DOI 10.37882/2223-2974.2026.01.26

К ВОПРОСУ О ПРАВОВОМ ОБЕСПЕЧЕНИИ ЗАЩИТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

ON THE ISSUE OF LEGAL PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE

D. Chaikovsky

Summary. The article is devoted to the analysis of the current state of legal support for the protection of critical information infrastructure in the Russian Federation. The author examines the theoretical and legal foundations of regulation. The paper analyzes the system of by-laws, primarily the documents of the FSTEC of Russia, and identifies problems of legal regulation. Special attention is paid to the problems of law enforcement, including low efficiency of administrative responsibility and staff shortage. In conclusion, ways to improve legal support are proposed, including: detailing and differentiating regulation by industry, creating incentive mechanisms, and legitimizing new technologies.

Keywords: critical information infrastructure (CI), legal support for CI protection, FSTEC of Russia, cyber threats.

Чайковский Дмитрий Станиславович
кандидат физ.-мат. наук, доцент, Саратовская государственная юридическая академия
chaikovskyds@yandex.ru

Аннотация. Статья посвящена анализу правового обеспечения защиты критической информационной инфраструктуры (КИИ) в Российской Федерации. Автор рассматривает теоретико-правовые основы регулирования. В работе проводится анализ системы подзаконных актов, прежде всего документов ФСТЭК России, выявляются проблемы правового регулирования. Особое внимание уделяется проблемам правоприменения, включая малую эффективность административной ответственности и кадровый дефицит. В заключении предлагаются пути совершенствования правового обеспечения, среди которых: детализация и дифференциация регулирования по отраслям, создание стимулирующих механизмов, правовая легитимизация новых технологий.

Ключевые слова: критическая информационная инфраструктура (КИИ), правовое обеспечение защиты КИИ, ФСТЭК России, киберугрозы.

Критическая информационная инфраструктура (КИИ) представляет собой совокупность информационных систем и телекоммуникационных сетей, обеспечивающих функционирование ключевых отраслей экономики и государства в целом. К ним относятся энергетика, здравоохранение, транспорт, связь, финансовая сфера, оборонно-промышленный комплекс и иные области, нарушение или прекращение функционирования которых ведет к тяжелым социально-экономическим, экологическим, политическим последствиям, угрожает национальной безопасности.

Теоретической основой правового регулирования защиты КИИ в России является концепция информационной безопасности, которая получила развитие в Стратегии национальной безопасности РФ [1] и Доктрине информационной безопасности [2]. Эти документы определяют КИИ как объект стратегической важности, защита которого требует специального правового режима. Основная цель регулирования — не просто защита информации как таковой, а обеспечение устойчивости и непрерывности жизненно важных процессов государства в условиях постоянно эволюционирующих киберугроз.

Основным нормативным актом, заложившим основы такого регулирования, стал Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Он ввел базовые понятия («субъект КИИ», «значимый объект КИИ», «кибератака»), установил принципы обеспечения безопасности, определил полномочия государственных органов (в первую очередь ФСТЭК и ФСБ) и обязанности субъектов КИИ. Данный закон создал рамочную конструкцию, детализация которой осуществляется через подзаконное нормотворчество.

Нормативно-правовая база в сфере защиты КИИ представляет собой многоуровневую систему. После принятия ФЗ-187 ключевую роль в ее наполнении сыграла Федеральная служба по техническому и экспортному контролю (ФСТЭК России). Был принят ряд основополагающих документов:

- Приказ ФСТЭК России от 25.12.2017 № 239 — утвердил детализированные Требования по обеспечению безопасности значимых объектов КИИ;
- Приказ ФСТЭК России от 21.12.2017 № 235 — установил порядок создания систем безопасности и обеспечения их функционирования;
- Приказ ФСТЭК России от 01.12.2023 № 240 — регламентировал процедуру оценки соответствия этим требованиям;
- «Методический документ. Методика оценки угроз безопасности информации»(утв. ФСТЭК России 05.02.2021) — утвердил новую методику модели-

рования угроз безопасности информации, обязательную для применения при планировании защиты.

Несмотря на внешнюю полноту, анализ данной системы выявляет ряд проблем.

Во-первых, проблема терминологической определенности и отграничения сфер регулирования. Понятийный аппарат ФЗ-187 остается достаточно широким. Это приводит к сложностям на этапе идентификации объектов КИИ, особенно в условиях распределенных и межотраслевых систем. Существуют значительные пересечения с законодательством о персональных данных (152-ФЗ) и о коммерческой тайне, что порождает дублирование обязанностей и коллизии для организаций, подпадающих под действие нескольких законов одновременно. Размытость границ предмета регулирования создает риски как избыточного администрирования, так и пробелов в защите.

Во-вторых, сложность и формализм требований ФСТЭК. Выполнение требований, изложенных в Приказе № 239, требует огромных ресурсов, что особенно тяжело для организаций среднего бизнеса, которые, однако, могут являться частью цепочки критически важных процессов. На практике это может привести к двум негативным сценариям: либо к формальному подходу, когда меры безопасности имитируются для получения положительного заключения по Приказу № 240, либо к полной невозможности соответствовать требованиям для малых и средних субъектов КИИ.

В-третьих, негибкость регулирования в условиях технологической динамики. Законодательство и подзаконные акты закрепляют подходы, ориентированные на традиционные, изолированные информационные системы. Однако современная цифровая трансформация основана на облачных сервисах, интернете вещей (IoT), использовании сторонних платформ. Правовой статус таких решений в контексте КИИ, вопросы ответственности провайдеров облачных услуг, требования к импортному программному обеспечению остаются недостаточно проработанными. Это создает «серые зоны» и замедляет технологическое обновление критически важных отраслей.

