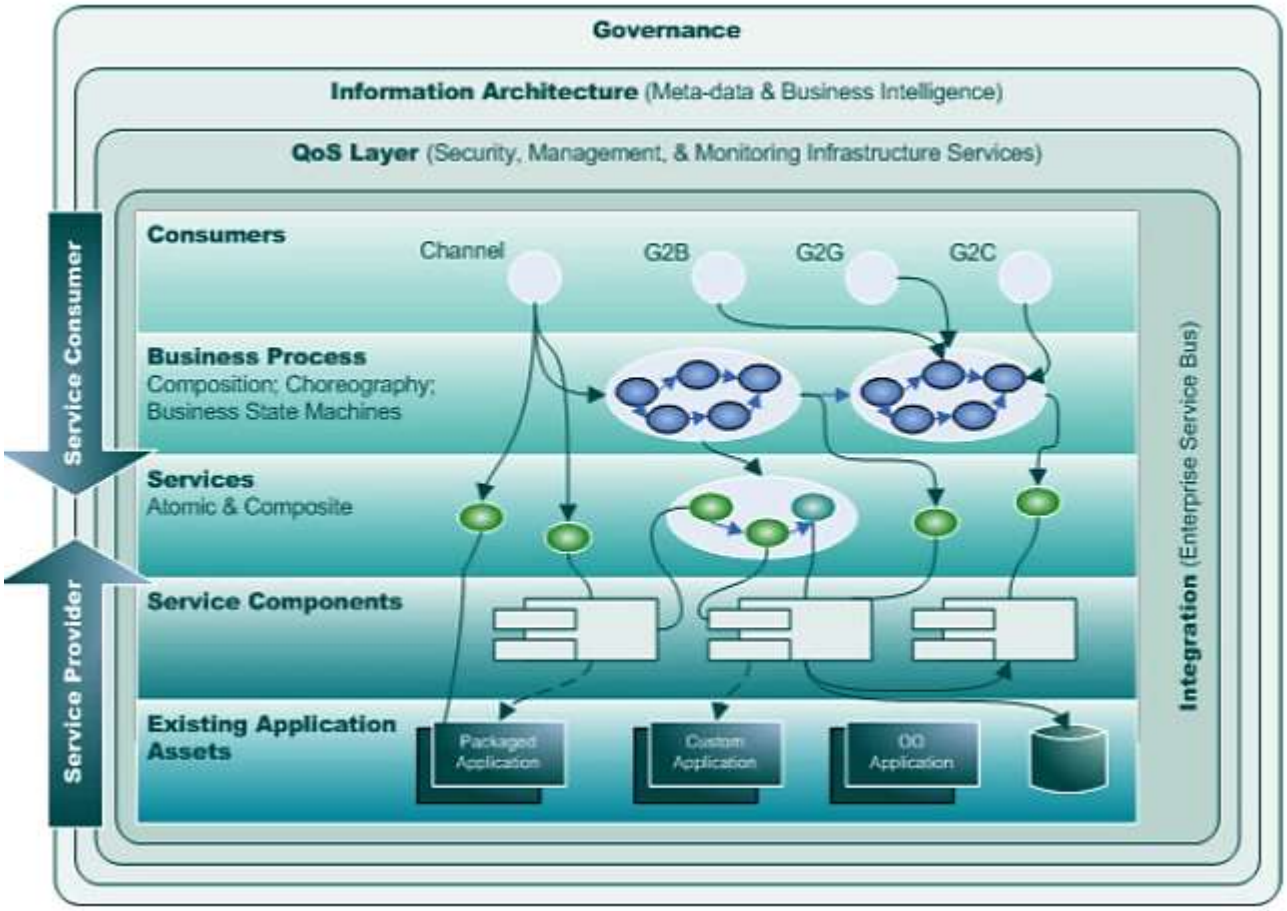


Рисунок 1 - Эталонная модель сервис-ориентированной архитектуры предприятия

На пользовательском уровне определяются требования к бизнес-сервисам, составу бизнес-процессов и используемых для их поддержки ИТ-сервисов приложений. ИТ-сервисы составлены из слабо связанных и легко заменяемых атомарных сервисов со стандартизированными интерфейсами. Многообразие атомарных сервисов позволяет оптимизировать ИТ-сервисы и влиять на эффективность приложений. Интерфейсы сервисов в SOA инкапсулируют детали реализации (операционную систему,

платформу, язык программирования) от остальных компонентов, таким образом обеспечивая комбинирование и многократное использование компонентов для построения сложных распределённых программных комплексов, обеспечивая независимость от используемых платформ и инструментов разработки, способствуя масштабируемости и управляемости создаваемых систем.

Атомарные сервисы конструктивно создаются на основе сервисных компонентов – микросервисов. Интеграция сервисов осуществляется с помощью программного обеспечения Enterprise Service Bus (ESB) - преобразование, маршрутизация, поддержка протоколов для передачи запросов на обслуживание сервисов к поставщику услуг, поддержка интеграции с платформами решений, возможность транспортировки результатов обработки сервисов получателям услуг и др. Для управления качеством сервисов выполняется мониторинг событий, позволяющий следить за работоспособностью сервисов, приложений, созданных на их основе, а также за состоянием ИТ-инфраструктуры. Информационный уровень SOA обеспечивает согласованное представление информации предприятия, участвует в управлении доступом и интеграцией данных разнородных источников с использованием метаданных, реализует политику информационной безопасности и защиты данных. Управления SOA строится на стандартах корпоративного уровня для реализации бизнес-целей и стратегий предприятия, ИТ-решений [8].

Информационная безопасность цифрового предприятия требует системного подхода к разработке и реализации системы информационной безопасности предприятия, сбалансированной относительно затрат на ее обеспечение и ценности защищаемых цифровых активов [9].

Традиционно информационная безопасность понимается как реализация требований по отношению к информационным ресурсам [10]:

- конфиденциальность контента (confidentiality of information), только авторизованные лица имеют доступ информации;
- целостность контента (integrity of information), в информации нет противоречий и несогласованности;
- доступность контента (the availability of information), авторизованным лицам доступна необходимая информация в нужное время, в нужном объеме.

В ряде источников по информационной безопасности указаны дополнительные требования, такие как владение или контроль информации, которые реализует владелец информации (ее авторы, а также авторизованные пользователи), аутентичность информации, актуальность, достоверность, точность; полезность информации для достижения целей системы управления и др. ([11], [12]). Экспликация понятий системы информационной безопасности представлена на Рис. 3.

Рисунок 2 - Основные понятия информационной безопасности

Цифровые активы предприятия рассматриваются в качестве объектов защиты, устанавливаются источники и виды угроз, риски, обусловленные воздействием угроз на объекты защиты. Деятельность по обеспечению информационной безопасности основывается на непрерывном мониторинге и обработки обнаруженных рисков, их анализа, оценках негативных последствий и выработке контрмер. Моделирование рисковых ситуаций предполагает создание концептуальной модели угроз, их проявления угроз для конкретных цифровых активов. Угрозы предпринимают следующие действия:

1) несанкционированный доступ к цифровым активам;
2) неправильное использование, нарушающее целостность цифровых активов;
3) незаконное раскрытие конфиденциальной информации;
4) несанкционированные изменения цифровых активов;
5) необеспеченность авторизованного доступа к цифровым активам и др.

Обеспечение информационной безопасности становится функцией системы управления предприятием, частью более широкого корпоративного контекста, оказывает влияние на все компоненты системы управления и архитектуру предприятия в целом, что объясняет необходимость перехода к гибкой архитектуре предприятия сервис-ориентированного типа.

Основные изменения в архитектурных моделях ([9], [12]):

1) мотивационная модель стейкхолдеров включает драйверы обеспечения информационной безопасности, стратегические цели и связанные с ними ограничения и конечные результаты;

2) бизнес-требования к ИТ-системе с позиций информационной безопасности определяют риск-аппетит, требования конфиденциальности, целостности, доступности цифровых активов;

3) новый раздел «Information Security/Информационная безопасность» модели бизнес-канвы представляет концепцию и принципы информационной безопасности;

4) элемент «Контракт» бизнес-архитектуры содержит заявление относительно информационной безопасности применения бизнес-сервисов для конченых потребителей;

5) раздел «Value Proposition/Ценностное предложение» бизнес-канвы представляет поток создания ценностей для конечного потребителя с учетом наличия системы информационной безопасности;

6) добавление в стратегическую модель формируемых компетенций с позиций цифровой трансформации и информационной безопасности, гибкости бизнеса (Business Agility);

7) стратегические цели и задачи информационной безопасности преобразуются в портфель ИТ-проектов – элемент Work Package, с указанием параметров и ресурсного обеспечения;

8) в модель функциональной структуры системы управления предприятием вводится подсистема «Информационная безопасность», в рамках которой организовано информационное обеспечение и процессное управление рисками;

9) разрабатываются модели процессов управления рисками информационной безопасности: идентификации, анализа, оценки, прогнозирования и мониторинга рисков;

10) модели информационного обеспечения системы информационной безопасности - структурs базы данных, наполнение базы знаний для принятия управленческих решений по отношению к рискам;

11) создание ИТ-сервисов для поддержки бизнес-процессов с учетом требований информационной безопасности на основе микросервисной программной архитектуры;

12) модель архитектуры ИТ-инфраструктуры на базе сервисов класса IaaS для обеспечения вычислительной мощности, объемов хранимых данных, требований цифровой платформы для вхождения в экосистемы цифрового предприятия;

13) изменения моделей организационной и ролевой структуры за счет цифровых компетенций, создание профилей ролей и др.

На Рис. 4 представлен фрагмент расширения архитектурной модели предприятия для системы обеспечения информационной безопасности (СИБ) и реализации функций информационной безопасности (ИБ).

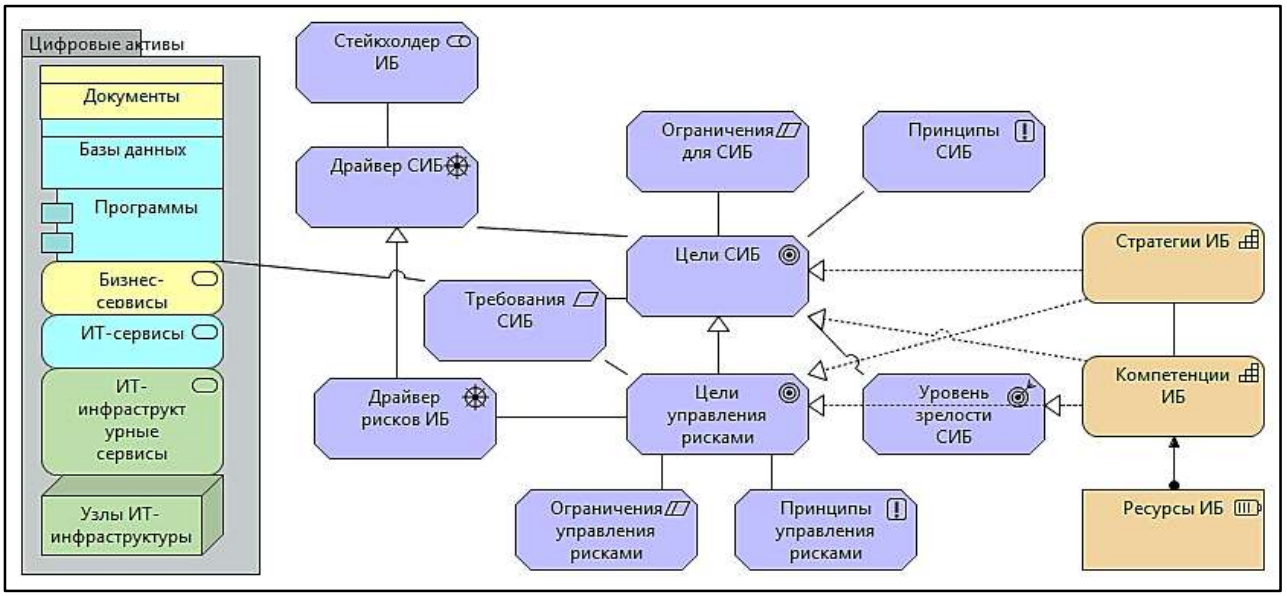


Рисунок 3 – Расширение архитектуры цифрового предприятия

Данная модель расширяется в процессе мониторинга рисков, уточняются значения свойств элементов модели. Портфель ИТ-решений формируется во исполнение поставленных целей СИБ – Рис. 5.

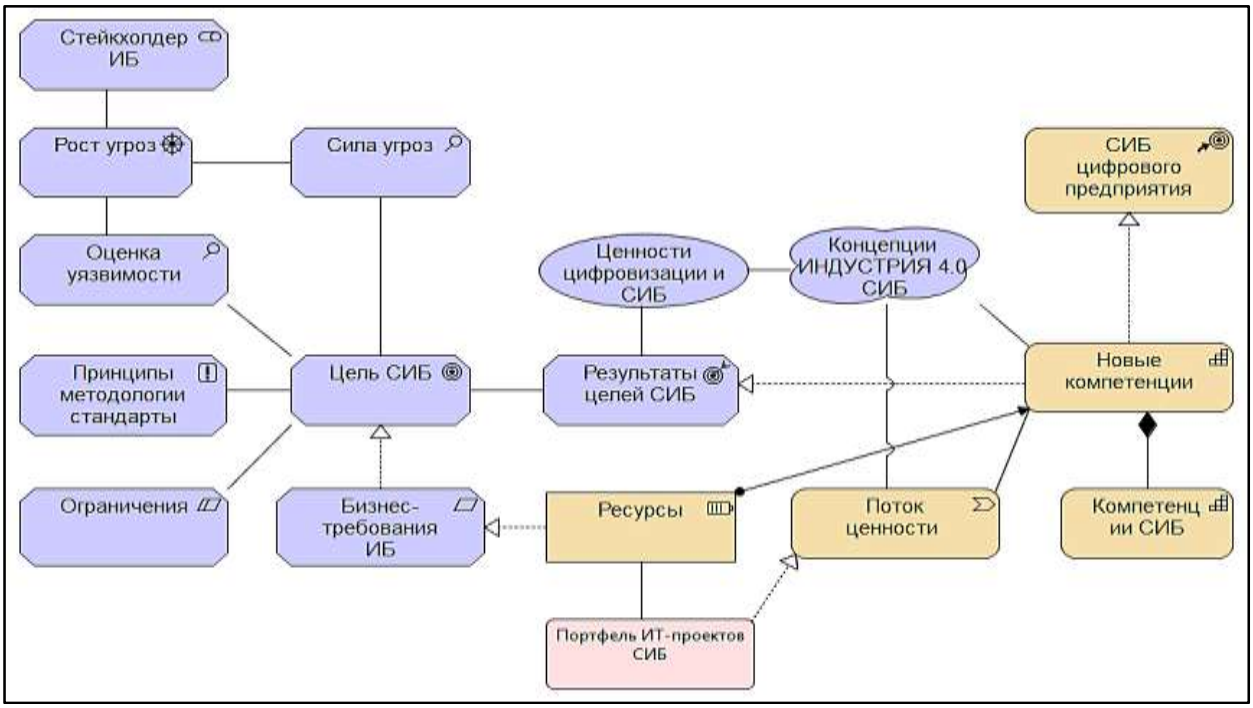


Рисунок 4 – Элементы архитектуры информационной безопасности

Литература

1. Паспорт федерального проекта «Информационная безопасность». [Электронный ресурс]. - URL: https://digital.ac.gov.ru/poleznaya-informaciya/material/Паспорт-федерального-проекта-Информационная-безопасность.pdf (дата обращения: 26.07. 2021).
2. Федеральный проект «Цифровые технологии». [Электронный ресурс]. - URL: // https://digital.ac.gov.ru/about/27/ (дата обращения: 26.07. 2021).
3. O-AA Security Playbook/ [Электронный ресурс]. - URL: https://pubs.opengroup.org/architecture/o-aa-standard/o-aa-security-playbook/index.html (дата обращения: 19.03.2021).
4. «Индустрия 4.0»: создание цифрового предприятия. [Электронный ресурс]. - URL: https://www.pwc.ru/ru/technology/assets/global_industry-2016_rus.pdf (дата обращения: 26.07. 2021).
5. ГОСТ Р ИСО 14258—2008 Национальный стандарт РФ «Промышленные автоматизированные системы. Концепции и правила для моделей предприятия»
6. ГОСТ Р 57100-2016/ISO/IEC/IEEE 42010:2011 Системная и программная инженерия. Описание архитектуры.
7. TOGAF 9.2. [Электронный ресурс]. - URL: https://www.opengroup.org/togaf (дата обращения: 19.03.2021).
8. Ильина О.П., Барабанова М.И. Методология гибкой цифровой трансформации предприятия // В сборнике «Технологическая перспектива в рамках евразийского пространства: новые рынки и точки экономического роста». Санкт-Петербург, 07-08 ноября 2019 г. - С. 223-232.
9. Ильина О.П., Сотавов А.К. Архитектурное моделирование системы информационной безопасности // Журнал «Технико-технологические проблемы сервиса». 2019. №2 (48). - С. 30-37.
10. Ильина О.П. Экосистема цифрового предприятия // В сборнике Цифровая конвергенция в экономике / [В.В. Трофимов и др.]; под ред. В.В. Трофимова, В.Ф. Минакова. СПб.: Изд-во СПбГЭУ, 2019. - С. 54-66.
11. Ильина О.П. Инфо-канва как модель инфокоммуникационного пространства предприятия. // В сборнике Проблемы жизнеспособности хозяйственных систем: к 75-летию победы в Великой Отечественной Войне/ [Т.А.Селищева]; под ред. Т.А. Селищевой. СПб.: Изд-во СПбГЭУ, 2020. - С. 187-196.
12. Ильина О.П. Архитектура системы информационной безопасности // В сборнике: Инновационные технологии и вопросы обеспечения безопасности реальной экономики. Сборник научных трудов по итогам Всероссийской научно-практической конференции. Под редакцией Г.В. Лепеша, О.Д. Угольниковой, С.Ю. Александровой. 2020. - С. 74-87.

УДК 33:614

Кириленко Вадим Владимирович
канд. экон. наук, доцент
Соколова Вера Васильевна
канд. мед. наук, доцент
Санкт-Петербургский государственный
педиатрический медицинский университет

ЭКОНОМИЧЕСКОЕ РАЗВИТИЕ МЕДИЦИНСКИХ ОРГАНИЗАЦИЙ КАК ОСНОВА БЕЗОПАСНОСТИ

Аннотация. В статье проведен анализ деятельности медицинских организаций и выявлены проблемы экономического развития и обеспечения безопасности их деятельности.

Ключевые слова: медицинская организация, экономическое развитие, безопасность.

Kirilenko V.V.
Sokolova V.V.
Saint-Petersburg State Pediatric Medical University

ECONOMIC DEVELOPMENT OF MEDICAL ORGANIZATIONS AS A BASIS OF SAFETY

Annotation. The article analyzes the activities of medical organizations and identifies the problems of economic development and ensuring the safety of their activities.

Keywords: medical organization, economic development, security.

Введение. Общее ухудшение здоровья и населения и низкая эффективность профилактики, лечения и реабилитации создает реальную угрозу будущему развитию страны. Не смотря на многолетнее реформирование такой важнейшей для всего общества отрасли, какой является здравоохранение, проводимые изменения в условиях ограничений ресурсов на реализацию государственной политики в области медицины приводили к накоплению проблем. За двадцатилетний период количество медицинских организаций первичного уровня, особенно в сельской местности, уменьшалось. Не преодолен кадровый голод в высококвалифицированных специалистах, что требует новых подходов и корректировки планов развития в целом отрасли и медицинской организации в частности.

На современном этапе развития государства отрасль здравоохранения и обеспечение безопасности находится в активной стадии изменений,

особое внимание уделяется достижению социально ориентированных результатов взаимодействия государства, медицинских работников и граждан. Государством принимается ряд мер, направленных на повышение качества, доступности медицинской помощи и безопасности населения.

Цель исследования. Разработка комплекса организационно-правовых и медико-экономических мероприятий и рекомендаций, направленных на экономическое развитие медицинских организаций, рациональное планирование и оптимизацию обеспечения безопасности их деятельности.

Материалы и методы. Исследование проводилось на базе ФГБОУ ВО «Санкт- Петербургского государственного педиатрического медицинского университета» Минздрава России. Источники информации: федеральная статистическая отчетность. Сбор и анализ данных затрат медицинских организаций субъектов РФ производился в специализированных информационных ресурсах ТОМС. Накопленные данные используются в ходе разработки и обоснования тарифов в системе ОМС.

Результаты. Реформы системы здравоохранения в России планировались и реализовывались «сверху вниз», что несло ошибочный характер преобразований на уровне медицинской организации в связи с качественно иным уровнем медицинской помощи в конкретной организации. Реформирование системы здравоохранения рекомендуется осуществлять, начиная с первичного звена, путем формирования «эталонных» элементов трехуровневой системы, включающей первичный, межрайонный и городской (региональный) уровни. Планы развития медицинских организаций рекомендуется реализовывать исходя из формирования необходимых для «эталона» условий и ресурсов (финансовых, кадровых, материально-технических, инфраструктурных, информационных и др.), а не выделенные ресурсы подгонять под выполнение задач.

Развитие медицинских организаций характеризуется разнонаправленными тенденциями. С одной стороны, государство все больше вкладывает ресурсов в реализацию программ государственных гарантий медицинской помощи населению, инвестиций в инфраструктуру, санитарно-эпидемическое благополучие и безопасность населения России, повышая доступность медицинской помощи. С другой стороны, экономическая неустойчивость медицинских организаций, в большей степени частных, приводит к сокращению медицинской помощи качественно и количественно.

Доля государственных расходов в размере 3-4% ВВП недостаточна для развития отрасли в целом и медицинской организации в частности. В системе здравоохранения работают более 300 тыс. врачей и около 550 тыс. чел. среднего медицинского персонала. Дефицит в настоящее время

составляет более 25 тыс. врачей и более 130 тыс. В большинстве медицинских организаций медперсонал в возрасте 40-60 лет составляет более 50%, а старше 61 года – около 12%. Хотя система подготовки специалистов-медиков и представлена 47 учреждениями науки, 51 учреждением высшего профессионального образования, 23 специализированными учреждениями самыми дефицитными являются терапевты, хирурги, педиатры, а также специалисты: рентгенологи, эндоскописты, врачи УЗИ и лаборанты.

Анализируя, деятельность первичного звена оказания медицинской помощи следует отметить, что задача экономического развития медицинской организации и безопасности ее деятельности является многоаспектной, требующей учета всех ее составляющих и в первую очередь подготовки и обучения медицинского персонала, разработки и внедрения применяемых передовых медицинских, фармацевтических, информационных и других средств и технологий, а так же выделения согласованных по времени, объему и качеству ресурсов. Среди основных причин, тормозящих развитие медицинской организации выделяются следующие:

- проблемы развития страховой медицины;
- проблемы распределения ресурсов;
- проблемы подготовки и формирования кадров.

Система управления здравоохранением на уровне медицинской организации недостаточно чувствительна к изменениям рыночных условий из – за громоздкости заложенных в модель финансового обеспечения медицинской помощи в различных условиях методик расчетов и рассчитываемых параметров и поправочных коэффициентов.

Проблемы развития системы обязательного и добровольного страхования в России. Система обязательного медицинского страхования не лишена недостатков:

- не удалось компенсировать поступления в фонды ОМС действующими тарифами страховых взносов при снижении финансовых потоков из бюджета;
- расходы на медицинскую помощь работающему и не работающему населению не сбалансированы;
- развитие системы страховой медицины тормозит жесткое регулирование и дублирование функций фондов ОМС и страховых компаний;
- дороговизна системы ОМС (около 17% поступающих в фонды финансовых ресурсов расходуется на обеспечение функционирования самой системы ОМС).

Проанализируем доходы и расходы медицинской организации применительно к сценарию ее развития.

Таблица 1 – Бюджет Федерального фонда ОМС РФ
в период 2014 – 2019 гг., млрд. руб.

Показатели	2013	2014	2015	2016	2017	2018	2019
Доходы	1101,4	1240,1	1619,8	1657,6	1737,2	1887,9	2196,3
Расходы	1048,7	1240,1	1662,8	1590,1	1655,0	1994,1	2267,5
Профицит	52,7	-	-	67,5	82,2	-	-
Дефицит	-	-	43,0	-	-	106,2	71,2

Поступления в Федеральный фонд ОМС РФ свидетельствует о дефиците ресурсов для развития медицинских организаций.

Таблица 2 – Структура расходов медицинской организации
в рамках реализации территориальной программы ОМС
по видам помощи 2013 – 2019 гг., %.

Показатели	2013	2014	2015	2016	2017	2018	2019
Стационарная МП	78,4	75,3	72,0	72,5	71,3	70,8	69,8
МП дневной стационар	0,6	1,1	1,7	1,5	1.8	1,9	2,6
Амбулаторная МП	13,7	18,2	19.7	19,8	20,1	20,2	20,3
Скорая МП (вне МО)	7,3	5,4	6,6	6,2	6,8	7,1	7,3

Только в последние годы ситуация со стационарами стала вправляться, т.к. сокращение стационаров и снижение количества коек отразилось на структуре затрат медицинской организации и не способствовало ее развитию.

Таблица 3 – Структура расходов средств ОМС медицинских организаций
в период 2013 -2019 гг., %.

Показатели	2013	2014	2015	2016	2017	2018	2019
Оплата труда	72,3	74.0	70,7	68,7	66,9	66,7	69,8
Медикаменты	14,1	13,8	15,7	16,1	16,7	16,8	17,1
Питание	2,5	3,3	2,6	2,3	2,5	2,7	2,4
Прочие	11,1	8,9	11,0	12.9	13,9	13,8	10,7

Развитие медицинских организаций предполагает более ускоренные темпы изменений структуры расходов на медикаменты и прочие расходы, включающие расходы на внедрение новых технологий.

План модернизации медицинской организации предполагает проведение комплексной подготовки, включающей:

- разработку нормативных и методических документов;
- подготовка проектно-сметной документации;
- подготовка основного и вспомогательного персонала для работы на закупаемом оборудовании;
- подготовка и привлечение персонала для работы в регионах;
- подготовка и проведение аукционов на выполнение проектно-сметной документации и проведение работ;
- подготовка и проведение процедур закупки и установки оборудования;
- сервисное обслуживание и ремонт оборудования.

Сценарий развития медицинской организации не может реализовываться в условиях, когда финансовые ресурсы расходуются не пропорционально целям разработки и внедрения новых технологий, когда значительные затраты осуществляются на оплату труда (см. таблицу 4).

Для медицинских организаций 2-го уровня оказания медицинской помощи доля расходов на диагностику и другие параклинические исследования составила около 27%, а для медицинских организаций 3-го уровня расходы достигают 36%. Разработка и освоение новых технологий с использованием современного оборудования уменьшает долю заработной платы в общем объеме затрат медицинской организации и соответственно увеличивает вес затрат на медикаменты и имущественный комплекс, увеличиваются так же прочие расходы, связанные с дополнительным обучением персонала, сервисным обслуживанием и приобретением расходных материалов.

Таблица 4 – Пропорции распределения заработанных медицинской организацией финансовых средств в 2019 г., %.

Условия предоставления МП, уровни медицинских организаций	Оплата труда	Медикаменты	Питание	Прочие
В амбулаторных условиях				
- I уровня	63,0 - 82,1	4,3 – 7.4	-	10,5 – 32,7
- II уровня	68,5 -78,5	2,4 – 7,4	-	18,2 – 23,2
- III уровня	64.2 -74,2	5,0 -10,0	-	19,7 – 24,7

Окончание табл. 4

Условия предоставления МП, уровни медицинских организаций	Оплата труда	Медикаменты	Питание	Прочие
В условиях дневного стационара				
- I уровня	56,4 - 66,4	16,0 – 21,0	-	17,6 – 22,6
- II уровня	40,5 - 50,5	26,2 – 31,2	-	23,3 – 28,3
- III уровня	35,4 - 45,4	30,2 – 35,2	-	24,4 – 29,4
В условиях круглосуточного стационара				
- I уровня	59,8 - 69,8	13,1 – 18,0	2,4 – 6,5	12,7 – 15,7
- II уровня	55,6 - 65,6	20,5 – 25,5	4,3 – 6,3	9,6 – 12,6
- III уровня	53,9 - 63,9	22,0 – 27,0	4,1 – 6.1	10,0 – 13,0
Вне медицинской организации				
Скорая медицинская помощь	72.0 - 82,0	3,0 – 8,0		15,0 – 20,0

Проблемы распределения ресурсов. Математическое описание многочисленных параметров, коэффициенты, в конечном итоге определяющие размеры оплаты медицинских услуг оказываемых медицинской организацией, основано на объединении заболеваний в клинико-статистические группы (КСГ) и суммировании затрат на лечение. Но чем больше мы вводим в свои расчеты те или иные коэффициенты для учета разнообразных условий и особенностей оказания медицинской помощи, тем менее чувствительной и восприимчивой к меняющимся условиям становится выстроенная система т.к. выше указанные правила влияют разнонаправлено на динамику увеличения базовой ставки оплаты по КСГ. Ежегодный пересмотр объемов финансирования, базовой ставки для оплаты медицинских услуг не делает систему финансового обеспечения и всю систему управления здравоохранением на уровне медицинской организации более управляемой и гибкой.

Определение оптимального соотношения затрат медицинской организации с дифференциацией по уровням оказания медицинской помощи способствует формированию гибкого подхода к финансированию медицинской организации, а предоставление руководству медицинской организации определенной свободы в распределении и трате на наиболее острые текущие потребности будет способствовать ее развитию за счет своевременного перераспределения имеющихся ресурсов и удовлетворения необходимых потребностей развития.

Данное предложение не нарушает принцип «нейтральности бюджета» и не входит в противоречие с действующими методиками расчета

оплаты оказанных медицинских услуг, т.к. предоставляет большую свободу в перераспределении уже заработанных (выделенных) медицинской организацией финансовых ресурсов.

Проводимое исследование выявило методологическую проблему по установлению единых подходов к формированию и реализации учетной политики в медицинских организациях для получения сопоставимых данных. На региональном уровне требуется увязка медицинских информационных систем с системами учета фактических затрат медицинской организации.

Проблемы подготовки и формирования кадров. Развитие медицинских организаций предполагает разработку и внедрение в повседневную деятельность медицинской организации опытных методик и новых технологий, которые не могут быть реализованы без подготовленных специалистов.

Среди основных требований, предъявляемых к выпускникам ВУЗов, выделяют высокий уровень владения иностранными языками, продвинутый уровень пользования программным обеспечением и прикладными программами, опыт работы.

Поэтому несмотря на то, что нет прямой зависимости между затратами на обучение и качеством образования существует необходимость в выработке новых подходов к системе подготовки медицинских кадров. Развитие медицинских организаций невозможно без трансформации исследований в опытные разработки и их перенос и реализацию в здоровье сберегающие технологии, требующих участия в этом процессе помимо медицинских специалистов и инженеров, конструкторов, технологов, программистов и др.

Необходимость преодоления кадрового голода в первую очередь ощущается в первичном звене, а потребности в высококлассных специалистах растут стремительными темпами, что требует пересмотра подходов к кадровому потенциалу отрасли.

Решение проблемы дефицита врачей, среднего и младшего персонала, коэффициент совместительства которых варьировался от 1,5 до 2.0 ставок, путем замены и пересмотра нормативов труда медицинского персонала в целях сокращения штата и интенсификации труда приводил к несоразмерному увеличению нагрузки по отношению к физическим возможностям персонала по обеспечению необходимых мер безопасности и качеству оказываемой медицинской помощи, что в реальности приводило к снижению оплаты труда и увольнению персонала.

Дополнительной мотивацией молодежи к научной деятельности будет формирование системы по реализации научных и творческих идей у молодых исследователей в России, что в первую очередь требует замены скопированной Западной системы выкачивания передовых идей и денег из умов и карманов российских ученых (т.к. признание и финансирование за рубежом) на национально ориентированную систему подготовки научных кадров.

Выводы:

1. С целью реализации государственной политики в сфере здравоохранения и для повышения гибкости и восприимчивости системы управления здравоохранением на уровне медицинских организаций предлагается устанавливать пропорции целевого распределения в расходовании заработанных медицинской организацией финансовых средств, что позволит решать проблемы путем своевременного перераспределения имеющиеся ресурсов.
2. Преодоление дефицита финансовых ресурсов в системе ОМС возможно при значительном увеличении оплаты труда работающего населения с одновременным увеличением отчислений работодателя из фонда оплаты труда.
3. Решение проблем подготовки кадров возможно путем дополнения подпрограммы «Развитие кадровых ресурсов в здравоохранении» формированием системы государственной поддержки и взращивания высококвалифицированных специалистов для подготовки медицинских кадров мирового уровня первичного звена оказания медицинской помощи населению.
4. Создание условий мотивации молодежи к формированию качеств научного исследователя и педагога.
5. Создание условий для реализации научных идей в России.

Литература

1. Российское агентство медико-социальной информации. [Электронный ресурс]. – URL: http://riaami.ru/read/13077
2. Единая межведомственная информационно-статистическая система. [Электронный ресурс]. – URL: http://www.fedstat.ru/indicators/start.do
3. Федеральная служба государственной статистики. Регионы России. Социальноэкономические показатели. [Электронный ресурс]. – URL: http://www.gks.ru/bgd/regl/b13_14p/Main.htm

УДК 656.09

Кропива Ирина Анатольевна
заведующий отделением колледжа бизнеса и технологий
Лунева Светлана Курусовна
старший преподаватель
Санкт-Петербургский государственный
экономический университет

ВОПРОСЫ ЭФФЕКТИВНОСТИ И БЕЗОПАСНОСТИ ДЕЯТЕЛЬНОСТИ ЛОГИСТИЧЕСКИХ ОРГАНИЗАЦИЙ В СОВРЕМЕННЫХ УСЛОВИЯХ

Аннотация. Целью работы является исследование ключевых показателей эффективности деятельности логистической системы, требований, предъявляемых к ней, вопросов совершенствования деятельности логистических систем организаций. В статье представлены основные элементы системы безопасности логистических систем, приводятся примеры современных информационных систем, нашедших широкое применение в логистических системах, рассмотрен опыт их применения, преимущества и возможности. Предложены рекомендации по повышению безопасности и эффективности функционирования логистических систем.

Ключевые слова: безопасность, эффективность деятельности, логистическая система, показатели эффективности логистической системы, элементы логистической системы.

Kropiva I.A.
Head Department of the College of Business and Technology
St. Petersburg State Economic University
Luneva S.K.
St. Petersburg State Economic University

ISSUES OF EFFICIENCY AND SAFETY OF THE ACTIVITIES OF LOGISTIC ORGANIZATIONS IN MODERN CONDITIONS

Annotation. The purpose of the work is to study the key performance indicators of the logistics system, the requirements for it, the issues of improving the activities of the logistics systems of organizations. The article presents the main elements of the security system of logistics systems, provides examples of modern information systems that have found wide application in logistics systems, considers the experience of their application, advantages and capabilities.

Recommendations for improving the safety and efficiency of the functioning of logistics systems are proposed.

Keywords: safety, operational efficiency, logistics system, indicators of the efficiency of the logistics system, elements of the logistics system.

В настоящее время от управления цепями поставок материальных ресурсов зависит эффективность деятельности организаций, поэтому вопросам логистики уделяется особое внимание. Широкое использование логистических систем дает возможность снизить затраты организаций, повысить ее конкурентоспособность. В настоящее время конкурентоспособность российских организаций остается невысокой, что объясняется не только технологическими проблемами, но и низкой эффективностью управления ресурсами, финансовыми и материальными потоками.

Для повышения конкурентоспособности российских организаций и экономики РФ в целом необходимо использовать имеющийся практический опыт зарубежных организаций с внедрением современных технологий.

Вопросы совершенствования функционирования логистических систем являются актуальными, вследствие чего необходимо определение комплекса индикаторов, характеризующих состояние логистической системы организации.

Для оценки эффективности логистической системы используют следующие показатели или индикаторы (Рис. 1) [1].

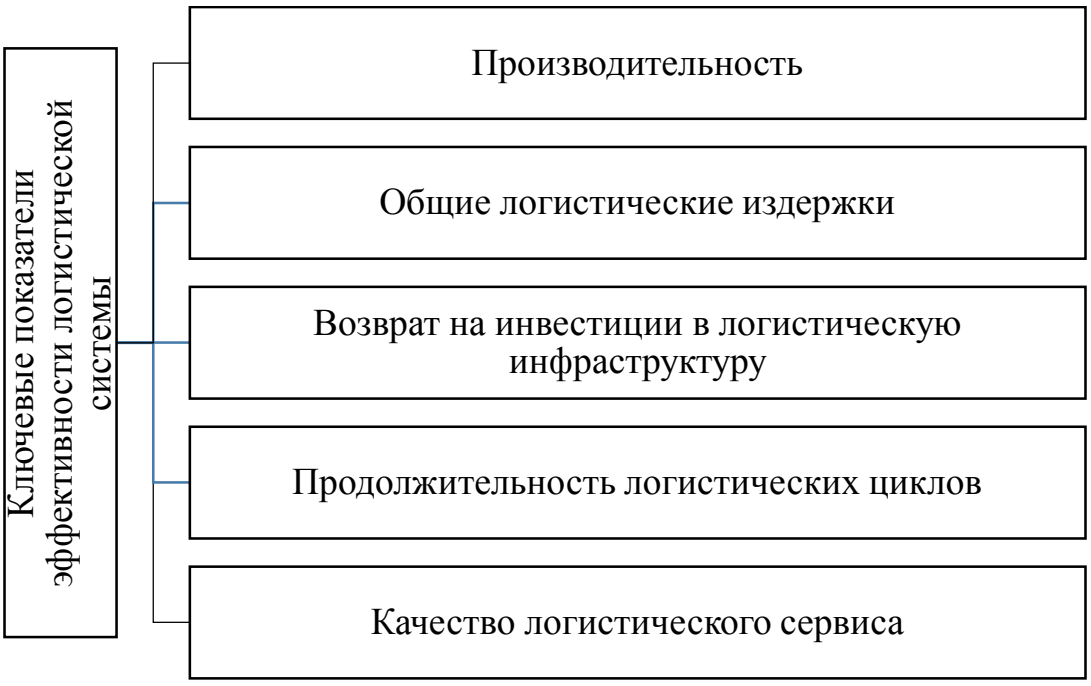


Рисунок 1 - Основные ключевые показатели эффективности логистической системы

В работе Д. Шехтера эффективность логистической системы определяется как «показатель (или система показателей), характеризующий уровень качества функционирования логистической системы при заданном уровне общих логистических затрат» [2].

В исследованиях Ю.М Неруша и А.Ю. Неруша показатель эффективность логистической системы представлен зависимостью от издержек и уровня организации «процессов снабжения, управления товарным рынком, производства и сбыта, включая и послепродажное обслуживание» [3].

По мнению К.С. Кривякина эффективность логистической системы выражается в показателе достижения уровня качества при оптимальном использовании всех имеющихся ресурсов, снижением запасов с оперативным и гибким функционированием предприятия с минимальным уровнем затрат [4].

Логистические системы, внедряемые на предприятиях, оцениваются по ее эффективности в соответствии с поставленной и достигнутой целью. Проблемы несовершенства организации логистической системы может привести к неритмичной работе или сбою в работе всего предприятия.

Для эффективной деятельности организации необходимо удовлетворение «логистической системы требованиям по оперативности и надежности сбора информационных данных по взаимодействию средств производства с транспортными средствами и наличию информационной системы поддержки принимаемых решений», охватывающей всех участников производственной деятельности [1].

Возникающие риски, в том числе в связи с глобальной проблемой распространения болезни современности - COVID-2019, стали импульсом для более широкого внедрения и применения информационных технологий, современных средств коммуникации и взаимодействия.

Своевременное обеспечение организации материально – техническими ресурсами достигается благодаря информационной логистической системе, что в итоге способствует качественному управлению поступающими ресурсами, что особенно важно для систем, работающих синхронно или для систем, работающих «Точно в срок». Логистическая система, отслеживая поступающие материальные ресурсы, анализирует имеющиеся запасы, что повышает эффективность управления запасами организации. Получение оперативной информации о движении материальных ресурсов дает возможность провести замену реальных запасов информационными потоками, приводя к уменьшению затрат.

Обмен информационными данными между поставщиками и транспортными компаниями дает возможность уменьшения расходов, обусловленных обеспечением функционирования логистической цепи, что способствует снижению затрат организации – производителю продукции [3].

Основной составляющей человеческой жизни в области логистики является грамотное и рациональное управление ресурсами с целью снижения затрат и времени на доставку исходного материала и продукции. Поэтому, это естественно, что в любую сферу деятельности внедряются новые технологии, непосредственно связанные с информационными ресурсами.

Наибольшее распространение в России получила программа WMS (Warehouse Management System). Впервые об этой системе заговорили в конце 90-х годов, в связи с экономическим кризисом и ростом курса доллара. В начале 2000-х, российские производителе начали изучать и перенимать опыт работы зарубежных фирм, что и привело к появлению на российском рынке одной из наиболее востребованных и в наши дни программы WMS.

В информационной логистической технологии WMS (Warehouse Management System) используются следующие ключевые компоненты (Рис. 2).

Рисунок 2 – Ключевые компоненты WMS (Warehouse Management System)

Основным задачами, решаемыми при использовании программы WMS, является значительное увеличение продуктивности, ускорения рабочего процесса, повышение производительности компании и не менее важное - обеспечение приема на склад с низким количеством ошибок.

Программа EDI (Electronic Data Interchange) используется для оперативности транспортировки грузов. Данная программа позволяет объединить и автоматизировать все этапы документирования, связанными с программным обеспечением и активными приложениями.

Программа EDI помогает стандартизировать и автоматизировать обмен коммерческой цифровой информацией, с возможностью оперативного программного взаимодействия компьютерных систем, разработанных на различных платформах. В России эта программа находится на первоначальном этапе, и, возможно, в недалеком будущем, сможет занять одно из главенствующих мест на рынке программных продуктов для транспортных компаний, финансового сектора, промышленности и топливно-энергетического комплекса, дистрибуции и ритейла.

Одной из важных проблем являются вопросы обеспечения безопасности. Система безопасности логистических процессов представляет совокупность технических решений и организационных мероприятий, направленных на превентивной анализ рисков с возможностью предотвращения и минимизации ущерба с целью обеспечения эффективности деятельности организации.

Большое количество участников логистической системы, заинтересованных в безопасности определенных участков логистической системы, нередко приводит к размыванию зон ответственности между участниками обеспечения безопасности системы, что может привести к неблагоприятным последствиям. В этой ситуации необходимо согласование принципов обеспечения безопасности и создание условий защищённости от внешних и внутренних угроз.

Эффективная и безопасная работа логистической системы организации предполагает создание организационных мероприятий с принятием технических решений, дающих возможность выявления и устранения факторов, дестабилизирующих экономические показатели деятельности. В современной России проблемы обеспечения безопасности логистических систем решается осуществлением контроля над последствиями случившихся рисков, с компенсацией убытков, но не устранением причин; или поэтапным контролем за факторами риска, что снижает последствия или минимизирует риск [6].

В настоящее время создаются «предпосылки для комплексного применения SCM (Supply Chain Management) - управление цепочками поставок» [6]. При помощи данных систем успешно решаются задачи «автома-

тизации и управления всеми этапами снабжения предприятия и контроля товародвижения» [6].

Также можно выделить «CALS-технологии (Continuous Acquisition and Lifecycle Support), решающие вопросы непрерывной информационной поддержки поставок и жизненного цикла изделий» [6].

Внедрение данных технологий интегрированной логистики дает возможность объединения всех этапов, что повышает эффективность и безопасность логистической системы.

Для решения вопросов безопасности необходимо системное рассмотрение логистических систем, состав подсистем и возможности влияния структурных компонентов на функционирование всей системы, на ее безопасность. Можно выделить основные элементы системы безопасности (Рис. 3).

Рисунок 3 – Основные элементы системы безопасности логистических систем [5]

Каждый элемент логистической системы решает определённые задачи обеспечения безопасности, что в совокупности способствует каче-

ственному обеспечению безопасности логистической системы. Наряду с данными элементами безопасности в настоящее время также рассматриваются такие сферы безопасности, как экологическая, техногенная, научно – техническая и др.

Повышение безопасности логистической системы достигается созданием общей концепции безопасности, предусматривающей постановку целей и задач перед каждым участником и элементом системы. Функционирование логистической системы должно быть на принципах эффективности, непрерывности, безопасности, законности, координации действий и др. Каждый элемент подсистемы обладает определенными объектами (рис.3), которые могут быть ранжированы по их значимости, и в отношении которых необходимо предусмотреть и выявить риски и угрозы с построением матрицы безопасности. Ранжирование объектов может производиться на основе экспертной оценки. Матрица безопасности представляет взаимосвязь объектов с необходимыми решениями по защите и предотвращению рисков.

Построение логистической системы необходимо осуществлять с учетом снижения рисков и угроз. Основной задачей, решаемой логистической системой, является повышение эффективности и безопасности, что свидетельствует о результативности функционирования логистической системы.

Одним из основных элементов исследования экономической безопасности действующего предприятия является выбор критериев, на основании которых формируется представление о настоящем положении и уровне экономической безопасности по финансовой устойчивости, ликвидности и безубыточности предприятия.

Для определения количественной оценки, чаще всего применяют индикаторный подход, вследствие которого используются пороговые значения показателей, которые характеризуют деятельность предприятия в его различных функциональных областях с соответствующим уровнем экономической безопасности.

На основе оценки состояния использования корпоративных ресурсов, уровень экономической безопасности предприятия проводится в соответствии с ресурсно-функциональным подходом факторов бизнеса, используемых владельцами и менеджерами [7].

Разработка мероприятий и решение технических задач обеспечения экономической безопасности организаций, является одной из приоритетных задач каждого предприятия. В связи с существованием внешних и внутренних угроз, любое предприятие должно быть готово к принятию продуманных, адекватных решений, в противном случае, может привести к ослаблению экономической безопасности и уязвимости во многих аспектах.

Проблема экономической безопасности требует комплексного подхода в решении и является достаточно сложной задачей. Поэтому, в логистической компании любой сферы деятельности, необходима тщательная теоретическая проработка вопроса экономической безопасности, понимание сущности и рисков.

Для эффективной деятельности предприятий необходимо проводить мониторинг и прогнозирование угроз, уделять внимание разработке инструментов и механизмов снижения рисков для поддержания стабильного и устойчивого развития предприятия в изменяющихся условиях, постоянно совершенствуя механизм обеспечения экономической безопасности.

Современные условия требуют использования более новых инновационных решений в том числе и в логистических системах. Одним из методов является внедрение современных цифровых технологий, позволяющих отслеживать цепи поставок от начального этапа до конечного этапа – потребителю. Цифровые технологии позволяют оптимизировать логистические потоки и маршруты, повышать эффективность использования активов логистических компаний, что способствует снижению затрат и росту эффективности.

