ПРАВОВЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 343.575

ПРАВОВЫЕ МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ УПРАВЛЕНИЯ

Иринин Кирилл Владимирович

Высшая технологическая школа Севастопольский приборостроительный институт, Севастопольский государственный университет, Севастополь
kirill.law116@yandex.ru

LEGAL MECHANISMS FOR ENSURING CYBERSECURITY OF GOVERNMENT INFORMATION SYSTEMS IN THE CONTEXT OF DIGITALIZATION OF PUBLIC ADMINISTRATION

Irinin Kirill V.

Higher Technological School Sevastopol Instrument-Making Institute, Sevastopol State University, Sevastopol
kirill.law116@yandex.ru

Аннотация. В статье исследуются правовые аспекты обеспечения кибербезопасности критической информационной инфраструктуры (КИИ) в условиях цифровизации государственных услуг. Проведен анализ действующего законодательства Российской Федерации, включая федеральные законы № 149-ФЗ, № 152-ФЗ и № 187-ФЗ, а также новые положения статьи 13.12.1 КоАП РФ, регламентирующей административную ответственность за нарушение требований к защите КИИ. Особое внимание уделено оценке эффективности реализации данных норм на практике, а также проблемам, связанным с недостаточной определенностью статуса операторов и разграничением их ответственности. Рассматриваются примеры киберприцидентов в государственных цифровых системах — Госуслуги, ГИС «ЖКХ», ГАС «Правосудие», которые демонстрируют

Abstract. The article examines the legal aspects of ensuring cybersecurity of the critical information infrastructure (CII) in the context of the digitalization of public services. It analyzes the current legislation of the Russian Federation, including Federal Laws No. 149-FZ, No. 152-FZ, and No. 187-FZ, as well as the new provisions of Article 13.12.1 of the Code of Administrative Offenses of the Russian Federation, which establishes administrative liability for violations of CII protection requirements. Particular attention is paid to assessing the effectiveness of the implementation of these norms in practice and to the problems associated with the insufficient clarity of the status of operators and the delineation of their responsibilities. The article examines examples of cyber incidents in government digital systems such as Gosuslugi, GIS Housing and Utilities, and GAS Justice, which demonstrate the vulnerability of state

уязвимость государственной информационной инфраструктуры перед внешними и внутренними угрозами. Также в статье представлены мнения современных отечественных исследователей, анализирующих состояние правового регулирования в сфере кибербезопасности и защиты персональных данных. Обоснована необходимость совершенствования законодательства с учетом технологических изменений, внедрения международных стандартов (ISO 27001, ISO 27701) и усиления ответственности должностных лиц за несоблюдение требований безопасности. В заключение предлагаются рекомендации по совершенствованию организационно-правовых механизмов защиты цифровых сервисов, повышению прозрачности их функционирования и формированию правовой культуры участников информационных отношений. Работа носит прикладной характер и может быть использована при разработке национальных стратегий цифровой безопасности и модернизации нормативно-правовой базы в сфере защиты КИИ.

Ключевые слова: кибербезопасность, критическая информационная инфраструктура, цифровизация, государственные услуги, правовое регулирование, информационная безопасность, ответственность операторов

information infrastructure to both external and internal threats. It also presents the views of contemporary Russian researchers analyzing the state of legal regulation in the field of cybersecurity and personal data protection. The study substantiates the need to improve legislation considering technological changes, to implement international standards (ISO 27001, ISO 27701), and to strengthen the personal liability of officials for non-compliance with security requirements. The conclusion offers recommendations for improving organizational and legal mechanisms for protecting digital services, increasing the transparency of their functioning, and fostering a legal culture among participants in information relations. The research is of an applied nature and can be used in the development of national digital security strategies and the modernization of the regulatory framework in the field of CII protection.

Keywords: cybersecurity, critical information infrastructure, digitalization, public services, legal regulation, information security, operator responsibility

Для цитирования: *Иринин К.В.* Правовые механизмы обеспечения кибербезопасности государственных информационных систем в условиях цифровизации управления // Проблемы правовой и технической защиты информации. 2025. № 13. С. 50–56.

