Научная статья / Research Article
УДК 316.4, 351/354
DOI: 10.14258/SSI(2025)3–15

Управленческие практики реализации государственной политики обеспечения безопасности критической информационной инфраструктуры в субъекте РФ

Галина Алексеевна Банных[1]

Павел Владимирович Туктарев[2]

[1]Уральский федеральный университет им. первого Президента России Б.Н. Ельцина, Екатеринбург, Россия, g.a.bannykh@urfu.ru, https://orcid.org/0000–0002–8175–591X

[2]Уральский федеральный университет им. первого Президента России Б.Н. Ельцина, Екатеринбург, Россия, Pavel.tuktariov@urfu.ru

Аннотация. Современное российское государство все больше сталкивается с внешней агрессией в информационном пространстве. Отмечается увеличение количества киберугроз (на 60% в 2024 г. по сравнению с 2023 г.), причем 64% от общего числа кибератак за 2024 г. пришлось на государственные органы и учреждения, в том числе имеющие объекты критической информационной инфраструктуры[74] (далее — КИИ). Нарушения в функционировании КИИ могут привести к крупным экономическим потерям, угрожать жизни и здоровью людей, производственной безопасности, обороноспособности страны, лишить ее научного и технического потенциала. Поэтому одним из главных направлений работы государственных органов становится защита КИИ. Цель статьи — изучить управленческие практики по реализации государственной политики обеспечения безопасности КИИ в субъекте РФ.

Методы исследования: анализ документов, формально-юридический метод, анализ статистических данных, анкетирование, экспертный опрос.

Схема взаимодействия с государственными регуляторами разработана для всех участников отношений в сфере КИИ, при этом субъекты КИИ несут дополнительные финансовые затраты на обеспечение безопасности значимых объектов КИИ, а методическая помощь со стороны органов публичной власти расценивается ими как недостаточная. Кроме типичных проблем (рост кибератак и нехватка квалифицированных кадров) к проблемам можно отнести и слабую защищенность таких объектов, как серверные, дата-центры и пр., от несанкционированного доступа, аварий и физического воздействия. Государственное регулирование использования информационных технологий и инфраструктур УФСТЭК по УрФО отстает от темпов их развития, участники отношений в сфере КИИ оказываются недостаточно защищенными от воздействующих на них информационных техногенных факторов.

---

[74] Число кибератак на российские компании за год выросло в 2,5 раза. URL: https://clck.ru/3JcQZc.

Государственная политика обеспечения безопасности КИИ РФ реализуется на основании НПА, регулирующих отношения всех участников в сфере КИИ, определяющих их полномочия, права и обязанности. Для эффективной реализации государственной политики необходимо внедрение обязательных требований в законодательство РФ по вопросам проведения процедуры категорирования объектов КИИ для субъектов КИИ из числа негосударственных юридических лиц; организация адресной методической помощи по вопросам категорирования объектов КИИ со стороны субъектов реализации государственной политики.

Ключевые слова: государственная политика, информационная безопасность, государственное регулирование, критическая информационная инфраструктура, объекты КИИ

Для цитирования: Банных Г.А., Туктарев П.В. Управленческие практики реализации государственной политики обеспечения безопасности критической информационной инфраструктуры в субъекте РФ // Society and Security Insights. 2025. Т. 8, № 3. С. 266–282. doi: 10.14258/ssi(2025)3–15.

Management Practices of Implementation of the State Policy for Security of Critical Information Infrastructure in the Subject of the Russian Federation

Galina A. Bannykh[1]

Pavel V. Tuktarev[2]

[1]Ural Federal University, Yekaterinburg, Russia, g.a.bannykh@urfu.ru, https://orcid.org/0000–0002–8175–591X

[2]Ural Federal University, Yekaterinburg, Russia, tuktarev93@mail.ru

Abstract. The modern Russian state is increasingly confronted with external aggression in the information space. There is an increase in the number of cyber threats (by 60% in 2024 compared to 2023), with 64% of the total number of cyberattacks in 2024 being on government bodies and institutions, including those with critical information infrastructure facilities (hereinafter — CII). Violations in the functioning of CII can lead to major economic losses, threaten human life and health, production security, defense capacity of the country, deprive its scientific and technical potential. Therefore, one of the main areas of work of state bodies becomes the protection of CII. Purpose of the article — to study managerial practices on implementation of state policy for security of CIII in the subject of the Russian Federation.

Methods of research: Document analysis, formal legal method, analysis of statistical data, questionnaire, expert survey.

The scheme of interaction with state regulators has been developed for all participants in relations in the sphere of CII, but the subjects of CII bear additional financial costs to ensure the security of significant objects of CII; and methodological assistance from public authorities is

regarded by them as insufficient. In addition to the typical problems (the growth of cyberattacks and the lack of qualified personnel), the problems also include poor protection of such facilities as server rooms, data centers, etc. from unauthorized access, accidents and physical impact. State regulation of the use of information technologies and infrastructures of UPTEC on UrFO lags behind their development, participants in relations in the sphere of CII are not sufficiently protected from the information technological factors affecting them.

The state security policy of the CII is implemented on the basis of legal acts, which regulate the relations of all participants in the sphere of the CII, defining their powers, rights and duties. For the effective implementation of state policy, it is necessary to introduce mandatory requirements in the legislation of the Russian Federation on the procedure for categorizing CII objects for CII entities among legal entities; Organization of targeted methodological assistance on the categorization of CII objects by the subjects of the state policy.

