5.1.2.

Публично-правовые (государственно-правовые) науки (юридические науки)

Public Law (State Law) Sciences

DOI: 10.33693/2072-3164-2025-18-5-25-34

УДК: 342

ГРНТИ: 10.15

EDN: SENMDB

Правовые основы цифрового суверенитета в Российской Федерации

© Спартак Сергей Андреевич

Московский государственный университет имени М.В. Ломоносова, г. Москва, Российская Федерация

sspartak@yandex.ru

Аннотация: *Актуальность темы цифрового суверенитета обусловлена вызовами в сфере информационной безопасности государства, тенденциями глобальной цифровой политики и нарастающей конкуренцией государств в киберпространстве. Целью исследования является анализ и систематизация правовой базы цифрового суверенитета в Российской Федерации. Проанализированы ключевые нормативные акты, формирующие основу национального цифрового суверенитета (в том числе Федеральные законы № 242-ФЗ, № 187-ФЗ, № 90-ФЗ и др.). Отдельное внимание уделено стратегическим документам, включая Доктрину информационной безопасности и Стратегию национальной безопасности Российской Федерации, которые определяют государственную политику в данной сфере. Рассмотрена практика реализации указанных мер и выявлены основные вызовы, среди которых усиление цензуры в информационном пространстве, фрагментация интернета по национальным границам и сохраняющаяся технологическая зависимость от зарубежных технологий, что препятствует достижению цифровой независимости. Кроме того, оцениваются перспективы развития правового регулирования с учётом стремительного развития новых технологий (искусственный интеллект, Интернет вещей, сети 5G/6G), несущих новые вызовы и требующих обновления законодательства в целях обеспечения цифрового суверенитета. По итогам исследования подчёркивается необходимость достижения оптимального баланса между укреплением национальной цифровой безопасности и сохранением свободы в цифровом пространстве.*

Ключевые слова: *цифровой суверенитет, информационная безопасность, правовое регулирование, цензура, фрагментация интернета, технологическая зависимость*

Для цитирования: *Спартак С.А. Правовые основы цифрового суверенитета в Российской Федерации // Пробелы в российском законодательстве. 2025. Т. 18. № 5. С. 25–34. DOI: 10.33693/2072-3164-2025-18-5-25-34. EDN: SENMDB*

© Издательский дом «Юр-ВАК»
Статья доступна по лицензии CC BY-NC-ND 4.0 International

DOI: 10.33693/2072-3164-2025-18-5-25-34

Legal Foundations of Digital Sovereignty in the Russian Federation

© Sergey A. Spartak

Lomonosov Moscow State University, Moscow, Russian Federation

sspartak@yandex.ru

Abstract: *The relevance of digital sovereignty is driven by challenges in the field of national information security, trends in global digital policy, and the growing competition among states in cyberspace. The aim of the study is to analyze and systematize the legal framework of digital sovereignty in the Russian Federation. The study analyzes key normative legal acts that form the basis of national digital sovereignty (including Federal Laws No. 242, No. 187, No. 90, etc.). Special attention is given to strategic documents, including the Information Security Doctrine and the National Security Strategy of the Russian Federation, which define state policy in this area. The study examines the practice of implementing these measures and identifies the main challenges, among which are increased Internet censorship, fragmentation of the Internet along national borders, and a persistent technological dependence on foreign technologies that hinders the achievement of digital independence. Additionally, the study evaluates the prospects for the development of legal regulation in light of the rapid development of new technologies (artificial intelligence, the Internet of Things, 5G/6G networks), which bring new challenges and require updating legislation to ensure digital sovereignty. Overall, the need to achieve an optimal balance between strengthening national digital security and preserving freedom in the digital space is emphasized.*

Keywords: *digital sovereignty; information security; legal framework; censorship; Internet fragmentation; technological dependence*

For citation: *Spartak, S.A. (2025). Legal foundations of digital sovereignty in the Russian Federation. Gaps in Russian Legislation, 18(5), 25–34. DOI: 10.33693/2072-3164-2025-18-5-25-34. EDN: SENMDB*

For citation: *Spartak S.A. "Legal Foundations of Digital Sovereignty in the Russian Federation." Gaps in Russian Legislation. Vol. 18 no. 5 (2025): 25–34. DOI: 10.33693/2072-3164-2025-18-5-25-34. EDN: SENMDB*

ВВЕДЕНИЕ

Цифровой суверенитет государства подразумевает способность государства самостоятельно контролировать свое цифровое пространство, инфраструктуру и данные, обеспечивая их безопасность и независимость от внешнего вмешательства. Российская Федерация в последние годы активно формирует политику, направленную на укрепление суверенитета в цифровой сфере—от разработки концептуальных основ до принятия конкретных нормативно-правовых актов, регулирующих национальный сегмент сети Интернет и защиту критически важной информационной инфраструктуры.

