

УГОЛОВНОЕ ПРАВО И КРИМИНОЛОГИЯ; УГОЛОВНО-ИСПОЛНИТЕЛЬНОЕ ПРАВО

CRIMINAL LAW AND CRIMINOLOGY; CRIMINAL AND PENAL LAW

Научная статья

УДК: 343.985.7:343.34:004(470+73)

DOI 10.33184/vest-law-bsu-2026.31.8

Аглетдинова Диана Ильдаровна

Уфимский юридический институт МВД России, Уфа, Россия,

agletdinovadiana@yandex.ru

ИНФОРМАЦИОННАЯ ЗАЩИТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ И ОСОБЕННОСТИ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ, ПРЕДУСМОТРЕННЫХ СТ. 274.1 УК РФ

Аннотация: В современных условиях, характеризующихся глобальной информатизацией и цифровизацией, защита критической информационной инфраструктуры Российской Федерации (далее – КИИ) приобретает ключевое значение для национальной безопасности. Статья посвящена актуальной проблеме расследования преступлений, связанных с неправомерным воздействием на объекты КИИ. На основе анализа отечественных и зарубежных инцидентов констатируется серьёзность последствий кибератак на КИИ, которые могут дестабилизировать общество или являться угрозой для жизни и здоровья граждан.

Делается вывод, что, несмотря на развитие законодательной базы, включая введение ст. 274.1 Уголовного кодекса Российской Федерации (далее – УК РФ), принятие Федерального закона №187-ФЗ от 26 июля 2017 г. и других нормативно-правовых актов, правоприменительная практика, связанная с привлечением к уголовной ответственности за неправомерное воздействие на КИИ, сталкивается со значительными трудностями. К ним относятся проблемы применения специальных технических знаний, вариативность и стремительное развитие способов совершения преступлений, сложности в выявлении и задержании преступников, зачастую действующих дистанционно и транснационально, высокая латентность преступления. Подчёркивается, что техническая специфика объектов КИИ, в том числе замкнутость информационных систем, использование специального программного обеспечения и необходимость соблюдения непрерывности технологических процессов, является дополнительным фактором, осложняющим производство следственных действий.

Отмечается отсутствие комплексной криминалистической методики, учитывающей все особенности данного состава преступления. Подчёркивается необходимость разработки криминалистической методики для практических органов с целью оптимизации их деятельности по расследованию неправомерного воздействия на КИИ.

Ключевые слова: критическая инфраструктура, неправомерное воздействие, криминалистика, информационная безопасность, методика расследования, компьютерная информация, специальные знания, компьютерная атака, национальная безопасность

Для цитирования: Аглетдинова Д.И. Информационная защита критической информационной инфраструктуры и особенности раскрытия преступлений, предусмотренных ст. 274.1 УК РФ / Д.И. Аглетдинова. – DOI 10.33184/vest-law-bsu-2026.31.8 // Вестник Института права Башкирского государственного университета. – 2026. – № 3. – С. 105–116.

Original article

Agletdinova Diana Ildarovna

Ufa Law Institute of the Ministry of Internal Affairs of Russia, Ufa, Russia,
agletdinovadiana@yandex.ru

THE CRITICAL INFORMATION INFRASTRUCTURE SECURITY AND THE SPECIFICS OF CRIME DETECTION UNDER THE ARTICLE 274.1 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION

Abstract. In modern conditions characterized by global informatization and digitalization, the protection of the critical information infrastructure of the Russian Federation (hereinafter – CII) is of key importance for national security. The article is devoted to the urgent problem of investigating crimes related to the unlawful impact on CII facilities. Based on the analysis of domestic and foreign incidents, the severity of the consequences of cyberattacks on CII, which can destabilize society or pose a threat to the citizens' life and health, is stated. It is concluded that, despite the development of the legislative framework, including the introduction of the Article 274.1 of the Criminal Code of the Russian Federation, the adoption of Federal Law No. 187 of July 26, 2017 and other regulatory legal acts, law enforcement practice related to criminal prosecution for unlawful influence on CII, it faces significant difficulties. These include the problems of applying special technical knowledge, the variability and rapid development of committing crimes' methods, difficulties in identifying and detaining criminals, often operating remotely and transnational and the high latency of the crime. It is emphasized that the technical specifics of the CII facilities, including the closed nature of information systems, the use of special software and the need to maintain the continuity of technological processes, is an

