Научная статья
УДК 004; 519; DOI: 10.61260/1998-8990-2024-3-41-54

РОЛЬ И МЕСТО ИНФОРМАЦИОННОЙ И ПОЖАРНОЙ БЕЗОПАСНОСТИ В ОБЕСПЕЧЕНИИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

✉Синещук Юрий Иванович;
Смирнов Алексей Сергеевич;
Терёхин Сергей Николаевич;
Шидловский Григорий Леонидович.
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
✉sinegal53@mail.ru

Аннотация. Наблюдаемая сегодня интеграция инновационных по форме и информационных по содержанию технологий в операции по обеспечению национальной безопасности привела к существенным достижениям, созданию более безопасных сообществ и более эффективных механизмов реагирования на чрезвычайные ситуации. При этом угрозы, создаваемые технологиями информационного века, еще более актуализируют проблему осмысления актуальных задач обеспечения национальной безопасности. Эти обстоятельства потребовали обобщения и конкретизации понятий, употребляемых в сфере безопасности на системном уровне, уточнения состава базовых, системообразующих видов национальной безопасности Российской Федерации и связей между ними. Основываясь на принципах системного подхода к исследованию сложных объектов, к числу которых относится система национальной безопасности Российской Федерации, в статье обосновывается перманентная значимость пожарной безопасности и возрастающая роль информационной безопасности в обеспечении всей совокупности видов национальной безопасности.

Ключевые слова: безопасность, пожарная безопасность, информационная безопасность, национальная безопасность, система национальной безопасности

Для цитирования: Синещук Ю.И., Смирнов А.С., Терехин С.Н., Шидловский Г.Л. Роль и место информационной и пожарной безопасности в обеспечении национальной безопасности // Проблемы управления рисками в техносфере. 2024. № 3 (71). С. 41–54. DOI: 10.61260/1998-8990-2024-3-41-54.

Scientific article

THE ROLE AND PLACE OF INFORMATION AND FIRE SAFETY IN ENSURING NATIONAL SECURITY

✉Sineshchuk Yuriy I.;
Smirnov Aleksey S.;
Terehin Sergey N.;
Shidlovskiy Grigoriy L.
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia
✉sinegal53@mail.ru

Abstract. The integration of innovative in form and content-based information technologies into national security operations has led to significant achievements, the creation of safer communities and more effective emergency response mechanisms. At the same time, the threats posed by the technologies of the information age further actualize the problem of understanding

the urgent tasks of ensuring national security. These circumstances required generalization and concretization of concepts used in the field of security at the systemic level, clarification of the composition of the basic, system-forming types of national security of the Russian Federation and the links between them. Based on the principles of a systematic approach to the study of complex objects, which include the national security system of the Russian Federation, the article substantiates the permanent importance of fire safety and the increasing role of information security in ensuring the totality of types of national security.

Keywords: security, fire safety, information security, national security, national security system

For citation: Sineshchuk Yu.I., Smirnov A.S., Terehin S.N., Shidlovskiy G.L. The role and place of information and fire safety in ensuring national security // Problemy upravleniya riskami v tekhnosfere = Problems of risk management in the technosphere. 2024. № 3 (71). P. 41–54. DOI: 10.61260/1998-8990-2024-3-41-54.

Введение

Начало XX в. охарактеризовалось повсеместным развитием цифровых продуктов и электронных услуг. Масштабность и интенсивность влияния на все отрасли экономики технологической компоненты, реализуемой в процессе цифровой трансформации, переходе к экономике данных, позволяет говорить о качественных, системных изменениях, происходящих и в сфере обеспечения национальной безопасности. Формирование сквозных информационных технологий обуславливает не только новые расширяющиеся возможности в различных предметных областях, но и требует активной реакции на обострившиеся традиционные и появившиеся новые угрозы безопасности [1].

Наиболее востребованные, интенсивно развивающиеся технологии сегодняшнего дня характеризуют качественное содержание четвертой промышленной революции, определяющей современный этап уровня развития человечества [2]. Например, беспилотные летательные аппараты с камерами и датчиками высокого разрешения могут быстро обследовать районы, пострадавшие от стихийных бедствий, предоставляя службам реагирования на чрезвычайные ситуации (ЧС) визуальные данные в режиме реального времени, что позволяет принимать более оперативные и обоснованные решения. Коммуникационные технологии обеспечивают интенсивный, устойчивый обмен мультимедийной информацией, улучшая координацию между задействованными службами и должностными лицами органов управления, принимающих решения. Технологии анализа больших данных (Big data) позволяют выявлять тенденции, закономерности в проявлении тех или иных деструктивных явлений и принимать упреждающие меры. Технологии искусственного интеллекта (ИИ, Artificial Intelligence – AI), интернета вещей (Internet of Things – IoT), «умного города» (smart-city) обеспечивают распознание объектов и ситуаций, контролируют общественные пространства, инфраструктуру, транспортные потоки. Глобальное, интенсивное проникновение информационных систем и технологий во все области жизнедеятельности человека, общества, государства приводит к формированию и постоянному возрастанию роли «информационной сферы» [3–6]. Вместе с тем возрастает и зависимость эффективного функционирования всех механизмов и структур государства от уровня информационной безопасности информационных систем и технологий, обеспечивающих их деятельность, от способности этих систем сохранять физическую целостность, устойчивость функционирования при реализации различных угроз техногенного характера и, в частности, – угроз возникновения пожара.