Официальный курс на обеспечение цифрового суверенитета во многом обусловлен стремлением государства защитить национальную безопасность и устойчивость работы цифровых систем на своей территории. В стратегии национального развития до 2030 г. установление «сетевого суверенитета» провозглашено необходимым условием технологического лидерства страны[1]. После принятия в 2019 г. так называемого закона «о суверенном Рунете»[2] российские власти заявляли, что эти меры нужны для защиты от внешних угроз, тогда как многие эксперты указывали на их направленность прежде всего на усиление внутреннего контроля и цензуры в сети[3]. Таким образом, тема цифрового суверенитета РФ находится на пересечении вопросов безопасности, прав человека и развития цифровой экономики, вызывая дискуссии в обществе и международном сообществе.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЦИФРОВОГО СУВЕРЕНИТЕТА

Понятие цифрового суверенитета сформировалось на стыке доктрины государственного суверенитета и современного этапа информационно-технологического развития. Под цифровым

[1] См.: Моржакова М. Суверенитет в Сети: российский путь // Новый проспект, 21.05.2024. URL: https://newprospect.ru/news/articles/suverenitet-v-seti-rossiyskiy-put/ (дата обращения: 01.09.2025 г.).

[2] См.: О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации»: Федеральный закон от 1 мая 2019 г. № 90-ФЗ // Официальный интернет-портал правовой информации. Номер опубликования: 0001201905010025. URL: https://publication.pravo.gov.ru/document/view/0001201905010025 (дата обращения: 01.09.2025 г.).

[3] См.: Моржакова М. Суверенитет в Сети: российский путь // Новый проспект, 21.05.2024. URL: https://newprospect.ru/news/articles/suverenitet-v-seti-rossiyskiy-put/ (дата обращения: 01.09.2025 г.).

суверенитетом государства обычно понимается его право и возможность самостоятельно определять политику в сфере информации и технологий, управлять собственной цифровой инфраструктурой и ресурсами, обеспечивать информационную безопасность на своей территории[4]. Иными словами, речь идет о распространении принципов государственного суверенитета (территориального верховенства и независимости) на киберпространство, национальный сегмент Интернета и связанные с ним цифровые объекты.

Одним из первых в российском дискурсе термин «цифровой суверенитет» ввел эксперт Игорь Ашманов, определив его как «право государства определять свою информационную политику самостоятельно, распоряжаться инфраструктурой, ресурсами и обеспечивать информационную безопасность»[5]. Данное определение отражает ключевые компоненты цифрового суверенитета: самостоятельность государства в управлении цифровой сферой и обязанность государства защищать эту сферу от внешних и внутренних угроз (например, кибератак, неконтролируемого выведения данных за рубеж, иностранной цензуры или доминирования иностранных технологических монополий).

Важно отметить, что близким понятием является информационный суверенитет, возникший еще ранее и акцентирующий независимость государства в информационном пространстве. Цифровой суверенитет можно рассматривать как более широкое и технологически ориентированное развитие этой идеи, учитывающее не только контент и информацию, но и техническую инфраструктуру (сети, серверы, центры обработки данных, программное обеспечение)[6]. В некоторых зарубежных концепциях используется термин «киберсуверенитет», особенно там, где выступают за принцип невмешательства во внутренние цифровые дела государств на международной арене[7]. Российский подход во многом созвучен этой позиции и исходит из того, что интернет-пространство не должно быть бесконтрольным наднациональным доменом: суверенные государства вправе устанавливать правила поведения в своем сегменте сети.

Теоретическое обоснование цифрового суверенитета в РФ опирается на следующие положения. Во-первых, государственный суверенитет, закрепленный в Конституции РФ, распространяется на всю территорию России, а в современном мире информация и киберпространство рассматриваются как часть этой территории в функциональном смысле. Во-вторых, обеспечение национальной безопасности требует контроля над критическими информационными системами, поскольку зависимость от иностранных ИТ-ресурсов и отсутствие барьеров против внешних информационных воздействий создают уязвимости для государства. В-третьих, цифровой суверенитет соотносится с понятием технологической независимости: развитие собственных технологий, отечественного программного обеспечения и аппаратных решений рассматривается как условие конкурентоспособности и устойчивости государства[8]. Так, в Доктрине информационной безопасности Российской Федерации 2016 г. прямо отмечалась необходимость ликвидации зависимости отечественной индустрии от зарубежных информационных технологий путем разработки и внедрения отечественных продуктов и услуг[9].

