DOI: 10.17803/1729-5920.2025.226.9.081-094

А. А. Шутова
Казанский инновационный университет имени В.Г. Тимирясова
г. Казань, Российская Федерация

Уголовно-правовое обеспечение безопасности критической цифровой инфраструктуры Российской Федерации (на примере учреждений здравоохранения)

Резюме. В статье рассмотрены особенности применения технологии искусственного интеллекта в системе здравоохранения, включая вопросы персональной ответственности врача при принятии решений о диагностике и лечении на основании сформулированного предложения (решения) алгоритма. Представлен обзор действующей системы правового регулирования ответственности медицинских работников, а также проведена оценка возможных вариантов распределения ответственности в связи с внедрением искусственного интеллекта в работу врачей. Раскрыты потенциальные направления совершенствования законодательства и выделены особенности, касающиеся медицинских организаций, медицинских работников и пациентов, которым будет оказана медицинская помощь с использованием интеллектуальных систем. Проанализированы тенденции распределения ответственности за причинение вреда при оказании медицинской помощи в таких случаях, что позволило выработать возможные варианты распределения ответственности между медицинской организацией и медицинским работником в будущем.
Ключевые слова: цифровизация; цифровое здравоохранение; искусственный интеллект; медицинские изделия на основе искусственного интеллекта; уголовная ответственность врачей; цифровые технологии; цифровая безопасность; машинное обучение
Для цитирования: Шутова А. А. Уголовно-правовое обеспечение безопасности критической цифровой инфраструктуры Российской Федерации (на примере учреждений здравоохранения). *Lex russica.* 2025. Т. 78. № 9. С. 81–94. DOI: 10.17803/1729-5920.2025.226.9.081-094

Благодарности. Работа выполнена за счет гранта Академии наук Республики Татарстан, предоставленного молодым кандидатам наук (постдокторантам) с целью защиты докторской диссертации, выполнения научно-исследовательских работ, а также выполнения трудовых функций в научных и образовательных организациях Республики Татарстан в рамках Государственной программы Республики Татарстан «Научно-технологическое развитие Республики Татарстан».

Criminal Law Measures to Ensure the Security of the Russian Federation's Critical Digital Infrastructure (the Case Study of Healthcare Institutions)

Albina A. Shutova
Kazan Innovative University named after V.G. Timiryasov
Kazan, Russian Federation

Abstract. The paper examines the specific features of applying artificial intelligence technologies in the healthcare system, including issues of physicians' personal liability when making diagnostic and treatment decisions based on an algorithm's recommendation (decision). The study provides a review of the current legal framework governing the liability of healthcare professionals and assesses possible options for allocating liability arising from the integration of artificial intelligence into physicians' work. The author examines possible directions for legislative

improvement and identifies the particular challenges that medical organizations, healthcare professionals and patients receiving care with intelligent systems may face. Trends in the allocation of liability for harm caused in the provision of medical care are analyzed, enabling the development of potential models for distributing responsibility between medical institutions and individual practitioners in the future.
Keywords: digitalization; digital healthcare; artificial intelligence; AI-based medical devices; physician criminal liability; digital technology; digital security; machine learning
Cite as: Shutova AA. Criminal Law Measures to Ensure the Security of the Russian Federation's Critical Digital Infrastructure (the Case Study of Healthcare Institutions). *Lex russica*. 2025;78(9):81-94. (In Russ.). DOI: 10.17803/1729-5920.2025.226.9.081-094

Acknowledgments. The study was supported by a grant from the Academy of Sciences of the Republic of Tatarstan awarded to young Candidates of Sciences (postdoctoral researchers) to facilitate the defense of a doctoral dissertation, the conduct of research, and the performance of employment duties in scientific and educational institutions of the Republic of Tatarstan under the State Program of the Republic of Tatarstan «Scientific and Technological Development of the Republic of Tatarstan».

Введение

В России отмечается рост количества зарегистрированных преступлений против критической информационной инфраструктуры (КИИ), что подтверждается статистическими сведениями МВД России. Уточним, что ответственность за неправомерное воздействие на КИИ РФ появилась в Уголовном кодексе РФ в 2017 г. (ст. 274.1). И если за первые годы после криминализации ответственности (с 2018 по 2020 г.) было зарегистрировано всего 27 преступлений (в 2018 г. — одно, в 2019 г. — четыре, в 2020 г. — 22), то уже за 2021 и 2022 гг. — 678 преступлений (в 2021 г. — 159, в 2022 г. — 519)[1]. В то же время, согласно статистике, приведенной Судебным департаментом при Верховном Суде РФ, растет и количество осужденных за преступления, предусмотренные статьей 274.1 УК РФ. Если с 2018 по 2020 г. было осуждено всего 12 человек, то с 2021 по 2023 г. уже 148 человек[2].

Статистические сведения о количестве зарегистрированных преступлений в 2023 г. МВД России не приведены. Тем не менее негативная тенденция к увеличению преступлений, предусмотренных статьей 274.1 УК РФ, остается. По данным Национального координационного центра по компьютерным инцидентам за 2023 г., количество атак на объекты КИИ РФ увеличилось по сравнению с 2022 г. на 16 % — до 65 тыс.[3]

Вопросы уголовно-правовой охраны КИИ приобрели особую актуальность в период проведения специальной военной операции на Украине[4].

Особенно распространены случаи неправомерного воздействия на КИИ учреждений системы здравоохранения РФ. Периодически экспертами Positive Technologies подтверждается, что самой атакуемой сферой становится здравоохранение[5]. Для медицинских организаций важна не просто система, формально соответствующая требованиям регуляторов, а реальная защищенность, которая позволяет предотвращать разного рода компьютерные инциденты, включая незаконное собирание данных и нарушения работы ее информационной инфраструктуры[6]. В свою очередь, воздействие на

[1] Сайт МВД России. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 10.11.2024).
[2] Официальный сайт Судебного департамента при Верховном Суде РФ. URL: www.cdep.ru/ (дата обращения: 10.11.2024).
[3] Субъектная защита // URL: https://www.kommersant.ru/doc/6679041 (дата обращения: 10.12.2024).
[4] *Малыгин И. И.* Уголовно-правовое противодействие неправомерному воздействию на критическую информационную инфраструктуру : автореф. дис. … канд. юрид. наук. М., 2023. С. 4.
[5] Positive Technologies: шифровальщики переключились на медицину // URL: https://www.ptsecurity.com/ru-ru/about/news/positive-technologies-shifrovalshchiki-pereklyuchilis-na-medicinu/ (дата обращения: 19.12.2024).
[6] *Бахтеев Д. В., Сосновикова А. М., Казенас Е. В.* Преодоление нелегальной трансграничной передачи персональных данных // Journal of Digital Technologies and Law. 2024. № 2 (4). С. 943–972. URL: https://doi.org/10.21202/jdtl.2024.45.

