Ученые записки Крымского федерального университета имени В. И. Вернадского
Юридические науки. – 2024. – Т. 10 (76). № 4. – С. 152–158.

УДК 34.096

ПУБЛИЧНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ КИБЕРБЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ. ПРИМЕНЕНИЕ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА

Баландин А. Ю.
МГЮА им. О. Е. Кутафина

Возрастающее число компьютерных атак и многообразие цифровой инфраструктуры в сочетании с предметной новизной нормативных актов обеспечения кибербезопасности может сыграть дезориентирующую роль в деятельности субъектов информационных правоотношений, существенно снизить оперативность и эффективность принятия мер обеспечения безопасности киберсреды. В рассматриваемой статье автором приводится методология риск-ориентированного подхода в достижении должного уровня кибербезопасности информационной инфраструктуры, обеспечивающего функционирование различных по роду субъектов в заданном диапазоне критериев эффективности. Сравнительный анализ отраслевого законодательства Российской Федерации, международных нормативных правовых актов и законодательства иностранных государств заложен в основу вывода о возможности применения риск-ориентированного подхода в качестве методологического инструмента обеспечения кибербезопасности объектов информационной инфраструктуры на национальном и на международном ровне, формировании проактивной защиты цифровой среды на основе прогнозирования вектора развития потенциальных киберугроз и приоритетности отражения кибератак для обеспечения функционирования объектов информационной инфраструктуры.

Ключевые слова: кибербезопасность, риск-ориентированный подход, киберугрозы, приоритетность, таксономия кибервреда, управление рисками, кибербезопасность элементов цепочки поставок.

Развитие современного информационного общества детерминировано высокой степенью технологичности и инновационностью социальной среды. Следствием стремительной компьютеризации общественных отношений является расширение цифрового ландшафта, в контексте кибербезопасности, рассматривающегося в качестве неизменного объекта реализации кибератак.

Необходимость обеспечения кибербезопасности информационных активов неоднократно указывалась в качестве одной из приоритетных задач обеспечения суверенитета РФ [1; 2]. Особая значимость рассматриваемому вопросу отводится в документах стратегического планирования [3; 4], поскольку современные реалии аккумулируют новые вызовы в сфере обеспечения безопасности информационных систем вне зависимости от сферы интеграции, а стремительные темпы развития информационной инфраструктуры обуславливают появление новых сегментов цифровой среды, со временем преобразующихся в отдельные функциональные социотехнические экосистемы. В связи с необходимостью защиты подведомственных объектов информационной инфраструктуры и формирования у субъектов информационных правоотношений надлежащей осмотрительности в киберсреде, законодателем принимаются различные по характеру и методу правового воздействия организационно-правовые меры, реализация которых направлена на систематическое повышение эффективности средств противодействия кибератакам и ликвидации уязвимостей компьютерной инфраструктуры.

Наряду с технологической компонентой кибербезопасности [5] не менее важное значение для обеспечения защищенности и устойчивости компьютерной инфраструктуры к деструктивным воздействиям имеет правовая основа деятельности

субъектов информационных правоотношений в киберпространстве, включая подлежащие всеобщей ратификации нормы международного права [6; 7]. Ученое сообщество неоднократно подчеркивало прогностическую функцию права как науки в условиях масштабной цифровизации [8; 9], в том числе в свете *анализа современных правовых рисков и угроз в области правового обеспечения информационной безопасности* [10]. Масштабность трансформации компьютерной среды подчеркивает актуальность аналитического подхода, в том числе для выработки комплексных мер противодействия кибератакам и оценки перспективности их внедрения владельцами информационных систем.

