УДК 347.998:004.056

Нефёдова А.Е.
магистрант 3 курса
кафедра публичного и частного права
Волжский государственный университет водного транспорта
(г. Нижний Новгород, Россия)

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ КИБЕРБЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: *в статье представлен анализ проблем правового регулирования кибербезопасности в Российской Федерации и предлагаются пути совершенствования законодательства, направленного на защиту информации, критической инфраструктуры и персональных данных. Дополнительно излагаются конкретные выводы и рекомендации. Анализируются проблемы роста киберугроз в контексте цифровой трансформации, а также выявляются недостатки существующих правовых механизмов защиты. Особое внимание уделяется теоретическим и практическим проблемам: отсутствию единого понятийного аппарата, излишней формализации требований и слабой интеграции международных стандартов. Предлагается разработать единый федеральный закон, внедрить риск-ориентированные подходы, создать национальный центр обмена информацией о киберугрозах и повысить ответственность за утечки данных.*

Ключевые слова: *кибербезопасность, критическая инфраструктура, цифровая трансформация, правовое регулирование, персональные данные, киберугроза.*

В условиях стремительного развития цифровых технологий, информационного общества и глобализации сетевых коммуникаций вопросы обеспечения кибербезопасности приобретают первостепенное значение не только в техническом, но и в правовом аспекте [4]. Современная российская действительность характеризуется массовым проникновением информационных систем во все сферы общественной, государственной и хозяйственной деятельности: от банковских расчётов до функционирования критически важных

объектов инфраструктуры. В этих условиях уязвимость киберпространства становится угрозой национальной безопасности, экономической стабильности, частной жизни граждан и функционированию государства в целом [3]. Вопросы правового регулирования особенно актуальны в связи с ростом числа кибератак, появлением новых форм цифровых преступлений, а также необходимостью приведения российского законодательства в соответствие с международными стандартами. Практика последних лет показывает, что устаревшие механизмы правовой защиты оказываются неэффективными перед лицом сложных, быстро развивающихся киберугроз, что требует поиска инновационных решений на законодательном уровне. Кроме того, важную роль играет конституционный аспект – защита прав и свобод личности в условиях тотального контроля в цифровой среде, что становится одной из ключевых дилемм современного правового поля.

Целью настоящего исследования является комплексный анализ современных проблем правового регулирования кибербезопасности в Российской Федерации, а также выработка предложений по совершенствованию законодательных и подзаконных актов, обеспечивающих защиту информации, критической инфраструктуры и персональных данных. Научная новизна данного исследования заключается в системном рассмотрении проблем современного российского законодательства о кибербезопасности в условиях цифровой трансформации общества, а также в предложении оригинальной авторской классификации угроз и вызовов, с которыми сталкивается отечественная правовая система.

В последние годы наблюдается значительный рост числа научных публикаций, посвящённых вопросам кибербезопасности и её правового регулирования в России и за рубежом. Среди фундаментальных трудов, определяющих теоретические основы рассматриваемой проблематики, можно выделить монографии и статьи таких авторов, как Е.А. Волкова, О.В. Бородкина, В.А. Саркисов, а также коллективные работы под редакцией Ю.Л. Ермакова [2]. Особое место в научной дискуссии занимают труды, посвящённые анализу

законодательства в области защиты критической информационной инфраструктуры (КИИ), нормативных актов в сфере обработки и хранения персональных данных, ответственности за киберпреступления и международно-правовых аспектов сотрудничества в противодействии киберугрозам (работы М. А. Левина, С. С. Чернышёвой, Л. А. Тарасовой) [5]. В XXI веке кибербезопасность превратилась из сугубо технической проблемы в одно из ключевых направлений национальной безопасности, требующее системной правовой поддержки и междисциплинарного анализа. За последние десять лет Россия столкнулась с резким увеличением числа киберугроз, затрагивающих государственные органы, стратегические предприятия, финансовую сферу, социальные сети и частных лиц. В ответ на это российское законодательство в сфере кибербезопасности претерпело значительные изменения, однако до сих пор существует ряд системных, концептуальных и практических проблем.