additional factor complicating the conduct of investigative actions. The absence of a comprehensive forensic methodology that takes into account all the features of this corpus delicti is noted. The necessity of developing a forensic methodology for practical agencies in order to optimize their activities in investigating unlawful impact on CII is emphasized.

Keywords: critical infrastructure, unlawful impact, criminalistics, information security, investigation methodology, computer information, specialized knowledge, computer attack, national security

For citation: Agletdinova D.I. The Critical Information Infrastructure Security and the Specifics of Crime Detection under the Article 274.1 of the Criminal Code of the Russian Federation. *Vestnik Instituta prava Bashkirskogo gosudarstvennogo universiteta = Bulletin of the Institute of Law of the Bashkir State University*, 2026, no. 3, pp. 105–116. (In Russian). DOI 10.33184/vest-law-bsu-2026.31.8

Введение. За последние годы информатизация наблюдается во всех сферах общественной жизни, множество организаций и учреждений государственного и частного сектора применяют технологии в своей деятельности и ведут документооборот в электронном виде. Этот постепенный переход, произошедший за два десятилетия, позволил не только оценить эффективность использования новых технологий и методов, но и проанализировать риски, связанные с обеспечением надлежащего уровня защиты для конфиденциальных сведений.

Внедрение цифровой инфраструктуры в различных отраслях привело к тому, что область информационной безопасности на данный момент является одной из ключевых в системе национальной безопасности Российской Федерации.

Особое внимание в последние годы уделено КИИ, которая является одним из важных элементов функционирования общества и его стабильного развития. Вместе с тем ускоренный технологический прогресс и внедрение его результатов на наиболее важных объектах инфраструктуры не всегда позволяют принять достаточные меры по их защите от внешних и внутренних угроз, что неизбежно приводит к киберинцидентам.

На монографическом уровне проблемы расследования неправомерного воздействия на КИИ до настоящего времени не рассматривались. Отдельные вопросы, касающиеся квалификации преступления [1, с. 211; 2, с. 89], предупреждения [3, с. 176], криминалистической характеристики [4, с. 52], следственных ситуаций на первоначальном этапе расследования [5, с. 257], освещались в научных статьях.

В диссертационном исследовании Малыгина И.И. (2023) были рассмотрены вопросы законодательного определения и уголовно-правовые аспекты квалификации неправомерного воздействия на КИИ. Однако задачи, связанные с криминалистическим исследованием данного преступления, и методика расследования в указанной работе не были предметом изучения.

Целью настоящего исследования является анализ проблем, возникающих в ходе расследования преступлений, связанных с неправомерным воздействием на КИИ.

Задачи исследования включают в себя анализ компьютерных инцидентов, направленных на КИИ, которые повлекли значительный ущерб, нормативно-правовых актов, касающихся КИИ, и их работу, а также эмпирических материалов, связанных с расследованием неправомерного воздействия на КИИ.

Методы исследования включают формально-логический и сравнительно-правовой анализ федеральных законов и нормативно-правовых актов, статистический метод для оценки динамики преступлений, совершённых в сфере компьютерной информации.

Зарубежный опыт. Инциденты, вследствие которых объекты КИИ подверглись неправомерному воздействию, за последние годы встречались достаточно часто, и организации, не способные обеспечить надлежащую защиту, столкнулись с серьёзными последствиями не только на территории Российской Федерации, но и за рубежом.