Постановка задачи. Новые угрозы безопасности объектов критической инфраструктуры и формы их реализации

Современное общество все больше зависит от множества взаимосвязанных информационных сетей и систем, обеспечивающих эффективное функционирование объектов критически важной инфраструктуры в различных областях жизнедеятельности

государства. Если эти системы будут скомпрометированы, последствия для безопасности государства могут быть серьезными. В условиях глобальной цифровизации возрастающая сложность и важность критически важной инфраструктуры государства обуславливает ее уязвимость и подверженность различным, все более сложным и множественным, кибератакам. В профессиональной среде специалистов по информационной безопасности используется термин «ландшафт угроз» (threat landscape), под которым понимается вся совокупность существующих киберугроз, способных создавать риски информационной безопасности для организации. Актуальной становится задача анализа ландшафта угроз, решение которой обуславливает возможность выявления потенциальных проблем в обеспечении требуемого уровня информационной безопасности того или иного объекта защиты и реализации проактивного подхода к защите информации путем принятия превентивных мер.

Общее количество инцидентов (успешных кибератак) в 2022 г. увеличилось на 20,8 %, что связывается с возросшей активностью и напряжением в киберпространстве (рис. 1) [7].

Примерами последствий реализации такого рода атак для объектов критически важной инфраструктуры могут быть следующие: транспортные сети – кибератака может нарушить работу этих систем (например: несанкционированное, деструктивное манипулирование системами светофоров), что приведет к значительным задержкам, несчастным случаям, а в некоторых случаях – и к гибели людей; энергетические системы, такие как электросеть, успешная кибератака на них может привести к массовым отключениям электроэнергии, затронув все – от больничных служб, промышленных и социальных объектов до водоочистных сооружений; коммуникационные сети – кибератака на эти системы может привести к нарушению экстренной связи и срыву усилий по реагированию на стихийные бедствия, невозможности передачи команд управления, недоступности или искажению, уничтожению или утечки передаваемой информации и др. [8–11].

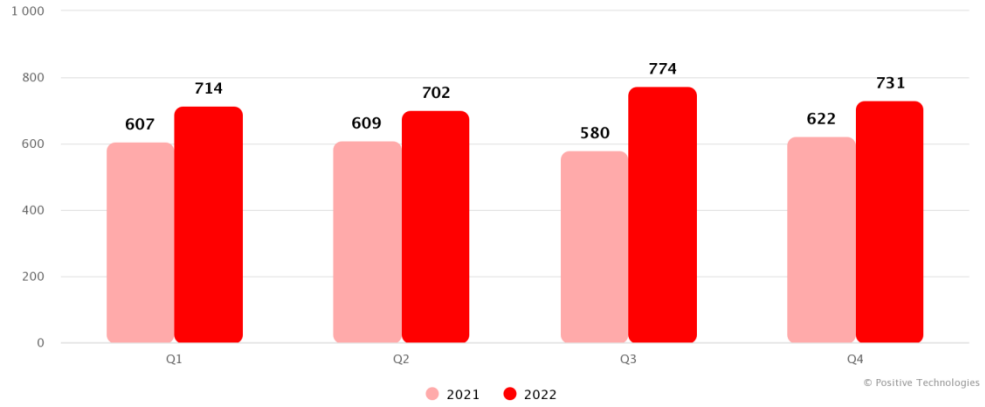

Рис. 1. **Количество инцидентов (успешных кибератак) в 2021 и 2022 гг. (по кварталам) [7]**

В качестве наиболее распространенных видов кибератак можно назвать: вредоносное программное обеспечение (ВПО, malware), предназначенное для повреждения, нарушения работы или получения несанкционированного доступа к компьютерной системе; фишинг (fishing – рыбалка, выуживание), кибератака, использующая электронную почту либо другие технологии общения (телефон – vishing, SMS – smishing, и др.), в ходе которой осуществляется замаскированное психологическое воздействие на человека с применением технологий социальной инженерии (social engineering); атаки, затрудняющие доступ легитимных пользователей к информационным ресурсам (отказ в обслуживании: Denial of Service – DoS или Distributed DoS – DDoS: распределённый DoS), происходят, когда несколько систем перегружают полосу пропускания или ресурсы целевой информационной

системы, вызывая ее сбой и прекращение предоставления услуг; целенаправленные (таргетированные) атаки (Advanced Persistent Threat – APT: «развитая устойчивая угроза»), особенность которых заключается в том, что они направлены на конкретную компанию или государственную организацию, они, как правило, имеют длительный подготовительный период, тщательно разработанный план и реализуют все этапы так называемые «цепочки кибер-убийства» (Cyber Kill Chain) – от идентификации атакуемой цели, вторжения, закрепления, уничтожения следов присутствия и до деструктивной реализации полученных привилегий; программы-вымогатели (ransomware) – разновидность вредоносных программ, которые в 2022 г. использовались в каждой второй (51 %) успешной атаке на организации с использованием ВПО [7], в ходе которых блокируется доступ к системе или шифруются данные с последующим требованием от своих жертв выкупа в обмен на предоставление доступа к данным.

Современный турбулентный (бурный, хаотичный, неустойчивый) мир существенным образом изменяет взгляды и подходы к обеспечению безопасности. Попытки адекватно описать ключевые особенности текущего состояния цивилизации привели к переходу от концепций в 1985 г. VUCA-мира (***V**olatility* – изменчивость, ***U**ncertainty* – неопределенность, ***C**omplexity* – сложность, ***A**mbiguity* – двусмысленность), до в 2016 г. – BANI-мира (***B**rittle* – хрупкий, ***A**nxious* – тревожный, ***N**onlinear* – нелинейный, ***I**ncomprehensible* – непостижимый) и в 2022 г. – SHIVA-мира (***S**plit* – расщепленный, ***H**orrible* – ужасный, ***I**nconceivable* – невообразимый, ***V**icious* – беспощадный, ***A**rising* – возрождающийся) [12].

