БЕЗОПАСНОСТЬ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ / SAFETY IN EMERGENCY SITUATIONS

УДК 004; 519

СИСТЕМНЫЕ ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ГЛОБАЛЬНОЙ ЦИФРОВИЗАЦИИ

Синещук Юрий Иванович[1], Терёхин Сергей Николаевич[1], Шидловский Григорий Леонидович[1], Ожегов Эдуард Александрович[2]

[1]Санкт-Петербургский университет ГПС МЧС России, г. Санкт-Петербург, Россия
[2] Уральский институт ГПС МЧС России, г. Екатеринбург, Россия

АННОТАЦИЯ

Окружающая человека естественная природная среда достаточно быстро, по историческим мерках, эволюционировала от биосферы к ноосфере и приобрела конкретное материалистическое воплощение в техносфере. Отличительной особенностью современного уровня развития техносферы является широкое использование киберфизических и социотехнических информационных систем, функционирование которых предполагает формирование определенной информационной среды (пространства, сферы). Проявляющийся при этом симбиоз техники, природы и человека характеризуется применением разнообразных технологий, которые сопровождаются появлением новых угроз и опасностей, актуализирующих проблему осмысления понятия «безопасность».

Необходимость независимого, суверенного существования любой страны обуславливает особое внимание вопросам национальной безопасности. Обеспечение национальной безопасности, помимо очевидной задачи – отражения военной угрозы, включает в себя достаточно широкую совокупность других задач. Благополучие населения часто зависит от безопасной работы критически важных инфраструктурных систем: от транспортных сетей до систем энергоснабжения, телекоммуникационных систем и автоматизированных информационных систем управления. Такого рода системы настолько жизненно важны для страны, что их выведение из строя или разрушение оказало бы пагубное воздействие на национальную безопасность. 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, 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. При исследовании рассматриваемых вопросов в качестве методологической базы выбраны системный, историко-ретроспективный, кибернетический подходы. В предлагаемой концепции системы национальной безопасности, позволяющей интегрировать усилия по обеспечению различных видов национальной безопасности в единый комплекс, системообразующей ос-

новой в реалиях современного информационного мира позиционируется информационная безопасность, обосновывается ее значимость и возрастающая роль в обеспечении всей совокупности видов национальной безопасности.

Ключевые слова: безопасность, техносфера, информационная безопасность, система национальной безопасности

SYSTEMIC FEATURES OF ENSURING NATIONAL SECURITY IN THE CONTEXT OF GLOBAL DIGITALIZATION

Yury I. Sineshchuk[1], Sergey N. Terehin[1], Grigory L. Shidlovsky[1], Eduard A. Ozhegov [2]

[1] Saint-Petersburg university of State fire service of EMERCOM of Russia, St. Petersburg, Russian Federation
[2] Ural Institute of State Fire Service of EMERCOM of Russia, Yekaterinburg, Russian Federation

ABSTRACT

By historical standards, the natural environment surrounding humans has rapidly evolved from the biosphere to the noosphere and has become materialistically embodied in the technosphere. A distinctive feature of the modern level of technosphere development is the wide use of cyberphysical and socio-technical information systems, the functioning of which implies the formation of a certain information environment (space, sphere). The emerging symbiosis of technology, nature and man is characterised by the application of various technologies, which are accompanied by the emergence of new threats and dangers that actualise the problem of understanding the concept of 'security'.

The need for any country to exist independently places special emphasis on national security. National security, in addition to repelling military threats, includes a fairly wide range of other tasks. The well-being of the population depends on the safe operation of critical infrastructure systems such as transport networks, energy supply systems, telecommunications systems and automated information management systems.

These types of systems are so vital to a country that disabling or destroying them would have a fatal impact on national security.The observed integration of innovative in form and informational in content into the national security operations has resulted in significant advances, safer communities and more effective emergency response mechanisms. At the same time, the threats posed by the technologies of the information age required the specification of the concepts used in the field of security at the system level, clarification of the composition of the basic system-forming types of national security of the Russian Federation and the links between them. Systemic, historical-retrospective, cybernetic approaches have become the methodological basis for the study of issues. In the proposed concept of the national security system, which allows integrating the efforts to ensure various types of national security into a single complex, the system-forming basis in the realities of the modern information world is positioned information security, its importance and increasing role in ensuring the totality of types of national security is substantiated.

Keywords: security, technosphere, information security, national security system

Введение

Глобальные динамические перемены политического, технологического, биосферного характера, которые определяют интенсивность и приоритеты развития человечества на современном этапе, порождают и новые аспекты безопасности, меняют роль и значимость ее отдельных видов. XXI в. обострил проблемы безопасности, усложнил механизмы ее обеспечения, поставил вопрос о системной интеграции используемых средств, методов, технологий защиты от различных угроз.

В 1943 г. американский психолог Абрахам Маслоу предложил иерархию потребностей человека, в качестве которых он указал пять главных: физиологические, потребность в безопасности, социальные потребности, уважение или признание, самореализация [1].

В этой иерархии возникновение одной потребности обычно зависит от удовлетворения другой, более мощной. Потребность человека в безопасности занимает здесь важнейшее место, уступая только реализации жизненно необходимых основных физиологических желаний (еда, питье, кров, одежда, тепло, сон, секс), без которых человек вообще не может существовать. Предложенная теория в дальнейшем получила свою наглядную и наиболее известную графическую интерпретацию в виде пирамиды Маслоу (Maslow) [2] (рис. 1).

История человечества изобилует многочисленными катаклизмами: от войн, природных и техногенных катастроф до социальных и индивидуальных трагедий, которые в большей или меньшей степени затрагивают вопросы безопасности. По мере развития цивилизации перечень и формы проявления угроз безопасности постоянно расширяются, ущербы от их реализации становятся все более существенными. В работе Ковалева А. А. [3] на основе компаративистского подхода, историко-логического, конкретно-исторического, культурологического и политологического методов анализа исследуется историография безопасности, обосновывается тезис о том, что современный турбулентный (бурный, хаотичный, неустойчивый) мир существенным образом изменяет взгляды и подходы к обеспечению безопасности, требует системного мультидисциплинарного взгляда на эту проблему.

