ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ: НОРМАТИВНО-ПРАВОВЫЕ ОСНОВЫ И СОВРЕМЕННЫЕ ВЫЗОВЫ

Дубень А.К.[1]

Ключевые слова: *правовое регулирование, трансформация права, цифровизация, правовая регламентация, кибербезопасность, вызовы и угрозы, риски.*

Аннотация

Цель работы: *определение современных правовых основ и механизмов обеспечения информационной безопасности, выявление вызовов, угроз и рисков, анализ нормативно-правовой базы, определение пробелов и противоречий, а также установление рекомендаций по совершенствованию нормативно-правовой базы в области обеспечения информационной безопасности.*

Методы исследования: *общенаучные методы анализа и синтеза, абстрагирования и моделирования, обобщения, описания, классификации и др., а также специальные частноправовые методы познания: историко-правовой, сравнительно-правовой, формально-юридический и др.*

Результаты исследования: *проанализированы нормы права, регулирующие правоотношения в области правового обеспечения информационной безопасности, выявлены актуальные проблемы, коллизии в российском законодательстве, сформулированы предложения по усовершенствованию отдельных нормативных правовых актов. Выделены актуальные и злободневные вызовы, угрозы и риски в области информационной безопасности. Сделан вывод, что необходимо реализовать комплекс мер, направленных на усиление регулирования в сфере информационной безопасности по ряду направлений: прежде всего, необходимо ввести единый правовой режим для защиты государственных информационных систем, систем, обрабатывающих персональные данные, объектов критической информационной инфраструктуры. Данные меры позволят решить ряд задач, направленных на обеспечение безопасности в современных условиях цифровизации, геополитических вызовов и рисков, всемирного социально-экономического кризиса, формирования многополярности в мире.*

DOI: 10.24412/1994-1404-2026-1-00-31

Введение

Вопросы информационной безопасности в современных условиях, в период трансформации права, изменения многополярного мира, новых вызовов и угроз, приобретают актуальность в доктрине информационного и международного права. Особенно следует подчеркнуть, что в настоящее время очевидна тенденция усиления роли информации при обеспечении национальной безопасности как одного из приоритетных экономических и политических ресурсов.

Согласно Стратегии национальной безопасности Российской Федерации, национальными интересами на современном этапе государства являются развитие безопасного информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия, а также поддержание стратегической стабильности, укрепление мира и безопасности, правовых основ международных отношений. Следовательно, нормативные акты стратегического характера свидетельствуют об актуальности и потребности укрепления информационного суверенитета государства и усилении его роли на международной арене.

Актуальность и значимость данной темы в отечественной науке подтверждается тем, что в условиях глобальной цифровой трансформации во всех сферах, обострившихся геополитических противоречий, усиливших межгосударственное информационное противоборство, проблемы правового обеспечения национальной и международной информационной безопасности приобретают ключевое значение. Президент Российской Федерации отметил: «Повышение

[1] ***Дубень Андрей Кириллович,*** *кандидат юридических наук, старший научный сотрудник Института государства и права Российской академии наук, г. Москва, Российская Федерация.*

E-mail: k.duben@mail.ru

уровня информированности граждан о вопросах безопасности в Интернете и необходимость образования в этой области по сей день являются важным вопросом. В современных условиях, когда киберугрозы становятся все более изощренными, развитие комплексных стратегий информационной безопасности является приоритетной задачей для обеспечения национальной безопасности страны»[2]. В 2026 году правовое обеспечение информационной безопасности остается приоритетной задачей в Российской Федерации. «В строгом соответствии с нормами закона важно и дальше обеспечивать безопасность информационного и цифрового пространства страны, вместе с МВД, Минцифры и другими профильными ведомствами внедрять новые средства противодействия киберпреступлениям с учетом стремительной динамики развития информационных технологий», — отметил Президент Российской Федерации[3]. Кроме того, отмечая важность вышеуказанных проблем, связанных с обеспечением информационной безопасности, необходима постоянная системная работа и координация с органами государственной власти в целях повышения грамотности общества в вопросах безопасного поведения в интернет-пространстве; надлежащей организации защиты пользователей сети Интернет от противоправного контента; подготовка высококвалифицированных кадров в области информационной безопасности; надлежащий контроль за соблюдением законодательства владельцами сайтов, провайдерами хостинга и операторами связи, оказывающими услуги по предоставлению доступа к сети Интернет; проведение системной информационно-просветительской работы, направленной на профилактику интернет-зависимости, информирование пользователей сети Интернет о безопасном поведении при использовании информационно-коммуникационных технологий и т. д.

