Научная статья
УДК 343.9
DOI 10.33184/vest-law-bsu-2025.28.28

Иванов Александр Сергеевич
ООО «Ритейл Дата-центр Технологии»; Российский государственный университет правосудия имени В.М. Лебедева, Москва, Россия, webhoster@yandex.ru

СИСТЕМА МОНИТОРИНГА ДВИЖЕНИЯ ЛЕКАРСТВЕННЫХ ПРЕПАРАТОВ КАК ОБЪЕКТ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. Система мониторинга движения лекарственных препаратов была создана в России и внедрена в фармацевтическую отрасль для защиты граждан от фальсифицированных и некачественных препаратов. Цель: анализ правового статуса и значения системы мониторинга движения лекарственных препаратов (МДЛП) в контексте законодательства о защите критической информационной инфраструктуры (КИИ) Российской Федерации. Методы: эмпирическое описание, интерпретация; теоретические методы формальной и диалектической логики. Автор исследует аспекты социальной, экономической и национальной значимости системы, анализирует риски, связанные с нарушением ее функционирования, и проводит оценку роли МДЛП в обеспечении устойчивости лекарственного снабжения населения и защиты национальной безопасности. Результаты: на основе сопоставления требований нормативно-правовой базы и проведенного анализа рисков обосновывается необходимость признания МДЛП объектом КИИ первой категории. Работа сочетает правовой и междисциплинарный подход, раскрывая место МДЛП в системе цифрового государственного контроля.

Ключевые слова: фармацевтический рынок, информационная инфраструктура, информационная безопасность, правовое регулирование

Для цитирования: Иванов А.С. Система мониторинга движения лекарственных препаратов как объект критической информационной инфраструктуры Российской Федерации / А.С. Иванов. – DOI 10.33184/vest-law-bsu-2025.28.28 // Вестник Института права Башкирского государственного университета. – 2025. – № 4. – С. 309–320.

Original article

Ivanov Alexander Sergeevich
Retail Data Center Technologies LLC; Lebedev Russian State University of Justice, Moscow, Russia, webhoster@yandex.ru

THE PHARMA DRUG MOVEMENT MONITORING SYSTEM AS AN OBJECT OF THE CRITICAL INFORMATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION

Abstract. The Drug Movement Monitoring System was developed in Russia and implemented in Russian pharmaceutical sector to protect citizens from counterfeit and substandard medicines. Purpose: to analyze the legal status and significance of the Drug Movement Monitoring System (MDLP) in the context of Russian legislation on the protection of critical information infrastructure (CII). Methods: empirical descriptions, interpretations; theoretical methods of formal and dialectical logic. The author explores the social, economic, and national systems, analyzes the risks associated with disruptions to its functioning, and assesses the role of the MDLP in ensuring the stability of pharmaceutical supply and safeguarding national security. The study substantiates the necessity of recognizing the MDLP as a first-category CII object by comparing the requirements of the regulatory framework and the results of the risk analysis. The research integrates legal and interdisciplinary approaches, revealing the role of the MDLP within the system of digital state control.

***Keywords**:* pharmaceutical market, information infrastructure, information security, legal regulation

For citation: Ivanov A.S. The Pharma Drug Movement Monitoring System as an Object of the Critical Information Infrastructure of the Russian Federation. *Vestnik Instituta prava Bashkirskogo gosudarstvennogo universiteta = Bulletin of the Institute of Law of the Bashkir State University,* 2025, no. 4, pp. 309–320 (In Russian). DOI 10.33184/vest-law-bsu-2025.28.28.

Введение. Система мониторинга движения лекарственных препаратов (МДЛП) была создана в России и в обязательном порядке внедрена в фармацевтическую отрасль для того, чтобы обеспечить прозрачность пути и контроль движения каждого лекарства – от завода до аптеки или больницы. Основная цель – защита граждан от фальсифицированных и некачественных препаратов. Благодаря системе можно отследить, где именно находится каждая упаковка, кто ее произвел, когда ввел в оборот и кому продал.