Результаты и обсуждение. Эволюция роли и места информационной и пожарной безопасности в системе национальной безопасности

Решение задач обеспечения безопасности в быстро меняющемся мире требует высокой оперативности принятия решений, что возможно только при глобальной цифровой трансформации. Информационная сфера, становясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. В формирующемся цифровом мире важное значение имеет понимание взаимосвязей между информационной безопасностью и другими видами (аспектами) национальной безопасности.

Обязанность государства по обеспечению национальной безопасности заложена в основных положениях Конституции Российской Федерации. Конкретизирует национальную безопасность (сочетающую в своем содержании различные виды безопасности, в том числе военную, экономическую, информационную и др.) целый ряд нормативно-правовых актов, посвященных регулированию ее обеспечения.

Достижение требуемого уровня защищенности национальных интересов предполагает создание целостной, структурированной по соответствующим видам, в зависимости от характера угроз и сферы жизнедеятельности государства, системы национальной безопасности Российской Федерации. Такая система представляет собой сложную систему, которая, в свою очередь, включает в себя систему обеспечения национальной безопасности, которую можно рассматривать в качестве управляющего компонента системы национальной безопасности, и систему видов национальной безопасности [13].

Состоявшаяся информатизация всех сфер жизнедеятельности государства, наблюдаемый в настоящее время процесс цифровизации позволяют утверждать, что национальная безопасность Российской Федерации начинает существенным образом зависеть от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать (рис. 2) [14].

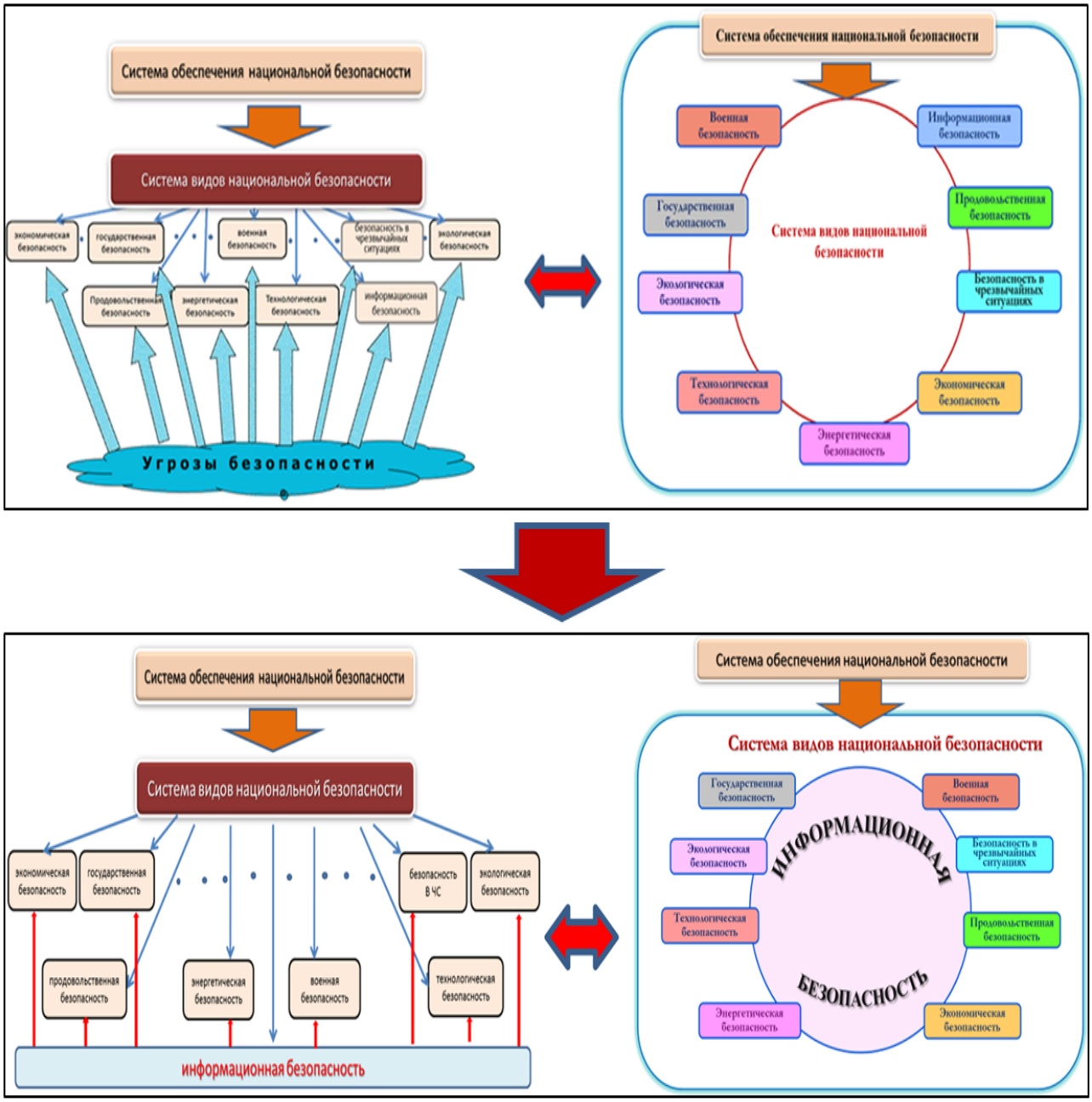

Рис. 2. **Эволюция роли и места информационной безопасности в системе национальной безопасности**

Растущая изощренность, сложность кибератак в сочетании с их взаимосвязанностью и трансграничностью создают реальную возможность для широкомасштабных сбоев и катастроф объектов критической инфраструктуры и в первую очередь объектов критической информационной инфраструктуры (КИИ), что актуализирует проблему обеспечения защиты этих объектов от киберугроз.