медицинские цифровые сервисы может не только причинить имущественный ущерб, но и поставить под угрозу жизнь и здоровье граждан. Если злоумышленники зададутся целью атаковать медицинскую инфраструктуру, они смогут нанести ей, ее операторам, владельцам и пациентам значительный ущерб, что повлечет многоуровневые цепи негативных последствий. Так, тысячи систем управления климатом производства Resource Data Management, используемые во многих больницах по всему миру, оказались уязвимы к удаленным кибератакам[7]. Гипотетически злоумышленники дистанционно в состоянии изменить температурный режим медицинских холодильников и уничтожить хранящиеся в них запасы крови, донорские органы и вакцины, что может повлечь необратимые последствия.

Ввиду нарастающей криминальной активности в отношении КИИ РФ существует потребность в эффективной модели ее уголовно-правовой охраны. Однако специалисты указывают на имеющиеся проблемы с толкованием признаков состава преступления, предусмотренного статьей 274.1 УК РФ[8]. Сложности, связанные с юридической оценкой противоправных деяний, возникают и в процессе правоприменения. Даже принятие постановления Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть “Интернет”»[9] не помогло разрешить коллизионные проблемы. По мнению Л. Л. Кругликова, С. Д. Бражника, И. А. Пилясова, запрет конструируется так, что лишает правоприменителя возможности применять и понимать содержание нормы[10]. Поэтому сто́ит остановиться на рассмотрении имеющихся теоретико-прикладных проблем уголовно-правовой охраны КИИ РФ в целях совершенствования нормы, предусмотренной статьей 274.1 УК РФ, и практики применения положений уголовного законодательства.

Предмет преступления: дискуссионный аспект

В соответствии со ст. 2 и 10 Федерального закона от 26.06.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее — Закон № 187-ФЗ)[11] объект КИИ РФ подлежит категорированию, и ему либо присваивается категория значимости (первая, вторая или третья), либо не присваивается. Однако уголовно-правовой охране (исходя из буквального понимания нормы) подлежат все объекты КИИ РФ (в том числе без категории). Полагаем, что уголовный закон не учитывает основной идеи Закона № 187-ФЗ относительно категорирования.

В связи с этим как в доктрине, так и в судебно-следственной практике сложились два подхода к оценке предмета преступного посяг-

---

7 Может ли цифровая медицина противостоять хакерам // URL: https://habr.com/ru/companies/trendmicro/articles/441908/ (дата обращения: 10.11.2024).

8 *Бегишев И. Р.* Проблемы противодействия преступным посягательствам на информационные системы критически важных и потенциально опасных объектов // Информационная безопасность регионов. 2010. № 1 (6). С. 9–13 ; *Он же.* Уголовно-правовая охрана информационной инфраструктуры критически важных и потенциально опасных объектов Российской Федерации // Россия — правовое государство: проблемы и пути формирования: материалы Всероссийской научно-практической конференции (г. Дербент, 4 марта 2010 г.). Дербент, 2010. С. 116–119 ; *Он же.* Понятие и виды преступлений в сфере обращения цифровой информации : автореф. дис. … канд. юрид. наук. Казань, 2017 ; *Малыгин И. И.* Актуальные проблемы квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации // Известия Юго-Западного государственного университета. Серия «История и право». 2023. Т. 13. № 2. С. 165–176. URL: https://doi.org/10.21869/2223-1501-2023-13-2-165-176 ; *Шульга А. В., Галиакбаров Р. Р.* Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) // Гуманитарные, социально-экономические и общественные науки. 2018. № 5. С. 238–242.

9 Российская газета. 2022. 28 декабря.

10 *Кругликов Л. Л., Бражник С. Д., Пилясов И. А.* Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ): некоторые проблемы определения признаков состава преступления // Журнал юридических исследований. 2019. № 3. С. 53–62.

11 СЗ РФ. 2017. № 31 (ч. I). Ст. 4736.

гательства, кардинальным образом отличающиеся друг от друга.

Первый подход связан с отнесением к предмету преступного посягательства всех объектов КИИ РФ (в том числе тех, которым не присвоена соответствующая категория). Подобной позиции придерживаются и некоторые суды. Так, по делу от 23.12.2021 № 1-148/2021 гражданин М. был признан виновным в совершении преступления, предусмотренного частью 4 ст. 274.1. В данном деле принадлежность к субъектам КИИ РФ установлена исходя из того, что учреждение относится к сфере здравоохранения (упоминается в Законе № 187-ФЗ)[12]. Сходная позиция приводится и в другом решении суда[13]. Второй подход основывается на том, что отечественный уголовный закон охраняет только значимые объекты КИИ РФ, то есть те, которые имеют соответствующую категорию. Так, по материалам дела от 28.04.2022 № 1-14/2022 (1-263/2021)[14], медицинская сестра вносила заведомо ложные сведения в информационную систему (ИС) о проведении профилактических прививок гражданам. В судебном решении констатируется, что, согласно письму Минздрава России от 27.08.2021[15], Единая государственная информационная система в сфере здравоохранения (ЕГИСЗ) относится к значимым объектам КИИ РФ.

На наш взгляд, значимость объекта КИИ РФ и его категория косвенно указывают на общественную опасность преступного посягательства, но в тексте УК РФ данное умозаключение не находит отражения, что в целом усложняет процесс правоприменения. И всё же, как нам представляется, объекты КИИ РФ, не имеющие подобной категории, не соответствуют показателям значений, установленных отраслевым законом.

В уголовно-правовой доктрине эта проблема также поднимается авторами. Л. Л. Кругликов, С. Д. Бражник, И. А. Пилясов отмечают, что редакция ст. 274.1 УК РФ не учитывает дифференциацию по категориям значимости, что является упущением[16].

В доктрине имеется и иная точка зрения. По мнению Д. С. Мирного, квалификация должна учитывать фактическую социальную ценность функционирования затронутых посягательством объектов КИИ независимо от факта их категорирования[17].

Основываясь на положениях базового Закона № 187-ФЗ и основной идее, вытекающей из него, полагаем, что следует признавать преступным только воздействие на значимый объект КИИ РФ, при этом посягательства на объекты КИИ без соответствующей категории квалифицировать по ст. 272–274 УК РФ.

Проблема конструирования объективной стороны состава преступления, предусмотренного частью 1 ст. 274.1 УК РФ

Спектр применения множества компьютерных программ, в том числе вредоносных, широк. Они могут быть использованы и против объектов КИИ РФ. В то же время создание компьютерных программ для посягательств на определенные объекты КИИ РФ маловероятно, так как такая компьютерная программа должна быть специально разработана именно для воздействия на объект КИИ РФ, что подтверждается понятием «заведомо» в конструкции уголовно-правовой нормы, свидетельствующим о прямом умысле лица на совершение преступления.