Литература

1. Данильченко М.А., Черноголовая К.И. Ключевые показатели эффективности логистики //Актуальные вопросы экономических наук, 2015. [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n
2. Шехтер Д. Логистика. Искусство управления цепочками поставок. М.: Альпина, 2013. 452 с.
3. Неруш Ю.М., Неруш А.Ю. Логистика: учебник для академического бакалавриата. 5-е изд., перераб. и доп. М.: Издательство Юрайт, 2016. 559 с.
4. Кривякин К.С. Механизм повышения эффективности организации логистической деятельности предприятия // Организатор производства. 2018. Т.26. №4. С. 77-89. DOI: 10.25987/VSTU.2018.68.55.007
5. Коломиец Б.Н., Кукарцев В. В., Особенности применения современных информационных технологий для оптимизации логистических процессов. Технические науки №31-1, 10.02.2015
6. Кузнецова Ю.Л., Ипатьева, И.А. Обеспечение безопасности логистической системы: проблемы и решения. Торгово-экономический журнал, 3(2), 163-172. doi: 10.18334/tezh.3.2.35407
7. Дмитриев А.В. Цифровые технологии прослеживаемости грузов в транспортно-логистических системах // Стратегические решения и риск-менеджмент. 2019. Т. 10. №1. С. 20-26. DOI: 10.17747/2618-947X-2019-1-20-26

УДК 331.453

Круглов Дмитрий Валерьевич
д-р экон. наук, профессор
Александрова Светлана Юрьевна
канд. экон. наук, доцент
Санкт-Петербургский государственный
экономический университет

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ТРУДА В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБЩЕСТВА

Аннотация. В статье рассматриваются воздействия неблагоприятных факторов на трудовые ресурсы, приводящие к сокращению объема валового внутреннего продукта. Политика государства в настоящее время не в полной мере способствует комплексному подходу к решаемым задачам в области охраны труда. К сожалению, и ситуация с травматизмом на производстве остается напряженной. Качество трудовой жизни можно изменить как в худшую, так и в лучшую сторону. Характерным примером может служить обучение сотрудников, движение по карьерной лестнице, повышение безопасности труда и т.д. В конечном итоге, за счет развития трудового потенциала на предприятии поддерживается высокая производительность труда и растет прибыль. Качество трудовой жизни, характеризуется еще и такими показателями как экологичность и безопасность. Внедрению цифровых технологий должны способствовать не только новые программные продукты на рынке, но и меры налоговой политики, стимулирующие внедрение и использование «чистых» энергосберегающих технологий. Для этого следует применять экономические рычаги, способствующие цифровизации сферы охраны труда.

Ключевые слова: неблагоприятные факторы, рынок труда, трудовые ресурсы, политика, безопасность, цифровизация, технологии.

Kruglov D.V.
Aleksandrova S.Y.
St. Petersburg State Economic University

ENSURING LABOR SAFETY IN THE CONDITIONS OF THE DIGITAL TRANSFORMATION OF SOCIETY

Annotation. The article examines the impact of unfavorable factors on labor resources, leading to a reduction in the volume of gross domestic prod-

uct. State policy at the present time does not fully contribute to an integrated approach to the tasks being solved in the field of labor protection. Unfortunately, the situation with industrial injuries remains tense. The quality of working life can be changed both for the worse and for the better. A typical example is training employees, moving up the career ladder, improving labor safety, etc. Ultimately, due to the development of labor potential, the enterprise maintains high labor productivity and increases profits. The quality of working life is also characterized by such indicators as environmental friendliness and safety. The introduction of digital technologies should be facilitated not only by new software products on the market, but also by tax policy measures that stimulate the introduction and use of "clean" energy-saving technologies. For this, economic levers should be used that contribute to the digitalization of the labor protection sphere.

Keywords: unfavorable factors, labor market, labor resources, politics, safety, digitalization, technologies.

Влияние на экономику любого региона России, безусловно оказывает состояние системы охраны труда. Воздействие неблагоприятных факторов, во-первых, снижает трудовой ресурс по причине профессиональных заболеваний и травматизма, что в дальнейшем приводит к сокращению объема валового внутреннего продукта. Во-вторых, на возмещение вреда пострадавшим отводится часть произведенного валового внутреннего продукта. В этой связи, поиск новых подходов управлению безопасностью труда в современных условиях, как на региональном, так и на федеральном уровнях обусловлен цифровой трансформацией общества. Политика государства в настоящее время не в полной мере обеспечивает комплексный подход к решаемым задачам в области охраны труда. В последние годы наблюдается снижение травм со смертельным исходом. По оперативным данным Роструда, наибольшее количество травм, как и в 2019 году зафиксировано в ЦФО (Центральном Федеральном Округе) (Рисунок 1,2), далее идет ПФО (Приволжский Федеральный Округ), СФО (Сибирский Федеральный Округ) и ДФО (Дальневосточный Федеральный Округ) [4].

В этой связи, одним их ключевых вопросов обеспечения качества трудовой жизни на предприятиях России, является удовлетворенность трудовой деятельностью. Качество трудовой жизни - это деятельность, направленная на предоставление возможностей индивиду развивать свои творческие способности и использовать их в процессе содержательного труда [1]. Основой концепции КТЖ (качества трудовой жизни) является рациональное использования трудового потенциала индивида.

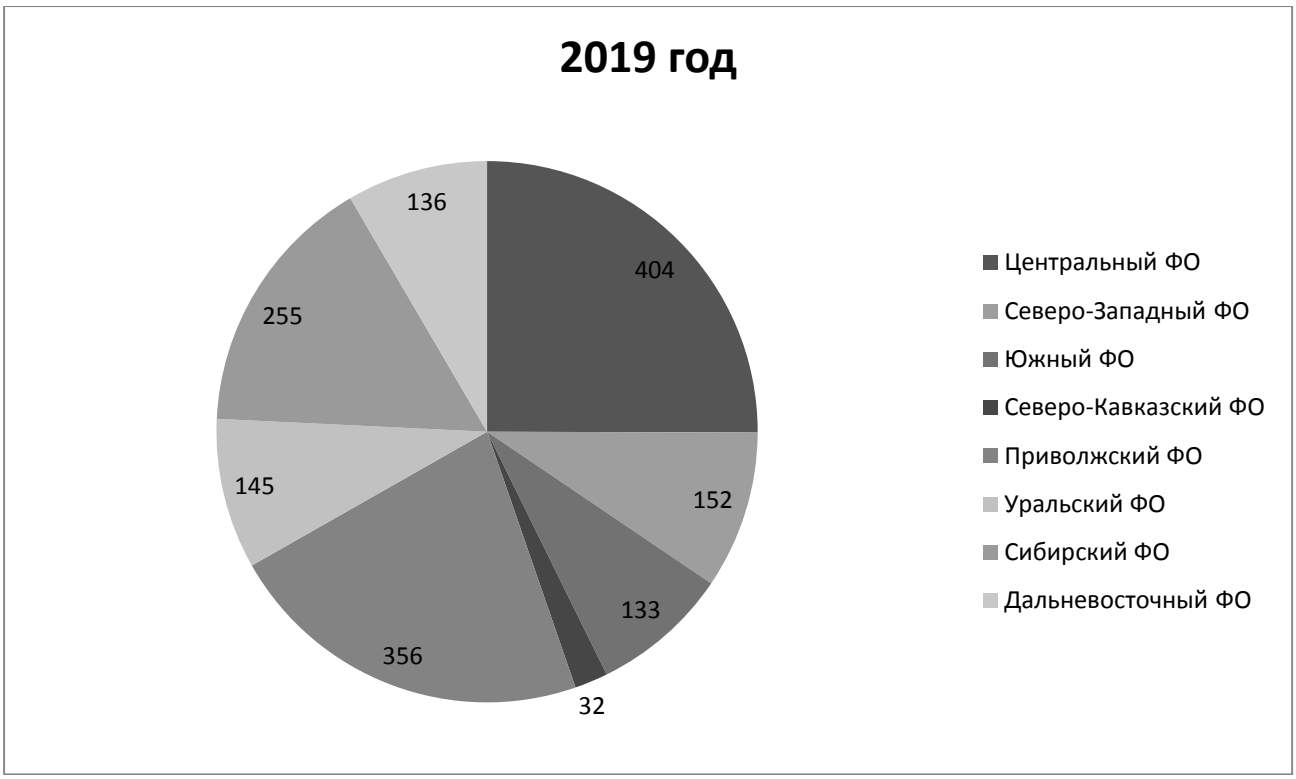


Рисунок 1 – Показатели производственного травматизма
со смертельным исходом по Федеральным Округам в 2019 году

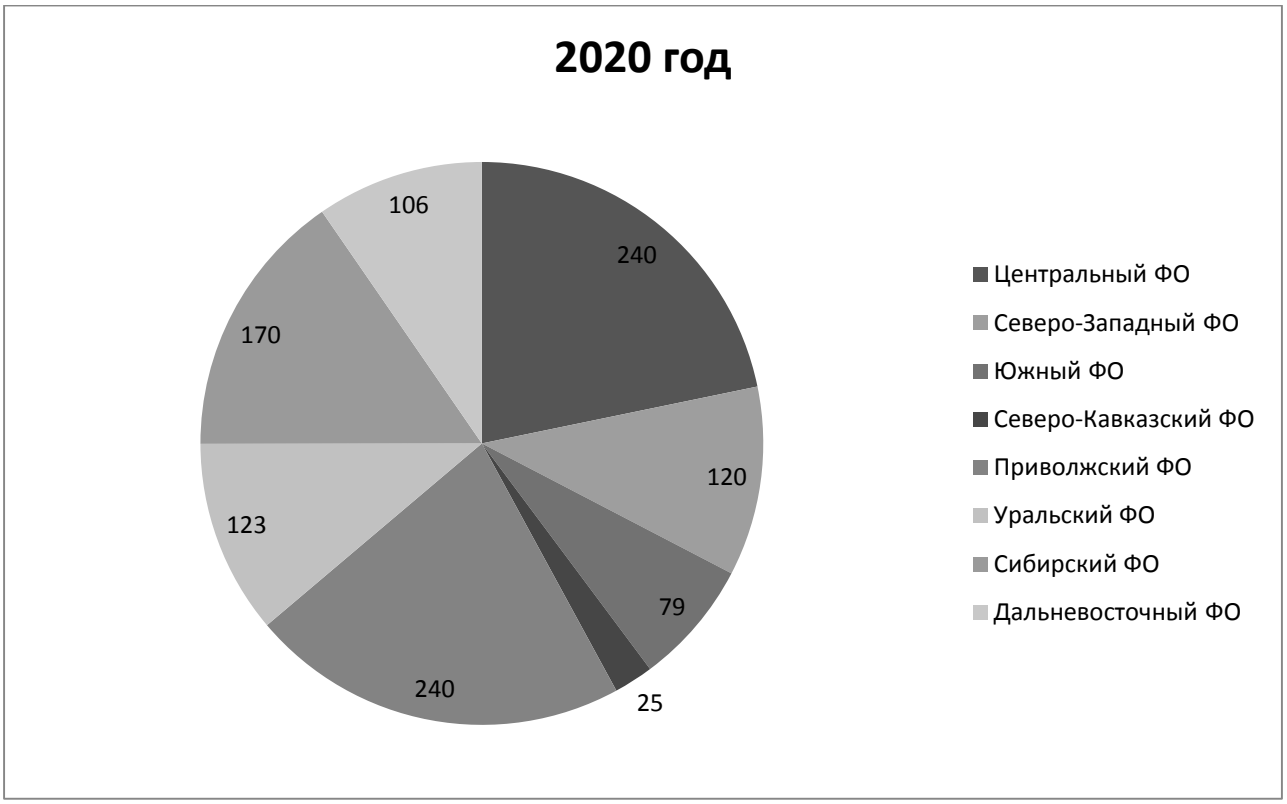


Рисунок 2 – Показатели производственного травматизма
со смертельным исходом по Федеральным Округам в 2020 году

Показатель КТЖ можно изменить как в худшую, так и в лучшую сторону. Характерным примером может служить обучение сотрудников, движение по карьерной лестнице, повышение безопасности труда и т.д. В конечном итоге, за счет развития трудового потенциала на предприятии поддерживается высокая производительность труда и растет прибыль. КТЖ характеризуется еще и такими показателями как экологичность и безопасность. Эти показатели и проблемы, которые с ними связаны, играют важную роль в концепции трудовой жизни. В дефиницию «условия труда» вложен большой смысл от вопросов, связанных с нормативно-правовым регулированием до психофизиологии трудовой деятельности. Данные факторы необходимо учитывать с целью повышения эффективности трудового процесса. Безусловно, в современных условиях в КТЖ включены и психофизиологические аспекты. В частности, это проблемы связанные с техникой наказаний и поощрений, а также с состоянием трудовой дисциплины на производстве. Для отечественной экономики характерен высокий удельный вес добывающих производств. Они являются наиболее травмоопасными. Не обошли стороной сферу охраны труда и мировые кризисные явления, связанные с пандемией коронавируса [3]. В этой связи, проблема безопасности труда в настоящее время становится более актуальной.

По данным Росстата за 2020 год, было зафиксировано 3,494 тысяч профессиональных заболеваний (Рисунок 3) и 28,7 тысяч несчастных случаев на производстве [5].

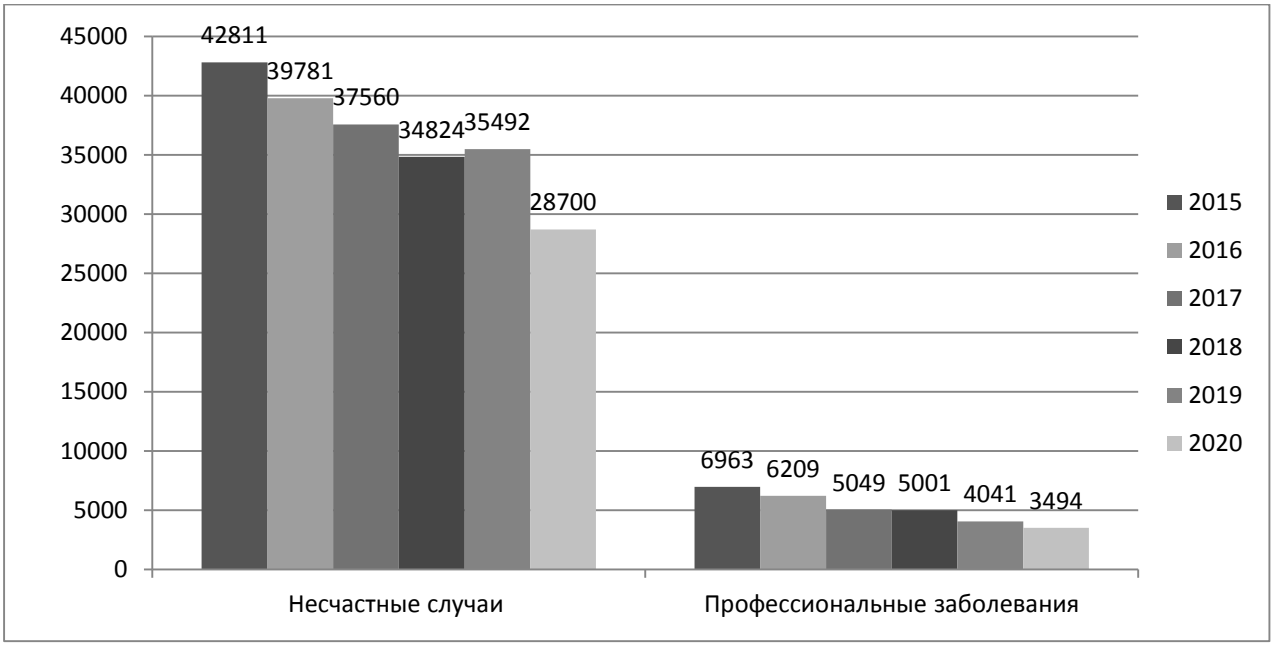


Рисунок 3 – Профессиональные заболевания и производственный травматизм за период 2015-2020 гг.
Составлен авторами по материалам [5].

Данные Роструда говорят о том, что 1,137 тысяч случаев были со смертельным исходом (Рисунок 4), среди которых 52 женщины [4].

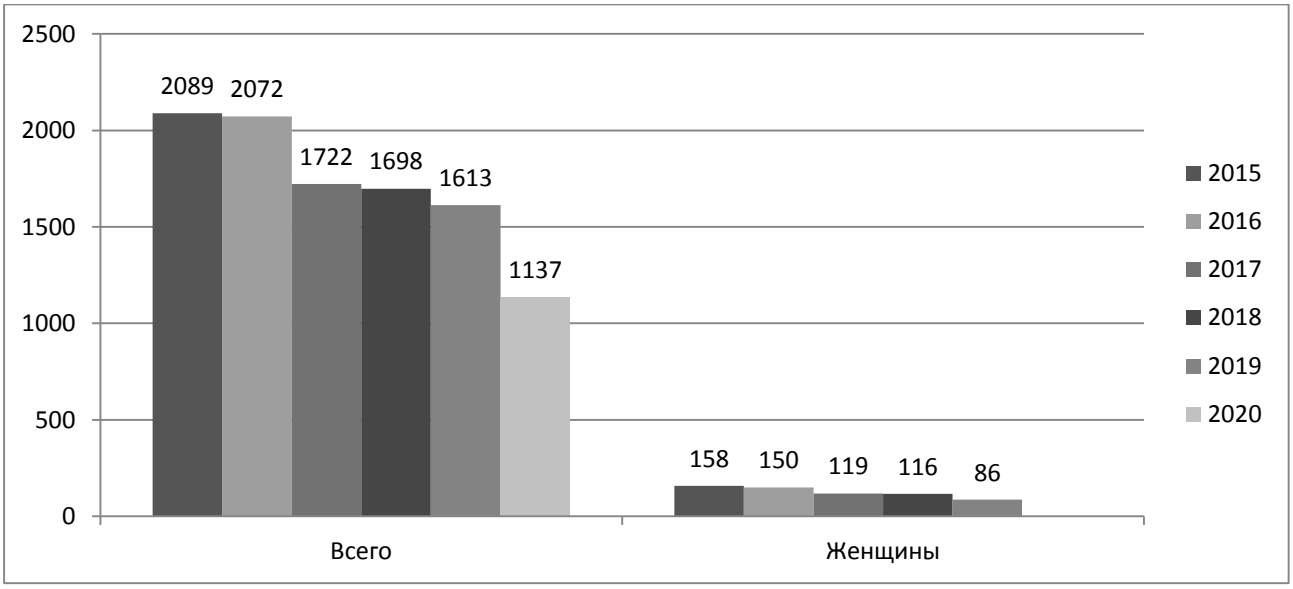


Рисунок 4 – Данные по производственному травматизму со смертельным исходом за период 2015 -2020 гг.

В настоящее время, информация становится важнейшим ресурсом развития экономики. В этой связи, цифровизация сфер деятельности не может не затронуть сферу охраны труда. Министерство труда планирует использовать цифровые технологии в данной сегменте. Совсем недавно Минтруд запустил проект по внедрению digital-технологий в области охраны труда. В министерстве разработали программу по переводу документов в сфере труда в электронную форму. В тестовом режиме проводится работа со следующими документами:

- допуск к работе;
- состав заработной платы работника;
- документы, связанные с командировками и отпусками;
- трудовые договоры;
- учет рабочего времени.
- К сфере охраны труда предъявляется ряд требований, которые можно разделить на 4 подгруппы:
- контроль за здоровьем работников;
- обучение работников;
- документооборот в области охраны труда;
- контроль за безопасными условиями труда.

В данных подгруппах имеются как положительные, так и отрицательные моменты. С помощью системы контроля невозможно в полной

мере наблюдать за экологическими и производственными процессами на самых травмоопасных участках. Традиционный документооборот на бумажных носителях отвлекает руководителей от контроля, за выполнением поставленных задач. Негативным моментом обучения сотрудников является то, что зачастую процесс обучения по охране труда сводится к приобретению удостоверения. Исходя из этого, с сфере охраны труда в рамках цифровизации экономики необходимо дать право работодателям осуществлять видео и аудио фиксацию в ходе процесса производства, а также осуществлять хранение этой информации на добровольной основе [2]. Доступным и объективным станет контроль в сфере охраны труда по следующим направлениям:

- дистанционный контроль с возможностью надзора контролируемых органов;
- на базе дистанционного контроля, увеличение периодичности оценки условий труда на отдельных участках;
- выявление производственных участков с вредными условиями труда.

Для обучения работников по охране труда современным требованиям в этой области, создается государственный ресурс, позволяющий дистанционно оценивать знания обучающихся по итогам обучения. Обучающие материалы будут размещены на данном портале, где специалист в любое время и с любого устройства сможет с ними ознакомиться. По завершении курса, обучаемый самостоятельно проходит тесты и получает удостоверение с ID кодом.

Динамика показателей в сфере экологии говорит об увеличении негативного воздействия предприятий на окружающую среду. Подъем экономики на фоне такого уровня выбросов, может отрицательно сказаться не только на экологии в целом, но и на рабочих местах в частности. Прогноз основных опасностей и угроз свидетельствует, что с обеднением кадрового состава на производствах сохраняется высокая степень риска возникновения крупных аварий и катастроф. В конечном итоге это будет приводить к конфликтным ситуациям между инженерами и менеджерами на предприятиях. Инженеру необходимо качественная и бесперебойная работа всех систем и механизмов, а менеджеру получаемая прибыль.

Исходя из этого, основой современной институциональной политики должна стать новая система регулирования в сфере экологии. Успешная реализация программы цифрового развития России, является большим вкладом в сохранение экологического потенциала. За последнее время в нашей стране резко вырос спрос на цифровые технологии в сфере охраны труда.

По охране труда в 2021 году разработан законопроект «Об обязательном прогнозировании несчастных случаев». Также, стали действовать 38 новых правил, связанных с охраной труда. Для соблюдения требований в сфере охраны труда, промышленной безопасности и экологии (ОТПБЭ), необходимы цифровые инструменты современного уровня. В компании «Инфосистемы джет» разработали систему цифровых решений в сфере охраны труда работников и промышленной безопасности. С помощью представленного программного продукта «Jet HSE» осуществляется автоматизированный сбор и контроль нарушений ОТПБЭ [6]. В состав комплекса Jet HSE входит десять подсистем. Учетная система, входящая в структуру ОТПБЭ, состоит из 22 модулей и ситуационного центра.

Таким образом, внедрению цифровых технологий должны способствовать не только новые программные продукты на рынке, но и меры налоговой политики, которые позволять внедрять и использовать «чистые» энергосберегающие технологии. В этой связи, будут использованы экономические рычаги для использования цифровых технологий в производственной, а также промышленной безопасности.

Литература

1. Горелов Н.А. Политика доходов и качество жизни населения [Текст] / Н.А. Горелов. - Спб.: Питер, 2003. - 653 с.
2. Костин К.Б., Березовская А.А. Современные технологии цифровой экономики как драйвер роста мирового рынка товаров и услуг. Экономические отношения. — 2019. — Том 9. — №2. - С.455-480.
3. Костин К.Б. Анализ кризисных явлений в мировой экономике. Известия Санкт-Петербургского экономического университета. – 2019. – №3 (117). – С. 7-14.
4. Роструд. [Электронный ресурс]. – URL: https://mintrud.gov.ru/labour/safety/321 (дата обращения: 20.04.21г.).
5. Росстат. [Электронный ресурс]. – URL: https://rosstat.gov.ru/working_conditions (дата обращения: 20.04.21г.).
6. C news «Инфосистемы джет» удовлетворит спрос на цифровые решения для охраны труда, промбезопасности и экологии. [Электронный ресурс]. – URL: https://cnews.ru/link/n526529 (дата обращения: 20.04.2021г.).

УДК 338

Лепеш Григорий Васильевич
д-р техн. наук, профессор
Шарафутдинова Лилия Ражаповна
аспирант
Санкт-Петербургский государственный
экономический университет

АНАЛИЗ МЕТОДИК ОЦЕНКИ УРОВНЯ ЦИФРОВИЗАЦИИ ПРОМЫШЛЕННОСТИ*

*Исследование выполнено при финансовой поддержке РФФИ и БРФФИ в рамках научного проекта № 20-510-00002.

Аннотация. Проведен анализ отечественных и зарубежных методов оценки уровня цифровой экономики, в измерение которой включены факторы отраслей промышленности. Выделены компоненты и способы их определения. Для оценки уровня цифровизации промышленных предприятий и обеспечения государственной поддержки предложено создание единой экоплатформы, работающей по принципу единого окна.

Ключевые слова: цифровизация, технологическое лидерство, государственная поддержка, методика, оценка, уровень.

ANALYSIS OF METHODS FOR ASSESSING THE LEVEL OF DIGITALIZATION OF INDUSTRY

Lepesh G.V.
Sharafutdinova L.R.
St. Petersburg State Economic University

Annotation. The analysis of domestic and foreign methods of assessing the level of the digital economy, the measurement of which includes factors of industries, is carried out. The components and methods of their determination are highlighted. To assess the level of digitalization of industrial enterprises and the provision of state support, it is proposed to create a single ecoplat form operating on the principle of a single window.

Keywords: digitalization, technological leadership, government support, methodology, assessment, level.

Современные государственные стимулы развития экономики сегодня направлены на технологическое лидерство, рассматриваемое как

ключевой фактор обеспечения устойчивости и экономического роста. Одним из основных стимулов развития, обеспечивающего переход к неоиндустриальной экономике и тем самым, обеспечивающим технологическое лидерство становится цифровизация. Для российской экономики цифровизация экономики стала «эликсиром», который обеспечит получение мгновенного эффекта развития во всех сферах общества. Для промышленности цифровизация рассматривается как головная стратегия вывода производства на новый уровень путем внедрения автоматизации производственных и управленческих процессов (умное производство), заменяющих человека интеллектуальными машинами, киберфизическими системами, работающими с реальными объектами и цифровыми двойниками, с большими данными, использующие блокчейн-технологии и функционирующие в рамках развитых экосистем [1]. В научной литературе этот этап рассматривается как четвертая промышленная революция, обеспечивающая слияние бизнеса, производства и общества с цифровыми технологиями.

Результаты проведенного мониторинга среди промышленных предприятий г. Санкт-Петербурга [2], показывают, что подавляющее большинство предприятий заинтересованы в цифровой трансформации производств и процессов, однако рассматривают его как постепенный переход и замену устаревшего оборудования и технологий на автоматизированные и оцифрованные с последующей интеграцией и возможной кооперацией на пути движения к цифровым экосистемам. Однако, на промышленных предприятиях процессы цифровой адаптации и трансформации тормозятся из-за отсутствия единой цифровой политики в области применения цифровых продуктов и подготовки соответствующего квалифицированного персонала, обладающего необходимыми компетенциями в области внедрения данных продуктов [3]. Большинство предприятий на свой страх и риск финансируют проекты внедрения цифровых инструментов на всех стадиях жизненного цикла продукции от разработки до ее сопровождения при эксплуатации и утилизации, применяя зачастую импортные программные продукты или разрабатываемые самостоятельно и не ориентированные на интеграцию как в рамках самого предприятия, так и в рамках кооперации при создании экосистем. В то же время ряд российских научных организаций и сообществ разрабатывают программные и цифровые инструменты, позволяющие успешно решать задачи цифровизации производственных и управленческих процессов на всех стадиях жизненного цикла продукции, успешно конкурирующих с импортными. Государство посредством Госкорпорации «Росатом», которая стала центром компетенций Федерального проекта «Цифровые технологии» Национальной программы «Цифровая экономика», в рамках

реализации мероприятий обеспечению технологической независимости российских предприятий создает платформу, объединяющую российские цифровые технологии с широким доступом для промышленных предприятий. Однако условия доступа, на сегодняшний день коммерческие, хотя и с наличием государственного софинансирования по грантам компаниям, внедряющим цифровые решения.

Эффективность государственной поддержки промышленных предприятий и экономики в целом в рамках реализации Национальной программы «Цифровая экономика» напрямую связана с мониторингом ее результатов, предусматривающем оценку уровня цифровизации. Однако несмотря на наличие многочисленных используемых подходов к оценке цифровизации экономики, вопрос измерения цифровизации промышленности освещен недостаточно, в связи с чем анализ методик измерения цифровизации промышленности имеет особую актуальность.

В данном исследовании рассматривается оценка уровня цифровой экономики, в измерение которой включены факторы отраслей промышленности. Рассмотрим их особенности.

Институтом статистических исследований и экономики знаний НИУ ВШЭ [4] предложен анализ цифрового климата на предприятиях промышленности с помощью *системы индикаторов, включающих композитные индексы цифровой конъюнктуры:*

- индекс цифрового климата;
- индекс цифровой занятости;
- индекс цифровой уязвимости.

Согласно описанию методики данного инструмента, вышеуказанные индексы рассчитываются методом главных компонент, консолидирующие оценки параметров программы наблюдения.

Индекс цифрового климата отражает обстановку в обрабатывающей промышленности через изменения параметров: цифровая активность, инвестиции в технологии, востребованность в использовании цифровых продуктов. Как показывают результаты исследования НИУ ВШЭ цифровая активность увеличена в 2020 году по сравнению с 2019 году на всех предприятиях промышленности. Интенсивность востребованности использования цифровых продуктов в 2020 году ослаблена в отличие от предшествующего периода. Если в 2019 году рост составил 25%, то в 2020 году 21%. Тем не менее, динамика показателя сохраняется положительной. Следующий компонент системы индикаторов «инвестиции в цифровые технологии» характеризует оценку инвестиционных расходов на предприятиях. По данным представленного обзора показатель незначительно увеличился.

Следующим индексом системы индикаторов является *индекс цифровой занятости*, измеряющий кадровые изменения в организациях среди сотрудников, компетентных в области информационно-коммуникационных технологий. Показатель характеризуется дефицитом специалистов ИКТ на предприятиях и привлечением сторонних лиц для выполнения профессиональных задач. Как показывают результаты опроса, 21% предприятий в 2019 году отметили низкий уровень цифровой грамотности специалистов.

Индекс цифровой уязвимости отражает подверженность предприятий колебаниям в развитии цифровизации, проблемам, ограничивающим технологическое развитие. Так, предприятия химического производства, нефтепродуктов, металлургии, лекарственных средств и материалов показывают низкую уязвимость к отраслевым ограничениям.

Готовность к цифровой трансформации значительно проявлена предприятиями фармацевтической отрасли, производствами машин и оборудования. Низкотехнологичные отрасли, такие как предприятия резиновых и пластмассовых изделий, текстиля, а также высокотехнологичные отрасли – производство электрического оборудования, машин и оборудования фиксируют достаточно неблагоприятные тенденции.

Методология Московской школы управления Сколково оценивает имидж цифровизации субъектов РФ качественно и количественно посредством индекса «Цифровая Россия» [5]. В данном исследовании отмечается в качестве недостатка предыдущих исследований – анализ формальных показателей, связанных с оценкой уровня информатизации. Например, количество компьютеров, степень проникновения интернета. Предлагаемый индекс включает семь субиндексов, каждый из которых измеряется количественно путем расчета средневзвешенной оценки:

– нормативное регулирование и административные показатели цифровизации;

– специализированные кадры и учебные программы;

– наличие и формирование исследовательских компетенций и технологических заделов, включая уровень НИОКР;

– информационная инфраструктура;

– информационная безопасность;

– экономические показатели цифровизации;

– социальный эффект от внедрения цифровизации.

Численная оценка представляет балльную экспертную оценку субфакторов. Каждому из них с помощью факторного анализа назначается вес. Далее субфакторы проходят качественную оценку, и с помощью кри-

териев интервал оценки субиндексов верифицируются для определения агрегированного индекса.

Результатом является итоговое значение индекса имиджа цифровизации, отраженное в сводной таблице субиндексов, в которой будут зафиксированы баллы субъекта РФ по каждому из 7-ми указанным направлениям в интервале от 0 до 100 единиц.

Анализ по регионам позволяет увидеть повышенный спрос со стороны бизнеса, государства на цифровые технологии, развитие центров компетенций. Регионами с наиболее высоким индексом являются Центральный, Уральский, Приволжский. Также при анализе бизнес-трендов была выявлена тенденция создания объединенных платформ (например, проекты «Сбербанк» и «Яндекс», совместно реализующие площадку электронной коммерции «Яндекс. Маркет»), что подчеркивает интерес предприятий к синхронизации цифровых решений. В результатах вышеприведенного исследования отмечено отсутствие мотивации у предприятий отраслей промышленности в связи с санкционными ограничениями для выхода на международный рынок и наличием достаточного уровня технологичности для выполнения текущих задач.

McKinsey Global Institute предложена методика расчета индекса цифровизации по секторам экономики Industry Digitization index [6]. Данный индекс объединяет 20 показателей для измерения *цифровых активов, цифрового использования, и сотрудников ИКТ* в каждом из секторов. Индекс оцифровки отраслей включает индикаторы, отражающий несколько способов оцифровки компаний. Так, например, для измерения цифровых активов учитываются расходы бизнеса на компьютеры, ПО и телекоммуникационное оборудование. Метрики цифрового использования включают использование в отрасли цифровых платежей, цифрового маркетинга, программного обеспечения для операций офисных сотрудников.

Показатели кадров оцениваются с помощью доли работников, связанных с цифровыми технологиями, определения цифровых расходов и активов в расчете на каждого сотрудника. Показатели, включенные в индекс оцифровки индустрии MGI:

Цифровые активы:

1) Затраты:

- расходы на оборудование (доля общих затрат на оборудование ИКТ);
- программное обеспечение и ИТ-услуги (доля общих затрат на ПО и ИТ-услуги);
- расходы на телекоммуникации (Доля общих расходов на телекоммуникации, например, широкополосный доступ, услуги мобильной передачи данных).

- Запасы цифровых активов:

- аппаратные активы (доля в общих активах, состоящая из оборудования ИКТ (например, компьютеры, серверы);

- программные активы (доля в общих активах, состоящих из программного обеспечения, например, приобретенные лицензии на программное обеспечение).

Цифровое использование:

1) Сделки:

- предприятия, продающие онлайн (годовые продажи через онлайн)

- предприятия, совершающие покупки через Интернет (доля компаний, совершающих не менее 1% покупок через любые компьютерные сети).

2) Взаимодействие между фирмами, клиентами и поставщиками:

- цифровая цепочка поставок (предприятия, реализующие производственную деятельность, через компьютерные сети, например, производственные планы, прогнозы, ход доставки);

- социальные сети;

- компании, интегрирующие ИКТ в повседневную деятельность

- компании, использующие ИКТ для работы с клиентами;

- компании, использующие социальные икт для работы с партнерами

- компании, в которых не менее половины бизнеса является цифровым (агрегированный балл, основанный на опросе MCKinsey цифровых возможностей фирм Европы и США);

3) Процессы:

- использование ресурсов планирования для предприятия (предприятия, использующие ERP, автоматизированный бух.учет, производство)

- управление взаимоотношениями с клиентами (предприятия, использующие CRM, или иное программное обеспечение для анализа информации о клиентах)

Труд

1) Цифровые затраты:

- расходы на оборудование для сотрудников;

- расходы на программное обеспечение и ИТ-услуги в расчете на одного работника

- расходы на телекоммуникации на одного работника (например, широкополосный доступ);

2) Цифровой капитал:

- аппаратные активы на одного работника (серверы, ПО и тд);

- программные активы на одного сотрудника (лицензии и тд);

3) Оцифровка работы:

- доля рабочих мест, которые являются цифровыми от общего числа рабочих мест (например, веб-дизайнеры, администраторы баз данных, специалисты по большим данным и т.д.).

Результаты показали недостаточно высокую цифровизацию секторов с тяжелыми активами, такими как промышленность, горнодобывающая отрасль, здравоохранение. Компании широко используют цифровые инструменты для взаимоотношений с клиентами, поставщиками, партнерами, но недостаточное проникновение цифровых технологий в физические активы.

Также в зависимости от компаний различаются возможности оцифровки. Например, Siemens предлагает возможности мониторинга и профилактического обслуживания клиентов, Bosch используют технологии RFID, завод в Лейпциге может представить архетип интеллектуального автоматизированного завода.

Наблюдается тенденция того, что некоторые отрасли оцифровались раньше и интенсивнее, чем другие, что может быть связано с наличием крупных фирм в отрасли. Например, большие предприятия, имеющие дело с длинными цепочками поставок, сложными операциями более оцифрованы, а также целенаправленно совершенствуются в использовании более рациональных и недорогих решений с применением аналитики больших данные, технологий локализации и отслеживания товаров.

Рекомендовано создание новых цифровых бизнес-моделей и ускорение цифрового взаимодействия с покупателями и поставщиками, использование различных моделей сотрудничества по обмену данными, виртуальному сотрудничеству. Для правительства в качестве основных направлений указаны меры по содействию стандартизации телекоммуникационных сетей, регулированию стандартов и логистики электронной коммерции для создания единого цифрового рынка, увеличения притока венчурного финансирования, продвижения инициатив по бесплатному использованию данных, внедрению в учебные программы занятий по развитию цифровых навыков, разработка целевых программы для устранения критической нехватки талантов.

Зарубежным научным сообществом предложен сводный индекс цифровизации [7], разработанный на основе шести компонентов: доступность, инвестиции в инфраструктуру, доступ к сети, емкость, цифровое использование и человеческий капитал. В результате расчета индекса построена эволюция оцифровки для отдельных стран в период с 1995 по 2011 гг., а также выявлены четыре группы стран:

- продвинутая группа (индекс свыше 50);
- переходная группа (индекс 35 – 50);

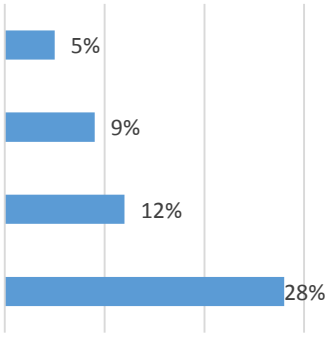
- развивающаяся (индекс 20 – 35);
- с ограничениями (индекс менее 20).

Основные проблемы, по мнению исследователей, заключаются в отсутствии стандартных показателей эффективности для измерения степени использования ИКТ, отсутствии инструментов для измерения воздействия цифровизации, необходимость новой политики и подходов к ускорению цифровизации и получении эффекта от нее.

Boston Consulting Group предложен индекс цифрового ускорения [8], с помощью которого можно оценить уровень цифрового развития компании. Методология заключалась в опросе 2 296 компаний в целях оценки цифровой зрелости по шкале от 1 до 4 в 36 категориях. Далее оценки агрегированы, взвешены, и каждая компания ранжирована по шкале от 0 до 100, в результате чего определена общая производительность компании – индекс цифрового ускорения. Организации с оценкой от 67 до 100 определены как цифровые («бионические») компании, от 44 до 66 на стадии развития цифрового уровня, 43 и меньше являются цифровыми отстающими. «Бионическая» компания – компания, в которой технологии сочетается с гибкостью, адаптивностью и всесторонним опытом людей (например, Google, Amazon, Apple). В опросе рассмотрены десять отраслей: потребительские товары и розничная торговля, энергетика, финансовые институты, здравоохранение, промышленные товары, страхование, СМИ, государственный сектор, технологии и телекоммуникации.

Четыре фактора цифровых («бионических») компаний:

- более 25% приложений являются цифровыми и связаны через API;
- более 25% бизнес-процессов автоматизированы;
- более 15% сотрудников на полной занятости с цифровыми навыками заняты в работе ИИ;
- более 10% сотрудников, занятых полный рабочий день, обучаются ИИ



Три ключевых результата цифровых («бионических») компаний: развернуто более 25% сценариев использования ИИ в больших масштабах; заработано более 15% дохода от больших данных достигнут рост EBIT более чем на 10% благодаря сценариям использования искусственного интеллекта.

В результате исследования выявлены факторы успешной цифровой трансформации «бионических» компаний: инвестиционные приоритеты (в технологии, повышение качества данных, укрепление цифровых навыков). Более 15% операционных расходов составляют затраты на цифрови-

зацию. В основе цифровой трансформации лежит искусственный интеллект, а также обучение искусственному интеллекту сотрудников компании, так как при таком подходе результаты внедрения цифровых технологий усиливаются. Следующим фактором является создание системы управления и внедрение операционной модели платформы. Как показывает исследование, бионическими компаниями установлено четкое управление и подотчетность за цифровые инициативы, наряду с руководителями бизнес-подразделений введено ответственное лицо за цифровую трансформацию. Также и на руководителей бизнес-подразделений возлагается ответственность за реализацию цифровых инициатив, предоставление ресурсов, финансирование и надзор за их реализацией. Внедрение операционной модели предполагает не централизованное управление цифровизацией, а внедрение цифровых инициатив командами внутри бизнес-подразделений, что подчеркивает важность обучения сотрудников. Также отмечено, что ключевым шагом является создание культура, вовлечение сотрудников и руководства в способы интеграции технологий и данных в свои повседневные задачи.

Значительно опережают в уровне цифровой зрелости финансовые учреждения, технологические компании и компании телекоммуникационной отрасли. В 2019 и 2020 гг. цифровое развитие ускорилось в здравоохранении и розничной торговле.

Энергетика, страхование и государственный сектор оказались наименее развитыми в цифровом отношении категории. Тенденция объяснима тем, что исторически энергетические компании уделяли больше внимания инженерным технологиям, чем ИКТ, так же, как и здравоохранение сталкивается с проблемами из сложной нормативно-правовой среды.

Национальной Академией науки и техники Acatech предложен Индекс зрелости Industrie 4.0 [9] для определения текущей стадии зрелости Индустрии 4.0 промышленных предприятий. В разработке индекса приняли участие научно-исследовательские институты в партнерстве с промышленными предприятиями. Методология включала четыре этапа, которые обеспечивали единую цепочку на всем протяжении исследования. Первый этап – научно-промышленный консорциум, включающий исследовательское и промышленное сообщество, в течение года совместно разрабатывающие основу исследования, находя баланс между теорией и практикой. Следующий этап состоял в апробации методологии в разных компаниях, третий этап подразумевал формирование конкретных рекомендаций, полученных на основе модели, четвертый этап проходил на протяжении всего проекта и включал постоянную проверку промежуточных результатов.

В основе подхода лежит предложение развития цифровизации на предприятии последовательно по следующим этапам: компьютеризация, интеграция систем, видимость, прозрачность, прогнозирование, адаптивность. Именно данная последовательность этапов обеспечивает полную цифровую трансформацию, а в случае отклонения возможно понимание, какие необходимы инструменты и методы для конкретного этапа.

В рамках отдельных предприятий конкретных отраслей (металлургическое предприятие) предлагается измерение готовности предприятий к условиям Индустрии 4.0 [10]. Первоначально с помощью опросного листа по восьми аспектам проведены аудит предприятия. На основе экспертных оценок определен уровень автоматизации предприятия, что позволило выявить наименее подготовленные к цифровизации процессы. Полученные результаты соотносятся с бизнес-процессами, которые определены для приоритетной проработки, что позволяет оценить эффективность существующих решений и определить необходимость дальнейших цифровых проектов. С помощью экспертной технической комиссии и экономической службы определяются пилотные проекты и запуск в промышленную эксплуатацию.

Национальный индекс развития цифровой экономики, предложенный в качестве пилота Госкорпорацией РОСАТОМ, рассматривает степень готовность, воздействие цифровых технологий на социально-экономическое развитие стран [11]. Индекс построен на основе последовательного агрегирования значений показателей (использование «принципа матрешки»). Интегральные показатели: человеческий капитал, НИОКР, деловая среда, кибербезопасность, цифровой сектор, цифровая инфраструктура, цифровое правительство, здравоохранение, цифровой бизнес, цифровые граждане, государственная политика и регулирование. Россия занимает 23 место в итоговом рейтинге из 32 стран.

Таблица 1 – Место России в отраслевых компонентах цифрового бизнеса по индексу развития цифровой экономики

Экономическая группировка	**Место России из 32-х стран**
Промышленность	20
Строительство	23
Электроэнергетика, кондиционирование воздуха и водоснабжение	22
Информационные и коммуникационные технологии	23
Индустрия гостеприимства	25
Недвижимость	19

Окончание табл. 1

Экономическая группировка	Место России из 32-х стран
Розничная торговля	18
Транспорт и хранение	21
Оптовая торговля	19

Значение подиндекса отраслей трактуются как уровень цифровизации соответствующих отраслей. Подиндекс промышленности РФ составляет 0,312. Самый высокий Финляндия со значением 0,479.

Европейской комиссией в 2016 году запущена инициатива «Цифровизация европейской промышленности» (DEI) [12]. Одной из ключевых концепций для реализации данной инициативы является введение Центра цифровых инноваций (DIH), предоставляющий услуги по экспертизе в области технологий, тестированию и созданию сетей для предприятий. В 2018 году Комиссия предложила на период 2021 – 2027 гг. программу «Цифровая Европа», которая сосредоточена в пяти областях: высокопроизводительные вычисления, искусственный интеллект, кибербезопасность и доверие, продвинутые цифровые навыки, функциональная совместимость. Для оценки цифрового прогресса ЕС измеряет индекс цифровой экономики и общества DESI, который отслеживает цифровую конкурентоспособность и включает пять компонентов: связь (покрытие широкополосной связью, мобильной связью), человеческий капитал, использование интернета, интеграция цифровых технологий (оцифровка бизнес и электронная коммерция), цифровые государственные услуги (электронное правительство) [13]. Наиболее актуальными для цифровизации европейской промышленности комиссия считается *связь, человеческий капитал, интеграция цифровых технологий*.

Основные направления европейской промышленной инициативы по оцифровке включают: координацию различных национальных и региональных инициатив, центры цифровых инноваций; укрепление лидерства через партнерства и промышленные платформы (учреждены ГЧП и совместные предприятия в области ключевых технологий – 5G, большие данные, высокопроизводительны вычисления, кибербезопасность, фотоника, робототехника, электронные компоненты и системы; нормативно-правовая база, цифровое образование (подготовка европейцев к цифровому будущему: стажировки «Цифровые возможности», поддержка развития цифровых компетенций, цифровое образование).

Также компаниями разрабатываются мероприятия по диагностике цифровой зрелости, как в России, так и за рубежом ([14], [15], [16]).

В отдельных работах предлагается рассматривать готовность к трансформации производства через оценку количества используемых пе-

редовых производственных технологий в ретроспективе по статическим данным, а также об организационной и стратегической готовности предприятий региона к цифровизации производства оценивать через затраты на технологические инновации [17].

Методика расчета целевых показателей национальной цели развития РФ «Цифровая трансформация» утверждена Приказом от 18 ноября 2020 г. №600 [18] включает показатели оценки цифровой зрелости промышленности:

- цифровая зрелость основных производственных процессов предприятий промышленности;
- цифровая зрелость вспомогательных процессов предприятий промышленности;
- доля предприятий, в отношении которых сформирован цифровой паспорт в Государственной информационной системе промышленности;
- доля предприятий, использующих технологию API для обмена данными, предоставления цифровых услуг и информационного взаимодействия с государственными информационными системами;
- доля предприятий, использующих технологии имитационного моделирования и виртуальных испытаний промышленной продукции;
- доля предприятий, использующих технологии предиктивной аналитики при прогнозировании и проведении послепродажного обслуживания промышленной продукции;
- доля предприятий, использующих технологии промышленного интернета вещей, сбора данных и диспетчерского контроля для управления производственными процессами в реальном времени;
- доля предприятий, использующих технологий «цифровой двойник производства».

Индекс по каждой отрасли рассчитывается как среднее из степени достижения целевых значений по каждому субиндексу (показателю). Сводная информация описанных методик представлена в Таблице 2.

Таблица 2 – Методики оценки уровня цифровизации

Наименование	**Авторы**	**Компоненты**	**Измерение (способ/подход)**
Система индикаторов цифровой конъюнктуры обрабатывающей промышленности	Центр конъюнктурных исследований Института статистических исследований и экономики знаний НИУ ВШЭ	– индекс цифрового климата; – индекс цифровой занятости; – индекс цифровой уязвимости	Индексы рассчитаны с помощью метода главных компонент, консолидирующие оценки параметров программы наблюдения

Продолжение табл. 2

Наименование	Авторы	Компоненты	Измерение (способ/подход)
Индекс «Цифровая Россия»	Московская школа управления Сколково	– нормативное регулирование и административные показатели цифровизации; – специализированные кадры и учебные программы; – наличие и формирование исследовательских компетенций и технологических заделов, включая уровень НИОКР; – информационная инфраструктура; – информационная безопасность; – экономические показатели цифровизации; – социальный эффект от внедрения цифровизации.	Отражает уровень использования в субъекте РФ потенциала цифровых технологий. Субиндексы рассмотрены через субфакторы, которые оценены экспертной оценкой. В целях снижения субъективности экспертной оценки: разработаны критерии экспертной оценки, механизм расчета взвешенных оценок, реализован механизм нормализации полученных данных, механизм взвешивания и агрегации, проведен анализ неопределенности и чувствительности, анализ зависимости основного индекса от субиндексов.
Сводный индекс цифровизации	Raul Katz, Pantelis Koutroumpis and Fernando Martin Callorda	– доступность, – инвестиции в инфраструктуру, – доступ к сети, – емкость, – цифровое использование – человеческий капитал	Индекс построен на шести равновзвешенных компонент, далее рассчитан для 184 стран за период 2004-2011 гг.
Индекс оцифровки по секторам экономики Industry Digitization Index	McKinsey Global Institute	– цифровые активы; – цифровое использование; – труд	Индекс оценивает степень использования цифровых возможностей различными странами.