Рис. 1. Безопасность в иерархии потребностей человека (пирамида Маслоу)
Fig. 1. Security in the hierarchy of human needs (Maslow's pyramid)

Попытки адекватно описать ключевые особенности текущего состояния цивилизации привели к переходу от концепций в 1985 г. VUCA-мира (Volatility — изменчивость, Uncertainty — неопределенность, Complexity — сложность, Ambiguity – двусмысленность) к в 2016 г. BANI-миру (Brittle — хрупкий, Anxious — тревожный, Nonlinear – нелинейный, Incomprehensible — непостижимый) и в 2022 г. SHIVA-мира(Split — расщепленный, Horrible — ужасный, Inconceivable — невообразимый, Vicious — беспощадный, Arising — возрождающийся) [4].

Российский академик Владимир Иванович Вернадский еще в начале XX в. писал, что человек, вооруженный новыми знаниями, кардинальным образом воздействует на окружающую его среду, преобразуя ее в своих интересах, что позволяет говорить о формировании в рамках биосферы новой среды обитания — ноосферы [5]. Ноосфера («сфера разума») может быть охарактеризована как пространство, где проявляется синергетический эффект целенаправленного воздействия на природу со стороны человека (общества) на основе накопленных знаний и применяемых технологических средств. Ноосфера является высшей стадией развития биосферы, связанной с возникновением и становлением в ней цивилизованного общества, когда разумная деятельность человека становится главным фактором развития на Земле. По сути, ноосфера — это биосфера, разумно управляемая человеком [6].

Современный этап развития человечества характеризуется дальнейшим стиранием граней между физической, цифровой и биологической сферами. Подчеркивая технологичность, технократизм взаимодействия человека и природы, на смену достаточно философскому, теоретическому понятию «ноосфера» пришло понятие «техносфера», определяемое как часть биосферы, где современный человек в процессе жизнедеятельности меняет среду вокруг себя, используя различные технические средства, системы и технологии [7]. В целом это весь окружающий нас мир, который используется, изучается, трансформируется человеком в своих интересах, разрабатывая, строя и применяя все более сложные системы, что позволяет рассматривать техносферу как материализацию идей и знаний, формирующих ноосферу.

Отличительной особенностью, характеризующей уровень развития техносферы, является широкое использование киберфизических и социотехнических информационных систем. Киберфизическая система (cyber-physical system — CPS) представляет собою комплекс исполнительных элементов (физических устройств) и компьютерных компонентов, которые взаимодействуют друг с другом для обеспечения безопасного и эффективного управления заданным процессом. Примеры CPS включают промышленные системы управления, системы водоснабжения, робототехнические системы, интеллектуальные сети и т. д. Социотехническая информационная система в своей трактовке акцентирует внимание на важности социальной составляющей, ее доминирующей роли в инфраструктуре информационной системы. По сути, к числу социотехнических (организационно-технических) можно отнести любую информационную систему, в которой человек (оператор, руководитель) принимает решение для осуществления воздействия на объект управления. Результативность такого воздействия в конечном счете, определяется эффективностью технической (компьютерной) составляющей системы на всех этапах ее жизненного цикла, таких как проектирование, разработка, внедрение, эксплуатация. Доминирующей тенденцией сегодняшнего дня можно назвать функциональную интеграцию киберфизических и социотехнических систем в виде социоки-

берфизических систем, поскольку в этих системах происходит совмещение объектов различной природы, а по составу функций управления эти системы сравнялись с функциями управления человека-оператора или лица, принимающего решения [8–10].

Функционирование киберфизических и социотехнических информационных систем предполагает формирование определенной информационной сферы (среды, пространства). В Доктрине информационной безопасности Российской Федерации, утвержденной указом Президента РФ № 646 от 05.12.2016, под информационной сферой понимается «совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сет ”Интернет”, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений».

Тогда с определенной долей условности современное представление о среде обитания человека можно отразить в виде, представленном на рис. 2.

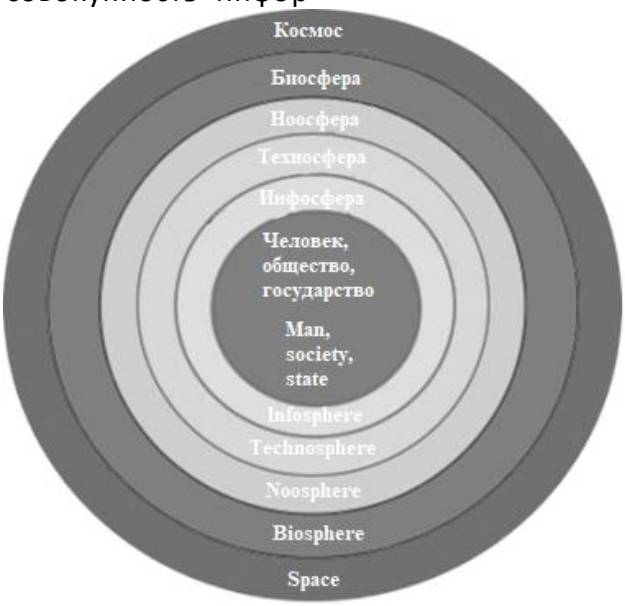

Рис. 2. Модель среды обитания человека
Fig. 2. Human habitat model

Таким образом, реалии современной цивилизации можно характеризовать как стадию киборгизации (симбиоза человека, техники и искусственного интеллекта), когда при осуществлении целенаправленных действий человек использует постоянно развивающиеся, сменяющие друг друга технологии, которые, в свою очередь, порождают и новый спектр угроз государству [11]. Эти обстоятельства требуют системной организации сил и средств, привлекаемых для противодействия этим угрозам, на единой технологической основе, позволяющей получить синергетический эффект решения задач обеспечения национальной безопасности.