Таким образом, в контексте ч. 1 ст. 274.1 УК РФ говорится о таких компьютерных программах, которые будут специально разработаны под отдельный объект КИИ РФ. Обязательно следует доказать заведомость. Но бóльшая часть компьютерных программ имеет универсальный характер и широкий спектр применения, то есть используется против лю-

[12] URL: https://www.securitylab.ru/blog/personal/valerykomarov/351780.php (дата обращения: 09.11.2024).

[13] Апелляционное определение Астраханского областного суда от 14.04.2022 № 22-787/2022 // URL: https://nalogcodex.ru/sud_pract/sou/apellyatsionnoe-opredelenie-astrahanskogo-oblastnogo-suda-(astrahanskaya-oblast)-ot-14.04.2022-_-22-787_2022 (дата обращения: 09.11.2024).

[14] URL: https://xn--90afdbaav0bd1afy6eub5d.xn--p1ai/65072117 (дата обращения: 09.11.2024).

[15] СПС «КонсультантПлюс».

[16] *Кругликов Л. Л., Бражник С. Д., Пилясов И. А.* Указ. соч. С. 53–62.

[17] *Мирный Д. С.* Функционирование значимых объектов критической информационной инфраструктуры как объект преступлений, предусмотренных статьей 274.1 УК РФ // Закон и право. 2024. № 6. С. 229–233 ; *Бегишев И. Р.* Безопасность критической информационной инфраструктуры Российской Федерации // Безопасность бизнеса. 2019. № 1. С. 27–32.

бой компьютерной информации, в том числе и против КИИ РФ. Как подчеркивают Р. И. Дремлюга, С. С. Зотов и В. Ю. Павлинская, большинство вредоносных средств обладают широким спектром применения и могут использоваться против объектов КИИ[18].

Несомненно, общественная опасность создания, распространения или использования компьютерных программ либо иной компьютерной информации учитывается нормотворческими органами, что нашло свою реализацию в ст. 273 УК РФ. Вместе с тем следует оценить, повышается ли степень общественной опасности компьютерных программ либо иной компьютерной информации, если они заведомо предназначены для неправомерного воздействия именно на КИИ РФ.

Судебно-следственной практике известны примеры применения ст. 274.1 УК РФ к случаям неправомерного использования компьютерных программ широкого спектра применения, то есть предназначенных не только для воздействия на КИИ РФ. DDoS-атаки используют в отношении ИС субъектов КИИ РФ, даже в отношении ресурсов Министерства обороны РФ и сайта Президента РФ с целью блокирования доступа к ним. Гражданин К. оказывал помощь Украине путем осуществления DDoS-атак на ИС Министерства обороны РФ и сайт Президента РФ. Ростовский областной суд признал его виновным в совершении преступления, предусмотренного частью 1 ст. 274.1 УК РФ[19]. Уточним: для вменения ч. 1 ст. 274.1 УК РФ необходимо доказать, что компьютерные программы либо иная компьютерная информация заведомо предназначены для неправомерного воздействия на КИИ РФ. Возможности DDoS-атак (осуществление вредоносных компьютерных атак, создающих нагрузку на сервер и приводящих к отказу системы в обслуживании) давно известны злоумышленникам и активно реализуются ими в процессе совершения преступлений для блокирования охраняемой законом компьютерной информации[20]. Применение DDoS-атак началось задолго до вступления в силу Закона № 187-ФЗ, поэтому едва ли компьютерную программу — DDoS-атаку можно называть предназначенной именно для воздействия на КИИ РФ (а не просто на всю компьютерную информацию в целях ее блокирования), как это трактуется судебно-следственными органами. М. А. Ефремова также придерживается позиции, согласно которой без формулирования критериев отграничения общих вредоносных программ от программ против КИИ РФ сложно говорить о правильной квалификации[21].

В связи с этим считаем уместным поставить вопрос о декриминализации состава преступления (ч. 1 ст. 274.1 УК РФ), предусмотрев ответственность за совершение деяния, его образующего, по соответствующим частям ст. 273 УК РФ.

Вред как криминообразующий признак в составах преступлений, предусмотренных частями 2 и 3 ст. 274.1 УК РФ: проблема оценки

Обратим внимание на определенную сложность в конструировании представленного уголовно-правового запрета, который содержит признаки как ст. 272, так и ст. 273 УК РФ, что демонстрирует общие начала конструирования уголовно-правовых норм (ст. 272, 273, 274.1). Состав преступления, предусмотренный частью 1 ст. 272, включает наступление общественно опасных последствий. Пункт 5 постановления Пленума № 37 раскрывает понятие «неправомерный доступ к компьютерной информации» применительно к ст. 272, а не к ст. 274.1 УК РФ. Для состава преступления, предусмотренного частью 2 ст. 274.1, обязательно причинение вреда КИИ РФ, а не последствий в виде «уничтожения, блокирования, модификации либо копирования компьютерной информации». При этом

---

[18] *Дремлюга Р. И., Зотов С. С., Павлинская В. Ю.* Критическая информационная инфраструктура как предмет преступного посягательства // Азиатско-Тихоокеанский регион: экономика, политика, право. 2019. Т. 21. № 2. С. 130–139.

[19] IT-специалист из Ростовской области получил три года колонии-поселения за атаку на госсайты // URL: https://www.securitylab.ru/news/538319.php ; URL: https://www.securitylab.ru/news/538319.php (дата обращения: 09.11.2024).

[20] Всё, что вы хотели знать о DDoS-атаках // URL: https://softline.ru/about/blog/vse-chto-vy-hoteli-znat-o-ddos-atakah (дата обращения: 09.11.2024).

[21] *Ефремова М. А.* Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Вестник Казанского юридического института МВД России. 2022. Т. 13. № 4 (50). С. 86–92.

неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ РФ, совершается с использованием компьютерных программ, либо иной компьютерной информации, либо иных вредоносных компьютерных программ.

Е. А. Русскевич к такому вреду относит «уничтожение, блокирование, модификацию, копирование информации, нейтрализацию средств защиты информации или выведение из строя аппаратных и программных средств, обеспечивающих функционирование КИИ РФ»[22]. Однако конструкция составов преступлений, предусмотренных статьями 272 и 274.1 УК РФ, разная.

Понятие вреда недостаточно конкретизировано, что детерминирует субъективность в процессе правоприменения. В то же время Верховный Суд РФ обязывает суды мотивировать, в чем выразился вред, причиненный КИИ РФ[23].

В уголовно-правовой доктрине единообразная позиция относительно толкования вреда, причиненного КИИ РФ, отсутствует. В связи с этим согласимся с Е. А. Соловьевой, которая полагает, что вред может носить иной (не только имущественный) характер[24]. Но Закон № 187-ФЗ не регламентирует безопасность субъекта экономической деятельности, так как он в целом посвящен безопасности государства.

