

ЗАЩИТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ (КИИ) В РОССИЙСКОЙ ФЕДЕРАЦИИ В УСЛОВИЯХ ГИБРИДНЫХ УГРОЗ

Автор:

Макаревич Полина Александровна,

*член Молодёжного совета Координационного центра доменов .RU/. РФ,
студентка 3 курса бакалавриата, факультет международных отношений
Санкт-Петербургского государственного университета*

Аннотация. В статье исследуется система защиты критической информационной инфраструктуры (КИИ) Российской Федерации в условиях современных гибридных угроз. Автором анализируется эволюция нормативно-правовой базы, современные механизмы и технологии защиты, а также ключевые вызовы, включая проблемы импортозамещения и кадрового дефицита. На основе проведённого анализа формулируются рекомендации по совершенствованию киберустойчивости КИИ в стратегической перспективе.

Ключевые слова: критическая информационная инфраструктура, гибридные угрозы, кибербезопасность, нормативно-правовое регулирование.

Введение

К 2026 году цифровая трансформация достигла уровня, при котором устойчивость критической информационной инфраструктуры (КИИ) стала неотъемлемым элементом национальной безопасности. Поскольку КИИ обеспечивает жизненно важные функции государства и общества, её уязвимость

представляет собой прямую стратегическую угрозу. Особую остроту этой проблеме придает современный гибридный контекст, характеризующийся последствиями пандемии, перманентным противостоянием в информационной сфере и санкционным давлением, оказываемым на Российскую Федерацию.

Существующая в Российской Федерации система правового регулирования (базирующаяся, в частности, на законе о безопасности КИИ [9]) демонстрирует разрыв между формальными требованиями и реальной практикой их реализации большинством субъектов КИИ. Основными проблемными зонами остаются недостаточная эффективность мер по обнаружению целевых атак, дефицит квалифицированных кадров и неполное выполнение требований по организационной и технической защите.

Понятие и структура КИИ в России

Ключевым нормативным актом, регулирующим деятельность по обеспечению безопасности критической информационной ин-

фраструктуры (КИИ) в Российской Федерации, является Федеральный закон от 26.07.2017 № 187-ФЗ “О безопасности критической информационной инфраструктуры Российской Федерации”. В нём же сформулировано точное определение, в котором под КИИ подразумеваются “объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов” [9]. При этом непосредственно к объектам КИИ относятся информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления субъектов критической информационной инфраструктуры. Таким образом, структурно КИИ формируют субъекты (организации-владельцы) и принадлежащие им объекты (технические системы).

К субъектам КИИ закон относит организации в сферах государственного управления, обороны, безопасности, здравоохранения, науки, транспорта, связи, энергетики, банковской и иных областей финансового рынка, топливно-энергетического комплекса, в области информационных технологий и других, чья деятельность критически важна для устойчивого функционирования общества и государства. К объектам КИИ, соответственно, относятся технологические и бизнес-системы этих организаций: автоматизированные системы управления технологическими процессами (АСУ ТП), корпоративные информационные системы, базы данных, центры обработки данных и т.д.

Широкий спектр гибридных угроз, включающий, помимо прочего, инструменты экономического давления, информационно-психологического воздействия и кибервойны [5], делает КИИ одной из наиболее приоритетных мишеней для атак. Например, с июля по сентябрь 2025 года было выявлено более 42 тысяч атак, это 40% от общего числа инцидентов за год и на 73% больше, чем за аналогичный период прошлого года. При этом количество высококритичных инцидентов в третьем квартале достигло 7,6 тысяч [10]. Данные показатели свидетельствуют о системном и целенаправленном характере угроз. Однако в сфере кибербезопасности и защиты критической информационной инфраструктуры сохраняется сложная и неоднозначная ситуация. Возникают случаи, когда привлечь к ответственности лиц, осуществляющих умышленные вредоносные атаки, не представляется возможным. Это происходит из-за ряда факторов, таких как нахождение преступников вне юрисдикции российского законодательства, низкий уровень согласованности правовых норм об экстрадиции, а также частое использование киберпреступников в качестве инструмента для дестабилизации социально-политической обстановки в России [2, с. 85].

Нормативно-правовые и организационные основы защиты КИИ в РФ

Эволюция правового регулирования защиты критической информационной инфраструктуры в Российской Федерации началась с формирования концептуальных основ в середине 2000-х годов. Отправной

точкой стал документ Совета Безопасности от 2005 года, установивший системные признаки критически важных объектов. Затем, в 2007 году, Федеральная служба по техническому и экспортному контролю России (ФСТЭК), являющаяся одним из главных органов в данной области, выпустила основополагающие руководящие документы, заложившие методическую базу для анализа угроз и требований к безопасности ключевых систем информационной инфраструктуры (КСИИ). Дальнейшее развитие получило целевую направленность с принятием Указа Президента №803 от 2012 года, сфокусированного на безопасности автоматизированных систем управления технологическими процессами (АСУ ТП), что было детализировано в приказе ФСТЭК 2014 года. Принципиальным этапом стало утверждение Доктрины информационной безопасности в 2016 году [6], создавшей стратегический контекст для последующего законодательства.