Указанные обстоятельства предопределяют необходимость регламентации и урегулирования многих проблем, связанных с информационным обменом и генерированием (производством) новых информационных ресурсов. При этом надо рассматривать два вопроса: вопрос защиты информации, которая становится одновременно более значимой, ценной и более уязвимой, с одной стороны, а с другой стороны – вопрос защиты от ложной или деструктивной информации, внедряемой в информационную систему в рамках соответствующих кибератак.

Система официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере изложена в Доктрине информационной безопасности Российской Федерации, где подчеркивается, что единым объектом защиты являются сбалансированные интересы личности, общества и государства в информационной безопасности. Их предполагается защищать в различных областях (оборонная; внутренняя; экономическая; научная и образовательная; духовная и др.), где происходит информационное взаимодействие этих субъектов с использованием информационных систем и технологий, от различного рода угроз, целью которых является оказание негативного воздействия на эти интересы путем осуществления кибератак.

В настоящее время для защиты критически важной инфраструктуры от кибератак используется широкий спектр мер и технологий, представляющих собою иерархический комплекс мер (рубежей) защиты. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» включает в состав этого комплекса совокупность, в последовательности их реализации, правовых, организационных и технических мер, последние из которых, в свою очередь, включают в себя широкий спектр средств защиты информации (рис. 3).

Рис. 3. **Система мер (рубежей) защиты информации**

В числе важнейших методов, средств и технологий, реализуемых в рамках этой системы мер защиты информации, можно отметить необходимость разработки политик и процедур безопасности, включающих многофакторную аутентификацию, шифрование и аудит, контроль и управление информационной безопасностью. Внедрение передовых технологий кибербезопасности может помочь быстрее обнаруживать уязвимости, выявлять и реагировать на кибератаки. Такие технологии и средства могут включать:

– системы обнаружения и предотвращения вторжений (IDS/IPS – Intrusion Detection System/Intrusion Prevention System), представляющие собою интеллектуальные системы, которые используют сложные алгоритмы и методы поведенческого анализа для непрерывного мониторинга сетевого трафика, оперативного выявления любых подозрительных действий или попыток несанкционированного доступа и блокирования их;

– системы, позволяющие оперативно, в режиме реального времени обобщать и анализировать многочисленные данные о событиях безопасности, выявлять потенциальные инциденты безопасности, обеспечивая возможность последующего эффективного управления реагированием на инциденты (системы управления информацией о безопасности и событиями (Security information management – SIEM);

– межсетевые экраны нового поколения (Next-Generation Firewall, NGFW), которые используют расширенные функции, такие как осведомленность о приложениях, глубокая проверка пакетов и пользовательские политики, для защиты сети от возникающих угроз;

– системы предотвращения утечки данных (Data Leak Prevention – DLP), позволяющие эффективно выявлять внутренние угрозы, осуществлять контроль легитимности пользовательских действий путем регистрации так называемых «индикаторов компрометации» (IoC-Indicator of Compromise) – информационных фрагментов, характеризующих вероятную деструктивную активность;

– Sandbox – технология песочницы, профилактирование поступающего потока информации путем запуска подозрительного ПО в специально подготовленную виртуальную информационную среду, изолированную от остальной инфраструктуры, где отслеживается поведение потенциально небезопасного ПО, что позволяет проактивно выявлять сложные целевые атаки, атаки использующие неизвестные для разработчика и пользователя уязвимости – так называемые уязвимости нулевого дня (Zero-day или 0-Day).

Непрерывно возрастает роль и расширяется сфера применения технологий ИИ и машинного обучения в кибербезопасности. Используя возможности ИИ (AI) и машинного обучения (machine learning – ML), область кибербезопасности получает значительные преимущества. ИИ и машинное обучение могут анализировать огромные объемы данных для выявления закономерностей и обнаружения аномалий, которые могут указывать на кибератаку. Эти технологии также могут автоматизировать реагирование на угрозы, повышая скорость и эффективность реагирования. Благодаря этой интеграции средства защиты кибербезопасности укрепляются и получают возможность проактивно защищать критически важные системы и сети от вредоносных вторжений, обеспечивая требуемый уровень зрелости процессов обеспечения информационной безопасности.

При этом надо понимать, что технологические решения, используемые для обеспечения информационной безопасности, могут быть эффективными только при достижении определенного уровня компьютерной грамотности, соблюдении правил «цифровой гигиены» сотрудников, обеспечении требуемой степени осведомленности по вопросам информационной безопасности. Регулярные программы обучения и повышения осведомленности могут гарантировать, что все сотрудники понимают свою роль в защите критически важной инфраструктуры – от распознавания потенциальных угроз до соблюдения процедур безопасности. Эффективным технологическим средством решения указанной задачи является применение «киберполигона» как сложной информационно-телекоммуникационной системы нового класса, предназначенной для обучения и отработки практических навыков специалистов в области информационной безопасности, а также для тестирования объектов информационной инфраструктуры путем моделирования компьютерных атак и отработки реакций на них [15–17].