Keywords: public policy, information security, state regulation, critical information infrastructure, ICT facilities

For citation: Bannykh, G.A., Tuktarev, P.V. (2025). Management practices of implementation of the state policy for security of critical information infrastructure in the subject of the Russian Federation. *Society and Security Insights, 8*(3), 266–282. (In Russ.). doi: 10.14258/ssi(2025)3–15.

Введение

Современное общество все больше полагается на цифровые технологии для функционирования экономики, управления государственными услугами, здравоохранения, транспорта и других жизненно важных сфер. Критические информационные системы становятся основой жизнедеятельности государств. С развитием цифровизации возрастает и число кибератак, направленных на нарушение работы ключевых инфраструктурных объектов.

В РФ реализуется государственная политика обеспечения безопасности КИИ как комплекс регуляторных и управляющих мер уполномоченных государственных органов. Государственная система обеспечения безопасности КИИ в РФ — это комплекс мер и механизмов, направленных на обеспечение надежной защиты информационной инфраструктуры объектов, отнесенных к категории критической, от угроз и опасностей, которые могут привести к ее нарушению, разрушению или нанести системным объектам ущерб. Указанная система состоит из нормативно-правовых актов (далее — НПА), стандартов, методологий и комплекса технических средств, а также организационных и кадровых мер, направленных на управление и контроль за процессом обеспечения безопасности КИИ. Она регулируется федеральными законами, правительственными решениями и распоряжениями в области информационной безопасности.

Развитие информационных технологий, увеличение угроз информационной безопасности, адаптация к механизмам и способам информационной защиты уязвимых данных потенциальных нарушителей идет гораздо более быстрыми темпами, чем развитие нормативного регулирования в этой сфере. В настоящее время нормативные документы не предусматривают обязательных требований выполнения законодательства в вопросах присвоения категории значимости объ-

ектам КИИ, принадлежащим юридическим лицам, а также не определены нормативные сроки начала и завершения процесса категорирования информационных систем этих организаций. Поэтому основным вопросом обеспечения защищенности становится реальная управленческая практика, приводящая к удовлетворительным результатам.

Цель работы — изучение управленческой практики в ходе реализации государственной политики обеспечения безопасности КИИ в Свердловской области. Последовательно планируется раскрыть вопросы, связанные с теоретическим и нормативно-правовым обоснованием феномена критической информационной безопасности, особенно в контексте цифровизации государственного управления. Далее в статье изучена практика государственного регулятора ФСТЭК России по УрФО в Свердловской области, проведен опрос участников отношений в сфере обеспечения безопасности КИИ, предложены выводы и рекомендации.

1. Теоретическая и нормативная рамка исследования

Значительная часть работ в отношении обеспечения информационной защищенности и объектов КИИ находится на стыке юридической науки и науки в сфере информационных технологий. Заметный вклад в разработку теории и методологии правового обеспечения информационной сферы внесли работы Т. А. Поляковой, В.В. Пекаревой, А.В. Минбалеева, А.А. Стрельцова (Новые горизонты развития …, 2022; Полякова, Антопольский и др., 2017; Пекарева, 2024, Стрельцов, Капустин и др., 2023). С.А. Кузнецов, И.А. Куликов, А.А. Фоминых (Кузнецов и др., 2021) сравнили отечественный и зарубежный опыт проведения процедуры категорирования субъектов КИИ. М.С. Валенцев (2020) исследовал положения о квалификации противоправного воздействия на КИИ РФ ее владельцами и пользователями, Х.А. Аккаева (2023) — особенности кибератак на объекты КИИ.

С позиций обеспечения национальной безопасности феномен КИИ был рассмотрен в работах Ю.А. Баяновой (2021), И. М. Кривоносова, А. Е. Дернового (2023). Работы В.В. Фисуна касаются вопросов применения различных методик оценки защищенности объектов КИИ. Автор анализирует основные вопросы и сложности проведения процедуры вышеуказанной оценки, а также приводит рекомендации для упрощения процесса (Фисун, 2022: 62). Геополитические факторы и риски обеспечения безопасности КИИ рассматривают П. Карасев, Д. Стефанович (2022). На роль инициатив Президента РФ по объединению мировых усилий в деле обеспечения информационной безопасности обращает внимание П. Кобец (2022).

Обеспечение безопасности КИИ — вопрос, напрямую затрагивающий национальную безопасность любого государства. Национальная безопасность — это защищенность ключевых интересов страны от внутренних и внешних угроз, которая достигается проведением единой государственной политики в области обеспечения безопасности, системой мер экономического, политического и иного характера, адекватных угрозам жизненно важных интересов личности, общества и государства. Для устойчивого развития государства необходимо предотвращение,

обеспечение безопасности и работа по минимизации последствий кибератак, что может быть реализовано при межведомственном подходе (Абидов, 2022: 255).

В теории и практике информационной безопасности и государственного управления пока не выработано единого подхода к пониманию того, что считать «критически важной инфраструктурой». Например, в США в одном из законов говорится о том, что критически важная инфраструктура — это «системы и активы, физические или виртуальные, настолько жизненно важные для Соединенных Штатов, что их выход из строя или разрушение окажет пагубное воздействие на национальную безопасность, экономическую безопасность, общественное здравоохранение или общественную безопасность»[75]. Некоторые исследователи относят концепцию защиты инфраструктуры критической информации к междисциплинарным феноменам, поскольку она зависит от разработки оценок потенциальных угроз, определения надлежащих ответных и превентивных мер и, наконец, от предложения, применения и осуществления соответствующих стратегий (Pagnacco, 2021: 488). Возможно, это оказало влияние и на политические решения в отношении КИИ: несмотря на общее понимание необходимости обеспечения безопасности КИИ в рамках национальной безопасности, различные государства формируют разные модели своего участия в этом процессе. Государственное вмешательство в обеспечение защиты КИИ может варьироваться от чисто государственного (через совместные соглашения между государственным и частным секторами) до чисто рыночного (где теоретически правительство не играет никакой роли) (Assaf, 2008: 7).