Материалы и методы

В различных исследованиях по вопросам безопасности государства анализируются те или иные аспекты обеспечения национальной безопасности, предусматривающей независимость и суве-

ренность страны. Так, в частности, работа Пирумова В. С. [12] посвящена рассмотрению методологических принципов и методов исследования национальной безопасности, в качестве которых обосновывается методология системного анализа как совокупности методов, приемов и процедур исследования общественно-политических процессов как открытых развивающихся систем, указывается важность принципов историзма и междисциплинарного анализа. В работах Медведева М. В. [13], Поддубного А. О. [14] рассматриваются различные подходы к определению самого понятия «национальная безопасность» сквозь призму национальных интересов, с позиции изменяющегося законодательства в отечественном правоведении, один из вариантов трактовки этого понятия приводит в своей монографии [15] Joseph J. Romm Romm: «…безопасность заключается в наилучшем балансе всех инструментов… в скоординированном обращении с оружием, дипломатией, информацией и экономикой; и в правильном соотношении всех мер внешней и внутренней политики». Административно-правовое обеспечение национальной безопасности различных стран как одно из значимых инструментов сравнивается в диссертационном исследовании Кикоть-Глуходедова Т. В. [16]. Вместе с тем в рассмотренных работах авторы, как правило, не предлагают целостного обобщения рассматриваемых вопросов на системном уровне, зачастую замещая одни понятия другими (система национальной безопасности, система обеспечения национальной безопасности, виды национальной безопасности).

Обязанность государства по обеспечению национальной безопасности заложена в основных положениях Конституции РФ. 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, и в первую очередь это указ Президента РФ от 02.07. 2021. № 400 «О Стратегии национальной безопасности Российской Федерации» (далее – Стратегия).

Стратегия базируется на принципе приоритетности, позволяющем выявить наиболее значимые виды национальной безопасности, соотнесенные с соответствующими сферами жизнедеятельности государства [17]. Программно-целевой характер Стратегии предполагает возможность расширения спектра видов национальной безопасности, определения перечня специфичных угроз и организации противодействия им в других нормативно-правовых актах применительно к конкретной сфере жизнедеятельности государства (*Федеральный закон от 28.06.2014 N 172-ФЗ «О стратегическом планировании в Российской Федерации», Федеральный закон от 31.05.1996 № 61-ФЗ «Об обороне», Военная доктрина Российской Федерации (утв. Президентом РФ 25.12.2014 № Пр-2976), указ Президента Российской Федерации от 19.04.2017 № 176 «О Стратегии экологической безопасности Российской Федерации на период до 2025 года», указ Президента Российской Федерации от 13.05.2017 № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года», указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и др.*). (рис. 3).

Рис. 3. Нормативно-правовая основа обеспечения национальной безопасности РФ
Fig. 3. Normative basis for ensuring national security of the Russian Federation

Стратегия определяет понятие «**национальная безопасность**» как «состояние защищенности национальных интересов РФ от внешних и внутренних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета РФ, ее независимости и государственной целостности, социально-экономическое развитие страны».

С учетом долгосрочных тенденций государство формулирует национальные интересы на современном этапе развития, реализация которых осложняется наличием объективных и субъективных, внешних и внутренних угроз. Процесс обеспечения национальной безопасности предусматривает реализацию в различных сферах жизнедеятельности государства разнообразных мер, направленных на противодействие угрозам национальной безопасности, рассматриваемым как совокупность условий и факторов, создающих прямую или косвенную возможность причинения ущерба национальным интересам РФ. Специфика деятельности подразделений МЧС России предполагает в большей или меньшей мере их участие в нейтрализации проявлений разнообразных угроз национальной безопасности, в решении задач обеспечения техносферной безопасности, что позволяет рассматривать МЧС России в качестве субъекта обеспечения национальной безопасности.

Начало XXI в. охарактеризовалось повсеместным развитием цифровых продуктов и электронных услуг, что привело к изменению роли и относительной важности компонентов, связанных с информацией и угрозами кибернетического характера, реализация которых отличается интенсивностью развития (сложность, разнообразие атак) и возросшей опасностью последствий (ущербов). 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. Наиболее востребованные, интенсивно развивающиеся технологии сегодняшнего дня характеризуют качественное содержание 4-й промышленной революции, определяющей современный этап уровня развития человечества [18, 19]. Вместе с тем возрастает и зависимость эффективного

функционирования всех механизмов и структур государства от уровня информационной безопасности информационных систем и технологий. 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 [20, 21]. 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.

В условиях глобальной цифровизации возрастающая сложность и важность критически важной инфраструктуры государства обуславливает ее уязвимость и подверженность для различных, все более сложных и множественных кибератак [22–24]. Актуальной становится задача анализа «ландшафта угроз» (threat landscape), решение которой обуславливает возможность выявления потенциальных проблем в обеспечении требуемого уровня информационной безопасности 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. 4) [25].