Система МДЛП начала действовать в полном объеме с 1 июля 2020 года, после нескольких лет пилотного проекта. Ее внедрение предусмотрено федеральным законом № 425-ФЗ от 28 декабря 2017 года и регулируется подзаконными нормативными актами. Администрирует систему Центр развития пер-

спективных технологий (ООО «Оператор-ЦРПТ», далее – ЦРПТ), который является назначенным государством оператором национальной системы цифровой маркировки «Честный знак». Контроль за реализацией проекта осуществляют Минздрав, Росздравнадзор и Минпромторг России.

Работа системы основана на обязательной маркировке каждой упаковки лекарственного средства уникальным цифровым кодом – DataMatrix. Этот код содержит сведения о производителе, названии, серии и сроке годности препарата. Когда лекарство производится, его код заносится в систему МДЛП. Далее, при каждой операции – импорте, оптовой продаже, передаче в аптеку или медицинскую организацию – каждый из участников рынка передает информацию о движении этой конкретной упаковки в систему МДЛП, а ее внутренние технологические механизмы обеспечивают контроль за корректностью и полнотой переданной информации. В итоге в систему МДЛП выстраивается полная цепочка движения каждой упаковки лекарственных препаратов. Если упаковка с определенным кодом появляется в продаже, но не имеет истории в системе, это сигнал о возможной подделке.

Хранимые в системе МДЛП данные предоставляются государственным органам и уполномоченным организациям для выполнения их контрольных и надзорных функций. Доступ к информации имеют Минздрав, Росздравнадзор, ФНС, ФТС и другие ведомства, участвующие в регулировании обращения лекарственных средств. Эти данные используются для мониторинга законности оборота препаратов, анализа обеспеченности регионов лекарствами и выявления нарушений или рисков дефицита, то есть информация из системы МДЛП служит не только инструментом отслеживания, но и основой для принятия управленческих решений в сфере здравоохранения.

Таким образом, система МДЛП обеспечивает контроль, прозрачность и достоверность данных обо всех лекарствах, обращающихся в стране.

Социальная значимость. Обеспечение доступности и качества лекарственных средств напрямую связано с сохранением жизни и здоровья граждан. Любые сбои в функционировании системы МДЛП неминуемо отражаются на доступности препаратов, могут приводить к задержкам поставок, возникновению локальных дефицитов и росту смертности в уязвимых группах населения. Статистическая информация, формируемая на основе данных системы МДЛП, используется государственными органами для контроля полноты лекарственного обеспечения и своевременного реагирования на угрозы дефицита.

Нарушение стабильности системы способно усугубить эпидемиологическую ситуацию, что особенно критично в условиях пандемий и сезонных эпидемий. Масштаб последствий может быть сопоставим с угрозами, возникающими при сбоях в таких базовых инфраструктурах, как энергетика, транспорт или поставки продовольствия.

В обзоре «Impact of Drug Shortages on Patients in the United States»[1], основанном на данных аналитического агентства IQVIA Medical Claims за 2016–2020 годы, отмечается, что дефицит лекарств – особенно инъекционных онкопрепаратов – приводит к значительной клинической нагрузке, росту заболеваемости и смертности среди пациентов с раком. Этот пример хорошо иллюстрирует, как сбои в цепочках поставок препаратов могут сказаться на общей доступности жизненно важных препаратов для населения. А ведь таким сбоем может оказаться и процесс отчетности в систему МДЛП в случае ее недоступности, так как без подтверждения системы МДЛП об успешной отчетности одного шага участники оборота препаратов не могут перейти к следующему.