Один из методов обеспечения кибербезопасности цифровой среды основан на установлении приоретизации уязвимостей информационной инфраструктуры в зависимости от степени критичности вероятных негативных последствий при их потенциальной эксплуатации в ходе проведения компьютерных атак. Практическим результатом внедрения данного концепта является применение программных продуктов (SGRC-платформ) с функцией моделирования рисков и аудита информационной безопасности. Принцип моделирования угроз безопасности киберсреды нормативно закреплен в актах отраслевого регулятора [11; 12; 13] и наряду с функцией проектирования эшелонированной защиты является методическим инструментом мониторинга защищенности инфраструктуры [14]. Указанные положения предусматривают возможность совместного проведения уполномоченным федеральным органом исполнительной власти и субъектом информационных правоотношений – владельцем информационной инфраструктуры, всестороннего анализа защищенности эксплуатируемых компьютерных систем при проектировании периметра защиты и мониторинга актуальных сведений о его текущем состоянии. Подобная таксономия детально анализируется и в зарубежной научной литературе [15], ассоциирующей кибербезопасность как средство устранения рисков различного типа. Вполне очевидно, что рассмотренная тактика обоснованно согласуется с финансовыми интересами различных учреждений, представленных в информационной среде, вне зависимости от организационно-правовой формы и принадлежности, поскольку формируется с учетом экономической целесообразности и основывается на комплексной оценке киберриска как вероятного следствия реализации компьютерных угроз. Вместе с тем, в контексте обеспечения кибербезопасности объектов критической информационной инфраструктуры приоритезация отдельных видов угроз не имеет нивелирующее значение по отношению к менее значимым (с точки зрения пагубности для защищаемых процессов и реализуемых с меньшей вероятностью) угрозам. Данное утверждение вполне закономерно и следует из основополагающего принципа, определяющего кибербезопасность как совокупность средств гарантированного обеспечения аутентичности информации и информационных сетей [16, с. 78] без каких-либо изъятий. Кроме того, в системе федеральных органов исполнительной власти реализован институт ведомственного контроля, имеющий аналогичную правовую основу и объединяющий в единую организационно-правовую систему требования к средствам противодействия компьютерным атакам, алгоритмы функционирования объектов информатизации в ходе реализации мер кибербезопасности, а также требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ и меры реализации государственного контроля в указанной области.

Ориентированность на оценку потенциальных угроз в качестве методологического инструмента обеспечения кибербезопасности объектов информационной инфраструктуры получило широкое распространение в различных социально-экономических сферах, и в настоящее время применяется субъектами информационных правоотношений вне зависимости от специфики их деятельности и стадии жизненного цикла. Несмотря на присущие каждому из направлений тематические особенности, последовательность интеграции рассматриваемого метода подразумевает наличие сущностного базиса, определяющего его уникальность и ценность практического применения. В любой отраслевой интерпретации просматривается детерминированный конечной целью принцип выявления и оценки рисков как потенциальной угрозы состоянию защищенности, их градации по степени опасности, в сочетании с последующим выстраиванием и управлением структурированной системы проактивной защиты, обеспечивающей функционирование информационной инфраструктуры на минимально необходимом уровне в условиях проведения компьютерных атак, что в конечном счете должно способствовать не противопоставлению протокола обеспечения кибербезопасности сущностными функциональным процессам, а скорее их взаимной синергии.

Следствием рассматриваемой детализации кризисной функциональности объекта организационно-правовой охраны является выработка комплексных мер противодействия противоправному посягательству: наряду с развертыванием в цифровой среде специализированного программного обеспечения широкое практическое применение находит дифференциация уровней доступа к информационным объектам, резервирование и очередность восстановления функций в зависимости от степени критичности цифрового сегмента, передача функций обеспечения кибербезопасности провайдеру управляемых сервисов (MSSP, Managed Security Services Providers) [17].

Инклюзивность риск-ориентированного подхода заключается в обеспечении надлежащей оценки кибербезопасности всех элементов цепочки поставок, включенных в общий анализ устойчивости цифровой инфраструктуры, что призвано снизить риски бесконтрольной интеграции элементов различных свойств в единую систему. Прикладное значение данное положение приобретает в случае инсталляции множества исторически дифференцированных программно-аппаратных решений, имеющих фундаментальные отличия и обладающих характерным набором эксплойтов [18], либо применение IoT (Internet of Things – интернет вещей), представляющего распределенные системы, что, с одной стороны, увеличивает поверхность атаки [19], а с другой стороны, наряду с иными компонентами, имеет элементы, применяющиеся в качестве средств реализации кибератак [20]. В свою очередь, дедуктивность анализа компонентного риска влечет выработку и принятие мер по обеспечению безопасности элементов цепочки поставок, либо корреспондирует данную функцию владельцам интегрируемых сегментов в контексте единой системы обеспечения кибербезопасности.