В РФ 2017 г. принят Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[76], который определяет основные термины и ключевые понятия в сфере обеспечения безопасности КИИ: автоматизированная система управления (АСУ), безопасность КИИ, значимый объект КИИ, компьютерная атака, компьютерный инцидент, КИИ РФ, объекты КИИ, субъекты КИИ. Согласно Федеральному закону № 187-ФЗ, к КИИ относятся объекты КИИ и сети электросвязи, которые используются для осуществления взаимосвязи таких объектов, нарушение работы которых приведет к неблагоприятным последствиям. Важнейшая информационная инфраструктура может быть разбита по ключевым областям: возможности подключения, хостинг, безопасность, оборудование и программное обеспечение (Hyslop, 2007: 62).

В данном контексте кибератака определяется как целенаправленное вредоносное воздействие на объекты критической информационной инфраструктуры (КИИ) с целью нарушения или прекращения их работы. Таким образом, к КИИ можно отнести информацию, хранящуюся в технических средствах обработки, базах данных, системах, предназначенных для передачи данных по линиям связи,

---

[75] Patriot ACT // Electronic Privacy Information Center. 24.10.2001. URL: http://epic.org/ privacy/terrorism/hr3162.html (дата обращения 30.04.2025).

[76] О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 № 187-ФЗ // СПС КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 30.04.2025).

а также сами сети электросвязи. С учетом изложенного государственная система обеспечения безопасности КИИ в РФ — это комплекс мер и механизмов, направленных на обеспечение надежной защиты информационной инфраструктуры объектов, отнесенных к категории критической, от угроз и опасностей, которые могут привести к ее нарушению, разрушению или нанести системным объектам ущерб.

Для определения значимости объектов КИИ определен перечень показателей[77] по сферам влияния: социальная, политическая, экономическая, экологическая, значимость для обеспечения обороны страны, безопасности государства и правопорядка.

С принятием закона были созданы нормативные основы, регулирующие отношения всех участников в сфере КИИ — субъектов КИИ и государственных регуляторов данной сферы, а также описаны Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (ГосСОПКА) и Национального координационного центра по компьютерным инцидентам (далее — НКЦКИ) в рамках государственной политики в вопросах обеспечения безопасности КИИ РФ. Согласно Указу Президента РФ от 25 ноября 2017 г. № 569, федеральным органом исполнительной власти, который уполномочен в сфере обеспечения безопасности КИИ, выступает ФСТЭК России[78]. Именно ФСТЭК России осуществляет государственный контроль в этой сфере в виде плановых и внеплановых проверок с последующим составлением предписания в случае обнаружения нарушений, допущенных предприятиями и организациями. Федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, является ФСБ России[79].

К субъектам КИИ относятся государственные учреждения и органы, юридические лица и индивидуальные предприниматели[80], которые владеют объектами КИИ[81]. Обязательным и необходимым условием является ведение де-

---

[77] Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений: Постановление Правительства РФ от 08.02.2018 N° 127 // СПС КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_290595/ (дата обращения 30.04.2025).

[78] О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента РФ от 16.08.2004 N° 1085: Указу Президента РФ от 25.11.2017 N° 569 // СПС КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_447665/ (дата обращения 30.04.2025).

[79] О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 N° 187-ФЗ // СПС КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 30.04.2025).

[80] С 01.09.2025 в п. 8 ст. 2 вносятся изменения Федеральным законом N° 58-ФЗ от 07.04.2025: индивидуальные предприниматели будут исключены из числа субъектов КИИ. URL: https://www.garant.ru/products/ipo/prime/doc/411724730/ (дата обращения 30.04.2025)

[81] О безопасности критической информационной инфраструктуры...

ятельности субъекта в одной из перечисленных отраслей (здравоохранение; наука; транспорт; связь; энергетика; банковская сфера и иные финансовые сферы; топливно-энергетический комплекс; область атомной энергии; оборонная промышленность; ракетно-космическая промышленность; горнодобывающая промышленность; металлургическая промышленность; химическая промышленность; юридические лица и/или индивидуальные предприниматели, которые осуществляют взаимосвязь и взаимодействие данных отраслей и систем»[82]. Организации разного типа, работающие в одной из перечисленных областей и имеющие у себя объект критической информационной инфраструктуры (КИИ), являются субъектами КИИ. Но к субъектам КИИ принадлежат не только компании, которые ведут деятельность непосредственно в этих областях. В эту категорию входят также предприятия, у которых есть разрешение на работу в данных сферах. Кроме того, к субъектам КИИ относятся фирмы, в уставе которых прописан вид деятельности, подпадающий под приведенный перечень сфер.

В 2024 г. был запущен национальный проект «Экономика данных и цифровая трансформация государства», в состав которого включены федеральные проекты «Инфраструктура кибербезопасности» и «Отечественные решения»[83]. Данные проекты призваны решить накопившиеся проблемы в реализации государственной политики в сфере обеспечения безопасности КИИ.