Стоит отметить, что по данным Минздрава России, к концу 2023 года перечень потенциально дефицитных лекарств за год увеличился на 58 позиций и составил 153 товарных наименования[2]. Также в первом квартале 2024 года опрос российских врачей выявил, что около 78,5 % опрошенных жалуются на дефицит лекарств в количестве более 400 товарных наименований, 74 из которых входят в перечень жизненно необходимых и важнейших лекарственных препаратов (ЖНВЛП)[3]. Эти факты показывают, что дефицит лекарств – далеко не абстрактная угроза, а существующая, при полностью функционирующей с 2020 года системе МДЛП, реальность.

Экономическая значимость. Фармацевтический рынок является стратегическим сектором экономики с многомиллиардным оборотом. Несмотря на значимость, он требует значительного контроля из-за своей привлекательности для фальсификаций и коррупционных схем. И данный тезис справедлив не только для России, но и на общемировом уровне. Согласно данным доклада «Trade in Counterfeit Pharmaceutical Products», оценивающего, как международная торговля поддельными лекарствами наносит ущерб экономике, подрывает доверие и влияет на здоровье граждан, в 2016 году масштаб международной торговли поддельными лекарствами оценивался примерно в 4,4 млрд

---

[1] Impact of Drug Shortages on Patients in the United States: A Case Study of Three Drugs: Office of the Assistant Secretary for Planning and Evaluation (ASPE); Washington (DC), 2024 [Электронный ресурс]. URL: https://www.ncbi.nlm.nih.gov/books/NBK608930/ (дата обращения: 20.10.2025).

[2] Перечень потенциально дефицитных лекарств за год увеличился на 58 позиций [Электронный ресурс] // РБК : сайт. URL: https://www.rbc.ru/society/30/12/2023/658f5d509a79477bcdfb14d5 (дата обращения: 20.10.2025).

[3] Корочкина А. Почти 80% опрошенных российских врачей пожаловались на дефицит лекарств [Электронный ресурс] // Forbes. 11 марта 2024. URL: https://www.forbes.ru/biznes/507888-pocti-80-oprosennyh-rossijskih-vracej-pozalovalis-na-deficit-lekarstv (дата обращения: 20.10.2025).

долларов[4]. А по данным ВОЗ от 3 декабря 2024 года, страны тратят уже около 30,5 млрд долларов США в год на некачественную и фальсифицированную медицинскую продукцию[5].

Таким образом, нарушения в работе системы МДЛП могут привести к существенным экономическим потерям, включая срыв государственных закупок, рост теневого оборота и распространение поддельных препаратов. Система выполняет функцию прозрачного контроля сроков годности, налоговых и таможенных операций с препаратами, препятствует реализации коррупционных схем, традиционно характерных для фармацевтического сектора. Так, по данным самой системы МДЛП, с 1 июня по 30 сентября 2025 года в России с помощью системы маркировки пресекли более 85 000 попыток продать просроченные медикаменты[6]. Система МДЛП выступает инструментом защиты законных интересов государства и участников рынка.

Технологический аспект. Система МДЛП объединяет всех участников цепи оборота лекарств: производителей, импортеров, дистрибьюторов, аптечные сети, медицинские организации и органы государственного контроля. Таким образом, любое нарушение работы системы может отразиться на всей цепочке поставок и контроля. Например, летом 2025 года аптеки не смогли продавать препараты из-за отсутствия интернета и связи с системой МДЛП[7]. Другой пример – кибератака и заражение вирусом-шифровальщиком крупного фармацевтического дистрибьютора, что привело к сбоям поставок лекарств в 6 000 аптек по всей Германии[8].

Высокая степень централизации и цифровизации обеспечивает эффективность государственного контроля, но одновременно формирует уязвимость: воздействие на систему даже ограниченного масштаба способно иметь системные последствия для всего фармацевтического рынка. В системе МДЛП ак-

---

[4] Trade in Counterfeit Pharmaceutical Products, Illicit Trade, OECD Publishing, Paris, [Электронный ресурс]. URL: https://doi.org/10.1787/a7c7e054-en. (дата обращения: 20.10.2025).

[5] Substandard and falsified medical products [Электронный ресурс]. URL: https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products (дата обращения: 20.10.2025).