С критической точки зрения, противники абсолютизации концепции цифрового суверенитета указывают, что излишний акцент на государственном контроле в цифровой среде чреват ограничением свобод интернет-пользователей и замедлением технологического развития. Интернет по своей природе глобален, и жесткое разграничение его по национальным юрисдикциям ведет к феномену «суверенных интернетов» и фрагментации глобальной сети. Международные правозащитные организации полагают, что под лозунгом цифрового суверенитета некоторые государства вводят цензуру и тотальную слежку, что противоречит принципам свободы информации. Тем не менее, сама по себе идея цифрового суверенитета стала фактом мировой политики: все больше стран стремятся защищать данные своих граждан, устанавливать национальные правила для глобальных платформ и развивать собственные цифровые мощности. Рассмотрим, как эти тенденции реализуются в правовой системе Российской Федерации.

НОРМАТИВНО-ПРАВОВАЯ БАЗА ЦИФРОВОГО СУВЕРЕНИТЕТА В РФ

Формирование правовых основ цифрового суверенитета в России осуществлялось поэтапно, отражая реагирование государства на новые вызовы цифровой эпохи. К настоящему времени можно выделить ряд ключевых нормативно-правовых актов и документов, которые составляют основу государственной политики в данной сфере.

Одним из первых значимых шагов к обеспечению цифровой независимости стало введение требования локального хранения персональных данных российских граждан. Федеральным законом № 242-ФЗ от 21.07.2014 были внесены изменения в Закон РФ «О персональных

[4] См.: Эмельянов А.А., Коршунов И.Л., Микадзе С.Ю. К вопросу о цифровом суверенитете России. Аналитическая статья Фонда «Росконгресс», 2022. URL: https://roscongress.org/materials/k-voprosu-o-tsifrovom-suverenitete-rossii-/ (дата обращения 01.09.2025 г.).

[5] См.: Эмельянов А.А., Коршунов И.Л., Микадзе С.Ю. К вопросу о цифровом суверенитете России. Аналитическая статья Фонда «Росконгресс», 2022. URL: https://roscongress.org/materials/k-voprosu-o-tsifrovom-suverenitete-rossii-/ (дата обращения 01.09.2025 г.).

[6] Подробнее см.: Couture S., Toupin S. What does the notion of «sovereignty» mean when referring to the digital? // New Media & Society. 2019. Vol. 21, No. 10. Pp. 2305–2322. URL: https://journals.sagepub.com/doi/full/10.1177/1461444819865984 (дата обращения: 02.09.2025 г.); Авдийский В.И., Иванов А.В., Царегородцев А.В. Взаимосвязь цифрового суверенитета и цифрового пространства: новые вызовы и перспективы // Вестник Евразийской науки. 2024. Т. 16, № 3. 19 с. URL: https://esj.today/PDF/21FAVN324.pdf (дата обращения: 02.09.2025 г.).

[7] См.: РСМД: Практика цифрового суверенитета в России и КНР URL: https://russiancouncil.ru/analytics-and-comments/analytics/praktika-tsifrovogo-suvereniteta-v-rossii-i-knr/ (дата обращения: 02.09.2025 г.).

[8] См.: РСМД: Практика цифрового суверенитета в России и КНР URL: https://russiancouncil.ru/analytics-and-comments/analytics/praktika-tsifrovogo-suvereniteta-v-rossii-i-knr/ (дата обращения: 02.09.2025 г.).

[9] См.: Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 г. № 646) // Российская газета. 2016. № 8.

данных» № 152-ФЗ[10], обязывающие всех операторов, собирающих персональные данные россиян, обеспечить запись, хранение и извлечение таких данных через базы данных, находящиеся на территории России[11]. Эта норма вступила в силу с 1 сентября 2015 г. и затрагивает широкий круг организаций, включая зарубежные компании, работающие на российском рынке (соцсети, интернет-сервисы, авиакомпании, электронную коммерцию и пр.). Невыполнение требования локализации может вести к административной ответственности вплоть до блокировки ресурса на территории РФ. Показательным случаем стала блокировка деловой социальной сети LinkedIn в 2016 г.: данная платформа стала первым крупным иностранным сайтом, отключенным в России за невыполнение закона о хранении данных российских пользователей на российских серверах[12]. Суд в Москве установил, что LinkedIn нарушал требования российского законодательства о персональных данных, и Роскомнадзор внес сайт в реестр нарушителей, после чего доступ к нему был ограничен[13]. Этот прецедент продемонстрировал серьезность намерений государства добиваться юрисдикционного контроля над данными граждан, даже ценой конфликта с международными интернет-компаниями.