For citation: *Irinin K.V.* Legal mechanisms for ensuring cybersecurity of government information systems in the context of digitalization of public administration. *Legal and Technical Problems of Information Security*. 2025. № 13. P. 50–56.

Развитие электронного правительства и цифровизация государственных услуг (портал Госуслуги, ГИС «ЖКХ», ГАС «Правосудие») значительно увеличили зависимость государственных органов от информационных технологий. Эти системы аккумулируют миллионы учетных записей граждан и обрабатывают огромные объемы данных, что делает их привлекательными объектами для кибератак. Как отмечают С.А. Фейламазова и З.М. Шихметова, «33% кибератак в апреле 2022 г. были направлены именно на государственные органы, что подтверждает их особую уязвимость и высокую привлекательность для злоумышленников» [8, с. 164].

На наш взгляд, цифровизация государственных услуг в России развивается более динамично, чем система их правовой защиты. Увеличение числа онлайн-сервисов происходит быстрее, чем совершенствование правового механизма их безопасности. Это приводит к тому, что фактическая защищенность цифровых платформ отстает от нормативных требований, а многие операторы ориентируются не на превентивные меры, а на устранение последствий киберинцидентов.

Целью исследования является анализ правовых механизмов обеспечения кибербезопасности государственных информационных систем РФ, выявление проблемных аспектов и предложение путей их совершенствования с учетом современных вызовов цифровизации.

Исследование базируется на анализе нормативных правовых актов Российской Федерации (Федеральные законы № 149-ФЗ, № 152-ФЗ, № 187-ФЗ, статья 13.12.1 КоАП РФ), а также научных публикаций, посвященных вопросам правового обеспечения информационной безопасности. В работе применяются методы сравнительно-правового анализа, формально-юридический метод, системный подход и правовое моделирование.

Основу нормативно-правового регулирования составляют Федеральные законы:

– № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.12.2017 г.[1];

– № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г.[2];

– № 152-ФЗ «О персональных данных» от 27.07.2006 г.[3]

Эти акты формируют правовой режим защиты информации в государственных системах. Однако, как отмечает А.В. Яковлева, «наряду со стремительным развитием цифровой экономики, информационно-коммуникационных технологий все же подталкивают правительство России внести в повестку дня вопрос о разработке закона «О кибербезопасности», который бы позволил системно регулировать отдельные отношения в сфере киберпространства, как на уровне федерального законодательства, так и на международном уровне»[10, с.79]. В то же время, как отмечает А.В. Зык, «создание гибкого правового регулирования должно учитывать специфику цифровой отрасли и не тормозить развитие технологий, одновременно обеспечивая защиту частной жизни и безопасности граждан» [4, с. 40–41].

До недавнего времени административная ответственность за нарушение требований безопасности КИИ отсутствовала. С введением статьи 13.12.1 КоАП РФ законодатель восполнил этот пробел, установив административные санкции за несоблюдение установленных мер защиты. Как справедливо отмечает В.В. Мочалов, «формирование законодательства в области обеспечения безопасности КИИ следует осуществлять в совокупности с административно-правовыми мерами» [6, с. 79]. Несомненно, оператор информационной системы КИИ должен быть осведомлен о том, что за свои действия или бездействия он будет нести ответственность, в зависимости от тяжести деяния уголовную или административную, поэтому во время проведения обучения операторов необходимо в курс подготовки включать не только общую осведомленность о защите критической информационной инфраструктуры, но и ответственность оператора,

[1] Федеральный закон № 187-ФЗ от 26 декабря 2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. 2018. № 1. Ст. 44.

[2] Федеральный закон № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (ч. 1). Ст. 3448.

[3] Федеральный закон № 152-ФЗ от 27 июля 2006 г. «О персональных данных» // Собрание законодательства РФ. 2006. № 31 (ч. 1). Ст. 3451.

а также обзор практики инцидентов на объектах КИИ.