Применение риск-ориентированного подхода обеспечения кибербезопасности нашло отражение в нормативных правовых актах иностранных государств. Примечателен в данном контексте организационно-правовой опыт правительства США [21], где для негосударственных систем безопасности в 2008 г. в США стартовала программа NIST C-SCRM – Управление рисками цепочки поставок в киберпро-

странстве, направленная на выявление, оценку и снижение рисков, связанных с распределенным и взаимосвязанным характером цепочек поставок продуктов и услуг информационных и операционных технологий [22].

Правительством КНР реализуются меры самостоятельной реализации национальными компаниями оценки рисков работы с иностранными партнерами [23], при этом с определенной периодичностью проводится оценка рисков объектов критически важной информационной инфраструктуры [24].

Вывод. В настоящее время в связи с высокими темпами развития информационных технологий и резкого увеличения цифрового ландшафта риск-ориентированный подход в вопросах обеспечения кибербезопасности представляется наиболее приемлемым и обоснованным не только с точки зрения финансовых затрат, но и с учетом специфики кадрового обеспечения информационной сферы. Реализация данной концепции основывается на процессном управлении и риск-ориентированном мышлении, как альтернативе формальному выполнению нормативных предписаний регулятора, сочетающей централизацию управления и позиционность оценки обеспеченного уровня кибербезопасности в условиях необходимости реализации текущих функциональных процессов на заданном уровне. Изложенное при конструктивном сотрудничестве субъектов информационных правоотношений позволяет анонсировать наиболее эффективную модель беспрерывного функционирования информационных систем в конкретных условиях с заданными критериями, позволяющую с большей эффективностью осуществлять упреждающие меры проактивной защиты технологической среды, и, как следствие, повышать уровень кибербезопасности национальной и наднациональной информационной инфраструктуры.

Список литературы:

1. Новые векторы развития системы правового обеспечения информационной безопасности как одного из приоритетов национальной безопасности (к 30-летию принятия закона Российской Федерации «О безопасности») / Т. А. Полякова, Г. Г. Камалова. – Текст : непосредственный // Правовое государство: теория и практика. – 2022. – № 2 (68). – С. 112-121.
2. Обзор международной научно-практической конференции «Информационное пространство: обеспечение информационной безопасности и право» – Первые Бачиловские чтения / Т. А. Полякова, А. В. Минбалеев, Н. В. Кроткова. – Текст : непосредственный // Государство и право. – 2018. – № 9. – С. 138-148.
3. Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Собр. законодательства РФ – 2021. – 5 июля. – Текст: непосредственный.
4. Указ Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // Собр. законодательства РФ – 2018. – 14 мая. – Текст: непосредственный.
5. Кибербезопасность сетевого периметра объекта критической информационной инфраструктуры / В. С. Горбатов, И. Ю. Жуков, В. В. Кравченко, Д. И. Правиков. – Текст : непосредственный // Безопасность информационных технологий. – 2022. – Т. 29. № 4. – С. 12-26.
6. Проблемы формирования системы международной информационной безопасности в условиях трансформации права и новых вызовов и угроз / Т. А. Полякова, Г. Г. Шинкарецкая. – Текст : непосредственный // Право и государство: теория и практика. – 2020. – № 10 (190). – С. 138-142.
7. Международно-правовые аспекты кибербезопасности / А. А. Данелян, Е. Е. Гуляева. – Текст : непосредственный // Московский журнал международного права. – 2020. – № 1. С. 44-53.
8. Технологические порядки и правовая мысль: дуалистическая парадигма развития / В. С. Осипов, А. В. Минбалеев – Текст : непосредственный // Журнал цифрового права. – 2021. Т. 2. № 3. – С. 71-77.
9. Вопросы построения юридических дефиниций в сфере искусственного интеллекта / В. Б. Наумов, Г. Г. Камалова. – Текст : непосредственный // Труды Института государства и права Российской академии наук. – 2020. – Т. 15. № 1. – С. 81-93.
10. Актуальные проблемы формирования системы правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе и транс-