Так, например, в декабре 2019 г. произошла кибератака на информационную систему правительства штата в Луизиане (США), в результате которой в городе было введено чрезвычайное положение. Техника местных служб оказалась заражённой вредоносной компьютерной программой. С целью предотвращения распространения компьютерного вируса по всей сети городских служб были приняты экстренные меры по отключению местных компьютеров и серверов, в том числе Центра по борьбе с преступностью в реальном времени. При этом никаких запросов со стороны преступников с требованиями о выкупе или выполнения других условий не поступало. По данным представителей местного самоуправления преступникам не удалось похитить конфиденциальные данные, содержащиеся на заражённых компьютерах, которые, скорее всего, изначально были их целью¹.

В марте 2019 г. норвежская металлургическая и нефтегазовая компания Hydro, занимающая третье место в мире по производству алюминия, подверглась компьютерной атаке посредством вредоносной программы типа «шифровальщик» LockerGoda². В результате часть производственных систем была заблокирована, что привело к временной остановке технологического процесса. Вместо выплаты преступникам выкупа, который они потребовали за расшифровку данных, компания оперативно среагировала на данный инцидент и предприняла необходимые меры по ликвидации проблем и минимизации последствий: перевела в ручной режим технологический процесс на заражённых

¹ В Новом Орлеане из-за кибератаки ввели режим чрезвычайной ситуации [Электронный ресурс] // Официальный сайт государственного информационного агентства «ТАСС». URL: <https://tass.ru/mezhdunarodnaya-panorama/7347757> (дата обращения: 02.02.2026).

² Промышленный гигант Hydro атакован шифровальщиком [Электронный ресурс] // Официальный сайт международной компании «Лаборатория Касперский». URL: <https://www.kaspersky.ru/blog/hydro-attacked-by-ransomware/22421/> (дата обращения: 02.02.2026).

вирусом заводах, изолировала от корпоративной сети блоки, подвергнувшиеся атаке вируса, и использовала резервные копии данных для восстановления зашифрованной информации. Таким образом, нельзя не отметить заметные сдвиги в сторону своевременного реагирования на компьютерные инциденты в частных компаниях.

В то время как последствия большинства компьютерных атак включают в основном материальные убытки и репутационные потери, встречаются и такие, которые могут нанести серьёзный вред здоровью граждан. Речь идет, например, о кибератаке на городскую систему очистки воды, произошедшей в феврале 2021 г. в американском городе Олдсмар. Преступник с помощью вредоносной программы получил удалённый доступ к системам очистки воды и изменил параметры концентрации гидроксида натрия в питьевой воде, что, по мнению экспертов, могло привести к отравлению и причинению вреда здоровью граждан. Жертвами данного преступления могли оказаться около 15 тысяч человек, однако сотрудник станции обратил внимание на превышение допустимых параметров и понизил уровень гидроксида натрия до допустимого. Сложно сказать, какие цели мог преследовать преступник, личность которого правоохранительным органам не удалось установить, тем не менее, последствия от его действий могли нанести серьёзный вред здоровью граждан³.

Компьютерные атаки на медицинские учреждения уже имеют случаи летального исхода для пациентов. Так, в сентябре 2020 г. из-за блокировки серверов университетской клиники Дюссельдорфского университета пришлось отложить операции и лечение больных, вследствие чего одна из пациенток умерла⁴.

С учётом актуальности проблемы защиты КИИ на международной арене отечественные авторы отмечают необходимость скоординированных и объединённых усилий мирового сообщества по устранению киберугроз, для чего потребовалась выработка общих международных стандартов, отличающихся универсальностью для всех стран мира [6, с. 49].

Для достижения указанных целей по инициативе Российской Федерации была разработана Конвенция против киберпреступности, являющаяся первым универсальным договором, предусматривающим укрепление международного сотрудничества в борьбе с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий, одобренная Организацией Объединённых Наций. Проект резолюции принятого документа подчёркивает особую важность борьбы с указанным видом преступлений, поскольку они зачастую связаны с отмыванием денег, террористическими и экстремистскими актами, неправомерным использованием криптовалют, коррупцией, торговлей людьми, незаконным изготовлением и оборотом оружия, наркотических и психотропных веществ и пр. [7, с. 118].