Анализ показывает, что при реализации интересов различных субъектов безопасности выявляются общие материальные объекты, подлежащие защите. К ним относятся: помещения, объекты инфраструктуры, средства информатизации и, конечно, люди. Это значит, что все усилия по обеспечению информационной безопасности, других видов безопасности могут быть нивелированы, если не будет обеспечена физическая целостность этих материальных объектов защиты, их устойчивость к воздействию различных опасных факторов, в первую очередь перманентно присутствующих во все времена и на всех объектах, опасных факторов пожара.

Пожары являются существенной угрозой для защищаемых объектов, представляющие собой высоко опасные общественные явления, замедляющие социально-экономическое развитие страны, и могут причинить вред здоровью, лишить жизни граждан. Обеспечение пожарной безопасности является одной из важнейших функций государства. Ежегодные ущербы, вызванные пожарами, позволяют рассматривать противодействие им как одну из главных задач государства в сфере обеспечения национальной безопасности.

Так сложилось, что пожары в России во все времена представляли собою достаточно серьезную угрозу для всех без исключения объектов, зачастую проявлялись как национальное бедствие, напрямую связанное с утратой жизни и здоровья людей, уничтожением материальных ценностей в значительных размерах. Тенденция последних лет (2021–2022 гг.) подтверждает прирост количества пожаров на поднадзорных объектах (табл.) [18].

Таблица

Количества пожаров на поднадзорных объектах (2021–2022 гг.) [18]

Поднадзорные объекты	2021	2022	Прирост, %
	Кол-во пожаров, ед		
Здания производственного назначения	2 070	2 405	16,2
Складские здания, сооружения	671	760	13,3
Сельскохозяйственные здания	592	621	4,9
Здания, сооружения и помещения предприятий торговли	2 144	2 329	8,6
Здания, помещения учебно-воспитательного назначения	283	324	14,5
Здания, помещения здравоохранения и социального обслуживания населения	266	293	10,2
Здания, помещения сервисного обслуживания населения	970	1 257	29,6
Административные здания	555	1 013	82,5
Здания, сооружения и помещения для культурно-досуговой деятельности населения и религ. обрядов	208	241	15,9
Здания и помещения для временного пребывания (проживания) людей	273	328	20,1
Другие объекты пожара	1 264	1 505	19,1
Жилой сектор	7 043	8 372	18,9
Россия	**16 339**	**19 448**	**19,0**

Несмотря на то, что угроза пожаров, учитывая географические масштабы, природное разнообразие, ресурсоемкость, интенсивное технологическое развитие, является одной из самых объективных, широко распространенных угроз безопасности в Российской Федерации, в Стратегии национальной безопасности (Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации») пожарная безопасность как одна из важнейших составляющих техносферной безопасности никак не обозначена. Принятый 21 декабря 1994 г. Федеральный закон № 69-ФЗ «О пожарной безопасности» определяет пожарную безопасность как состояние защищенности личности, имущества, общества и государства от пожаров, что в очередной раз позволяет выявить общность объектов защиты для всех видов национальной безопасности. Появившийся позднее Федеральный закон от 22 июля 2008 г. № 123-ФЗ «Технический регламент о требованиях пожарной безопасности» определил единые трактовки основных понятий в области пожарной безопасности («опасные факторы пожара», «пожарная безопасность объекта защиты», «пожарный риск» и др.), представил показатели и дал классификацию технологических сред по их пожаро- и взрывоопасности, определил классификацию пожаров и опасных факторов

пожара, что позволило обозначить области применения средств пожаротушения, определить состав привлекаемых для тушения пожаров сил и средств, обосновать необходимые меры пожарной безопасности для защиты людей и имущества и др.

Указанные документы позволяют в значительной мере упорядочить и регламентировать права и обязанности организаций и должностных лиц по обеспечению пожарной безопасности в различных областях жизнедеятельности государства, создают основу нормативно-правовой базы пожарной безопасности в стране. Динамика развития нормативно-правовой базы, ее адаптация к изменяющимся условиям, технологиям и средствам решения задач обеспечения пожарной безопасности подтверждаются введением в действие с 1 сентября 2023 г. документа: «Методика определения расчетных величин пожарного риска в зданиях, сооружениях и пожарных отсеках различных классов функциональной пожарной опасности», утвержденного приказом МЧС России от 14 ноября 2022 г. № 1140.

В настоящее время государство осуществляет постоянный пожарный надзор за критически важной для национальной безопасности инфраструктурой (оборонные предприятия, крупные железнодорожные узлы, атомные электростанции, гидротехнические сооружения, морские порты, объекты КИИ и др.), поскольку ее объекты постоянно находятся под угрозой террористического характера. В условиях сегодняшнего дня, во время проведения специальной военной операции, резкое увеличение производственных мощностей повышает риски возникновения возгораний, и в этой связи пожары и ЧС на объектах критической инфраструктуры могут нанести существенный урон обороноспособности России [19].

Таким образом, пожарную безопасность можно вполне закономерно и обоснованно рассматривать как структурный элемент (вид) национальной безопасности [20, 21]. А учитывая подверженность угрозам возникновения пожаров практически всех сфер жизнедеятельности государства, пожарную безопасность следует позиционировать как системообразующий элемент, наряду с информационной безопасностью, в отношении которой пожарную безопасность можно рассматривать как своеобразную физическую платформу, от качества обеспечения которой зависит возможность реализации всех других видов национальной безопасности [22] (рис. 4).