Обозначенные условия неизбежно влекут меры по усилению внутренних позиций государства в условиях конкурентоспособной информационной борьбы как с уже существующими, так и с новыми центрами силы, а также по дальнейшему совершенствованию правового регулирования отдельных положений развития средств и методов защиты информации на основе использования передовых цифровых технологий.

Принятие поправок к Конституции Российской Федерации расширило функции государства при обеспечении информационной безопасности личности и общества, положение ст. 71 коррелируется со ст. 24 Конституции, в данной норме закреплено положение об информационной безопасности личности, связанной со сбором, хранением, использованием и распространением информации о частной жизни гражданина и его персональных данных, личные данные требуют сегодня особой правовой защиты [1, с. 294; 2]. Важно отметить, что основные направления государственной политики в области обеспечения информационной безопасности в соответствии с указами Президента Российской Федерации имеют большой спектр вопросов, затрагивающих все сферы жизнедеятельности [3]. Указами Президента России утверждены такие концептуальные акты, как: Стратегия развития информационного общества в Российской Федерации на 2017—2030 годы, Доктрина информационной безопасности Российской Федерации, Концепция общественной безопасности в Российской Федерации, Основы государственной политики Российской Федерации в области международной информационной безопасности, Концепция противодействия терроризму в Российской Федерации, о развитии искусственного интеллекта в Российской Федерации, о дополнительных мерах по обеспечению информационной безопасности Российской Федерации и др. [4].

Значительным шагом на пути укрепления информационной безопасности стало издание Указа Президента Российской Федерации «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»[4]. Данным указом на руководителей федеральных и региональных органов исполнительной власти, государственных корпораций (компаний), стратегических предприятий и иных организаций возложена персональная ответственность за обеспечение информационной безопасности. Кроме того, предписано создание в каждом таком органе (организации) специализированного структурного подразделения, осуществляющего функции по обеспечению информационной безопасности, либо возложение данных функций на существующее структурное подразделение. Данным нормативным правовым актом предусмотрено осуществление мониторинга защищенности информационных ресурсов, принадлежащих таким органам (организациям) [5, с. 139].

Постановка задачи

Исследование данного вопроса показало, что в современных условиях цифровизации, геополитических вызовов, угроз и рисков, всемирного социально-экономического кризиса усиливаются угрозы информационной безопасности, что ставит задачу совершенствования национальной системы правового обеспечения информационной безопасности в Российской Федерации [6].

Основные вопросы безопасности в информационной сфере комплексно и системно закреплены в Доктрине информационной безопасности Российской Федерации; в данном нормативном правовом акте выделены общественные отношения, которые позволяют целенаправ-

[2] Путин обсудил с членами Совбеза вопросы информационной безопасности. URL: https://www.5-tv.ru/news/5004753/putin-obsudil-sclenami-sovbeza-voprosy-informacionnoj-bezopasnosti/ (дата обращения: 24.02.2026).

[3] Путин заявил о необходимости внедрять новые методы против киберпреступности. URL: https://www.interfax.ru/russia/1074398 (дата обращения: 24.02.2026).

[4] Указ Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» // Собрание законодательства РФ. 2022. № 18. Ст. 3058.

ленно обеспечивать защищенность государства в информационной сфере и определять векторы дальнейшего совершенствования правовых институтов в целях баланса интересов личности, общества и государства в целом.

Сто́ит особо обратить внимание на состояние правового обеспечения информационной безопасности; согласно п. 8 Доктрины информационной безопасности Российской Федерации можно выделить следующие особенности национальных интересов России:

1) прозрачность и транспарентность деятельности государства в информационной сфере;

2) гарантия защиты конституционных прав и свобод граждан, касающихся информационной безопасности;

3) взаимное и согласованное функционирование государства и гражданского общества, в том числе в рамках укрепления нравственных ценностей общества;

4) обеспечение надлежащего функционирования информационной инфраструктуры в случае непосредственного влияния информационных угроз, в том числе в военное время и в период стабильной мирной обстановки в стране;

5) стимулирование научно-технического прогресса и развития экономических отраслей, способствующих обеспечению информационной безопасности;

6) интеграционное взаимодействие с другими государствами для обеспечения международной информационной безопасности и стратегической стабильности.