³ Во Флориде хакер попытался добавить едкое вещество в систему водоочистки [Электронный ресурс] // Официальный сайт ежедневной деловой газеты «РБК». URL: <https://www.rbc.ru/rbcfreenews/60224bff9a79475bebacb2c6> (дата обращения: 02.02.2026).

⁴ В Дюссельдорфе пациентка умерла после хакерской атаки на клинику [Электронный ресурс] // Официальный сайт государственного информационного агентства «ТАСС». URL: <https://tass.ru/obschestvo/9482283> (дата обращения: 02.02.2026).

Отечественный опыт. Одновременно с этим, внешнеполитическая ситуация является дополнительным фактором, осложняющим защиту КИИ. Начальник управления развития информационно-коммуникационных технологий и инфраструктуры связи при Администрации Президента Российской Федерации (далее – РФ) Т. Матвеева отмечает, что с момента начала российской спецоперации в Украине кибератакам подверглось около 90 % российских ведомств и структур; мощность DDoS-атак возросла практически в 20 раз; в кибернападениях участвовало более 0,5 млн человек. Целями атак стали сайты медиаресурсов, госведомств, системы госуправления, банки и ритейлеры, а также компании и предприятия с государственным участием из авиационно-космической и электроэнергетической отраслей. Кибератакам подверглись 90 % инфраструктуры госсектора РФ⁵.

Нами были рассмотрены наиболее известные случаи неправомерного воздействия, совершенные в отношении зарубежных объектов КИИ, однако в последние годы и отечественная КИИ всё чаще подвергается компьютерным атакам.

Так, в октябре 2024 г. государственная автоматизированная система Российской Федерации «Правосудие» (далее – ГАС «Правосудие»), а также официальный сайт Федеральных арбитражных судов РФ стали объектом неправомерного воздействия со стороны неустановленных лиц. Указанные информационные системы были недоступны для пользователей в течение нескольких дней⁶.

В апреле 2024 г. компьютерной атаке подверглась Единая автоматизированная информационная система Федеральной таможенной службы Российской Федерации (далее – ФТС РФ), функционирование которой было приостановлено. Следствием этого стал временный переход сотрудников ФТС РФ на бумажные носители, что существенно замедлило процессы оформления необходимых документов для пересечения границы участниками внешнеторговой деятельности⁷.

Значительные неблагоприятные последствия наступили и в результате сбоя в информационной системе компании «Аэрофлот», произошедшего в июле 2025 г. Данная компьютерная атака стала причиной задержки и отмены более чем 100 рейсов авиакомпании по всей России⁸.

⁵ Кибератакам подверглось 90 % инфраструктуры госсектора РФ [Электронный ресурс] // Официальный сайт информационного агентства «Интерфакс». URL: <https://www.interfax-russia.ru/moscow/news/kiberatakam-podvergnos-90-infrastruktury-gossektora-rf-nachalnik-upravleniya-ap> (дата обращения: 02.02.2026).

⁶ Хакеры атаковали правительственный сервис ГАС «Правосудие» [Электронный ресурс] // Официальный сайт российского общественно-политического интернет-издания «Газета.ру». URL: <https://www.gazeta.ru/tech/news/2024/10/07/24097453.shtml?updated> (дата обращения: 02.02.2026).

⁷ Хакеры обрушили электронную систему ФТС [Электронный ресурс] // Официальный сайт российской ежедневной деловой газеты «Ведомости». URL: https://www.vedomosti.ru/business/articles/2023/04/11/970397-hakeri-obrushili-elektronnyuyu-sistemu-fts?from=copy_text (дата обращения: 02.02.2026).