Формы обеспечения безопасности КИИ выражаются в правотворческой, правореализационной, правоохранительной и контрольно-надзорной деятельности субъектов обеспечения безопасности КИИ. Экономические методы управления в сфере обеспечения безопасности КИИ осуществляются федеральными органами исполнительной власти (ФСТЭК России и ФСБ России) и компаниями, специализирующимися на информационной безопасности. Ответственными за исполнение данных методов являются руководители предприятий и уполномоченные государственные служащие.

Одним из основных управленческих объектов в исследуемой сфере и ключевой частью системы защиты КИИ РФ является процедура категорирования объектов КИИ, которую проводит самостоятельно субъект КИИ. Согласно законодательству организации самостоятельно составляют перечень процессов (управленческие, технологические, финансово-экономические, производственные и др.) и оценивают их критичность. Согласно установленному порядку[84] объекты КИИ классифицируются по трем категориям значимости: самая высокая категория — первая, самая низкая — третья. Для субъектов КИИ из числа государственных организаций указанная процедура носит *обязательный* характер, для субъектов КИИ из числа российских юридических лиц и/или индивидуальных предпринимателей указанная процедура носит *рекомендательный* характер.

---

82 Там же

83 Национальный проект «Экономика данных и цифровая трансформация государства» // Официальный сайт Правительства РФ. URL: http://government.ru/rugovclassifier/923/about/ (дата обращения 30.04.2025).

84 О безопасности критической информационной инфраструктуры…

При этом нормативные документы не предусматривают обязательных требований выполнения законодательства в вопросах присвоения категории значимости объектам КИИ, принадлежащим юридическим лицам, а также ими не определены нормативные сроки начала и завершения процесса категорирования информационных систем этих организаций. Для сравнения: в США политика стимулирования частных организаций к разработке собственных стандартов в сфере защиты КИИ (крупные организации и корпорации) либо согласие с оценкой/проверкой обеспечения безопасности государственными организациями (для субъектов малого и среднего бизнеса) — федеральный приоритет (Patterson, Personick, 2003: 5).

В апреле 2025 г. был принят Федеральный закон № 58-ФЗ[85], который изменил подход субъектов КИИ к оценке объектов КИИ и их категорированию: теперь отраслевые ведомства должны принять в качестве нормативного акта перечни типовых объектов КИИ и особенности категорирования таких объектов, а субъект КИИ больше не должен будет определять «критичность процессов», а ориентироваться на типовые перечни. Таким образом, самостоятельно субъекту КИИ больше не нужно определять критичность процессов и автоматизирующих их систем, согласуя это все со ФСТЭК, достаточно выбрать подходящие объекты из типовых перечней. Федеральный закон вступает в силу с 1 сентября 2025 г., поэтому в настоящей статье исследования строились на предыдущей версии ФЗ № 127.

Для выполнения задачи обеспечения безопасности КИИ субъекты КИИ несут финансовые затраты на:

1) «создание структурных подразделений, ответственных за защиту информации и обеспечения информационной безопасности;

2) поиск и наем сотрудников с необходимым уровнем компетенций в сфере обеспечения безопасности КИИ, оплату их обучения, курсов, семинаров по тематике защиты КИИ;

3) приобретение специализированного программного обеспечения, необходимого для обеспечения безопасности КИИ, и его эксплуатацию, включая обновление и поддержку;

4) оплату услуг, оказываемых специалистами специализированных организаций по информационной безопасности»[86].

Могут быть предусмотрены и финансовые издержки — штрафные санкции за несоблюдение законов и нормативных актов в области защиты информации. Получается, что юридические лица и ИП (относящиеся к посредникам в цепи услуг, деятельность которых косвенно затрагивает КИИ и пр.) при проведении категорирования объектов несут дополнительные расходы, а непроведение процедуры создает угрозы национальной безопасности.

---

[85] О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации»: Федеральный закон от 07.04.2025 N° 58-ФЗ (документ не вступил в силу) // СПС Гарант. URL: https://www.garant.ru/products/ipo/prime/doc/411724730/ (дата обращения 20.04.2025).

[86] О безопасности критической информационной инфраструктуры...

2. Методы и материалы исследования

Для достижения целей исследования использовался в первую очередь метод анализа документов, в качестве которых рассматривались теоретические источники: аналитические материалы государственных органов, осуществляющих политику в сфере обеспечения безопасности КИИ, и документы стратегического планирования в сфере обеспечения безопасности КИИ. Источниками для формально-юридического метода послужила система зарубежного (в частности, США) и отечественного законодательства в сфере обеспечения безопасности КИИ.

Эмпирической базой для анализа статистических данных послужили данные, содержащиеся в аналитических отчетах уполномоченных субъектов КИИ (а именно обращения субъектов КИИ, поступившие в УФСТЭК России по УрФО за 2021–2023 гг.), контент официальных сайтов уполномоченных органов, а также официальные страницы в социальных сетях.

В качестве количественного метода исследования применялся опросный метод. Опрос методом анкетирования среди 55 представителей субъектов КИИ Свердловской области в октябре 2023 г. (n = 55, примерно 8% от субъектов КИИ Свердловской области, прошедших процедуру категорирования).

В ходе исследования также применялся качественный метод — экспертное интервью. Экспертное интервью с руководителем уполномоченного территориального ФОИВ (очное, формализованное) происходило после обработки статистических данных и результатов анкетирования субъектов КИИ.