формации права / Т. А. Полякова, А. В. Минбалеев. – Текст : непосредственный // Теория и практика юридической науки. – 2019. – № 3 (56). С. 67-73.
11. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собр. законодательства РФ. – 2012. – 5 ноября. – Текст: непосредственный.
12. Методика оценки угроз безопасности информации : утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 15.08.2023). – Текст: электронный.
13. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных : утв. заместителем директора ФСТЭК России 14 февраля 2008 г. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodika-ot-14-fevralya-2008-g (дата обращения: 07.08.2023). – Текст: электронный.
14. Приказ ФСБ России от 11 мая 2023 г. № 213 «Об утверждении порядка осуществления мониторинга защищенности информационных ресурсов, принадлежащих федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов Российской Федерации, государственным фондам, государственным корпорациям (компаниям), иным организациям, созданным на основании федеральных законов, стратегическим предприятиям, стратегическим акционерным обществам и системообразующим организациям российской экономики, юридическим лицам, являющимся субъектами критической информационной инфраструктуры Российской Федерации либо используемых ими». Доступ из справ.-правовой системы «КонсультантПлюс» – Текст: электронный.
15. Иоаннис Аграфиотис, Джейсон Р.К. Медсестра, Майкл Голдсмит, Сэди Криз, Дэвид Аптон. Таксономия кибер-вреда: определение последствий кибератак и понимание того, как они распространяются. – Текст: электронный // Журнал кибербезопасности. – 2018. – Т. 4. Выпуск 1, tyy006. – URL: https://doi.org/10.1093/cybsec/tyy006 (дата обращения: 07.08.2023).
16. Полякова, Т. А. Новые горизонты развития системы информационного права в условиях цифровой трансформации : Монография / отв. ред. Т. А. Полякова, А. В. Минбалеев, В. Б. Наумов [и др.] – Москва : ИГП РАН, 2022. – 368 с. – Текст : непосредственный.
17. О совершенствовании инфраструктуры SOC MSSP / В. Г. Жуков, М. Н. Жукова. – Текст: непосредственный // Решетневские чтения. – 2016. – Т. 2. – С. 250-251.
18. Анализ моделей и методик, используемых для атрибуции нарушителей кибербезопасности при реализации целевых атак / И. Котенко, С. С. Хмыров. – Текст: непосредственный // Вопросы кибербезопасности. – 2022. – № 4 (50). – С. 52-79.
19. О кибербезопасности систем Интернета Вещей / Д. Е. Намиот, В. А. Сухомлин. – Текст: непосредственный // International Journal of Open Information Technologies. – 2023. – Т. 11. – № 2. – С. 85-97.
20. Жаркова, М. В. Основные аспекты DDOS-атаки как угрозы информационной безопасности в современном мире / М. В. Жаркова. – Текст : электронный // THE BEST SOLUTIONS FOR RESEARCH CHALLENGES. – 2021. – С. 6-10. – URL: https://www.elibrary.ru/item.asp?id=46410139 (дата обращения: 17.08.2023).
21. The Comprehensive National Cybersecurity Initiative. – URL: https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf (дата обращения: 14.08.2023).
22. Кибер-управление рисками цепочки поставок (C-SCRM). – URL: https://csrc.nist.rip/scrm/ (дата обращения: 14.08.2023).
23. Меры по оценке безопасности экспорта данных : утв. Приказом Государственной службы интернет-информации КНР от 7 июля 2022 г. № 11. – URL: http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm (дата обращения: 17.08.2023). – Текст: электронный.
24. Положение о защите критически важной информационной инфраструктуры : утв. Постановлением Государственного совета КНР от 17 августа 2021 г. – URL: https://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm (дата обращения: 17.08.2023). – Текст: электронный.

Balandin A.Yu. Implementation of a risk-based approach to issues of public law regulation of cybersecurity in the Russian Federation // Scientific notes of V. I. Vernadsky crimean federal university. Juridical science. – 2024. – T. 10 (76). № 4. – P. 152-158.

The increasing number of computer attacks and the diversity of digital infrastructure, combined with the subject novelty of cybersecurity regulations, can play a disorienting role in the activities of subjects of information legal relations, significantly reduce the efficiency and effectiveness of taking measures to ensure the security of the cyber environment. In the article under consideration, the author provides a methodology for a risk-based approach to achieving the proper level of cybersecurity of the information infrastructure, ensuring the functioning of various entities in a given range of performance criteria. A comparative analysis of the sectoral legislation of the Russian Federation, international regulatory legal acts and legislation of foreign states is the basis for the conclusion that a risk-based approach can be used as a methodological tool to ensure cybersecurity of information infrastructure facilities at the national and international levels, the formation of proactive protection of the digital environment based on forecasting the vector of development of potential cyber threats and the priority of repelling cyber attacks to ensure the functioning of information infrastructure facilities.