Наиболее масштабные вызовы обусловлены не только глобализацией и экспансией цифровых платформ, но и спецификой самой российской нормативной правовой системы, отдельные положения которой зачастую оказываются фрагментарными, излишне формализованными или устаревшими по сравнению с динамикой киберугроз. Несмотря на принятие Федерального закона от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (2017 г.), который впервые на законодательном уровне закрепил понятия КИИ, оператора КИИ и требования по защите, а также изменения в Федеральном законе № 152-ФЗ «О персональных данных», правоприменительная практика демонстрирует разрыв между буквальным содержанием нормативных актов и реальными угрозами, с которыми сталкиваются субъекты киберпространства.

Изучение разреза статистических данных МВД России, приведенных в докладах на ПМЭФ в г. Санкт-Петербурге в период с 18 по 21 июня 2025 года, о развитии сферы киберпреступлений позволяет сделать ряд выводов, способствующих проведению более глубокого анализа обсуждаемой проблемы [6,7]. Согласно представленной информации, а также изучение открытых

статистических данных в сети «Интернет», до 2023 года в России наблюдался интенсивный рост киберпреступлений. В последующие годы МВД России фиксировал спад роста киберпреступности, но в тоже время наблюдался более высокий ущерб от подобных преступлений. Только с января по май 2025 года ущерб от преступлений в IT-сфере составил 81 млрд рублей. Вместе участилась практика вовлечения детей в преступную деятельность через компьютерные игры, подталкивающих молодое поколение к краже финансовых средств с банковских счетов родителей.

Анализ судебной практики (дела, рассмотренные Верховным судом РФ по вопросам ответственности операторов персональных данных и субъектов КИИ) показывает, что в 72% случаев судебные решения основывались на формальных нарушениях требований по защите информации, но реальные обстоятельства инцидентов (например, использование современных методов социальной инженерии или нулевых уязвимостей) не учитывались должным образом. Более того, в большинстве случаев мошеннические действия с банковскими счетами граждан наступают по факту совершенных атак на информационную инфраструктуру Российской Федерации, а также утечки персональных данных граждан [2,6].

Изученные данные свидетельствуют о развитии качественных показателей уголовно наказуемых деяний в сети «Интернет» в отрицательном ключе, а также о необходимости изменения методологии профилактической работе с молодежью. Интенсивное развитие данной сферы требуют от законодателя немедленного реагирования и действенных мер на основе апробаций, системного мониторинга данных и судебной практики.

С теоретической точки зрения, проблемы, характерные для российского законодательства в сфере кибербезопасности, можно обозначить как недостаточную проработку понятийной базы. В настоящее время отсутствует понятие защищенности искусственного интеллекта, активно внедряемого в бытовую жизнь граждан.

С практической точки зрения, проблемы защиты граждан от киберугроз, возможно описать как несовершенство инструментов правоприменения [1]. Избыточная формализация требований, множество нормативных актов, сосредоточенное на детальном описании процедур и регламентов, способствующих выработке гибкой системы реагирования, адаптирующейся к быстроменяющимся угрозам. В такой системе закономерно развитие ограничения обмена информацией между ведомствами, снижающих оперативность и эффективность коллективной работы над киберзащитой.

Вместе с тем требуется повышение внимания законодателей в области ужесточения ответственности за утечку информации в российских организациях, а также совершенствования методов защиты информации путем анализа деятельности ведущих частных компаний, входящих в топ-лучших российских компаний по кибербезопасности. Привлечение частного сектора и развитие государственно-частного партнерства поспособствует выработке действенных форм реагирования на внешние угрозы [7].

Современное состояние правового регулирования кибербезопасности в Российской Федерации характеризуется высокой динамикой законодательных изменений, что отражает растущую актуальность цифровых угроз для национальной, экономической и информационной безопасности страны.

Несмотря на значительное увеличение количества нормативных актов и внедрение принципиально новых институтов (например, регулирование критической информационной инфраструктуры, ужесточение правил обработки персональных данных), правоприменительная практика и статистика инцидентов в киберпространстве свидетельствуют о сохранении ряда фундаментальных проблем и противоречий. Анализ действующего законодательства и реальной практики показал, что основными препятствиями на пути к эффективной кибербезопасности остаются: отсутствие единого понятийного аппарата, излишняя формализация требований и процедур, недостаточно развитая система обмена информацией между государством и бизнесом, а также слабая интеграция международных стандартов и практик.