⁸ В «Аэрофлоте» остановлены полеты. Хакеры заявили об уничтожении ИТ-инфраструктуры авиакомпании [Электронный ресурс] // Официальный сайт российского издания «СNews». URL: https://www.cnews.ru/news/top/2025-07-28_hakery_vzyali_na_sebya_otvetstvennost (дата обращения: 02.02.2026).

Данные примеры свидетельствуют о необходимости выработки системных решений для сотрудников объектов КИИ в области информационной безопасности. Создание алгоритмов действий и инструкций при возникновении компьютерных инцидентов, ознакомление и следование им может минимизировать последствия компьютерных атак.

Принимая во внимание современные тенденции, законодатель дополняет уголовное законодательство специальной уголовно-правовой нормой, а именно ст. 274.1 УК РФ, которая введена Федеральным законом от 26 июля 2017 г. № 194-ФЗ⁹. Данная статья относится к преступлениям в сфере компьютерной информации и предусматривает ответственность за неправомерное воздействие на объекты КИИ.

Обеспечение безопасности КИИ затрагивает и ряд других нормативно-правовых актов, среди которых основным является Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры»¹⁰, дающий определения основополагающим терминам, закрепляющий принципы обеспечения безопасности КИИ, разъясняющий основные направления деятельности в сфере безопасности КИИ и полномочия конкретных государственных органов. Подчеркивает значимость рассматриваемого вопроса его упоминание в Стратегии национальной безопасности (далее – Стратегия), утверждённой Указом Президента РФ от 02 июля 2021 г. № 400¹¹, где отмечено, что выведение из строя объектов КИИ является одной из задач специальных служб иностранных государств наряду с разведывательной и иной деятельностью в российском информационном пространстве. Вместе с тем, в отдельную задачу выделено предотвращение деструктивного информационно-технического воздействия на российские информационные ресурсы, включая объекты КИИ.

Помимо этого, в соответствии с задачами Стратегии, закрепляющими обеспечение приоритетного использования в информационной инфраструктуре РФ российских информационных технологий и оборудования, в Указе Президента РФ от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»¹² законодательно установлено, что субъектам КИИ запрещается использовать иностранное программное обеспечение на

⁹ О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»: федеральный закон от 26.07.2017 № 194-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 02.02.2026).

¹⁰ О безопасности критической информационной инфраструктуры Российской Федерации: федеральный закон от 26.07.2017 № 187-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 02.02.2026).

¹¹ О Стратегии национальной безопасности Российской Федерации: указ Президента РФ от 02.07.2021 № 400 // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 02.02.2026).

¹² О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации: указ Президента РФ от 30.03.2022 № 166 // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 02.02.2026).

принадлежащих им значимых объектах КИИ, что должно снизить возможности неправомерного воздействия на КИИ.

Большинство подзаконных нормативно-правовых актов, касающихся КИИ, являются приказами Федеральной службы по техническому и экспортному контролю Российской Федерации (далее – ФСТЭК России). К ним относятся: приказ ФСТЭК России от 6 декабря 2017 г. № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»¹³, приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»¹⁴, приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»¹⁵. Для соблюдения соответствующего уровня информационной безопасности на рассматриваемых объектах законодатель вводит новые и обновляет старые требования к защите информационных систем КИИ.

Устанавливая таким образом конкретные правила и требования обеспечения безопасности объектов КИИ, государственные органы стремятся к полной правовой регламентации данного вопроса.

Исходя из вышеизложенного, можно сделать вывод о положительных тенденциях в российском законодательстве, направленных на регулирование как сферы КИИ в целом, так и её информационной безопасности в частности.

Однако, несмотря на значительные улучшения в законодательной базе, согласно отчётам ФСТЭК России в рамках проведения проверочных мероприятий выявлено около 1400 нарушений обязательных требований обеспечения безопасности значимых объектов КИИ. Кроме того, 40 % указанных нарушений являются грубыми, т. е. могут привести к отклонению от устойчивого функционирования защищаемого объекта. Вместе с тем, отмечен крайне низкий показатель по осуществлению минимального базового уровня защиты от актуальных угроз безопасности – требования были соблюдены лишь у 13 % проверенных организаций. Ещё 40 % объектов КИИ имеют, по оценке экспертов, низкий уровень защиты, при котором не все базовые требования законодательства выполнены¹⁶.