3. Результаты исследования

Анализ статических данных по обращениям субъектов КИИ, направленным в адрес УФСТЭК России по УрФО (табл. 1 и 2), показывает, что наиболее востребованная тема обращений в каждый исследуемый год остается неизменной — тема категорирования объектов КИИ, при этом количество обращений ежегодно увеличивается.

Таблица 1
Table 1

Количество обращений субъектов КИИ, в отношении которых УФСТЭК России по УрФО осуществляет контрольную деятельность (ранжирование тем обращений)

Number of referrals from CII subjects, in respect of which the Russian Federal Office for Trade and Industry carries out monitoring activities (ranking of referrals)

Номер строки	Тема обращения	Количество обращений за 2021 г.	Количество обращений за 2022 г.	Количество обращений за 2023 г.
1	Категорирование	5	7	8
2	Организация системы защиты объектов КИИ	2	1	2
3	Актуализация объектов КИИ	2	2	1

4	Квалификационные требования к должностным лицам, ответственным за обеспечение безопасности КИИ организации	1	1	2
5	Другие темы	1	1	2
6	Итого	11	12	15

Составлено авторами.

Количество обращений по оставшимся заявленным темам не меняется. Это подтверждает наличие противоречий в практике категорирования объектов КИИ в текущем законодательстве.

Таблица 2
Table 2

Количество обращений субъектов КИИ, в отношении которых УФСТЭК России по УрФО осуществляет контрольную деятельность (по сферам деятельности)

Number of referrals from CII subjects, in respect of which the Russian Federal Office for Trade and Industry carries out control activities (by areas of activity)

Номер строки	Сфера субъекта КИИ	Количество обращений за 2021 г.	Количество обращений за 2022 г.	Количество обращений за 2023 г.
1	Промышленность	5	3	1
2	Наука	1	1	2
3	Транспорт	5	8	11
4	Энергетика	0	1	1
	Итого	11	12	15

Составлено авторами.

Динамика обращений субъектов КИИ показывает разные тенденции в зависимости от отрасли. Так, в сфере транспорта наблюдается активизация процесса категорирования, что выражается в росте числа обращений; это говорит о том, что у субъектов КИИ при проведении категорирования своих объектов возникает наибольшее количество вопросов по данным процедурам. Вероятнее всего, причиной данного факта является отсутствие исчерпывающих разъяснений в методических рекомендациях УФСТЭК России по данным вопросам. В то же время в промышленности фиксируется стабильное снижение количества обращений, в сферах науки и энергетики количество обращений в целом не изменяется. Это говорит о том, что УФСТЭК России приняты достаточные меры по доведению и разъяснению установленных требований до субъектов КИИ в сфере промышленности.

Количество проведенных УФСТЭК России по УрФО координационно-методических советов (далее — КМС) показывает и приоритетные сферы, и тенденции к потребности организаций в обратной связи и взаимодействии (табл. 3).

Таблица 3
Table 3

Количество проведенных КМС (ранжирование по темам советов)

Number of CMC's conducted (Council Topic Ranking)

Номер строки	Сфера субъекта КИИ	Количество нарушений за 2021 г.	Количество нарушений за 2022 г.	Количество нарушений за 2023 г.
1	Промышленность	2	2	3
2	Наука	0	0	1
3	Транспорт	0	0	0
4	Энергетика	0	1	0
5	Общего назначения	1	1	1

Составлено авторами.

Ежегодно наибольшее количество КМС приводится в интересах и по вопросам промышленности (что логично, учитывая промышленную ориентацию макрорегиона — УрФО). УФСТЭК России по УрФО в наибольшей степени оказывал методическое сопровождение организациям и ИП по вопросам обеспечения безопасности объектов КИИ в сфере промышленности. В результате выбранная УФСТЭК России по УрФО политика по проведению тематических КМС в сфере промышленности в период 2021–2023 гг. оправдала свои ожидания, вследствие чего в указанный период количество обращений от субъектов КИИ с вопросами сокращалось. Вопросы сфер транспорта, науки и энергетики рассматривались только в рамках КМС общего назначения. КМС по профилю «Транспорт» за 2021–2023 гг. не проводились. Из-за отсутствия специализированных КМС для транспортной сферы количество обращений соответствующих субъектов КИИ в указанный период возрастает, что указывает на их недостаточную осведомленность в законодательстве в сравнении с субъектами промышленности.

Участники отношений в сфере использования КИИ оказываются недостаточно защищенными от воздействующих на них информационных техногенных факторов. Указанная уязвимость может быть обусловлена следующими факторами. Во-первых, программы профессиональной переподготовки специалистов в сфере защиты КИИ не успевают адаптироваться под динамично развивающиеся формы киберугроз на объекты КИИ. Например, программы направления «Безопасность значимых объектов КИИ» составляют лишь 9% от всех направлений информационной безопасности, согласованных ФСТЭК России.

Во-вторых, в 2023 г. среди специалистов в сфере информационной безопасности наблюдался дефицит на рынке труда, что подтверждается увеличением на 51% количества размещенных вакансий по отношению к году ранее.

Совместная деятельность органов публичной власти и организаций в области обеспечения КИИ — один из принципов открытости и установления доверительных отношений всех участников данного процесса. В соответствии с концеп-

цией открытости федеральных органов исполнительной власти УФСТЭК России по УрФО поддерживает информационное взаимодействие с системами «Мониторинг Госсайтов» и «Инфометр».