Д. С. Мирный предлагает слова «причинение вреда» в ст. 274.1 УК РФ заменить словами «нарушение устойчивого функционирования» для уточнения содержания уголовной ответственности и приближения закона к сущности ценностей, охраняемых профильным законодательством, исключив при этом привлечение к мерам уголовно-правового реагирования за недостаточно определенный круг посягательств, которые могут причинить неопределенный вред элементу КИИ[25].

По мнению Ю. В. Трунцевского, вред может быть тоже абсолютно разным[26].

С точки зрения И. Н. Мосечкина, конструкция ч. 2 ст. 274.1 УК РФ затрудняет работу правоприменителя. Кроме того, усугубляет ситуацию неконкретизированный вред КИИ РФ[27], с чем невозможно не согласиться.

В судебно-следственной практике под вредом КИИ РФ понимают:

1) нарушение объективности, достоверности и актуальности компьютерной информации, циркулирующей в базах данных объектов КИИ РФ[28];

2) вред, нанесенный деловой репутации субъекта КИИ РФ[29];

3) имущественный ущерб, нанесенный субъекту КИИ РФ[30].

---

[22] *Русскевич Е. А.* Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации : дис. … д-ра юрид. наук. М., 2020.

[23] Постановление Пленума Верховного суда РФ от 29.11.2016 № 55 «О судебном приговоре» // Российская газета. 2016. 7 декабря.

[24] *Соловьева Е. А.* Вред как криминообразующий признак в составах преступлений, предусмотренных частями 2 и 3 статьи 274.1 УК РФ // Пермский юридический альманах. 2023. № 6. С. 560–561.

[25] *Мирный Д. С.* О соотношении объекта преступлений, предусмотренных ст. 274.1 УК РФ, и объекта охраны законодательства в сфере безопасности критической информационной инфраструктуры // Государственная служба и кадры. 2024. № 3. С. 193–197.

[26] *Трунцевский Ю. В.* Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов // Журнал российского права. 2019. № 5. С. 99–106.

[27] *Мосечкин И. Н.* Проблемы уголовно-правовой охраны критической информационной инфраструктуры Российской Федерации // Всероссийский криминологический журнал. 2023. Т. 17. № 1. С. 22–34.

[28] Дело от 19.02.2021 № 1-88/2021 // URL: https://xn--90afdbaav0bd1afy6eub5d.xn--p1ai/57016749 ; Вынесен обвинительный приговор в отношении Ф., обвиняемой в совершении преступления, предусмотренного ч. 4 ст. 274.1 УК РФ // URL: https://pskov.bezformata.com/listnews/obvinyaemoy-v-sovershenii-prestupleniya/136291547/ (дата обращения: 09.11.2024).

[29] Дело от 19.02.2021 № 1-88/2021 ; решение по уголовному делу от 29.07.2020 № 1-805/2020 // URL: https://abakansky--hak.sudrf.ru/modules.php?delo_id=1540006&name=sud_delo&name_op=doc&new=0&number=20399213&srv_num=1&text_number=1 (дата обращения: 09.11.2024).

[30] Приговор Первомайского районного суда г. Владивостока (Приморский край) от 25.09.2019 по делу № 1-376/2019 // URL: https://pervomaysky--prm.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=13978988&delo_id =1540006&new=0&text_number=1 (дата обращения: 09.12.2024).

Однако, согласно ст. 1 и 2 Закона № 187-ФЗ, нарушение работы и прекращение деятельности ИС, информационно-телекоммуникационных сетей, автоматизированных систем управления (АСУ) субъектов КИИ РФ признается причинением вреда. Согласно ст. 1 приведенного Закона, он регулирует отношения в области обеспечения безопасности КИИ РФ в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак. Следовательно, сто́ит констатировать, что именно компьютерные атаки нарушают безопасность объектов КИИ РФ. Поэтому цель компьютерной атаки — это нарушение и (или) прекращение их функционирования и (или) создание угрозы безопасности обрабатываемой объектами КИИ информации (ст. 2 Закона). В результате компьютерной атаки происходит неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ РФ, что влечет причинение вреда КИИ РФ или иные тяжкие последствия.

Часть 2 ст. 7 Закона № 187-ФЗ дает более детальное описание причинения вреда[31]. Полагаем, что именно указанные виды последствий и заложены в уголовный закон для их оценки как тяжкие, наступление которых (при наличии других признаков состава преступления) влечет ответственность по ч. 5 ст. 274.1 УК РФ.

Пленум Верховного Суда РФ под тяжкими последствиями понимает (п. 14 постановления Пленума № 37)[32]:

— причинение вреда жизни и здоровью человека;

— незаконный оборот компьютерной информации (ее незаконное распространение и собирание);

— воздействие на объекты КИИ РФ, повлекшее приостановку или нарушение их работы.

Юридическая конструкция уголовно-правового запрета сформулирована таким образом, что тяжкие последствия включают в себя следующее (табл. 1):

Таблица 1

Цифровая атака на значимый объект КИИ РФ	Последствия, наступившие в результате цифровой атаки	
	Вред, причиняемый значимому объекту КИИ РФ	Иные негативные последствия, которые возникли у субъекта КИИ РФ

До момента разъяснений Пленума Верховного Суда РФ в теории специалистами предлагались различные позиции по определению тяжких последствий. Ю. В. Трунцевский и М. А. Ефремова[33] в своих работах относили к тяжким применительно к ч. 5 ст. 274.1 УК РФ также широкий круг вредных последствий, распространяющихся как на объекты КИИ, так и в целом на деятельность субъектов КИИ. Выводы, сформулированные авторами, нашли свое отражение в постановлении Пленума № 37. Однако в акте толкования одно определяемое («тяжкие последствия») трактуется через другой термин («длительная приостановка»), что, по нашему мнению, не вносит какой-либо ясности в понимание тяжких последствий и снова вызывает сложности у правоприменительных органов. Резонный вопрос: что следует понимать под длительной приостановкой работы предприятия? Приостановление его работы на сутки или больше?

Законодательный подход, связанный с установлением неконкретизированных общественно опасных последствий, не соответствует конструкции ст. 274 УК РФ, также закрепляющей ответственность за несоблюдение обязательных требований (правил). В результате возникла рассогласованность между нормами регулятивного и уголовного законодательства, направленного на охрану подобных обществен-

[31] «…Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимальное по времени отсутствие доступа к государственной услуге для получателей услуг».

[32] «…В частности, длительную приостановку или нарушение работы предприятия, учреждения или организации, получение доступа к информации, составляющей охраняемую законом тайну, предоставление к ней доступа неограниченному кругу лиц, причинение по неосторожности смерти, тяжкого вреда здоровью хотя бы одному человеку и т.п.».

[33] *Ефремова М. А.* Указ. соч. С. 86–92.