¹³ Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации: приказ ФСТЭК России от 06.12. 2017 № 227 // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 02.02.2026).

¹⁴ Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования: приказ ФСТЭК России от 21.12.2017 № 235 // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 02.02.2026).

¹⁵ Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: приказ ФСТЭК России от 25.12.2017 № 239 // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 02.02.2026).

¹⁶ Регулятор дал плохую оценку защищенности компаний России от кибератак [Электронный ресурс] // Официальный сайт российского новостного издания «News.ru». URL: <https://news.ru/society/regulator-dal-plohuyu-ocenku-zashishennosti-kompanij-rossii-ot-kiberatak> (дата обращения: 02.02.2026).

Обеспечение полной безопасности КИИ является практически невыполнимой задачей, вследствие чего расследование неправомерного воздействия на КИИ является актуальной проблемой для правоохранительных органов в обозримом будущем.

На современном этапе, когда уголовно-правовая норма, закреплённая в статье 274.1 УК РФ, была введена законодателем относительно недавно и судебная практика находится на этапе формирования, расследование дополнительно осложнено спецификой самого преступления и предмета посягательства.

В первую очередь необходимо учитывать, что данное деяние относится к категории преступлений в сфере компьютерной информации, что само по себе предполагает использование специальных знаний и привлечение специалиста как в процессуальной, так и в непроцессуальной формах [8, с. 12]. Кроме того, предмет преступления, представляющий собой объект КИИ, также имеет характерные свойства, которые необходимо учитывать при проведении следственных действий.

Так, стоит принимать во внимание такие особенности объектов КИИ как замкнутость и изолированность информационной среды с целью предотвращения внешних воздействий, использование специального программного обеспечения, а главное – непрерывность технологических процессов, напрямую зависящих от объектов КИИ.

Необходимо отметить, что объекты КИИ могут иметь специфические особенности в соответствии со сферой их применения (здравоохранение, транспорт, связь и т. д.), исходя из этого, архитектура построения системы КИИ в корне различается с другими системами с учётом выполняемых задач.

Следующей проблемой, с которой правоохранительные органы сталкиваются при расследовании неправомерного воздействия на КИИ, является вариативность способов совершения данного преступления. В УК РФ законодатель выделяет три основные формы неправомерного воздействия, а именно:

- создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на КИИ (ч. 1 ст. 274.1 УК РФ);
- неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ (ч. 1 ст. 274.1 УК РФ);
- нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ (ч. 3 ст. 274.1 УК РФ).

Каждая из этих форм может быть осуществлена различными способами. При этом они могут совершаться как дистанционно, так и предполагать физическое воздействие на объекты КИИ. Более того, можно с уверенностью констатировать тот факт, что, как и в других преступлениях, использующих информационно-телекоммуникационные технологии, количество способов совершения данного преступления стремительно увеличивается [9, с. 103].

Несмотря на отсутствие официальной статистики по количеству зарегистрированных преступлений, квалифицируемых как неправомерное воздействие на КИИ, стоит отметить, что количество привлечённых к уголовной ответственности за указанное деяние составляет в 2022 г. – 54 человека, в 2023 – 79, 2024 – 77, что указывает на крайне низкие показатели раскрываемости данного состава преступления. По нашему мнению, это является следствием не только вышеупомянутых проблем, но и сложностями с обнаружением и задержанием преступников, которые осуществляют неправомерное воздействие на КИИ дистанционно, в том числе за пределами Российской Федерации. Кроме того, статистические показатели данного состава преступления на фоне общей статистики по другим преступлениям в сфере компьютерной информации, число которых за последние годы увеличилось в несколько раз, свидетельствуют о высокой латентности неправомерного воздействия на КИИ.