Несмотря на относительную новизну правовых норм, введение данной статьи стало важным шагом, однако правоприменительная практика пока не демонстрирует устойчивых результатов. Требуется разработка детализированных подзаконных актов, конкретизирующих порядок привлечения к ответственности и разграничивающих обязанности между должностными лицами и подрядчиками.

Наличие нормативной базы не исключило проблем в правовом регулировании кибербезопасности КИИ. В настоящее время можно указать прежде всего на неопределенность ответственности операторов. Существующее законодательство не устанавливает четкую персональную ответственность должностных лиц за нарушение требований безопасности КИИ. М.А. Ефремова отмечает, что «даже статья 274.1 УК РФ имеет серьезные недостатки законодательной техники, что снижает эффективность ее применения»[3, с.86]. Это проявилось на практике: в 2021 г. в системе ГАС «Правосудие» произошла утечка служебных данных из-за ошибок подрядчика, однако механизмов привлечения к ответственности не было. Полагаем, что формальное наличие ответственности не гарантирует ее реализации без четкого распределения ролей и обязанностей участников процесса.

Также, по мнению Р.В. Наталичева и его коллег, «одной из существенных проблем является определенное недопонимание на местах, особенно в реальном секторе экономики, необходимости введения и роли нового механизма обеспечения безопасности в общем комплексе мер информационной безопасности»[7, с. 6]. Данная позиция отражает общий тренд формального исполнения требований без осознания их практического значения, что снижает эффективность правоприменения.

Нужно отметить также недостаточную защиту персональных данных. Именно, несмот-ря на наличие закона № 152-ФЗ, уровень защиты персональных данных остается низким. О.Е. Кошелева указывает, что «защищенность персональных данных пользователя на портале “Госуслуги” зависит не только от уровня защиты системы, но и от действий самого пользователя» [5, с.115]. Вместе с тем Н.В. Филиппова подчеркивает: «Эффективное правовое регулирование защиты информации в государственных информационных системах невозможно без корректного определения мер и средств защиты, обеспечивающих комплексную безопасность на всех этапах жизненного цикла системы» [9, с.75]. Например, в 2022 г. Роскомнадзор сообщил о многочисленных фишинговых сайтах, имитирующих портал «Госуслуги», через которые злоумышленники получали доступ к учетным записям граждан.[4] Это показало слабую реализацию механизмов двухфакторной аутентификации, а также слабой информированности граждан о бдительности при работе с информационным порталом. При этом О.В. Бойченко отмечает: «Портал “Госуслуги” по результатам независимого тестирования получил индекс надежности HTTPS всего 12 из 108 возможных баллов, что указывает на низкий уровень защищенности пользовательских данных»[1, с. 7].

Полагаем, что приоритетом должно стать развитие системы превентивного государственного контроля, а не реагирования на инциденты. Требуется внедрить механизм независимого аудита безопасности порталов, аналогичный банковскому надзору, что повысит прозрачность и доверие граждан к цифровым сервисам.

[4] «Госуслуги» взломают «белые хакеры». Зачем это нужно и на что готовы власти и крупнейшие ИТ-компании ради безопасности // Московские новости. 2022. 5 октября. URL: https://www.mn.ru/smart/gosuslugi-vzlomayut-belye-hakery-zachem-eto-nuzhno-i-na-chto-gotovy-vlasti-i-krupnejshie-it-kompanii-radi-bezopasnosti (дата обращения: 08.10.2025).

Обеспечение кибербезопасности не должно ограничиваться техническими средствами. Необходима система правового мониторинга, контролирующая исполнение операторами требований защиты данных, включая регулярные аудиты и отчетность. В то же время имеет место отставание правового регулирования от технологического развития. Законы, регулирующие защиту информации, часто не успевают за развитием искусственного интеллекта, блокчейна и интернета вещей.

М.А. Ефремова подчеркивает: «…причинение вреда критической информационной инфраструктуре может привести к катастрофическим последствиям — выходу из строя объектов жизнеобеспечения и массовой гибели людей» [3, с. 90–91].