Продолжение табл. 2

Наименование	Авторы	Компоненты	Измерение (способ/подход)
			Исследуются секторы экономики через призму цифровых активов, цифрового использования и сотрудников, задействованных в ИКТ. Данный индекс объединяется 20 показателей для измерения цифровых активов, цифрового использования, и сотрудником ИКТ в каждом из секторов
Индекс цифрового ускорения (BCG Digital Acceleration Index (DAI)	Boston Consulting Group	Девять KPI: снижение затрат, рост цен на акции, рост доли рынка, три типа влияния EBIT (общее влияние, от цифровых технологий, от искусственного интеллекта), ROI, общая стоимость предприятий, выручка.	Опрос 2300 компаний в десяти отраслях. Организации с оценкой от 67 до 100 определены как бионические компании, от 44 до 66 на стадии развития цифрового уровня, 43 и меньше являются цифровыми отстающими.
Индекс зрелости Industrie 4.0	Национальная Академия науки и техники Acatech	Методология включала четыре этапа, которые обеспечивали единую цепочку на всем протяжении исследования: Разработка методологии партнерами из исследования и промышленность, Заседания руководящего комитета для рассмотрения результатов проекта, Проверка общей	В основе предлагаемого подхода лежит поэтапное выполнение уровней развития индустрии 4.0. Этапы развития включают следующие: компьютеризация, интеграция систем, видимость, прозрачность, прогнозирование, адаптивность.

Продолжение табл. 2

Наименование	Авторы	Компоненты	Измерение (способ/подход)
		методологии, мониторинг и проверка на протяжении всего исследования	
Анализ уровня готовности предприятия металлургической промышленности	Фролов В.Г., Трофимов О.В., Мартынова Т.С.	Оценка степени развития предприятия в соответствии с концепцией Индустрии 4.0 по различным информационным системам, их интеграции в производственную деятельность и оценка состояния	На основе экспертных оценок определен уровень автоматизации предприятия, что позволило выявить наименее подготовленные к цифровизации процессы.
Оценка экономической эффективности цифровизации с использованием инструментов нечеткой логики	Коханова В.С.	оценка экономической эффективности цифровизации с использованием инструментов нечеткой логики.	
Национальный индекс развития цифровой экономики	Госкорпорация РОСАТОМ	Индекс построен на основе последовательного агрегирования значений показателей (использование «принципа матрешки»). Интегральные показатели: человеческий капитал, НИОКР, деловая среда, кибербезопасность, цифровой сектор, цифровая инфраструктура, цифровое правительство, здравоохранение, цифровой бизнес, цифровые граждане, государственная политика и регулирование.	Оценка уровня развития цифровой экономики РФ в сопоставлении с международным уровнем. В основе системный подход, определяющий оценку условий (факторов), влияющих на развитие и использование цифровых технологий, процессов цифровизации различных отраслей экономики (включая промышленность), социально-экономические эффекты от использования цифровых технологий.

Продолжение табл. 2

Наименование	Авторы	Компоненты	Измерение (способ/подход)
Индекс цифровой экономики и общества DESI	Европейская комиссия	– связь (покрытие широкополосной связью, мобильной связью), – человеческий капитал, – использование интернет, – интеграция цифровых технологий (оцифровка бизнес и электронная коммерция), – цифровые гос.услуги (электронное правительство)	
Методика расчета целевых показателей национальной цели развития РФ «Цифровая трансформация»	Приказ от 18.11.2020 №600 «Об утверждении методик расчета целевых показателей национальной цели развития Российской Федерации «Цифровая трансформация»	Показатели цифровой зрелости в промышленности: – цифровая зрелость основных производственных процессов предприятий промышленности; – цифровая зрелость вспомогательных процессов предприятий промышленности; – доля предприятий, в отношении которых сформирован цифровой паспорт в Государственной информационной системе промышленности; – доля предприятий, использующих технологию API для обмена данными, предоставления цифровых услуг и информационного взаимодействия с государственными ин-	Достижение цифровой зрелости рассчитывается в соответствии с методикой, как на уровне субъектов РФ, так и на федеральном уровне.

Окончание табл. 2

Наименование	Авторы	Компоненты	Измерение (способ/подход)
		формационными системами; – доля предприятий, использующих технологии имитационного моделирования и виртуальных испытаний промышленной продукции; – доля предприятий, использующих технологии предиктивной аналитики при прогнозировании и проведении послепродажного обслуживания промышленной продукции; – доля предприятий, использующих технологии промышленного интернета вещей, сбора данных и диспетчерского контроля для управления производственными процессами в реальном времени; доля предприятий, использующих технологий «цифровой двойник производства».	

Заключение

Анализ данных методик, направленных на оценку уровня цифровизации цифровой конъюнктуры стран, отраслей, хозяйствующих субъектов, показывает ориентированность на определение широты охвата информационными технологиями, на инфраструктуру. Основное отличие методик заключается в подборе первичных показателей, которые характеризуют уровень использования цифровых технологий. Формирование международных рейтингов осуществляется при участии бизнеса.

С аналитической точки зрения достаточно трудно определить причины и проблемы в производительности отраслей промышленности на основе данных, предлагаемых в агрегированном индексе. Недостаточное внимание уделяется фактически достигнутым результатам, оценке информационной безопасности. Среди проблем также следует отметить трудность сбора данных, которых может быть недостаточно для оценки уровня цифровизации, сложная сопоставимость стран, неполные данные, получение достоверных данных, незаинтересованность организаций. Учитывая скорость изменений, необходима постоянная актуализация информации.

В контексте цифровой трансформации актуальными направлениями развития могут быть запуск единого окна для предприятий, чтобы воспользоваться инновационными цифровыми возможностями; оценка процессов и результатов на основе показателей, отражающих различные аспекты предприятия (совокупность организационно-управленческого, инфраструктурного, финансово-экономического, кадрового направлений предприятия), что позволит анализировать функционирование предприятий с учетом существующих методов производства и с использованием цифровых технологий.

Литература

1. Лепеш Г.В., Угольникова О.Д., Шарафутдинова Л.Р. Концептуальные основы цифровой индустриализации (на примере стран с различными технологическими укладами //Технико-технологические проблемы сервиса. №2(56), 2021 г. С. 3 – 8

2. Лепеш Г.В., Макарова И.В Базовые параметры современной региональной промышленной политики сотрудничества в Республикой Беларусь. //Технико-технологические проблемы сервиса. №1(55), 2021 г. С. 3–8

3. Лепеш Г.В. Совершенствование форм взаимодействия между предприятиями в контексте цифровой трансформации // Технико-технологические проблемы сервиса. №2(52), 2020 г. - С. 3 – 11

4. Цифровизация обрабатывающей промышленности в 2020 г.: векторы цифровой эволюции в пандемию COVID-19. М.: НИУ ВШЭ, 2021. – 19 с. Доклад_ Цифровой климат _ промышл__Лола_ (hse.ru). [Электронный ресурс].– URL: https://www.hse.ru/mirror/pubs/share/452706577.pdf

5. Индекс «Цифровая Россия». [Электронный ресурс]. – URL: https://finance.skolkovo.ru/downloads/documents/FinChair/Research_Reports/SKOLKOVO_Digital_Russia_Report_Full_2019-04_ru.pdf

6. Digital Europe: oushing the frontier. Capturing the benefits. McKinsey global institute. [Электронный ресурс]. – URL: Digital-Europe-Full-report-June-2016.ashx (mckinsey.com)

7. Raul Katz, Pantelis Koutroumpis and Fernando Martin Callorda Using a digitization index to measure the economic and social impact of digital agendas Using a digitization index to measure the economic and social impact of digital agendas (citicolumbia.org)

8. Методология расчета индекса цифрового ускорения. индекс цифрового ускорения (DAI) создания цифровой ценности БЦЖ (bcg.com)

9. acatech_STUDIE_Maturity_Index_eng_WEB.pdf

10. Фролов В.Г., Трофимов О.В., Мартынова Т.С. Анализ готовности металлургического предприятия к «Индустрии 4.0» и стратегия внедрения цифровых решений // Креативная экономика. – 2019. – Том 13. - № 6. – С. 1117-1132. URL: Analiz_gotovnosti_metallurgiceskogo_predpriatia_k_(1).pdf

11. Национальный индекс развития цифровой экономики: Пилотная реализация. М., Госкорпорация «Росатом», 2018. – 92 с. [Электронный ресурс]. – URL: df063a504b10a3af5a1ce7cbb07e35fd.pdf (minenergo.gov.ru)

12. Специальный доклад по цифровизации европейской промышленности [Электронный ресурс]. – URL: https://op.europa.eu/webpub/eca/special-reports/digitising-eu-industry-19-2020/en/#annexiv

13. The Digital Economy and Society Index (DESI) (archive-it.org). [Электронный ресурс]. – URL: https://wayback.archive-it.org/12090/20200704052344/https:/ec.europa.eu/digital-single-market/en/desi

14. Industrie 4.0-Проверка готовности (industrie40-readiness.de). [Электронный ресурс] – URL: https://www.industrie40-readiness.de/?lang=en

15. Оценка цифровой зрелости (komanda-a.pro). [Электронный ресурс]. – URL: https://komanda-a.pro/

16. Оценка цифровой зрелости/ Центр перспективных управленческих решений (cpur.ru). [Электронный ресурс]. – URL: https://cpur.ru/digitalconsulting/

17. Куприянова М.В., Симикова И.П. Методологические подходы к оценке уровня цифровизации промышленного производства. Издательский дом «Среда». [Электронный ресурс]. – URL: elibrary_41775327_59964120.pdf

18. Приказ Минцифры России от 18.11.2020 N 600 «Об утверждении методик расчета целевых показателей национальной цели развития Российской Федерации «Цифровая трансформация» (вместе с «Методикой расчета показателя «Достижение «цифровой зрелости» ключевых отраслей (np-ss.org)

УДК 004.942

Ложкина Ольга Владимировна
д-р техн. наук, канд. хим. наук, профессор
Санкт-Петербургский университет Государственной
противопожарной службы МЧС России

РАЗВИТИЕ ПРОГНОСТИЧЕСКИХ МЕТОДОВ ОЦЕНКИ ЭКОЛОГИЧЕСКОГО УЩЕРБА ОТ ТРАНСПОРТНОГО СЕКТОРА В КОНТЕКСТЕ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ РЕАЛЬНОЙ ЭКОНОМИКИ

Аннотация. В статье описан новый метод мониторинга и прогнозирования экологического ущерба реальной экономике со стороны транспортного сектора. Методически алгоритм выстраивается на принципе последовательного отслеживания эффектов: городской транспорт как источник выбросов загрязняющих веществ и парниковых газов – уровень загрязнения окружающей среды – негативное воздействие на здоровье населения, флору, фауну, объекты инфраструктуры, климат – денежная оценка этого воздействия. Разработанный метод был апробирован в Санкт-Петербурге. Было установлено, что социально-экономический ущерб от загрязнения воздушной среды городским транспортом может достигать 0,68-0,78 % валового регионального продукта.

Ключевые слова: реальная экономика, городской транспорт, загрязнение окружающей среды, социально-экономический ущерб, прогнозирование.

Lozhkina O. V.
St. Petersburg University of State Fire
service of EMERCOM of Russia

FORECASTING METHOD FOR ASSESSMENT OF ENVIRONMENTAL COSTS OF TRANSPORTATION SECTOR IN THE CONTEXT OF IMPROVING THE SECURITY OF THE REAL ECONOMY

Annotation. The article describes a new method for monitoring and forecasting environmental damage to the real economy from the transport sector. Methodologically, the algorithm is built on the principle of sequential tracking of effects: urban transport as a source of emissions of pollutants and greenhouse gases - the level of environmental pollution - negative impact on public health, flora, fauna, infrastructure, climate - the monetary value of this impact. The de-

veloped method was tested in St. Petersburg. It was found that the socio-economic damage from air pollution by urban transport can reach 0.68-0.78% of the gross regional product.

Keywords: real economy, urban transport, environmental pollution, socio-economic damage, forecasting.

Проблема чрезмерного антропогенного воздействия на окружающую среду и осознание его масштабных социально-экономических издержек привело мировую общественность к разработке стратегии развития современной цивилизации, задокументированной в декларации «Повестка дня на XXI век», подписанной представителями 172 государств в 1992 г. в Рио-де-Жанейро, и выраженной в 27 принципах устойчивого развития [1].

На современном этапе эффективность принятия решений, направленных на минимизацию социально-экономического ущерба от загрязнения среды обитания во многом зависит от возможности **осуществления мониторинга и прогнозирования негативного экологического воздействия любого вида антропогенной деятельности на единой и понятной для всех основе – денежной оценке причиняемого ущерба (**[2] – [9]).

Формирование дорожной карты стратегии потребовало разработки инструмента для оценки причиняемого ущерба реальной экономике в денежном выражении. В рамках развития обозначенных подходов в странах Европейского Союза с конца прошлого века велись разработки соответствующих методологий, в т.ч. методологии Externe.

На основе методологии Externe нами был разработан оригинальный метод оценки экологического ущерба (внешних издержек) в натуральных и стоимостных показателях, вызванного загрязнением атмосферного воздуха опасными веществами, поступающими в окружающую среду в результате транспортной деятельности. Рис. 1 отражает последовательность отслеживания негативных эффектов согласно разработанному подходу.

Транспорт рассматривается как источник химического и шумового загрязнения окружающей среды.

Модель оценки внешних издержек от функционирования транспорта реализуется в 4 стадии:

- 1-ая стадия – стадия оценки среднегодовых валовых выбросов загрязняющих веществ, парниковых газов и среднегодового акустического загрязнения в исследуемом регионе;

- 2-ая стадия – стадия определения среднемесячных, среднесезонных или среднегодовых уровней загрязнения атмосферного воздуха по показателям превышения предельно-допустимых концентраций загрязняющих веществ и предельно допустимого уровня шумовой нагрузки;

- 3-я стадия – стадия оценки ущерба в натуральных показателях, например, в натуральных показателях ущерба здоровью населения (насколько выросла заболеваемость населения острыми респираторными инфекциями, астмой, сердечно-сосудистыми заболеваниями в период высокого уровня загрязнения воздуха по сравнению с нормально-благоприятной ситуацией);

- 4-я стадия - стадия денежной оценки причиненного ущерба.

Рисунок 1 – Структурная схема комплексной модели отслеживания негативного воздействия транспорта на население и окружающую среду

Новый метод дает возможность осуществлять мониторинг и прогнозирование экологического ущерба, наносимого реальному сектору экономики, по таким факторам негативного воздействия, как повышение смертности и заболеваемости населения, снижение урожайности в сельском хозяйстве, сокращение площадей зеленых насаждений, порча объектов городской инфраструктуры в результате коррозионного действия поллютантов.

Метод применим для оценки ущерба от всех видов транспорта, работающих на углеводородных энергоносителях, а также электрического транспорта (включая электромобили, троллейбусы, трамваи, электропоезда метрополитена) в эквиваленте выбросов поллютантов при производстве электроэнергии (предполагая, что используемая электроэнергия вырабатывается тепловыми электростанциями).

Показатели ущерба «доза – ответ» в натуральных оценках ущерба здоровью устанавливались с использованием статистических социально-

демографических данных (данных о численности и состава населения, смертности, заболеваемости респираторными заболеваниями, астмой, бронхитом) и с использованием зарубежных источников информации, адаптированных к социально-экономическим показателям Санкт-Петербурга. Стоимостные оценки ущерба здоровью в показателях риска преждевременной смертности осуществляли методом, основанным на теории полезности человека для общества, и методом международных сравнений [9]. Стоимостные оценки других видов ущерба производились методом международных сравнений с учетом валового внутреннего (регионального) продукта [9]. В Табл. 1 приведены стоимостные оценки ущерба в пересчете на 1 кг загрязнителя для Санкт-Петербурга, выбранного нами в качестве региона исследования, Латвии, Эстонии, Великобритании и Люксембурга. Стоимостные оценки для зарубежных государств были установлены с использованием программного обеспечения Ecosense, разработанного в Европейском Союзе в ходе реализации межгосударственного проекта Externe, направленного на определение внешних издержек от функционирования городского транспорта.

Таблица 1 – Стоимость ущерба от загрязнения атмосферного воздуха в пересчете на 1 кг поллютанта

	СПб	Латвия	Эстония	Англия	Люкс-г
NO_X					
Ущерб здоровью, €	4.234	2.248	0.994	5.495	11.594
Повышение смертности, €	2.927	1.629	0.707	4.077	8.510
Повышение заболеваемости, €	1.307	0.619	0.287	1.418	3.084
Ущерб инфраструктуре от коррозии, €	0.071	0.047	0.031	0.042	0.104
Ущерб лесопарковым хоз-вам, €	1.075	0.749	0.709	0.768	1.916
∑ ущерб	5.380	3.363	2.002	6.647	13.943
SO_2					
Ущерб здоровью, €	4.773	2.432	1.613	9.463	17.053
Повышение смертности, €	4.057	2.161	1.430	8.155	14.898
Повышение заболеваемости, €	0.716	0.271	0.183	1.308	2.155
Ущерб инфраструктуре от коррозии, €	0.253	0.129	0.098	0.19	0.450
Ущерб лесопарковым хоз-вам, €	0.475	0.188	0.263	0.284	0.751
∑ ущерб	5.501	2.765	1.983	9.953	18.307
$PM_{2.5}$					
Ущерб здоровью, €	13.923	4.915	2.539	16.283	26.707
Повышение смертности, €	12.252	4.354	2.253	14.642	23.896
Повышение заболеваемости, €	1.671	0.561	0.286	1.641	2.811
CO					
Ущерб здоровью, €	0.033	0.0034	0.0034	0.0034	0.007
C_XH_Y					
Ущерб здоровью, €	0.491	0.527	0.463	0.676	1.220

Анализ данных, приведенных в Табл. 1, показывает, что основной социально-экономический ущерб обществу от загрязнения атмосферы городов проявляется в виде риска развития опасных заболеваний и риска преждевременной смертности.

Апробация данного подхода была осуществлена на примере Санкт-Петербурга. Санкт-Петербург - второй по значению город Российской Федерацию и крупнейший транспортный узел нашей страны с развитой системой городского наземного и подземного транспорта, включающей автотранспорт, трамваи, троллейбусы, электропоезда, метрополитен, речной и морской транспорт, железнодорожный транспорт.

Сведения о структуре городского транспорта отражены в ежегодных сборниках Росстата и Петростата, доступных в свободном режиме на официальных сайтах учреждений (http://www.gks.ru/ и http://petrostat.gks.ru/), данные за 2015-2020 гг. приведены в Табл. 2.

Таблица 2 – Основные сведения об общественном городском транспорте Санкт-Петербурга за 2015-2020 гг.

		2015	2016	2017	2018	2019	2020
Протяженность маршрутной сети ГПТ	км	10150,61	10046,64	10172,3	10012,19	10023,32	н/д
линий метро	км	113,6	113,6	113,6	118,6	118,6	н/д
автобусной сети соц. маршрутов	км	4473,5	4534,9	4618,4	4610,7	4638,2	н/д
трамв. сети	км	484,5	488,0	476,3	486,2	460,0	н/д
трол. сети	км	511,0	511,05	527,8	533,6	543,5	н/д
автобусной сети ком. маршрутов	км	4568	4399,16	4436,2	4263,15	4263	н/д
Объем трансп. работы:		433423,6	435733,9	444308,2	462189,9	н/д	н/д
метро	тыс. ваг.-км	211446	213080	215915	228805	н/д	н/д
трамвай	тыс. км	34826,3	34367,9	34038,5	33301,6	н/д	н/д
троллейбус	тыс. км	27907,3	28681,1	29538,3	32094,1	н/д	н/д
автобус (соц. маршруты)	тыс. км	159244	159604,9	164816,4	167989,2	н/д	н/д
вагоны метро	ед.	1680	1711	1805	1903	1914	1935

Окончание табл. 2

		2015	2016	2017	2018	2019	2020
трамваев	ед.	790	787	771	770	776	772
троллейбусов	ед.	640	635	698	682	680	735

Анализ данных, приведенных в табл. 1, показывает, что протяженность автобусной сети социальных маршрутов в Санкт-Петербурге за с 2015 г. по первое полугодие 2019 г. выросла 3,7%, а путей метрополитена – на 3,5%, троллейбусной сети – на 14,8%. В то же время эксплуатационная протяженность трамвайных путей сократилась на 5%, а протяженность автобусной сети коммерческих маршрутов – на 6,7%. За этот же период практически пропорционально изменились показатели транспортной работы (ТР): объем ТР метро увеличился на 7,4%, социальных автобусов – на 7,4%, троллейбусов – на 15%, а объем ТР трамваев сократился на 4,4. Аналогичные тенденции наблюдались и в структуре ГПТ в 2015-2020 гг.: троллейбусный парк вырос на 6,3%, число вагонов метро – на 15,2%, а численность трамвайного парка сократилась на 2,3%. Кроме того, анализ данных табл. 2 свидетельствует о том, что транспортная работа, исчисляемая в тыс. км, городских общественных автобусов в 2,6 раза выше совокупной транспортной работы наземного городского электрического транспорта.

Согласно официальным отчетным документам Правительства Санкт-Петербурга и результатам собственных исследований ([10]-[12]), одним из ключевых источников загрязнения атмосферного воздуха Северной столицы, вклад которого составляет более 70%, является автомобильный транспорт. В Табл. 3 отражена динамика изменения численности автотранспортных средств в 2010-2020 гг.

Таблица 3 – Динамика изменения количества зарегистрированных автотранспортных средств в Санкт-Петербурге за 2010-2020 гг.

Год	Количество автотранспортных средств, ед.			
	Легковые автомобили	Грузовые автомобили	Автобусы	Всего
2010	1 462 461	129 043	22 714	1 614 218
2011	1 525 967	138 967	20 965	1 685 899
2012	1 537 473	201 033	22 449	1 760 955
2013	1 741 267	220 067	21 513	1 982 847
2014	1 636 336	213 123	19 838	1 869 297
2015	1 638 183	217 738	20 221	1 876 142

Окончание табл. 3

Год	Количество автотранспортных средств, ед.			
	Легковые автомобили	Грузовые автомобили	Автобусы	Всего
2016	1 676 379	214 003	19 659	1 910 041
2017	1 710 811	223 662	29 798	1 964 271
2018	1 724 410	226 975	20 948	1 972 333
2019	1 744 133	229 764	21 061	1 994 958
2020	1 771 034	231 735	20 951	2 023 720

Анализ представленных в Табл. 3 данных свидетельствует о том, что с 2010 по 2020 г. численность автомобильного парка Санкт-Петербурга выросла в 1,2 раза за счет увеличения парка легковых автомобилей, количество которых выросло с 1462461 в 2010 г. до 1771034 единиц в 2020 г., и грузовых автомобилей, число которых выросло практически в 2 раза за этот период со 129043 до 231735 единиц в 2020 г. По состоянию на 2020 г. суммарная численность автотранспортных средств в Санкт-Петербурге впервые превысила 2 млн. и достигла значения 2023720 единиц.

Результаты расчета, проведенного по разработанной методике, показали, что в Санкт-Петербурге суммарные внешние издержки от загрязнения воздушной среды городским транспортом в 2015-2020 гг. составили ≈0,68-0,78 % от валового регионального продукта. При этом в суммарном экономическом ущербе обществу по показателям риску здоровья населения доминируют оксиды азота и сопряженные с ними посредством фотохимических атмосферных взаимодействий органические пероксиды и озон, их вклад составляет ≈75 %, мелкодисперсные взвешенные частицы PM_{10} и $PM_{2.5}$ (≈15 %) и диоксид серы (≈8 %).

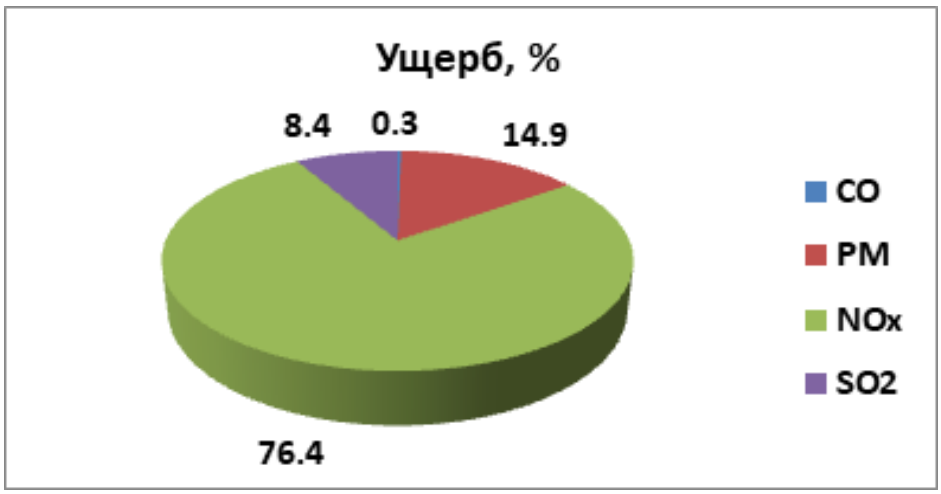


Рисунок 2 – Доля приоритетных атмосферных загрязнителей в суммарном экономическом ущербе обществу по показателям риска для здоровья

Оценочные расчеты за 2019 г., проведенные с учетом определенных с помощью программного обеспечения COPERT объемов годовых валовых выбросов NO_X, SO_2, PM_{10} и $PM_{2.5}$ и значений социально-экономических показателей, включая численность населения, численность работающего населения, среднемесячную заработную плату, среднестатистическую стоимость медицинских услуг, валового регионального продукта Санкт-Петербурга и пр., показали, что экономический ущерб обществу от загрязнения воздуха этими поллютантами мог составить 26,9, 2,87 и 5,38 млрд. рублей соответственно.

Литература

1. Jeffrey D. Sachs, Christian Kroll, Guillaume Lafortune, Grayson Fuller, and Finn Woelm. Sustainable Development Report 2021:The Decade of Action for the Sustainable Development Goals // Cambridge University Press. Available at: https://s3.amazonaws.com/sustainabledevelopment.report/2021/2021-sustainable-development-report.pdf

2. Luo Y., Chen H., Zhu Q., Peng C., Yang G., Yang Y., Zhang Y. Relationship between air pollutants and economic development of the provincial capital cities in China during the past decade // PLoS One. 2014. 9(8). e104013.

3. Tambo E., Duo-Quan W., Zhou X.N. Tackling air pollution and extreme climate changes in China: Implementing the Paris climate change agreement // Environ Int. 2016. 95. P.152-156.

4. Md Arif Hasan, David J. Frame, Ralph Chapman, Kelli M. Archie Costs and emissions: Comparing electric and petrol-powered cars in New Zealand / // Transportation Research Part D: Transport and Environment. 2021. 102671.

5. Wang, T. How can the UK road system be adapted to the impacts posed by climate change? By creating a climate adaptation framework / Tianni Wang, Zhuohua Qu, Zaili Yang, et al // Transportation Research Part D: Transport and Environment. – 2019. – V. 77. – P. 403-424.

6. Лепеш Г.В. Комплексная безопасность реальной экономики // Технико-технологические проблемы сервиса. 2018. №1 (43). С. 3-5.

7. Лепеш Г.В., Моисеев Е.Н. Прогнозирование безопасности технических систем // Технико-технологические проблемы сервиса. 2019. №2 (48). С. 9-16.

8. Лепеш Г.В. Безопасность населения и территорий в стратегии устойчивого развития РФ // Технико-технологические проблемы сервиса. 2018. №4 (46). С. 3-9. Мусиенко Т.В., Ложкин В.Н., Ложкина О.В. Методология прогноза экологического ущерба от транспортного сектора в

Санкт-Петербурге // Ученые записки Международного банковского института. – 2019. – №3 (29). – С. 91-106.

10. Ложкина О.В., Комашинский В.И. К вопросу о совершенствовании информационного процесса мониторинга и прогнозирования опасного воздействия транспортных выбросов на среду обитания и население // Научно-аналитический журнал Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. – 2021. – № 2. – С. 100-108.

11. Ложкина О.В. К вопросу о совершенствовании моделей и методов информационного процесса мониторинга негативного воздействия городского транспорта на окружающую среду // В книге: Комплексные проблемы техносферной безопасности. Научный и практический подходы к развитию и реализации технологий безопасности. Сборник тезисов по материалам XVII Международной научно-практической конференции. Воронеж, 2021. С. 76-77.

12. Ложкин В.Н., Ложкина О.В. Комплексная методология оценки и прогнозирования экологических угроз и социально-экономического ущерба, обусловленных опасным воздействием объектов транспорта и теплоэнергетики на население крайнего севера // Технико-технологические проблемы сервиса. 2019. №1 (47). С. 8-11.

УДК 330.123.6

Лунева Светлана Курусовна
старший преподаватель
Санкт-Петербургский государственный
экономический университет

ВОПРОСЫ БЕЗОПАСНОСТИ УСЛУГ, ИМЕЮЩИХ МАСШТАБНЫЕ СОЦИАЛЬНЫЕ ПОСЛЕДСТВИЯ

Аннотация. В статье рассмотрены вопросы оказания услуг здравоохранения, влияющие на безопасность населения, их особенности. Проанализированы факторы, влияющие на рост объемов платных услуг здравоохранения в России; представлены данные по заболеваемости в России инфекционными заболеваниями в 2018-2019 гг. и показатели экономического ущерба от инфекционных заболеваний в РФ. Для повышения безопасности услуг, имеющих масштабные социальные последствия, предложено совершенствование услуг иммунопрофилактического характера

созданием централизованной системы с единой базы вакцинации, аккумулирующей данные по проводимым мероприятиям иммунопрофилактического характера.

Ключевые слова: безопасность услуг, медицинские услуги, иммунопрофилактические мероприятия, вакцинация, услуги здравоохранения, инфекционные заболевания.

Luneva S.K.
St. Petersburg State Economic University

SAFETY ISSUES FOR SERVICES HAVING GREAT SOCIAL IMPACT

Annotation. The article discusses the issues of providing health care services that affect the safety of the population, their features. The factors influencing the growth of the volume of paid healthcare services in Russia are analyzed; presents data on the incidence of infectious diseases in Russia in 2018-2019. and indicators of economic damage from infectious diseases in the Russian Federation. To improve the safety of services with large-scale social consequences, it is proposed to improve immunoprophylactic services by creating a centralized system with a single vaccination database, which accumulates data on ongoing immunoprophylactic measures.

Keywords: safety of services, medical services, immunization measures, vaccination, health services, infectious diseases.

Одной из наиболее важных социально – экономических вопросов, решаемых на уровне государства, являются вопросы обеспечения безопасности населения, реализующие конституционные права гражданина на охрану здоровья, как одного из важнейших социальных прав. В ст. 41. Конституции РФ закреплены права на охрану здоровья и медицинскую помощь, гарантирующие предоставление услуг здравоохранения каждому гражданину РФ, а также другим лицам, в том числе иностранным гражданам в соответствие с международными договорами, находящимся на территории России [1]. Право на охрану здоровья и оказание медицинской помощи должно обеспечивать возможность получения качественной, квалифицированной, доступной, при необходимости высокотехнологичной услуги здравоохранения.

Поддержание хорошего уровня физического и психического здоровья населения в течение жизни достигается в том предоставлением гарантированной возможности пользования социальными благами в области общественного производства и распределения, выражаемыми в предоставлении необходимой помощи для защиты и поддержания здоровья.

Система здравоохранения является важнейшим элементом сохранения здоровья и жизни населения на высоком уровне, влияет на качество и продолжительность жизни, на показатели инвалидизации и смертности населения. Таким образом услуги здравоохранения можно охарактеризовать как услуги, ориентированными на «поддержание и восстановление здоровья человека» [2]. Особенностью медицинской услуги является то, что потребитель услуги нуждается в ней в определенный момент времени, поэтому услуги здравоохранения могут носить как кратковременный характер, так и долговременный, с потребностью данной услуги в течение длительного периода жизни. Необходимо отметить, что некоторые услуги здравоохранения, оказываемые населению, в силу своих особенностей, а также характера влияния и последствий могут иметь масштабные социальные последствия, воздействуя на здоровье и безопасность значительных слоев населения [3].

Услуги здравоохранения являются одними из наиболее важных услуг. Одним из показателей уровня услуг здравоохранения государства, уровня социально – экономической политики является показатель продолжительности жизни населения. В странах с высоким уровнем развития медицинских услуг, характеризуемой в том числе ее технологичностью, инновационными методами лечения, реабилитации пациентов, продолжительность жизни превышает 80 лет, так в 2019 г. продолжительность жизни в странах составила: в Японии 83,3 года, Гонконг - 83,73 года, Италия - 82,84 года, Швейцария - 82,66 года, Сингапур - 82,64 года [4].

В России продолжительность жизни также постепенно увеличивается и достигла в 2019 году значения 73,4 года, благодаря в том числе предпринимаемым мерам в сфере здравоохранения [5]. Жизненно – необходимость услуг здравоохранения обуславливает постоянное совершенствование системы здравоохранения.

Реформирование системы здравоохранения, предпринимаемое в последние годы, не решило до конца проблем доступности, безопасности, качества оказания услуг. Увеличение объёма платных услуг, демонстрируемое в последние годы в России, представляет их растущую востребованность (Рис. 1) [5].

Анализ структуры объема платных медицинских услуг представляет, что особенно востребованными являются услуги высокотехнологичного характера, которые невозможно получить в государственных лечебно–профилактических учреждениях. Важнейшими факторами обращения в учреждения за платными услугами являются оснащенность медицинского учреждения оборудованием и техникой. Приобретение новой техники, высокотехнологичного оборудования способствует увеличению спектра оказания услуг с целью удовлетворения потребностей потребителей, что в

конечном результате повышает конкурентоспособность медицинской организации, оказывающей платные услуги здравоохранения.

Рисунок 1 – Объемы медицинских платных услуг, млн. руб.

Одними из наиболее востребованными видами услуг являются услуги в области диагностики, стоматологии, гинекологии и урологии, что обусловлено в том числе недофинансированием государственных медицинских организаций, отсутствием вариативности выбора лечения и лекарственных средств, отсутствием современного диагностического оборудования. Все эти факторы способствуют росту платных услуг здравоохранения.

В условиях неуклонного роста объема платных услуг населению возникает необходимость усиления роли государственного контроля предоставляемых медицинских услуг здравоохранения, влияющих на социально – экономические показатели и безопасность значительной части населения.

Увеличение объемов платных услуг связаны также с снижением государственных обязательств по предоставлению населению гарантированной медицинской помощи, связанной с снижением количества больничных коек в медицинских организациях практически по всем направлениям специализации оказания медицинской помощи (Рис. 2, Рис. 3) [5].

Вопросы оказания услуг здравоохранения предполагают обеспечение безопасности больших масс населения, в том числе предоставлением эффективной, доступной и качественной услуги. Проблемы сохранения здоровья, увеличения продолжительности жизни, предотвращение развития массовых инфекционных заболеваний, осложнений и последствий заболеваний – все эти вопросы являются вопросами социально-экономического характера ([6], [7]).

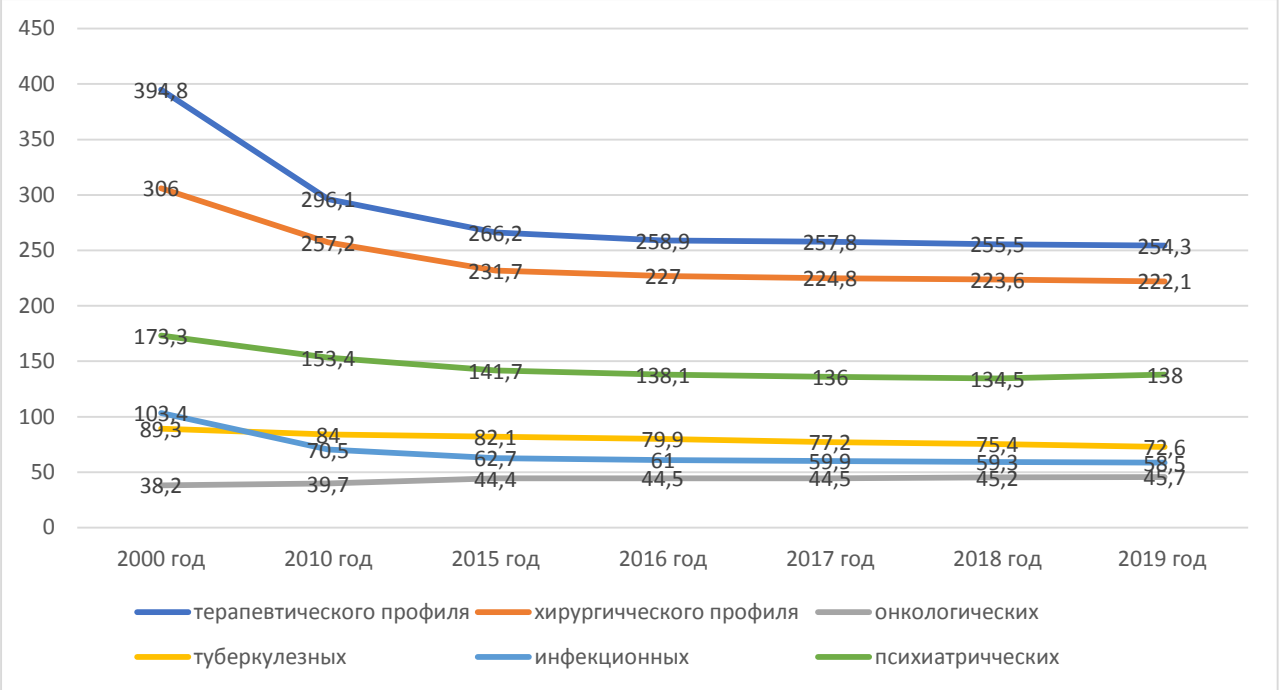


Рисунок 2 – Количество больничных коек в медицинских учреждениях РФ по специализации, тыс. ед. [5]

Рисунок 3 – Количество больничных коек
на 100 тыс. человек населения, ед. [5].

Применение цифровых технологий в медицинские услуги, частичное внедрение высокотехнологичных способов оказания помощи позволили повысить качество и доступность услуг здравоохранения.

Однако несмотря на некоторые успехи в решении вопросов здравоохранения, анализ заболеваемости в нашей стране демонстрирует рост заболеваемости некоторыми, в том числе инфекционными и пара-

зитарными заболеваниями, который остается на высоком уровне по сравнению с развитыми странами. Заболеваемость детей до 14 лет инфекционными и паразитарными заболеваниями в РФ в 2019 г. составила 1792,0 тыс. заболеваний, заняв вторую позицию после заболеваний органов дыхания ([9], [10]).

Данные государственных докладов за 2019-2018 гг. представляют рост экономического ущерба от многих заболеваний инфекционного характера, снижение ущерба в отношении которых возможно проведением иммунопрофилактических мероприятий (Рис.4) ([9], [10]).

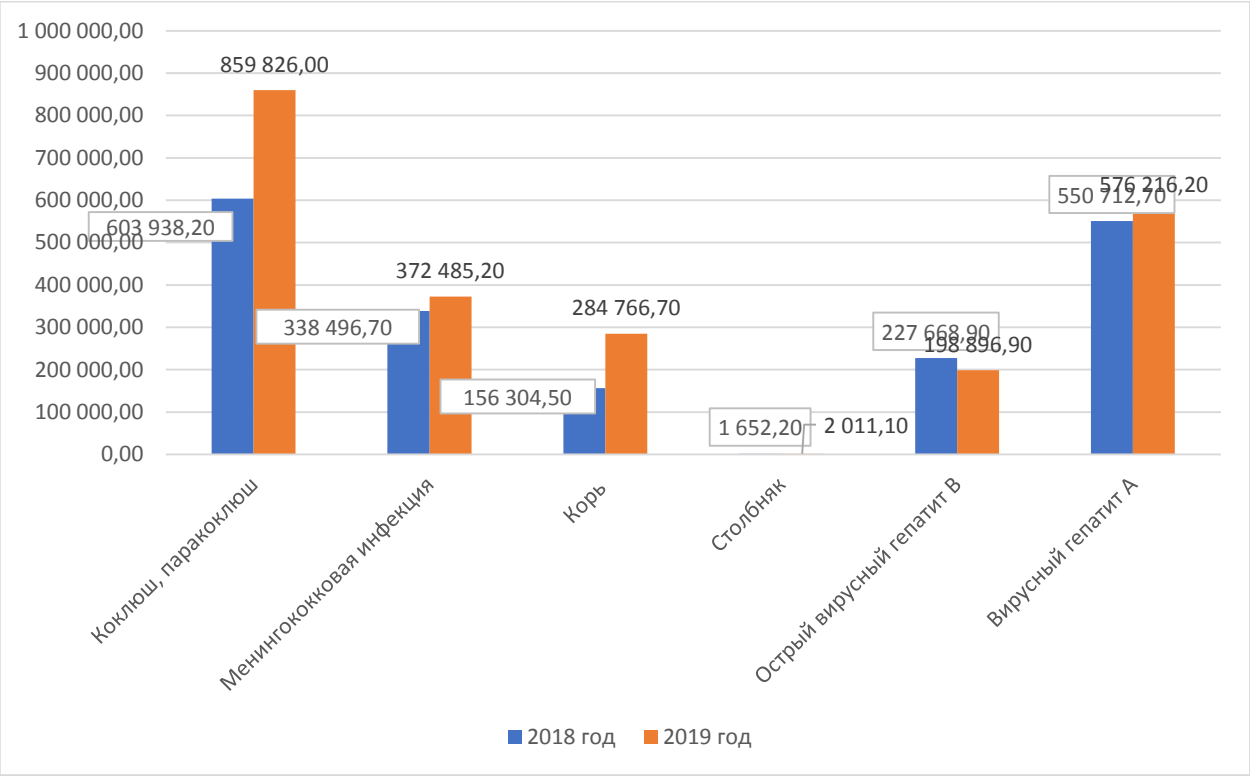


Рисунок 4 – Показатели экономического ущерба от некоторых инфекционных заболеваний в РФ, предотвращаемых вакцинацией в 2018-2019 гг. ([9], [10]).

Практически все нозологические формы демонстрируют рост в 2019 году. Экономический ущерб, нанесенный в 2019 г инфекционными заболеваниями, составил 646 590 653,3 тыс. руб., превысив данные 2018 года на 8 958 149,70 тыс. руб., против данных 2018 года, которые составляли 637 632 503,60 тыс. руб. Ущерб, наносимый экономике государства инфекционными заболеваниям, возможный предотвращением проведением вакцинации в рамках национального календаря профилактических прививок (НКПП) является значительным, но как считают эксперты, наиболее снижение экономического ущерба от инфекционных заболеваний, управ-

ляемых вакцинацией, что еще раз подтверждает экономическую эффективность данных мероприятий [8].

Необходимо отметить, что ущерб, наносимый экономике государства нозологическими формами, в отношении которых существуют вакцины, но не вакцинируемых в рамках НКПП является в настоящее время значительным. На Рис.5 представлены данные экономического ущерба за 2019 год в отношении значительных нозологических форм.

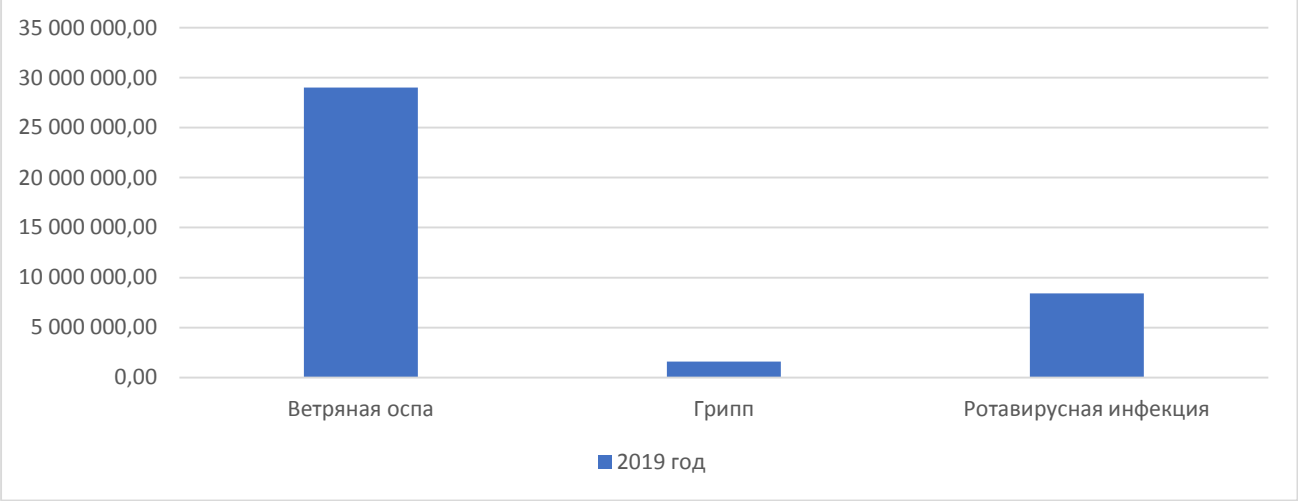


Рисунок 5 – Показатели экономического ущерба от некоторых инфекционных заболеваний в РФ за 2019 гг. ([9], [10]).

Увеличение экономического ущерба свидетельствует о некоторых проблемах, возникающих в борьбе с той или другой нозологической формой, рост заболеваемости в разных возрастных категориях дает возможность анализа причин, что может быть также обусловлено ростом непривитых лиц. Большинство заболеваний инфекционного характера возможно предотвратить своевременной вакцинацией.

По данным ВОЗ проведение иммунопрофилактики дает возможность сохранения от 2 млн. до 3 млн. жизней, избежать инвалидизации, связанной с осложнениями, вызванными с протеканием заболевания. Именно вакцинация является наиболее экономически выгодной мерой обеспечения безопасности населения [4].

Мероприятия иммунопрофилактического характера, проводимые многими странами в рамках НКПП, дают возможность повысить безопасность населения, снизить не только заболеваемость, но и негативные последствия, связанные с последующими осложнениями, вызванными протеканием инфекционных заболеваний [7].

Новые угрозы, связанные с развитием неблагополучной эпидемиологической ситуацией, вероятностью возникновения новых инфекционных

заболеваний, показали важность дальнейшего совершенствования системы услуг здравоохранения, в том числе и иммунопрофилактического направления, направленных на повышение безопасности населения.

Вакцинация, являясь наиболее эффективным средством защиты от заболеваний, также способствует поддержанию коллективного иммунитета, служащего защитой для всего населения, в том числе и не имеющего возможности вакцинироваться вследствие определенных особенностей здоровья.

Одним из важнейших направлений деятельности в сфере здравоохранения населения и охраны здоровья является обеспечение безопасности населения, в том числе предоставлением безопасных услуг [7]. Проблемы безопасности предоставления услуг здравоохранения касаются не только самого потребителя услуг, но и сама услуга и результат этой услуги, могут оказать влияние на большие социальные группы, иногда не связанных с получателем услуг устойчивыми социальными отношениями [4].

Современное общество, характеризуется высоким уровнем урбанизации, представляющий концентрацию населения на определенных территорий, что предполагает необходимость принятия мер по обеспечению безопасности населения предотвращением развития эпидемиологических процессов. Также одним из факторов распространения заболеваний является возможность перемещений или миграция больших групп населения, что также активизирует процессы переноса и распространения заболеваний.

Для повышения безопасности услуг предлагается совершенствовать систему услуг созданием единой базы вакцинации, аккумулирующей данные по проведенным мероприятиям иммунопрофилактического характера с возможностью доступа всем заинтересованным лицам [3].

В настоящее время отсутствие единой базы, отсутствие единого контроля, несогласованность действий сотрудников медицинских организаций различной организационно – правой формы, выдача недействительных справок и медицинских отводов, отсутствие альтернативности услуги, отсутствие квалифицированной консультации, поствакцинального сопровождения пациента – эти и другие причины способствуют снижению качеству и безопасности услуг, нарушения в оказании которых могут привести к масштабным социальным последствиям [3].

