УДК 34

Демчук А.Р.

магистрант

Институт безопасности жизнедеятельности

Санкт-Петербургский университет ГПС МЧС России

им. героя РФ генерала армии Е.Н. Зиничева

(г. Санкт-Петербург, Россия)

ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация: *в статье рассматриваются правовые основы обеспечения информационной безопасности Российской Федерации в условиях цифровизации. Анализируются конституционные гарантии, положения федерального законодательства об информации, персональных данных и безопасности критической информационной инфраструктуры, а также стратегические документы. Выделяются основные проблемы правоприменения, связанные с ростом объёма цифровых данных, усложнением киберугроз, распределением ответственности между участниками информационных отношений и необходимостью соблюдения баланса между публичными интересами и правами граждан. Сформулированы предложения по совершенствованию правовых и организационных механизмов защиты информации.*

Ключевые слова: *информационная безопасность, цифровизация, защита информации, персональные данные, кибербезопасность, критическая информационная инфраструктура, правовое регулирование.*

Введение.

Цифровизация государственного управления, экономики и социальной сферы сопровождается расширением использования информационных систем, электронных сервисов, облачных платформ и сетевых коммуникаций. Значительная часть юридически значимых действий совершается в электронной

форме: граждане получают государственные услуги дистанционно, организации обмениваются документами через информационные системы, а органы публичной власти используют цифровые ресурсы для принятия управленческих решений. В результате информация становится не только объектом гражданского оборота, но и важнейшим ресурсом обеспечения устойчивости государства, функционирования организаций и реализации прав человека.

1. Понятие и конституционные основы информационной безопасности.

В российском законодательстве информационная безопасность регулируется совокупностью норм конституционного, административного, гражданского, уголовного и информационного права. При этом единое универсальное определение информационной безопасности применяется прежде всего в стратегических документах. Доктрина информационной безопасности Российской Федерации рассматривает информационную сферу как совокупность информации, объектов информатизации, информационных систем, сайтов и сетей связи, а также субъектов, осуществляющих деятельность в этой сфере [1]. Такой подход позволяет учитывать как содержание информации, так и инфраструктуру ее создания, хранения, обработки и передачи.

Конституционные основы правового регулирования формируются несколькими взаимосвязанными положениями. Статья 23 Конституции Российской Федерации закрепляет право на неприкосновенность частной жизни, личную и семейную тайну, защиту чести и доброго имени, а также тайну переписки и иных сообщений. Статья 24 запрещает сбор, хранение, использование и распространение информации о частной жизни лица без его согласия, кроме предусмотренных законом случаев. Статья 29 гарантирует свободу мысли и слова, право свободно искать, получать, передавать, производить и распространять информацию законным способом. Следовательно, государственная политика в сфере информационной безопасности должна одновременно обеспечивать защищенность информации и не допускать необоснованного ограничения конституционных прав.

2. Система нормативного правового регулирования.

Базовое значение в рассматриваемой сфере имеет Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Он определяет общие принципы правового регулирования отношений, связанных с поиском, получением, передачей, производством и распространением информации, применением информационных технологий и обеспечением защиты информации [2]. Закон закрепляет правовые категории информации, информационной системы, обладателя информации и оператора информационной системы, а также устанавливает общие требования к защите информации.

Важным элементом системы является Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Он регулирует отношения, связанные с обработкой персональных данных государственными органами, муниципальными органами, юридическими и физическими лицами [3]. Закон устанавливает принципы и условия обработки данных, права субъектов персональных данных, обязанности операторов, требования к обеспечению безопасности и правила трансграничной передачи. Для цифровой экономики значение данного акта постоянно возрастает, поскольку персональные данные используются при предоставлении услуг, дистанционном заключении договоров, кадровом администрировании и работе государственных информационных систем.

Отдельное направление регулируется Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [4]. Его действие направлено на обеспечение устойчивого функционирования значимых объектов критической информационной инфраструктуры при проведении компьютерных атак. Закон определяет категории субъектов КИИ, порядок категорирования объектов, полномочия государственных органов, обязанности субъектов и основы взаимодействия при обнаружении, предупреждении и ликвидации последствий компьютерных атак. Критически важными являются информационные системы

и сети в установленных законом сферах, включая здравоохранение, транспорт, связь, энергетику, банковскую сферу и иные отрасли.

Стратегический уровень регулирования представлен Доктриной информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 5 декабря 2016 г. № 646 [1]. Доктрина определяет национальные интересы, основные информационные угрозы, стратегические цели и направления обеспечения информационной безопасности. Дополнительные организационные меры предусмотрены Указом Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [5]. Указ ориентирован, в частности, на повышение устойчивости информационных ресурсов и организацию деятельности по обеспечению безопасности в государственных органах и отдельных организациях.

3. Основные проблемы правоприменения в условиях цифровизации.