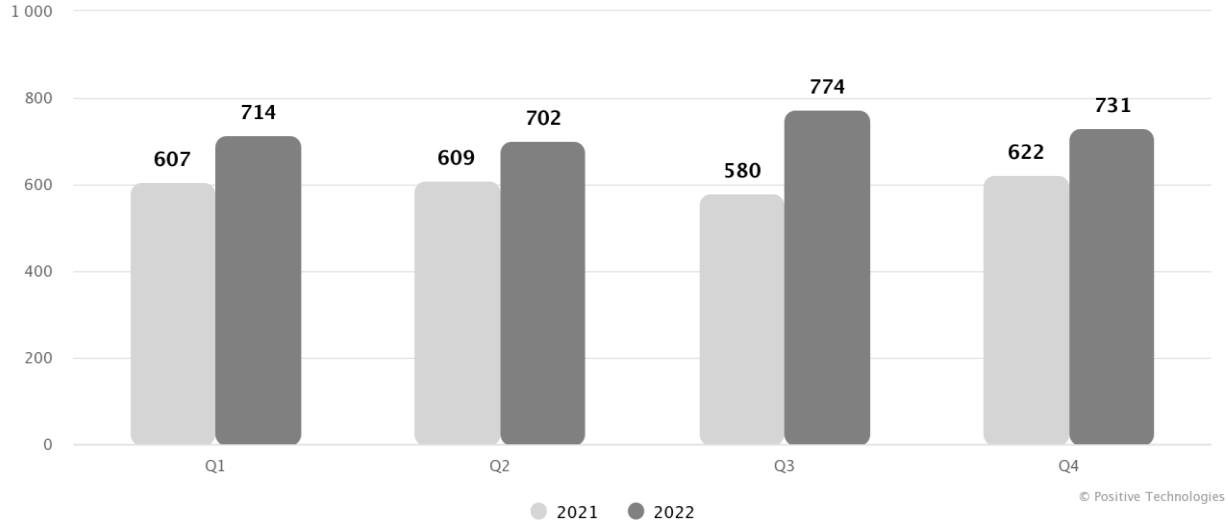

Рис. 4. Количество инцидентов (успешных кибератак) в 2021 и 2022 гг. (по кварталам)
Fig. 4. Number of incidents (successful cyber attacks) in 2021 and 2022 (by quarter)

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: распределенная (множественная) DoS–атака); целенаправленные (таргетированные) атаки (Advanced Persistent Threat — APT), особенность которых заключается в том, что они, как правило, направлены на конкретный объект критической инфраструктуры государства, имеют длительный подготовительный период, тщательно разработанный план и реализуют все этапы т. н. 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 [25], в ходе которых блокируется доступ к системе или шифруются данные с последующим требованием от своих жертв выкупа в обмен на предоставление доступа к данным.

Указанные обстоятельства предопределяют необходимость регламентации и урегулирования многих проблем, связанных с информационным обменом и генерированием (производством) новых информационных ресурсов, актуализируют проблему обеспечения защиты этих ресурсов от киберугроз. 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.

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 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» включает в состав этого комплекса совокупность в последовательности реализации правовых, организационных и технических мер, последние, в свою очередь, включают в себя широкий спектр средств защиты информации (рис. 5).

Рис. 5. Модель системы мер (рубежей) защиты информации
Fig. 5. Model of the information security measures (boundaries) system

В числе важнейших методов, средств и технологий, реализуемых в рамках этой системы мер защиты информации, особую актуальность приобретают те из них, которые позволяют обнаруживать уязвимости, выявлять и оперативно реагировать на кибератаки, эффективно реализовывать процесс управления информационной безопасностью. 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 мониторинга информационной безопасности, 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 and Event 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 т. н. 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, т. н. уязвимости нулевого дня (Zero-day, или 0-Day).

Непрерывно возрастает роль и расширяется сфера применения технологий искусственного интеллекта и машинного обучения в кибербезопасности. Используя возможности искусственного интеллекта (AI) и машинного обучения (machine learning — ML), область кибербезопасности получает значительные преимущества. Искусственный интеллект 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 интеграции этих технологий появляется возможность проактивной защиты от вредоносных вторжений.

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. Эффективным технологическим средством решения указанной задачи является применение «киберполи-

гона», предназначенного 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 [26–28].

Применение в рамках представленного анализа предметной области актуальных, в первую очередь информационных и соответствующих технологических аспектов обеспечения национальной безопасности: системного, историко-ретроспективного и кибернетического подходов позволяет сделать вывод о том, что в условиях формирования глобального информационного (кибер) пространства задача обеспечения информационной безопасности приобретает системный межведомственный характер и обуславливает необходимость позиционирования возрастающей роли и значимости этого вида национальной безопасности в современной концепции системы национальной безопасности.

Результаты и их обсуждение

Достижение требуемого уровня защищенности национальных интересов предполагает создание целостной, структурированной, в зависимости от характера угроз и сферы жизнедеятельности государства системы национальной безопасности РФ.

Как и в случае с термином «безопасность», понятие «система национальной безопасности» в действующих нормативно-правовых актах не определено. В ныне утратившем силу законе РФ от 05.03.1992 № 2446-I «О безопасности» говорилось, что «систему безопасности образуют органы законодательной, исполнительной и судебной властей, государственные, общественные и иные организации и объединения, граждане, принимающие участие в обеспечении безопасности в соответствии с законом, а также законодательство, регламентирующее отношения в сфере безопасности». На сайте МЧС России, в разделе термины (https://mchs.gov.ru/ministerstvo/o-ministerstve/terminy-mchs-rossii/term/1048), по сути, это же определение: «совокупность органов законодательной, исполнительной и судебной властей, государственных и иных организаций и объединений граждан, а также законодательных актов, регламентирующих отношения в сфере безопасности личности, общества и государства», трактуется уже как «система национальной безопасности». При этом в обоих случаях не упоминаются основные составляющие системы национальной безопасности — ее разнообразные виды. Приведенные определения в большей степени соответствуют сформулированному в Стратегии понятию «**система обеспечения национальной безопасности**» как «совокупность осуществляющих реализацию государственной политики в сфере обеспечения национальной безопасности органов публичной власти и находящихся в их распоряжении инструментов», которое можно рассматривать в качестве управляющего компонента современной **системы национальной безопасности** наряду с **системой видов национальной безопасности** (рис. 6).