[6] В России пресекли более 85 тыс. попыток продать просроченные лекарства [Электронный ресурс] // РБК : сайт. 08.10.2025. URL: https://www.rbc.ru/rbcfreenews/68e682a09a79476221022ba5 (дата обращения: 20.10.2025).

[7] Гордеева М. Аптеки не могут продать лекарства из-за проблем с интернетом [Электронный ресурс] // Фармацевтический вестник. 09.07.2025. URL: https://pharmvestnik.ru/content/news/Apteki-ne-mogut-prodat-lekarstva-iz-za-problem-s-internetom.html (дата обращения: 20.10.2025).

[8] Martin A. Ransomware attack hits German pharmaceutical wholesaler, disrupts medicine supplies [Электронный ресурс] // therecord.media. November 1st, 2024. URL: https://therecord.media/ransomware-attack-hits-german-pharmaceutical-wholesaler-disruptions (дата обращения: 20.10.2025).

кумулируются данные обо всех операциях с лекарственными препаратами на территории РФ с самого начала маркировки лекарств. С точки зрения аналитики, этих данных достаточно, чтобы полностью проследить всю историю производства, перемещений, импорта, экспорта, продаж и использования любого лекарственного препарата на территории РФ с июля 2020 года, что отражает значительность угрозы в случае утечки этих данных из централизованной системы.

Национальная безопасность. Система МДЛП выполняет роль одного из ключевых инструментов контроля за оборотом жизненно необходимых и стратегически значимых лекарств. Целенаправленные кибератаки на систему способны использоваться как элемент гибридного воздействия, направленного на дестабилизацию социально-экономической ситуации. Потеря или блокировка доступа к данным о движении препаратов может стать фактором угрозы безопасности страны. В связи с этим защита информационной инфраструктуры системы МДЛП должна рассматриваться не только как задача здравоохранения, но и как элемент национальной безопасности, аналогичный защите систем управления транспортом, энергетикой или связью.

Развитие цифровой экономики, усложнение технологических цепочек, а также важность обеспечения безопасности информации, имеющей существенное значение для государства, жизни и здоровья населения, обусловили законодательное введение понятия критической информационной инфраструктуры (КИИ), а также формирование для нее самостоятельного правового режима в Российской Федерации. Цель данного правового режима – обеспечить устойчивость и бесперебойность критичных процессов (управленческих, технологических, производственных, финансово-экономических), минимизировать последствия компьютерных инцидентов и установить обязанности субъектов КИИ по их предотвращению/реагированию. Эти цели детализируются через: категорирование объектов; создание и функционирование систем безопасности; требования к обеспечению защиты; государственный контроль.

Нормативной базой выступает Федеральный закон от 26.07.2017 № 187-ФЗ[9], дополненный подзаконным массивом (Постановление Правительства РФ № 127, приказы ФСТЭК № 235, № 239, № 227 и другие).

В законе закреплены основные понятия:

– объекты КИИ – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, принадлежащие субъектам КИИ;

– субъекты КИИ – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании при-

[9] О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26.07.2017 № 187-ФЗ // Собрание законодательства Российской Федерации от 31 июля 2017 г. N 31 (часть I) ст. 4736.

надлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, государственной регистрации прав на недвижимое имущество и сделок с ним, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей;

– значимый объект КИИ – тот, которому присвоена категория значимости и который внесен в реестр объектов КИИ;

– безопасность КИИ – состояние защищенности значимых объектов от компьютерных атак, способных вызвать нарушение их функционирования.

Субъект КИИ обязан самостоятельно составить перечень объектов КИИ, осуществить их категорирование и передать эти сведения во ФСТЭК России для внесения в реестр объектов КИИ. Далее, руководствуясь требованиями приказов ФСТЭК России № 235 и № 239, субъект КИИ обязан провести анализ уязвимостей значимых объектов КИИ, спроектировать и внедрить у себя систему обеспечения информационной безопасности для всех объектов КИИ, систему безопасности значимых объектов КИИ и обеспечить их функционирование.