Таким образом, закрепленный в документах стратегического планирования перечень национальных интересов является правовым фундаментом (наряду с целями и задачами), на котором стоит вся система национальной безопасности.

В рамках поставленной задачи полагаем возможным рассмотреть вопрос о принятии новой Доктрины информационной безопасности Российской Федерации, которая бы определила новые цели и задачи на основе современных вызовов, угроз и рисков. Вместе с тем стоит согласиться с позицией А.В. Минбалеева: так, под эгидой Совета Безопасности Российской Федерации началась работа по обновлению Доктрины информационной безопасности Российской Федерации. Предыдущая редакция документа была утверждена еще в 2016 году; за прошедший период, безусловно, риски цифровой среды значительно изменились, что обуславливает необходимость модернизации положений данного важнейшего документа [7]. В обновленном нормативном правовом акте необходимо реализовать комплекс мер, направленных на усиление регулирования в сфере информационной безопасности по ряду направлений; прежде всего, необходимо ввести единый правовой режим для защиты государственных информационных систем, систем, обрабатывающих персональные данные, объектов критической информационной инфраструктуры. При этом обновленный документ необходим для совершенствования механизмов контроля выполнения требований по информационной безопасности, создания действенных механизмов оперативного контроля защищенности и принятия мер по устранению выявленных недостатков.

Решение поставленной задачи

Исследование показывает, что сегодня правовое регулирование отношений в сфере национальной безопасности определяется потребностями урегулирования общественных отношений, которые сложились между субъектами по вопросам национальной безопасности и создание условий для достижения оптимального уровня безопасности в политических, правовых, военных, информационных и социально-экономических сферах.

Развитие информационных технологий и их внедрение для достижения национальных целей развития государства, а также реализации политики построения цифровой экономики повлияло на формулирование принципов обеспечения информационной безопасности. Так, в Паспорте национального проекта «Национальная программа „Цифровая экономика Российской Федерации“»[5] содержится комплекс мероприятий, реализация которых согласно данному документу «базируется на основополагающих принципах информационной безопасности»; между тем, на наш взгляд, представленные принципы позволяют обеспечивать экономический и информационный суверенитет России.

На основе положений Доктрины информационной безопасности Российской Федерации можно выделить отдельные аспекты исследуемой темы, которые отражены в ряде подзаконных актов органов государственной власти (к примеру, распоряжения Правительства Российской Федерации: «Об утверждении Концепции технологического развития на период до 2030 года», «Об утверждении стратегического направления в области цифровой трансформации образования, относящейся к сфере деятельности Министерства просвещения Российской Федерации», «Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий» и т. д.)[6]. При этом обеспечение информационной

[5] Паспорт национального проекта «Национальная программа „Цифровая экономика Российской Федерации“» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 4 июня 2019 г. № 7) // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: https://digital.gov.ru (дата обращения: 24.02.2026).

[6] Распоряжение Правительства РФ от 20 мая 2023 г. № 1315-р «Об утверждении Концепции технологического развития на период до 2030 года» // Собрание законодательства РФ, 2023, № 21, ст. 3123; Распоряжение Правительства РФ от 18 октября 2023 г. № 2894-р «Об утверждении стратегического направления в области цифровой трансформации образования, относящейся к сфере деятельности Министерства просвещения Российской Федерации» // Собрание законодательства РФ, 2023, № 44, ст. 7911; Распоряжение Правительства РФ от 30 декабря 2024 г. № 4154-р «Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий» // Собрание законодательства РФ, 2025, № 2, ст. 76.