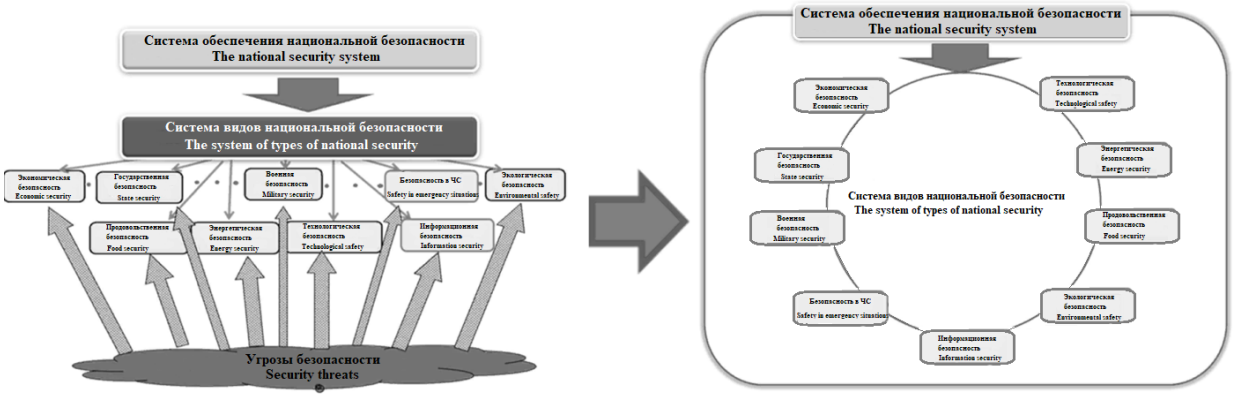

Рис. 6. Модель системы национальной безопасности РФ
Fig. 6. Model of the national security system of Russian Federation

Система национальной безопасности создается в государстве для стабильного, благополучного существования общества, она отражает приоритеты государства по обеспечению его жизнедеятельности в различных сферах и позволяет прогнозировать, своевременно выявлять и успешно противодействовать воздействиям различных внешних и внутренних угроз [29].

Комплексное решение всей совокупности задач, предусмотренных в рамках стратегических национальных приоритетов, реализуется на основе управляющих воздействий, вырабатываемых системой обеспечения национальной безопасности, имеющей в своем составе арсенал средств, которые позволяют выполнять мероприятия по защите национальных интересов РФ в различных сферах деятельности от различного рода угроз. Накопленный опыт решения различных задач, осуществляемых в интересах обеспечения национальной безопасности, показывает, что все виды системы национальной безопасности находятся между собой в тесных взаимосвязи и взаимодействии. В отдельные периоды развития общества приоритеты тех или иных видов безопасности могут меняться, что не исключает необходимости соблюдать баланс между всеми видами.

В качестве отличительных свойств (признаков), присущих системе национальной безопасности как сложной системе, можно назвать следующие:

— наличие совокупности взаимосвязанных и взаимодействующих в интересах достижения общей цели элементов (подсистем), определяющих целостность системы и формирующих ее качественное состояние;

— адаптивные возможности, определяющие способность сохранять свою устойчивость в условиях непрерывно и динамично варьируемых внутренних и внешних факторов;

— синергичность, определяющая однонаправленность действий элементов системы, интеграцию усилий в системе, которые приводят к возрастанию, умножению конечного результата функционирования системы.

При этом надо отметить, что современная Стратегия национальной безопасности РФ впервые включает информационную безопасность в перечень стратегических национальных приоритетов. Растущая изощренность, сложность кибератак в сочетании с их взаимосвязанностью и трансграничностью создано реальную возможность для широкомасштабных сбоев и катастроф объектов критической инфраструктуры, в первую очередь объектов критической информационной инфраструктуры (КИИ) [30].

В формирующемся цифровом мире важное значение имеет понимание взаи-

мосвязей между информационной безопасностью и другими видами (аспектами) национальной безопасности. Государство, осознавая роль и значение информационных средств и систем автоматизации процессов управления во всех сферах жизнедеятельности, последовательно уделяет серьезное внимание обеспечению их безопасности, принимая соответствующие нормативно-правовые акты: «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры РФ» (утверждены Президентом РФ 03.02.2012, № 803), Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (утверждена Президентом РФ 12.12.2014, № К 1274), указ Президента РФ «Доктрина информационной безопасности Российской Федерации» № 646 от 5.12.2016, Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», приказ ФСТЭК России от 09.08.2018 № 138 «О внесении изменений в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей, и для окружающей природной среды, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 14.03.2014 № 31, и в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25.12.2017 № 239», указ Президента РФ от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» и др.

Информационная безопасность, в отличие от других видов безопасности, выделяемых в структуре системы национальной безопасности, играет роль платформенного, системообразующего вида, обеспечение которого позволяет эффективно решать задачи во всех сферах жизнедеятельности государства, создает условия для решения задач обеспечения безопасности конкретного вида и национальной безопасности в целом (рис. 7) [31].

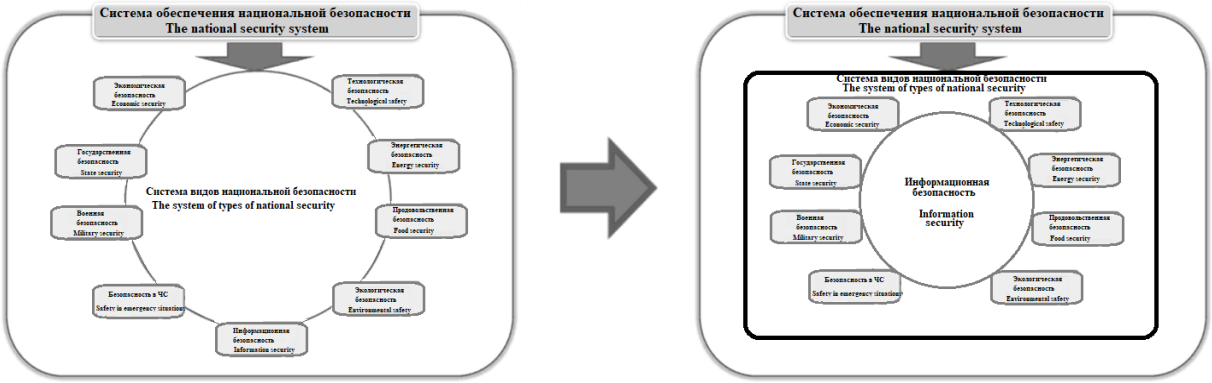

Рис. 7. Эволюция роли и места информационной безопасности в системе национальной безопасности

Fig. 7. The evolution of the role and place of information security in the national security system

Представленная концепция системы национальной безопасности позволяет увидеть интегративность и сбалансированность всех свойств этой системы, выделить ряд аспектов, определяющих возможность реализации функций управления:

— функционирование системы национальной безопасности должно рассматриваться во взаимодействии с внешней средой, что позволяет позиционировать ее как элемент (подсистему) в иерархической структуре метасистемы, в качестве которой в общем случае может выступать система международной безопасности;

— система национальной безопасности, которая включает в себя в качестве элементов (подсистем) другие сложные объекты более низкого уровня, в качестве которых выступают ее виды (экономическая, военная, технологическая, информационная, другие виды безопасности и их составляющие), в свою очередь, должна рассматриваться как сложная многоуровневая система;

— целостность системы национальной безопасности достигается целевой направленностью взаимосвязей составляющих ее видов безопасности, единством их функционирования, обеспечиваемым информационно-телекоммуникационными средствами и технологиями, а также процедурами обеспечения их информационной безопасности, при котором обеспечивается своевременное выявление, предотвращение, нейтрализация и минимизация ущербов от угроз различного характера за счет применения комплекса мер по защите интересов граждан, имущества, общества, государства [32].

Такого рода систему можно характеризовать как организационно-техническую управляющую (социокиберфизическую) систему, функциональным назначением которой является:

— определение жизненно-важных интересов государства в различных сферах жизнедеятельности, реализация которых обеспечивает его устойчивое прогрессивное развитие;

— анализ различных аспектов, оказывающих существенное влияние на возможность достижения требуемого уровня национальной безопасности РФ;

— прогноз, оценка риска, выявление угроз реализации интересов государства в различных сферах жизнедеятельности, анализ возможных последствий и ущербов, последующее упорядочивание угроз в соответствии с их катастрофичностью;

— осуществление комплекса мероприятий, направленных на предупреждение и нейтрализацию значимых угроз безопасности национальным интересам РФ путем применения соответствующих по форме проявления и уровню опасности угроз, методов, способов, средств защиты.

Указанные обстоятельства позволяют утверждать, что национальная безопасность РФ существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Заключение

Многочисленные войны, природные и социальные трагедии постоянно присутствуют в истории человечества. Эти обстоятельства всегда остро ставили проблему обеспечения безопасности личности, общественной и государственной безопасности, что предопределило необходимость обоснования системы национальной безопасности, адекватной динамично изменяющемуся спектру угроз безопасности в различных сферах жизнедеятельности государства. Прогнозирование и выявление угроз национальной безопасности, осуществление непрерывного мониторинга динамично изменяющихся событий в сфере безопасности,

обоснование методов и средств нейтрализации угроз является важной функцией государственных органов, решающих задачи обеспечения национальной безопасности. Сформулированная в статье концепция системы национальной безопасности позволяет выявить ее видовые элементы, определить основные процедуры обеспечения национальной безопасности, включающие такие механизмы защиты, как выявление, предотвращение, управление. В рамках этой системы МЧС России как один из субъектов обеспечения национальной безопасности в сфере гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций, обеспечения пожарной безопасности, безопасности людей на водных объектах также использует в основе своей деятельности эту, достаточно универсальную последовательность реагирования на возникающие угрозы. Умение правильно позиционировать место и роль подразделений МЧС России в системе национальной безопасности, способность своевременно выявлять угрозы национальной безопасности, требующие реагирования МЧС России, позволяют повысить качество решения задач, стоящих перед ведомством.

Проведенный анализ эволюции роли и места информационной безопасности в обеспечении национальной безопасности позволяет сделать вывод о том, что, в отличие от других видов безопасности, информационная безопасность является платформенным, системообразующим видом, имеющим в каждом из других видов безопасности свой собственный объект защиты. При этом именно информационная безопасность определяет эффективность, а в ряде случаев и возможность обеспечения других видов национальной безопасности, позволяет интегрировать усилия по обеспечению различных видов национальной безопасности в единый комплекс.

СПИСОК ИСТОЧНИКОВ

1. Maslow A. H. A theory of human motivation // Psychological Review. 1943. № 50. pp. 370–396;
2. Маслоу А. Мотивация и личность. СПб. : Питер, 2003. 352 с.
3. Ковалев А. А. История безопасности как новая область западной исторической науки // Genesis: исторические исследования. 2021. № 12. С. 225–241.
4. Кирикова, А., Арбузова, А. VUCA, BANI и SHIVA: буквы, объясняющие мир // РБК Тренды : сайт. URL: https://trends.rbc.ru/trends/futurology/62866fde9a794701a4c38ae4 (дата обращения: 05.09.2024).
5. Вернадский В. И. Несколько слов о ноосфере // Антология философской мысли. Русский Космизм. М. : Педагогика-Пресс, 1993. 368 с.
6. Вернадский В. И. Начало и вечность жизни. М. : Сов. Россия, 1989. 704 с.
7. Шаповалова И. С., Гоженко Г. И. Понятие техносферы: аналитический обзор формирования и изучения // Научный результат. 2015. № 2. С. 51–57. (Социология и управление).
8. Edward A. Lee The Past, Present and Future of Cyber-Physical Systems: A Focus on Models, Sensors // Basel. 2015. № 15 (3). pp. 4837–4869.
9. Kotenko I., Saenko I., Sineshchuk Yu. Optimizing Secure Information Interaction in a Distributed Computing System by the Method of Sequential Concessions : proceedings – 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, PDP 2020. 28. 2020. С. 429-432.
10. Analysis and Design of Cyber-Physical Systems. A Hybrid Control Systems Approach / R. G. Sanfelice et. al. // Cyber-Physical Systems: From Theory to Practice CRC Press. 2015. С. 3-31.
11. Малькова Т. П. Киборгизация: онтологические проблемы исследования // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. Тамбов : Грамота, 2018. № 3 (89). С. 87–92.
12. Пирумов В. С. Некоторые аспекты методологии и исследования проблем национальной безопасности России в современных условиях // Геополитика и безопасность. 1993. № 1. С. 7–17.
13. Медведев, М. В. Подходы к трактовке понятия «национальная безопасность» // Молодой ученый. 2020. № 23 (313). С. 517–520. URL: https://moluch.ru/archive/313/71316/ (дата обращения: 04.11.2023).
14. Поддубный А. О. К вопросу о понятии «национальная безопасность» // Российская юстиция. 2019. № 6. С. 6–7.