Keywords: cybersecurity, risk-based approach, cyber threats, priority, taxonomy of the cyber environment, risk management, cybersecurity of supply chain elements.

Spisok literatury:

1. Novye vektory razvitiya sistemy pravovogo obespecheniya informacionnoj bezopasnosti kak odnogo iz prioritetov nacional'noj bezopasnosti (k 30-letiyu prinyatiya zakona Rossijskoj Federacii «O bezopasnosti») / T. A. Polyakova, G. G. Kamalova. – Tekst : neposredstvennyj // Pravovoe gosudarstvo: teoriya i praktika. – 2022. – № 2 (68). – S. 112-121.
2. Obzor mezhdunarodnoj nauchno-prakticheskoj konferencii «Informacionnoe prostranstvo: obespechenie informacionnoj bezopasnosti i pravo» – Pervye Bachilovskie chteniya / T. A. Polyakova, A. V. Minbaleev, N. V. Krotkova. – Tekst : neposredstvennyj // Gosudarstvo i pravo. – 2018. – № 9. – S. 138-148.
3. Ukaz Prezidenta RF ot 2 iyulya 2021 g. № 400 «O Strategii nacional'noj bezopasnosti Rossijskoj Federacii» // Sobr. zakonodatel'stva RF – 2021. – 5 iyulya. – Tekst: neposredstvennyj.
4. Ukaz Prezidenta RF ot 7 maya 2018 g. № 204 «O nacional'nyh celyah i strategicheskih zadachah razvitiya Rossijskoj Federacii na period do 2024 goda» // Sobr. zakonodatel'stva RF – 2018. – 14 maya. – Tekst: neposredstvennyj.
5. Kiberbezopasnost' setevogo perimetra ob"ekta kriticheskoj informacionnoj infrastruktury / V. S. Gorbatov, I. YU. ZHukov, V. V. Kravchenko, D. I. Pravikov. – Tekst : neposredstvennyj // Bezopasnost' informacionnyh tekhnologij. – 2022. – T. 29. № 4. – S. 12-26.
6. Problemy formirovaniya sistemy mezhdunarodnoj informacionnoj bezopasnosti v usloviyah transformacii prava i novyh vyzovov i ugroz / T. A. Polyakova, G. G. SHinkareckaya. – Tekst : neposredstvennyj // Pravo i gosudarstvo: teoriya i praktika. – 2020. – № 10 (190). – S. 138-142.
7. Mezhdunarodno-pravovye aspekty kiberbezopasnosti / A. A. Danelyan, E. E. Gulyaeva. – Tekst : neposredstvennyj // Moskovskij zhurnal mezhdunarodnogo prava. – 2020. – № 1. S. 44-53.
8. Tekhnologicheskie poryadki i pravovaya mysl': dualisticheskaya paradigma razvitiya / V. S. Osipov, A. V. Minbaleev – Tekst : neposredstvennyj // ZHurnal cifrovogo prava. – 2021. T. 2. № 3. – S. 71-77.
9. Voprosy postroeniya yuridicheskih definicij v sfere iskusstvennogo intellekta / V. B. Naumov, G. G. Kamalova. – Tekst : neposredstvennyj // Trudy Instituta gosudarstva i prava Rossijskoj akademii nauk. – 2020. – T. 15. № 1. – S. 81-93.
10. Aktual'nye problemy formirovaniya sistemy pravovogo regulirovaniya obespecheniya informacionnoj bezopasnosti v usloviyah bol'shih vyzovov v global'nom informacionnom obshchestve i transformacii prava / T. A. Polyakova, A. V. Minbaleev. – Tekst : neposredstvennyj // Teoriya i praktika yuridicheskoj nauki. – 2019. – № 3 (56). S. 67-73.
11. Postanovlenie Pravitel'stva RF ot 1 noyabrya 2012 g. № 1119 «Ob utverzhdenii trebovanij k zashchite personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh» // Sobr. zakonodatel'stva RF. – 2012. – 5 noyabrya. – Tekst: neposredstvennyj.
12. Metodika ocenki ugroz bezopasnosti informacii : utv. Federal'noj sluzhboj po tekhnicheskomu i eksportnomu kontrolyu 5 fevralya 2021 g. Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus» (data obrashcheniya: 15.08.2023). – Tekst: elektronnyj.
13. Metodika opredeleniya aktual'nyh ugroz bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh : utv. zamestitelem direktora FSTEK Rossii 14 fevralya 2008 g. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodika-ot-14-fevralya-2008-g (data obrashcheniya: 07.08.2023). – Tekst: elektronnyj.
14. Prikaz FSB Rossii ot 11 maya 2023 g. № 213 «Ob utverzhdenii poryadka osushchestvleniya monitoringa zashchishchennosti informacionnyh resursov, prinadlezhashchih federal'nym organam ispolnitel'noj vlasti, vysshim ispolnitel'nym organam gosudarstvennoj vlasti sub"ektov Rossijskoj Federacii, gosudarstvennym fondam, gosudarstvennym korporaciyam (kompaniyam), inym organizaciyam, sozdannym na osnovanii federal'nyh zakonov, strategicheskim predpriyatiyam, strategicheskim akcionernym obshchestvam i sistemoobrazuyushchim organizaciyam rossijskoj ekonomiki, yuridicheskim licam, yavlyayushchimsya sub"ektami kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii libo ispol'zuemyh imi». Dostup iz sprav.-pravovoj sistemy «Konsul'tantPlyus» – Tekst: elektronnyj.
15. Ioannis Agrafiotis, Dzhejson R.K. Medsestra, Majkl Goldsmit, Sedi Kriz, Devid Apton. Taksonomiya kiber-vreda: opredelenie posledstvij kiberatak i ponimanie togo, kak oni rasprostranyayutsya. – Tekst: elektronnyj // ZHurnal kiberbezopasnosti. – 2018. – T. 4. Vypusk 1, tyy006 . – URL: https://doi.org/10.1093/cybsec/tyy006 (data obrashcheniya: 07.08.2023).
16. Polyakova, T. A. Novye gorizonty razvitiya sistemy informacionnogo prava v usloviyah cifrovoj transformacii : Monografiya / otv. red. T. A. Polyakova, A. V. Minbaleev, V. B. Naumov [i dr.] – Moskva : IGP RAN, 2022. – 368 s. – Tekst : neposredstvennyj.
17. O sovershenstvovanii infrastruktury SOC MSSP / V. G. ZHukov, M. N. ZHukova. – Tekst: neposredstvennyj // Reshetnevskie chteniya. – 2016. – T. 2. – S. 250-251.
18. Analiz modelej i metodik, ispol'zuemyh dlya atribucii narushitelej kiberbezopasnosti pri realizacii celevyh atak / I. Kotenko, S. S. Hmyrov. – Tekst: neposredstvennyj // Voprosy kiberbezopasnosti. – 2022. – № 4 (50). – S. 52-79.