Современные исследователи в области права информационной безопасности в целом сходятся во мнении, что законодательство о защите КИИ в России за последние годы стало более системным и конкретным благодаря уточняющим подзаконным актам (ФСТЭК и ФСБ), появлению национальных стандартов (ГОСТ Р 59711-2022 и др.), созданию и регламентации государственных структур обеспечения безопасности КИИ, таких как ГосСОПКА и НКЦКИ.

Однако, несмотря на значительный прогресс в развитии законодательства о защите КИИ, в данной сфере сохраняется ряд проблем. Так, например, неоднозначность определения категорий КИИ в действующем законодательстве отмечают в своих работах Шабуров А.С., Двойнишников Н.Э., Шлыков А.И. [1], К.В. Наташова, С.С. Соколов, О.Н. Губернаторов, А.П. Ныркова, А.В. Кириков [2], Константин Саматов [3] и другие.

Как справедливо отмечают Репьева В.Д. и Ханмагомедов А.Х., существует значительный риск целенаправленного занижения категории значимости объекта КИИ из-за того, что, в соответствии с действующей нормативной базой, присвоение объекту категории значимости, оценку возможного ущерба и выбора мер защиты проводит сам субъект КИИ, то есть чаще всего владелец объекта. С точки зрения «бизнеса» владелец стремится сократить расходы на внедрение мер защиты КИИ и, как следствие, ему становится невыгодно на этапе присвоения категории значимости объекта КИИ учитывать любой ущерб, кроме собственного [4, с. 195].

Современные научные работы о правовом регулировании КИИ затрагивают не только вопросы определения значимости объектов, но и проблемы уголовно-правовой охраны КИИ.

Федеральный закон № 187-ФЗ предусматривает государственный контроль в сфере безопасности КИИ, включая проверочные мероприятия и ответственность за нарушение установленных требований. Уголовно-правовые средства выполняют «страхующую» функцию, защищая не только собственность и информацию, но и общественную безопасность, устойчивость экономики и государственного управления.

В части административно-правового регулирования КИИ действуют составы КоАП РФ, устанавливающие ответственность за нарушение требований в области безопасности КИИ (например, ст. 13.12.1 КоАП РФ – за несоблюдение порядка информирования и реагирования на инциденты), а также за непредставление сведений уполномоченным органам (ст. 19.7.15 КоАП РФ).

В сфере уголовно-правовой защиты КИИ основной является ст. 274.1 УК РФ «Неправомерное воздействие на КИИ РФ», охватывающая:

– создание, распространение и использование программ или иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на КИИ;

– неправомерный доступ к охраняемой информации КИИ, повлекший вред;

– нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации в КИИ;

– иные квалифицирующие признаки: тяжкие последствия и деяния, совершенные в составе группы лиц.

Параллельно действует ст. 274.2 УК РФ о нарушении правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования сети «Интернет» и сети связи общего пользования. Эти нормы соотносятся с общими составами главы 28 УК РФ (ст. 272–274) по общим правилам конкуренции уголовно-правовых норм, однако некоторые исследователи, как например, И.И. Малыгин [5, с. 167], А.Б. Абазов и Т.А. Файрушин [6, с. 90] обращают внимание на неоднозначность толкования содержащихся в ст. 274.1 УК РФ конструктивных и квалифицирующих признаков, унаследованную от предшествовавших ей ст. 272–274 УК РФ. Кроме того, Н.В. Ермолаев [7, с. 71] и Е.А. Соловьева [8, с. 553] отмечают сложность применения частей 2 и 3 ст. 274.1 УК РФ в отношении КИИ, связанную с неопределенностью понятия «вред» как криминообразующего признака и трудностями его доказывания.