Кроме того, с целью повышения уровня открытости деятельности ФСТЭК России выполняются следующие мероприятия:

1) на официальном сайте ФСТЭК России размещен ведомственный порядок организации работы по обеспечению доступа к информации о деятельности ФСТЭК России, а также правила и условия использования контента сайта;

2) ежеквартально осуществлялся мониторинг разделов сайта на предмет актуальности размещаемой в них информации в целях своевременного внесения изменений и дополнений. Всего внесено 562 изменения в информационные ресурсы сайта, включающие размещение 230 новых информационных материалов, обновление 287 и удаление 45 документов по 170 заявкам;

3) проведены работы по обновлению программных средств (модулей, приложений, расширений), входящих в состав действующей версии системы управления контентом сайта;

4) обеспечены условия доступности сайта для инвалидов по зрению[87].

УФСТЭК России по УрФО работает совместно с другими федеральными органами исполнительной власти, органами местного самоуправления и организациями. Например, руководитель управления занимает должность заместителя председателя КМС по информационной безопасности при полномочном представителе Президента Российской Федерации в Уральском федеральном округе. Кроме того, осуществляется взаимодействие с расположенными на территории Уральского федерального округа территориальными органами федеральных органов исполнительной власти Российской Федерации, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, высшими учебными заведениями по подготовке специалистов по технической защите информации, предприятиями оборонно-промышленного комплекса и организациями.

Оценка открытости, доверия и вовлечения между участниками отношений в сфере обеспечения безопасности КИИ показала, что взаимоотношения между УФСТЭК России по УрФО и субъектами КИИ Свердловской области осуществляются на должном уровне.

Среди участников процедуры категорирования объектов КИИ был проведен опрос с целью установления основных проблемных моментов, связанных с управлением в этой сфере. Результаты анкетирования показали, что 80% участников столкнулись с трудностями при проведении категорирования своих объектов КИИ. При этом быстрее всех среди участников анкетирования процедуру категорирования завершили субъекты КИИ в сфере энергетики, а дольше всех — в сфере транспорта.

---

[87] Составлено авторами по информации на официальном сайте ФСТЭК России: Официальный сайт ФСТЭК России. URL: https://fstec.ru/territorialnye-organy/uralskij-federalnyj-okrug/deyatelnostufo/ofitsialnye-meropriyatiya-ufo (дата обращения 30.04.2025).

Большинство респондентов (76%) обозначили наличие проблем и трудностей в процессе категорирования, однако способы их решения в разных сферах различны. Так, участники в сфере промышленности их решали через КМС, субъекты КИИ в сфере науки — через официальный сайт ФСТЭК России, в сфере транспорта — через официальный сайт ФСТЭК России и специалистов УФСТЭК России по УрФО, в сфере энергетики — через официальный сайт ФСТЭК России и сторонние организации. Это свидетельствует о большей осведомленности промышленных предприятий об источниках получения необходимых для категорирования сведений от ФСТЭК России.

Кроме того, для обоснования актуальности причин сложившейся проблемной ситуации было проведено экспертное интервью руководителя УФСТЭК России по УрФО.

По мнению эксперта, «*при планировании проведения КМС учитываются интересующие субъектов КИИ вопросы. Проводится анализ наиболее встречающихся проблем, решение которых доводится публично до участников КМС. Наиболее проблемные вопросы и их решение публикуются на официальном сайте ФСТЭК России. Однако следует отметить, что планирование тематических КМС, например для конкретной сферы деятельности субъектов КИИ, на основании поступивших тематик обращений в УФСТЭК России по УрФО и ФСТЭК России не предусмотрено и не осуществляется*». Соответственно такая результативная практика, как работа в рамках КМС по возникающим вопросам субъектов КИИ в определенной сфере, фактически зависит от активности и осведомленности самих субъектов КИИ.

Также эксперт отметил, что «*информация, размещаемая ФСТЭК России на официальном сайте, актуализируется 1 раз в квартал. У каждой сферы деятельности присутствуют свои специфика, особенности и проблемные моменты в процессе категорирования. Каждая сфера руководствуется различными НПА и показателями при определении категории значимости объектов КИИ. Поэтому считаю, что УФСТЭК России по УрФО для организации адресной методической помощи субъектам КИИ целесообразно проводить так называемые тематические КМС, ориентированные на конкретные сферы деятельности*». Действительное, такие тематические КМС позволят более детально проработать проблемные вопросы, которые в остальных сферах не встречаются. Такой формат на данном этапе работы в области обеспечения безопасности КИИ позволит более эффективно использовать возможности проводимых КМС.

Эксперт также подтвердил актуальность проблемы категорирования среди субъектов КИИ, уточнив, что количество обращений от организаций в УФСТЭК России по УРФО по указанной теме стабильно увеличивается каждый год: «*в настоящее время больше всего интересуют субъекты КИИ вопросы из категории "Категорирование", значительно меньше — категории "Организация системы защиты объектов КИИ", "Актуализация объектов КИИ", "Квалификационные требования к должностным лицам, ответственным за обеспечение безопасности КИИ организации"*». Свой вывод эксперт подтвердил

статическими данными из обращений субъектов КИИ, направленных в адрес УФСТЭК России по УрФО в 2021–2023 гг.