Централизация информационной базы будет способствовать повышению безопасности населения путем содержания достоверных данных, прозрачности, объективности данных, открытого доступа заинтересован-

ных лиц в получении необходимой информации в системе, что снизит недостоверность и фальсификацию данных и источников, повышением личной ответственности.

Литература

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).
2. Лунева С.К. О вопросах безопасности оказания услуг здравоохранения, имеющих масштабные общественные последствия // Технико-технологические проблемы сервиса. 2021.- №1 (52), с.73-78.
3. Константинова Н. Н, Лунева С.К., Малинин А.М. Некоторые аспекты формирования новой системы оказания медицинских услуг, имеющих масштабные общественные последствия (на примере иммунопрофилактики инфекционных болезней) // Технико-технологические проблемы сервиса. 2019.- №3.
4. Всемирная организация здравоохранения (ВОЗ). [Электронный ресурс]. - URL: https://www.who.int/ru
5. Федеральная служба государственной статистики. [Электронный ресурс]. - URL: https://rosstat.gov.ru).
6. Федеральный закон от 21.11.2011 № 323-ФЗ (ред. от 29.05.2019) «Об основах охраны здоровья граждан в Российской Федерации». [Электронный ресурс]. - URL: http://www.consultant.ru/document/cons_doc_LAW_121895/
7. Лунева С.К. Некоторые аспекты оказания услуг здравоохранения, имеющих масштабные общественные последствия // Технико-технологические проблемы сервиса. 2021.- №1 (52). - С.73-78.
8. Михеева М.А., Михеева И.В. Динамика рейтинга экономического ущерба от инфекционных болезней как критерий эффективности эпидемиологического контроля. Журнал микробиологии, эпидемиологии и иммунобиологии. 2020; 97(2): 174-181. [Электронный ресурс]. – DOI: https://doi.org/10.36233/0372-9311-2020-97-2-174-181
9. Государственный доклад «О состоянии санитарно-эпидемиологического благополучия населения в Российской Федерации в 2019 г.». [Электронный ресурс]. – URL: https://rospn.gov.ru
10. Государственный доклад «О состоянии санитарно-эпидемиологического благополучия населения в Российской Федерации в 2018 г.». [Электронный ресурс]. - URL: https://rospn.gov.ru

УДК 323

Мартынов Василий Львович
д-р геогр. наук, профессор
Российский государственный педагогический
университет им. А.И. Герцена
Алексеева Ольга Владимировна
канд. геогр. наук, доцент
Ленинградский государственный
университет им. А.С. Пушкина

ГОСУДАРСТВЕННАЯ СИМВОЛИКА И ЕЕ РОЛЬ В МОДЕЛИРОВАНИИ НАЦИОНАЛЬНОЙ ИДЕНТИЧНОСТИ

Аннотация. Одним из главных символов государственности является флаг. Государственная символика России в виде флага, переживала свое становление эпизодически, в соответствии с политическими изменениями и внешней политикой страны. Неотъемлемой чертой моделирования государственности является национальная идентичность, благодаря которой в том числе современная Россия сохраняет богатство культурного и языкового разнообразия. Национальная идентичность («гражданственность») предполагает общность политических принципов и институтов на территории всех регионов России.

Ключевые слова: государственная символика, национальная идентичность, трансформация флага.

STATE SYMBOLS AND THEIR ROLE IN NATIONAL IDENTITY DEVELOPMENT

Martynov V.L.
Herzen State Pedagogical University of Russia
Alekseeva O.V.
Pushkin Leningrad State University

Annotation. One of the main symbols of statehood is the flag. The state symbols of Russia in the form of the flag, experienced their formation episodically, in accordance with political changes and foreign policy of the country. The national identity of modern Russia allows us to preserve the richness of cultural and linguistic diversity of Russia. National identity is an essential feature of the model of statehood. National identity ("citizenship") implies the commonality of political principles and institutions on the territory of all Russiat regions.

Keywords: state symbols, national identity, flag transformation.

В данной статье рассматривается главный символ государственности – государственный флаг, его зарождение и преобразование в период становления и развития российской государственности. Сформированная на сегодняшний день в России национальная идентичность позволяет сохранять богатство культурного и языкового разнообразия страны. Национальную идентичность следует рассматривать в современном контексте развития России, как и «гражданственность», которая является неотъемлемой чертой моделирования государственности. Российская идентичность позволяет объединять многонациональное российское общество, напомним по данным последней переписи населения 2010 г., этнический состав населения составил 190 народностей [1, с. 48]. Одним из главных символов государственности является флаг. Именно флаги представляют собой символы государственного суверенитета [2]. Как утверждает Г. Элгениус, «Появление национальных флагов представляет собой маркеры государственного строительства и отражает политические перемены» [3]. Государственная символика России в виде флага, переживала свое развитие эпизодически, в соответствии с политические изменениями и внешней политикой страны. Становление государственных символов, страны происходило медленно в результате сохранения в российском обществе феодальной структуры до конца XIX века. Флаг России с момента своего зарождения трансформировался под воздействием как внешних, так и внутренних географических условий развития Российского государства. Национальную идентичность следует рассматривать в современном контексте развития России, как и «гражданственность», которая является неотъемлемой чертой моделирования государственности. Национальная идентичность («гражданственность») предполагает общность политических принципов и институтов на территории всех регионов России, в том числе в 22 республиках, где титульной нацией выступает не русская национальность. По мнению Г. Эльгениуса, «появление национальных флагов представляет собой маркер государственного образования и отражает политические изменения» [3, с. 28]. Каждая республика России имеет свой республиканский флаг.

Исследованиями флагов и флажной системы занимается научная дисциплина, которая называется вексиллология. Термин «вексиллология» был впервые предложен в 1958 году американским учёным Уитни Смитом, и наибольшего развития вексиллологические исследования получили именно в США, где выходят научные журналы и существуют учёные общества вексилоллогов, издаётся научная литература по этой тематике. Флаг США действительно один из сильнейших символов государственности, если рассматривать его в сравнение с другими суверенными государ-

ствами. «Флаговедение» в качестве научной дисциплины рассматривалось уже в начале XX века в трудах российского исследователя флагов П.И. Белавенца, но его исследования в России после 1917 года не использовались, а в других странах они так и остались неизвестны [4]. Родиной флагов является Европа - для ее небольших государств необходимо было использовать символы, составленные более или менее по единому стандарту и позволяющие разделить инсайдеров («нас») и аутсайдеров («их»). Для понимания того, как и когда появились те или иные флаги, требуются главным образом историко-географические изыскания. Изучение того, как эти флаги используются в современном мире, требуется применение социально-географических, культурно-географических, политико-географических, а иногда и экономико-географических подходов.

Современная система мирового флага сложилась в условиях европейской цивилизации, в результате изменений социальных и экономических образований, где феодальная «Европа социальных категорий», с гербом в качестве главной символики, стала буржуазной «Европой народов», где флаг стал главным символом. Для флагов большее значение имели природные, экономические и политические характеристики государств и территорий, например, наличие и уровень развития ткацкого производства, наличие природных красителей для определенной территории, границы и отношения с другими государствами. С технической точки зрения «рождение флагов» обусловлено двумя обстоятельствами. Первым из них стало широкое распространение шерстяных тканей в Европе, в то время основным производителем была Фландрия, а затем Англия. Поэтому для изготовления флагов использовалась специальная разновидность шерстяной ткани, называемая «флагшток». Второе обстоятельство - географические открытия направили импорт новых натуральных красителей из Южной Америки и Восточной Азии в Европу. Шерстяные ткани и красители из заморских стран в конце XVI - начале XVII веков «сходятся» в Нидерландах. Первый в мире флаг был поднят жителями Нидерландов (Республики объединенных провинций) во время освободительной войны против Испании. Британский флаг можно считать вторым в мире. В то время Голландия и Великобритания начинали бороться за господство в мировых морских коммуникациях, поэтому им необходим был флаг, чтобы отличать свои корабли от кораблей противника, а также отличать их от кораблей бывших хозяев мирового океана - Испании и Португалии. Третьим национальным флагом в мире является флаг США. Впервые он был поднят во время Революционной войны, как «антагонист» английского флага. Цвета американского и британского флагов одинаковы, но узоры различаются. Впервые в истории цивилизации он воспринимается не только как

государственный символ, но и как символ нации, более того, в это время флаг становится главным национальным символом. Четвертый национальный флаг Франции, он был сформирован во время Французской революции. После этой революции флаг воспринимался как необходимость для каждого государства, таким образом, началось формирование системы флагов.

Согласно мнению М. Пастуро, флаг «олицетворяет или имеет смысл только в том случае, если его сравнивают или противопоставляют другим флагам» Географический характер любого национального, регионального, городского или другого флага заключается только в «сравнении или контрасте». Визуализация», как правило, становится важным вопросом в вексиоллогеографических исследованиях, в то время как символы государств, регионов и городов, в первую очередь представленные флагами, появляются в качестве «нового начала» этих изображений» [5, с. 128]. Культурная география применяет также культурную политику изображений [6]. Однако изучение государственной символики с точки зрения «сравнения или контраста», предложенное М. Пастуро, показывает интересные и необычные результаты.

В Европе, в частности, некоторые флаги характеризуются как «зеркальные» («флаг-отражение»). В качестве примера можно привести историю флагов Англии и Дании, которая, скорее всего, начинается в то время, когда эти государства находились в конфликте друг с другом. Цвета польского и бранденбургского флагов возникли на их гербах, для Польши это белый орел на красном поле, а для Бранденбурга - красный орел на белом поле. История «зеркальных» флагов произошла во время событий 11-13 веков до н.э., когда немцы вытеснили славянские племена с границ нынешней Восточной Германии. Поэтому на территориях, вовлеченных в боевые действия германских и славянских народов, родились новые государства, ставшие соответственно Бранденбургом (ныне часть Германии) и Польшей. Установление официального государственного флага российской нации было долгим и сложным. В настоящее время флаг Российской Федерации основан на последнем флаге Российской империи. Впервые этот флаг возник в конце XVII века, во время правления Петра I. Первоначально он появился в виде знака, который Петр I поднял на первых российских кораблях, он фигурировал в истории как «Царь Московский флаг». Основой этого знака стало изображение герба Московского царства - Золотого двуглавого орла, вышитого на фоне трех полос - белого, синего и красного. Почему именно это цветовое сочетание было выбрано, точно не известно, более того, этому выбору нет объяснения. Но сочетание белого, синего и

красного цветов флага было одним из самых распространенных в то время, можно легко предположить, что это было связано с преобладанием натуральных красителей, как растительных, так и минеральных, которые позволяли окрашивать ткань в эти конкретные цвета. Бело-голубые-красные знамена зародились еще в детстве Петра I, что хорошо объясняется появлением в 1693 году на его морских судах больших игрушек, состоявших из этих цветов так называемого «Флага Царя Московского». Уже в ходе Нарвской битвы (1700 г.) значительная часть петровских войск сражалась под трехцветными знаменами с вышитым двуглавым орлом. Большое количество этих знамен после поражения в Нарве выпало на долю шведов, эти «доказательства» до сих пор есть на картинах, поэтому мы точно знаем, как они выглядели [7].

В первые годы правления Петра I эти знамена широко использовались. Но в 1720 году бело-голубо-красный флаг без изображения двуглавого орла был объявлен купеческим. Торговые флаги в то время не воспринимались как государственные символы. Белый флаг с синим косым крестом - военно-морской флаг России, известный как «Андреевский флаг» (флаг Андрея Первозванного, считавшегося святым покровителем России). Белый цвет флага был выбран по нескольким причинам. Прежде всего, белый цвет имитировал морской флаг Французского королевства. Петр I был найден во Франции, он пытался скопировать Францию различными способами. Создание Петергофского парка фонтанов в Санкт-Петербурге, как имитация Версаля. Вторая причина, по которой белый флаг резко отличался от флагов противников флота на расстоянии. Главным военно-морским врагом России на Балтике была Швеция. Шведский флаг был синим с золотым прямым крестом (этот флаг остался прежним), а главным врагом в Черном море была Османская империя, для него использовались красные военно-морские флаги с полумесяцем и звездой. Императорский военно-морской штандарт был основан на новом гербе России - черном двуглавом орле на золотом поле. Это цветовое сочетание было взято из Священной Римской империи германской нации, так как в 1721 году Россия также провозгласила себя империей, в то время второй по величине в Европе. От Священной Римской империи германской нации Российская империя приняла систему титулов, воинских званий и различных символов (государственных, городских, дворянских и т.д.).

На протяжении XVIII и большей части XIX вв. главным символом феодальной Российской империи был герб; государственного или национального флага вообще не существовало. В 1858 году указом императора Александра II был объявлен «цветной герб империи» - черный, золотой и белый [8, с. 264].

Рисунок 1 – Флаг герба Российской империи 1858 - 1883 гг.

Считается, что указ о цветах герба привел к появлению первого в истории России государственного флага, но в самом указе о флаге ничего не сказано. Вышеупомянутые цвета были предписаны для украшения зданий в праздничные дни. До начала 1880-х годов Российская империя считала Пруссию, Австрию и другие германские государства своими главными союзниками. Так, черно-золотисто-белый «флаг гербового цвета» 1858 года похож на черно-красно-золотой «флаг германского единства», официально поднятый при провозглашении Германского союза в 1848 году. Только в первых «цветах гербов» Российской империи красный революционный цвет был заменен на «цветы флага гербов». После присоединения Александра III с 1883 г. для этой же цели требовались белый, синий и красный цвета («убранство зданий») [9]. Смена цветов флагов или гербов обычно ассоциировалась с изменением внешнеполитической направленности России. С начала 1880-х годов главным союзником России стала Франция, чей флаг полностью совпадал по цвету с российским купеческим флагом на кораблях, отличавшимся лишь положением полос. Впоследствии к франко-российскому союзу присоединилась Великобритания, флаг которой также отличается сочетанием белого, красного и синего цветов. Таким образом, сочетание белого, синего и красного цветов становится общим для флагов всех трех основных стран Антанты. В 1898 году указом императора Николая II белый, синий и красный флаги были объявлены «национальным флагом во всех случаях» [10]. Следует отметить, что Россия в тот период прошла через большие трудности в переходе от феодализма к капитализму, вопрос о флаге мало волновал государство и не представлял интереса для общества. Ни черно-золото-белый, ни бело-сине-красный флаги не воспринимались населением Российской империи как репрезентация страны, в отличие от ее герба с двуглавым орлом. Почти полное отсутствие интереса к государственному флагу подтверждается тем фактом, что ни одно российское дореволюционное произведение искусства не посвящено ни одному флагу Российской империи. Флаги, которые воспринимаются как символ нации, как правило, являются предметом многих произведений искусства всех видов. Самым известным

примером в этом отношении является флаг США, даже его гимн является «пением» флага.

Однако в начале XX века интерес к флагу России возрос, как в силу внешних, так и внутренних обстоятельств. В силу внешних обстоятельств Россия активно участвовала в империалистическом разделении мира как один из ключевых игроков, и она становилась просто необходимостью национального флага, символа, похожего на флаги других империалистических государств. Внутренние обстоятельства на рубеже XIX-XX веков - центробежные тенденции внутри империи усиливались, движимые быстрым развитием этнических и общественных движений. Каждое или почти каждое из этих движений стало использовать свой собственный флаг, наиболее распространенным из которых был обыкновенный красный. Хранителям «государственного единства и политического порядка требовался флаг, под которым они могли демонстрировать свою преданность империи. Белый, синий и красный флаг, который еще в начале правления Николая II (1896 г.) служил «праздничным украшением», с каждым годом становился все более востребованным, приобретая функцию национального флага.

Во время Февральской революции в 1917 году использовался красный флаг, который затем предлагалось превратить в государственный флаг. Однако Временное правительство сохранило белый, синий и красный флаги, полагая, что вопрос о государственном флаге, как и другие вопросы государственной жизни России, будет рассматриваться Учредительным собранием. Учредительное собрание, собравшееся в начале 1918 года, было немедленно распущено большевиками и не решило ни одного вопроса, в том числе вопроса о государственной символике. Во время Октябрьской революции 1917 года вновь были подняты красные флаги. Красное полотно без гербов, символов и герба де-факто являлось флагом Советской России с момента его появления до весны 1918 года. После подписания Брест-Литовского мирного договора, который предусматривал, среди прочего, установление дипломатических отношений между Советской Россией и государствами «четвертого Союза» (Германия, Австро-Венгрия, Османская империя, Болгария) и Украиной, возникла неожиданная проблема - красный флаг сам по себе не мог представлять Советскую Россию за ее пределами, красный флаг не обозначал ни одну страну. В июне 1918 года был создан новый флаг для использования небольшим количеством иностранных представительств РСФСР. Это был золотой красный флаг, стилизованный под славянскую письменность, буквы «РСФСР» (расшифровка аббревиатуры: «Российская Социалистическая Федеративная Советская Республика»).

Рисунок 2 – Флаг Российской Социалистической Федеративной Советской Республики 1918 - 1937 гг.

С тех пор сохранилось сочетание красного и золотого цветов, присущее всем флагам советской эпохи. Это сочетание цветов раньше использовалось на царских флагах до-Петровского времени, а после 1918 года, между прочим, это сочетание не использовалось ни на каких российских флагах или знаменах. С точки зрения географического подхода, возвращение к допетринским основам государственной жизни проявилось в возвращении российской столицы в Москву. Таким образом, красно-золотое цветовое сочетание, впоследствии использованное всем мировым коммунистическим движением, имеет свои истоки в средневековой московской символике. Красно-золотое облачение, которое использовалось православными священниками на пасхальных службах, и, возможно, это отражает тот факт, что красно-золотой флаг прочно утвердился как «главный» флаг страны, несмотря на то, что его символика в советском обществе была далека от христианской [11].

Советская символика, в частности, основывалась на использовании христианских ценностей, но в искаженном виде. Вместо креста использовался перекрещивающийся молот и серп. Так, буквальное обожествление вождей революции (день памяти В.И. Ленина изначально был днем его смерти как христианского святого, а не дня рождения), а также красные и золотые флаги, напоминающие о красной и золотой символике Воскресения Христова. В 1922 году был образован Союз Советских Социалистических Республик и его флаг. Следует отметить, что Союз Советских Социалистических Республик, был единственной страной в истории человечества, не имевшей географического указания в своем названии. Впервые этот флаг был описан в 1924 году в Конституции СССР как красный или алый флаг с золотым изображением серпа и молотка и красной звездой.

Рисунок 3 – Флаг СССР фактически по 1922 г., законодательно 1924-1991 гг.

В 1937 году слово «алый» исчезло из описания флага, оставив только «красный». Этот флаг стал широко известен не только как национальный флаг, но и как «международный» флаг всех коммунистов мира. В Советском Союзе вплоть до его распада в 1991 году использовался комбинированный флаг красно-золотого цвета с золотым изображением серпа и молотка, а также красной звезды. В Российской Федерации в период переформатирования три флага использовались разными политическими силами. Красный флаг был флагом сторонников Советской власти, бело-сине-красный флаг использовался «демократическими» силами, черно-золото-белый флаг - националистами. В итоге в 1990-е годы были созданы флаги субъектов Федерации, многие из них принимали флаги в зависимости от политических предпочтений населения – «прокоммунистические» регионы выбирали флаги на основе флагов советского времени, «демократические» - на основе белого, синего и красного флагов. Однако были и другие подходы к созданию региональных флагов. Например, Москва и Санкт-Петербург приняли «гербовые цвета» красных флагов, фон городских гербов в обоих городах был красным с XVIII века. В целом в России не существовало и не существует системы создания региональных или муниципальных флагов.

В августе 1991 года был принят «исторический флаг России» бело-лазурного и алого цвета (впервые в истории России).

Рисунок 4 – Флаг России 1991-1993 гг.

Под этим флагом Российская Федерация в 1992-1993 гг. пережила один из самых сложных периодов своей истории. В ходе вооруженного противостояния сторонников Президента Ельцина и Верховного Совета РСФСР в начале октября 1993 года этот флаг использовался обеими сторонами. Однако сторонники Верховного Совета использовали и другой черно-золотисто-белый флаг, который в 1990-е годы по непонятным причинам стал известен как «флаг императорских цветов» [10, с. 213]. В декабре 1993 г. флаг Российской Федерации был изменен. Об этом изменении, как и обо всех предыдущих, российские граждане были только извещены. После политического события октября 1993 года утверждение государственного флага путем демократических процедур было рискованным по разным причинам.

Рисунок 5 – Государственный флаг Российской Федерации,
с 1993 года по настоящее время

Технически флаг почти полностью изменился по сравнению с версией флага 1991 года с «лазурным и алым». Сочетание красного и золотого цветов исторически значимо для России. Для значительной части населения России эпоха СССР была «золотым веком», а сама современная Россия воспринималась как «государство-продолжатель» Советского Союза. Флаг СССР воспринимается как один из главных символов победы в Великой Отечественной войне 1941-1945 годов, а флаг, который 12 апреля 1961 года вывел в космос Ю. Гагарин.

Официально белый, синий и красный флаг был утвержден только в декабре 2000 года Федеральным конституционным законом «О Государственном флаге Российской Федерации». В то же время в гербе Российской Федерации сохранено сочетание красного и золотого цветов, которое сначала сформировалось в символах до Петровского Московского государства, а затем исчезло, возродившись впоследствии как основное цветовое сочетание советской символики. Полагаем, что если в силу каких-то обстоятельств в Российской Федерации появится «флаг гербов», то он будет повторять цвета флага СССР.

Восприятие действующего флага Российской Федерации на современном этапе неоднозначно. Для старшего поколения трехцветный флаг не является «родным», и ими воспринимается, как слабый национальный символ, иногда даже «негативный», в ряде случае и не является предметом гордости. Напротив, для подрастающего поколения государственный флаг является первостепенным национальным символом, которым гордятся.

Заключение

На основе вышесказанного, следует сделать вывод. Флаги – отличительные национальные символы западноевропейской цивилизации, впервые появившиеся в капиталистическую эпоху, представляют собой факт «буржуазно-национального» этапа развития общества, факт становления государственности. Сохранение до конца XIX века преимущественно феодальной структуры российского общества привело к очень медленному формированию нации, ее национальной символики, национальной идентичности, в том числе и флага. Первые флаги появились в России в начале XVIII века.

Бурный переход от «феодализма к социализму» привел к формированию советской символики, природа этих символов была формально идеологической, а не национальной, но в то же время эти символы основывались на цветовых сочетаниях предпетербургского периода Московского царства (Царства России). Советский общественный строй был ликвидирован в начале 90-х годов XX века, были созданы новые государственные символы. В результате современная национальная символика Российской Федерации сочетает в себе «дореволюционный» бело-сине-красный флаг и красно-золотой герб (которые являются цветами советской эпохи). Трехцветный флаг современной России является «молодым» национальным символом, несмотря на этот факт, сформированная в Российской Федерации национальная идентичность позволяет сохранять богатство культурного и языкового разнообразия.

Литература

1. Экономическая и социальная география России. География экономических районов России, под. Ред. Бабурина В.Л. Ратанова М.П. Ленанд, 2017, 640
2. Опрятов В. И. Геральдика и вексиллология как науки о государственных символах и их соотношение с конституционным правом // Ученые записки Орловского государственного университета. Серия: Гуманитарные и социальные науки. 2011. №2 (40). - С. 177 – 180
3. Elgenius G. National Flag Origins: Religion, Revolution and Rivalry. // Symbols of Nations and Nationalism. London Palgrave Macmillan, 2011. - С. 25 – 50. DOI: 10.1007/978-0-230-31704-8_3
4. Белавенец П.И. Краткая записка о старинных русских знамёнах. СПб.: Сенатская типография. 1911. 78 с.
5. Пастуро М. Символическая история европейского Средневековья (перевод с французского). СПб.: Александрия, 2012. С. 279
6. Rose G. (2016). Cultural geography going viral. Social and Cultural Geography,17, 763-767. [Электронный ресурс]. – URL: https://www.tandfonline.com/doi/full/10.1080/14649365.2015.1124913
7. Григорьев А. А. Роль знаков, символов и образов в географическом страноведении // Вестник СПбГУ. Науки о Земле. 2009. №3.
8. Полное собрание законов Российской империи. Собрание 1825 – 1881 годов. Т. 33. С. 752. №33289.
9. Указ Президента Российской Федерации №2126 от 11 декабря 1993 года «О государственном флаге Российской Федерации

10. Полное собрание законов Российской империи. Собрание 1881 – 1913 годов. Т. 16. Ч. 1. №12858.

11. Martynov V. L., Sazonova I. Ye. Socio-geographical and Socio-philosophical Approaches to the Study of Vexillological Problems // Humanitarian Vector. 2020. Vol. 15, No. 2. PP. 121–130. DOI: 10.21209/1996-853-2020-15-2-121-130.

УДК 33: 338: 339: 332

Пастухов Александр Львович
канд. фил. наук, доцент
Российская академия народного хозяйства и
государственной службы при Президенте Российской Федерации
Северо-Западный институт управления

ЭКОЛОГО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ В КОНТЕКСТЕ РЕАЛЬНОЙ ЭКОНОМИКИ

Аннотация. Статья посвящена развитию экономики, основанному на управлении и учете экологических последствий хозяйственно-экономической деятельности в контексте обеспечения национальной безопасности, ресурсосбережения и устойчивого развития.

В ней представлены концептуальные аспекты экономического развития на основе инноваций в сфере экологии и рационального природопользования, а также рассмотрены вопросы экологической политики предприятий.

Ключевые слова: экология, экономика, ресурсосбережение, экологическая безопасность, национальная безопасность, инновации, устойчивое развитие, экономическое развитие, циркулярная экономика.

Pastukhov A.L.
The Russian Presidential Academy of National Economy
and Public Administration, North-West Institute of Management

ENVIRONMENTAL-ECONOMY SECURITY IN THE CONTEXT THE REAL ECONOMY

Annotation. The article is devoted to the development of the economy, based on the management and accounting of the environmental consequences of

economic and economic activities in the context of ensuring national security, resource saving and sustainable development.

It presents conceptual aspects of economic development based on innovations in the field of ecology and environmental management, as well as issues of environmental policy of enterprises.

Keywords: ecology, economy, resource conservation, environmental security, national security, innovation, sustainable development, economic development, circular economy.

В настоящее время перед человечеством встает проблема выживания. В экономически развитых странах применяющаяся ранее парадигма социально-экономического развития меняется на новую парадигму устойчивого развития, включающую взаимосвязь развития общества и экономики с поддержанием стабильности окружающей среды.

Более того, сохранение стабильности окружающей среды начинает рассматриваться как системообразующий фактор социально-экономического развития, а экологическая составляющая хозяйственной деятельности – не только как товар, но и как капитал.

Следует отметить, что еще в 1934 году Л. Браун, один из идеологов концепции устойчивого развития, создал Институт всемирного наблюдения, а затем некоммерческой организации Earth Policy Instituteruen (США) для выявления и анализа экологических проблем развития общества.

В нескольких своих научных трудах он указывал, что проблемы экологии могут привести к продовольственному кризису в развивающихся странах с большой численностью населения, что в свою очередь создает угрозы в сфере продовольственной безопасности [1, с. 12; 2, с. 30].

В 1972 году в рамках Организации объединенных наций была принята программа по окружающей среде (UNEP): «Окружающая среда в интересах развития» [3].

Основными направлениями реализации данной программы являются:

- выявление конфликтных ситуаций, связанных с антропогенным воздействием и использованием природных ресурсов; их анализ и оценка уровня угроз;

- внедрение экологической политики в политическую систему стран мира, включая комплекс мер по ограничению роста антропогенного воздействия на окружающую среду, а также принятие экологической политики на уровне субъектов хозяйственно-экономической деятельности;

- создание и внедрение новых технологий, открытие новых производств с целью сохранения природных ресурсов и рационального природопользования;

- развитие регионального и межрегионального (межстранового) сотрудничества в вопросах экологии, управления климатом и ресурсосбережения, а также ресурсораспределения;

- развитие правового института экологии;

- глобальная защита окружающей среды;

- поддержка общественного сектора в сфере экологии и ресурсосбережения.

В 1988 году Всемирный банк начал разрабатывать институциональную систему устойчивого развития. Один из разработчиков концепции экономики устойчивого развития Г. Дейли в 1988-1994 годах сформулировал принципы экономики устойчивого развития, которые был приняты Всемирным банком и отражены в его нормативных документах, как, например, «Социльно-экологичекие принципы Всемирного банка» [4, с. 102; 5, с. 15].

В 1987 году Роберт Констанца создал Международное общество экологической экономики и сформулировал ее основные положения.

В Российской Федерации вопросам экологии посвящены научные труды отечественных ученых М. Игнатьевой, А. Козицина, О. Романовой, Н. Реймерса и др., а важнейшие аспекты, связанные с государственной экологической политикой рассмотрены в работах А.В. Яблокова.

В контексте выраженной тенденции повышения значимости экологической проблематики в мировом сообществе следует обратить внимание на вопросы обеспечения экологической безопасности Российской Федерации в контексте национальной безопасности с учетом взаимосвязи и взаимодействия органов государственной власти Российской Федерации и государственных административных структур управления с региональными органами государственной власти, органами местного самоуправления и общественностью, а также субъектами хозяйственно-экономической деятельности с целью реализации государственной экологической и экономической политики.

При этом, под термином «экологическая безопасность», по нашему мнению, следует понимать состояние защищенности человека и окружающей среды от различных негативных природных и антропогенных факторов воздействия в настоящем и будущем, которое должно обеспечиваться системой экологической безопасности: сочетанием политико-правовых, экономических, технико-технологических, финансовых, социокультурных институтов, включающей в себя комплекс взаимосвязанных решений, мероприятий и действий по выявлению, локализации, минимизации соответствующих угроз возникновения ситуаций природного и техногенного характера.

Обеспечение экологической безопасности включает в себя оценку экологического состояния окружающей среды определенной территории, ее мониторинг и управленческие решения и является частью экологической политики государства, а также корпоративной политики предприятий, основанной на определенных принципах, целях и задачах.

Под эколого-экономической безопасностью следует понимать защищенность интересов человека, общества и окружающей среды (природы) от негативного воздействия процесса и результатов индивидуальной и коллективной (совместной) хозяйственно-экономической деятельности человека в настоящем и будущем, в том числе учет интересов и жизненно важных потребностей будущих поколений.

При этом следует отметить, что для обеспечения устойчивого развития хозяйственных связей необходима соответствующая нормативно-правовая база, регламентирующая и регулирующая совокупность хозяйственно-экономических отношений, учитывающая разделение целей, задач и полномочий соответствующих органов власти в зависимости от территориального разделения и группировки:

- территория страны и все, что находится в исключительной экономической зоне страны, включая материковый шельф, острова и сооружения;
- территория региона и муниципального образования в рамках определенной границы;
- территория населенного пункта и городская агломерация (обычно в радиусе 100-200 километров от крупного населенного пункта).

К ресурсам, обеспечивающим эколого-экономическую стабильность и возможность реализации жизненно важных интересов личности и общества относятся не только природные ресурсы (земля, воздух, леса и т.д.), но и земная поверхность, водная акватория в исключительной экономической зоне страны, растительный и животный мир, семенной фонд, недра и подземные воды, воздушное и космическое пространство.

Для обеспечения эколого-экономической безопасности важно формирование инновационной модели экономического развития, основанного не на традиционном экономическом подходе максимизации прибыли, а на закономерностях эколого-экономического развития, с учетом следующих аспектов:

- результативность и оптимальность экономической деятельности;
- эффективность функционирования предприятий, производственных объединений, в том числе кластеров и технопарков;
- соотношение выгоды и отрицательного воздействия на окружающую среду в результате хозяйственно-экономической деятельности.

Инновационное развитие на местном, региональном и национальном уровнях предполагает использование всего комплекса ресурсного потенциала для обеспечения технологического роста и повышения конкурентоспособности. При этом инновационная система Российской Федерации может быть рассмотрена как комплекс институтов, функционирующих в экономической, политической, технико-технологической и социокультурной средах. В ее задачи в том числе входит и обеспечение эколого-экономической безопасности на различных уровнях:

1. Стабильность для реализации необходимых изменений.
2. Восприимчивость к изменениям.
3. Адаптивность на уровне управляющих систем.

Для обеспечения устойчивого развития необходимы:

1. Распределение функций, полномочий, обязанностей и меры ответственности по обеспечению экологической и эколого-экономической безопасности в рамках территории местного самоуправления, региональном или национальном уровне.
2. Обеспечение воспроизводства возобновляемых природных ресурсов.
3. Увеличение доли использования возобновляемых природных ресурсов.
4. Внедрение систем и технологий минимизации антропогенного воздействия человека и природную среду.
5. Восстановление природных ресурсов.
6. Развитие общественного контроля, системы экологического просвещения и воспитания.
7. Внедрение системы дистанционного приборного мониторинга состояния окружающей среды.

Для решения задач эколого-экономической безопасности и развития системы народного хозяйства на местном, региональном и национальном уровнях соответствующие органы власти должны прилагать политическую волю, формировать соответствующие цели, задачи, разрабатывать методы их достижения, находить организационные и финансовые ресурсы для обеспечения возможности трансформации системы хозяйствования в направлении большей инновационности, экологичности, природосообразности и ресурсосбережения.

Этапы разработки системы обеспечения эколого-экономической безопасности включает в себя:

1. Определение и формулировка целей и задач.
2. Разработка технико-экономического обоснования достижения соответствующих целей и задач, а также расчет материально-финансового обеспечение.

3. Разработка соответствующих методов решения задач и достижения цели.

4. Оценка результативности и эффективности внедрения принимаемых решений, реализуемых мероприятий, применяемых технологий.

Далее необходимы нормативные документы и детализированные программы с применением различных методов, с учетом имеющихся технологий.

В режиме функционирования системы обеспечения эколого-экономической безопасности можно выделить следующие компоненты:

1. Социальная среда.

2. Экономические отношения.

3. Природа (природная среда).

4. Организационные структуры.

5. Методы управления.

6. Информационные модели.

7. Работники субъектов хозяйственно-экономической деятельности и домохозяйства.

Рассматривая систему эколого-экономической безопасности как систему управления следует учитывать следующие элементы: интересы участников хозяйственной деятельности и угрозы их неосуществления.

Для эффективного обеспечения эколого-экономической безопасности на этапе целеполагания и технико-экономического обоснования проводится оценка территории, ее ресурсов и потенциала, позволяющих учитывать жизненно-важные интересы не только жителей данной территории, но и всех участников социального сообщества (государства), включая:

- составление кадастра объектов, способных нанести ущерб окружающей среде в настоящем и будущем;

- идентификация и классификация экологических рисков;

- районирование с учетом устойчивости различным угрозам;

- учет загрязненных территорий и использованных ресурсов;

- определение и обоснование выбора индикаторов оценки безопасности и устойчивого развития.

На третьем этапе создания системы эколого-экономической безопасности важно организовать и обеспечить эко-экономический мониторинг, который включает в себя:

- нормирование;

- контроль источников негативного воздействия и создания угроз для окружающей среды и человека;

- контроль качества состояния ресурсов и компонентов окружающей среды;

- мониторинг показателей выбранных индикаторов.

Также этот этап предполагает формирование экологической политики, включая:

- подсистему предупреждения экологических угроз;

- подсистему управления экологическими рисками;

- нормативно-правовая подсистема.

При этом, система контроля качества состояния ресурсов и компонентов окружающей среды предполагает применение различных методов:

- методы количественных измерений;

- биологические методы;

- методы моделирования и прогнозирования;

- комбинирования методы.

На уровне микроэкономики важна разработка экологической политики предприятий, институциализированной в форме различных корпоративных нормативно-правовых документов, регламентов, паспортов, инструкций.

Предприятия, деятельность которых связана с появлением отходов как побочного результата экономической деятельности должны:

1. Определить перечень и количество отходов производства, идентифицировать их по классам опасности (очень опасные, умеренно опасные, малоопасные и практически безопасные отходы) [6].

2. В зависимости от перечня отходов выявить возможности и экономическую целесообразность их переработки, обработки и рекуперации с целью дальнейшего использования в народном хозяйстве.

3. Определить формы и методы утилизации отходов, при технической невозможности или экономической нецелесообразности их дальнейшего использования, продажи или обмена.

4. Определить нормативно-правовые основы обращения с данными видами отходов, затраты, связанные с их хранением и утилизацией и регламентирующие процедуры.

5. Разработать паспорт безопасности отходов и самого производства.

6. Составить технологическую карту работы с отходами, технологические карты, включая систему контроля и мониторинга обращения с отходами и назначение ответственных лиц.

Паспорта безопасности, кроме общих данных о предприятии, продукции, применяемых технологиях, общих характеристиках производства должны содержать следующие сведения:

- перечень рисков и потенциальных угроз для окружающей среды;
- методологию оценки рисков и угроз;
- описание и обоснование применяемой методологии оценки рисков и угроз;
- выводы по показателям степени рисков;
- рекомендации по мерам предотвращения рисковых обстоятельств и реализации выявленных угроз;
- технологию и комплекс мер по защите окружающей среды от потенциальных угроз;
- примерный расчет затрат на природоохранные мероприятия, ресурсосбережение, страхование;
- прогнозный расчет величины ущерба для окружающей среды, ресурсных потерь для предприятия в случае реализации выявленных угроз и возникновения неблагоприятных последствий экономической деятельности.

К различным видам паспортов безопасности, применяемым в хозяйственно-экономической деятельности, можно отнести:
- паспорт безопасности отходов;
- паспорт безопасности хранения и утилизации отходов;
- паспорт безопасности продукции;
- паспорт безопасности технологии;
- паспорт безопасности веществ (сырья, полуфабрикатов);
- паспорт безопасности грузов;
- паспорт безопасности помещения, сооружения;
- паспорт безопасности территории.

В настоящее время цифровизация получаемых и используемых ресурсов, паспортизация рисков и угроз на уровне предприятий является важным компонентом эколого-экономической безопасности, позволяющей органам государственной власти и местного самоуправления обеспечить своевременность и действенность мер по защите окружающей среды, восстановлению и сохранению природных ресурсов, а также выявить потенциал и рассчитать экономическую эффективность создания на определенных территориях промышленных симбиозов с целью более рационального природопользования, снижения и распределения антропогенной нагрузки и повышения качества жизни граждан с учетом баланса их жизненно важных интересов, производственных и финансовых целей предприятий, экономических задач регионов и обеспечения национальной безопасности страны в целом.

В данном контексте важна интенсификация разработки и внедрения в практическую деятельность предприятий реального сектора эко-

номики новых ресурсосберегающих технологий, а также современных технологий переработки, рекуперации отходов производства. Это будет способствовать не только снижению антропогенной нагрузки, но и способно повысить экономическую эффективность деятельности предприятий, за счет снижения расходов, платежей в бюджеты различного уровня, получения финансовых льгот и преференций, повышения инвестиционной привлекательности бизнеса. Кроме того, это будет способствовать улучшению экологического состояния как отдельных населенных пунктов, так и регионов.

Следует определить и включить в комплекс мероприятий регионального развития создание эко-технопарков, основанных на технологиях рециклинга не только местного, но и регионального, а также межрегионального уровней.

Рециклинг как важнейший компонент формирования циркулярной экономики должен стать системной основой дальнейшего развития реального сектора экономики в рамках современной эколого-экономической парадигмы функционирования народного хозяйства.

Поэтому, развитие рециклинга и внедрение «зеленых технологий» может не только обеспечить необходимый уровень эколого-экономическую безопасности, снижения угроз в сфере природопользования, но и будет способствовать дальнейшему экономическому развитию.

Литература

1. Браун Л. Как избежать климатических катастроф? План Б 4.0: Спасение цивилизации / Л. Р. Браун, М.: Эксмо, 2010. — 416 с.
2. Браун Л. Мир на грани. Как предотвратить экологический и экономический коллапс / Л. Р. Браун, М.:АСТ-Пресс, 2013.-208 с.
3. Приоритетные области развития. [Электронный ресурс]. - URL: http://www.unepcom.ru/index.php?go=home (дата обращения: 12.06.21)
4. Дейли Г. На общее благо. Переориентация экономики к людям, окружающей среде и устойчивому будущему / Г. Дэйли, Дж. Кобб // пер. с англ. под ред. А.Ю. Ретеюма и П.И. Сафонова М.: Российское отделение ISEE, 1994. - 323 с.
5. Оценивая нашу Землю. Экономика, экология, этика /под ред. Г. Дэйли и К. Таунсенда // перевод с англ. под ред. А.Ю. Ретеюма и П.И. Сафонова), М.: Российское отделение ISEE, 1994.-268 с.
6. Федеральный закон №89-ФЗ «Об отходах производства и потребления» от 24.06.1998 года (ред. от 02.07.2021)

УДК 338

Ризов Алексей Дмитриевич
канд. экон. наук
АО «Чусовской Металлургический Завод»
Пермский край
Угольникова Ольга Дмитриевна
канд. физ. - матем. наук
Санкт-Петербургский государственный
экономический университет
Мордовец Виталий Анатольевич
канд. экон. наук
Санкт-Петербургский университет
технологий управления и экономики

ПРОМЫШЛЕННАЯ ПОЛИТИКА В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ*

*Исследование выполнено при финансовой поддержке РФФИ и БРФФИ в рамках научного проекта № 20-510-00002

Аннотация. Статья посвящена развитию системы оценки уровня цифровизации промышленных предприятий. Научная и практическая значимость: исследованы методики оценки уровня цифровой зрелости промышленных предприятий; выполнен анализ названных методик; намечены подходы к проведению исследований высокой степени точности по установлению для промышленных предприятий их уровня цифровизации, что необходимо для корректировки планов мероприятий реализуемой промышленной политики.

Ключевые слова: цифровая трансформация, цифровизация промышленных предприятий, методики оценки уровня цифровой зрелости и цифровизации.

Rizov A.D.
Chusovoy Metallurgical Works
Perm region
Ugolnikova O.D.
St. Petersburg State University of Economics
Mordovets V.A.
Saint-Petersburg University of Management
Technologies and Economics

INDUSTRIAL POLICY IN THE CONTEXT OF DIGITAL TRANSFORMATION

Annotation. The article is devoted to the development of a system for assessing the level of digitalization of industrial enterprises. Scientific and practical significance: the methods of assessing the level of digital maturity of industrial enterprises are investigated; the analysis of these methods is carried out; approaches to conducting research of a high degree of accuracy are outlined to establish for industrial enterprises their level of digitalization, which is necessary to adjust the action plans of the implemented industrial policy.

Keywords: digital transformation, digitalization of industrial enterprises, methods for assessing the level of digital maturity and digitalization.

Трансформация архитектуры мировой экономики на основе промышленной специализации территорий, разделении труда, направлена на формирование глобальных гибких сетей по типу межтерриториальных, в том числе размещенных в различных государствах, равноправных партнеров. Возникает научный интерес к исследованию особенностей формирования современной государственной промышленной политики в условиях Индустрии – 4.0, к которым относится цифровизация и сетевизация экономики.

Бурное развитие систем связи, передачи, обработки данных, IT-сферы привели к цифровизации процессов отраслей промышленности. В совокупности с технико-математическими средствами машинного контроля и управления производственным процессом, киберметодами и средствами управления производственными процессами, ИКТ-технологиями, как коммуникациями производственных процессов и баз данных; стали основой новых цифровых и математических моделей производственных и организационных процессов, преобразований традиционных производственных комплексов и систем управления ими. Поэтапный процесс развития указанных направлений (автоматизация, информатизация, цифровизация) привел к целой системе - цифровой трансформации промышленных предприятий, отраслей, промышленности в целом.

Цифровая трансформация промышленности на современном этапе глобальной конкуренции стала стратегией мировых экономик. Цифровая трансформация была объявлена национальной целью развития России до 2030 г. [1]. Ее целевыми показателями были заявлены:

– «цифровая зрелость» ключевых отраслей экономики и социальной сферы;

– доведение до 95% доли электронных массовых социально значимых для населения услуг;

– доведение до 97% доли домохозяйств, обеспеченных широкополосным доступом к интернет-сети;

– рост в 4 раза вложений в отечественные решения в сфере ИТ по сравнению с 2019 г.

Наиболее высокую степень готовности к цифровой трансформации демонстрируют крупные промышленные предприятия. Принятие в процессе их функционирования как важнейших стратегических, так и оперативных управленческих решений напрямую соотносится с возможностями цифровых технологий, что в полной мере соответствует их структурной организации, представляющей сложную сеть. Кроме этого, возможны производственные связи между промышленными предприятиями различных регионов, включая регионы Союзного государства РФ и РБ, обеспечивающие их кооперацию.

Министерство цифрового развития, связи и массовых коммуникаций РФ утвердило методики расчета указанных целевых показателей по цели «цифровая трансформация» (Приказ №600 от 18.11.2020 г.) [2].

Для промышленности среди 10 других были установлены следующие показатели:

1. цифровая зрелость основных производственных процессов предприятий промышленности;
2. цифровая зрелость вспомогательных процессов предприятий промышленности;
3. доля предприятий, в отношении которых сформирован цифровой паспорт в ГИСП;
4. доля предприятий, использующих технологию API для обмена данными, предоставления цифровых услуг и информационного взаимодействия с государственными информационными системами;
5. доля предприятий, использующих технологии имитационного моделирования и виртуальных испытаний промышленной продукции (применяющих технологию «цифровой двойник изделия»);
6. доля предприятий, использующих технологии предсказательной (предиктивной) аналитики при прогнозировании и проведении послепродажного (сервисного) обслуживания промышленной продукции;
7. доля предприятий, использующих технологии промышленного интернета вещей, сбора данных и диспетчерского контроля для управления производственными процессами в реальном времени;
8. доля предприятий, использующих технологию «цифровой двойник производства».

Официальная информация по показателям формируется Минцифрой России, исполнительной властью регионов, федеральными органами исполнительной власти.

Базовые значения компонент - значения 2019 года отбираются в соответствии с информацией по: а) форме федерального статистического наблюдения №1-З «Анкета выборочного обследования рабочей силы»; б) форме федерального статистического наблюдения №3-информ «Сведения об использовании цифровых технологий и производстве связанных с ними товаров и услуг».

Компонентами для расчета цифровой зрелости отраслей экономики и социальной сферы выбраны:

1). $К_{ии}$ - доля в % достижения целевого значения численности специалистов, занятых в экономике, интенсивно использующих информационно-коммуникационные технологии («ии» - интенсивно использующих);

2). $К_{рцр}$ - доля в % достижения целевого значения роста расходов предприятий на внедрение и применение современных цифровых решений («рцр» - расходы на цифровые решения);

3). $К_{ЦЗО}$ - доля в % достижения целевого значения цифровой зрелости отраслей экономики и социальной сферы («ЦЗО» - цифровая зрелость отрасли»).

На основе $К_{ии}$, $К_{рцр}$, $К_{ЦЗО}$ проводятся вычисления ЦЗО (цифровая зрелость отраслей экономики и социальной сферы, %):

$$ЦЗО = (0{,}25 \times К_{ии} + 0{,}25 \times К_{рцр} + 0{,}5 \times К_{цзо}) \quad (1)$$

Индекс цифровой зрелости i-ой отрасли рассчитывается по формуле (2), промышленность входит в перечень десяти выбранных отраслей экономики и социальной.

$$К_{ЦЗО_i} = \frac{\sum_{j=1}^{n} x_j}{n} \times 100\% \quad (2)$$

$К_{ЦЗО_i}$ – индекс цифровой зрелости i-ой отрасли. x_j - отношение j-го показателя цифровой зрелости i-ой отрасли к целевому значению в 2030 г. (указаны в Приложении к Приказу). Так, целевое значение цифровой зрелости основных производственных процессов предприятий промышленности составляет 85%. n - количество индексов цифровой зрелости i-ой отрасли, в случае промышленности десять показателей перечислены выше.

Выбрав j-й показатель цифровой зрелости из десяти для промышленности, найдя отношение числового значения этого показателя для базового 2019 года к его целевому числовому значению, найдем суммируемый в формуле (2) x_j.

Находя $И_{ЦЗО_i}$ для каждого последующего года, можно проследить динамику индекса цифровой зрелости промышленности в целом. На регионы данная методика, как следует из Приказа, не распространяется.