Вопрос отнесения системы мониторинга движения лекарственных препаратов (МДЛП) к объектам критической информационной инфраструктуры Российской Федерации представляется принципиально важным в контексте обес-

печения как национальной безопасности, так и устойчивости системы лекарственного снабжения населения.

В соответствии со статьей 7 Федерального закона №187-ФЗ от 26.07.2017, значимые объекты КИИ подлежат категорированию с учетом показателей их социальной, политической, экономической и иной значимости. Конкретные критерии определены в Постановлении Правительства РФ от 08.02.2018 № 127, утвердившем Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации.

Информация о включении ФГИС МДЛП в реестр объектов КИИ и о присвоенной ей категории значимости не является открытой. Тем не менее, если соотнести изложенные в настоящей работе доводы о характере и важности данных, аккумулируемых в системе МДЛП, для функционирования системы лекарственного обеспечения населения, с критериями значимости, установленными Постановлением Правительства РФ № 127, можно обоснованно предположить, что система МДЛП соответствует сразу нескольким показателям:

– социальная значимость (п. 1 – возможное причинение ущерба жизни и здоровью людей, п. 2 – прекращение или нарушение обеспечения жизнедеятельности населения, п. 5 – недоступность государственной услуги);

– экономическая значимость (п. 9 – ущерб федеральному бюджету);

– значимость для обеспечения обороны страны, безопасности государства и правопорядка (п. 14 – прекращение функционирования информационной системы в данной сфере).

Исходя из совокупности указанных факторов, а также федерального масштаба функционирования системы МДЛП, можно также предположить, что она должна соответствовать первой категории значимости объектов КИИ. Такой вывод представляется обоснованным не только формально-правовыми нормами, но и содержательным анализом последствий возможного нарушения работы системы, поскольку сбои в ее функционировании способны непосредственно затронуть здоровье миллионов граждан и вызвать дестабилизацию фармацевтического рынка в целом.

Следует подчеркнуть, что для объектов первой категории Приказом ФСТЭК от 25.12.2017 N 239 (ред. от 28.08.2024) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» установлены наиболее строгие технические и организационные меры защиты, такие как:

– использование сертифицированных средств защиты информации и вычислительной техники с повышенными классами защиты (п. 29);

– применение маршрутизаторов на границе с интернетом, сертифицированных на соответствие требованиям по безопасности информации (п. 29.1);

– безопасная разработка и тестирование прикладного ПО, включая обязательный динамический анализ кода и фаззинг-тестирование (п. 29.3);

– территориальная локализация всех средств обработки и хранения данных в пределах РФ (п. 31);

– специальные меры противодействия атакам отказа в обслуживании (DoS/DDoS), включая резерв каналов и обязательное взаимодействие с ГосСОПКА (пп. 22 (2), 26 (2), 26 (3)) и др.

Выводы. Таким образом, систему мониторинга движения лекарственных препаратов в силу юридического статуса и фактической роли в жизнеобеспечении страны следует рассматривать как объект критической информационной инфраструктуры первой категории, на который распространяется весь комплекс установленных законом требований. Данное обстоятельство определяет не только особый режим ее функционирования, но и подчеркивает стратегическое значение системы в обеспечении национальной и экономической безопасности Российской Федерации.

Список источников

1. Шабуров А.С. Особенности реализации требований по категорированию объектов критической информационной инфраструктуры / А.С. Шабуров, Н.Э. Двойнишников, А.И. Шлыков // Вестник УрФО. Безопасность в информационной сфере. – 2018. – № 4 (30). – С. 75–82.

2. Наташова К.В. К вопросу о категорировании объектов критической информационной инфраструктуры морских портов / К.В. Наташова, С.С. Соколов, О.Н. Губернаторов, А.П. Ныркov, А.В. Кириков // Безопасность информационных технологий. – 2020. – Т. 27, № 2. – С. 35–46.