Оценивая ситуацию, можно сказать, что правовая система нередко реагирует на факты постфактум. Закон должен работать на опережение, задавая рамки для безопасного внедрения новых технологий. Для примера — использование ИИ при обработке обращений граждан в системе «Инцидент Менеджмент» не имеет правового статуса: неясно, кто несет ответственность за ошибочные решения, принятые на основе алгоритмов. Нормативная база также должна быть технологически нейтральной, т.е. включать общие принципы безопасности, применимые ко всем видам технологий, а не фиксировать отдельные категории.

Рассматриваемую проблему усложняет также ограниченная интеграция международных стандартов. Именно российская система регулирования мало использует стандарты ISO/IEC 27001 или рекомендации NIST, широко применяемые в США и ЕС. В ЕС действует директива NIS 2, предусматривающая обязательные меры защиты и отчетность операторов, в то время как российские организации часто руководствуются ведомственными приказами, не охватывающими весь спектр рисков.

Как отмечает А.В. Яковлева, «очевидно, что неуправляемость и неурегулированность киберпространства, в том числе и на международном уровне, является серьезной проблемой для всех правительств мира, поэтому на первый план выходит вопрос обеспечения кибербезопасности в киберпространственной среде, который должен регулироваться нормативно-правовыми документами»[10, с.72] Для решения проблемы необходимо гармонизировать российское правовое регулирование с международной практикой, особенно в части мер ответственности и стандартов защиты.

Адаптация международных стандартов могла бы повысить уровень совместимости российских государственных систем с зарубежными, а также улучшить внутренние процедуры риск-менеджмента. Мировая практика показывает, что развитые страны рассматривают защиту государственных цифровых платформ как элемент национальной безопасности. Так, в США рамка NIST Cybersecurity Framework используется при защите государственных сетей и налоговых сервисов. Ее гибкость позволяет адаптировать меры под разные ведомства. В Европейском союзе директива NIS2 вводит обязательные меры защиты для публичных и критических цифровых систем. Такой подход усиливает контроль, но увеличивает бюрократию. В Китае действует централизованная модель, где государство контролирует не только безопасность, но и технические стандарты всех госуслуг. Это обеспечивает высокую устойчивость, но снижает автономию организаций.

Р.И. Дремлюга отмечает: «К критической информационной инфраструктуре относятся компьютерные системы, принадлежащие органам государственной власти или обслуживающие их». При этом он подчеркивает: «Отсутствие унификации в вопросе определения критериев и признаков КИИ снижает эффективность борьбы с киберпреступностью на международном уровне»[2, с. 31].

На наш взгляд, Россия могла бы объединить преимущества зарубежных подходов — американской гибкости, европейской системности и китайской централизации. Оптимальным решением было бы создание адаптивной правовой модели, позволяющей одновременно обеспечивать надежность и не препятствовать цифровым инновациям.

Современная правовая система России формирует основу защиты КИИ, однако для государственных цифровых сервисов необходимы дополнительные меры. Можно предложить следующие рекомендации:

– уточнить ответственность операторов и подрядчиков путем введения дифференцированных санкций;

– четкое разграничить обязанности между операторами, подрядчиками и должностными лицами, что позволит повысить контроль над безопасностью и предотвратит формальный подход к защите КИИ;

– ввести дифференцированную ответственность, что мотивирует участников соблюдать стандарты безопасности и обеспечит прозрачность при расследовании инцидентов;

– усилить правовые механизмы защиты персональных данных и ввести обязательные аудиты безопасности.

– ввести обязательное шифрование и сертифицирование средств защиты, причем это должно стать нормой для всех государственных сервисов.