Важным фактором трансформации технологий обеспечения пожарной безопасности является их интеграция в процессе повышения уровня автоматизации, цифровизации, сетевой организации систем противопожарной защиты на базе новых информационных технологий.

Рис. 4. **Роль и место информационной и пожарной безопасности в системе национальной безопасности**

По сути, речь может идти о внедрении интеллектуальных автоматизированных систем противопожарной защиты на основе технологии интернета вещей (IoT). Сетевая интеграция широко используемых в настоящее время современных систем автоматической противопожарной защиты, рассматриваемых как функциональная разновидность информационных систем, с другими системами обеспечения безопасности объекта защиты позволит получить все преимущества новых информационных технологий (оперативность, точность, адаптивность и др.). Кроме того, внедрение сетевых структур на базе технологии IoT, как правило, позволяет получить и экономический выигрыш путем применения технологии Power over Ethernet (PoE), позволяющей передавать электроэнергию и данные по одной линии за счет оптимизации эксплуатационных расходов на основе динамического, удаленного мониторинга состояния системы.

При этом как бы ни казалась пожарная безопасность областью, далекой от кибербезопасности, неизбежно встает вопрос о защите информационных ресурсов (информация обстановки, командная информация, пароли, программное обеспечение и т.п.) сетевых структур систем пожарной автоматики, поскольку у потенциального злоумышленника появляется возможность деструктивного воздействия на эти структуры (искажение или уничтожение информации, запуск или отключение датчиков, устройств сигнализации, элементов системы оповещения и управления эвакуацией людей и т.п.) и целенаправленного использования систем пожарной автоматики в своих вредительских интересах.

Заключение

Проведенный анализ эволюции роли и места информационной и пожарной безопасности в обеспечении национальной безопасности позволяет сделать вывод о том, что в отличие от других видов безопасности, выделяемых в структуре системы национальной безопасности, информационная и пожарная безопасность являются платформенными, системообразующими видами, имеющими в каждом из других видов безопасности свой собственный объект защиты, защищенность которого от угроз пожарной и информационной безопасности позволяет решать задачи обеспечения безопасности конкретного вида и национальной безопасности в целом.

При этом информационная безопасность позволяет интегрировать усилия по обеспечению различных видов национальной безопасности в единый комплекс, а пожарная безопасность призвана обеспечить живучесть материальных ресурсов объектов защиты. Тем самым обосновывается возрастающая роль информационной и пожарной безопасности, функциональность которых определяет эффективность, а в ряде случаев и возможность обеспечения других видов национальной безопасности.

Авторы отдают себе отчет в том, что предложенные трактовки тех или иных понятий, расставленные акценты и приоритеты, хотя и объективно отражают реалии и тенденции сегодняшнего дня, во многом определяются областью их научных интересов и профессиональной деятельности. Вместе с тем системность рассмотрения различных аспектов информационной и пожарной безопасности в обеспечении национальной безопасности позволяет подчеркнуть практическую применимость и возможность адаптации предложенных подходов в других предметных сферах деятельности.

Список источников

1. Лапидус Л.В. Эволюция цифровой экономики // Ломоносовские чтения – 2018. Секция экономических наук. Цифровая экономика: человек, технологии, институты: сб. тезисов выступлений. М.: Экономический факультет МГУ им. М.В. Ломоносова, 2018. С. 153–158.

2. Клаус Шваб, Николас Дэвис. М.: Эксмо, 2018. 320 с.

3. Kateryna Bondar. Challenges and Opportunities of Industry 4.0 – Spanish Experience // International Journal of Innovation, Management and Technology. 2018. № 5. С. 202–208.

4. Шестакова И.Г. Новая темпоральность цифровой цивилизации: будущее уже наступило // Научно-технические ведомости СПбГПУ. Гуманитарные и общественные науки. 2019. Т. 10. № 2. С. 20–29. DOI: 10.18721/JHSS.10202.

5. Дубровин Е.Р., Дубровин И.Р. Современная система национальной безопасности Российской Федерации. URL: https://topwar.ru/159640-sovremennaja-sistema-nacionalnoj-bezopasnosti-rossijskoj-federacii-i-ee.html (дата обращения: 18.06.2024).

6. Theoretical and methodological substantiation of the structure of the state national security system / M.Yu. Zelenkov [et al.]. LAPLAGE EM REVISTA 2021. № 7 (3B). P. 421–437. DOI: 10.24115/S2446-6220202173B1569p.421-437.

7. Актуальные киберугрозы: итоги 2022 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (дата обращения 18.06.2024).

8. Синещук Ю.И. Киберпространство и кибербезопасность: системологический анализ базовых понятий // Региональная информатика (РИ–2018): материалы XVI Междунар. конф. СПб., 2018. С. 168–170.

9. Chobanyan V.A., Shahalov I.Yu. Analysis and synthesis of the requirements for safety systems of objects of critical information infrastructure // Issues of cybersecurity. 2013. № 1 (1). P. 7–27.

10. Peter W. Singer and Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2014.

11. Синещук Ю.И. Информационная безопасность предприятия в условиях цифровой трансформации // Научные труды Северо-Западного института управления РАНХиГС. 2022. Т. 13. № 2 (54). С. 125–131.

12. Кирикова А., Арбузова А. VUCA, BANI и SHIVA: буквы, объясняющие мир. URL: https://trends.rbc.ru/trends/futurology/62866fde9a794701a4c38ae4 (дата обращения 18.06.2024).