В целом новизна данного состава преступления в совокупности со его специфическими чертами, не позволяющими полностью экстраполировать ранее накопленный опыт по расследованию преступлений в сфере компьютерной информации, приводит к острой необходимости создания методики расследования неправомерного воздействия на КИИ, учитывающей характерные черты данного преступления и предлагающей решение вышеуказанных проблем.

Заключение. Количество кибератак на критическую информационную инфраструктуру России увеличилось в четыре раза в 2025 г. Об этом сообщила пресс-служба Совета безопасности РФ после заседания межведомственной комиссии по информационной безопасности¹⁷.

Субъекты критической информационной инфраструктуры из-за своей значимости и в дальнейшем будут подвержены компьютерным атакам, улучшение средств защиты приводит к появлению новых способов их преодоления.

По мнению автора, в законодательстве РФ в достаточной мере закреплены меры по защите КИИ и регламентирована уголовная ответственность за посягательство на объекты КИИ, что является положительной тенденцией. В то же время в правоприменительной практике возникают трудности с расследованием неправомерного воздействия на КИИ, что помимо проблем, связанных с применением специальных технических знаний, разнообразием способов совершения преступления и латентностью, является следствием отсутствия разработанной криминалистической методики для расследования данной категории преступлений. Отсутствуют рекомендации по организации и осуществлению расследования на первоначальном этапе, тактике производства отдельных следственных действий, проводимых на этапе раскрытия и расследования неправомерного воздействия на КИИ.

Изложенное позволяет заключить, что создание методики расследования неправомерного воздействия на КИИ является актуальной задачей для российской уголовно-правовой науки и правоприменительной практики.

¹⁷ Число кибератак на информационную инфраструктуру России выросло в четыре раза [Электронный ресурс] // Официальный сайт российской ежедневной общественно-политической газеты «Коммерсантъ». URL: <https://www.kommersant.ru/doc/8101273> (дата обращения: 02.02.2026).

Список источников

1. Мельникова Е.Ф., Родионов А.Д. Вопросы квалификации неправомерного доступа к объектам критической информационной инфраструктуры / Е.Ф. Мельникова, А.Д. Родионов // Юридическая наука и практика. – Вестник Нижегородской академии МВД России. – 2024. – № 3 (67). – С. 208–215.
2. Ефремова М.А. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации / М.А. Ефремова // Вестник Казанского юридического института МВД России. – 2022. – № 4 (50). – С. 86–92.
3. Витвицкая С.С., Исакова Ю.И., Кейдунова Е.Р. Противодействие неправомерному воздействию на критическую информационную инфраструктуру Российской Федерации / С.С. Витвицкая, Ю.И. Исакова, Е.Р. Кейдунова // Уголовное право: стратегия развития в XXI веке. – 2023. – № 3. – С. 173–181.
4. Голубев Ф.А. Криминалистическая характеристика расследования неправомерного воздействия на критическую информационную структуру Российской Федерации / Ф.А. Голубев // Право и политика. – 2020. – № 10. – С. 50–59.
5. Степаненко Д.А., Гармышев Я.В. Типовая ситуационно-версионная характеристика первоначального этапа расследования неправомерного воздействия на критическую информационную инфраструктуру: уголовно-правовые и криминалистические аспекты / Д.А. Степаненко, Я.В. Гармышев // Всероссийский криминологический журнал. – 2023. – Т. 17, № 3. – С. 254–262.
6. Нугаева Э.Д., Чаплыгина В.Н. Опыт международных проектов в сфере борьбы с киберпреступлениями / Э.Д. Нугаева, В.Н. Чаплыгина // Современное уголовно-процессуальное право – уроки истории и проблемы дальнейшего реформирования: сборник материалов Международной научно-практической конференции, Орел, 12–13 октября 2023 г.: в 2 ч. / отв. ред. К.В. Муравьев. – Орел: Орловский ЮИ МВД России им. В.В. Лукьянова, 2023. – Ч. 2. – С. 45–50.
7. Харисова З.И. Проблемы и пути совершенствования деятельности по собиранию цифровых доказательств при расследовании преступлений в сфере компьютерной информации / З.И. Харисова // Вестник Уфимского юридического института МВД России. – 2025. – № 2 (108). – С. 116–126.
8. Грамович Г.И. Тактика использования специальных знаний в раскрытии и расследовании преступлений: учеб. пособие / Г.И. Грамович. – Минск: МВШ МВД СССР, 1987. – 144 с.
9. Батоев В.Б. Преступления, совершаемые с использованием или применением информационно-телекоммуникационных технологий: способы их совершения и количественные характеристики / В.Б. Батоев // Правопорядок: история, теория, практика. – 2023. – № 3 (38). – С. 101–112.