Ключевым законодательным актом, сформировавшим полноценную правовую систему защиты КИИ, стал уже упомянутый Федеральный закон №187-ФЗ “О безопасности критической информационной инфраструктуры Российской Федерации” от 26 июля 2017 года [9]. На его основе был принят комплекс подзаконных нормативных правовых актов в 2017-2019 годах, включая постановления Правительства о категорировании объектов КИИ и государственном контроле, а также многочисленные приказы ФСТЭК и ФСБ России, которые установили детальные

требования к безопасности значимых объектов КИИ, порядку реагирования на компьютерные инциденты и функционированию Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). Современный этап, начиная с 2022 года, характеризуется сдвигом в сторону обеспечения технологического суверенитета и импортонезависимости КИИ. Это закреплено в Указе Президента РФ №166 (2022) “О мерах по обеспечению технологической независимости и безопасности КИИ” [7]. Реализация данной политики предполагает не только ужесточение требований к программному обеспечению и оборудованию (вплоть до запрета использования иностранного), но и ускоренное развитие отечественных решений, проведение дополнительных исследований устойчивости КИИ в условиях целенаправленного воздействия на цепочки поставок и сервисного обслуживания. Также продолжается активная разработка отраслевых перечней типовых объектов КИИ и методических документов, таких как методика ФСТЭК 2024 года по оценке состояния технической защиты.

Формирование и эволюция нормативно-правовой базы защиты КИИ в РФ во многом является ответом на нарастающий характер гибридных угроз, где кибер- и информационно-технические воздействия становятся ключевым инструментом для достижения стратегических целей без объявления открытого конфликта. Законодательные ново-

введения, особенно после 2017 года, направлены на создание устойчивой к таким комплексным воздействиям системы, интегрирующей техническую защиту, оперативное обнаружение атак и централизованное управление инцидентами.

Основными регуляторами в сфере защиты критической информационной инфраструктуры являются ФСТЭК России и ФСБ России. Если обратить внимание на разделение полномочий между органами власти, то складывается следующая картина: Правительство Российской Федерации устанавливает ключевые процедуры, включая порядок категорирования объектов КИИ по степени значимости (социальная, политическая, экономическая, экологическая, оборонная и для безопасности государства), что является ключевым организационным механизмом, введенным Ф3-187. Установленная категория напрямую определяет объем и строгость применяемых требований по безопасности, что позволяет дифференцированно и рационально распределять ресурсы на защиту, фокусируясь на наиболее критических объектах в условиях гибридных угроз. Помимо этого Правительство РФ осуществляет организацию государственного контроля в области их безопасности, а также правила подготовки сетей связи для их функционирования. ФСТЭК России, в свою очередь, отвечает за ведение реестра значимых объектов КИИ, непосредственную разработку требований по информационной безопасности и контроль за их исполнением, включая проверку правильности категорирования [1, с.

500]. ФСБ России сосредоточена на создании и эксплуатации ГосСОПКА, обеспечивает подключение к ней объектов КИИ, осуществляет управление инцидентами информационной безопасности, а также проводит оценку защищенности этих объектов.

Современные механизмы и технологии защиты КИИ от гибридных угроз

Важной практической технологией является обязательная категоризация объектов КИИ и их сегментирование по степени значимости, что, как уже было упомянуто, позволяет дифференцировать меры защиты. Для объектов первой и второй категорий значимости вводятся строгие требования, включая использование только сертифицированных средств защиты информации (СЗИ), имеющих сертификаты ФСТЭК и ФСБ России, таких как межсетевые экраны, системы обнаружения вторжений (СОВ) и предотвращения утечек (DLP) [4]. Активно внедряются отечественные аппаратно-программные комплексы, например, на базе операционных систем «Астра Линукс» и «РЕД ОС», которые обеспечивают защиту данных до уровня государственной тайны «особой важности» и позволяют снизить зависимость от иностранного ПО, уязвимого для санкционных ограничений.