13. Аспекты техносферной безопасности в концепции системы национальной безопасности / Ю.И. Синещук [и др.] // Проблемы управления рисками в техносфере. 2024. № 2 (70). С. 8–19. DOI: 10.61260/1998-8990-2024-2-8-19.

14. Синещук Ю.И. Информационная безопасность в системе национальной безопасности // Региональная информатика и информационная безопасность: сб. статей С.-Петерб. Междунар. и межрег. конф. 2018. С. 167–170.

15. Синещук М.Ю., Шестаков А.В., Гавкалюк Б.В. Инфологическая модель и критерии качества решений по построению ведомственных организационно-технических систем класса «киберполигон» // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2023. № 1. С. 121–137.

16. Miloslavskaya N., Tolstoy A. Cyber polygon site project in the framework of the MEPhI network security intelligence center // Brain-Inspired Cognitive Architectures for Artificial Intelligence: BICA* AI 2020: Proceedings of the 11th Annual Meeting of the BICA Society 11. Springer International Publishing. 2021. P. 295–308.

17. Андреев А.С., Иванцов А.М. Опыт применения комплексов (полигонов) в области обеспечения информационной безопасности // Информационное противодействие угрозам терроризма. 2015. Т. 1. № 25. С. 15–17.

18. Анализ обстановки с пожарами и их последствиями на территории Российской Федерации за 12 месяцев 2022 г. URL: https://xn--d1afzn.xn--p1ai/files/306/analiz-dnpr-2022.pdf (дата обращения: 12.06.2024).

19. Солдатов Р., Перевощикова М. Стена от огня: в РФ усилят пожарный надзор за критической инфраструктурой. URL: https://iz.ru/1531907/roman-soldatov-mariia-perevoshchikova/stena-ot-ognia-v-rf-usiliat-pozharnyi-nadzor-za-kriticheskoi-infrastrukturoi (дата обращения: 12.06.2024).

20. Зарецкий А.Д. Пожарная безопасность как составная часть стратегии национальной безопасности России // Национальные интересы: приоритеты и безопасность. 2010. № 1 (58). С. 74–77.

21. Капранова Ю.В., Овсепян Г.М. Пожарная безопасность в системе национальной безопасности: отдельные аспекты законодательного регулирования // Юрисконсульт в строительстве. 2021. № 12. С. 38–42.

22. Синещук Ю.И., Терёхин С.Н., Шидловский Г.Л. Правовое обоснование роли и места пожарной безопасности в обеспечении информационной безопасности // Информационная безопасность регионов России (ИБРР-2023). XIII С.-Петерб. межрег. конф.: материалы конф. СПб.: СПОИСУ, 2023. С. 50–51.

References

1. Lapidus L.V. Evolyuciya cifrovoj ekonomiki // Lomonosovskie chteniya – 2018. Sekciya ekonomicheskih nauk. Cifrovaya ekonomika: chelovek, tekhnologii, instituty: sb. tezisov vystuplenij. M.: Ekonomicheskij fakul'tet MGU im. M.V. Lomonosova, 2018. S. 153–158.

2. Klaus Shvab, Nikolas Devis. M.: Eksmo, 2018. 320 s.

3. Kateryna Bondar. Challenges and Opportunities of Industry 4.0 – Spanish Experience // International Journal of Innovation, Management and Technology. 2018. № 5. S. 202–208.

4. Shestakova I.G. Novaya temporal'nost' cifrovoj civilizacii: budushchee uzhe nastupilo // Nauchno-tekhnicheskie vedomosti SPbGPU. Gumanitarnye i obshchestvennye nauki. 2019. T. 10. № 2. S. 20–29. DOI: 10.18721/JHSS.10202.

5. Dubrovin E.R., Dubrovin I.R. Sovremennaya sistema nacional'noj bezopasnosti Rossijskoj Federacii. URL: https://topwar.ru/159640-sovremennaja-sistema-nacionalnoj-bezopasnosti-rossijskoj-federacii-i-ee.html (data obrashcheniya: 18.06.2024).

6. Theoretical and methodological substantiation of the structure of the state national security system / M.Yu. Zelenkov [et al.]. LAPLAGE EM REVISTA 2021. № 7 (3B). P. 421–437. DOI: 10.24115/S2446-6220202173B1569p.421-437.

7. Aktual'nye kiberugrozy: itogi 2022 goda. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (data obrashcheniya: 18.06.2024).

8. Sineshchuk Yu.I. Kiberprostranstvo i kiberbezopasnost': sistemologicheskij analiz bazovyh ponyatij // Regional'naya informatika (RI–2018): materialy XVI Mezhdunar. konf. SPb., 2018. S. 168–170.

9. Chobanyan V.A., Shahalov I.Yu. Analysis and synthesis of the requirements for safety systems of objects of critical information infrastructure // Issues of cybersecurity. 2013. № 1 (1). P. 7–27.

10. Peter W. Singer and Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2014.

11. Sineshchuk Yu.I. Informacionnaya bezopasnost' predpriyatiya v usloviyah cifrovoj transformacii // Nauchnye trudy Severo-Zapadnogo instituta upravleniya RANHiGS. 2022. T. 13. № 2 (54). S. 125–131.

12. Kirikova A., Arbuzova A. VUCA, BANI i SHIVA: bukvy, ob"yasnyayushchie mir. URL: https://trends.rbc.ru/trends/futurology/62866fde9a794701a4c38ae4 (data obrashcheniya 18.06.2024).