Несмотря на значительное количество нормативных правовых актов, правоприменение сталкивается с рядом проблем. Первая из них связана с быстрым изменением технологий. Законодательные нормы рассчитаны на длительное применение, тогда как способы обработки данных, архитектура информационных систем и методы совершения компьютерных атак меняются значительно быстрее. В результате отдельные требования могут нуждаться в регулярном уточнении, а участникам правоотношений становится сложнее определять применимые правила при использовании новых технологических решений.

Третья проблема связана с недостаточным уровнем информационной культуры и правовой грамотности пользователей. Значительная доля инцидентов обусловлена не только техническими уязвимостями, но и ошибками работников: использованием простых паролей, переходом по вредоносным ссылкам, передачей учетных данных третьим лицам, несоблюдением правил работы с документами. Наличие формального локального акта само по себе не

гарантирует защищенность системы, если сотрудники не знают установленных требований и не понимают последствий их нарушения.

4. Направления совершенствования правового регулирования.

Совершенствование правовых основ информационной безопасности целесообразно осуществлять по нескольким направлениям. Прежде всего необходимо обеспечить согласованность нормативных требований, относящихся к защите информации, персональных данных и критической информационной инфраструктуры. Участники правоотношений должны иметь возможность определить применимые обязанности без противоречий между отраслевыми актами. Для этого важны систематизация подзаконного регулирования, своевременное обновление методических документов и понятные разъяснения уполномоченных органов.

Третье направление предполагает повышение ответственности организаций за фактическое исполнение требований, а не только за наличие формальной документации. Внутренние положения об информационной безопасности должны определять роли и полномочия работников, порядок предоставления и прекращения доступа, правила использования съемных носителей, процедуру сообщения об инцидентах, порядок резервного копирования и восстановления данных. Необходимы регулярные проверки соблюдения этих правил и обучение персонала с учетом его должностных обязанностей.

Пятое направление связано с укреплением гарантий прав граждан. Развитие цифровых сервисов должно сопровождаться прозрачностью обработки персональных данных, понятными механизмами получения информации о целях и основаниях обработки, возможностью реализации прав субъекта данных и эффективными способами обжалования действий операторов. Важную роль играет своевременное информирование о нарушениях безопасности в случаях и порядке, предусмотренных законом. Доверие к цифровой среде невозможно обеспечить исключительно техническими средствами: оно зависит от

предсказуемости правовых правил и реальной возможности защитить нарушенное право.

Заключение.

Проведенный анализ позволяет сделать вывод о том, что правовые основы обеспечения информационной безопасности в Российской Федерации представляют собой многоуровневую систему, включающую конституционные положения, федеральные законы, стратегические документы и подзаконные нормативные акты. Ее центральными элементами выступают Федеральный закон № 149-ФЗ, регулирующий общие отношения в сфере информации и ее защиты, Федеральный закон № 152-ФЗ, устанавливающий правовой режим персональных данных, и Федеральный закон № 187-ФЗ, направленный на обеспечение безопасности критической информационной инфраструктуры.

Представляется, что дальнейшее развитие законодательства должно быть направлено на согласование нормативных требований, применение риск-ориентированного подхода, повышение реальной ответственности организаций, совершенствование межведомственного взаимодействия и укрепление гарантий прав граждан. Комплексное решение этих задач позволит сформировать устойчивую правовую среду, в которой цифровые технологии будут развиваться при соблюдении требований законности, безопасности и защиты прав человека.

СПИСОК ЛИТЕРАТУРЫ:

1. Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 05.12.2016 № 646
2. «Об информации, информационных технологиях и о защите информации»: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. по состоянию на 26.06.2026)
3. «О персональных данных»: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. по состоянию на 26.07.2026)

4. «О безопасности критической информационной инфраструктуры Российской Федерации»: Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 07.04.2025)

5. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации: Указ Президента РФ от 01.05.2022 № 250 (ред. от 13.06.2024)

6. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 (с учетом действующих поправок)

Demchuk A.R.

master's degree student

Institute of Life Safety

St. Petersburg University of State Fire Service of EMERCOM of Russia

named after E.N. Zinichev

(St. Petersburg, Russia)

LEGAL FOUNDATIONS FOR ENSURING INFORMATION SECURITY IN RUSSIA AMID DIGITALIZATION

Abstract: *this article examines the legal foundations for ensuring information security in Russia amid digitalization. It analyzes constitutional guarantees, federal legislation on information, personal data, and the security of critical information infrastructure, as well as strategic documents. Key challenges in applying these laws are identified, including the growing volume of digital data, increasingly complex cyber threats, the allocation of responsibility among participants in information relations, and the need to balance public interests with citizens' rights. Proposals are made to improve legal and organizational mechanisms for protecting information.*

Keywords: *information security, digitalization, information protection, personal data, cybersecurity, critical information infrastructure, legal regulation.*