Данная методика проходит апробацию с 2021 года в рамках пилотных проектов, в которых участвуют:

– АО «ОДК–Климов» (Санкт-Петербург),

– АО «ОМК» (объединяет Выксунский МК, Трубодеталь – г. Челябинск, Альметьевский трубный завод - Республика Татарстан, ОМК Стальной путь - Москва, Благовещенский завод арматуры - Республика Башкортостан, Чусовой металлургический - Пермский край, Россия, Белэнергомаш – Белгород),

– АО «Объединенная двигателестроительная корпорация» (Москва),

– ООО «Газпром бурение»,

– АО «ИЭМЗ «Купол» (Москва).

Уровень цифровой зрелости предприятий оценивается на основе анализа основных бизнес-процессов (в цепочке создания добавленной стоимости с точки зрения стадий жизненного цикла продукции), вспомогательных бизнес-процессов, дополнительной группы (технологические решения, обеспечивающие общий уровень развития ИТ на предприятии) [3].

К основным бизнес-процессам отнесены: управление подготовкой производства; управление производством; управление качеством продукции; упаковка и хранение; управление сбытом и логистикой; монтаж, эксплуатация и послепродажное обслуживание; управление маркетинговыми исследованиями; управление опытно-конструкторскими работами; управление МТО и закупками.

К вспомогательным бизнес-процессам отнесены: стратегическое управление предприятием, управление финансами (бюджетирование, казначейство, бухгалтерский и налоговый учет), управление ИТ, управление персоналом, юридическое управление, управление эксплуатацией и обслуживанием оборудования, управление безопасностью, организационное развитие и повышение операционной эффективности, управление документооборотом и корпоративным контентом, управление охраной труда, экологией и промышленной безопасностью.

К технологическим решениям отнесены: управление развитием и цифровизацией предприятия, единое информационное пространство, применение технические средств автоматизации производственных процессов, применение сквозных и наилучших доступных технологий, средства защиты информации, уровень оснащения АРМ и высококвалифицированные кадры, специализированные ИТ-решения.

Управления процессами осуществляется через классы систем, например, специализированные системы (системы безопасности / защиты информации, управления ИТ-службой, ИТ-инфраструктурой и ИТ-активами, специализированные ИТ-решения); системы управления проектами, исследованиями, разработкой, проектированием и внедрением (Project

management, PLM/PDM, системы математического и имитационного моделирования) и др. [3].

Имеющиеся рекомендации для индекса цифровой трансформации предприятия формулируют ряд условий. Индекс: рассчитывает уровень цифровизации конкретного предприятия; оценивает цифровизацию по отдельным бизнес-процессам; учитывает эффективность внедрения и готовность к цифровой трансформации предприятия; представляет собой интегральный показатель; состоит из показателей нижнего уровня; является измеримым показателем – через анкеты, открытые данные, существующие данные. Эти условия формируют критерии оценки существующих методик по оценке уровня цифровизации предприятий.

Полностью удовлетворяющей потребностям методики оценки уровня цифровой зрелости промышленных предприятий нет. Наиболее приближена к сформулированным требованиям методика, используемая ИТ-компаниями при оценке внедрения платформ (процессы, классы ИТ-систем, эффекты, стоимость, дорожная карта внедрения).

Из известных методик: индекс развития ИКТ, анкетирование предприятий при внедрении производственных ИТ-систем, индекс сетевой готовности, модель цифровой зрелости, индекс цифровой трансформации, индекс развития ИКТ, цифровое пианино (последняя методика связана с аналогиями в нотной грамоте: как выбранным 7 нотам, определены 7 трансформационных категорий элементов цепочки создания стоимости предприятия – бизнес модель, оргструктура, трудовые ресурсы, процессы, ИТ-возможности, предложения, модель взаимодействия).

Текущий уровень цифрового развития промышленного предприятия может быть определен при помощи цифрового паспорта. Цифровой паспорт — перечень характеристик предприятия, сформированный в рамках ГИСП, включающий информацию об уровне цифровой зрелости и готовности к внедрению цифровых технологий [4, Ст. 14].

На ресурсе Министерства промышленности и торговли РФ – размещена Государственная информационная системе промышленности (ГИСП). Эта система создана как продукт по реализации ФЗ «О промышленной политике Российской Федерации» №488-ФЗ от 31.12.2014 г. «в целях автоматизации процессов сбора, обработки информации, необходимой для обеспечения реализации промышленной политики и осуществления полномочий федеральных органов исполнительной власти по стимулированию деятельности в сфере промышленности, информирования о предоставляемой поддержке субъектам деятельности в сфере промышленности, а также для повышения эффективности обмена информацией о состоянии промышленности и прогнозе ее развития» [5].

Возможность получения государственной поддержки стала для промышленных предприятий стимулом активно применять цифровые техно-

логии, иметь развитые управленческие характеристики. Государственная поддержка гарантирована выдачей цифрового паспорта промышленного предприятия. Сервис ГИСП «Цифровой паспорт промышленного предприятия» на базе вводимых и подтверждаемых документами данных выполняет расчеты и дает заключение о реализуемых проектах цифровизации и цифровой трансформации предприятия. Получение Цифрового паспорта промышленного предприятия доступно с июня 2021 года [6].

Цифровой паспорт - проект по цифровой трансформации. Цель ее - цифровизация производственных и административных процессов промышленных предприятий. Паспорт послужит индикатором цифровой зрелости предприятий, уровня цифровизации отечественной промышленности России. Предприятия получают заключение об уровне цифровизации своего предприятия, отраслей промышленности, возможность подобрать ИТ-решения, уточнить меры государственной поддержки по цифровизации и технологическим решениям.

Разработанная пошаговая методика позволяет оценить степень использования современных систем решений ИКТ для различных бизнес-процессов предприятия, установить уровень его цифровизации.

Например, в Пермском крае (Приволжский ФО, Уральский экономический район) разработана методика «пирамиды процесса цифровизации», подразделяющая процессы на «первичную локальную цифровизацию; частичную цифровизацию; комплексную цифровизацию; «умную» организацию; цифровую экосистему» [7]. Уровень цифровизации характеризует готовность предприятия к жесткой конкурентной борьбе на рынках, составляет фундамент стратегии развития предприятия. Дорожная карта исследования включала 3 этапа: заполнение анкеты с проведением самодиагностики уровня цифровизации предприятия; автоматизированный сбор данных и обработка результатов анкетирования предприятий в программе MS Excel; разработка (корректировка) стратегии цифровизации предприятия. Анкета, на основе которой делаются заключения по уровню цифровизации предприятия, содержится в [7] на стр. 2385 – 2390.

Уровень «Локальная цифровизация» (1-й уровень цифрового развития) присваивается предприятию, в 30% бизнес-процессах которого используется специализированное программное обеспечение и сервисы. Следующий уровень «Частичная цифровизация» присваивается предприятию, в 80% бизнес-процессах которого используется специализированное программное обеспечение и сервисы. Третий уровень «Комплексная цифровизация» присваивается предприятию, в 100% бизнес-процессах которого используется специализированное программное обеспечение и сервисы. В этом случае при и реализации процессов взаимодействия данного предприятия в цифровом пространстве с 50% контрагентов оно получает статус «Умная» организация» (четвертый уровень). Наконец, пятый уро-

вень - «Цифровая экосистема» присваивается предприятию статуса комплексной цифровизации, но взаимодействующего в цифровом пространстве с 60%–100% контрагентов.

Авторы анализируемого исследования относят предложенную методику к универсальной, достоверной с обобщенной оценкой степени цифровизации предприятия и отрасли, возможностью «контролировать измерения в области цифровизации, выявлять и развивать перспективные точки роста, а также определять ближайшие перспективы цифровой трансформации от отдельного бизнес-процесса до отрасли и региона в целом» [7, с. 2393]. Признавая удачным подход - пошаговая методика «с максимальным проникновением до отдельных хозяйствующих субъектов» [7, с. 2381], отметим, что учет только использования специализированного программного обеспечения и сервисов для объективной оценки уровня цифровизации предприятия, очевидно, недостаточен. Разделение бизнес-процессов на основные, управленческие и вспомогательные, технологические решения, обеспечивающие общий уровень развития предприятия не рассматривались. С этих позиций наиболее предпочтительной является методика оценки уровня цифровой зрелости предприятия, предложенная Минпромторгом России в [4].

Метод самообследования предприятия не позволяет гарантировать необходимый уровень специалистов, привлеченных к проведению анкетирования. Нужна верификация результатов [8].

В отечественных исследованиях (Республика Башкортостан, Приволжский ФО, Уральский экономический район) поднята проблема разработки стратегии цифровой трансформации, связанной с уровнем цифровой зрелости предприятия. Действительно, требуемый результат цифровых преобразований достигается не в ходе выполнения отдельных проектов цифровизации предприятия, а в ходе реализации стратегии цифровой трансформации. Суть такой трансформации - гибкая компания, постоянно адаптирующаяся к изменениям вследствие внутренних и внешних факторов условиям за счет технологий, организационного обучения и принятия решений на основе высококачественных данных, доступных в наиболее короткие сроки [9].

В Германии разработан и применяется индекс зрелости Индустрии 4.0 acatech, который предоставляет предприятию возможность такой трансформации. Индекс включает шесть этапов развития для четырех ключевых областей предприятия. Индекс можно использовать для разработки программы цифрового преобразования конкретного предприятия. В рамках модели обязательным является постоянное получение дополнительной информации для непрерывного обучения. Данный индекс был предложен заинтересованными партнерами в исследовательском и промышленном секторах страны [10].

Данный опыт был развит в отечественных исследованиях: предложена схема управления цифровой зрелостью предприятия, где предусмотрена оценка и преодоление значительного разрыва между текущим и целевым уровнями зрелости, отмечено отсутствие требуемой организационной культуры - эти и другие особенности следует отнести к барьерам достижения высокого уровня цифровой зрелости предприятиями.

Темпы цифровой трансформации промышленности связаны с ростом инвестиций в основной капитал на 13,8% даже в условиях пандемии: затраты промышленных предприятий на создание, распространение и использование цифровых технологий в 2019 г. и составили 176,3 млрд. руб.; доля в валовой добавленной стоимости в отрасли (суммарные вложения) составила 1,2% [11], что соответствует 2 месту в рейтинге отраслей российской экономики. Аналогичная ситуация в рейтинге по индексу цифровизации.

Вывод. Достижение высокого уровня цифровой зрелости, определяющего цифровую трансформацию предприятия, представляет собой сложный процесс, траектория которого во многом индивидуальна. Пилотные проекты, реализующиеся в рамках программы Министерства промышленности и торговли РФ, а также научными коллективами различных российских регионов, включая регионы Уральского экономического района, позволят предложить сценарии цифровой трансформации, соответствующие требуемым изменениям организационной структуры и культуры промышленных предприятий.

Цифровая трансформация промышленного пространства как стратегическая национальная цель страны требует «цифровой зрелости» ключевых отраслей экономики и 4-кратном росте вложений в российские ИТ - решения по отношению к показателю базового 2019 г. Они к 2030 году будут способствовать цифровой трансформации промышленности, получив поддержку внедрения отечественных проектов программного обеспечения на промышленных предприятиях.

В завершение укажем, что данное исследование является продолжением статьи [12], а также составной частью работ ([13] – [15]).

Литература

1. Указ Президента Российской Федерации от 21.07.2020 г. №474 «О национальных целях развития Российской Федерации на период до 2030 года». [Электронный ресурс]. – URL: http://www.kremlin.ru/acts/bank/45726

2. Об утверждении методик расчета целевых показателей национальной цели развития Российской Федерации «цифровая трансформация». Приказ от 18 ноября 2020 г. №600 Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

3. Основные принципы по оценке уровня цифровой зрелости, реализованные в рамках модуля ГИСП «Цифровой паспорт промышленных предприятий». [Электронный ресурс]. – URL: https://minprom.samregion.ru/wp-content/uploads/sites/9/2021/08/czifrovoj-pasport-predpriyatiya-19.08.2021.pdf

4. Показатели цифровой зрелости отрасли «промышленность». [Электронный ресурс]. – URL: https://www.economy.gov.ru/material/file/371da805d6a083111877a2ac0f9f9b29/Minpromtorg.pdf

5. Федеральный закон от 31 декабря 2014 г. №488-ФЗ «О промышленной политике в Российской Федерации» (с изменениями и дополнениями. Редакция от 20.07.2020 г.). [Электронный ресурс]. - URL: http://www.consultant.ru/document/cons_doc_LAW_173119/

6. Информация Министерства промышленности и торговли РФ от 7 июня 2021 г. [Электронный ресурс]. – URL: https://www.garant.ru/products/ipo/prime/doc/400771487/

7. Мерзлов И.Ю., Шилова Е.В., Санникова Е.А., Сединин М.А. Комплексная методика оценки уровня цифровизации организаций // Экономика, предпринимательство и право. – 2020. – Том 10. – №9. – С. 2379-2396. doi: 10.18334/epp.10.9.110856

8. Куприянова М.В., Симикова И.П. Методологические подходы к оценке уровня цифровизации промышленного производства // Экономика: вчера, сегодня, завтра. Том: 10. Номер: 8-1. 2020 г. С. 327-334.

9. Гилева Т.А. Цифровая зрелость предприятия: методы оценки и управления // Вестник УГНТУ. Наука, образование, экономика. Серия: Экономика. №1 (27), 2019. С. 38-52.

10. Шу, Г., Андерл, Р., Гауземайер, Ю., тен Хомпель, М., Вальстер, В. (и др.): Индекс зрелости Индустрии 4.0 – Управление цифровым преобразованием компаний (acatech ИССЛЕДОВАНИЕ), Munich: Herbert Utz Verlag 2017.

11. Цифровая трансформация отраслей: стартовые условия и приоритеты: докл. к XXII Апр. междунар. науч. конф. по проблемам развития экономики и общества, Москва, 13–30 апр. 2021 г. / Г. И. Абдрахманова, К. Б. Быховский, Н. Н. Веселитская, К. О. Вишневский, Л. М. Гохберг и др.; рук. авт. кол. П.Б. Рудник; науч. ред. Л.М. Гохберг, П. Б. Рудник, К. О. Вишневский, Т.С. Зинина; Нац. исслед. ун-т «Высшая школа экономики». – М.: Изд. дом Высшей школы экономики, 2021. — 239,

12. Цифровизация российской промышленности (на примере уральского региона) / Угольникова О.Д., Воротков П.А., Ризов А.Д. - Научно-технический журнал «Технико-технологические проблемы сервиса», СПб.: Изд-во СПбГЭУ, 2021. №3 (57), с. 56-62.

13. Промышленная политика индустриально развитых регионов РФ: новая реальность / Лепеш Г.В., Макарова И.В., Угольникова О.Д. – Изве-

стия Санкт-Петербургского государственного экономического университета, СПб.: Изд-во СПбГЭУ, 2020. №6(126), с. 42-47.

14. Методологические основы исследования модернизации промышленных комплексов в контексте неоиндустриализации / Курегян С.В., Лепеш Г.В., Макарова И.В., Угольникова О.Д., Мелешко Ю.В. - Экономическая наука сегодня : сборник научных статей / Белорусский национальный технический университет, Факультет технологий управления и гуманитаризации, Кафедра «Экономика и право» ; редкол.: С. Ю. Солодовников (гл. ред.) [и др.]. – Минск : БНТУ, 2020. – Вып. 12. – С. 65-72.

15. Цифровая адаптация российской экономики: особенности, проблемы, перспективы / Угольникова О.Д. - Инновационные технологии и вопросы обеспечения безопасности реальной экономики : сборник научных трудов по итогам Всероссийской научно-практической конференции «Инновационные технологии и вопросы обеспечения безопасности реальной экономики». Санкт-Петербург. 27 марта 2020 года / под ред. д-ра техн. наук, проф. Г.В. Лепеша, канд. физ.-мат. наук, доц. О.Д. Угольниковой, канд. экон. наук, доц. С.Ю. Александровой. – СПб. : Изд-во СПбГЭУ, 2020, с. 214-221.

УДК 376

Смекалин Сергей Владимирович
преподаватель
Чекарев Леонид Васильевич
преподаватель
Санкт-Петербургское государственное казенное учреждение
дополнительного профессионального образования
«Учебно-методический центр по гражданской обороне
и чрезвычайным ситуациям»

ОСНОВЫ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В ОБЛАСТИ ЗАЩИТЫ НАСЕЛЕНИЯ НА СОВРЕМЕННОМ ЭТАПЕ

Аннотация. В настоящей статье раскрыты основы государственной политики в области защиты населения на современном этапе развития общества. Авторы представили краткий обзор законодательных и нормативно-правовых актов в области защиты населения и территорий от чрезвычайных ситуаций и предлагают практическое применение их в повседневной жизнедеятельности.

Ключевые слова: чрезвычайная ситуация, гражданская оборона, режимы функционирования РСЧС, режим чрезвычайной ситуации.

Smekalin S.V.
Chekmarev L.V.
St. Petersburg state institution of additional
professional education «Educational and methodical center
civil defense and emergency situations»

FUNDAMENTALS OF STATE POLICY IN THE FIELD OF POPULATION PROTECTION AT THE PRESENT STAGE

Annotation. This article reveals the foundations of state policy in the field of protecting the population at the present stage of development of society. The authors presented a brief overview of legislative and regulatory acts in the field of protection of the population and territories from emergencies and offer their practical application in everyday life.

Keywords: emergency situation, civil defense, modes of operation of the RSChS, emergency mode.

Защита населения и территорий от чрезвычайных ситуаций (далее - ЧС) является одной из важнейших задач государственной политики Российской Федерации и является частью системы государственного управления в сфере национальной безопасности страны.

Управление в области защиты населения и территорий от ЧС, обеспечения пожарной безопасности, безопасности людей на водных объектах, а также деятельностью федеральных органов исполнительной власти в рамках единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (далее - РСЧС) осуществляет Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий.

К основным видам ЧС, которые сегодня наносят значительный ущерб экономике страны относятся:

техногенные;

природные;

биолого-социальные.

По данным МЧС России в 2020 году на долю техногенных чрезвычайных ситуаций пришлось 50,5% от общего числа ЧС, на долю природных – 31,4%, а на долю биолого-социальных – 18,1%.

Число погибших людей в результате ЧС составило 326 чел., из которых:

от воздействия техногенных ЧС – 322 чел.;

от природных ЧС – 4 человека.

Число людей, пострадавших в результате ЧС в 2020 г. составило 6257 чел., из которых:

при техногенных ЧС – 1 727 чел.;

при природных ЧС – 4 366 чел.;

при биолого-социальных ЧС – 164 человека.

Число спасенных людей составило 2627 чел., из которых:

при техногенных ЧС – 859 человек;

при природных ЧС – 1 768 человек

В целях предупреждения ЧС органами управления и силами аварийно-спасательных служб проводился комплекс организационно-технических мер по уменьшению и предотвращению источников возникновения ЧС. На потенциально-опасных объектах созданы технические и материальные ресурсы для решения задач по предупреждению и ликвидации ЧС техногенного характера, объекты оснащены системами предотвращения аварий, растет количество объектов, оборудованных автоматической пожарной сигнализацией и автоматическими системами пожаротушения.

Органами надзора были организованы и постоянно проводились профилактические мероприятия по снижению риска и последствий возникновения ЧС в производственной деятельности, такие как:

контроль за хранением опасных веществ и материалов;

контроль за наличием и состоянием средств пожаротушения;

своевременное проведение противопожарных мероприятий, направленных на ограничение распространения огня в случае возгорания;

создание условий для быстрой эвакуации людей и материальных ценностей;

контроль за правильным выполнением технологических процессов на производстве;

использование систем сигнализации и блокировок (закрытия-открытия задвижек, аварийного отключения компрессоров).

Особое внимание на объектах уделялось проведению планово-предупредительных ремонтов и техническому обслуживанию оборудования (его обновлению), а также оснащению потенциально опасных объектов системами аварийного контроля и предотвращения аварий.

В 2020 г. на территории Российской Федерации было зарегистрировано 439394 пожара, в которых погибло 8313 человек и получило травмы 8434 граждан. По сравнению с 2019 годом количество пожаров уменьшилось на 6,8%, количество погибших людей при пожарах – на 3,0%, количество людей, получивших травмы при пожарах – на 11,0%.

Особо хочется отметить уменьшение количества погибших при пожарах детей - на 12,1%.

В целях совершенствования также борьбы с пожарами, пожарно-спасательными гарнизонами субъектов Российской Федерации в повседневной деятельности реализуются основные функции:

мониторинг и прогнозирование;

оценка складывающейся обстановки;

формирование информационных ресурсов центров управления в кризисных ситуациях всех уровней.

Мероприятия, направленные на повышение эффективности тушения пожаров, проводимые подразделения государственной противопожарной службы:

осуществляется составление, корректировка и отработка документов предварительного планирования на местности с привлечением администрации объекта;

проводится проверка работоспособности и исправности водоисточников в районе выезда пожарно-спасательных подразделений;

в 74 субъектах Российской Федерации был установлен особый противопожарный режим.

Учитывая возрастание опасных факторов и угроз в результате прогнозируемых природных катаклизмов и техногенных аварий на территории России, неуклонно повышается роль и значимость государственной политики в области защиты населения и территорий России. Реализация основ государственной политики Российской Федерации в области защиты населения и территорий от чрезвычайных ситуаций, задачи и приоритетные направления деятельности на период до 2030 года определены Указом Президента РФ от 11 января 2018 года №12, способствует сокращению числа ЧС и уменьшению числа погибших и пострадавших.

Президентом РФ, исходя из анализа обстановки в стране, подчеркнуто, что основными угрозами, влияющими на состояние защиты населения и территорий Российской Федерации на современном этапе, являются:

- стихийные бедствия, в том числе вызванные глобальным изменением климата, активизацией геофизических и космогенных процессов;

- техногенные аварии и катастрофы, в том числе вызванные ухудшением состояния объектов инфраструктуры, а также возникшие вследствие пожара или стихийного бедствия;

- особо опасные инфекционные заболевания людей, животных и растений, в том числе связанные с увеличением интенсивности миграционных процессов и повышением уровня урбанизации;

- новые угрозы, вызванные негативным изменением окружающей среды, а также усложнением технологических процессов, что влечет за собой увеличение размеров ущерба в результате аварий [3].

Устойчивое развитие страны и уровня безопасности жизнедеятельности вовлекает большое количество участников, сил, материальных, финансовых и других ресурсов, требует умелого их использования.

Данная задача не может быть решена без слаженной работы и взаимодействия органов государственной власти, местного самоуправления, организаций и самих граждан. Уровень подготовки должностных лиц и работников, принимающих участие в организации и выполнении мероприятий по защите населения является существенным фактором обеспечения их эффективности и результативности, а это в свою очередь повышает безопасность граждан и общества.

Организационно-правовые нормы в области защиты граждан Российской Федерации, иностранных граждан и лиц без гражданства, находящихся на территории РФ (далее-население), всего земельного, водного, воздушного пространства в пределах Российской Федерации или его части, объектов производственного и социального назначения, а также окружающей среды (территории) от чрезвычайных ситуаций определяет Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» 21 декабря 1994 г. №68-ФЗ [2].

Целями настоящего Федерального закона являются:

- предупреждение возникновения и развития чрезвычайных ситуаций;

- снижение размеров ущерба и потерь от чрезвычайных ситуаций;

- ликвидация чрезвычайных ситуаций;

- разграничение полномочий в области защиты населения и территорий от чрезвычайных ситуаций между федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления и организациями [2].

В настоящее время основной упор в вопросах защиты населения делается на профилактику и предупреждение чрезвычайных ситуаций на основе комплексного управления рисками. Одним из направлений реализации данного подхода является развитие системы мониторинга и прогнозирования чрезвычайных ситуаций.

Единая государственная система в настоящее время функционирует в трех режимах готовности. При отсутствии угрозы возникновения чрезвычайных ситуаций органы управления и силы единой системы функционируют мы работаем и отдыхаем в режиме ***повседневной деятельности.***

Решением руководителей субъектов Российской Федерации, органов местного самоуправления и организаций, если на их территории создалась угроза возникновения или возникла чрезвычайная ситуация могут быть установлены следующие режимы функционирования:

а) ***режим повышенной готовности*** - при угрозе возникновения чрезвычайных ситуаций граждане обязаны:

- соблюдать общественный порядок, требования законодательства Российской Федерации о защите населения и территорий от чрезвычайных ситуаций, о санитарно-эпидемиологическом благополучии населения;

- выполнять законные требования (указания) руководителя ликвидации чрезвычайной ситуации, представителей экстренных оперативных служб и иных должностных лиц, осуществляющих мероприятия по предупреждению и ликвидации чрезвычайной ситуации (далее - уполномоченные должностные лица);

- при обнаружении пострадавшего (пострадавших) принимать меры по вызову уполномоченных должностных лиц и до их прибытия при отсутствии угрозы жизни и здоровью оказывать пострадавшему (пострадавшим) первую помощь [4].

б) ***режим чрезвычайной ситуации*** - при возникновении и ликвидации чрезвычайных ситуаций [4].

Дальнейшее развитие основ государственной политики в области защиты населения от ЧС на современном этапе развития общества закреплено в Постановлении Правительства РФ от 2 апреля 2020 года №417 «Правила поведения, обязательные для исполнения гражданами и организациями, при введении режима повышенной готовности или чрезвычайной ситуации» (далее - Правила) [4].

При угрозе возникновения или возникновении ЧС гражданам запрещается:

- создавать условия, препятствующие и затрудняющие действия уполномоченных должностных лиц и работников общественного транспорта;

- заходить за ограждение, обозначающее зону чрезвычайной ситуации или иную опасную зону;

- осуществлять действия, создающие угрозу собственной безопасности, жизни и здоровью;

- распространять заведомо недостоверную информацию об угрозе возникновения или возникновении чрезвычайной ситуации [4].

В Правилах доступно раскрыты порядок действий населения и руководителей различного уровня при получении информации или сигнала оповещения об угрозе или возникновении ЧС, а также введении режима повышенной готовности или чрезвычайной ситуации на той или иной территории. Ранее этого в нормативных документах раскрыто не было.

В субъектах Российской Федерации продолжается развитие систем раннего обнаружения быстроразвивающихся опасных природных явлений

и процессов, модернизация существующих и разработка современных технологий и методов прогнозирования, и повышение эффективности предупреждения ЧС.

Для приема сообщений о чрезвычайных ситуациях, в том числе вызванных пожарами, необходимо использовать единый номер вызова экстренных оперативных служб «112».

Вывод: Основы государственной политики в области защиты населения заключаются в полном и четком выполнении мероприятий, закрепленных новыми нормативными правовыми актами, главная задача - повсеместное внедрение их в практику. Дальнейшая перспектива в совершенствовании систем ГО и РСЧС состоит в ее объединении с целью исключения дублирования их деятельности.

Литература

1. Федеральный закон «О гражданской обороне» от 12.02.1998 №28-ФЗ.

2. Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» от 21.12.1994 №68-ФЗ.

3. Основы государственной политики Российской Федерации в области защиты населения и территорий от чрезвычайных ситуаций, задачи и приоритетные направления деятельности на период до 2030 года определены Указом Президента РФ от 11 января 2018 года №12.

3. Постановление Правительства РФ от 18 сентября 2020 г. №1485 «Об утверждении Положения о подготовке граждан Российской Федерации, иностранных граждан и лиц без гражданства в области защиты от чрезвычайных ситуаций природного и техногенного характера».

4. Постановление Правительства РФ от 2 апреля 2020 г. №417 «Об утверждении Правил поведения, обязательных для исполнения гражданами и организациями, при введении режима повышенной готовности или чрезвычайной ситуации».

5. Постановлением Правительства РФ от 30 декабря 2003 г. №794 «О единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций».

6. Предупреждение и ликвидация чрезвычайных ситуаций. Учебное пособие для органов управления РСЧС. под общей редакцией Ю.Л. Воробьева, М, 2002 год, гл.1-3.

УДК 60. 654. 09

Соленов Юрий Александрович
канд. воен. наук, доцент
преподаватель СПб ГКУ ДПО
«Учебно-методический центр
по гражданской обороне и чрезвычайным ситуациям»

ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМ ОПОВЕЩЕНИЯ И ИНФОРМИРОВАНИЯ НАСЕЛЕНИЯ

Аннотация. На основе анализа положений нормативно-правовых документов по оповещению и информированию населения об опасностях в мирное и военное время, требований, предъявляемых к системам оповещения, а также изучения опыта применения систем оповещения в различных условиях изложены особенности функционирования и перспективы развития существующих систем оповещения и информирования населения.

Ключевые слова: оповещение и информирование населения об опасностях, сигналы оповещения, экстренная информация, системы оповещения и информирования, терминальные комплексы, зона экстренного оповещения.

Solenov Y.A.
St. Petersburg state institution of additional
professional education «Educational and methodical center
civil defense and emergency situations»

FEATURES OF FUNCTIONING AND PROSPECTS OF DEVELOPMENT OF PUBLIC NOTIFICATION AND INFORMATION SYSTEMS

Annotation. Based on the analysis of the provisions of the regulatory documents on warning and informing the population about the dangers in peacetime and wartime, the requirements for warning systems, as well as the study of the experience of using warning systems in various conditions, the features of the functioning and prospects for the development of existing warning systems and informing the population are described.

Keywords: warning and informing the public about hazards, warning signals, emergency information, warning and information systems, terminal complexes, emergency warning zone.

Анализ современных опасностей и угроз, накопленный опыт войн и военных конфликтов, ликвидаций чрезвычайных ситуаций природного и техногенного характера убедительно свидетельствуют о том, что эффективность мероприятий защиты находится в самой прямой зависимости от своевременности и полноты информирования населения об опасностях, как в военное, так и в мирное время. Поэтому оповещение и информирование население является важнейшей задачей гражданской обороны (далее – ГО) и единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (далее – РСЧС).

Следует отметить, что понятия «оповещение» и «информирование», несмотря на кажущуюся схожесть, все-таки имеют принципиальное отличие. Оповещением корректно называть такой порядок, когда те или сведения необходимо довести незамедлительно, как правило, в виде условных сигналов, команд, экстренных сообщений. Оповещение также обычно предполагает выполнение определенных, заранее установленных защитных мероприятий. В то время как информирование населения об опасностях заключается в заблаговременном доведении различных сведений, информации в соответствии с прогнозированием развития обстановки, когда есть время подготовиться и принять меры для минимизации возможных негативных последствий. Информирование по своему содержанию более широкое понятие, чем оповещение.

В связи с этим оповещение характерно для военного времени или при возникновении быстроразвивающихся ЧС, а информирование в большей степени присуще мирному времени. Хотя, безусловно, и в военное и в мирное время может иметь место, как оповещение, так и информирование населения об опасностях.

Под *оповещением* населения о чрезвычайных ситуациях подразумевается доведение до населения сигналов оповещения и экстренной информации об опасностях, возникающих при угрозе возникновения или возникновении чрезвычайных ситуаций (далее – ЧС) природного и техногенного характера, а также при ведении военных действий или вследствие этих действий, о правилах поведения населения и необходимости проведения мероприятий по защите.

Информирование населения о чрезвычайных ситуациях - это доведение до населения через средства массовой информации и по иным каналам информации о прогнозируемых и возникших чрезвычайных ситуациях, принимаемых мерах по обеспечению безопасности населения и территорий, приемах и способах защиты, а также проведение пропаганды знаний в области гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций, в том числе обеспечения безопасности людей на водных объектах, и обеспечения пожарной безопасности [1].

В военное время основным способом оповещения населения и работников организаций об опасностях, которые могут возникнуть вследствие военных действий *является доведение сигналов оповещения ГО.*

Сигнал оповещения ГО - сигнал, передаваемый в системе управления гражданской обороной и являющийся командой для проведения мероприятий силами гражданской обороны, а также для применения населением средств и способов защиты [2]. В этом определении следует обратить внимание на то, что сигнал оповещения ГО является *командой*. То есть, передача сигналов оповещения ГО не предполагает каких-то разъяснений и дополнительной информации. Наоборот, (как *исполнительная команда!)* требует от получивших ее, немедленного выполнения определенных действий и, как правило, проведения заранее установленных мероприятий защиты. Это принципиально важно.

Кроме сигналов оповещения ГО с 1989 года для привлечения внимания населения установлен единый предупредительный сигнал «ВНИМАНИЕ ВСЕМ!*»,* который передается звуком сирен, гудками предприятий и другими сигнальными средствами. По этому сигналу население обязано включить приемники проводного и радиовещания, телевизионные приемники, другие средства массой информации для получения сигнала оповещения ГО или прослушивания экстренного сообщения о сложившейся обстановке и порядке дальнейших действий. Как правило, сразу же после окончания звука сирены должно быть передано речевое сообщение (сигнал оповещения ГО) об угрозе или возникновении конкретной опасности военного (мирного) времени.

Недавно изданный совместный приказ МЧС России и Министерства цифрового развития, связи и массовых коммуникаций РФ от 31.07.2020 №578/365 «Об утверждении Положения о системах оповещения» установил, что передача сигналов оповещения и экстренной информации населению осуществляется подачей сигнала «ВНИМАНИЕ ВСЕМ!» путем включения сетей электрических, электронных сирен и мощных акустических систем длительностью до 3 минут с последующей передачей по сетям связи, в том числе сетям связи телерадиовещания, через радиовещательные и телевизионные передающие станции операторов связи и организаций телерадиовещания с перерывом вещательных программ аудио- и (или) аудиовизуальных сообщений длительностью не более 5 минут.

В мирное время основным способом информирования населения об опасностях является доведение речевой (текстуальной) информации в виде *типовых информационных сообщений*.

На каждый типовой (характерный и наиболее вероятный для конкретной территории) случай возникновения ЧС природного и техногенного характера органами управления РСЧС субъекта РФ разработаны вари-

анты соответствующих текстовых сообщений. В содержании этих типовых сообщений отражается не только информация о наличия тех или иных опасностей, но и наиболее эффективные меры защиты от поражающих факторов опасных природных явлений, аварий и катастроф, полученные в результате их прогнозирования (моделирования).

Разработанные варианты информационных сообщений записаны и хранятся на различных носителях дежурных (дежурно-диспетчерских) служб органов повседневного управления РСЧС (операторов узлов сетей вещания).

Если появляется угроза или возникает опасная ситуация, отличная от ранее прогнозируемой (в том числе - типовой), то в этом случае оперативные дежурные службы территориальных органов МЧС России немедленно проводят всесторонний анализ обстановки, вырабатывают, утверждают у руководства и доводят до населения соответствующие экстренные сообщения для минимизации негативных последствий.

В настоящее время существуют и совершенствуются различные системы оповещения и информирования населения, которые отличаются своим назначением, содержанием решаемых задач, а функционируют в соответствии с установленным порядком.

Системы оповещения и информирования населения

Система оповещения населения включается в систему управления ГО и РСЧС, обеспечивающей доведение до населения, органов управления и сил ГО и РСЧС сигналов оповещения и (или) экстренной информации, и состоит из комбинации взаимодействующих элементов, состоящих из специальных программно-технических средств оповещения, средств комплексной системы экстренного оповещения населения (далее – КСЭОН), общероссийской комплексной системы информирования и оповещения населения (далее – ОКСИОН) в местах массового пребывания людей, громкоговорящих средств на подвижных объектах, мобильных и носимых средств оповещения, а также обеспечивающих ее функционирование каналов линий связи и сетей передачи данных единой сети электросвязи Российской Федерации [3].

Системы оповещения населения создаются на следующих уровнях функционирования РСЧС:

- *на региональном уровне* – региональная автоматизированная система централизованного оповещения (далее – РАСЦО);

- *на муниципальном уровне* – муниципальная автоматизированная система централизованного оповещения (далее – МАСЦО);

- *на объектовом уровне* – локальная система оповещения (далее – ЛСО).

РАСЦО и МАСЦО создают соответственно органы государственной власти субъектов РФ и органы местного самоуправления.

Границами зон действия РАСЦО и МАСЦО являются административные границы субъекта РФ и муниципального образования соответственно.

Системы оповещения могут быть задействованы как в мирное, так и в военное время.

РАСЦО является главной системой оповещения населения в военное время и доведения экстренных сообщений в мирное время. Основной задачей РАСЦО является обеспечение доведения сигналов оповещения и экстренной информации до:

- руководящего состава ГО и РСЧС субъекта РФ;
- территориального органа МЧС России по субъекту РФ;
- органов, специально уполномоченных на решение задач в области защиты населения и территорий от ЧС и ГО при органах местного самоуправления;
- единых дежурно-диспетчерских служб муниципальных образований;
- сил ГО и РСЧС субъекта РФ;
- дежурных (дежурно-диспетчерских) служб организаций, имеющих ЛСО;
- людей, находящихся на территории соответствующего субъекта РФ.

Комплекс технических средств РАСЦО включает в себя несколько подсистем. Так, например, РАСЦО Санкт-Петербурга состоит из:

- подсистемы управления и каналов связи;
- подсистемы электросиренного оповещения;
- подсистемы речевого оповещения на базе сетей связи операторов связи проводного радиовещания на территории Санкт-Петербурга;
- подсистемы оперативного задействования каналов радиовещательных и телевизионных станций в Санкт-Петербурге;
-подсистемы задействования систем оповещения объектов, сопряженных с РАСЦО;
- автоматизированной подсистемы оповещения по телефонным линиям;
- подсистемы задействования специальных технических средств оповещения;
- других подсистем задействования комплексов технических средств и информационных технологий, используемых для оповещения населения Санкт-Петербурга о чрезвычайных ситуациях [4].

Основной задачей МАСЦО является обеспечение доведения сигналов оповещения до:

- руководящего звена ГО и звена территориальной подсистемы РСЧС муниципального образования;

- сил ГО и РСЧС муниципального образования;

- дежурных (дежурно-диспетчерских) служб организаций, имеющих ЛСО, и дежурных служб (руководителей) социально значимых объектов;

- людей, находящихся на территории соответствующего муниципального образования.

После расследования причин и последствий наводнения в Краснодарском крае в 2012 году для устранения выявленных недостатков и совершенствования системы оповещения населения Президентом Российской Федерации 13.11.2012 был издан указ №1522 «О создании комплексной системы экстренного оповещения населения об угрозе или возникновении чрезвычайных ситуаций».

Целью создания КСЭОН является достижение гарантированного оповещения населения на территориях, подверженных воздействию быстроразвивающихся опасных природных явлений и техногенных процессов (в зонах экстренного оповещении) [5].

КСЭОН - это элемент системы оповещения населения о чрезвычайных ситуациях, представляющий собой комплекс программно-технических средств систем оповещения и мониторинга опасных природных явлений и техногенных процессов, обеспечивающий доведение сигналов оповещения и экстренной информации до органов управления РСЧС и до населения в автоматическом и (или) автоматизированном режимах [1].

КСЭОН создается на *региональном, муниципальном и объектовом уровнях* в зависимости от наличия территорий, подверженных риску возникновения быстроразвивающихся опасных природных явлений и техногенных процессов, представляющих непосредственную угрозу жизни и здоровью людей, находящихся на них. Отличительной особенностью функционирования КСЭОН стало привлечение к оповещению и информированию населения операторов мобильной связи и информационно-телекоммуникационной сети «Интернет». Границами зон действия (создания) КСЭОН являются границы зон экстренного оповещения населения. В Санкт-Петербурге, например, установлена 21 зона экстренного оповещения населения в местах размещения химически опасных объектов [6].

ОКСИОН предназначена для информирования и оповещения людей в местах их массового пребывания. ОКСИОН является составной частью системы управления РСЧС и обеспечивает информационную поддержку при выявлении ЧС, принятии решений и управлении в кризисных ситуациях. Информирование и оповещение населения происходит при помощи терминальных комплексов, которые включают в себя:

- жидкокристаллические панели, размещенные в зданиях с массовым пребыванием людей (образовательные учреждения, вокзалы, аэропорты, учреждения культуры, спорта, торговые, развлекательные центры и т.п.);

- светодиодные экраны на открытых пространствах (на зданиях, площадях, пересечениях городских магистралей, при въездах в город и т.п.);

- устройства типа «бегущая строка», информационные стойки;

- мобильные комплексы информирования и оповещения населения.

Применение ОКСИОН (с 2006 г.) повысило оперативность одновременно оповещаемых (информируемых) людей в местах их массового пребывания об угрозах и правилах поведения.

ЛСО создают организации, эксплуатирующие опасные производственные объекты I и II классов опасности, особо радиационно опасные и ядерно опасные производства и объекты, последствия аварий на которых могут причинять вред жизни и здоровью населения, проживающего или осуществляющего хозяйственную деятельность в зонах воздействия поражающих факторов за пределами их территорий, гидротехнические сооружения чрезвычайно высокой опасности и гидротехнические сооружения высокой опасности [3].

Основной задачей ЛСО является обеспечение доведения сигналов оповещения и экстренной информации до:

- руководящего состава ГО и персонала организации, эксплуатирующей вышеуказанные объекты, объектового звена РСЧС;

- объектовых аварийно-спасательных формирований, в том числе специализированных;

- единых дежурно-диспетчерских служб муниципальных образований, попадающих в границы зоны действия ЛСО;

- руководителей и дежурных служб организаций, расположенных в границах зоны действия ЛСО;

- людей, находящихся в границах зоны действия ЛСО.

При помощи ЛСО можно в короткие сроки оповестить о возникновении угрозы вследствие аварии работников своего предприятия, а также руководство всех учреждений, организаций и населения, которые могут попасть в зону действия опасных факторов. В этих условиях оповещение осуществляется непосредственно дежурным диспетчером самого предприятия. Границы зон действия конкретных ЛСО определяются в соответствии с законодательством РФ.

Важно отметить, что не только организации, имеющие особо опасные объекты, должны иметь собственную систему оповещения. Федеральный закон №68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» устанавливает, что

организации обязаны «предоставлять в установленном порядке информацию в области защиты населения и территорий от чрезвычайных ситуаций, а *также оповещать работников организаций об угрозе возникновения или возникновении чрезвычайных ситуаций* (подпункт «з» ч.1 ст. 14).

Это требование конкретизирует Свод правил СП 133.13330.2012 «Сети проводного радиовещания и оповещения в зданиях и сооружениях. Нормы проектирования». Во-первых, нормативный документ вводит понятие «объектовая система оповещения» (далее – ОСО). Под *ОСО понимается совокупность технических и организационных средств оповещения, обеспечивающая доведение сигналов и информации оповещения до руководителей и персонала объекта, объектовых сил и служб гражданской обороны* (п.3.10). Во-вторых, обязывает создавать ОСО *на объектах и в организациях с одномоментным нахождением более 50 человек (включая персонал), а также на социально важных объектах и объектах жизнеобеспечения населения вне зависимости от численности одномоментно находящихся людей* (п.5.5). ОСО создают на базе существующей сети связи, сети звукофикации объекта и специальной аппаратуры комплекса оповещения (п.5.6) [7].

Кроме того, в соответствии с ч.2 ст.54 Федерального закона №123-ФЗ «Технический регламент о требованиях пожарной безопасности» системы пожарной сигнализации, оповещения и управления эвакуацией (далее – СОУЭ) людей при пожаре должны быть установлены на объектах, где воздействие опасных факторов пожара может привести к травматизму и (или) гибели людей. Таких организаций большинство! При этом СОУЭ 3-го, 4-го и 5-го типов (учитывается степень пожарной опасности объекта защиты) кроме звукового и светового оповещения имеют и *речевое оповещение.*

В нормативном документе указывается, что для оповещения работников организации и иных граждан, находящихся на ее территории, об угрозе возникновения или возникновении чрезвычайных ситуаций применяются как технические средства оповещения, так и элементы СОУЭ [3].

Неотъемлемой составной частью ОСО должна быть сеть проводного радиовещания, ретрансляционные точки которой во многих организациях, к сожалению, находятся в неработоспособном состоянии. Необходимо понимать, что в военное время характерным результатом применения противником современных средств поражения будет резкое нарушение, а иногда и полное отсутствие электроснабжения населенных пунктов, что, в свою очередь, исключит функционирование многих традиционных источников информации, средств массой коммуникации. Более того, уже в настоящее время оружие в военных конфликтах применяется в сочетании с мощным радиоэлектронным подавлением прак-

тически всех видов связи, что также обусловливает необходимость иметь надежные каналы передачи информации. В этих условиях именно проводное радиовещание отличается высокой помехозащищенностью, живучестью и энергонезависимостью.

Совершенно правильно поступают те руководители организаций, учреждений и предприятий, которые не только восстановили свои радиоточки, но и путем установки аппаратуры сопряжения подключают ОСО к комплексу технических средств РАСЦО (МАСЦО). В Санкт-Петербурге, например, к РАСЦО подключено более 600 объектовых систем оповещения.

Функционирование систем оповещения

Применение по предназначению систем оповещения планируется и осуществляется в соответствии с разработанными положениями о данных системах, а также планами гражданской обороны и защиты населения (планами гражданской обороны) и планами действий по предупреждению и ликвидации чрезвычайных ситуаций.

Дежурные (дежурно-диспетчерские) службы органов повседневного управления РСЧС, получив в системе управления ГО и РСЧС сигналы оповещения и (или) экстренную информацию, подтверждают получение и немедленно доводят их до руководителей высших исполнительных органов государственной власти субъектов РФ, органов местного самоуправления, организаций (собственников объектов, производства, гидротехнического сооружения), на территории которых могут возникнуть или возникли чрезвычайные ситуации, а также органов управления и сил ГО и РСЧС соответствующего уровня.

Решение на применение РАСЦО, МАСЦО и ЛСО (ОСО) принимается соответственно высшими должностными лицами субъекта РФ, руководителями органов местного самоуправления (главами местных администраций) и руководителями организаций, имеющих ЛСО (ОСО).

КСЭОН применяется в автоматическом режиме от систем мониторинга опасных природных явлений и техногенных процессов или в автоматизированном режиме по решению высшего должностного лица субъекта РФ, руководителя органа местного самоуправления, организации (собственника объекта, производства, гидротехнического сооружения), в ведении которого находится соответствующая КСЭОН.

Передача сигналов оповещения и экстренной информации может осуществляться *в автоматическом, автоматизированном или ручном режимах функционирования* систем оповещения.

В *автоматическом режиме* функционирования системы оповещения включаются (запускаются) по заранее установленным программам при получении управляющих сигналов (команд) от систем оповещения

вышестоящего уровня или непосредственно от систем мониторинга опасных природных явлений и техногенных процессов без участия соответствующих дежурных (дежурно-диспетчерских) служб, ответственных за включение (запуск) систем оповещения.

В *автоматизированном режиме* функционирования включение (запуск) систем оповещения осуществляется соответствующими дежурными (дежурно-диспетчерскими) службами, уполномоченными на включение (запуск) систем оповещения, с автоматизированных рабочих мест при поступлении установленных сигналов (команд) и распоряжений.

В *ручном режиме* функционирования:

- уполномоченные дежурные (дежурно-диспетчерские) службы органов повседневного управления РСЧС осуществляют включение (запуск) оконечных средств оповещения непосредственно с мест их установки, а также направляют заявки операторам связи и (или) редакциям средств массовой информации на передачу сигналов оповещения и экстренной информации в соответствии с законодательством;

- задействуются громкоговорящие средства на подвижных объектах, мобильные и носимые средства оповещения [3].

Автоматический режим функционирования является основным для ЛСО и КСЭОН, при этом для них допускается и автоматизированный режим. Основной режим функционирования РАСЦО и МАСЦО – автоматизированный.

Рассмотрение вопросов об организации оповещения населения и работников организаций, определение способов и сроков оповещения осуществляется комиссиями по предупреждению и ликвидации чрезвычайных ситуаций и обеспечению пожарной безопасности соответствующего уровня.

С целью контроля за поддержанием в готовности систем оповещения населения проводятся их комплексные и технические проверки с установленной нормативными документами периодичностью. Для обеспечения оповещения максимального количества людей, попавших в зону ЧС, в том числе неохваченных автоматизированными системами централизованного оповещения, создается *резерв технических средств оповещения* (стационарных и мобильных). Номенклатура, объем, порядок создания и использования устанавливаются создающими этот резерв органами государственной власти субъектов РФ, органами местного самоуправления и организациями [3].