безопасности осуществляется на всех уровнях органов государственной власти, местного самоуправления и негосударственными организациями [8, с. 164]. Как справедливо отмечает Р.Н. Ключко, научный анализ Доктрины информационной безопасности Российской Федерации позволяет формулировать новые понятия и конструировать их правовые определения, создает фундамент для развития правового аппарата, информационная безопасность как четко обозначаемый феномен современной социальной действительности единодушно признается в правовой доктрине самостоятельным объектом правового регулирования и охраны и в правовом поле [9]. Анализируя положения Доктрины информационной безопасности Российской Федерации, можно отметить, что в современных условиях цифровизации и влияния цифровых технологий активизировались позиции о роли и значении суверенитета государства в киберпространстве, основой которых послужила трансформация информационного общества [10, с. 49]. Г.Г. Камалова справедливо отмечает, что цифровые технологии открывают новые организационные и технологические возможности в различных областях, а с другой стороны, их использование требует решения группы взаимосвязанных правовых вопросов, где ключевым является обеспечение национальной безопасности государства в информационном пространстве [11, с. 179].

Выводы

Отечественная информационно-правовая политика является сегодня регулятором публичных и частных правоотношений, посредством чего реализуются стратегические задачи государства. Обеспечение информационной безопасности как вида национальной безопасности своим регуляторным воздействием пронизывает все многообразие общественных отношений, возникающих в процессе жизнедеятельности человека и государства. На основе проведенного анализа нормативных актов, регулирующих правовое обеспечение информационной безопасности государства, целесообразно внести изменения и принять новую редакцию Доктрины информационной безопасности Российской Федерации, которая будет направлена на решение ряда задач, в том числе на обеспечение безопасности в современных условиях цифровизации, геополитических вызовов и рисков, всемирного социально-экономического кризиса, формирования многополярности в мире, укрепления организационно-правового противодействия уязвимости российских информационных ресурсов, информационных систем и объектов информационной инфраструктуры.

Литература

1. Полякова Т.А. Развитие конституционно-правовых основ обеспечения информационной безопасности // Новеллы Конституции Российской Федерации и задачи юридической науки. М., 2021. С. 294—299.
2. Виноградова Е.В., Данилевская-Урбанова И.Л. Информационный суверенитет в правовом поле конституционной государственности // Правовая информатика. 2025. № 3. С. 126—133.
3. Троян Н.А. Правовое обеспечение цифрового суверенитета России: актуальные проблемы и перспективные направления // Право и государство: теория и практика. 2024. № 6 (234). С. 169—172.
4. Полякова Т.А., Троян Н.А. Стратегические задачи обеспечения технологического и цифрового суверенитета: правовые аспекты формирования новой информационной среды // Правовая информатика. 2025. № 1. С. 70—78.
5. Правовое обеспечение суверенитета и кодификация информационного законодательства / Ю.М. Батурин, Т.А. Полякова, А.В. Минбалеев [и др.]. М. : Институт государства и права РАН, 2024. 228 с.
6. Савченко Е.А. Актуальность вопроса кодификации законодательства, регулирующего отношения в виртуальном пространстве // Правовая информатика. 2025. № 2. С. 47—56.
7. Минбалеев А.В. Доктрина информационной безопасности Российской Федерации: современное состояние и перспективы развития // Вестник УрФО. Безопасность в информационной сфере. 2016. № 3 (21). С. 62—66.
8. Лось Л.В. Информационная безопасность в системе национальной безопасности Российской Федерации // Вопросы российского и международного права. 2019. Т. 9. № 3А. С. 159—170.
9. Ключко Р.Н. Информационная безопасность в социально-гуманитарном измерении: дискурс уголовно-правовой институционализации // Журнал российского права. 2025. № 10. С. 140—155.
10. Полякова Т.А., Троян Н.А. Обеспечение суверенитета в информационном пространстве — стратегическая задача национальной политики // Правовая политика и правовая жизнь. 2024. № 1. С. 41—53.
11. Камалова Г.Г. Некоторые проблемы правового обеспечения конфиденциальности информации в условиях цифровизации и геополитических рисков // Цифровые технологии и право: сборник научных трудов II Межд. науч.-практ. конф. В 6 т. Казань, 22 сентября 2023 года. Казань : Познание, 2023. С. 178—185.