19. O kiberbezopasnosti sistem Interneta Veshchej / D. E. Namiot, V. A. Suhomlin. – Tekst: neposredstvennyj // International Journal of Open Information Technologies. – 2023. – T. 11. – № 2. – S. 85-97.
20. ZHarkova, M. V. Osnovnye aspekty DDOS-ataki kak ugrozy informacionnoj bezopasnosti v sovremennom mire / M. V. ZHarkova. – Tekst : elektronnyj // THE BEST SOLUTIONS FOR RESEARCH CHALLENGES. – 2021. – S. 6-10. – URL: https://www.elibrary.ru/item.asp?id=46410139 (data obrashcheniya: 17.08.2023).
21. The Comprehensive National Cybersecurity Initiative. – URL: https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf (data obrashcheniya: 14.08.2023).
22. Kiber-upravlenie riskami cepochki postavok (C-SCRM). – URL: https://csrc.nist.rip/scrm/ (data obrashcheniya: 14.08.2023).
23. Mery po ocenke bezopasnosti eksporta dannyh : utv. Prikazom Gosudarstvennoj sluzhby internet-informacii KNR ot 7 iyulya 2022 g. № 11. – URL: http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm (data obrashcheniya: 17.08.2023). – Tekst: elektronnyj.
24. Polozhenie o zashchite kriticheski vazhnoj informacionnoj infrastruktury : utv. Postanovleniem Gosudarstvennogo soveta KNR ot 17 avgusta 2021 g. – URL: https://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm (data obrashcheniya: 17.08.2023). – Tekst: elektronnyj.

.