Перспективы развития систем оповещения и информирования населения

1. Общим направлением развития систем оповещения и информирования населения является повышение уровня готовности технических

средств оповещения, а также совершенствование профессиональной подготовленности дежурного (дежурно-диспетчерского) и технического обслуживающего персонала.

2. Создание резерва технических средств оповещения (стационарных и мобильных) особенно для обеспечения оповещения максимального количества людей, попавших в зону чрезвычайной ситуации, в том числе на территориях, неохваченных автоматизированными системами централизованного оповещения.

3. Модернизация (реконструкция) систем оповещения за счет внедрения новых научных разработок в совершенствование технических устройств, программно-аппаратных средств, осуществляющих прием, обработку и передачу аудио- и аудиовизуальных, иных сообщений об угрозе или возникновении чрезвычайных ситуаций и правилах поведения населения и работников организаций.

4. Увеличение зон охвата оповещаемого работающего и неработающего населения о различных угрозах и опасностях, как в мирное, так и в военное время. Достижение перекрытия зон оповещения различными техническими средствами для гарантированного доведения экстренной информации особенно в местах массового пребывания людей, в районах расположения потенциально опасных объектов.

5. Достижение уверенного контроля и визуализации хода оповещения в реальном масштабе времени с отображением списка оповещаемых объектов (органов управления, должностных лиц), типа сигнала оповещения, общего состояния каналов оповещения, результирующего времени оповещения.

6. Развитие сети мониторинга опасных природных явлений и техногенных процессов за счет внедрения технических средств запуска систем оповещения (особенно КСЭОН, ЛСО) в автоматическом режиме функционирования, сокращение времени от установления возможной угрозы или факта возникновения чрезвычайной ситуации до оповещения или информирования населения.

7. Создание в категорированных организациях, организациях, продолжающих работу в военное время, а также в организациях с массовым пребыванием людей, образовательных, медицинских, имеющих важное социальное значение, на объектах обеспечения жизнедеятельности и других учреждениях собственных объектовых систем оповещения. Состав этих систем оповещения должен соответствовать особенностям территориально-производственной или иной деятельности организаций с обязательным программным и техническим сопряжением с РАСЦО (МАСЦО, КСЭОН).

8. Активизация работы по привлечению к оповещению и информированию населения на региональном и муниципальном уровнях операторов мобильной связи, различных платформ информационно-телекоммуникационной сети «Интернет», сети систем персонального радиовызова, ведомственных сетей связи. Развитие сети местной телефонной связи, в том числе установка таксофонов, предназначенных для оказания универсальных услуг телефонной связи с функцией оповещения.

9. Создание в обязательном порядке во всех новых районах массовой жилой застройки населенных пунктов дополнительных, вновь создаваемых фрагментов соответствующих систем РАСЦО (МАСЦО) с соблюдением установленных норм расположения технических средств оповещения: сети электрических (электронных) сирен; сети уличной радиофикации; сети проводного радиовещания и т.п.

10. Совмещение (интеграция, техническое сопряжение) систем оповещения и информирования населения (технических устройств) с системами безопасности (отдельными элементами). Например, с системами видеонаблюдения, аппаратно-программным комплексом «Безопасный город», системами управления доступом, датчиками контроля пороговых значений уровней ионизирующего излучения, концентрации опасных веществ в атмосфере и другими.

Таким образом, несмотря на различия в предназначении, масштабе решаемых задач, уровнях функционирования, применяемых технических средствах и других показателей, имеющиеся системы оповещения в значительной степени интегрированы, сопрягаются технически и в целом взаимно дополняют друг друга. Это является материальной основой для своевременного доведения до населения, работников организаций сигналов оповещения, экстренной и иной информации, как в мирное, так и в военное время.

Литература

1. Федеральный закон РФ от 21.12.1994 №68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера».

2. ГОСТ 42.0.02-2001 «Гражданская оборона. Термины и определения основных понятий».

3. Приказ МЧС России и Министерства цифрового развития, связи и массовых коммуникаций РФ от 31.07.2020 №578/365 «Об утверждении Положения о системах оповещения населения».

4. Постановление Правительства Санкт-Петербурга от 06.08.2012 №798 «Об организации оповещения населения Санкт-Петербурга о чрезвычайных ситуациях мирного и военного времени».

5. Указ Президента РФ от 13.11.2012 №1522 «О создании комплексной системы экстренного оповещения населения об угрозе или о возникновении чрезвычайных ситуаций».

6. Постановление Правительства Санкт-Петербурга от 04.07.2013 №473 «О мерах по реализации Указа Президента РФ от 13.11. 2012 №1522», приложение №2.

7. СП 133.13330.2012 «Сети проводного радиовещания и оповещения в зданиях и сооружениях. Нормы проектирования».

УДК 338

Угольников Владимир Владимирович
канд. экон. наук
Санкт-Петербургский государственный
химико-фармацевтический университет
Минздрава России
Угольникова Ольга Дмитриевна
канд. физ.-матем. наук
Санкт-Петербургский государственный
экономический университет

СПЕЦИФИКА ЦИФРОВОЙ ТРАНСФОРМАЦИИ ЗДРАВООХРАНЕНИЯ (НА ПРИМЕРЕ ФАРМАЦЕВТИЧЕСКИХ ПРЕДПРИЯТИЙ)*

*Исследование выполнено при финансовой поддержке РФФИ и БРФФИ в рамках научного проекта № 20-510-00002

Аннотация. Статья посвящена вопросам цифровой трансформации фармацевтический предприятий, входящих в структуру здравоохранения. Рассмотрены факторы, способствующие развитию цифровой трансформации в фармацевтике, системы оценки цифровизации здравоохранения.

Ключевые слова: цифровая трансформация, цифровые технологии, здравоохранение, фармацевтические предприятия, организации, государственные проекты и программы развития.

Ugolnikov V.V.
Saint Petersburg State Chemical Pharmaceutical University
Ugolnikova O.D.
St. Petersburg State University of Economics

THE DIGITAL TRANSFORMATION OF HEALTHCARE SPECIFICS

Annotation. The article is devoted to the issues of digital transformation of pharmaceutical enterprises that are part of the healthcare structure. The factors contributing to the development of digital transformation in pharmaceuticals, the evaluation system of digitalization of healthcare are considered.

Keywords: digital transformation, digital technologies, healthcare, pharmaceutical enterprises, organizations, government projects and development programs.

Актуальность темы исследования подтверждается глубоким интересом мирового научного сообщества к выработке теории и методологии трансформации производства в условиях зарождения седьмого технологического уклада в рамках «Индустрии 4.0».

В индексах цифровизации на конец 2019 г. Российская Федерация имеет невысокие рейтинги, например, по Индексу цифровой связности — 49 место (из 79), Индекс цифровой конкурентоспособности — 38 место (из 63).

Данные результаты вызвали необходимость выработки стратегических решений на уровне обеспечения национальной безопасности [1].

Главным этапом преобразований, трансформации экономики в целом, является «цифровая трансформация». Ее структура эволюционно складывалась из этапов автоматизации (передачи управления производственными процессами машине), информатизации (ИКТ в обеспечение связей производственных процессов и массивов данных) [2], цифровизации (установление цифровых систем сбора, обработки, хранения и передачи данных). Цифровая трансформация представляет целостный комплекс преобразований, в том числе бизнес-моделей.

В систему государственных проектов по обеспечению национальной безопасности входит национальный проект «Здравоохранение» [3]. Его реализация способствует решению взаимоувязанных проблем медицинской, демографической, социально-экономической, экономической безопасности. В структуре [3] содержится 8 проектов федерального значения, в том числе «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)» ([4], [5]).

На этапе цифровизации радикально меняется управление в сфере здравоохранения, корпоративная культура, внешние коммуникации. Фармацевтическая промышленность является одной из основных составляющих здравоохранения. Новые условия хозяйствования фармацевтических предприятий, с цифровизацией коммуникаций, планирования, мониторинга, производственных процессов востребуют соответствующую стратегию цифровой трансформации фармпредприятий. На цифровой платформе происходит передача информации производителям фармацевтической продукции о тенденциях заболеваемости, потенциальном спросе на конкретные виды лекарственных препаратов, платежеспособности населения и т.д., что позволяет принимать эффективные управленческие решения этого уровня.

Необходимо отметить такие факторы, способствующие востребованности цифровых решений в здравоохранении, как старение населения, повышение пенсионного возраста, сокращение рабочих мест в экономике в целом и конкуренция на рынке труда человеческого капитала, в структуру которого входит капитал здоровья, на рынке труда, пандемия COVID-19 как новая угроза жизни и здоровью жителей планеты, резкий рост требований населения к качеству услуг здравоохранения. Непосредственно среди фармацевтических предприятий идет острая конкуренция на рынке лекарственных средств.

Уровень и новизна постановки задачи исследования подтверждается неразработанностью теории и практики цифровой трансформации отраслей экономики - здравоохранения и промышленности. В частности, отсутствует интегральный показатель цифровой зрелости фармацевтических предприятий.

Сложность исследования состоит в обосновании параллельного оперирования понятиями «цифровизация и цифровая трансформация здравоохранения» и «цифровая трансформация фармацевтических предприятий». В условиях всеобщей глобальной цифровизации дано описание первого.

В рамках целостного исследования были использованы: эволюционный и этимологический подход, метод сравнения, подход, логический метод, анализ, описание и обобщение, классификация, метод статистического анализа, аналогия. Работа опирается на фундаментальные теоретические исследования о циклическом развитии экономики, теорию экономической эффективности, инновационного менеджмента, дискуссионные статьи и труды ученых по цифровизации и трансформации экономики как доминантах мирового экономического развития.

Новизна определяется выводом автора о требовании методических разработок, относящихся к системе количественных оценок цифровой трансформации фармацевтических предприятий.

Здравоохранение является один из крупнейших сегментов мирового рынка, его емкость составляет около $3,7 млрд. долларов США. Спрос на услуги цифрового здравоохранения увеличивается из-за роста численности населения, увеличения продолжительности жизни, улучшения благосостояния в странах с развивающейся экономикой. Среди уже обозначившихся тенденций цифрового здравоохранения находятся как признанные лидеры, так и потенциально перспективные. Четко проявившимися или только обозначившимися трендами являются, например, [6]:

– телемедицина как дистанционные консультации врачей (среднегодовой темп роста глобального рынка телемедицины по прогнозам составит 19,3%, к 2026 году рынок вырастет $45 до $175 млрд.),

– мониторинг состояния здоровья и простой доступ пациента к широкому спектру клинических анализов, цифровые решения для которых встроены в существующие наборы для тестирования,

– приложения и веб-сайты для поиска врачей и специалистов на электронной карте из большого числа учреждений здравоохранения по симптомам заболевания,

– неэкстренные транспортировки в лечебные учреждения по медицинским показаниям для регионов без необходимой инфраструктуры,

– управление приемом лекарств и питанием пациентов.

Фармацевтические предприятия работают в едином цифровом поле здравоохранения в следующих формах:

1. собственные разработки и создание платформ для внедрения фармпродуктов в терапевтические области или иные области здравоохранения;

2. разработки поведенческих программ для воздействия на результаты стартапов;

3. чистое инвестирование в ИТ-компании.

Большое значение имеют ожидания и потребительские требования пациентов, подключенных к интернет-сети, стремящихся максимально контролировать состояние здоровья, питания, лечения. Фармацевтические организации, лечебно-профилактические учреждения, работодатели, пациенты на протяжении полного цикла медицинской помощи или другого ведения пациента вовлечены в тесное взаимодействие.

Цифровая эпоха требует изменений структуры фармацевтических предприятий, компаний. Во-первых, требуются ресурсы на разработку и коммерциализацию цифровых продуктов. Во-вторых, необходимы в управленческом звене предприятий ИТ- специалисты нового класса «цифровых директоров».

Цифровые технологии в медицине крайне перспективны. Это влечет требование по созданию современных траекторий партнерских отношений

фармацевтических и медицинских организаций, совместного участия в процессе разработки технологии влияния на пациента, который, в свою очередь, является информированным потребителем. Часть предприятий выбрала стратегию развития и совершенствования через улучшение коммуникаций. В качестве примера зарубежных партнерств можно привести партнерство стартапа Pear Therapeutics [7] и крупной фармкомпании Sandoz в области цифровой терапии (2018 г.). Суть проекта: вместе с лекарством предлагается цифровая терапевтика - психосоциальная роль (пациент через мобильное приложение получает весь требуемый объем помощи от сертифицированных консультантов и групп поддержки). В силу сложности цифровой трансформации фармкомпании данный проект был остановлен ее руководителем.

Другим примером партнерства служит соглашение о сотрудничестве фармкомпании Bayer с 11-ю стартапами в сфере цифрового здравоохранения по реализации цифровых решений при заболеваниях органов зрения, сердечно-сосудистой системы, органов дыхания, онкологических заболеваниях.

Инвестиции в отрасль цифровой медицины рассмотрим на следующих примерах: компания NeuroMetrix (Уолтем, штат Массачусетс) разработала носимое болеутоляющее устройство Quell; компания Novartis (Швейцария) вложилась в IT-системы Numinous Games, что позволяет ей изучить проблемы лечения нейроэндокринных опухолей с помощью мультимодального подхода; транснациональная фармацевтическая корпорация Sanofi (Франция) - исследует, разрабатывает и производит фармпрепараты, потребительские товары для здоровья и вакцины - заключила соглашение с компанией FoodPrint, специализирующейся на информации пользователям о связи принимаемой пищи и ее влиянием на их здоровье. В 2017 году лидерами фармацевтического рынка стали скупаться mHealth-стартапы по разработке систем класса искусственной поджелудочной железы. Разработчики аналогичных систем для больных сахарным диабетом mySugr и Glooko сотрудничали с Roche и Novo Nordisk, соответственно. Заключение данных соглашений позволяет сделать вывод: потенциал приложений для контроля лечения социально значимых заболеваний крайне высок, а данное направление цифровой фармацевтики стало приоритетом.

Кейсы внедрения отечественных цифровых технологий в отрасли [8]:

Российская компания Intellogic разработала платформу Botkin.AI на базе ИИ, которая используется для анализа и обработки медицинских изображений, включая результаты компьютерной томографии, маммографии, рентгена и флюорографии. Сервис позволяет не только уменьшить нагрузку на медицинский персонал и ускорить процесс постановки диагноза, но и снизить вероятность врачебной ошибки [Botkin, 2021]

Компания «К-Скай» разработала платформу Webiomed, которая представляет собой систему поддержки принятия врачебных решений на базе ИИ, позволяющую производить групповую и индивидуальную оценку рисков развития заболевания (система предиктивной аналитики). Система может использоваться врачом при определении тактики лечения, инструментом внутреннего контроля качества оказания медуслуг. Решение используется в медицинских организациях регионов России [Webiomed, 2021]

С 2021 г. на федеральном уровне организуется мониторинг цифровой зрелости здравоохранения по направлениям: запись на прием к врачу с использованием ЕПГУ; интегрированная электронная медкарта, доступная на ЕПГУ; централизованная обработка и хранение в электронном виде результатов диагностических исследований; дистанционный мониторинг состояния здоровья; телемедицинские консультации в форматах «врач - врач» и «врач - пациент» посредством ЕПГУ с использованием видеоконференцсвязи; внедрение Единой региональной диспетчерской скорой медицинской помощи. По итогам 2020 г. в тройку лидеров по перечисленным направлениям вошли Тульская, Тамбовская и Ленинградская области.

В целях анализа предложенных законодателем показателей и количественных оценок процесса цифровизации организаций здравоохранения, подсистемой которого являются фармацевтические предприятия и организации, рассмотрим более подробно проект «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)» [9] с планируемым периодом реализации до конца 2024 г.

Цель проекта - преобразование и повышение эффективности функционирования отрасли здравоохранения на всех уровнях, условия для использования гражданами электронных услуг и сервисов в сфере здравоохранения.

ЕЦК (единый цифровой контур) является инструментом повышения отраслевой эффективности, и как многофункциональный инструмент, способен формировать тренды информатизации здравоохранения страны и развития отрасли на ближайшие десятилетия.

Во исполнение указанного выше проекта вышел Приказ Министерства здравоохранения [9] о методике расчета показателей реализации этого проекта. Содержание показателей:

1. Основной показатель «Число граждан, воспользовавшихся услугами (сервисами) в Личном кабинете пациента «Мое здоровье» на Едином портале государственных услуг и функций, млн. чел.».

2. Пять дополнительных показателей:

2.1. «Доля медицинских организаций государственной и муниципальной систем здравоохранения, использующих медицинские информационные системы для организации и оказания медицинской помощи гражданам, обеспечивающих информационное взаимодействие с ЕГИСЗ, %»;

2.2. «Доля записей на прием к врачу, совершенных гражданами дистанционно, %»;

2.3. «Доля граждан, являющихся пользователями ЕПГУ, которым доступны электронные медицинские документы в Личном кабинете пациента Мое здоровье по факту оказания медпомощи, %»;

2.4. «Доля случаев оказания медпомощи, по которым предоставлены электронные медицинские документы в подсистемы ЕГИСЗ, %»;

2.5. «Доля медицинских организаций государственной и муниципальной систем здравоохранения, подключенных к централизованным подсистемам ГИС в сфере здравоохранения субъектов РФ, %».

В Приложениях №1- №5 к Приказу предложены их методики расчета.

Приложение №1. Методика расчета основного показателя.

Он равен числу граждан, воспользовавшихся услугами (сервисами) в личном кабинете пациента Мое здоровье на Едином портале государственных и муниципальных услуг (функций), тыс. чел., базовой из которых является формула:

$$\mathrm{C}_{\text{общ РФ}} = \sum_1^n C_{n_i} + C_{\text{ип}} \qquad (1)$$

где $\mathrm{C}_{\text{общ РФ}}$ - число российских граждан, воспользовавшихся услугами (сервисами) в личном кабинете Мое здоровье;

n - число субъектов РФ;

$C_{\text{ип}}$ – число российских граждан, не отнесенных ни к одному субъекту РФ, воспользовавшихся указанными выше услугами и сервисами.

Приложение №2. Методика расчета дополнительного показателя 2.1 в % по следующей формуле:

$$D_{\text{МО}}\left[\left(\mathrm{C}_{\text{ФЭР ОТП}}/\mathrm{C}_{\text{ФЭР МО}} + \mathrm{C}_{\text{ИЗМ КОТП}}/\mathrm{C}_{\text{ИЗМ КМО}}\right)\mathrm{X}100\%\right]/2 \qquad (2)$$

где $\mathrm{C}_{\text{ФЭР ОТП}}$ - количество территориально-выделенных структурных подразделений медицинских организаций государственной и муниципальной систем здравоохранения, оказывающих первичную медико-санитарную медицинскую помощь, передающих информацию в подсистему «Федеральная электронная регистратура» ЕГИСЗ, ед.;

$С_{ФЭР\ МО}$ - количество территориально-выделенных структурных подразделений медицинских организаций указанных систем здравоохранения, подключенных к сети «Интернет», оказывающих первичную медико-санитарную медицинскую помощь, сведения о которых содержатся в подсистеме «Федеральный реестр медицинских организаций», ед.;

$С_{ИЗМ\ КОТП}$ - количество таких же структурных подразделений медорганизаций указанных выше систем здравоохранения, передающих информацию в подсистему «Федеральная интегрированная электронная медицинская карта» ЕГИСЗ, ед.;

$С_{ИЗМ\ КМО}$ - общее количество таких же структурных подразделений медорганизаций указанных выше систем здравоохранения, подключенных к сети «Интернет», оказывающих медпомощь и осуществляющих оформление медицинской документации, сведения о которых содержатся в подсистеме «Федеральный реестр медицинских организаций» ЕГИСЗ, ед.

Приложение №3. Методика расчета дополнительного показателя 2.2 (%):

$$D_{дистз} = \frac{С_{фзрз}}{С_{омсз}} \text{ x } 100\% \quad (3)$$

где $D_{дистз}$ - доля записей к врачу, совершенных дистанционно;

$С_{фзрз}$ - число записей к врачу в подсистеме «Федеральная электронная регистратура» ЕГИСЗ по всем источникам записи (за исключением регистратуры), ед.;

$С_{омсз}$ - общее число посещений, получаемых из ГИС ОМС, ед.

Приложение №4. Методика расчета дополнительного показателя 2.3 (%):

$$D_{эмдгр} = \frac{С_{рэмд}}{С_{омсгр}} \text{ x } 100\% \quad (4)$$

где $D_{эмдгр}$ - доля граждан - пользователей ЕПГУ, которым доступны электронные медицинские документы в кабинете Мое здоровье по факту оказания медпомощи, %;

$С_{рэмд}$ - число граждан - пользователей ЕПГУ, по которым по обращениям за медпомощью по ОМС зарегистрированы электронные медицинские документы в подсистеме ЕГИСЗ, чел.;

$С_{омсгр}$ - общее число граждан, получивших медпомощь по ОМС, чел.

Приложение №5. Методика расчета дополнительного показателя 2.4 (%):

$$D_{эмдсл} = \frac{С_{эмд}}{С_{омссл}} \text{ x } 100\% \quad (5)$$

где $D_{эмдсл}$ - доля случаев оказания медпомощи, по которым предоставлены электронные медицинские документы в подсистемы ЕГИСЗ;

$С_{эмд}$ - число зарегистрированных электронных медицинских документов в подсистемах «Федеральный реестр электронных медицинских документов» и «Федеральная интегрированная электронная медицинская карта» ЕГИСЗ, ед.;

$С_{омссл}$ - общее число случаев оказания медпомощи, получаемых из ГИС ОМС, ед.

Приложение №6. Методика расчета дополнительного показателя 2.5. Показатель рассчитывается по формуле:

$$D_з=\frac{V_у D_у+ V_с D_с+V_л D_л+V_а D_а+V_и D_и+V_ц D_ц+V_{ли} D_{ли}+V_{бр} D_{бр}+V_о D_о+ V_д D_д+V_б D_б+V_т D_т}{V_у+V_с+V_л+V_а+V_и+V_ц+V_{ли}+V_{бр}+V_о+V_д+V_б+V_т} \quad (6)$$

где $D_у$ - доля территориально-выделенных структурных подразделений медорганизаций государственной и муниципальной систем здравоохранения, передающих информацию в подсистему «Управление потоками пациентов» ГИС здравоохранения субъекта РФ от общего числа таких же структурных подразделений медорганизаций указанных систем здравоохранения, оказывающих медпомощь амбулаторно, стационарно и в условиях дневного стационара, коэффициент,

$V_у$ - вес показателя $D_у$, характеризующий влияние данной подсистемы на качество организации медпомощи, значение которого установлено экспертным путем и равно 1,3.

$D_с$ - доля таких же структурных подразделений медорганизаций, передающих информацию в подсистему «Управление скорой и неотложной медпомощи» в сфере здравоохранения субъекта РФ, от общего числа таких же структурных подразделений медорганизаций вышеуказанных систем здравоохранения, оказывающих медпомощь в условиях вне медорганизации (по месту вызова бригады скорой), коэффициент,

$V_с$ - вес показателя $D_с$, характеризующий влияние подсистемы на качество организации медпомощи, значение которого установлено экспертным путем и равно 1,3.

$D_л$ - доля таких же структурных подразделений медорганизаций указанных выше систем здравоохранения, в которых осуществляется назначение пациенту ЛС, отпускаемых бесплатно или со скидкой, и оформление рецептов на указанные ЛС при оказании медпомощи, передающих информацию в подсистему «Управление льготным лекарственным обеспечением» ГИС здравоохранения субъекта РФ, от общего числа аналогичных структурных подразделений медорганизаций указанных выше систем здравоохранения,

$V_{л}$ - вес показателя $D_{л}$, характеризующий влияние указанной подсистемы на качество организации медпомощи, значение которого установлено экспертным путем и равно 1,3.

$D_{а}$ - доля аптечных организаций, отпускающих пациенту или его законному представителю ЛС для медприменения по рецептам на ЛС, подлежащие бесплатному или со скидкой отпуску, передающих информацию в указанную выше подсистему, от общего числа таких аптечных организаций,

$V_{а}$ - вес показателя $D_{а}$, характеризующий влияние указанной подсистемы в части автоматизации деятельности аптечных организаций, характеризующий ее влияние на качество организации медпомощи, значение которого установлено экспертным путем и равно 1,3.

$D_{и}$ - доля таких же структурных подразделений медорганизаций указанных выше систем здравоохранения, передающих информацию в подсистему «Региональная интегрированная электронная медицинская карта» ГИС здравоохранения субъекта РФ, к общему числу таких же структурных подразделений названных медорганизаций указанных выше систем здравоохранения, оказывающих медпомощь,

$V_{и}$ - вес показателя $D_{и}$, характеризующий влияние указанной выше подсистемы на качество организации медпомощи, значение которого установлено экспертным путем и равно 1,3,

$D_{ц}$ - доля таких же структурных подразделений медорганизаций указанных выше систем здравоохранения, передающих информацию в подсистему «Центральный архив медицинских изображений» ГИС здравоохранения субъекта РФ, к общему числу таких же структурных подразделений медорганизаций указанных выше систем здравоохранения, оказывающих медпомощь в части инструментальной диагностики, за исключением фельдшерско-акушерских пунктов и фельдшерских пунктов, а также таких же структурных подразделений медорганизаций указанных выше систем здравоохранения, оказывающих скорую и паллиативную медицинскую помощь, коэффициент,

$V_{ц}$ - вес показателя $D_{ц}$, характеризующий влияние указанной выше подсистемы на качество организации медпомощи, значение которого установлено экспертным путем и равно 1,3.

$D_{ли}$ - доля таких же структурных подразделений медорганизаций указанных выше систем здравоохранения, передающих информацию в подсистему «Лабораторные исследования» ГИС здравоохранения субъекта РФ, к общему числу таких же структурных подразделений медорганизаций указанных выше систем здравоохранения, оказывающих медпомощь в части клинической лабораторной диагностики, за исключением скорой и паллиативной медпомощи, коэффициент,

$V_{\text{ли}}$- вес показателя $D_{\text{ли}}$, характеризующий влияние указанной выше подсистемы на качество организации медпомощи, значение которого установлено экспертным путем и равно 1,3.

$D_{\text{бр}}$ - доля таких же структурных подразделений медорганизаций указанных выше систем здравоохранения, передающих информацию в подсистему «Организации оказания медицинской помощи по профилям «Акушерство и гинекология» и «Неонатология» (Мониторинг беременных)» ГИС здравоохранения субъекта РФ, к общему числу таких же структурных подразделений медорганизаций указанных выше систем здравоохранения, оказывающих медпомощь по указанным профилям, коэффициент,

$V_{\text{бр}}$- вес показателя $D_{\text{бр}}$, характеризующий влияние указанной подсистемы на качество организации медпомощи, значение которого установлено экспертным путем и равно 1.

D_o - доля территориально-выделенных структурных подразделений медорганизаций указанных выше систем здравоохранения, передающих информацию в подсистему «Организации оказания медпомощи больным онкологическими заболеваниями» ГИС здравоохранения субъекта РФ, к общему числу таких же структурных подразделений медорганизаций указанных выше систем здравоохранения, оказывающих первичную медико-санитарную помощь и специализированную, в том числе высокотехнологичную, медпомощь по профилю «Онкология», коэффициент,

V_o- вес показателя D_o , характеризующий влияние указанной выше подсистемы на качество организации медпомощи, значение которого установлено экспертным путем и равно 1.

$D_{\text{д}}$ - доля территориально-выделенных структурных подразделений я, передающих информацию в подсистему «Организации оказания профилактической медицинской помощи (диспансеризация, диспансерное наблюдение, профилактические осмотры)» ГИС здравоохранения субъекта РФ, к общему числу таких же структурных подразделений медорганизаций указанных выше систем здравоохранения, оказывающих профилактическую медпомощь, коэффициент,

$V_{\text{д}}$ - вес показателя $D_{\text{д}}$, характеризующий влияние указанной выше подсистемы на качество организации медпомощи, значение которого установлено экспертным путем и равно 1.

$V_{\text{б}}$ - доля территориально-выделенных структурных подразделений медорганизаций указанных выше систем здравоохранения, передающих информацию в подсистему «Организации оказания медицинской помощи больным сердечно-сосудистыми заболеваниями» ГИС здравоохранения субъекта РФ, к общему числу таких же структурных подразделений ме-

дорганизаций указанных выше систем здравоохранения, оказывающих медпомощь по профилю «Кардиология», коэффициент,

$V_б$ - вес показателя $V_б$, характеризующий влияние указанной выше подсистемы на качество организации медпомощи, значение которого установлено экспертным путем и равно 1,

$D_т$ - доля территориально-выделенных структурных подразделений медорганизаций указанных выше систем здравоохранения, оказывающих медпомощь с применением телемедицинских технологий, и передающих информацию в подсистему «Телемедицинские консультации» ГИС здравоохранения субъекта РФ, к общему числу таких же структурных подразделений медорганизаций указанных выше систем здравоохранения, оказывающих медпомощь с применением телемедицинских технологий, коэффициент,

$V_т$ - вес показателя $D_т$, характеризующий влияние указанной выше подсистемы на качество организации медпомощи, значение которого установлено экспертным путем и равно 1.

$D_з$ - средневзвешенное показателей по подсистемам ГИС здравоохранения субъекта РФ: «Управление потоками пациентов», «Управление системой оказания скорой медпомощи и медэвакуацией», «Управление льготным лекарственным обеспечением», «Региональная интегрированная электронная медицинская карта», «Центральный архив медицинских изображений», «Лабораторные исследования», «Организация оказания медпомощи по профилям…» к общему числу территориально-выделенных структурных подразделений медорганизаций указанных выше систем здравоохранения на основе правил настройки входимости данных подсистемы ЕГИСЗ.

К 2024 г. время ожидания пациентами медпомощи произойдет за счет реализации системы управления маршрутизацией и потоками пациентов. Все медорганизации, осуществляющие первичный прием граждан и амбулаторно-поликлиническую помощь, будут подключены к централизованной региональной системе «Управление потоками пациентов». Весь процесс лекарственного обеспечения от формирования заявки медорганизации на закупку ЛС до получения сведений о их выдаче будет автоматизирован. Результат - своевременное получение льготных ЛС, качественный мониторинг остатков ЛС в медорганизациях и аптеках. Консультации по сложным клиническим вопросам будут проводиться по централизованной телемедицинской системе. В 2024 г. во всех регионах страны планируется введение системы электронных рецептов и автоматизированное управление льготным лекарственным обеспечением. В личном кабинете «Мое здоровье» на портале государственных услуг будут доступны: запись к врачу, запись на диспансери-

зацию, подача заявления на медицинский полис, медицинские документы. Будут практиковаться выдача электронных рецептов на лекарства, система удаленных покупок лекарств. Проанализированный проект является системным документом, объединяющим в единую сеть производителя лекарственных препаратов, медицинских изделий, лечебно-профилактические учреждения и пациентов.

В статье были исследованы направления деятельности фармацевтических предприятий в развивающейся цифровой среде фармацевтической отрасли; направления цифровой фармацевтики, цифровая трансформация фармацевтической отрасли в целом. Необходимо исследовать понятие цифровой трансформации фармацевтической отрасли, которая содержит новый тип организационно-управленческих решений, производственной культуры фармпредприятий в условиях цифровой трансформации.

На основе анализа показателей цифровой трансформации здравоохранения и количественных оценок согласно формул расчета этих показателей необходимо разработать аналогичную систему цифровой зрелости фармпредприятий, отрасли.

В завершение укажем, что данное исследование является продолжением статей ([10] – [13]), а также составной частью ([14] - [15]).

Литература

1. Указ Президента Российской Федерации от 21.07.2020 г. №474 «О национальных целях развития Российской Федерации на период до 2030 года». [Электронный ресурс]. – URL: http://www.kremlin.ru/acts/bank/45726

2. Федеральный закон от 20.02.1995 г. №24-ФЗ (ред. от 10.01.2003 г.) «Об информации, информатизации и защите информации».

3. Национальный проект «Здравоохранение» (утвержден президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 24 декабря 2018 г. №16) [Электронный ресурс]. – URL: https://roszdravnadzor.ru/i/upload/images/2018/7/25/15325 12237.26174-1-15781.pdf

4. Паспорт федерального проекта «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)». [Электронный ресурс]. – URL: https://base.garant.ru/72185920/#block_777

5. Приказ Минздравсоцразвития №364 от 28.04.2011 об утверждении Концепции создания единой государственной информационной си-

стемы в сфере здравоохранения. [Электронный ресурс]. – URL: https://www.rosminzdrav.ru/documents/7200-prikaz-

6. Цифровая медицина в России. [Электронный ресурс]. – URL: https://evercare.ru/category/cifrovaya-medicina-v-rossii

7. Pear Therapeutics. Пионеры в области цифровой терапии по рецепту. [Электронный ресурс]. – URL: https://peartherapeutics.com/

8. Цифровая трансформация отраслей: стартовые условия и приоритеты: докл. к XXII Апр. междунар. науч. конф. по проблемам развития экономики и общества, Москва, 13–30 апр. 2021 г. / Г.И. Абдрахманова, К.Б. Быховский, Н.Н. Веселитская, К.О. Вишневский, Л.М. Гохберг и др.; рук. авт. кол. П.Б. Рудник ; науч. ред. Л.М. Гохберг, П.Б. Рудник, К.О. Вишневский, Т.С. Зинина; Нац. исслед. ун-т «Высшая школа экономики». – М.: Изд. дом Высшей школы экономики, 2021. — 239 с.

9. Приказ Министерства здравоохранения РФ от 2 апреля 2021 г. №290 «Об утверждении методик расчета показателей федерального проекта «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)», входящего в национальный проект «Здравоохранение».

10. Цифровизация экономики: теоретические аспекты и опыт зарубежных стран / Угольникова О.Д., Угольников В.В. – Экономический обозреватель, №20.31.0.105.

11. Сычев И.С., Угольников В.В. Экономическая безопасность фармацевтических предприятий – особенности текущего периода / Безопасность в профессиональной деятельности : сборник научных статей / под ред. д-ра техн. наук, проф. Г.В. Лепеша, канд. экон. наук, доц. С.Ю. Александровой, канд. физ.-мат. наук, доц. О.Д. Угольниковой – СПб. : Изд-во СПбГЭУ, 2021. С. 266-279.

12. Томилин Ю.А., Угольников В.В. Вопросы финансовой устойчивости фармацевтических предприятий / Безопасность в профессиональной деятельности : сборник научных статей / под ред. д-ра техн. наук, проф. Г.В. Лепеша, канд. экон. наук, доц. С.Ю. Александровой, канд. физ.-мат. наук, доц. О.Д. Угольниковой – СПб. : Изд-во СПбГЭУ, 2021. С. 279 – 287.

13. Маликова Н.Т., Угольников В.В. Технико-технологическая безопасность предприятий фармацевтической отрасли / Безопасность в профессиональной деятельности : сборник научных статей / под ред. д-ра техн. наук, проф. Г.В. Лепеша, канд. экон. наук, доц. С.Ю. Александровой, канд. физ.-мат. наук, доц. О.Д. Угольниковой – СПб. : Изд-во СПбГЭУ, 2021. С. 161 – 170.

14. Угольников В.В. Развитие фармацевтической отрасли в условиях обострения эпидемиологических угроз: экономический аспект / Уголь-

ников В.В. - Инновационные технологии и вопросы обеспечения безопасности реальной экономики : сборник научных трудов по итогам Всероссийской научно-практической конференции «Инновационные технологии и вопросы обеспечения безопасности реальной экономики». Санкт-Петербург. 27 марта 2020 года / под ред. д-ра техн. наук, проф. Г.В. Лепеша, канд. физ.-мат. наук, доц. О.Д. Угольниковой, канд. экон. наук, доц. С.Ю. Александровой. – СПб. : Изд-во СПбГЭУ, 2020. - С. 147-155.

15. Угольникова О.Д. Цифровая адаптация российской экономики: особенности, проблемы, перспективы / Угольникова О.Д. - Инновационные технологии и вопросы обеспечения безопасности реальной экономики : сборник научных трудов по итогам Всероссийской научно-практической конференции «Инновационные технологии и вопросы обеспечения безопасности реальной экономики». Санкт-Петербург. 27 марта 2020 года / под ред. д-ра техн. наук, проф. Г.В. Лепеша, канд. физ.-мат. наук, доц. О.Д. Угольниковой, канд. экон. наук, доц. С.Ю. Александровой. – СПб. : Изд-во СПбГЭУ, 2020, с. 214-221.

УДК 368.01.

Федорова Татьяна Аркадьевна
д-р экон. наук, профессор
Санкт-Петербургский государственный
экономический университет

ВНЕШНИЕ ШОКИ КАК ГЛОБАЛЬНАЯ УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Аннотация. В статье рассматриваются внешние шоки как особая группа глобальных рисков, угрожающих экономической безопасности современного общества на всех уровнях его организации. Сделана попытка раскрытия природы этих рисков и их определяющей роли в переходе на восстановительный тип экономического роста. Исследованы формы государственного регулирования этих процессов. Раскрыта роль страхования в финансировании рисков постпандемийной экономики.

Ключевые слова: глобальные риски экономической безопасности, инвестиционные мультипликаторы глобальные цепочки поставок, страхование.

Fedorova T.A.
St. Petersburg State University of Economics

EXTERNAL SHOCKS AS A GLOBAL THREAT TO ECONOMIC SECURITY

Annotation. The article discusses external shocks as a special group of global risks that threaten the economic security of modern society at all levels of its organization. An attempt is made to reveal the nature of these risks and their decisive role in the transition to a recovery type of economic growth. The forms of state regulation of these processes have been investigated. The role of insurance in financing the risks of a post-pandemic economy is revealed.

Keywords: global risks to economic security, investment multiples, global supply chains, insurance.

1. Внешние шоки как особая группа рисков, угрожающих экономической безопасности

Внешние шоки – это негативные события, которые воздействуют на экономическую систему извне из окружающей среды и практически не поддаются прогнозированию. По своей природе это неэкономические риски, обладающие высоким потенциалом опасности и огромной разрушительной силой. К ним относятся пандемии, климатические изменения, природные катастрофы. Действие таких рисков не локализовано в границах отдельных регионов и стран и зачастую носит общепланетарный характер. Это поистине глобальные риски, природа которых остается неясной ни по существу, ни по степени их связи с хозяйственной деятельностью человека.

В настоящее время наблюдается одновременное наступление этих рисков на человечество, которое отличается удивительной синхронностью и последовательностью, что позволяет предположить здесь наличие определенной тенденции. Вероятно, не случайно в последнее время в хозяйственную жизнь вошло понятие экосистемы, поднявшееся из глубин общественного подсознания. Финансовые и телекоммуникационные корпорации спешно формируют собственные экосистемы, пытаясь замкнуть в них как можно большее количество потребителей и производителей различных услуг в целях укрепления своей экономической власти. Но человек – это тоже элемент общей природной экосистемы, в которой его роль далеко не так очевидна, а положение не так неуязвимо, как представляется. Об этом говорят исторические факты, свидетельствующие о существовании в далеком прошлом на земле многих цивилизаций, от которых остались лишь отдельные артефакты. Можно предположить, что современная цивилизация с ее технологиями и агрессивной деструктивной идеологией

стала фактором планетарного риска и разрушения фундаментальных законов мироустройства. Ответы глобальной экосистемы достаточно очевидны, вероятно, одним из них стала пандемия коронавируса как удар со стороны самых древних и простых форм биологической жизни, находящихся на границе между живой и неживой материей и присутствующих в геноме человека.

Шоковый характер глобальных рисков выражается в их полной неожиданности. Перед ними бессильны все методы и модели прогнозирования и риск-менеджмента, не помогают огромные объемы больших данных и искусственный интеллект. Однако эта неожиданность и непредвиденность в определенной степени все же – лукавство, поскольку гибельные последствия действий отдельных индивидуумов и сообществ для них самих и для внешней среды, как правило, хорошо им известны. Неизвестны время и масштабы грядущих последствий. Поэтому в группу внешних шоков вполне могут быть включены конечные результаты деятельности людей, которые незаметно для них самих приобретают катастрофический характер и обрушиваются на них страшными бедствиями. Это техногенные и экологические катастрофы, торговые войны, геополитические конфликты, переходящие в гражданские и мировые войны. Все эти риски культивируются усилиями многих заинтересованных лиц, но не воспринимаются как реальные угрозы в текущем моменте.

Важным фактором, усугубляющим развитие гибельных тенденций, является разрушение традиционного сознания, заключающееся в отказе от ключевых человеческих ценностей и норм морали. Интернет и социальные сети стали инфраструктурой этого процесса, набирающего силу с каждым днем. Реальностью стало движение к торжеству зла в самых откровенных формах «эстетики» насилия, убийств, сексуальных извращений, всех возможных проявлений мракобесия и сатанизма. Направление удара – сознание детей, молодежи. Целью является дестабилизация социальной и политической жизни общества и его разрушение.

Масштабы распространения деструктивных воздействий на сознание детей и подростков в России оцениваются на уровне 7 млн. человек при ежегодном приросте вовлечения молодежи в экстремистские группы в 2 млн. человек. По результатам исследований Н. Касперской, основанных на данных анализа поисковых запросов в интернете, 40-50% подростков вовлечены в процесс деструктивной обработки сознания [1]. С полным основанием можно сделать вывод, что главной опасностью для существования России и многих других стран и народов являются их собственные дети, ставшие орудием мирового зла. На этом фоне готовность общества к объективному осознанию стоящих перед ним проблем явно недостаточна.

Современная рисковая ситуация характеризуется резким ростом уровня глобальной неопределенности, увеличением частоты и тяжести

ущербов. В результате растут масштабы экономических потерь, которые могут принимать две формы. Первая – реальный материальный ущерб в виде разрушения производства и потери ресурсов и инфраструктурных систем жизнеобеспечения. Вторая форма - выпадающие доходы и недопроизводство продукта, вызванные остановкой и свертыванием производства.

До 2020 года внешние шоки выражались в экологических и климатических рисках, которые поднялись от форм эпизодических материальных ущербов от загрязнения воды, воздуха, почвы, вырубки лесов до уровня глобального уничтожения среды обитания человека. Масштабы ущербов и потенциал разрушительного воздействия этих рисков неуклонно растут. По данным ООН за период с 1970 по 2015 год в результате природных катастроф пострадали 3,5 млн. человек, а размеры экономического ущерба выросли в 8,3 раза при росте объема мирового ВВП в 3 раза [2]. При этом нельзя не понимать, что оценка экономических потерь носит весьма условный характер. В 2020 году ущерб от крупных природных катастроф достиг 150 млрд. долл., максимума за все годы наблюдений; погибло более 3,5 тысяч человек и 13,5 миллионов вынуждены были покинуть места проживания [3]. Формы катастроф достаточно разнообразны. На российской территории ежегодно свирепствуют лесные пожары и наводнения В частности, 2019-20 годы ознаменовались катастрофическими лесными пожарами в Сибири, в результате которых сгорели десятки миллионов гектаров леса, а ущерб оценивается в 15-20 млрд. руб.

В современных условиях риски природных катастроф становятся важной экономической проблемой. При существующем уровне использования невоспроизводимых природных ресурсов и росте народонаселения экономика приблизилась к исчерпанию источников экономического роста. Разрушительные проявления природных рисков ведут к тому, что все большая часть ВВП должна направляться на восстановление разрушенных материальных активов и обеспечение простого воспроизводства общественного продукта. Этот неутешительный факт абсолютно не согласуется с господствующей в общественном сознании концепцией экономического роста, провозглашающий непрерывный рост общественного богатства и благосостояния как нечто незыблемое.

Пандемия 2020 года внесла новый и существенный акцент в хозяйственную жизнь. Риск пандемии коронавируса обладает особенностями, отличающими его от других глобальных рисков. Во-первых, он направлен непосредственно на физическое уничтожение населения и обладает исключительно высокой скоростью распространения и мутаций. Начавшись в Китае, пандемия за два-три месяца охватила все континенты, включая самые отдаленные и предельно изолированные от внешних воздействий северные территории. Во-вторых, она не сопровождается уничтожением

материальных активов, но ведет к временному прекращению хозяйственной деятельности с неопределенными горизонтами продолжительности. В-третьих, риск пандемии обладает способностью активного взаимодействия с экономическими рисками и порождает выраженный эффект кумуляции рисков. Пандемия стала шоком, обрушившим мировую экономику и ввергнувшим ее в рукотворный кризис, вызванный длительным карантином и запретом на хозяйственную деятельность. Вначале предполагалось, что локдаун закончится к концу 2020 года и начнется интенсивное восстановление экономики. Но в 2021 году ситуация принципиально не изменилась и его итоги пока трудно предугадать.

2. Риски и проблемы постпандемийной экономики

Приостановка хозяйственной и всякой иной деятельности в результате карантина в 2020 году привела к невиданному ранее сокращению объемов ВВП во всех странах мира, кроме Китая [4].

Таблица 1 – Показатели роста номинального ВВП по странам в 2020 году (в %)

Страна	**Темпы прироста ВВП в %**
Китай	+1,85
Россия	- 4,12
США	- 4,27
Япония	- 5,27
Германия	- 5,88
Великобритания	- 9,76
Индия	- 10,29
Франция	- 9,76
Италия	- 10,65
Испания	- 10,83
Всего по миру	- 4,36

В условиях ухудшения рисковой ситуации возможности экономического роста, то есть расширенного воспроизводства общественного продукта, сокращаются, и задачей текущего момента после каждой катастрофы становится перезапуск производства и восстановление утраченных фондов. Это называется восстановительным ростом, хотя на самом деле является попыткой удержаться на уровне простого воспроизводства, что удается далеко не сразу. Эта проблема не простая и ставит регулятора перед многими вопросами. В частности, как быстро остановить процесс свертывания объемов производства, каковы источники финансирования восстановительного роста.

Практика показывает, что главным источником финансирования являются государственные инвестиции, бюджетные субсидии и страховые фонды, покрывающие ущербы застрахованных организаций и домохозяйств. В развитых странах соотношение между государственными ресурсами и страховыми фондами в покрытии этих ущербов оценивается на уровне 70% и 30% [5]. В России страховые фонды недостаточны для решения таких проблем. Глубина проникновения страхования в экономику, рассчитываемая как отношение суммы собираемых страховых премий к ВВП составляет 1,35%. Вся надежда возлагается на государственное бюджетное финансирование в виде прямых инвестиций в восстановление разрушенных объектов, помощь малому и среднему бизнесу, безработным, поддержку семей с детьми и т.д. В первый пандемийный год государственные расходы должны были поддержать падающий спрос и дать возможность существования предприятиям, которым для сохранения производства и рабочих мест нужно продавать свою продукцию. В 2020 году государственные расходы достигли рекордных показателей за весь постсоветский период [6]. Они составили 39,5% к ВВП или 42,15 трлн. руб. Из этой суммы 54% приходится на федеральный бюджет.

Возможности привлечения частных инвестиций к финансированию инвестиций восстановления ограничены, так как такого рода инвестиции не могут быть достаточно прибыльными для бизнеса. Более того, практика привлечения частных инвесторов к финансированию восстановительных программ в форме государственно-частных партнерств зачастую не дает положительных результатов. Это означает необходимость обеспечения этим инвесторам определенной нормы прибыли за счет завышения объемов инвестиций. Сращивание по сути общественных средств бюджета с частным капиталом ведет к их трансформации в государственный капитал, распорядители которого тоже не хотят оставаться без прибыли. Даже выполнение подрядных работ по восстановление жилого фонда в районах природных катастроф за счет государственных средств, как правило, связано с хищениями и чрезвычайно низким качеством работ.