15. Romm Joseph J. Defining National Security: The Nonmilitary Aspects // Council on Foreign Relations. April 1, 1993. Published by the Council on Foreign Relations Press, 58 East 68th St., New York, NY 10021. 1993 - pp.122.

16. Кикоть-Глуходедова Т. В. Административно-правовое обеспечение национальной безопасности в России, США и странах Европы (сравнительное исследование) : дис. … д-ра юрид. наук. М., 2019. 418 с.

17. Бартош А. А. Эволюция стратегии национальной безопасности России. Часть 2. Трансформация законодательной базы России в сфере обеспечения безопасности // Обозреватель. 2016. № 8 (319). С. 5–16.

18. Шваб К., Дэвис Н. Технологии четвертой промышленной революции. М. : Эксмо, 2018. 320 с.

19. Bondar K. Challenges and Opportunities of Industry 4.0 – Spanish Experience (англ.) // International Journal of Innovation, Management and Technology. 2018. Т. 9, № 5. С. 202–208.

20. 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.

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

22. 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.

23. Правовые аспекты безопасности единого информационного пространства силовых ведомств (МВД, МЧС, МО) / А. И. Примакин [и др.] // Вестник Санкт-Петербургского университета МВД России. 2012. № 2 (54). С. 234–240.

24. Singer P., Friedman A. Cybersecurity and Cyberwar: What Everyone Needs to Know. New York : Oxford University Press, 2014. 306 p.

25. Актуальные киберугрозы: итоги 2022 года // Positive Technologies : сайт. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (дата обращения: 05.09.2024).

26. Синещук М. Ю., Шестаков А. В., Гавкалюк Б. В. Инфологическая модель и критерии качества решений по построению ведомственных организационно-технических систем класса «киберполигон» // Вестник Санкт-Петербургского университета ГПС МЧС России. 2023. № 1. С. 121–137.

27. 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. Pp. 295–308.

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

29. Дубровин, Е. Р., Дубровин, И. Р. Современная система национальной безопасности Российской Федерации // Военное обозрение : сайт. URL: https://topwar.ru/159640-sovremennaja-sistema-nacionalnoj-bezopasnosti-rossijskoj-federacii-i-ee.html (дата обращения: 05.09.2024).

30. 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). Pp. 7–27.

31. Синещук Ю. И. Информационная безопасность в системе национальной безопасности // Региональная информатика и информационная безопасность : сб. ст. Санкт-Петербургской междунар. и межрег. конф. 2018. С. 167–170.

32. Theoretical and methodological substantiation of the structure of the state national security system / M. Yu. Zelenkov et. al. // LAPLAGE EM REVISTA. 2021. № 7 (3B). Pp. 421–437. DOI: 10.24115/S2446-6220202173B1569.

REFERENCES

1. Maslow, A. H. A theory of human motivation. Psychological Review, 50, 1943, 370–396.

2. Maslow A. Motivation and personality. St. Petersburg: Peter. 2003; 352.

3. Kovalev A.A. The history of security as a new field of Western historical science // Genesis: historical research. 2021; 12: 225–241. DOI: 10.25136/2409-868X.2021.12.34867 (rus).

4. Kirikova A., Arbuzova A. VUCA, BANI and SHIVA: letters explaining the world. https://trends.rbc.ru/trends/futurology/62866fde9a794701a4c38ae4. (rus).

5. Vernadsky V. I. A few words about the noosphere. In the collection: An anthology of philosophical thought. Russian Cosmism. Moscow, Pedagogy-Press, 1993; 368. (rus).

6. Vernadsky V. I. The beginning and eternity of life. Moscow, Sov. Russia, 1989; 704. (rus).

7. Shapovalova I.S., Gozhenko G.I. The concept of the technosphere: an analytical review of formation and study. Online scientific and practical journal "Scientific result" (from e r and I "Sociology and Management". 2015; 2: 51–57. (rus).

8. Edward A. Lee The Past, Present and Future of Cyber-Physical Systems: A Focus on Models, Sensors (Basel). 2015; 15(3): 4837–4869.

9. Kotenko I., Saenko I., Sineshchuk Yu. Optimizing Secure Information Interaction in a Distributed Computing System by the Method of Sequential Concessions. Proceedings – 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, PDP 2020. 28. 2020. C. 429-432. (rus).

10. Sanfelice R. G., Rawat D., Rodrigues J., Stojmenovic I. Analysis and Design of Cyber-Physical Systems. A Hybrid Control Systems Approach // Cyber-Physical Systems: From Theory to Practice. CRC Press, 2015. C. 3-31.

11. Malkova T. P. Cyborgization: ontological research problems. Historical, philosophical, political and legal sciences, cultural studies and art criticism. Questions of theory and practice. Tambov: Gramota, 2018; 3(89): 87–92. (rus).

12. Pirumov V.S. Some aspects of methodology and research of the problems of national security of Russia in modern conditions // Geopolitics and security. 1993; 1: 7–17. (rus).

13. Medvedev M. V. Approaches to the interpretation of the concept of "national security" // Young scientist. 2020; 23 (313): 517–520. URL: https://moluch.ru/archive/313/71316 / (accessed 04.11.2023). (rus).

14. Poddubny A. O. On the question of the concept of "national security" // Russian Justice. 2019; 6: 6–7. (rus).

15. Romm, Joseph J. “Defining National Security: The Nonmilitary Aspects.” Council on Foreign Relations, April 1, 1993. Published by the Council on Foreign Relations Press, 58 East 68th St., New York, NY 10021. 1993 - pp.122.

16. Kikot-Glukhodedova T. V. Administrative and legal support of national security in Russia, the USA and European countries : a comparative study : dissertation of the degree of Doctor of Law: Moscow State Law University named after O.E. Kutafin (MGUA)]. Moscow, 2019; 418. https://studizba.com/files/show/pdf/59201-77-dissertaciya.html (rus).