В-четвертых, недостаточность правовых механизмов обмена информацией. Эффективное противодействие сложным кибератакам невозможно без оперативного обмена данными об угрозах и уязвимостях между субъектами КИИ и государством. Однако действующее законодательство, например, защищая коммерческую тайну, создает правовые барьеры для такого обмена. Страх гражданско-правовой или репутационной ответственности за разглашение информации об инциденте часто перевешивает потенциальную пользу.

Проблемы правоприменения тесно связаны с выявленными законодательными пробелами. Административная ответственность за нарушение требований безопасности КИИ (ст. 13.12.1 КоАП РФ) применяется недостаточно активно. Сложность заключается в процедуре доказывания факта нарушения и причинно-следственной связи. Кроме того, санкции в виде крупных штрафов или приостановления деятельности для критически важного объекта могут оказаться контрпродуктивными, парализовав его работу. Это сдерживает регулятора от их широкого применения, снижая превентивный эффект закона. Кроме того, наблюдается сложность в квалификации неправомерного воздействия на КИИ, это объясняется тем, что ст. 274.1 УК РФ содержит несколько самостоятельных форм преступного посягательства неправомерного воздействия на КИИ России [3].

Еще одной практической проблемой является кадровый дефицит. Отсутствие достаточного количества квалифицированных специалистов по информационной безопасности, понимающих как технические аспекты, так и специфику правового регулирования КИИ, является серьезным препятствием для реализации установленных требований.

Для преодоления обозначенных проблем необходима комплексная модернизация правового обеспечения защиты КИИ по следующим направлениям:

Детализация и дифференциация регулирования. Целесообразно разработать и внедрить отраслевые профили требований безопасности, учитывающие специфику и реальный уровень рисков в энергетике, транспорте, здравоохранении и т.д. Это позволит уйти от универсальных, зачастую избыточных предписаний.

Внедрение риск-ориентированного подхода [4]. Регулирование должно смещаться от формального соблюдения списка мер к управлению рисками. Это предполагает большую гибкость для субъектов КИИ в выборе конкретных средств защиты, адекватных выявленным угрозам, при усилении контроля со стороны регулятора за самим процессом управления рисками.

Создание стимулирующих механизмов. Помимо карательных мер, необходимо развитие инструментов государственной поддержки: налоговых льгот, субсидий, программ компенсации затрат на внедрение средств защиты для субъектов КИИ, особенно малого и среднего бизнеса.

Правовая легитимизация новых технологий. Требуется ускоренная разработка и принятие нормативных актов, регламентирующих использование облачных вычислений, больших данных [5], IoT-устройств [6], искусственного интеллекта в контуре КИИ, с четким опреде-

лением зон ответственности заказчиков и поставщиков услуг.

Таким образом, правовое обеспечение защиты КИИ в России находится на этапе развития. Созданный нормативный массив, по мнению автора, нуждается в совершенствовании, направленном на преодоление избыточной формализации и стимулировании повышения киберустойчивости критически важных объектов государства.

ЛИТЕРАТУРА

1. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // «Собрание законодательства РФ», 05.07.2021, N 27 (часть II), ст. 5351.
2. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»// «Собрание законодательства РФ», 12.12.2016, N 50, ст. 7074.
3. Евдокимов К.Н. Вопросы квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (по материалам судебной практики) // Российский следователь. 2023. № 5. С. 15–19.
4. С.Д. Ерохин, А.Н. Петухов, П.Л. Пилюгин Особенности управления информационной безопасностью критических информационных инфраструктур // Радиоэлектронные устройства и системы для инфокоммуникационных технологий» («РЭУС-ИТ 2024»): Доклады Всероссийской конференции, посвященной Дню радио, Москва, 31 мая 2024 года. Москва: Российское научно-техническое общество радиотехники, электроники и связи им. А.С. Попова, 2024. С. 378–382.
5. Чайковский Д.С. Средства обработки больших данных // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2018. № 12. С. 101–105.
6. Чайковский Д.С., Изотова В.Ф. Правовое регулирование Интернета вещей: современное состояние и перспективы развития // Современная наука: актуальные проблемы теории и практики. Серия: Экономика и право. 2025. № 6. С. 182–186.
7. Optimizing the implementation of university digitalization practices / N.N. Kovaleva, P.V. Eresko, V.F. Izotova, Ye.R. Gafarov // European proceedings of social and behavioural sciences: International Scientific and Practical Conference «State and Law in the Context of Modern Challenges» (SLCMC 2021), Саратов, 17 июня 2021 года / Editor(s): Sergey Afanasyev, Alexander Blinov, Sergey Belousov. Vol. 122. Саратов: European Publisher, 2022. P. 353–359.
8. Данилова М.А. Цифровые технологии современного офиса//Вестник Саратовского государственного социально-экономического университета. 2020. № 2 (81). С. 10–12.
9. Ересько П.В. Создание и модификация шаблонов типовых юридических документов компьютерными программными средствами // Вестник Саратовской государственной академии права. — 2008. — № 6(64). — С. 135–139.
10. Данилова М.А. Искусственный интеллект в юридической практике: новые вызовы и возможности для повышения эффективности // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и Технические Науки, 2025. №04-2. С. 70–72.

Журнал «Современная наука: актуальные проблемы теории и практики»