13. Aspekty tekhnosfernoj bezopasnosti v koncepcii sistemy nacional'noj bezopasnosti / Yu.I. Sineshchuk [i dr.] // Problemy upravleniya riskami v tekhnosfere. 2024. № 2 (70). S. 8–19. DOI: 10.61260/1998-8990-2024-2-8-19.

14. Sineshchuk Yu.I. Informacionnaya bezopasnost' v sisteme nacional'noj bezopasnosti // Regional'naya informatika i informacionnaya bezopasnost': sb. Statej S.-Peterb. Mezhdunar. i mezhreg. konf. 2018. S. 167–170.

15. Sineshchuk M.Yu., Shestakov A.V., Gavkalyuk B.V. Infologicheskaya model' i kriterii kachestva reshenij po postroeniyu vedomstvennyh organizacionno-tekhnicheskih sistem klassa «kiberpoligon» // Nauch.-analit. zhurn. «Vestnik S.-Peterb. un-ta GPS MCHS Rossii». 2023. № 1. S. 121–137.

16. Miloslavskaya N., Tolstoy A. Cyber polygon site project in the framework of the MEPhI network security intelligence center // Brain-Inspired Cognitive Architectures for Artificial Intelligence: BICA* AI 2020: Proceedings of the 11th Annual Meeting of the BICA Society 11. Springer International Publishing. 2021. P. 295–308.

17. Andreev A.S., Ivancov A.M. Opyt primeneniya kompleksov (poligonov) v oblasti obespecheniya informacionnoj bezopasnosti // Informacionnoe protivodejstvie ugrozam terrorizma. 2015. T. 1. № 25. S. 15–17.

18. Analiz obstanovki s pozharami i ih posledstviyami na territorii Rossijskoj Federacii za 12 mesyacev 2022 g. URL: https://xn--d1afzn.xn--p1ai/files/306/analiz-dnpr-2022.pdf (data obrashcheniya: 12.06.2024).

19. Soldatov R., Perevoshchikova M. Stena ot ognya: v RF usilyat pozharnyj nadzor za kriticheskoj infrastrukturoj. URL: https://iz.ru/1531907/roman-soldatov-mariia-perevoshchikova/stena-ot-ognia-v-rf-usiliat-pozharnyi-nadzor-za-kriticheskoi-infrastrukturoi (data obrashcheniya: 12.06.2024).

20. Zareckij A.D. Pozharnaya bezopasnost' kak sostavnaya chast' strategii nacional'noj bezopasnosti Rossii // Nacional'nye interesy: prioritety i bezopasnost'. 2010. № 1 (58). S. 74–77.

21. Kapranova Yu.V., Ovsepyan G.M. Pozharnaya bezopasnost' v sisteme nacional'noj bezopasnosti: otdel'nye aspekty zakonodatel'nogo regulirovaniya // Yuriskonsul't v stroitel'stve. 2021. № 12. S. 38–42.

22. Sineshchuk Yu.I., Teryohin S.N., Shidlovskij G.L. Pravovoe obosnovanie roli i mesta pozharnoj bezopasnosti v obespechenii informacionnoj bezopasnosti // Informacionnaya bezopasnost' regionov Rossii (IBRR-2023). XIII S.-Peterb. mezhreg. konf.: materialy konf. SPb.: SPOISU, 2023. S. 50–51.

Информация о статье:
Статья поступила в редакцию: 20.07.2024; одобрена после рецензирования: 11.09.2024;
принята к публикации: 19.09.2024

The information about article:
The article was submitted to the editorial office: 20.07.2024; approved after review: 11.09.2024;
accepted for publication: 19.09.2024

Информация об авторах:
Синещук Юрий Иванович, профессор кафедры пожарной безопасности зданий и автоматизированных систем пожаротушения Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), доктор технических наук, профессор, заслуженный работник высшей школы Российской Федерации, e-mail: sinegal53@mail.ru, SPIN-код: 4663-4378
Смирнов Алексей Сергеевич, первый заместитель начальника Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), доктор технических наук, профессор, e-mail: sas@igps.ru, SPIN-код: 1677-1402
Терёхин Сергей Николаевич, профессор кафедры пожарной безопасности зданий и автоматизированных систем пожаротушения Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), доктор технических наук, доцент, e-mail: expert_terehin@igps.ru, SPIN-код: 9342-2440
Шидловский Григорий Леонидович, начальник кафедры пожарной безопасности зданий и автоматизированных систем пожаротушения Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), кандидат технических наук, доцент, e-mail: shidlovsky.g@igps.ru, SPIN-код: 4345-1531

Information about the authors:
Sineshchuk Yuriy I., professor of the department of fire safety of buildings and automated fire extinguishing systems of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), doctor of technical sciences, professor, honored worker of the higher school of the Russian Federation, e-mail: sinegal53@mail.ru, SPIN: 4663-4378
Smirnov Alexey S., first deputy head of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), doctor of technical sciences, professor, e-mail: sas@igps.ru, SPIN: 1677-1402
Terekhin Sergey N., professor of the department of fire safety of buildings and automated fire extinguishing systems of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), doctor of technical sciences, associate professor, e-mail: expert_terehin@igps.ru, SPIN: 9342-2440
Shidlovsky Grigoriy L., head of the department of fire safety of buildings and automated fire extinguishing systems of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), candidate of technical sciences, associate professor, e-mail: shidlovsky.g@igps.ru, SPIN: 4345-1531