Одной из технических мер по защите КИИ в РФ является сегментация сетей, которая проводится не только по функциональному признаку, но и с обязательным выделением технологических сегментов, управляющих критически важными процессами, которые

изолируются физически или логически. Используемые системы обнаружения и предотвращения вторжений (IDS/IPS), такие как отечественные разработки “Киберпротект” или “АПКШ Континент”, проходят обязательную сертификацию в ФСТЭК России и настраиваются под специфику конкретного объекта, включая сигнатуры атак на АСУ ТП. Это позволяет не только детектировать известные угрозы, но и блокировать неестественную активность в реальном времени. Мониторинг всей этой совокупности событий безопасности обеспечивается SIEM-системами (например, российскими “MaxPatrol SIEM” или “Solar SIEM”), которые агрегируют данные с сетевого оборудования, СОВ, антивирусов и журналов аудита. Их настройка ведётся с учётом профилей типовых атак на КИИ, определённых регулятором, а корреляционные правила позволяют выявлять сложные многоэтапные компрометации, характерные для гибридных угроз.

Особую роль играют средства криптографической защиты информации (СКЗИ), сертифицированные ФСБ России по требованиям безопасности информации (например, семейство “КриптоПро”). Они используются не только для защиты каналов связи, но и для обеспечения целостности и подлинности программного обеспечения и команд управления в технологических системах. Для противодействия деструктивному воздействию, ставшему отличительным признаком современных гибридных атак, закреплены жёсткие требования к технологиям резерв-

ного копирования и обеспечению отказоустойчивости. Для объектов высших категорий значимости создаются изолированные, физически защищённые резервные центры обработки данных (ЦОДы), а часто и полностью дублированные технологические линии. Политики резервного копирования предписывают хранение копий критически важных данных и конфигураций на автономных, не подключаемых к сети носителях, что является ключевой практикой защиты от вирусов-шифровальщиков и целенаправленного саботажа.

В условиях гибридных угроз особое внимание уделяется защите от целевых атак (APT) и деструктивного ПО, что подтверждается опытом отражения таких инцидентов, как атаки вирусов-шифровальщиков на объекты инфраструктуры. Помимо технических мер, реализуется комплекс организационных практик: создание собственных CERT-команд (команд реагирования на компьютерные инциденты) в организациях КИИ, их взаимодействие с Национальным координационным центром по компьютерным инцидентам (НКЦКИ), а также постоянный мониторинг угроз на основе информации от спецслужб. Для противодействия информационно-психологическому компоненту гибридных угроз, направленному на персонал, проводится обязательное обучение и аттестация ответственных сотрудников, внедряются политики безопасности и модели нарушителя.

Таким образом, все перечисленные технические меры, работая в связке с организационными, формируют фундамент киберустойчивости, позволяя не только предотвращать инциденты, но и гарантировать восстановление нормального функционирования КИИ в минимальные сроки даже в случае успешной реализации гибридной угрозы. В целом, можно отметить, что современный российский подход к защите КИИ представляет собой симбиоз жёсткого нормативного регулирования, централизованного сбора и анализа угроз, импортозамещения ключевых технологий и наращивания компетенций по киберустойчивости непосредственно на объектах.

Проблемы и пути совершенствования системы защиты КИИ

Несмотря на активное нормативное регулирование и внедрение практических мер по защите КИИ в условиях гибридных угроз, остается комплекс ключевых вызовов, препятствующий достижению гарантированной сохранности инфраструктуры. Одним из наиболее острых является внутренний вызов, связанный с неполным соответствием многих организаций-субъектов КИИ требованиям законодательства, в частности, Федерального закона №187-ФЗ. По результатам проверки 700 значимых объектов КИИ, ФСТЭК России выявила свыше 1,2 тыс. нарушений, а минимальный уровень киберзащиты достигнут лишь у 36% организаций [8]. Несмотря на истечение установленных сроков, значительное число компаний, особенно в регионах и в негосударственном

секторе, до сих пор не завершили в полном объеме мероприятия по категорированию объектов КИИ и внедрению систем безопасности, что создает “прорехи” в общей системе защиты. Эта проблема усугубляется дефицитом квалифицированных кадров в области кибербезопасности и отстранением ИБ-специалистов от бизнес-процессов, что, как отмечает представитель ФСТЭК РФ, приводит к невозможности своевременного реагирования на инциденты [8].

Внешний вызов определяется беспрецедентным санкционным давлением и действиями недружественных государств в киберпространстве, что было многократно подтверждено, в том числе в заявлениях ФСБ России и НКЦКИ [3]. Ограничения на поставки высокотехнологичного зарубежного оборудования и программного обеспечения, включая средства защиты информации, вынуждают осуществлять импортозамещение в сжатые сроки, что зачастую приводит к внедрению менее зрелых и протестированных отечественных решений, потенциально снижая общий уровень защищенности на переходный период. Санкции также затрудняют международное сотрудничество по обмену данными об угрозах и лучшими практиками, изолируя российских специалистов от глобального опыта, что в долгосрочной перспективе может привести к отставанию в понимании развивающихся тактик и техник гибридного противодействия.