ных отношений. Диспозиция уголовно-правовой нормы, закрепленной в ст. 274.1 УК РФ, является бланкетной, и для своего правильного понимания и определения тех или иных категорий, выявления особенностей нормативного регулирования она отсылает нас к базовому Закону № 187-ФЗ. Однако на данный момент корреляция между ними отсутствует. По нашему убеждению, именно это обстоятельство негативным образом сказывается на правоприменении, в том числе в результате несовершенства юридической конструкции уголовно-правового запрета.

В статье 274.1 УК РФ дифференциация ответственности исходя из ущерба (крупный ущерб, тяжкие последствия) не проводится. Отсюда возникает вопрос о юридической технике конструирования запрета, применяемой в других статьях гл. 28 УК РФ.

Вред КИИ РФ, о котором говорится в диспозиции анализируемой уголовно-правовой нормы, представляет собой некую универсальную категорию, которая также включает в себя имущественный ущерб и иные негативные последствия, в том числе нематериального характера. Следовательно, Закон № 187-ФЗ и статья 274.1 УК РФ во взаимосвязи устанавливают, что при определении вреда, причиняемого КИИ РФ, следует учитывать положение п. 4 ст. 2 Закона № 187-ФЗ, закрепляющего понятие «компьютерная атака». Однако это универсальное понятие, которое относится как к последствиям, указанным в ч. 3 и 4 ст. 274.1, так и к ч. 5 ст. 274.1 УК РФ. Но законодатель видит между ними различия, таким образом, наблюдается дифференциация ответственности. При этом постановление Пленума № 37 не раскрывает, что́ следует понимать под вредом КИИ РФ, толкуя только «тяжкие последствия», еще больше усложняя процесс правоприменения, поскольку содержит такую оценочную категорию, как «длительная приостановка работы предприятия».

Исходя из законодательной конструкции уголовно-правового запрета и акта официального толкования, сформулируем, что́ следует относить к вреду КИИ РФ и тяжким последствиям (табл. 2).

Таблица 2

Вред, причиняемый объектам КИИ РФ	**Тяжкие последствия, наступившие в результате неправомерного воздействия на объекты КИИ РФ**
Незначительное нарушение работы предприятия, учреждения или организации	*Прекращение* функционирования объекта КИИ
Создание угрозы безопасности обрабатываемой объектами КИИ информации	*Значительное нарушение* работы предприятия, учреждения или организации
	Получение доступа к информации, составляющей охраняемую законом тайну
	Предоставление к информации, составляющей охраняемую законом тайну, доступа неограниченному кругу лиц
	Причинение смерти по неосторожности
	Причинение тяжкого вреда здоровью хотя бы одному человеку по неосторожности и т.п.
	Крупный ущерб — ущерб, сумма которого превышает 1 млн руб.

На наш взгляд, вред применительно к ст. 274.1 УК РФ следует понимать как причинение его именно КИИ РФ.

В судебной практике также имеются случаи отнесения к причинению вреда КИИ РФ (как общественно опасному последствию) причинение вреда деловой репутации субъекта КИИ (суды относят иногда к объекту КИИ[34]). Однако нам такое решение видится дискуссионным. Статьей 152 ГК РФ охраняется деловая репутация юридического лица. Сложно представить, как может быть причинен вред деловой репутации ИС субъектов КИИ РФ. Вместе с тем деловая репутация юридического лица защищена с точки зрения гражданско-правовых средств воздействия. Возникает вопрос: есть ли необ-

[34] Дело от 19.02.2021 № 1-88/2021.

ходимость в ее уголовно-правовой охране? Кроме того, Закон № 187-ФЗ и его положения во взаимосвязи не регулируют экономические отношения. Поэтому считаем отнесение подобного вида вреда непосредственно к вреду КИИ РФ неверным. Косвенно наш вывод подтверждает и структура Особенной части УК РФ, а именно расположение ст. 274.1 в гл. 28 УК РФ, непосредственно не охраняющей общественные отношения в сфере экономики.

Определение понятия «вред КИИ РФ» вызывает проблемы в судебно-следственной практике, что демонстрирует неоднозначность подходов правоприменителей к юридической оценке подобного вида вреда. Достаточно часто можно встретиться с позицией судов, согласно которой внесение заведомо ложных сведений в информационные системы субъектов КИИ РФ является модификацией компьютерной информации. В таких случаях злоумышленникам инкриминируется ч. 4 ст. 274.1 УК РФ. При этом правоохранительные органы полагают, что, внося недостоверные сведения в ИС КИИ РФ, лица «нарушают целостность» ИС, в результате чего сведения «теряют объективность, достоверность и актуальность».

Так, программист одной из больниц, использовав чужой доступ к ЕГИСЗ, внес заведомо ложные сведения для получения сертификата о вакцинации от коронавируса и QR-кода для себя и своих родственников. В отношении него был вынесен обвинительный приговор по ч. 4 ст. 274.1 УК РФ[35]. Оцениваем весьма положительно оправдательный приговор в отношении О. в связи с отсутствием состава преступления, предусмотренного частью 1 ст. 274.1 УК РФ, за совершение таких деяний (внесение заведомо ложных сведений в ЕГИСЗ о прохождении вакцинации)[36].

Проблема заключается в том, что компьютерная форма вносимых недостоверных сведений фактически позволяет органам предварительного следствия относить их к компьютерной информации, предназначенной для неправомерного воздействия на КИИ. То есть если недостоверные сведения внесены не в информационную систему, а в документы (например, журналы, ведущиеся в бумажном виде), то эти действия влекут оценку как подлог документов, а если внесены цифровые данные в ИС, то лицо подлежит уголовной ответственности по ст. 274.1 УК РФ (тяжкое преступление). Как нам представляется, это обстоятельство свидетельствует о неверном толковании и применении уголовного закона правоприменительными органами. Иначе говоря, неправомерное внесение недостоверных сведений в ИС рассматривается правоохранительными органами как модификация компьютерной информации и как причинение вреда КИИ РФ. Медицинские работники не совершают компьютерную атаку, а используют предоставленные им пароли, логины (сертификаты безопасности) для внесения заведомо ложных сведений, не преследуя цели нарушить или прекратить функционирование объектов КИИ либо создать угрозу обрабатываемой ими информации. Кроме того, имеются случаи осуждения по ст. 274.1 УК РФ за внесение ложных сведений сотрудником в целях сокрытия факта опоздания на работу[37]. Точно так же возникают вопросы о том, каким образом и как была реализована компьютерная атака и как она в целом повлияла на работоспособность и функционирование объекта КИИ РФ.