Заключение

Безопасность КИИ в РФ — это не только техническая, но и стратегическая задача. Ее решение требует комплексного подхода: от законодательных инициатив и импортозамещения до повышения квалификации персонала и внедрения передовых технологий защиты. Обеспечение безопасности КИИ в РФ в настоящее время — важное условие обеспечения национальной безопасности. Информационные системы, информационно-технические системы, автоматизированные информационные системы и прочие ресурсы, которые сегодня составляют информационную экосистему государства, являются общими элементами сети, связывающей абсолютно все организации. Соответственно уязвимости в отдельно взятой организации могут нанести серьезный ущерб государственным информационным системам, с которыми работают органы публичной власти. Предельно важно, чтобы процесс обеспечения безопасности КИИ оставался прозрачным и доверительным для всех участников — субъектов КИИ, а также простым, без дополнительной административной и финансовой нагрузки, учитывая рекомендательный характер процедур категорирования.

Одним из вариантов решения проблемы могут стать регулярные тренинги или онлайн-занятия для всех участников системы КИИ безопасности, в том числе в рамках противодействия технологиям социальной инженерии, категорирования объектов КИИ и обеспечения простых условий физической безопасности инфраструктурных объектов.

Проведенное исследование показало, что процедура категорирования объектов КИИ сложна для субъектов КИИ, особенно тех, кто является коммерческими и некоммерческими предприятиями. Вариантом решения проблемы будет совершенствование законодательной базы по вопросам категорирования объектов КИИ, что позволит облегчить этот процесс и повысить прозрачность процедур, а также изменить подходы в соответствии с отраслевыми особенностями (что и было предусмотрено в принятом, но пока не вступившем в силу ФЗ № 58).

Оценка открытости, доверия и вовлечения между участниками отношений в сфере обеспечения безопасности КИИ показала, что взаимоотношения между УФСТЭК России по УрФО и субъектами КИИ Свердловской области реализуются в соответствии с требованиями законодательства. Однако в процессе взаимоотношений не все субъекты КИИ можно назвать партнерами, далеко не всем известны тонкости процедуры и потенциал взаимодействия. Это приводит к отсутствию адресной методической помощи по вопросам категорирования объектов КИИ со стороны государственного регулятора — УФСТЭК России по УрФО: проводимые УФСТЭК России по УрФО КМС по вопросам КИИ не учитывают поступившие тематики обращений от субъектов КИИ; проведение тематических КМС, ориентированных на конкретную сферу деятельности субъектов КИИ и предоставление адресной методической помощи, не предусмотрено и не осуществляется.

Возможно, эти проблемы можно снять за счет создания системы непрерывного обучения субъектов КИИ, в которое будут вовлекаться образовательные учреждения региона, обеспечивающие подготовку специалистов в рамках информационной безопасности.

СПИСОК ИСТОЧНИКОВ

Абидов Р. Р. Кибератаки на критическую информационную инфраструктуру, как угроза национальной безопасности // Пробелы в российском законодательстве. 2022. Т. 15, № 4. С. 251–255.

Аккаева Х. А. Кибератаки на критическую информационную инфраструктуру // Право и управление. 2023. № 9. С. 347–351. DOI: 10.24412/2224–9133–2023–9–347–351

Баянова Ю. А. Критическая информационная инфраструктура как объект обеспечения безопасности // Инновационная наука. 2021. № 10–2. С. 63–65.

Валенцев М. С. Критическая информационная инфраструктура: ответственность владельцев за нарушение ее функционирования // Синергия Наук. 2020. № 43. С. 685–689.

Карасев П. А., Стефанович Д. В. Кибербезопасность критически важной инфраструктуры: новые вызовы // Россия в глобальной политике. 2022. Т. 20, № 6. С. 147–164. DOI 10.31278/1810–6439–2022–20–6–147–16

Кобец П. Н. Роль Президента Российской Федерации В. В. Путина в объединении усилий мирового сообщества по совершенствованию информационной безопасности в киберпространстве // Правопорядок: история, теория, практика. 2022. № 2. С. 62–68.

Кривоносов И. М., Дерновой А. Е. Критическая информационная инфраструктура — новые понятия и аспекты безопасности в современных реалиях // Гидротехника. 2023. № 2. С. 54–56. DOI 10.55326/22278400_2023_2_54.

Кузнецов С. А., Куликов И. А., Фоминых А. А. Сравнение КИИ и методов категорирования КИИ в РФ и США // Актуальные научные исследования в современном мире. 2021. № 6–1. С. 63–68.

Новые горизонты развития системы информационного права в условиях цифровой трансформации / отв. ред.: Т. А. Полякова, А. В. Минбалеев, В. Б. Наумов. М.: Институт государства и права РАН, 2022. 368 с.

Пекарева В. В. Критическая информационная инфраструктура как объект уголовно-правовой охраны // Вестник общественной научно-исследовательской лаборатории «Взаимодействие уголовно-исполнительной системы с институтами гражданского общества: историко-правовые и теоретико-методологические аспекты». 2024. № 35. С. 120–127.

Полякова Т. А., Антопольский А. А. и др. Об основных направлениях развития информационного права за 2000–2015 гг. // Государство и право. 2017. № 1. С. 71–79.

Стрельцов А. А., Капустин А. Я., Полякова Т. А. и др. Международная безопасность в среде информационно-коммуникационных технологий. М.: НАМИБ, 2023. 132 с.

Фисун В. В. Методика оценки защищенности в интеллектуальной системе управления информационной безопасностью объектов критической информационной инфраструктуры // Национальная Ассоциация Ученых. 2022. № 77. С. 59–62. DOI: 10.31618/nas2413–5291.2022.1.77.575

Assaf D. Models of critical information infrastructure protection // International Journal of Critical Infrastructure Protection. 2008. Vol. 1. P. 6–14. DOI: 10.1016/j.ijcip.2008.08.004

Hyslop M. Critical Information Infrastructure. Springer US, 2007. P. 61–76.