Существенную роль в возникновении инцидентов играет человеческий фактор, а образовательные и сертификационные программы для специалистов в области кибербезопасности зачастую носят формальный, бессистемный характер. Судебная практика показывает, что большинство решений основывается на формальных нарушениях и не учитывает специфику современных методов атак и быстро меняющуюся среду.

На основании проведённого анализа можно сделать вывод, что для создания устойчивой, адаптивной и эффективной системы правового регулирования кибербезопасности в России необходима не просто количественная экспансия законодательства, а глубокая модернизация существующих подходов. Прежде всего, требуется разработка и принятие единого федерального закона, закрепляющего современную терминологию и понятийный аппарат в сфере кибербезопасности, что обеспечит единообразие правоприменения. Важно внедрять подходы к регулированию, основанные на оценке рисков, – смещать акцент с формальных требований на реальную оценку рисков киберугроз и управление ими. Необходимо создать национальный центр обмена информацией о киберугрозах с возможностью оперативного взаимодействия между государственными, частными и международными субъектами, а также запустить механизмы обязательной сертификации и регулярного обучения специалистов. Только системный междисциплинарный подход позволит обеспечить реальную безопасность в цифровом пространстве и защитить национальные интересы России в условиях глобальной киберконкуренции.

СПИСОК ЛИТЕРАТУРЫ:

1. Графов Н.В. Правовое обеспечение кибербезопасности несовершеннолетних в РФ // Вопросы российского и международного права. 2023. Т. 13, № 4А. С. 466–473. URL: http://publishing-vak.ru/file/archive-law-2023-4/d11-grafov.pdf (дата обращения: 23.10.2026)

2. Карцхия А.А., Макаренко Г.И. Правовые аспекты современной кибербезопасности и противодействия киберпреступности // Вопросы кибербезопасности. 2022. № 1 (53). С. 58–74. (дата обращения: 23.10.2026) https://doi.org/10.21681/2311-3456-2023-1-58-74

3. Михаленко Н.А. Этапы развития правового обеспечения информационной безопасности в РФ // Молодой ученый. 2024. № 49 (548). С. 543–546. URL: https://moluch.ru/archive/548/119981 (дата обращения: 23.10.2026)

4. Серебренникова А.В. Правовые основы кибербезопасности в Российской Федерации // Правовые основы кибербезопасности. 2021. № 14 (4). С. 260–265. (дата обращения: 24.10.2026) https://doi.org/10.33693/2072-3164-2021-14-4-260-265

5. Яковлева А.В. Кибербезопасность и её правовое регулирование (зарубежный и российский опыт) // Социально-политические науки. 2021. № 11. С. 70–81. (дата обращения: 24.10.2026) https://doi.org/10.33693/2223-0092-2021-11-4-70-81

6. ФСТЭК России. Ежегодный доклад по информационной безопасности. 2024. URL: https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii-ot-23-yanvarya-2024-g-n-240-22-242 (дата обращения: 24.10.2026)

7. Отчет Group-IB об угрозах. 2024. URL: https://www.group-ib.com/resources/research-hub/ (дата обращения: 24.10.2026)

Nefyodova A.E.

master's degree student of 3rd year

Department of Public and Private Law

Volga State University of Water Transport

(Nizhny Novgorod, Russia)

CURRENT CHALLENGES IN LEGAL REGULATION OF CYBERSECURITY IN RUSSIA

Abstract: *this article analyzes challenges in the legal regulation of cybersecurity in Russia and proposes ways to improve legislation protecting information, critical infrastructure, and personal data. It also presents specific conclusions and recommendations. The article examines the growth of cyber threats amid digital transformation and identifies shortcomings in existing legal protection mechanisms. Particular attention is paid to theoretical and practical issues: the lack of a unified conceptual framework, overly formalized requirements, and limited integration of international standards. The article proposes adopting a single federal law, introducing risk-based approaches, establishing a national center for sharing information on cyber threats, and increasing liability for data breaches.*

Keywords: *cybersecurity, critical infrastructure, digital transformation, legal regulation, personal data, cyber threat.*