Исходя из этого действующая редакция уголовно-правового запрета представляется нам не позволяющей единообразно применять положения уголовного закона. Полагаем возможным связать диспозицию нормы непосредственно с цифровой атакой, что позволит судебно-следственным органам единообразно применять положения закона, в том числе не рассматривать случаи неправомерного доступа, не влекущие угрозу функционирования объекта КИИ РФ, как содержащие признаки состава преступления. Поэтому такая юридическая конструкция нормы обязует правоприменителей устанавливать прямую причинно-следственную связь между цифровой атакой и последствиями в виде воздействия на объекты КИИ РФ.

Вернемся к отнесению действий в виде внесения недостоверных сведений в ИС, являющуюся объектом КИИ, к неправомерному воздействию на КИИ РФ. Напрашивается вопрос об общественной опасности подобных деяний: она столь велика, что должна рассматриваться

---

[35] Обзор судебной практики по статье 274.1 УК РФ // Информационная безопасность. 2022. № 2. С. 10–11.

[36] Дело от 28.04.2022 № 1-14/2022 (1-263/2021).

[37] Суд оштрафовал на 200 тыс. руб. системного администратора за внесение изменений в работу СКУД оборонного предприятия // URL: https://habr.com/ru/news/667086/ (дата обращения: 10.12.2024).

как тяжкое преступление? Установив факт внесения заведомо ложных сведений в информационную систему, владелец данных вправе удалить недостоверные сведения из информационной базы. При этом так называемые целостность и актуальность информации будут восстановлены.

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[38] и Закон № 187-ФЗ имеют разные цели применения. Если первый нормативный правовой акт относится к концепции информационного общества и связан с охраной информации (предоставляемой в любом виде), то второй направлен на обеспечение устойчивости функционирования ИС, ИКТС и АСУ при совершении на них компьютерных атак. Поэтому Законом № 187-ФЗ не охраняются информация и ее основные свойства. Ввиду этого сто́ит констатировать, что, внося недостоверные сведения в ИС, ИКТС и АСУ, злоумышленник не посягает на устойчивость функционирования объектов КИИ РФ. Логично поставить и вопрос о том, как внесение недостоверных сведений в систему о проведении вакцинации в целом влияет на национальную безопасность и вообще связано с компьютерными атаками. При этом работоспособность ИС или иных объектов КИИ РФ остается незатронутой и ненарушенной.

На основе проведенного нами исследования предлагаем дополнить постановление Пленума № 37 следующими положениями:

1. Под вредом значимым объектам критической цифровой инфраструктуры РФ как квалифицирующим признаком в ст. 274 УК РФ следует понимать незначительное нарушение функционирования значимых объектов критической цифровой инфраструктуры РФ или создание угрозы безопасности обрабатываемой значимыми объектами критической цифровой инфраструктуры РФ информации.

2. Совершение цифровой атаки на значимые объекты критической цифровой инфраструктуры РФ должно отражаться на устойчивости функционирования объектов критической цифровой инфраструктуры РФ и должно быть связано с нарушением работоспособности значимых объектов критической цифровой инфраструктуры РФ.

3. Судам следует установить, что в результате цифровой атаки на ИС, ИКТС, АСУ или информацию наступают негативные последствия, оказывающие влияние на устойчивость функционирования объекта критической цифровой инфраструктуры РФ.

Проблемы квалификации преступления, предусмотренного частью 3 ст. 274.1 УК РФ

Диспозиция уголовно-правовой нормы является бланкетной и требует обращения (для верного толкования) к законодательным актам. Так, нами уже отмечена рассогласованность между нормами базового отраслевого закона — Закона № 187-ФЗ и уголовного закона. В то же время Закон № 187-ФЗ направлен на регулирование общественных отношений в области обеспечения безопасности КИИ РФ в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак. Следовательно, криминализации должны подлежать деяния, связанные с компьютерной атакой как целенаправленным воздействием программных и (или) программно-аппаратных средств на объекты КИИ. При этом компьютерная атака совершается в целях нарушения и (или) прекращения функционирования объектов КИИ РФ и (или) создания угрозы безопасности обрабатываемой объектами КИИ РФ информации. Однако действующая законодательная конструкция состава преступления, предусмотренного статьей 274.1 УК РФ, вообще не связана с цифровой атакой. Под словом «целенаправленное» мы понимаем реализацию объективной стороны состава преступления с прямым умыслом, чего также не наблюдается в диспозиции уголовно-правовой нормы, закрепленной в ст. 274.1 УК РФ.

В Законе № 187-ФЗ не содержится обязанностей по соблюдению субъектами правил эксплуатации или правил доступа.

Полагаем, что действия лиц по нарушению правил эксплуатации или правил доступа не связаны с реализацией компьютерной атаки. Ввиду этого расположение представленного состава преступления в конструкции ст. 274.1 УК РФ вообще нецелесообразно, поскольку нарушения правил эксплуатации или правил доступа напрямую не связаны с компьютерной атакой.

Криминализировав деяние, законодатель старался тем самым обезопасить (и охранять) национальную безопасность государства. Несомненно, информационная безопасность — часть

[38] СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

национальной безопасности РФ[39], поэтому и противоправные посягательства должны быть направлены против информационной (в нашем случае цифровой) безопасности РФ. В свою очередь, неосторожные действия виновных вообще нельзя назвать целенаправленными в контексте компьютерной атаки. Предлагаем ответственность за нарушение правил эксплуатации либо правил доступа закрепить в ст. 274 УК РФ.

Трансформация информационной инфраструктуры в цифровую

В свете настоящего исследования хотелось бы остановиться на том, что современная информационная инфраструктура с практической (технико-технологической) точки зрения полностью основывается на цифровых технологиях, в том числе в ней применяются методы цифровой обработки, хранения и передачи данных, используются цифровые системы и устройства и в целом цифровое программное обеспечение. Таким образом, цифровые технологии оказывают значительное влияние на базовую форму представления информации — цифровых данных. При этом формируемая цифровая инфраструктура является подвидом информационной инфраструктуры, как бы дополняя ее цифровой составляющей. Поэтому цифровая инфраструктура — часть информационной, и они соотносятся как часть и целое.

По нашему мнению, слово «информационная» в определении «объекты КИИ» и иных («субъекты КИИ» и т.д.) в контексте Закона № 187-ФЗ не в полном объеме раскрывает предназначение таких объектов и их содержание. Вместе с тем категория «информация (информационная)» в контексте КИИ РФ и Закона № 187-ФЗ не отражает процессов, происходящих в современных АСУ и сетях, их объединяющих. Сто́ит уточнить, что обработке цифровыми устройствами и технологиями в сети Интернет подлежит именно цифровая (а не компьютерная) информация. В связи с этим полагаем необходимым в Законе № 187-ФЗ и в ст. 274 и 274.1 УК РФ аббревиатуру «КИИ РФ» заменить на словосочетание «критическая цифровая инфраструктура», а также термин «компьютерная атака» заменить на «цифровая атака».