Pagnacco A. Critical Information Infrastructure Protection: Between Cybersecurity and Policymaking // ITASEC. 2021. С. 488–498.

Patterson C. A., Personick S. D. (ed.). Critical information infrastructure protection and the law: an overview of key issues. Washington DC: National academy press. 2003. 93 p.

REFERENCES

Abidov, R. R. (2022). Cyber attacks on critical information infrastructure as a threat to national security. *Probely v rossijskom zakonodatel'stve*, *15*(4), 251–255. (In Russ.).

Akkaeva, Kh. A. Cyber attacks on critical information infrastructure. *Pravo i upravlenie*, *9*, 347–351. DOI: 10.24412/2224–9133–2023–9–347–351

Bajanova, Ju. A. (2021). Critical information infrastructure as a security object. *Innovacionnaya nauka*, *10–2*, 63–65. (In Russ.).

Valencev, M. S. (2020). Critical information infrastructure: ownership responsibility for disruption. *Sinergiya Nauk*, *43*, 685–689. (In Russ.).

Karasev, P. A., Stefanovich, D. V. (2022). Cybersecurity of the critical infrastructure: new challenges. *Rossiya v global'noj politike, 20*(6), 147–164. DOI: 10.31278/1810–6439–2022–20–6–147–164 (In Russ.).

Kobets, P. N. (2022). The Role of the President of the Russian Federation V. V. Putin in Combining the Efforts of the World Community to Improve Information Security in Cyberspace. *Pravoporjadok: istoriya, teoriya, praktika*, *2*, 62–68. (In Russ.).

Krivonosov, I. M., Dernovoj, A. E. (2023). Critical information infrastructure — new concepts and aspects of security in modern realities. *Gidrotehnika*, *2*, 54–56. (In Russ.). DOI 10.55326/22278400_2023_2_54

Kuznetsov, S. A., Kulikov, I. A., Fominykh, A. A. (2021). Comparison of critical infrastructure and methods of categoring critical infrastructure in Russian Federation and USA. *Aktual'nye nauchnye issledovaniya v sovremennom mire*, *6–1*, 63–68. (In Russ.).

Poljakova, T. A., Minbaleev, A. V., Naumov, V. B. (ed). (2022). *New horizons for the development of the information law system in the context of digital transformation.* Moskva: Institut gosudarstva i prava RAN. (In Russ.).

Pekareva, V. V. (2024). Critical information infrastructure as an object of criminal law protection. *Vestnik obshchestvennoj nauchno-issledovatel'skoj laboratorii «Vzaimodejstvie ugolovno-ispolnitel'noj sistemy s institutami grazhdanskogo obshchestva: istoriko-pravovye i teoretiko-metodologicheskie aspekty»*, *35*, 120–127. (In Russ.).

Poljakova, T. A., Antopol'skij, A. A., et al. (2017). On the main directions of development of information law for 2000–2015. *Gosudarstvo i parvo*, *1*, 71–79. (In Russ.).

Strel'cov, A. A., Kapustin, A. Ja., Poljakova, T. A., et al. (2023). *International security in the information and communication technology environmen*t. Moskva: NAMIB. (In Russ.).

Fisun, V. V. (2022). Security assessment methodology in the intelligent information security management system of critical infrastructure objects. *Nacional'naya Associaciya Uchenyh*, *77*, 59–62. (In Russ.). DOI: 10.31618/nas2413–5291.2022.1.77.575

Assaf, D. (2008). Models of critical information infrastructure protection. *International Journal of Critical Infrastructure Protection*, *1*, 6–14. DOI: 10.1016/j.ijcip.2008.08.004

Hyslop, M. (2007). *Critical Information Infrastructure*. New-York: Springer US.

Pagnacco, A. (2021). Critical Information Infrastructure Protection: Between Cybersecurity and Policymaking. *ITASEC*, 488–498.

Patterson, C. A., Personick S. D. (ed.) (2003). *Critical information infrastructure protection and the law: an overview of key issues*. Washington DC: National academy press.

INFORMATION ABOUT THE AUTHORS / СВЕДЕНИЯ ОБ АВТОРАХ

Галина Алексеевна Банных — канд. социол. наук, доцент, доцент кафедры теории, методологии и правового обеспечения государственного и муниципального управления Уральского федерального университета им. Первого президента России Б.Н. Ельцина, Екатеринбург, Россия

Galina A. Bannykh — Dr. Sci. (Sociology), Associate Professor, Associate Professor of the Department of Theory, Methodology and Legal Support of State and Municipal Administration, Ural Federal University named after the First President of Russia B.N. Yeltsin, Yekaterinburg, Russia

Павел Владимирович Туктарев — магистрант кафедры теории, методологии и правового обеспечения государственного и муниципального управления Уральского федерального университета им. Первого президента России Б.Н. Ельцина, Екатеринбург, Россия

Pavel V. Tuktarev — Master's Degree Student of the Department of Theory, Methodology and Legal Support of State and Municipal Administration, Ural Federal University named after the First President of Russia B.N. Yeltsin, Yekaterinburg, Russia

Статья поступила в редакцию 24.07.2025;
одобрена после рецензирования 19.09.2025;
принята к публикации 19.09.2025.
The article was submitted 24.07.2025;
approved after reviewing 19.09.2025;
accepted for publication 19.09.2025.