Потери от временной остановки хозяйственной деятельности в результате карантина – это совсем иной вид ущербов в сравнении с материальными убытками. В 2020 году бытовало мнение, что снятие ограничений по экономической активности приведет к скорому восстановлению экономики и все снова будет так, как было раньше. На самом деле обнаружилось, что восстановление ВВП, потерянного за год, не может произойти за несколько месяцев, а при продолжении полных или частичных локдаунов падение производства может прибрести затяжной инерционный характер. Все дело в действии мультипликаторов расходов, механизм

действия которых был раскрыт Дж. М. Кейнсом в годы мирового экономического кризиса и Великой депрессии 1929-1933 годов. Эти механизмы не раз помогали экономикам многих стран выходить из кризисов, используя инструменты государственного регулирования, несмотря на жесткую критику кейнсианства со стороны сторонников неолиберализма. В преодолении последствий мирового финансового кризиса 2008-2010 гг. методы государственной поддержки банков и стимулирования экономического роста сыграли решающую роль. Речь идет об автономных (государственных) и индуцированных (частных) инвестициях, об увеличении внутреннего потребительского и инвестиционного и внешнего спроса. Вложения в определенную отрасль дают умноженный эффект в виде роста ВВП благодаря межотраслевым связям. Самый высокий мультипликационный эффект дают вложения в производства, на которых висит целая гроздь межотраслевых поставок. В прошлом веке это были автомобилестроение и жилищное строительство, на которых многие страны «выезжали» из мировых кризисов и послевоенной разрухи. Какие отрасли сейчас могут сыграть такую роль, надо считать.

Однако надо иметь в виду, что мультипликатор расходов с тем же успехом действует не только в направлении роста, но и падения. Через снижение спроса и инвестиций, переходящее от одной отрасли к другой, начинает действовать механизм последовательного обрушения экономики. Прошедший год отчетливо показал, как это происходит. Прекращение международного туризма привело к остановке авиасообщения, остановка авиасообщения – к консервации парка самолетов, вывод авиабортов из эксплуатации - к прекращению деятельности авиационных сервисов, к прекращению поставок узлов и деталей, необходимых для ремонта и эксплуатации, к снижению спроса на авиационное топливо и продукцию авиационного машиностроения и т.д. В каждом звене разрывающейся цепи поставок возникает снижение объемов производства и конечных доходов, которые, в свою очередь, формируют конечный спрос.

Самый опасный момент наступает тогда, когда разрыв цепочек поставок достигает ядра экономики – реального сектора, и спираль сокращения объемов производства начинает разворачиваться внутри него. Свертывание реального производства – самое худшее, к чему может привести пандемия, провоцирующая затухание любой хозяйственной активности. Падение конечного потребительского спроса делает бессмысленными собственные вложения в производство со стороны бизнеса, чем и объясняется практика финансовой поддержки государством конечного спроса потребителей. Но бюджетные возможности государства ограничены, к тому же фактор времени работает против него.

Способность экономики к восстановлению зависит от многих факторов. Показатель ВВП, используемый как во внутреннем информационном обороте, так и для межстрановых сопоставлений, не отражает в полной мере состояние реальной экономики. Все зависит от структуры экономики страны и степени ее самодостаточности в отношении самых важных потребительских товаров и средств производства. Если ВВП сокращается за счет выпадения доходов торговли и непроизводственных услуг, это не критично, хотя ничего хорошего не сулит с точки зрения возможностей восстановления бизнеса. Если ВВП сокращается вследствие закрытия фабрик и заводов, выпускающих продукты питания и средства производства, из-за разрыва кооперационных связей, это может привести к дефициту самых необходимых товаров и услуг со всеми вытекающими последствиями. Худший и самый распространенный сценарий состоит в разрыве глобальных цепочек поставок.

Прекращение или сокращение производства в отдельных странах немедленно сказывается на экономике предприятий стран-партнеров и передается дальше с растущим коэффициентом мультипликации. Степень взаимозависимости предприятий разных стран стала реальным фактором риска для них. По данным агентства Dun & Bradstreet, более чем у 51000 компаний по всему миру есть хотя бы один поставщик в Китае, в районе Ухань, первичном очаге инфекции [7]. Это только один частный пример одного региона. Эти десятки тысяч компаний, в свою очередь, встроены в кооперационные цепочки регионального или глобального масштаба. Установлено, что глобальная экономика, основанная на сетевой информационной инфраструктуре, способна к быстрому экспоненциальному масштабированию сигналов и событий, попадающих в нее [8]. В данном случае пандемия короновируса стала фактором экспоненциального масштабирования экономических потерь от разрыва глобальных цепочек поставок. Мощным ускорителем этого процесса становится сокращение, а в ряде случаев полное прекращение транспортных коммуникаций между странами.

Таким образом, можно сделать вывод, что экономическая ситуация может существенно различаться в странах в зависимости от степени их включенности в систему мировых интеграционных связей. У каждой из них будут выявлены собственные узкие места в обеспечении условий собственного существования и возможности ликвидации этих узких мест. При этом для реальной оценки происходящих процессов должен использоваться не только ВВП, а разные показатели, в том числе, показатели объемов производства и товарных запасов в натуральном выражении по важнейшим позициям общественного продукта; показатели, характеризу-

ющие состояние важнейших систем жизнеобеспечения, таких как энергетика, производство продуктов питания, жилищная инфраструктура, здравоохранение и образование и т.д. Если по критически важным позициям для существования и развития экономики региона обнаруживается невосполнимый в кратчайшие сроки дефицит, то уже не важно, какой в этом регионе валовой региональный продукт. Особенно, если он формируется в основном за счет прибыли и фондов оплаты труда в организациях непроизводственной сферы.

3. Роль страхования в финансировании рисков постпандемийной экономики

В связи с переходом на восстановительный тип экономического роста роль страхования как источника финансирования рисков неизбежно будет возрастать, так как именно для компенсации потерь от наступления непредвиденных случайных событий предназначены страховые фонды. Но это будет происходить не в результате самопроизвольного развития страхового рынка, а по мере понимания регулятором необратимости тех изменений, которые происходят в механизмах общественного воспроизводства под влиянием меняющейся рисковой ситуации.

Страховая услуга как финансовый продукт кардинально отличается от других продуктов финансового рынка. В отличие от них она не обладает и не может обладать внутренней привлекательностью для потребителя, так как она не обещает ему дополнительных благ и обогащения. Эти отличительные особенности страхования могут быть сведены к трем пунктам. Во-первых, формирование страховых фондов является необходимостью, условием получения относительной экономической безопасности. Страхование не обладает собственными внутренними стимулами развития. Это общественный институт, создаваемый целенаправленно государством. Именно этим обстоятельством объясняется, в частности, головокружительный успех КНР в развитии национальной системы страхования. Формирование страхового рынка началось в Китае в середине 1990-ых годов, как и в России. В 2019 году Китай вышел на второе место в мире после США по объемам страхования, а где оказалось российское страхование, нам известно. Уровень проникновения страхования в экономику КНР оценивается в 14,8%, тогда как в России он составляет менее 2%. По плотности страхования, то есть по объему страховой премии на душу населения, Китай с учетом Гонконга занимал в 2016 году четвертое место в мире (6278 долл.), тогда как в США этот показатель составляет 4174 долл. В России плотность страхования составляла 117 долл. [9].

Стремительный рост страхования в Китае обусловлен двумя факторами. Это высокие темпы роста экономики, прежде всего экспортного производства, что предполагает массовое использование международных практик страхования производства, грузов и финансовых рисков. Другой важный фактор – жесткое государственное регулирование отрасли. Из этого следует вторая особенность страхования как отрасли финансов.

Каждая страна создает систему страхования под свои цели, она рукотворна в полном смысле этого слова. Например, пенсионная система страны может быть страховой, нестраховой и смешанной, может иметь различную институциональную структуру и т.д. Поэтому незначительная роль страхования в системе финансовых рынков РФ обусловлена позицией регулятора, направляющего финансовые ресурсы общества преимущественно в банковскую сферу и фондовый рынок, где, на его взгляд, создается в больших объемах новая стоимость.

И наконец, еще одно свойство страхования. Оно не может обладать значительной инвестиционной привлекательностью ни для потребителя услуг, ни для их производителя. Капитал, вложенный в страхование, не может рассчитывать на сверхвысокие прибыли, пританцовывая на угольках пожарищ, на руинах и костях, оставшихся после стихийных и прочих бедствий. Страхование имеет другие всем понятные цели. Большую часть своей прибыли страховые компании во всем мире получают от инвестиционной деятельности, вкладывая временно свободные средства страховых резервов в различные виды активов, приносящих доход.

Потенциал развития страхования связан с исчерпанием традиционных источников расширенного воспроизводства и ростом числа и масштабов ущербов, ставящих под угрозу системы обеспечения жизнедеятельности общества. Возможности бюджетного финансирования рисков всегда ограничены, тем более в условиях сокращения объемов ВВП. Встает вопрос о повышении роли страхования в компенсации потерь. Казалось бы, это невозможно в сложившейся социально-экономической ситуации.

Однако столь низкий уровень проникновения страхования в экономику страны как-то не вяжется с весьма значительными объемами частных инвестиций в банковские вклады и ценные бумаги. Вероятно, причина такого положения кроется не только в бедности значительной части населения, но и в отсутствии интереса в приобретении страховой защиты у тех, кто располагает какими-то финансовыми ресурсами. Когда такой интерес есть, страховые полисы начинают пользоваться спросом, что подтверждается опытом добровольного медицинского, автомобильного страхования и инвестиционного страхования жизни.

Перераспределение денежных активов в пользу финансирования рисков, угрожающих не только отдельным субъектам хозяйствования, а всей национальной экономике, становится необходимостью при радикальных изменениях в условиях воспроизводства общественного продукта. Это может быть сделано путем непосредственной увязки объемов бюджетного финансирования с наличием страховой защиты предприятий и населения от соответствующих рисков.

Литература

1. Касперская Н. «Проблемы деструктивных движений в Рунете». [Электронный ресурс]. – URL: file:///C:/Users/%D0%A2%D0%B0%D1%82%D1%8C%D1%8F%D0%BD%D0%B0/Downloads/Forum_TsG_Kasperskaya_Destruktivnye_techenia_28_03_2019.pdf

2. Природные катастрофы с 1970 года – ущерб на триллионы. Вести. Экономика. 2015. 27 апреля. [Электронный ресурс] – URL: http://www.vestifinance.ru/articles/56610

3. Ущерб от крупных природных катаклизмов в мире составил 150 млрд. долл. Это рекорд за все время наблюдений // Moscow Daily News. 28.12.2020// [Электронный ресурс]. – URL: https://www.mn.ru/ articles/ushherb-ot-krupnyh-prirodnyh-kataklizmov-v-mire-v-2020-godu-sostavil-150-mlrd-eto-rekord-za-vsyu-istoriyu-nablyudenij

4. Насколько вырос ВВП России и стран мир в 2020 году. Деловая жизнь. [Электронный ресурс]. - URL: http://bs-life.ru/makroekonomika/vvp2021.html

5. Токарева Е.А. «Мировой опыт страхования рисков природных катастроф». Автореферат диссертации. М., 2016. - С.10.

6. Госрасходы России в 2020 году стали рекордными за постсоветскую историю. [Электронный ресурс]. – URL: https://arb.ru/b2b/news/gosraskhody_rossii_v_2020_godu_stali_rekordnymi_za_postsovetskuyu_istoriyu-10459394/?source=mail

7. Хансен Сара «Холодный душ для перегретого рынка». [Электронный ресурс]. – URL: https://www.forbes.ru/finansy-i-investicii/394939-holodnyy-dush-dlya-peregretogo-rynka-kak-koronavirus-iz-medicinskoy

8. Миловидов В. «Коронавирус проникает в глобальные цепочки поставок». [Электронный ресурс]. – URL: https://www.if24.ru/koronavirus-pronikaet-v-globalnye-tsepochki-postavok/?utm_source=newsletter&utm_medium=email&utm_campaign=novosti_investklimata&utm_term=2020-02-28

9. Финансовая система Китая. Учебник. Под редакцией Иванова В.В., Покровской Н.В. – Москва: Проспект, 2018. - С.285-288.

УДК 330.354

Хайкин Марк Михайлович
д-р экон. наук, профессор
Санкт-Петербургский горный университет

ПРОБЛЕМЫ И УСЛОВИЯ РОСТА КОНКУРЕНТОСПОСОБНОСТИ ЭКОНОМИЧЕСКИХ СИСТЕМ

Аннотация. Обосновывается необходимость использования креативного подхода в управлении хозяйственными процессами. Особый акцент сделан на оценке наукоемкости экономики как единого целого в качестве условия роста конкурентоспособности экономических систем.

Ключевые слова: экономические системы, креативность, экономическая безопасность, конкурентоспособность.

Haikin M.M.
Saint Petersburg mining University

PROBLEMS AND CONDITIONS OF GROWTH OF COMPETITIVENESS OF ECONOMIC SYSTEMS

Annotation. The necessity of using a creative approach in the management of economic processes is justified. Special emphasis is placed on the assessment of the knowledge intensity of the economy as a whole as a condition for the growth of the competitiveness of economic systems.

Keywords: economic systems, creativity, economic security, competitiveness.

Развитие экономических систем в условиях современных реалий подвержено влиянию многих внутренних и внешних факторов, воздействие которых системным образом меняет содержание и характер функционирования экономики. В последние два десятилетия все чаще эти факторы называют «системные вызовы». В этой связи стоит особо отметить три момента.

Во-первых, любая экономика функционирует как система. Поэтому изменения на уровне функционирующих ее элементов всегда системным образом меняют работу этой системы.

Во-вторых, если исследовать многовековой и даже тысячелетний исторический пласт развития хозяйственной жизни общества, становится очевидным, что в долгосрочном интервале любая экономика является трансформационной. Причем трансформации носят системный характер – по мере развития производительных сил и производственных отношений,

в том числе технологических укладов, роль которых в современной экономике изучается особенно пристально многими исследователями [1]. В соответствии с общепризнанным определением под технологическим укладом понимается совокупность взаимосвязанных производств, которые развиваются синхронно и имеют единый технический уровень [2]. Таким образом, речь идет о совершенствовании факторов производства в результате развития науки и техники, но не об экономике в целом, которая в результате трансформируется.

В-третьих, наступление каждого последующего технологического уклада в экономике непосредственно ведет к изменению ее производительных сил. Это, в свою очередь, не может в конечном итоге тем или иным образом не трансформировать экономику, коренным образом не меняя содержание и характер функционирования экономической системы.

Экономическое мышление создает условия и основу для познания и учета экономических законов, недопущения их игнорирования в принятии решений. Особенно это важно, когда принимаемые решения концептуальные, стратегические, системного характера. Развитие экономического мышления на уровне власти создает условия и основу для познания и учета экономических законов, недопущения их игнорирования в принятии государственных решений. Так, например, в соответствии с марксистской школой действуют закон соответствия производственных отношений характеру и уровню развития производительных сил, экономический закон опережения производства средств производства над производством предметов потребления, и другие. В соответствии с классической школой экономической теории имеют место экономический закон убывающей предельной производительности, экономический закон предельных издержек и другие. Важно отметить, что результаты экономических исследований уже XXI века свидетельствуют о том, что в эпоху использования современных цифровых технологий не действуют такие важнейшие экономические законы, как: закон стоимости, закон предельных издержек, закон убывающей предельной производительности и некоторые другие.

В рамках проводимой экономической политики игнорирование экономических законов развития общества «оборотной стороной медали» сказывается на состоянии национального хозяйства, как всей страны, так и регионов. А состояние российской экономики оставляет желать много лучшего. Главная проблема сегодня – низкий внутренний спрос. На фоне действия внешних причин этого состояния (повышения зависимости экономики России от мирового хозяйства, мирового экономического кризиса, экономических санкций со стороны США и западных стран, изменения мировых цен на ресурсы, вступления России в ВТО, геополитическими риски в связи с событиями на Украине, Ближнем Востоке и др.) основны-

ми причинами выступают внутренние. К внутренним причинам можно отнести: исчерпание возможностей экспортно-сырьевой модели и экстенсивных источников экономического роста – труда и капитала; глобальные ошибки денежно-кредитной политики государственных финансовых институтов (в частности, допущенные ошибки в проводимой политике Банка России, которая направлена на финансовую стабилизацию и борьбу с инфляцией, но в ущерб целям национального экономического развития и долгосрочного роста); чрезмерная открытость экономики, допускающая вывоз огромных сумм капитала за границу; ослабленные защитные механизмы от внешних шоков и другие. Все это способствовало кризисному состоянию экономики. На нее указывают многие факты: существенное отставание от многих стран мира по уровню производительности труда в промышленности; высокая затратность, ресурсоемкость промышленного производства; общее технологическое отставание от ведущих промышленно развитых стран (за исключением отдельных отраслей промышленности); высокий физический и моральный износ основных производственных фондов, достигший в ряде отраслей промышленности критического уровня (при этом их обновление далеко не всегда осуществляется на инновационной основе – на базе современных информационных технологий и электроники); «утечка мозгов»; вывоз капитала (что существенно снижает общий инвестиционный потенциал национальной экономики); неравномерность экономического развития регионов; снижение доходов населения; перекредитование потребителей [3].

Именно научное обеспечение существования, функционирования и развития экономических систем есть теоретико-методологическая основа экономической безопасности и роста конкурентоспособности экономических систем. Таким образом, особенно актуальным является рост наукоемкости экономики в целом в качестве научного фундамента функционирования окружающей среды и общественного воспроизводства.

Понимание сущности экономики подменяется словесными наукообразными названиями. Так в настоящее время появились экономики: транзитивная; рыночная; сервисная; циркулярная; корпоративная; цифровая; инновационная и др. – всего насчитывается более 30 названий современной экономики. В этом перечне часто упоминается «креативная экономика». В связи с этим следует рассмотреть сущность понятий креатив или креативный подход в экономике.

Экономические процессы и, соответствующая им экономическая деятельность, состоят из 3-х частей: 1) детерминированной – определенной, 2) стохастической – вероятностной и 3) эмерджентной – порождаемой.

Для детерминированной части управления экономическими процессами достаточно профессиональных знаний специалиста. Для стохастиче-

ской части требуются не только знания, но и опыт, благодаря которому формируются количественные оценки вероятностных ситуаций, включая и вероятности рисков.

Все субъекты экономической деятельности представляют собой так называемые «большие» системы. Такие системы обладают рядом признаков и свойств, важнейшим из которых является эмерджентность. Эмерджентность характеризуется способностью системы порождать дополнительные свойства, не выводимые из свойств составляющих её подсистем. Иными словами, система или процесс есть нечто большее, чем сумма составляющих астей. Эмерджентность означает, что большую систему невозможно математически описать исчерпывающим образом, т.е.

$$C = D \cup S \cup E,$$

где D – детерминированная (определенная) часть большой системы;
S – стохастическая (вероятностная) часть большой системы;
E – часть большой системы, порождаемая эмерджентностью.

Эмерджентность преодолевается с помощью креативного подхода к управлению экономической деятельностью, а это означает, что управление не только наука, но и искусство. Таким образом, эмерджентность есть объект приложения креативного подхода, в котором решающую роль играет интуиция специалиста.

Рассматривая эмерджентность, следует иметь в виду и синергетику (греч. synergetikos – совместные действия) – согласованное поведение подсистем, при котором возрастает упорядоченность, снижается неопределенность.

Новые свойства, порождаемые совметсными действиями подсистем, являются положительными: возникает синергетический эффект. В связи с этим правомерно считать синергетику как положительное проявление эмерджентности.

В результате согласованного поведения подсистем, т.е. структурных подразделений предприятия, возрастает степень упорядоченности всей системы-предприятия, вследствие чего снижается энтропия – неопределенность, а вместе с этим происходит самоорганизация системы. Согласно теории синергетики, как научной дисциплины, в результате взаимодействия компонентов структур образуется новая система на более высоком уровне. Именно для такой системы присущ синергизм. Изложенные действия представляют собой креатив или креативный подход в управлении предприятием (лат. creation – творение, создание).

Именно самоорганизация является непосредственным источником синергизма. В связи с этим прослеживается следующая последовательность креативного подхода:

– система-предприятие, состоящая из конечного числа подсистем - структурных подразделений;

– формулировка проблемы в деятельности предприятия – постановка общей цели;

– взаимодействие и согласованные действия подсистем;

– упорядоченность элементов системы и подсистем;

– самоорганизация системы – снижение неопределенности;

– синергетический эффект;

– решение проблемы – эффективность.

Синергетический эффект достигается в том случае, когда предприятие функционирует как система, т.е. когда структуры и персонал взаимосвязаны между собой для достижения общей цели, каковой является решение данной проблемы в управлении предприятием.

Для креатива или, что тоже самое, в составе креатива должна быть сформулирована проблема. В свою очередь, проблема (греч. problema – задача) представляет собой теоретические или практические вопросы, требующие разрешения. Трудности, на основе которых сформулирована проблема, обусловлены рисками, угрозами и опасностями, т.е. всем тем, что нарушает экономическую безопасность данного предприятия.

Проблема конкретизируется с помощью четко поставленной цели. Из изложенного следует, что управленческий персонал предприятия – менеджеры – должны четко сформулировать проблемы и задачи, которые нарушают эффективное функционирование данного предприятия как экономической системы. Следует подчеркнуть, что речь идет не об интуитивном понимании трудностей, стоящих перед предприятием, а именно о проблеме в сугубо научном понимании.

Для решения проблемы в научной постановке требуется теория. Разработка теории и есть креативный процесс. Итак, креатив (креативный подход, креативный процесс) есть следующая последовательность: «трудности – проблема – теория – решение – практический результат – эффективность».

Креативный процесс тесно связан с творческой деятельностью. Творчество есть деятельность, порождающая нечто новое, а поэтому результат творчества характеризуется оригинальностью или уникальностью. В творчестве проявляется индивидуальность исследователя или специалиста.

Таким образом, выявляются атрибуты – определяющие особенности: креатив – процесс научной формулировки проблемы и разработка теории для её решения; творчество – процесс создания принципиально нового. Отсюда следуют ключевые слова: для креатива – это проблема, для творчества – это новшество. А в остальном креатив и творчество – понятия равнозначные. Место креатива и творчества представлено на Рисунке 1.

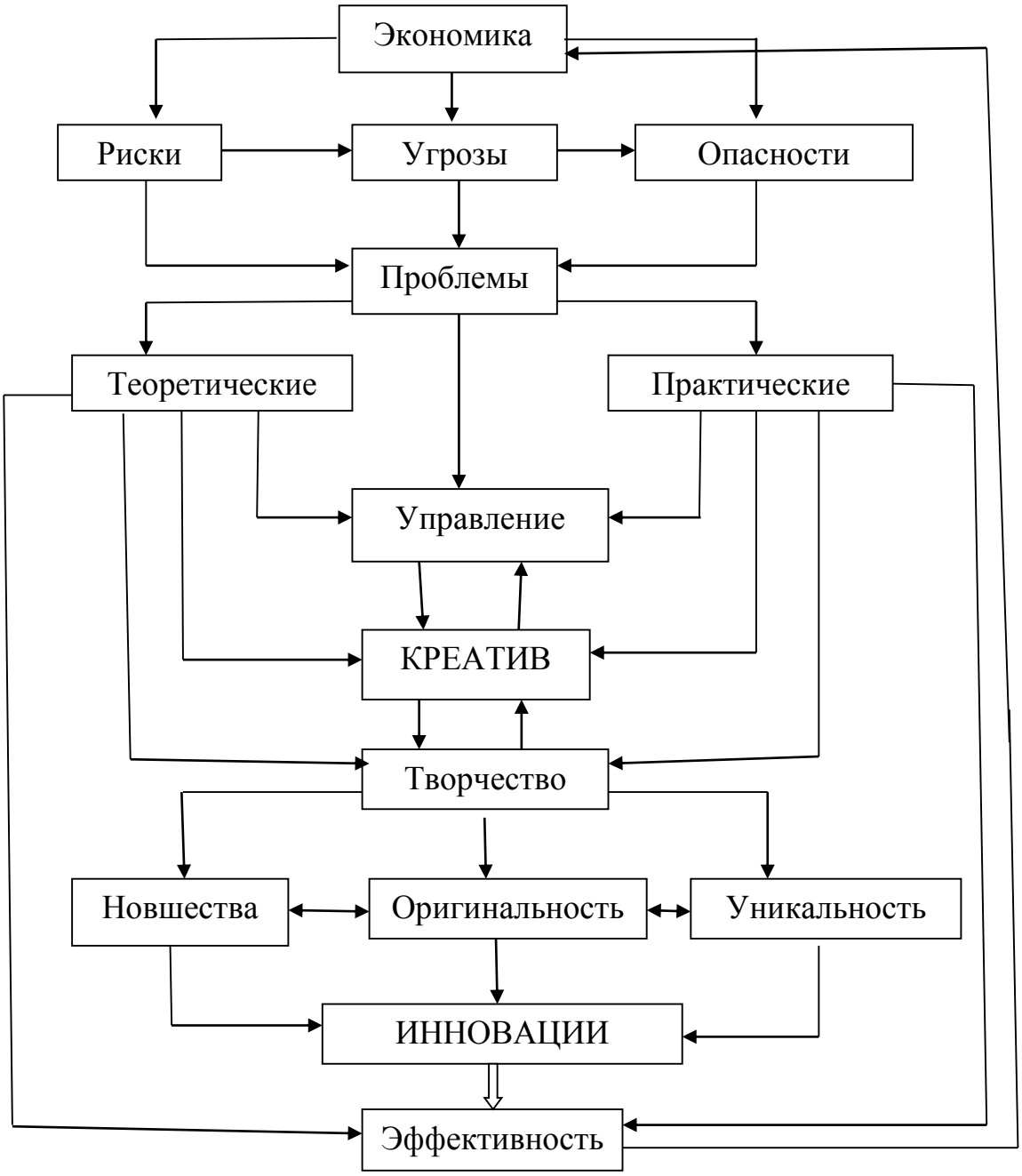


Рисунок 1 – Место креатива и творчества в экономических инновациях

Креатив направлен на решение проблемы, творчество – это поиск нового. В креативном процессе могут быть использованы имеющиеся достижения науки и практики. Результатом творчества являются инновации. Итак, креатив – решение текущих проблем, творчество – научная новизна и практическая значимость.

В общетеоретическом плане экономическая деятельность осуществляется под воздействием необходимых видов обеспечения, каковыми являются: научное, трудовое, информационное, техническое, правовое, финансовое, организационное. Рассмотрим их.

Как и в любой сфере деятельности в экономике основополагающим является научное обеспечение, которое и определяет её наукоемкость. Основные теоретические положения позволяют установить количественные характеристики наукоемкости экономики, а именно:

1) доля наукоемкой продукции – товаров и услуг в промышленном производстве;

2) объем экспорта наукоемкой продукции;

3) величина экспорта патентов и лицензий на изобретения и ноу-хау;

4) объем продаж франшизы по наукоемким технологически процессам;

5) доля науки в ВВП – Валовом Внутреннем Продукте;

6) использование на практике научных достижений Нобелевских премий по экономике;

7) объем научно-исследовательских работ (НИР) по экономике в специализированных научных учреждениях и высших учебных заведениях (университетах);

8) количество ученых в составе занятого населения.

В целом научное обеспечение экономики базируется на положениях экономической теории и на комплексе прикладных научных экономических дисциплин – функциональных и отраслевых.

Из сущности научного обеспечения следует императив: «В экономике все решения должны приниматься строго по науке». При этом к абсолютному минимуму должно быть сведено «ручное управление» как на макро-, так и на микроэкономическом уровнях. Таким образом, экономика должна функционировать в ламинарном режиме.

В современном обществе используются достижения следующих наук: теория информации; материаловедение; физика твердого тела (полупроводники); физика электромагнитных волн; электротехника; радиоэлектроника; химия; космос: спутниковая связь и навигация; метеорология; науки о человеке: биология, физиология, медицина и др.

В научном обеспечении экономики важное место занимает совершенствование математического аппарата для моделирования экономических категорий равновесия, устойчивости и роста. Кроме этого, математика служит средством доказательства экономических положений.

Наука и экономика находятся друг с другом в неразрывной связи: с одной стороны, развитая экономика служит источником финансовых средств для научных исследований, а с другой – результаты научных исследований прямо или опосредованно направлены на повышение эффективности экономики.

Результаты научных исследований должны обогащать аппарат экономической теории – фундамента всех экономических наук – функциональных и отраслевых.

Важнейшей составляющей производительных сил экономики является труд – работники сферы общественного производства. Непосредственно в сфере производственно-экономической деятельности персонал подразделяется на следующие группы: управленческий персонал: руководители, менеджеры и топ-менеджеры; специалисты; исполнители. К этому следует добавить и научно-исследовательский персонал – ученых научных учреждений (НИИ и КБ) и высших учебных заведений.

Основным требованием трудового обеспечения к персоналу является наличие высокого уровня профессионализма и квалификации. Для профессий и специальностей действует жизненный цикл: отмирают старые профессии, под воздействием научно-технического прогресса (НТП) появляются новые профессии и специальности или старые профессии получают новое содержание. Повседневная деятельность персонала должна отвечать требованиям Научной организации труда (НОТ).

В свою очередь источником научного обеспечения экономики является система подготовки специалистов-экономистов. В настоящее время высшее профессиональное экономическое образование остро нуждается в системном улучшении. Основной причиной сложившегося положения в образовании является отрыв от реальной практики. Большинство профессорско-преподавательского состава экономических вузов (университетов) не имеют опыта работы в реальном секторе экономики. А поэтому университеты утратили статус научных учреждений.

В учебных программах отсутствуют достижения экономической науки на уровне Нобелевских премий по экономике. Из более, чем 90 – лауреатов Нобелевской премий по экономики: 70 лауреатов – это американские ученые-экономисты, свои исследования они проводили в американских университетах [4]. Столь высокий интеллектуальный уровень экономической науки следует считать важнейшей причиной сохранения доминирующего положения США в мировой экономике [5].

Производственно-экономическая деятельность порождает огромный объем информации, но с другой стороны, для управления экономическими процессами необходима информация: достоверная, полная, оперативная. Информационное обеспечение экономики включает:

1) данные статистического учета и отчетности – в полном соответствии с научными методами экономической статистики;
2) данные бухгалтерского учета и отчетности;
3) плановые показатели деятельности субъектов экономики;
4) отчетные данные оперативно-хозяйственного учета;
5) методы экономического анализа, включая анализ бухгалтерского баланса, аудит;
6) полная компьютеризация информационных процессов и операций.

Всеобщая компьютеризация представляет собой цифровизацию информационного обеспечения. В целом информационное обеспечение базируется на положениях экономической теории и прикладных научных дисциплинах, а поэтому цифровизация информационного обеспечения способствует повышению экономической эффективности хозяйственных процессов. Следует особо отметить, что именно с этих позиции всю современную экономику именовать цифровой некорректно, а информационное обеспечение может быть и должно быть цифровым.

Современная экономика характеризуется высоким уровнем механизации и автоматизации производственных процессов и трудовых операций, что достигается с помощью основных производственных и непроизводственных фондов. В техническое обеспечение входят также и оборотные средства – расходные материалы, используемые в производственно-экономической деятельности. Основные производственные фонды как составная часть производительных сил экономики включает: производственно-технические здания; сооружения; передаточные устройства; силовые машины и оборудование; рабочие машины и оборудование; измерительные и регулирующие приборы, лабораторное оборудование и средства, средства обработки информации; транспортные средства всех видов; инструменты всех видов, производственный и хозяйственный инвентарь. Приведенная классификация предусматривает дифференциацию основных фондов по их роли в экономической деятельности – производстве и торговле, а поэтому является объективной и стабильной. Такая классификация позволяет учитывать достижения научно-технического прогресса: появление новых видов оборудования, средств связи и коммуникации, вычислительной техники и др. Основные фонды характеризуются длительными сроками службы, а поэтому физический износ и моральный возраст основных фондов должен быть в пределах нормативных сроков. К техническому обеспечению относятся техническое обслуживание (ТО) и ремонты, согласно установленным регламентам.

С позиций рассматриваемой проблемы, правовое обеспечение должно обладать стимулирующим действием: законодательство должно поощрять и предоставлять преимущественное право субъектам с высоким уровнем наукоемкости, например, в арбитражной практике или договорных отношениях. Основное требование правового обеспечения – это создание благоприятной правовой среды для предпринимательства, что предусматривает стабильность законодательных актов с учетом положительных традиций хозяйственной деятельности.

Как правило, предприятия с высоким уровнем наукоемкости характеризуются инновационной активностью, что также создает определенные правовые преференции и преимущества.

Современная экономика строится на товарно-денежных отношениях между своими субъектами, вследствие чего такая экономика по своей сущности является монетарной. Согласно теории Лауреата Нобелевской премии М. Фридмана (1976 год), финансы занимают приоритетное положение, а это означает, что для эффективной экономической деятельности, прежде всего, должны быть отрегулированы финансы. А это означает, что предприятие должно обладать устойчивым финансовым состоянием: положительным балансом, необходимой кредитоспособностью и платежеспособностью, отсутствием финансового дефицита. Финансовое обеспечение предусматривает и такие важные мероприятия: благоприятное кредитование наукоемкой экономической деятельности; льготное налогообложение. В целом финансовое обеспечение входит в компетенцию банковского сектора экономики, который осуществляет постоянный контроль за деятельностью каждого предприятия.

Согласно теории и практике, организационное обеспечение предусматривает упорядочение в пространстве и во времени всех составляющих любой деятельности – в данном случае экономической. Такое упорядочение есть не что иное, как соблюдение оптимальных пропорций структурными составляющими.

Таким образом, прежде всего, должна быть сформирована оптимальная структура всей экономики, т.е. на макроэкономическом уровне. Так, оптимальной структурой должен обладать интегрированный рынок – рынок, который охватывает всю экономику. Структура интегрированного рынка представлена в Таблице 1.

Таблица 1 – Интегрированный рынок в экономическом пространстве

Производство и инфраструктура		Объекты (отрасли) экономики
ПРОИЗВОДСТВО	Предметы труда	- сырье - материалы - энергоносители - изделия - электроэнергия - вторичные материальные ресурсы
	Труд	- рабочие, специалисты, - руководители, менеджеры
	Орудия труда	-основные фонды (машины, оборудование)
ИНФРА-СТРУКТУРА	Производственная инфраструктура (отрасли)	- транспорт - ремонтное обслуживание - строительство - инновации и инвестиции

Окончание табл. 1

Производство и инфраструктура		Объекты (отрасли) экономики
		- научно-технические знания - наука - недвижимость - имущественное страхование - информация
	Социальная инфраструктура (отрасли)	- продовольствие - предметы потребления - товары - бытовое и коммунальное обслуживания - медицинские услуги - образование - личное страхование - жилье
	Институциональная инфраструктура	- финансы и кредит - ценные бумаги - валюта - банковские услуги - реклама

Организационное обеспечение требует соблюдение оптимальных пропорций по критерию эффективности производственно-экономической деятельности. Нарушение структуры экономики проявляется при преобладании добывающей промышленности – такая экономика именуется сырьевой. В ряде стран (в том числе и в России) в экономике преобладают добыча и экспорт нефти и газа в ущерб обрабатывающей промышленности.

С точки зрения экономической науки, в организационном обеспечении рассматриваются:

1) Общая отраслевая структура экономики с преобладанием производства средств производства и предметов потребления;

2) Оптимум внешнеторгового оборота с положительным балансом экспорта и импорта;

3) Развитая социальная инфраструктура;

4) Научно обоснованная структура субъектов экономики (исключающая «ручное управление»);

5) Функционирование экономики, в том числе и каждого предприятия, в ламинарном режиме

Оптимальные пропорции должны охватывать всю экономику – от макроэкономического и до микроэкономического уровней [6]. Все виды обеспечения воздействуют на экономику, что иллюстрируется сетевым графиком (рисунок 2).

Условные обозначения:
Н – научное обеспечение;
Тр – трудовое обеспечение;
И – информационное обеспечение;
Тех – техническое обеспечение;
П – правовое обеспечение;
Ф – финансовое обеспечение;
О – организационное обеспечение.

Как следует из графика, организационное обеспечение, кроме всего прочего, является средством сопряжения всего комплекса обеспечивающих подсистем с экономикой.

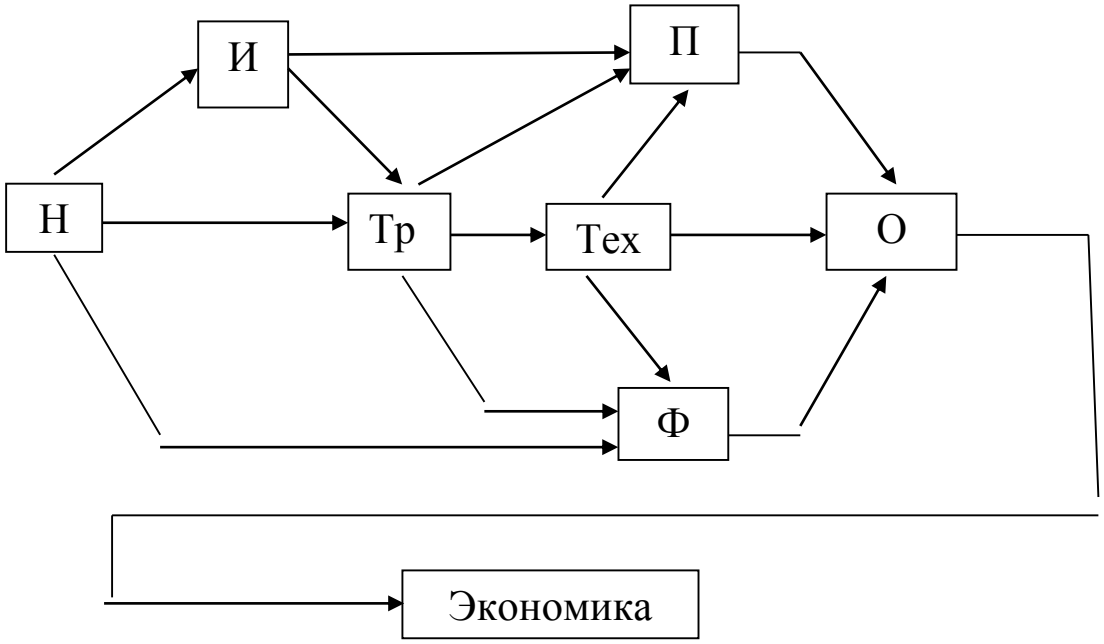


Рисунок 2 – Связи видов обеспечения экономики

За последнее время для обозначения нежелательных состояний в экономике все чаще стало употребляться прилагательное «турбулентный». Такое определение рассматривается как беллетристический оборот или сравнение для большей выразительности речи или текста. На практике ламинарность и турбулентность (L&T) употребляются как противоположные, несовместимые характеристики. Ламинарность (от лат. lamina – пластина) – это спокойное движение потока без перемешивания слоев, т.е. струйное течение. Турбулентность (от лат. turbulentus – беспорядочный) – неупорядоченное, хаотичное движение.

В целом экономика должна иметь ламинарный характер, т.е. функционировать «спокойно». Однако в некоторых случаях в экономике может проявляться и своеобразная турбулентность, обусловленная наличием препятствий или иных нарушений (например, нарушение потока в товаро-

проводящих путях в форме «затоваривания» или нарушения финансовых потоков вследствие утраты платежеспособности и т.п.).

Ламинарность определяет положительное состояние экономической системы, турбулентность же характеризует отрицательные и нежелательные экономические ситуации. Основные характеристики ламинарности и турбулентности представлены в Таблице 2.

Таблица 2 – Характеристики ламинарности и турбулентности

№ пп	Ламинарность	№ пп	Турбулентность
1	Конкурентоспособность	1	Отсутствие конкурентных преимуществ
2	Устойчивость	2	Неустойчивость
3	Ритмичность	3	Неритмичность
4	Периодичность	4	Непериодичность
5	Высокий уровень детерминированности	5	Постоянная стохастичность
6	Энтропия, близкая к нулю	6	Максимальная неопределенность
7	Эластичность = max	7	Низкая реакция на изменение внутренних и внешних факторов
8	Эффективная управляемость	8	Низкая «обратная связь»
9	Системное функционирование	9	Нарушение системности
10	Высокая рентабельность	10	Убыточность и кризисные состояния
11	Безотходные технологии, рециклинг	11	Большие отходы производства и потребления (> 50 %)
12	Соблюдение законодательства и традиций	12	Нарушение законодательства на грани криминала
13	Соблюдение налоговой дисциплины	13	Уклонение от уплаты налогов
14	«Прозрачность» деятельности	14	Сокрытие доходов и «коммерческие» тайны
15	Постоянная профилактика рисков	15	Появление рисковых событий

Как следует из Таблицы 2, сравнительные характеристики ламинарности и турбулентности (L&T) имеют диаметрально противоположное значение: от необходимой полезности и до категорической недопустимости.

Турбулентность есть крайнее проявление беспорядка на том или ином предприятии [7].

Существенным образом различается результативность, а точнее – последствия ламинарных и турбулентных состояний. Последствия ламинарного состояния:

1) постоянная кредитоспособность;
2) инновационная активность;
3) скорая окупаемость инвестиций;
4) процесс накопления финансовых средств;
5) развитие и расширение объемов производственно-коммерческой деятельности;
6) наличие систиемообразующих факторов и реальное управление цепями поставок;
7) функционирование в оптимальном режиме по критериям выгоды и полезности (оптимум по Парето).

Последствия турбулентного состояния:

1) периодические сбои и кризисные ситуации;
2) нарушение производственных ритмов и «ручное» управление;
3) предбанкротное состояние – вплоть до внешнего управления предприятием;
4) объявление предприятия банкротом.

В физике для характеристики потоковых процессов используется число Рейнольдса: ламинарное движение жидкости возможно только до определенного значения числа Рейнольдса, которое выражается формулой:

$$R = \frac{pvl}{m}$$

Экономическое толкование параметров числа Рейнольдса допускает несколько вариантов. Так, в частности, предлагается такая интерпретация:

1) p – цена как мера полезности реализуемой продукции;
2) v - интенсивность или скорость продаж – время нахождения товара в процессе реализации («пролёживания»), измеряется величиной запасоемкости производства и реализации;
3) l – «пропускная способность» товаропроводящей сети, например, в форме торговых площадей или системы торговли в целом;
4) m – товарная ликвидность в форме объема продаж за определенный период.

Для оценки уровня ламинарности и соответственно, опасности турбулентности для данного предприятия (фирмы) экономическое число Рей-

нольдса ($R_{эк}$) должно стремиться к минимуму, т.е. $R_{эк}$ = min. В рассматриваемом случае речь идет о физическом моделировании экономических процессов.

Ламинарность характеризует научный подход к управлению экономическими системами и процессами. А поэтому экономическое число Рейнольдса может количественно оценивать уровень наукоемкости экономики как в целом, так и отдельных её составляющих – регионов, отраслей, предприятий. Компоненты экономического числа Рейнольдса учитываются статистикой, а поэтому доступны для расчета уровня наукоемкости экономики.

Показатели, входящие в состав индикатора ламинарного состояния, как правило, находятся в открытом доступе. Поэтому заинтересованные предприятия могут выполнить соответствующие расчеты при выборе деловых партнеров и установлении хозяйственных связей. В таком случае расчет ламинарности может стать важной составляющей при выполнении трансакционных операций.

Со временем индикаторы ламинарности могут стать важнейшими характеристиками предприятий и экономики в целом. Этот показатель должен быть основным ориентиром для менеджмента, а также для банков при решении вопросов о кредитовании крупных инновационных и инвестиционных мероприятий.

В финансовой сфере скачки котировок ценных бумаг или валютных курсов вполне можно характеризовать как проявление турбулентности. В этом случае в рамках аналитической работы с высокой степенью достоверности может быть установлено критическое значение R(критич).

Консалтинговые фирмы должны в порядке своего саморазвития параллельно выполнять расчеты уровня ламинарного состояния и турбулентности по конкретным данным обслуживаемых предприятий. По мере накопления информации могут быть установлены критические значения индикаторов R(критич) для групп предприятий: производственных и торговых, по специализации производимой и реализуемой продукции, по размерам предприятий.

Подводя некоторые итоги, следует особо отметить, что развитие науки, его творческого начала есть фундаментальные основания в решении проблем обеспечении экономической безопасности и роста конкурентоспособности экономики как целого и одновременно необходимыми условиями достижения этого.

Литература

1. Глазьев С.Ю. Уроки очередной Российской революции: Крах либеральной утопии и шанс на «экономическое чудо».– Экономическая газета, 2011.

2. Лопатников Л.И. Технологический уклад // Экономико-математический словарь: Словарь современной экономической науки. 5-е изд. – М.: Дело, 2003.– 520 с.

3. Хайкин М.М. Междисциплинарный подход к развитию экономического мышления в современных условиях // Инновационные подходы развития экономики и управления в XXI веке: сборник трудов III национальной научн. - практ. конф. – СПб.: ПУПС, 2020, С.318-321.

4. Плоткин Б.К., Хайкин М.М. Введение в современную экономику. – СПб.: ЛЕМА, 2019. – 204 с.

5. Хайкин М.М., Плоткин Б.К. От показателей эффективности – до экономической эффективности // Экономическая наука сегодня. 2020.– №11. С. 18-26.

6. Конкурентоспособность в системе экономической безопасности предприятия // Технико-экономические проблемы сервиса. 2020. – №4. С 66-70.

7. Бурлачков В. Турбулентность экономических процессов: теоретические аспекты // Москва: Русский Либмонстр (LIBMONSTER.RU). [Электронный ресурс]. – URL: https://libmonster.ru/m/articles/view/ (дата обращения: 01.09.2021).

УДК 004.056.5

Чернокнижный Геннадий Михайлович
канд. техн. наук, доцент
Санкт-Петербургский государственный
экономический университет

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПУТИ ИХ РЕШЕНИЯ

Аннотация. В статье рассматривается актуальные угрозы информационной безопасности, возникшие в последние годы, степень их опасности, а также возможные способы противостояния им, предлагаемые информационным сообществом.

Ключевые слова: угроза, атака, уязвимость, злоумышленник, критическая информационная инфраструктура, центр обеспечения безопасности.

Chernoknizhny G. M.
St. Petersburg state University of Economics

CURRENT PROBLEMS OF INFORMATION SECURITY AND WAYS TO SOLVE THEM

Annotation. The article examines the current threats to information security that have emerged in recent years, the degree of their danger, as well as possible ways to counter them proposed by the information community.

Keywords: threat, attack, vulnerability, attacker, critical information infrastructure, security operations center.

В современном обществе хорошо известно, как быстро растут угрозы информационности безопасности (ИБ), однако действительность еще суровее, чем это представляется на бытовом уровне. Мир стал технологически другим, и оценка ситуации во всех высокотехнологичных областях должна производиться непрерывно в режиме реального времени.

Подобным мониторингом в различных направлениях защиты информации - от физической защиты объектов и субъектов, до интеллектуальных средств анализа и осуществления защиты - занимаются высококвалифицированные специалисты известных зарубежных компаний, например, Институт системного администрирования, аудита, сетей и безопасности (The SysAdmin, Audit, Network, Security Institute, SANS), Gartner и ряд других. Однако для России, на наш взгляд, более актуальными являются исследования ведущих российских компаний, таких как Positive Technologies, Код безопасности, Digital Security, Group-IB, «Лаборатория Касперского» и ряда других, которые содержат, в том числе, и сведения об угрозах и атаках на информационные структуры нашей страны. По сведениям Национального координационного центра по компьютерным инцидентам (НКЦКИ) за 2020 год на Россию было совершено более четырех миллиардов кибератак.

Особенно актуальными для России являются атаки на критические информационные инфраструктуры (КИИ), которые направлены на нарушение доступности инфраструктуры, нарушения конфиденциальности информации, запуск вредоносного программного обеспечения.

Рассмотрим уровень защищенности Российских КИИ, степень опасности появляющихся угроз, тенденции их развития и новые технологии защиты от этих угроз.

В ходе инструментального анализа, проведенного специалистами Positive Technologies [1] на ряде предприятий (с их согласия) обнаружены 9483 уязвимости на 599 узлах (из 3514, включая сетевые устройства, сер-

веры и рабочие станции). Причины уязвимостей заключались в том, что не проводились регулярные обновления программного обеспечения, использовались простые пароли, пароли по умолчанию, а также были найдены ошибки в коде веб-приложений и в их конфигурации.

В 84% организаций выявлены уязвимости высокого уровня риска.

В 58% организаций обнаружены уязвимости высокого уровня риска, для которых существуют общедоступные эксплойты. Таким образом, использовать такого рада уязвимости может даже начинающий хакер.

В 2020 году злоумышленники атаковали все более крупные цели с использованием шифровальщиков, постоянно увеличивая суммы выкупов. На подпольных форумах широко распространяются сервисы «программа-вымогатель как услуга». Количество атак шифровальщиков выросло более чем на 150% по сравнению с предыдущим годом.