LEGAL SUPPORT OF INFORMATION SECURITY OF THE RUSSIAN FEDERATION: REGULATORY FRAMEWORKS AND CURRENT CHALLENGES

Andrei K. Duben[7]

Keywords: *legal regulation, transformation of law, digitalization, legal regulation, cybersecurity, challenges and threats, risks.*

Abstract

The purpose of the work *is to identify modern legal frameworks and mechanisms for ensuring information security, identify challenges, threats and risks, analyze the regulatory framework, identify gaps and contradictions, and establish recommendations for improving the regulatory framework in the field of information security.*

The following general scientific methods *have become research methods: analysis and synthesis, abstraction and modeling, generalization, description, classification, etc. Special private-law methods of cognition were used: historical-legal, comparative-legal, formal-legal, etc.*

The results of the study. *The legal norms governing legal relations in the field of legal provision of information security are analyzed, actual problems and conflicts in Russian legislation are identified, and proposals for improving certain regulatory legal acts are formulated. The current and topical challenges, threats and risks in the field of information security are highlighted. It is concluded that it is necessary to implement a set of measures aimed at strengthening regulations in the field of information security in a number of areas. First of all, it is necessary to introduce a unified legal regime for the protection of state information systems, systems that process personal data, and critical information infrastructure facilities. These measures will allow us to solve a number of tasks aimed at ensuring security in modern conditions of digitalization, geopolitical challenges and risks, the global socio-economic crisis, and the formation of multipolarity in the world.*

References

1. Poliakova T.A. Razvitie konstitutsionno-pravovykh osnov obespecheniia informatsionnoi bezopasnosti // Novelly Konstitutsii Rossiiskoi Federatsii i zadachi iuridicheskoi nauki. M., 2021. S. 294–299.
2. Vinogradova E.V., Danilevskaia-Urbanova I.L. Informatsionnyi suverenitet v pravovom pole konstitutsionnoi gosudarstvennosti // Pravovaia informatika. 2025. No. 3. S. 126–133.
3. Troian N.A. Pravovoe obespechenie tsifrovogo suvereniteta Rossii: aktual'nye problemy i perspektivnye napravleniia // Pravo i gosudarstvo: teoriia i praktika. 2024. No. 6 (234). S. 169–172.
4. Poliakova T.A., Troian N.A. Strategicheskie zadachi obespecheniia tekhnologicheskogo i tsifrovogo suvereniteta: pravovye aspekty formirovaniia novoi informatsionnoi sredy // Pravovaia informatika. 2025. No. 1. S. 70–78.
5. Pravovoe obespechenie suvereniteta i kodifikatsiia informatsionnogo zakonodatel'stva / Iu.M. Baturin, T.A. Poliakova, A.V. Minbaleev [i dr.]. M. : Institut gosudarstva i prava RAN, 2024. 228 s.
6. Savchenko E.A. Aktual'nost' voprosa kodifikatsii zakonodatel'stva, reguliruiushchego otnosheniia v virtual'nom prostranstve // Pravovaia informatika. 2025. No. 2. S. 47–56.
7. Minbaleev A.V. Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii: sovremennoe sostoianie i perspektivy razvitiia // Vestnik UrFO. Bezopasnost' v informatsionnoi sfere. 2016. No. 3 (21). S. 62–66.
8. Los' L.V. Informatsionnaia bezopasnost' v sisteme natsional'noi bezopasnosti Rossiiskoi Federatsii // Voprosy rossiiskogo i mezhdunarodnogo prava. 2019. T. 9. No. 3A. S. 159–170.
9. Kliuchko R.N. Informatsionnaia bezopasnost' v sotsial'no-gumanitarnom izmerenii: diskurs ugolovno-pravovoi institutsionalizatsii // Zhurnal rossiiskogo prava. 2025. No. 10. S. 140–155.
10. Poliakova T.A., Troian N.A. Obespechenie suvereniteta v informatsionnom prostranstve – strategicheskaia zadacha natsional'noi politiki // Pravovaia politika i pravovaia zhizn'. 2024. No. 1. S. 41–53.
11. Kamalova G.G. Nekotorye problemy pravovogo obespecheniia konfidentsial'nosti informatsii v usloviiakh tsifrovizatsii i geopoliticheskikh riskov // Tsifrovye tekhnologii i pravo: sbornik nauchnykh trudov II Mezhd. nauch.-prakt. konf. V 6 t. Kazan', 22 sentiabria 2023 goda. Kazan' : Poznanie, 2023. S. 178–185.

[7] ***Andrei K. Duben,*** *Ph.D. (Law), Senior Researcher at the Institute of State and Law of the Russian Academy of Sciences, Moscow, Russian Federation.*
E-mail: k.duben@mail.ru