3. Саматов К. Проблемные вопросы процедуры категорирования объектов КИИ / К. Саматов // Информационная безопасность. – 2019 [Электронный ресурс]. – URL: https://www.itsec.ru/articles/problemnyye-voprosy-protsedura-kategorirovaniya-kiya-obyekty (дата обращения: 20.10.2025).

4. Репьева В.Д. Особенности и проблемы категорирования объектов критической информационной инфраструктуры / В.Д. Репьева, А.Х. Ханмагомедов // Вестник науки. – 2023. – Т. 5, № 1 (58). – С. 193–196.

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

6. Абазов А.Б. К вопросу об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) / А.Б. Абазов, Т.А. Файрушин // Вестник Уфимского юридического института МВД России. – 2023. – № 4 (102). – С. 86–92.

7. Ермолаев Н.В. К вопросу о содержании признака «вред критической информационной инфраструктуре Российской Федерации» для целей частей 2 и 3 статьи 2741 Уголовного кодекса Российской Федерации / Н.В. Ермолаев // Вестник Казанского юридического института МВД России. – 2024. – Т. 15, № 1 (55). – С. 68–75.

8. Соловьева Е.А. Вред как криминообразующий признак в составах преступлений, предусмотренных частями 2 и 3 статьи 274.1 УК РФ / Е.А. Соловьева // Пермский юридический альманах. – 2023. – № 6. – С. 553–569.

References

1. Shaburov A. S., Dvoinishnikov N. E., Shlykov A. I. Features of the Implementation of Requirements for the Categorization of Critical Information Infrastructure Objects*. Journal of the Ural Federal District. Information security,* 2018, no. 4(30), pp. 75–82. (In Russian).

2. Natashova K. V., Sokolov S. S., Gubernatorov O. N. et al. On the Issue of Categorization of Objects of Critical Information Infrastructure of Seaports. *IT Security*, 2020, vol. 27, no. 2, pp. 35–46. (In Russian).

3. Samatov K. Problem Issues of the CII Object Categorization Procedure. *Information Security, 2019.* Available at: https://www.itsec.ru/articles/problemnyye-voprosy-protsedura-kategorirovaniya-kiya-obyekty. (In Russian).

4. Repyeva V. D., Khanmagomedov A. Kh. Features & Problems of Category of Objects of Critical Information Infrastructure. *Bulletin of Science*, 2023, vol. 5, no. 1(58), pp. 193 – 196. (In Russian).

5. Malygin I. I. Actual Problems of Qualification of Unlawful Impact on the Critical Information Infrastructure of the Russian Federation. *Proceedings of the Southwest State University. Series: History and Law*, 2023, vol. 13, no. 2, pp. 165–176. (In Russian).

6. Abazov A. B., Fairushin T. A. On the Issue of Criminal Liability for Unlawful Influence on the Critical Information Infrastructure of the Russian Federation (Article 274.1 of the Criminal Code of the Russian Federation). *Bulletin of the Ufa Law Institute of MIA of Russia,* 2023, no. 4 (102), pp. 86– 92. (In Russian).

7. Ermolaev N. V. The Content of the Sign “Harm to the Critical Information Infrastructure of the Russian Federation” for the Purposes of Article 274.1 of the Criminal Code of the Russian Federation. *Bulletin of the Kazan Law Institute of MIA Russia*, 2024, vol. 15, no. 1(55), pp. 68–75. (In Russian).

8. Solovyova E. A 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, no. 6, pp. 553–569. (In Russian).

Информация об авторе

Иванов Александр Сергеевич – *руководитель отдела разработки аналитических проектов, аспирант кафедры судебных экспертиз и криминалистики*

Information about the Author

Ivanov Alexander Sergeevich *– Head of the Analytical Projects Development Department, Postgraduate Student of the Chair of Forensic Expertise and Criminalistics*

Статья поступила в редакцию 13.11.2025; одобрена после рецензирования 27.11.2025; принята к публикации 04.12.2025.
The article was submitted 13.11.2025; approved after reviewing 27.11.2025; accepted for publication 04.12.2025.