В прошлом году многократно возросло количество APT-атак (advanced persistent threat), то есть целевых, хорошо подготовленных, проводимых группой специалистов высокого уровня, имеющей целью проникновения в инфраструктуру компании с целью использования ее ресурсов как можно дольше. Такого рода атаки особенно опасны для критических информационных структур России. Проводится APT-атака в несколько этапов:

- сбор данных о жертве всеми доступными способами;
- вторжение: проведение мощной продуманной социальной (фишинговой) атаки, проникновение в внутреннюю сеть, используя уязвимости системы и применяя эксплойты нулевого дня; сбор данных об инфраструктуре;
- установления полного контроля над жертвой с использованием полученной информации;
- сохранение в системе как можно дольше.

Для иллюстрации способов, применяемых злоумышленниками, приведем несколько известных примеров.

В атаке на Google, которую впоследствии назвали Aurora, группе сотрудников направлялись письма от адресатов, которые заслуживали доверие [2]. В письмах была ссылка на сайт, который содержал сценарий, эксплуатировавший уязвимость, благодаря которой на компьютеры пользователей внедрялся бэкдор для контроля над системой по HTTPS через 443 порт, и постепенно устанавливался контроль над ресурсами внутренней сети.

Эксперты Positive Technologies обнаружили хакерскую группу Calypso [3], предположительно имеющую китайские корни, которая действует с 2016 года, и нацелена на государственные учреждения. Выявлена деятельность группы в ряде стран, в том числе, в России.

В середине 2020 года эксперты «Лаборатории Касперского» обнаружили новую, весьма продвинутую вредоносную северокорейскую кампанию APT-группы Lazarus [4]. Ранее группа атаковала финансовые учреждения, но с 2020 года среди целей злоумышленников оказались и предприятия оборонной промышленности. Специалисты «Лаборатории Касперского» изучили одну из атак и выяснили, что начало атаки осуществлялось путём целевого фишинга. Сотрудникам отправлялись письма с вредоносными документами Microsoft Word или ссылками на такие документы на тему профилактики или диагностики коронавирусной инфекции. Письма были адресованы от имени сотрудника медицинского центра, входящего в состав атакованной организации. Если пользователь открывал вредоносный документ и разрешал выполнение макросов, эксплойт начинал разворачиваться во внутренней сети, и после установки бэкдора ThreatNeedle хакеры получали полный контроль над компьютером.

Буквально в последние два года наметилась и активно развивается тенденция использования в фишинговых атаках искаженных префиксов URL-адресов: вместо традиционного формата http:// или https:// злоумышленники для атак по электронной почте используют префикс http:/\, обходя таким образом сканеры электронной почты.

Отметим: все известные крупные APT-атаки начинались с мощной, продуманной фишинговой атаки. Ключевые выводы из извлеченных уроков по фишинговым атакам сделал Матан Бен Дэвид [5], аналитик по реагированию на инциденты компании Checkpoint:

1. Электронная почта, безусловно, является вектором номер один для злоумышленников, чтобы проникнуть в бизнес-сети. Фишинговые письма, заставляющие пользователей раскрывать свои учетные данные организации или нажимать на вредоносную ссылку/файл, являются угрозой номер один в пространстве электронной почты. Организации всегда должны включать для себя решение для защиты электронной почты, предназначенное для предотвращения таких атак автоматически с использованием постоянно обновляемых механизмов безопасности.
2. Обучайте своих сотрудников: правильное и постоянное обучение сотрудников угрозе в пространстве электронной почты.
3. При работе с банковскими переводами всегда обязательно добавляйте вторую проверку, либо позвонив человеку, который попросил сделать перевод, либо позвонив принимающей стороне.
4. Всегда захватывайте как можно больше криминалистических доказательств, когда имеете дело с подозрительными или подтвержденными инцидентами кибербезопасности.
5. Используйте инструмент для идентификации новых зарегистрированных доменов, похожих на ваше собственное доменное имя.

Пандемия и удаленная работа сделали эффективные средства защиты информации востребованными как никогда. Организациям пришлось срочно масштабировать и защищать средства удаленного доступа на фоне возросших рисков нарушения информационной безопасности.

Компания Cisco определила основные тенденции 2020 г. в области защиты информации и дала рекомендации, на что обратить внимание в 2021 г. Переход на удаленную работу в 2020 г. подразумевал [6]:

- во-первых, что все сотрудники должны иметь возможность безопасно работать из дома;
- во-вторых, что они сохраняют доступ ко всем необходимым корпоративным ресурсам.

Поэтому многие обратились к технологии рабочих столов Remote Desktop, которая позволяет пользователю удаленно подключаться к компьютеру, однако протокол RDP создает проблемы кибербезопасности: кража идентификационных данных, атака man-in-the middle и дистанционное выполнение кода. В случае компрометации любое решение для удаленных рабочих столов дает злоумышленнику доступ к ресурсам всей сети.

Главные выводы Cisco:

- не следует пользоваться RDP непосредственно через Интернет. Сначала необходимо установить VPN -соединение, по которому сотрудники смогут безопасно получать доступ к необходимым ресурсам по протоколу RDP;
- необходимо использовать многофакторную аутентификацию;
- следует блокировать доступ после разумного числа неудачных попыток.

В 2020 г. на фоне вспышки пандемии критичной точкой в области обеспечения ИБ стала сфера здравоохранения. Риски здесь особенно высоки, ведь медицинские ИТ-системы — основа современного ухода за больными, и от их защищенности зависит человеческая жизнь.

Серьезной угрозой, которой до недавнего времени не уделялось должного внимания, является проблема закладок в оборудование, которые могут внедряться, в том числе, во время цепочек поставок.

Атаки такого рода:

- программные, например, внесение изменений в прошивку BIOS, позволяющая читать информацию в защищенных областях;
- замена элементов, например, замена фильтрующего конденсатора на муляж, с целью упрощения проведения атак по сторонним каналам на чип, отвечающий за криптографию;
- добавление посторонних элементов, например, добавление между разъёмом Ethernet и контроллером дополнительного микроконтроллера,

позволяющего блокировать передачу трафика, передавать весь трафик третьему лицу, модифицировать его;

- чип посередине, например, добавление микроконтроллера под usb-контроллер, собирающего информацию о файлах с подключаемых носителей и пересылающий нужные из них третьим лицам;
- добавление интегральной схемы на чип, например, схемы, позволяющей считывать набираемую на клавиатуре и выводимую на монитор информацию;
- импланты в интегральной схеме, например, добавление элемента, блокирующего полностью или изменяющего данные, получаемые от периферийных устройств (например, от датчиков АСУ ТП).

Факты реализации таких угроз, а затем выявление соответствующих последствий, стали довольно многочисленными (пострадавшими компаниями называют, в частности, американские корпорации Amazon и Apple) и могут исполняться, начиная с момента производства чипов, а затем во всех промежуточных пунктах цепочки поставок: сборка изделия – транспортировка - основной дистрибьютор – транспортировка - локальный дистрибьютер – транспортировка - потребитель.

Противодействовать этой угрозе, особенно опасной для КИИ, можно следующими способами:

- оптимизация цепочек поставок;
- контроль за процессом поставки;
- контроль полученного оборудования на отсутствие закладок.

Последний этап является технически очень сложным и должен производиться высокопрофессиональным персоналом на специализированном оборудовании.

Как отвечает современная индустрия ИБ на описываемые вызовы?

На нормативно-методологическом уровне опубликованы документы регуляторов, определяющие основные действия по оценке событий информационной безопасности и взаимодействию субъектов КИИ с регуляторами, в частности с НКЦКИ:

- «Методика оценки угроз безопасности информации. Методический документ». Утвержден ФСТЭК России 5 февраля 2021 г.
- Приказ ФСБ России №281, который распространяется на средства обнаружения, предупреждения, ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. Требования Приказа применимы ко всем субъектам КИИ, в том числе и к субъектам КИИ, функционирующим в банковской сфере и в иных сферах финансового рынка;
- Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирова-

ния на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации». Приказ определяет срок, в который субъект КИИ должен проинформировать НКЦКИ;

- Приказ ФСБ России от 6 мая 2019 г. №196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты». Определяет требования к средствам ГосСОПКА (Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак), которые реализуются одним или несколькими техническими, программными и программно-аппаратными средствами.

Если же рассматривать проблему с технической точки зрения, то информационное сообщество отвечает на вызовы созданием SOC (Security Operations Center) или Центров обеспечения безопасности, которые призваны сыграть роль своего рода «СОБР» - отряда быстрого реагирования на возникающие угрозы ИБ, ликвидацию последствий вторжений, расследование инцидентов в режиме реального времени. Создаются они на корпоративном или ведомственном уровне. При этом в задачи SOC входят не только постоянный мониторинг состояния информационной безопасности в корпоративной сети, но предотвращение угроз путем анализа возможных уязвимостей и вновь возникающих угроз. Анализ инцидентов с целью формирования и корректировки модели угроз и шаблонов поведения злоумышленника – еще одна важнейшая задача, стоящая перед сотрудниками SOC, которую нужно решать в условиях огромного потока информации. Для этого в SOC должна быть создана единая база, хранящая данные обо всех инцидентах, атаках и угрозах, а также инструменты автоматизации поиска нужной информации по заданным критериям.

Известная американская исследовательская компания Gartner назвала три составляющие SOC [7]:

- SIEM (Security information and event management);
- EDR (Endpoint Detection and Response);
- NTA (Network Traffic Analysis).

SIEM – система сбора и корреляции событий, предназначенная для автоматизации процесса выявления угроз. Анализируя информацию, поступающую от различных источников (IDS, межсетевых экранов, DLP-систем и т.д.) SIEM-система отслеживает, анализирует информацию, выявляет корреляцию между событиями и, при нахождении отклонений от штатного (нормального) поведения информационной системы, выдает оповещение администратору информационной безопасности и предоставляет

информацию в виде отчета. SIEM позволяет акцентировать внимание только на критических и действительно важных угрозах, работать не с событиями, а с инцидентами, выявляя их на ранних стадиях. Информация, собираемая SIEM-системой, используется в дальнейшем для расследования инцидентов, проведения аудита ИБ и корректировки политики безопасности.

SIEM-системы разрабатываются и внедряются довольно давно и хорошо известны (примеры) [8]:

- Alert Logic (alertlogic.com);
- IBM QRadar (ibm-security.syssoft.ru);
- McAfee Enterprise Security Manager (mcafee.com/enterprise/ru-ru/products/enterprise-security-manager) от Intel Security;
- КОМРАД – SIEM-система, разработанная «НПО «Эшелон».

EDR — относительно новый класс решений для обнаружения и изучения вредоносной активности на конечных точках: подключенных к сети рабочих станциях, серверах, устройствах Интернета вещей и т.д. Компании редко подключают конечные точки в качестве источников событий в SIEM систему. Соответственно EDR дополняют информационную картину, предоставляемую SIEM. При этом EDR-решения ориентированы на выявление целевых атак и сложных угроз (целенаправленные атаки с использованием неизвестного вредоносного кода, скомпрометированных учетных записей, бесфайловых методов, легитимных приложений и действий, не несущих под собой ничего подозрительного), требующих многоуровневого подхода к обнаружению с использованием передовых технологий [9].

EDR-система состоит из сервера и агентов, устанавливаемых на конечные точки. Агент ведет мониторинг запущенных процессов, действий пользователя и сетевых коммуникаций в реальном времени и передает информацию на сервер. Сервер анализирует полученные данные, в том числе, при помощи технологий машинного обучения, сопоставляет их с базами индикаторов компрометации (IoC) и другой доступной информацией о сложных угрозах. Если EDR-система обнаруживает событие с признаками киберинцидента, она оповещает об этом сотрудников службы безопасности. При этом EDR-система может интегрироваться с SIEM-системами и другими средствами защиты.

Злоумышленник зачастую уничтожает свои следы, но поскольку EDR-система фиксирует все события, связанные с действиями атакующего на хостах в виде последовательности событий, то при анализе атаки можно проследить всю цепочку действий злоумышленника. Это позволяет быстро принимать меры по оперативному предотвращению угрозы.

NTA - системы анализа трафика - выявляют угрозы ИБ, исследуя события на уровне сети. Они позволяют обнаружить присутствие злоумышленников на ранней стадии атаки, оперативно локализовать угрозы и контролировать соблюдение регламентов ИБ. В отличие от других систем, работающих с трафиком (Brandmauer, IDS), которые устанавливаются на периметре сети, NTA-системы анализируют трафик также и в инфраструктуре. Таким образом удается обнаружить действия злоумышленников, уже проникших в систему. Эти системы используются в расследовании инцидентов, в проактивном поиске угроз. В NTA атаки определяются комплексным методом: машинное обучение, индикаторы компрометации, поведенческий анализ. Например, NTA-система Positive Technologies [10] определяет более 85 протоколов, разбирает до уровня L7 включительно 30 наиболее распространенных из них, что позволяет получить подробную картину событий в корпоративной сети и повышает эффективность работы SOC.

В дополнение к указанному комплексу технологий и средств ИБ можно добавить интеграцию в него системы класса User [and Entity] Behavioral Analytics (UEBA/UBA), что можно перевести, как «поведенческая аналитика пользователей и сущностей», но принято называть такие комплексы как «системы поведенческого анализа» или UEBA-системы.

Формально UEBA и UBA относятся к одному классу систем, но при этом UBA-системы берут за основу информацию, связанную только с пользовательской активностью, а UEBA-системы информацию о пользователях и ролях дополняют информацией о системном окружении — хостах, приложениях, сетевом трафике и системах хранения данных. Благодаря этому UEBA-системы способны идентифицировать более широкий класс угроз, связанных и с пользователями, и с объектами ИТ-инфраструктуры.

Анализируя собранные данные, UEBA-система строит шаблон нормального поведения пользователя и его взаимодействия с корпоративными системами на основе статистических алгоритмов и с помощью алгоритмов машинного обучения. Помимо этого, UEBA-системы могут строить модели поведения целых групп пользователей и определять отклонения каждого из них от общей модели.

Если какие-то действия пользователей выходят за рамки соответствующей модели, UEBA-система определяет эту ситуацию как аномальную и посылает предупреждение администратору безопасности. Это должно происходить в режиме реального времени.

Имея накопленный массив данных, системы поведенческого анализа ведут статистику по каждому пользователю и на основе собранных дан-

ных по его аномальной активности оценивают риски по каждому из них. В дальнейшем эти оценки ранжируются по степени важности событий для дальнейшего анализа администратором ИБ безопасности.

Кроме аналитики внешних угроз, системы поведенческого анализа способны эффективно определять аномальную активность инсайдеров – сотрудников организации – в части внешнего взаимодействия с корпоративными системами, повышения привилегий и т.д. Анализируются системные журналы, почтовая переписка, сообщения мессенджеров. Это повышает эффективность основных DLP-систем и снижает риски внутренних угроз.

В настоящее время UEBA-системы создаются, как правило, на базе существующих SIEM-, DLP-, IDS-систем в виде наложенных расширений, например, IBM QRadar UBA; на ряде фирм появляются собственные программные решения, например, Splunk UBA. Однако тенденция последних двух лет говорит о том, что технологии и продукты поведенческого анализа будут интегрироваться крупными вендорами в свои продукты для создания комплексных систем защиты информации.

В некоторые отечественные продукты включен функционал поведенческого анализа:

- Secure Portal от Group IB;
- Kaspersky Fraud Prevention от «Лаборатории Касперского»;
- Solar Dozor от Solar Security;
- Гарда БД от «МФИ Софт»;
- Контур информационной безопасности (КИБ) от SearchInform.

Единая система из указанных составляющих, собранная в SOC, позволит проводить автоматическое реагирование на инциденты в КИИ, изолировать атакованные хосты, выключать скомпрометированные сервисы и передавать сведения о найденных угрозах и инцидентах в ГосСОПКА.

Отдельно хотелось бы отметить такую важную часть КИИ, как АСУ ТП, которые могут быть подвергнуты атакам любого рода, как со стороны внешних хакеров, так и со стороны внутренних злоумышленников. Это может привести к серьезным последствиям – от выпуска брака, до выхода их строя объекта управления.

Очевидным решением, чтобы избавиться от внешних угроз, является полностью изолированная локальная сеть АСУ ТП, не связанная с корпоративной сетью предприятия. При этом проблема любого рода обновлений – как в части технологических процессов, так и в части системного и прикладного ПО – может быть решена путем установки обновлений с внешних носителей строгой отчетности, на которые (после тщательного контроля) обновления заносятся уполномоченными сотрудниками из числа оперативного персонала службы ИБ.

Для контроля умышленных или непреднамеренных действий персонала, рассматриваемых как действия внутренних нарушителей, обычно используются различного рода логические блокировки, но на современном уровне являющиеся специализированными модулями DLP-систем. Такие средства позволят предотвратить не только нарушения технологического процесса и выход из стоя системы управления, но и выход из стоя самого объекта управления. Кроме этого такие модули будут вести документальный учет всех действий оперативного персонала в соответствующих журналах. Это позволить провести быстрое расследование причин брака и других произошедших инцидентов, а также сообщать о них в НКЦКИ.

Если на производстве все же принимают решение связать АСУ ТП с другими модулями ERP-системы, например, системой автоматизированного проектирования, автоматизированной системой технологической подготовки производства то, наряду с очевидными вопросами аутентификации и разграничения доступа, встает вопрос защиты от внешних угроз, которым подвергается вся корпоративная сеть. Здесь традиционные средства защиты информации решить поставленную задачу не в состоянии, поскольку они не предусматривают, в частности, защиту нижнего уровня АСУ ТП – контроллеров, устройств связи с объектом, датчиков, исполнительных механизмов. В такой ситуации возможно применение только сертифицированных программно-аппаратных средств защиты информации отечественной разработки, например, InfoWatch ARMA Industrial Firewall или USER GATE.

Включение АСУ ТП в сферу деятельности SOC корпорации является обязательным условием успешного функционирования КИИ.

Общей методологии создания SOC в России пока не существует, как нет и нормативных документов по их организации. Поэтому создание таких Центров обеспечения безопасности решается на местах на основе собственного подхода, целесообразного в конкретной ситуации. Можно, конечно, пользоваться материалами американских NIST и Mitre, но только в ознакомительном смысле. Очевидно, что базовыми основами создания SOC являются модель угроз, модель нарушителя, оценка рисков, масштаб и потенциальные возможности самой организации.

Считается, что затраты на создание SOC окупаются в среднесрочной перспективе за счет минимизации вторжений и эффективного устранения их последствий, а, следовательно, снижения ущерба. Однако на этапе создания Центра предстоит тщательная работа по выбору необходимых программных и технических средств, а также подбору специалистов. Здесь есть серьезная проблема, связанная с дефицитом кадров: необходимы спе-

циалисты, обладающие компетенциями как в области ИБ (аудит информационной безопасности, пентестинг), так и в отраслевой предметной области (АСУ ТП, финансовая сфера и т.д.). При этом подготовка таких «комплексников» занимает определенное время. И, конечно, в создании Центров обеспечения безопасности должно быть заинтересовано руководство компании, понимая, что это не затраты, а инвестиции.

Однако подход к созданию собственного Центра обеспечения безопасности должен быть тщательно взвешен. В ряде случаев бывает целесообразно воспользоваться услугами провайдера SOC.

В заключении отметим, что соотношение сил киберпреступников и защитников всегда оказывается в пользу атакующих, которые действуют на шаг вперед, очень быстро и высокопрофессионально: изобретают новые технологии атак, используют новейшие уязвимости, часто меняют инструментарий. Отсюда наблюдается такой рост в потребности интеллектуальных средств защиты и в подготовке профессионалов в области информационной безопасности.

Литература

1. Уязвимости периметра корпоративных сетей. [Электронный ресурс]. - URL: https://www.ptsecurity.com/ru-ru/research/analytics/vulnerabilities-corporate-networks-2020/ (дата обращения: 20.03.2021).
2. Операция «Aurora». Удар по Google и прочим. [Электронный ресурс]. - URL: https://habr.com/ru/post/81137/ (дата обращения: 22.03.2021)
3. Мария Нефёдова. Хак-группа Calypso атакует госучреждения с 2016 года. [Электронный ресурс]. - URL: https://xakep.ru/2019/11/01/calypso/ (дата обращения: 21.03.2021).
4. «Лаборатория Касперского»: Lazarus атакует оборонные предприятия по всему миру. [Электронный ресурс]. - URL: https://www.kaspersky.ru/about/press-releases/2021_lazarus-advanced-persistent-threat-group-targets-the-defense-industry (дата обращения: 20.03.2021).
5. Matan Ben David. Incident Response Casefile – A successful BEC leveraging lookalike domains. [Электронный ресурс]. - URL: https://research.checkpoint.com/2019/incident-response-casefile-a-successful-bec-leveraging-lookalike-domains/ (дата обращения: 20.03.2021).
6. Hazel Burton. Out today: Defending against critical threats: A 12 month roundup. [Электронный ресурс] - URL: https://blogs.cisco.com/security/out-today-defending-against-critical-threats-a-12-month-roundup (дата обращения: 21.03.2021).

7. Applying Network-Centric Approaches for Threat Detection and Response. [Электронный ресурс]. - URL: https://www.gartner.com/en/documents/3904768/applying-network-centric-approaches-for-threat-detection (дата обращения: 21.03.2021).

8. Чернокнижный Г.М. Защита сетевых информационных технологий: учебное пособие / Г.М. Чернокнижный. – СПб.: Изд-во СПбГЭУ, 2018. – 128 с.

9. Endpoint Detection & Response (EDR). [Электронный ресурс]. - URL: https://encyclopedia.kaspersky.ru/glossary/edr-endpoint-detection-response/ (дата обращения: 20.03.2021).

10. PT Network Attack Discovery. [Электронный ресурс]. - URL: https://www.ptsecurity.com/upload/corporate/ru-ru/products/nad/PT-NAD_PB_15-2021.pdf (дата обращения: 24.03.2021).

УДК 621.039.58

Якушкина Ирина Георгиевна
преподаватель
Комитет по вопросам, законности, правопорядка и безопасности
Санкт-Петербургское государственное казенное
учреждение дополнительного профессионального образования
«Учебно-методический центр по гражданской обороне и
чрезвычайным ситуациям»

ПРОБЛЕМНЫЕ ВОПРОСЫ ЭКСПЛУАТАЦИИ ИССЛЕДОВАТЕЛЬСКИХ РЕАКТОРОВ

Аннотация. В статье проводится анализ проблемных вопросов, касающихся безопасности эксплуатации исследовательских реакторов, а также задач, решаемых при проведении исследований, введении в действие научных разработок с помощью исследовательских реакторов. Классификация, история создания исследовательских реакторов; технические характеристики, вопросы безопасности исследовательских реакторов; задачи, решаемые с помощью исследовательских реакторов. Характеристики исследовательских реакторов У-3, ПИК, МБИР.

Ключевые слова: безопасность исследовательских реакторов; исследования, проводимые на исследовательских реакторах; реакторы У-3, ПИК, МБИР.

Yakushkina I.G.
Saint-Petersburg State Institution of Additional Professional Education
«Training and Methodological Center for Civil Defense
and Emergency Situations»

PROBLEMATIC ISSUES OF OPERATION RESEARCH REACTORS

Annotation. The article analyzes the problematic issues related to the safety of operation of research reactors, as well as the tasks solved during research, the introduction of scientific developments with the help of research reactors. Classification, history of the creation of research reactors; technical characteristics, safety issues of research reactors; problems solved with the help of research reactors. Characteristics of research reactors U-3, PIK, MBIR.

Keywords: safety of research reactors; research conducted at research reactors; U-3, PIK, MBIR reactors.

Российская наука, шаг за шагом, постепенно, возвращает себе мировое первенство, в области научных исследований и разработок, почти утерянное в 90-е, и в первую очередь, это касается вопросов ядерной безопасности, применения ядерной энергии, эксплуатации исследовательских реакторов.

Цель данной работы провести анализ проблемных вопросов, касающихся безопасности эксплуатации исследовательских реакторов, а также задач, которые успешно решаются при проведении исследований, введении в действие научных разработок с помощью исследовательских реакторов.

Ядерные реакторы - это устройства, предназначенные для организации и поддержания управляемой цепной реакции деления ядер [2], могут быть различных видов: транспортные, энергетические, промышленные, исследовательские и т.д.

Наиболее потенциально опасными считаются энергетические реакторы, вырабатывающие электрическую энергию на атомных электростанциях (далее – АЭС). Эксплуатирующая организация всех российских АЭС – это АО «Концерн Росэнергоатом». Российская атомная отрасль является одной из передовых в мире по уровню научно-технических разработок в области проектирования реакторов, ядерного топлива, опыту эксплуатации атомных станций, квалификации персонала АЭС [6].

В общей сложности в России на 11 АЭС эксплуатируются 38 энергоблоков установленной мощностью 30,576 ГВт. Сегодня Ленинградская АЭС – продолжает оставаться самой мощной атомной станцией нашей страны. Установленная мощностью АЭС составляет 4400 МВт [6].

На АЭС сегодня реализуются все необходимые меры безопасности.

Исследовательские реакторы отличаются от промышленных ядерных реакторов, конечно же, в первую очередь, меньшей мощностью и меньшим объемом, но не меньшей потенциальной опасностью.

Такие реакторы предназначены для проведения фундаментальных и прикладных исследований, при которых нейтроны и гамма-кванты используются как инструмент или объект исследований [3]. В мире насчитывается порядка 250 исследовательских ядерных реакторов. В России их чуть больше 20.

В Российской Федерации все исследовательские реакторы находятся в ведении Корпорации «Росатом». Принадлежат, как правило, организациям, их эксплуатирующим, научным центрам.

Физический первый – Ф-1 исследовательский реактор был введен в эксплуатацию уже в 1946 году под руководством академика Игоря Васильевича Курчатова. Впервые в Евразии после запуска реактора были проведены необходимые исследования для проектирования промышленного производства плутония. Исключительно ценный опыт и проведенные исследования по ядерной физике позволили перейти к проектированию и сооружению других реакторов. Реактор Ф-1 находится в рабочем состоянии до сих пор, и его периодически используют.

Исследовательские реакторы всегда выполняют три основные задачи:

облучение материалов и сборок и затем их для после - реакторное исследование;

изучение поведения материалов и сборок прямо в реакторе;

вывод нейтронного (нейтринного) излучения в лабораторные установки вокруг.

Сегодня исследовательские реакторы также широко используются для производства конкретной продукции: наработки изотопов медицинского или промышленного назначения, наработки ядерно-легированного кремния для электронной промышленности и прочее.

С момента создания первого исследовательского ректора были разработаны все необходимые меры их безопасной эксплуатации.

Ядерная безопасность исследовательского реактора - свойство исследовательского реактора предотвращать ядерные аварии и ограничивать их последствия [2].

Прежде всего, все системы и элементы исследовательских реакторов, важные для безопасности, должны проектироваться с учетом механических, тепловых, химических, радиационных и прочих внутренних воздействий, возможных при нормальной эксплуатации и при нарушениях нормальной эксплуатации, включая проектные аварии, а также с учетом внешних воздействий природного и техногенного происхождения, возможных на площадке размещения исследовательских реакторов [2].

Международная шкала ядерных событий разработана Международным агентством по атомной энергии (МАГАТЭ) в 1988 году и используется в целях единообразия оценки чрезвычайных случаев, связанных с аварийными радиационными выбросами в окружающую среду, связанными с гражданской атомной промышленностью.

МАГАТЭ (Международное агентство по атомной энергии) рекомендует оповещать страны-участники в 24-часовой срок о всех авариях выше 2 уровня опасности, когда имеются хотя бы незначительные выбросы радиации за пределы производственной площадки, в случаях событий 0 и 1 уровней, если того требует общественный интерес за пределами страны, в которой они произошли. Информация передаётся в СМИ странами-участниками и самим МАГАТЭ, в том числе посредством интернета. Такой подход позволяет оперативно и согласованно оповещать общественность о значимости с точки зрения безопасности событий на ядерных установках, о которых поступают сообщения. Это позволит населению вовремя предпринять все необходимые меры защиты в случае повышения радиационного фона. В норме он равен 18-27 мкР/час (0,18-0,27 мкЗв/час).

В отношении потенциальной опасности, которую они представляют, исследовательские реакторы можно разделить на следующие основные группы (Рис. 1) [4]:

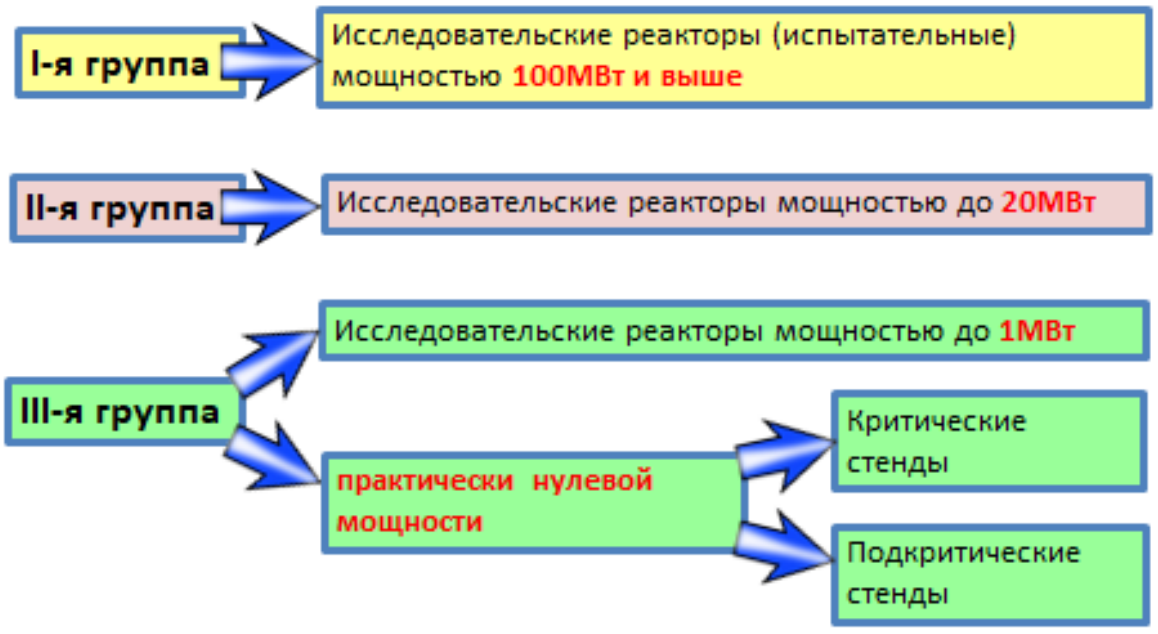


Рисунок 1 - Основные группы исследовательских реакторов по степени потенциальной опасности

I-я группа - исследовательские реакторы (испытательные) мощностью 100МВт и выше, для которых возможны запроектные аварии по всем

уровням Международной Шкалы Событий. Реакторы этой группы предназначены в большинстве случаев для испытаний материалов и оборудования для атомной энергетики и т.д.;

II-я группа - исследовательские реакторы мощностью до 20МВт, предназначенные для учебных целей, фундаментальных физических исследований и производства радиоактивных изотопов;

III-я группа - исследовательские реакторы мощностью до 1МВт, критические и подкритические стенды практически нулевой мощности, не требующие систем принудительного аварийного расхолаживания активной зоны.

Критические и подкритические стенды не являются радиационно опасными объектами. Уровень любых событий на них должен находиться ниже минимального уровня, установленного Международной Шкалой Событий. Они отличаются незначительной мощностью (обычно максимум несколько киловатт).

Критический стенд - это сборка ядерного реактора, геометрические и физические свойства которой позволяют осуществлять управляемую цепную реакцию деления ядер в заданных условиях [5].

Подкритический стенд - это устройство для проведения экспериментальных исследований, содержащее размножающую нейтроны среду [5].

По данным, основанным на отечественной и международной практике, для реакторов мощностью до 1-2 МВт, не должно быть событий выше 2-3 уровней Международной Шкалы Событий, что обусловлено их внутренней самозащищенностью и выполнением требований специальных норм и правил [5].

Согласно свода правил СП 165.1325800.2014 «Инженерно-технические мероприятия по гражданской обороне» [1], зону возможного радиоактивного загрязнения для ядерных установок (за исключением атомных станций), пунктов хранения ядерных материалов и радиоактивных веществ ограничивают границами проектной застройки указанных объектов и примыкающей к ней санитарно-защитной зоной.

Санитарно-защитная зона - территория вокруг радиационного объекта, на которой уровень облучения людей в условиях нормальной эксплуатации техногенных источников ионизирующего излучения может превысить установленный предел допустимой дозы облучения населения. В санитарно-защитной зоне проводится радиационный контроль, запрещается размещение жилых здания, детских учреждений, больниц, госпиталей, санаториев и других учреждений общего пользования, а также промышленных и подсобных помещений, не относящихся к объекту, для которого установлена санитарно-защитная зона [8].

Размеры санитарно-защитной зоны подбираются индивидуально с учетом мощности, климатических условий и других характеристик.

Санитарно-защитные зоны устанавливают санитарный разрыв между промышленными предприятиями и жилыми или общественными зданиями, защищают население от влияния вредных факторов (шум, запылённость, выбросы химических, радиоактивных веществ). Это позволяет эксплуатировать исследовательские реакторы, находящиеся в городской черте.

Тем не менее, существует ряд специфических сложностей эксплуатации всех типов исследовательских реакторов, что может стать источником потенциальной опасности реакторов:

высокая частота переходных режимов при работе (пуски, остановки, изменения мощности в широком диапазоне, динамические эксперименты), при которых чаще всего и происходят нарушения в работе исследовательской ядерной установки;

частые перегрузки активных зон и постоянное перемещение облученных изделий (на исследования, в бассейны выдержки, на длительное хранение, на утилизацию и т.д.);

меньшее, чем у энергетических реакторов количество физических барьеров, препятствующих распространению продуктов деления, особенно у бассейновых исследовательских реакторов и критических сборок;

износ технических средств на реакторах, не прошедших модернизацию;

оснащенность экспериментальными устройствами и связанные с ними особенности эксплуатации;

расположение реакторов в крупных городах с многомиллионным населением среди городской застройки;

исследовательский реактор часто является частью большого исследовательского центра или университета, где имеется потенциально много пользователей, представляющих различные научные дисциплины.

Так, в Ленинградской области, в Гатчине (это порядка 30 км от Санкт-Петербурга) 8 февраля 2021 года произошел запуск на полную мощность одного из самых мощных исследовательских реакторов в мире - высокопоточного пучкового реактора «ПИК». Его мощность 100 МВт - это I группа потенциальной опасности. Самый мощный в мире исследовательский реактор, генерирующий поток нейтронов. Гипотетически, у такого реактора возможны аварии любого уровня потенциальной опасности.

Санитарно-защитная зона вокруг реактора ПИК установлена в радиусе 900 метров. Реактор находится в черте города, но комплекс занимает закрытую территорию под усиленной охраной внутренних войск.

На базе реактора ПИК планируется создание Международного центра нейтронных исследований. Центр открывает широкие перспективы взаимодействий ядерной физики, медицины, материаловедения, нанобиотехнологий.

Нейтронами можно просвечивать вещество как рентгеновскими лучами, но в отличие от рентгена нейтронные пучки лучше реагируют с лег-

кими атомами, из которых в основном состоят биологические ткани. С помощью нейтронов можно увидеть буквально структуру органических и неорганических материалов и конструкций. Пучки нейтронов дают возможность биологам выяснить структуру сложных молекул, в состав которых входят элементы, не распознаваемые рентгеном.

Так, в авиационной промышленности благодаря нейтронным исследованиям ученые доказали, что часть соединений фюзеляжа самолета, делавшиеся раньше заклепками, можно заменить сварным швом. Фюзеляж – это основная часть конструкции самолета (вертолета), служащая для соединения в одно целое всех его частей, а также для размещения экипажа, пассажиров, оборудования и грузов. Сварной шов вместо заклепок дает экономию на массе приблизительно 5%. Пять процентов — это огромная экономия в топливе и в эксплуатационных расходах. Таким образом, исследуя структуру вещества, можно изменять достаточно серьезные технологии производства и промышленности.

С помощью нейтронов медики могут эффективно облучать всю структуру раковой опухоли, также разрабатываются инновационные лекарственные препараты, методы лечения онкологических заболеваний.

В Санкт-Петербурге Крыловский государственный научный центр – федеральное государственное унитарное предприятие, научно-исследовательский институт, занимающийся фундаментальными исследованиями, связанными с морем, а также кораблестроением и смежной деятельностью. Основан центр в 1894 году. Исследовательский ядерный реактор У-3 спроектирован специалистами ЦНИИ им. Крылова и запущен в декабре 1964 года. Реактор относится к третьей группе потенциальной опасности. Его мощность составляет 50 кВт.

Сегодня в Петербурге – это единственный радиационно опасный объект, находящийся в городской черте. Вокруг реактора установлена санитарно-защитная зона в радиусе 100 м (Рис. 2). К сожалению, когда реактор только строился, эта была дальняя окраина города. Вокруг стояли заводы. В последние же годы эту промышленную зону начали застраивать жилищными комплексами. Сегодня срок эксплуатации реактора продлен до 2024 года [7]. Система отвечает всем современным требованиям и продолжает использоваться.

У-3 – работает на малых мощностях и возможности реактора ограничены – это реактор на тепловых (медленных) нейтронах, так называемые «тепловой реактор». Его применяют для отдельных экспериментов и получения короткоживущих изотопов [7].

С помощью реактора У-3 было решено множество задач, определивших облик современного отечественного атомного флота:

обеспечение высочайших стандартов прочности подводных лодок, боевых надводных кораблей и судов всех типов;

разработка средств физической защиты экипажа атомных подводных лодок от радиационного излучения и защиты по радиационным полям;

создание высокоэффективных гребных винтов для отечественных кораблей и зарубежных судов;

обеспечение лидирующего положения в мире в области создания кораблей и зарубежных судов принципиально новых типов или с новыми качествами [7].

Рисунок 2 - Санитарно-защитная зона вокруг реактора У-3 в Санкт-Петербурге

Запуск самого мощного в мире исследовательским ядерным реактором на быстрых нейтронах из всех действующих, сооружаемых и даже только проектируемых запланирован на 2028 год. Им станет Многоцелевой исследовательский ядерный реактор - МБИР в Димитровграде (Ульяновская область). Его тепловую мощность 150 МВт [9].

На базе МБИР планируется создать Международный центр исследований. Основным предназначением реактора МБИР будет проведение массовых реакторных испытаний инновационных материалов и макетов элементов активных зон для новейших ядерно-энергетических систем.

Вывод. Возникающие проблемные вопросы безопасности при эксплуатации исследовательских реакторов успешно решаются. Сегодня, исследовательские реакторы зарекомендовали себя с только с положительной стороны. Они играют важнейшую роль в развитии ядерной энергетики и используются для выполнения широкой программы фундаментальных исследований в различных областях науки и техники. Меры безопас-

ности исследовательских реакторов соблюдаются в соответствии с классификацией их потенциальной опасности, которая зависит, в первую очередь, от тепловой мощности исследовательского реактора. Технические характеристики исследовательских реакторов, гарантируют надёжное обоснование и поддержание на должном уровне безопасности объектов и прилегающих территорий.

Литература

1. Инженерно-технические мероприятия по гражданской обороне: СП 165.1325800.2014// Актуализированная редакция СНиП 2.01.51-90 – М. [Электронный ресурс]. – URL: https://docs.cntd.ru/document/1200118578 (дата обращения: 29.03.2021).
2. Об утверждении федеральных норм и правил в области использования атомной энергии «Правила ядерной безопасности исследовательских реакторов». Приказ Ростехнадзора ФНП в области использования атомной энергии от 11 сентября 2017 №295. [Электронный ресурс]. – URL: https://docs.cntd.ru/document/436762418 (дата обращения: 29.03.2021).
3. ГОСТ 23082-78 // (Изм. 01.03.2005). Реакторы ядерные. Термины и определения. [Электронный ресурс]. – URL: https://docs.cntd.ru/document/1200015295?section=text (дата обращения: 29.03.2021).
4. Кузнецов В.Н. Безопасность ядерных исследовательских установок Российской Федерации. - 2001г. [Электронный ресурс]. – URL: http://www.seu.ru/programs/atomsafe/books/Kuznecov/Doclad3.htmhttps://speclit.su/image/catalog/978-5-299-00869-2/978-5-299-00869-2.pdf (дата обращения: 29.03.2021).
5. Гончаров В.В. Исследовательские реакторы // Советская атомная наука и техника: сборник статей. – 1967 г. [Электронный ресурс]. – URL: http://elib.biblioatom.ru/text/sovetskaya-atomnaya-nauka-i-tehnika_1967/go,6/ (дата обращения: 29.03.2021).
6. Официальный сайт Госкорпорации «Росатом» [Электронный ресурс]. - URL: https://www.rosatom.ru/about/ (дата обращения: 29.03.2021).
7. Официальный сайт Крыловского государственного научного центра. [Электронный ресурс]. - URL: https://krylov-centre.ru/, http://flnph.jinr.ru/images/ content/Books/Nuclear_Facilities/069.pdf (дата обращения: 29.03.2021).
8. Словарь терминов МЧС России. [Электронный ресурс]. - URL: https://www.mchs.gov.ru/ministerstvo/o-ministerstve/terminy-mchs-rossii (дата обращения: 29.03.2021).
9. Официальный сайт Международного Центра исследований МБИР (Росатома) [Электронный ресурс].- URL: http://mbir-rosatom.ru/ (дата обращения: 29.03.2021).

СВЕДЕНИЯ ОБ АВТОРАХ

Александрова Светлана Юрьевна – канд. экон. наук, доцент кафедры безопасности населения и территорий от чрезвычайных ситуаций Санкт-Петербургского государственного экономического университета, e-mail: varg-su@mail.ru

Алексеева Ольга Владимировна – канд. геогр. наук, доцент кафедры педагогики и педагогических технологий Ленинградского государственного университета им. А.С. Пушкина, e-mail: okrukova@gmail.com

Васильева Ирина Николаевна – канд. физ.-мат. наук, доцент кафедры вычислительных систем и программирования Санкт-Петербургского государственного экономического университета, Санкт-Петербургский университет МВД России, e-mail: i_vasy@mail.ru

Воротков Павел Александрович – аналитик Автономной некоммерческой организации «Агентство по привлечению инвестиций Свердловской области», г. Екатеринбург, e-mail: p.vorotkov@ai-so.ru

Ильина Ольга Павловна – канд. экон. наук, профессор кафедры информатики Санкт-Петербургского государственного экономического университета, e-mail: ilop@mail.ru

Кириленко Вадим Владимирович – канд. экон. наук, доцент кафедры общественного здоровья и здравоохранения Санкт-Петербургского государственного педиатрического медицинского университета, e-mail: vadimvlkir@bk.ru

Кропива Ирина Анатольевна – заведующий отделением колледжа бизнеса и технологий Санкт-Петербургского государственного экономического университета, e-mail: irina-kropiva@yandex.ru

Круглов Дмитрий Валерьевич – профессор, доктор экон. наук, профессор кафедры экономики труда Санкт-Петербургского государственного экономического университета, e-mail: kdvspb@list.ru

Лепеш Григорий Васильевич – профессор, доктор техн. наук, заведующий кафедрой безопасности населения и территорий от чрезвычайных ситуаций Санкт-Петербургского государственного экономического университета, e-mail: GregoryL@yandex.ru

Ложкина Ольга Владимировна – профессор, доктор техн. наук, канд. хим. наук, профессор кафедры физико-химических основ процессов горения и тушения Санкт-Петербургского университета Государственной противопожарной службы МЧС России, e-mail: olojkina@yandex.ru

Лунева Светлана Курусовна – старший преподаватель кафедры безопасности населения и территорий от чрезвычайных ситуаций Санкт-Петербургского государственного экономического университета, e-mail: isvetlana1508@mail.ru

Мартынов Василий Львович – профессор, доктор геогр. наук, профессор кафедры экономической географии Российского государственного педагогического университета им. А.И. Герцена, e-mail: lwowich@herzen.spb.ru

Мордовец Виталий Анатольевич – доцент, канд. экон. наук, заведующий кафедрой экономики и управления социально-экономическими системами Санкт-Петербургского университета технологий управления и экономики, e-mail: mordovets@mail.ru

Пастухов Александр Львович – доцент, канд. филол. наук, доцент кафедры безопасности Северо-Западного института управления – филиала Российской академии народного хозяйства и государственной службы при Президенте РФ, e-mail: alpast@yandex.ru

Ризов Алексей Дмитриевич – канд. экон. наук, начальник электротехнической лаборатории АО «Чусовской металлургический Завод», Пермский край, e-mail: aleksejrizov@rambler.ru

Смекалин Сергей Владимирович – преподаватель Санкт-Петербургского государственного казенного учреждения дополнительного профессионального образования «Учебно-методический центр по гражданской обороне и чрезвычайным ситуациям», e-mail: smekalin77@mail.ru

Соколова Вера Васильевна – канд. мед. наук, доцент кафедры общественного здоровья и здравоохранения Санкт-Петербургского государственного педиатрического медицинского университета, e-mail: vera-sokol@inbox.ru

Соленов Юрий Александрович – канд. воен. наук, доцент, преподаватель Санкт-Петербургского государственного казенного учреждения дополнительного профессионального образования «Учебно-методический центр по гражданской обороне и чрезвычайным ситуациям», e-mail: vasiliostrov.spb-umc@mail.ru

Угольников Владимир Владимирович – канд. экон. наук, доцент кафедры экономики и управления Санкт-Петербургского государственного химико-фармацевтического университета Минздрава России, e-mail: ougalaynnen@mail.ru

Угольникова Ольга Дмитриевна – доцент, канд. физ.-мат. наук, доцент кафедры безопасности населения и территорий от чрезвычайных ситуаций Санкт-Петербургского государственного экономического университета, e-mail: olga_ugolnikova@mail.ru

Федорова Татьяна Аркадьевна - профессор, доктор экон. наук, профессор кафедры банков, финансовых рынков и страхования Санкт-Петербургского государственного экономического университета, e-mail: linatic@mail.ru

Хайкин Марк Михайлович – профессор, доктор экон. наук, заведующий кафедрой экономической теории Санкт-Петербургского горного университета, e-mail: marcmix.spb@gmail.com

Чекарев Леонид Васильевич – преподаватель Санкт-Петербургского государственного казенного учреждения дополнительного профессионального образования «Учебно-методический центр по гражданской обороне и чрезвычайным ситуациям», e-mail: chekarevl@list.ru

Чернокнижный Геннадий Михайлович – канд. техн. наук, доцент кафедры вычислительных систем и программирования Санкт-Петербургского государственного экономического университета, e-mail: chernokniznyy.g@unecon.ru

Шарафутдинова Лилия Ражаповна – аспирант Санкт-Петербургского государственного экономического университета, e-mail: liliya.sharafutdinova22@gmail.com

Якушкина Ирина Георгиевна – Комитет по вопросам, законности, правопорядка и безопасности, преподаватель Санкт-Петербургского государственного казенного учреждения дополнительного профессионального образования «Учебно-методический центр по гражданской обороне и чрезвычайным ситуациям», e-mail: yakushkina-spb@mail.ru

СОДЕРЖАНИЕ

Научное издание

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ И ВОПРОСЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ РЕАЛЬНОЙ ЭКОНОМИКИ

Сборник научных трудов
по итогам III Всероссийской научно-практической конференции
«Инновационные технологии и вопросы обеспечения безопасности реальной экономики»

Санкт-Петербург

31 марта 2021 года

Под редакцией
доктора технических наук, профессора Г.В. Лепеша,
кандидата физико-математических наук, доцента О.Д. Угольниковой
кандидата экономических наук, доцента С.Ю. Александровой

Подписано в печать 21.10.2021. Формат 60×84 1/16.
Усл. печ. л. 14,5. Тираж 500 экз. Заказ 853.

Издательство СПбГЭУ. 191023, Санкт-Петербург,
наб. канала Грибоедова, д. 30-32, лит. А.

Отпечатано на полиграфической базе СПбГЭУ