Исходя из существующих мер и практик, а также вызовов, можно предложить следующие ключевые рекомендации по защите КИИ в РФ от гибридных угроз:

1. Разрабатывать и ежегодно актуализировать стратегические планы защиты КИИ на 3-5 лет, интегрированные в общую стратегию кибербезопасности организаций.
2. Ежегодно актуализировать модель угроз КИИ с фокусом на гибридные сценарии, сочетающие кибератаки, информационно-психологическое воздействие и физическую дестабилизацию, а также регулярно проводить сценарный анализ и моделирование гибридных инцидентов.
3. Обеспечить регулярное целевое обучение специалистов по безопасности КИИ, включая актуальные угрозы, стандарты и практики, проводить ежегодные комплексные киберучения с отработкой гибридных сценариев противодействия.
4. Формализовать требования по кибербезопасности для всех поставщиков и подрядчиков, взаимодействующих с инфраструктурой КИИ, в том числе путем проведения аудита безопасности критических сторонних компонентов и программного обеспечения, используемого в КИИ.
5. Активно участвовать в рабочих группах и экспертных комитетах по кибербезопасности и защите КИИ в рамках международных объединений с участием РФ, таких как БРИКС, ШОС и СНГ, содействуя выработке и гармонизации общих принципов,

стандартов и критериев безопасности КИИ, учитывающих национальные особенности и суверенитет государств-участников.

Заключение

Сформированная к 2026 году нормативно-правовая база в области защиты КИИ создала необходимый каркас для обеспечения киберустойчивости. Однако, несмотря на прогресс в области регулирования и внедрения технологий, система защиты КИИ сталкивается с системными вызовами. В геополитическом измерении, учитывая эскалацию гибридного противостояния, можно прогнозировать дальнейшую консолидацию национальных систем защиты КИИ и их ориентир на замкнутые технологические контуры. Одновременно, для России остаётся критически важным сохранение и развитие каналов международного сотрудничества в области кибербезопасности в рамках БРИКС, ШОС и других объединений, что позволит гармонизировать подходы и противостоять общим угрозам, не жертвуя технологическим суверенитетом.

Таким образом, защита КИИ в России эволюционирует от задачи обеспечения базовой технической защищённости к формированию комплексного иммунитета, способного гарантировать функционирование критически важных систем государства и общества даже в условиях перманентного, многомерного гибридного воздействия.

Библиографический список:

1. Акапьев, В.Л. Публично-правовое регулирование обеспечения безопасности объектов критической информационной инфраструктуры / В.Л. Акапьев, С.Е. Савотченко // Вестник Удмуртского университета. Серия “Экономика и право”. – 2024. – Т. 34, № 3. – С. 494-503.
2. Емельянов, А.А. К вопросу о цифровом суверенитете России / А.А. Емельянов, И.Л. Коршунов, С.Ю. Микадзе // Известия Санкт-Петербургского государственного экономического университета. – 2022. – № 6 (138). – С. 84-90. – ISSN 2311-3464
3. Минцифры заявило о “беспрецедентных кибератаках” на сайты правительства [Электронный ресурс] // Журнал Компания. URL: <https://ko.ru/news/mintsifry-zayavilo-ob-espretsedentnykh-kiberatakakh-na-sayty-pravitelstva/> (дата обращения: 04.02.2026).
4. Приказ ФСТЭК России от 25.12.2017 №239 (ред. от 28.08.2024) "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации"
5. Россия в эпоху гибридных войн [Электронный ресурс] // Научно-исследовательский центр проблем национальной безопасности. URL: <https://nic-pnb.ru/vneshnepoliticheskie-aspekty-bezopasnosti/rossiya-v-epohu-gibridnyh-vojn/?ysclid=lruoou2wey968466436> (дата обращения: 04.02.2026)
6. Указ Президента РФ от 05.12.2016 г. №646 "Об утверждении Доктрины информационной безопасности Российской Федерации"
7. Указ Президента РФ от 30.03.2022 №166 (ред. от 07.04.2025) "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации"
8. Уязвительное — рядом [Электронный ресурс] // Коммерсант. URL: <https://www.kommersant.ru/doc/8380028> (дата обращения: 04.02.2026).
9. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 №187-ФЗ (последняя редакция)
10. RED Security SOC: В третьем квартале количество кибератак выросло на 73% [Электронный ресурс] // RED Security SOC. URL: <https://redsecurity.ru/news/red-security-soc-v-tretem-kvartale-kolichestvo-kiberatak-vyroslo-na-73> (дата обращения: 04.02.2026).