17. Bartosh A.A. Evolution of the national security strategy of Russia. Part 2. Transformation of the Russian legislative framework in the field of security. The browser. 2016; 8 (319): 5–16.

18. Klaus Schwab, Nicholas Davis. Technologies of the Fourth Industrial Revolution. Eksmo, 2018; 320.

19. Kateryna Bondar. Challenges and Opportunities of Industry 4.0 – Spanish Experience // International Journal of Innovation, Management and Technology. 2018; 9 (5): 202–208.

20. Shestakova I. G. The new temporality of digital civilization: the future has already come // Scientific and Technical Bulletin of St. Petersburg State University. Humanities and social sciences. 2019; 10 (2): 20–29. DOI: 10.18721/JHSS.10202 (rus).

21. Lapidus L.V. Evolution of the digital economy. Lomonosov Readings-2018. Section of Economic Sciences. Digital economy: man, technology, institutions: a collection of abstracts of speeches. Moscow, Faculty of Economics of Lomonosov Moscow State University, 2018; 153–158. (rus).

22. Sineshchuk Yu.I. Information security of the enterprise in the context of digital transformation. Scientific papers of the Northwestern Institute of Management of the RANEPA. 2022; 13.2 (54): 125–131. (rus).

23. Primakin A.I., Sineshchuk Yu.I., Pantikhovsky O.V., Sineshchuk M.Yu. Legal aspects of the security of the unified information space of law enforcement agencies (Ministry of Internal Affairs, Ministry of Emergency Situations, Ministry of Defense). Bulletin of the St. Petersburg University of the Ministry of Internal Affairs of Russia. 2012; 2 (54): 234–240. (rus).

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

25. Current cyber threats: results of 2022. https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/

26. Sineshchuk M.Yu., Shestakov A.V., Gavkalyuk B.V. Infological model and criteria for the quality of solutions for the construction of departmental organizational and technical systems of the cyberpolygon class // Scientific and analytical journal "Bulletin of the St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia". 2023; 1: 121–137. (rus).

27. 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; 295–308. (rus).

28. Andreev A.S., Ivantsov A.M. The experience of using complexes (polygons) in the field of information security // Information counteraction to terrorist threats. 2015; 1 (25): 15–17. (rus).

29. Dubrovin E.R., Dubrovin I.R. The modern national security system of the Russian Federation. Military Review, July 2019. https://topwar.ru/159640-sovremennaja-sistema-nacionalnoj-bezopasnosti-rossijskoj-federacii-i-ee.html (rus).

30. Vladimir A. Chobanyan, Igor Yu. Shahalov. Analysis and synthesis of the requirements for safety systems of objects of critical information infrastructure. Issues of cybersecurity. 2013; 1(1): 7–27. (rus).

31. Sineshchuk Yu.I. Information security in the national security system/ In the collection: Regional informatics and information security. Collection of articles of the St. Petersburg International and interregional conferences. 2018; 167–170. (rus).

32. Zelenkov M. Yu. , Smulsky S. V., Herrera L. M., Shalmieva D. B., Nefedova L. V. Theoretical and methodological substantiation of the structure of the state national security system. 2021. LAPLAGE EM REVISTA 7(3B):421-437. DOI:10.24115/S2446-6220202173B1569. (rus).

Информация об авторах

Юрий Иванович Синещук, доктор технических наук, профессор, Заслуженный работник высшей школы Российской Федерации, профессор кафедры пожарной безопасности зданий и автоматизированных систем пожаротушения Санкт-Петербургского университета ГПС МЧС России, Россия, 196105, г. Санкт-Петербург, Московский пр., д. 149, SPIN-код: 4663-4378, AuthorID: 693471;
e-mail: sinegal53@mail.ru

Сергей Николаевич Терёхин доктор технических наук, доцент, профессор кафедры пожарной безопасности зданий и автоматизированных систем пожаротушения Санкт-Петербургского университета ГПС МЧС России, Россия, 196105, г. Санкт-Петербург, Московский пр., д. 149, SPIN-код: 9342-2440, AuthorID: 831558;
e-mail: expert_terehin@igps.ru

Григорий Леонидович Шидловский, кандидат технических наук, доцент, начальник кафедры пожарной безопасности зданий и автоматизированных систем пожаротушения Санкт-Петербургского университета ГПС МЧС России, Россия, 196105, г. Санкт-Петербург, Московский пр., д. 149, SPIN-код: 4345-1531, AuthorID: 851462;
e-mail: shidlovsky.g@igps.ru

Information about the authors

Yury I. Sineshchuk, Doctor of Technical Sciences, Professor, Honored Worker of the Higher School of the Russian Federation; 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 (149, Moskovskiy Ave., Saint Petersburg 196105, Russian Federation; SPIN-код: 4663-4378, AuthorID: 693471,
e-mails: sinegal53@mail.ru

Sergey N. Terehin, Doctor of Technical Sciences, Associate Professor, 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, 149, Moskovskiy Ave., Saint Petersburg 196105, Russian Federation; SPIN-код: 9342-2440, AuthorID: 831558,
e-mail: expert_terehin@igps.ru

Grigory L. Shidlovsky Cand. Sci. (Eng.), Associate Professor, 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 149, Moskovskiy Ave., Saint Petersburg 196105, Russian Federation), SPIN-код: 4345-1531, AuthorID: 851462,
e-mail: shidlovsky.g@igps.ru

Ожегов Эдуард Александрович, кандидат технических наук, доцент, доцент кафедры пожарной безопасности в строительстве Уральского института ГПС МЧС России, 620062, Россия, г. Екатеринбург, ул. Мира, д. 22, Author ID: 843941;
e-mail: upch.urigps@bk.ru

Eduard A. Ozhegov, Cand. Sci. (Eng.), Associate Professor, Associate Professor of the Department of Fire Safety in Construction of Ural Institute of State Fire Service of EMERCOM of Russia, 22, Mira St., Yekaterinburg 620062, Russian Federation; Author ID: 843941,
e-mail: upch.urigps@bk.ru