Заключение

Во-первых, здравоохранение выступает важной сферой общественной жизни, от качества которой зависят продолжительность жизни и сохранность здоровья граждан в целом. Во многих странах сектор здравоохранения рассматривается как важнейшая национальная инфраструктура, наряду с водоснабжением, электричеством и транспортными сетями. Поэтому вопросы уголовно-правовой охраны цифровой инфраструктуры учреждений системы здравоохранения, несомненно, важны и актуальны. Однако предлагаемые нами меры касаются не только непосредственно медицины, а вообще любого субъекта, указанного в Законе № 187-ФЗ, и носят своего рода универсальный характер.

При этом уголовно-правовой запрет должен коррелировать с положениями Закона № 187-ФЗ. По мнению А. П. Кузнецова, законодатель должен стремиться к унификации правовых предписаний, их гармонизации для целенаправленного регулирования правового поведения субъектов с учетом тех или иных социальных интересов[40].

Складывающаяся судебная практика полностью дискредитировала понятие «КИИ РФ», потому что главными источниками угроз КИИ РФ являются, исходя из вышеуказанной судебной практики, студенты, менеджеры, школьники, медицинские сестры и т.д.[41]

Во-вторых, действующая редакция ст. 274.1 УК РФ демонстрирует рассогласованность между положениями УК РФ и Законом № 187-ФЗ. Следовательно, как таковой угрозой безопасности КИИ РФ выступает именно *цифровая атака* (напомним, что в Законе № 187-ФЗ она называется компьютерной атакой).

В-третьих, предлагаем в качестве предмета преступления, предусмотренного статьей 274.1 УК РФ, указать «значимые объекты критической цифровой инфраструктуры РФ».

---

[39] Исходя из Доктрины информационной безопасности Российской Федерации, утв. Указом Президента РФ от 05.12.2016 № 646 // СЗ РФ. 2016. № 50. Ст. 7074.

[40] *Кузнецов А. П.* Проблемы рассогласованности положений главы 22 УК РФ с положениями отраслевых законодательств // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2016. № 2 (34). С. 167–173.

[41] Приговор по делу от 29.07.2020 № 1-805/2020 ; дело от 19.02.2021 № 1-88/2021.

В-четвертых, предлагаем внести следующие изменения в УК РФ:

1. Статья 274:

а) ч. 2 изложить в следующей редакции:

«2. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, обращающейся в значимом объекте критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, либо правил доступа к такой информации, если оно повлекло причинение вреда значимым объектам критической цифровой инфраструктуры Российской Федерации»;

б) дополнить частью 3:

«3. Деяние, предусмотренное частью первой или второй настоящей статьи, если оно повлекло тяжкие последствия».

2. Статья 274.1:

а) наименование изложить в следующей редакции:

«Статья 274.1. Совершение цифровой атаки на значимые объекты критической цифровой инфраструктуры Российской Федерации»;

б) текст изложить в следующей авторской редакции:

«1. Совершение цифровой атаки на значимые объекты критической цифровой инфраструктуры Российской Федерации, —

наказывается…»;

«2. То же деяние, если оно совершено группой лиц по предварительному сговору, или организованной группой, или лицом с использованием своего служебного положения, —

наказывается…»;

«3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия, —

наказываются…».

В-пятых, п. 14 постановления Пленума № 37 предлагаем дополнить определением понятия «вред значимым объектам критической цифровой инфраструктуры РФ как квалифицирующий признак в ст. 274 УК РФ», изменить понятие «тяжкие последствия» как «длительное прекращение (более суток) или значительное нарушение функционирования значимых объектов критической цифровой инфраструктуры Российской Федерации, причинение крупного ущерба… (далее действующего разъяснения)».

Кроме того, п. 14 дополнить следующим абзацем:

«Судам следует установить, находится ли в прямой причинно-следственной связи подвергшийся цифровой атаке значимый объект критической цифровой инфраструктуры Российской Федерации с устойчивостью его функционирования».

СПИСОК ЛИТЕРАТУРЫ

Бахтеев Д. В., *Сосновикова А. М.*, *Казенас Е. В.* Преодоление нелегальной трансграничной передачи персональных данных // Journal of Digital Technologies and Law. 2024. № 2 (4). С. 943–972. DOI: 10.21202/jdtl.2024.45. EDN: MJUIGD.

Бегишев И. Р. Безопасность критической информационной инфраструктуры Российской Федерации // Безопасность бизнеса. 2019. № 1. С. 27–32.

Бегишев И. Р. Понятие и виды преступлений в сфере обращения цифровой информации : автореф. дис. … канд. юрид. наук. Казань, 2017. 30 с. EDN: YRTZMD.

Бегишев И. Р. Проблемы противодействия преступным посягательствам на информационные системы критически важных и потенциально опасных объектов // Информационная безопасность регионов. 2010. № 1 (6). С. 9–13. EDN: MBFKTH.

Бегишев И. Р. Уголовно-правовая охрана информационной инфраструктуры критически важных и потенциально опасных объектов Российской Федерации // Россия — правовое государство: проблемы и пути формирования: материалы Всероссийской научно-практической конференции (г. Дербент, 4 марта 2010 г.). Дербент, 2010. С. 116–119. EDN: YOTKDM.

Дремлюга Р. И., *Зотов С. С.*, *Павлинская В. Ю.* Критическая информационная инфраструктура как предмет преступного посягательства // Азиатско-Тихоокеанский регион: экономика, политика, право. 2019. Т. 21. № 2. С. 130–139.

Ефремова М. А. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Вестник Казанского юридического института МВД России. 2022. Т. 13. № 4 (50). С. 86–92. DOI: 10.37973/KUI.2022.10.11.011.

Кругликов Л. Л., *Бражник С. Д.*, *Пилясов И. А.* Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ): некоторые проблемы определения признаков состава преступления // Журнал юридических исследований. 2019. № 3. С. 53–62.

Кузнецов А. П. Проблемы рассогласованности положений главы 22 УК РФ с положениями отраслевых законодательств // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2016. № 2 (34). С. 167–173.

Малыгин И. И. Актуальные проблемы квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации // Известия Юго-Западного государственного университета. Серия «История и право». 2023. Т. 13. № 2. С. 165–176.

Малыгин И. И. Уголовно-правовое противодействие неправомерному воздействию на критическую информационную инфраструктуру : автореф. дис. … канд. юрид. наук. М., 2023. 24 с.

Мирный Д. С. О соотношении объекта преступлений, предусмотренных ст. 274.1 УК РФ, и объекта охраны законодательства в сфере безопасности критической информационной инфраструктуры // Государственная служба и кадры. 2024. № 3. С. 193–197.

Мирный Д. С. Функционирование значимых объектов критической информационной инфраструктуры как объект преступлений, предусмотренных статьей 274.1 УК РФ // Закон и право. 2024. № 6. С. 229–233. DOI: 10.24412/2073-3313-2024-6-229-233.