References

1. Melnikova E.F., Rodionov A.D. Issues of Qualification of Unauthorized Access to Critical Infrastructure Facilities. *Legal Science and Practice: Journal of Nizhny*

Novgorod Academy of the Ministry of Internal Affairs of Russia, 2024, no. 3 (67), pp. 208–215. (In Russian).

2. Efremova M.A. Criminal Liability for Unlawful Impact on the Critical Information Infrastructure of the Russian Federation. *Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia*, 2022, no. 4 (50), pp. 86–92. (In Russian).

3. Vitvitskaya S.S., Isakova Yu.I., Keydunova E.R. Countering Unlawful Influence on the Critical Information Infrastructure of the Russian Federation. *Criminal Law: Development Strategy in the 21st Century*, 2023, no. 3, pp. 173–181. (In Russian).

4. Golubev F.A. Criminalistic Characteristic of Investigation of Undue Influence upon Critical Information Structure of the Russian Federation. *Law and Politics*, 2020, no. 10, pp. 50–59. (In Russian).

5. Stepanenko D.A., Garmyshev Ya.V. Typical Situational-Version Features of the Initial Stage of Investigating Unlawful Impact on Critical Information Infrastructure: Criminal Law and Criminalistic Aspects. *Russian Journal of Criminology*, 2023, vol. 17, no. 3, pp. 254–262. (In Russian).

6. Nugaeva E.D., Chaplygina V.N. Experience of International Projects in the Field of Combating Cybercrimes. *Modern Criminal Procedure – Law Lessons of History and Problems of Further Reforming. Collection of Materials of the International Scientific and Practical Conference, Orel, October 12–13, 2023*. Orel, Lukyanov Orel Law Institute of the Interior of Russia, 2023, pp. 45–50. (In Russian).

7. Kharisova Z.I. Problems and Ways to Improve the Collection of Digital Evidence in Cybercrimes Investigation. *Bulletin of Ufa Law Institute of the Ministry of Internal Affairs of Russia*, 2025, no. 2 (108), pp. 116–126. (In Russian).

8. Gramovich G.I. Tactics of Using Specialized Knowledge in Detection and Investigation of Crimes: Textbook. Minsk, Minsk Higher School of the USSR Ministry of Internal Affairs, 1987. 144 p. (In Russian).

9. Batoev V.B. Offences Committed through the Use or Application of Information and Telecommunication Technologies: Methods of Their Commission and Quantitative Characteristics. *Legal Order: History, Theory, Practice*, 2023, no. 3 (38), pp. 10–112. (In Russian).

Информация об авторе

Аглетдинова Диана Ильдаровна –
адъюнкт адъюнктуры Уфимского
юридического института МВД Рос-
сии

Information about the Author

Agletdinova Diana Ildarovna – adjunct
of the Ufa Law Institute of the Ministry
of Internal Affairs of Russia

Статья поступила в редакцию 15.05.2026 г.; одобрена после рецензирования 17.08.2026 г.; принята к публикации 17.08.2026.

The article was submitted 15.05.2026; approved after reviewing 17.08.2026; accepted for publication 17.08.2026.