– укрепить доверие граждан к цифровому государству за счет системного подхода к контролю обработки данных;

– гармонизировать российское законодательство путем учета международных стандартов. Рекомендуется адаптировать российские госуслуги к стандартам ISO 27001 (информационная безопасность) и ISO 27701 (защита персональных данных). Это позволит выстроить совместимые процессы при обмене информацией с зарубежными структурами, включая взаимодействие с международными платежными и миграционными системами;

– развивать систему обучения и повышения квалификации специалистов по кибербезопасности. Следует создать специализированные учебные программы для операторов государственных цифровых платформ и сотрудников ведомств. Практика показывает, что большинство инцидентов связано не с техническими сбоями, а с человеческим фактором — ошибками при работе с конфиденциальными данными.

Цифровизация государственных услуг делает взаимодействие граждан и государства более удобным, но одновременно повышает уровень уязвимости КИИ. Анализ показывает, что существующие меры правовой защиты носят базовый характер и требуют адаптации к современным технологиям.

Подводя итог, считаем, что эффективная защита государственных информационных систем возможна только при сочетании трех факторов: развитой нормативной базы, профессиональной компетенции специалистов и международного взаимодействия. Именно это обеспечит баланс между цифровизацией и безопасностью, который сегодня определяет устойчивость государства в киберпространстве.

Библиографический список

1. Бойченко О. В. Тренд на цифровизацию: уязвимости портала «Госуслуги» // Проблемы информационной безопасности социально-экономических систем: VIII Всероссийская с международным участием научно-практическая конференция. Симферополь — Гурзуф, 17–19 февраля 2022 г. Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2022. С. 7–9. EDN KNCDUZ (дата обращения: 15.10.2025).

2. Дремлюга Р.И. Критическая информационная инфраструктура как предмет пося-

гательства в законодательстве зарубежных стран // Журнал зарубежного законодательства и сравнительного правоведения. 2022. Т. 18. № 3. С. 27—36. DOI: 10.12737/jflcl.2022.033 (дата обращения: 15.10.2025).

3. 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. EDN FIXTKU (дата обращения: 15.10.2025).

4. Зык А.В. Правовое регулирование кибербезопасности в системе обеспечения органов внутренних дел // Научный дайджест Восточно-Сибирского института МВД России. 2022. № 1(15). С. 39–46. EDN KKTJGK (дата обращения: 15.10.2025).

5. Кошелева О.Э. Защита информации на портале Госуслуг // Теория и практика управления государственными функциями и услугами. Тарифное регулирование: сборник научных трудов по итогам IV национальной научно-практической конференции, Санкт-Петербург, 10–17 ноября 2021 года. СПб. : Санкт-Петербургский государственный экономический университет, 2021. С. 113–118. EDN YNVEEN (дата обращения: 15.10.2025).

6. Мочалов В.В. Юридическая ответственность за правонарушения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации // Вестник Уральского института экономики, управления и права. 2021. № 1(54). С. 77–79. EDN TGXUEG (дата обращения: 15.10.2025).

7. Наталичев Р.В., Горбатов В.С., Гавдан Г.П., Дураковский А.П. Эволюция и парадоксы нормативной базы обеспечения безопасности объектов критической информационной инфраструктуры // Безопасность информационных технологий. 2021. № 3. DOI: 10.26583/bit.2021.3.01 (дата обращения: 15.10.2025).

8. Фейламазова С.А. Обзор угроз кибербезопасности и государственные меры укрепления IT сферы // Современные цифровые технологии: материалы I Всероссийской научно-практической конференции, Барнаул, 1 июня 2022 г. Барнаул: Алтайский государственный технический университет им. И.И. Ползунова, 2022. С. 162–165. EDN BCTQXY (дата обращения: 15.10.2025).

9. Филиппова Н.В. Правовое регулирование защиты информации в государственных информационных системах // Охрана, безопасность, связь. 2021. № 6-2. С. 73–78. EDN KVOYBQ (дата обращения: 15.10.2025).

10. Яковлева А.В. Кибербезопасность и ее правовое регулирование (зарубежный и российский опыт) // Социально-политические науки. 2021. № 4. СПб., 2021. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-i-ee-pravovoe-regulirovanie-zarubezhnyy-i-rossiyskiy-opyt (дата обращения: 15.10.2025).