Мосечкин И. Н. Проблемы уголовно-правовой охраны критической информационной инфраструктуры Российской Федерации // Всероссийский криминологический журнал. 2023. Т. 17. № 1. С. 22–34. DOI: 10.17150/2500-1442.2023.17(1).22-34. EDN: OLQBCA.

Русскевич Е. А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации : дис. … д-ра юрид. наук. М., 2020. 521 с. EDN: IXNSFI.

Русскевич Е. А. Уголовная ответственность за преступления в сфере компьютерной информации по законодательству Китайской Народной Республики: сравнительно-правовой анализ // Журнал зарубежного законодательства и сравнительного правоведения. 2018. № 5. С. 108–113.

Соловьева Е. А. Вред как криминообразующий признак в составах преступлений, предусмотренных частями 2 и 3 статьи 274.1 УК РФ // Пермский юридический альманах. 2023. № 6. С. 560–561.

Трунцевский Ю. В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов // Журнал российского права. 2019. № 5. С. 99–106.

Шульга А. В., *Галиакбаров Р. Р.* Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) // Гуманитарные, социально-экономические и общественные науки. 2018. № 5. С. 238–242.

REFERENCES

Bakhteev DV, Sosnovikova AM, Kazenas EV. Overcoming illegal cross-border transfer of personal data. *Journal of Digital Technologies and Law.* 2024;2(4):943-972. (In Russ.). DOI: 10.21202/jdtl.2024.45. EDN: MJUIGD.

Begishev IR. Criminal law protection of the information infrastructure of critical and potentially dangerous facilities of the Russian Federation. In: Russia — the rule of law: Problems and ways of formation. Proceedings of the All-Russian Scientific and Practical Conference. Derbent; 2010. (In Russ.).

Begishev IR. Problems of counter action to the criminal encroachments on the information systems of critical and potentially dangerous objects. *Informatsionnaya bezopasnost regionov.* 2010;1(6):9-13. (In Russ.).

Begishev IR. Security of critical information infrastructure of the Russian Federation. *Bezopasnost biznesa*. 2019;1:27-32. (In Russ.).

Begishev IR. The Concept and Types of Crimes in the Sphere of Digital Information Circulation. Cand. Sci. (Law). Author's Abstract. Kazan; 2017.

Dremlyuga RI, Zotov SS, Pavlinskaya VYu. Critical information infrastructure as object of a criminal offence. *PACIFIC RIM: Economics, Politics, Law*. 2019;21(2):130-139. (In Russ.).

Efremova MA. Criminal liability for unlawful impact on the critical information infrastructure of the Russian Federation. *Bulletin of the Kazan Law Institute of MIA Russia*. 2022;13(4(50)):86-92. (In Russ.). DOI: 10.37973/KUI.2022.10.11.011.

Kruglikov LL, Brazhnik SD, Pilyasov IA. Undue influence on the critical information infrastructure of the Russian Federation (article (article 274.1 of the criminal code of the Russian Federation): some problems of definition of signs of a crime. *Journal of legal Studies*. 2019;3:53-62. (In Russ.).

Kuznetsov AP. Problems of legal inconsistencies between the provisions of chapter 22 of the criminal code and the provisions of branch legislation. *Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*. 2016;2(34):167-173. (In Russ.).

Malygin II. Actual problems of qualification of unlawful impact on the critical information infrastructure of the Russian Federation. Proceedings of Southwest State University. The series: History and Law. 2023;13(2):165-176. (In Russ.). https://doi.org/10.21869/2223-1501-2023-13-2-165-176.

Malygin II. Criminal law counteraction to unlawful impact on critical information infrastructure. Cand. Sci. (Law). Author's Abstract. Moscow; 2023. (In Russ.).

Mirny DS. On the ratio of the object of crimes provided for in article 274.1 of the criminal code of the Russian Federation and the object of protection of legislation in the field of security of critical information infrastructure. *Gosudarstvennaya sluzhba i kadry*. 2024. № 3. С. 193–197.

Mirny DS. Operation of significant objects of critical information infrastructure as an object of crimes provided for in article 274.1 of the Criminal Code of the Russian Federation. *Zakon i pravo*. 2024;6:229-233. (In Russ.). DOI: 10.24412/2073-3313-2024-6-229-233.

Mosechkin IN. Problems of the criminal law protection of critical information infrastructure of the Russian Federation. *Russian Journal of Criminology*. 2023;17(1):22-34. (In Russ.). DOI: 10.17150/2500-1442.2023.17(1).22-34.

Russkevich EA. Criminal liability for computer crimes under the laws of the chinese people's republic: comparative-legal analysis*. Journal of Foreign Legislation and Comparative Law*. 2018;5:108-113. (In Russ.).

Russkevich EA. Differentiation of responsibility for crimes committed with the use of information and communication technologies and problems of their qualification. Dr. Sci. (Law) Diss. Moscow; 2020. (In Russ.).

Shulga AV, Galiakbarov RR. Ugolovnaya otvetstvennost' za nepravomernoye vozdeystviye na kriticheskuyu informatsionnuyu infrastrukturu Rossiyskoy Federatsii (st. 274.1. UK RF) [Criminal Liability for Unlawful Interference with the Critical Information Infrastructure of the Russian Federation (Art. 274.1, Criminal Code of the Russian Federation)]. *Humanities, Social-Economic and Social Sciences*. 2018;5:238-242. (In Russ.).

Solovyeva EA. Harm as a criminogenic factor in the *corpus delicti* under Part 2 and 3 of Article 274.1 of the Criminal Code of the Russian Federation (hereinafter referred to as CC of the RF). *Perm Legal Almanac*. 2023;6:560-561. (In Russ.).

Truntsevskiy YuV. Unlawful impact on critical information infrastructure: the criminal liability of its owners and operators. *Journal of Russian Law*. 2019;5:99-106. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Шутова Альбина Александровна, кандидат юридических наук, старший научный сотрудник Научно-исследовательского института цифровых технологий и права, доцент кафедры уголовного права и процесса Казанского инновационного университета имени В.Г. Тимирясова
Московская ул., д. 42, г. Казань 420111, Российская Федерация
shutova1993@inbox.ru

INFORMATION ABOUT THE AUTHOR

Albina A. Shutova, Cand. Sci. (Law), Senior Researcher, Research Institute of Digital Technologies and Law, Associate Professor, Department of Criminal Law and Process, Kazan Innovation University named after V.G. Timiryasov, Kazan, Russian Federation
shutova1993@inbox.ru

Материал поступил в редакцию 14 декабря 2024 г.
Статья получена после рецензирования 12 февраля 2025 г.
Принята к печати 15 августа 2025 г.

Received 14.12.2024.
Revised 12.02.2025.
Accepted 15.08.2025.