Следующим элементом стала законодательная база для оперативного контроля за электронными коммуникациями. В 2016 г. принят так называемый «пакет Яровой»—два федеральных закона (№ 374-ФЗ и № 375-ФЗ от 6 июля 2016 г.[14]), внесшие изменения в законодательство о связи, информации и противодействии терроризму. Эти поправки обязали телекоммуникационных операторов и «организаторов распространения информации» (т.е. владельцев интернет-сервисов, мессенджеров) хранить содержание сообщений и передаваемые данные пользователей в течение установленного срока, а также предоставлять спецслужбам средства для декодирования зашифрованного трафика. По сути, данные нормы создали предпосылки для массового мониторинга интернет-трафика государственными органами. Именно на основании данного требования ФСБ потребовала от мессенджера Telegram передачи ключей шифрования для доступа к переписке пользователей, что компания категорически отвергла, сославшись на конфиденциальность. В результате в апреле 2018 г. суд принял решение о блокировке Telegram на территории РФ за неисполнение закона[15]. Роскомнадзор внес сервис в реестр запрещенных и пытался технически ограничить к нему доступ, что привело к масштабным сбоям (были заблокированы миллионы IP-адресов из-за использования Telegram облачных серверов)[16]. Хотя блокировка не достигла ожидаемого результата (многие пользователи обходили ее через VPN), данный пример стал знаковым в контексте цифрового суверенитета: государство продемонстрировало готовность серьезно обеспечить выполнение своих законов в цифровой сфере, даже если это сопровождается технологическими трудностями и общественной критикой. Спустя два года, в 2020 г., ограничение доступа к Telegram было официально снято—во многом признано, что сервис пошёл на сотрудничество по вопросам экстремизма, а технические возможности контроля возросли. Тем не менее, прецедент Telegram закрепил в правоприменительной практике потенциал государства блокировать глобальные платформы во имя суверенных интересов.

Важной вехой стало принятие Федерального закона № 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры РФ»[17]. Этот закон установил основы защиты значимых объектов информационных систем—таких, как системы управления на транспорте, в энергетике, банковском секторе, связи, а также госинформсистемы. Закон обязал владельцев объектов критической информационной инфраструктуры (далее—КИИ) внедрять меры защиты, проводить мониторинг инцидентов, уведомлять государство об атаках, а также предусмотрел создание государственной системы обнаружения и предупреждения компьютерных атак (далее—ГосСОПКА). Реализация положений этого закона напрямую связана с обеспечением цифрового суверенитета, поскольку направлена на предотвращение внешних деструктивных воздействий на ключевые цифровые ресурсы страны. В развитие данной политики в 2018 г. Министерство цифрового развития (тогда—Минкомсвя-

[10] См.: Федеральный закон от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» // Собрание законодательства Российской Федерации. 2014. № 30 (ч. I). Ст. 4243. URL: https://publication.pravo.gov.ru/Document/View/0001201407220042 (дата обращения: 01.09.2025 г.).

[11] См.: Duane Morris LLP—Russia's New Personal Data Localization Law Goes into Effect in September 2015. URL: https://www.duanemorris.com/alerts/russia_new_personal_data_localization_law_into_effect_september_2015_0615.html (дата обращения: 02.09.2025 г.).

[12] См.: Stubbs J., Ostroukh A. Russia to ban Telegram messenger over encryption dispute // Reuters, 13.04.2018. URL: https://www.reuters.com/article/russia-telegram-block-idUSKBN1HK10B (дата обращения: 01.09.2025 г.).

[13] См.: Walker S. Russia blocks access to LinkedIn over foreign-held data // The Guardian, 17.11.2016. URL: https://www.theguardian.com/world/2016/nov/17/russia-blocks-access-to-linkedin-over-foreign-held-data (дата обращения: 01.09.2025 г.).

[14] См.: Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон "О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Собрание законодательства Российской Федерации. 2016. № 28. Ст. 4558. URL: https://publication.pravo.gov.ru/Document/View/0001201607070016 (дата обращения: 01.09.2025 г.); Федеральный закон от 6 июля 2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Собрание законодательства Российской Федерации. 2016. № 28. Ст. 4559. URL: https://publication.pravo.gov.ru/Document/View/0001201607070042 (дата обращения: 01.09.2025 г.).

[15] См.: Stubbs J., Ostroukh A. Russia to ban Telegram messenger over encryption dispute // Reuters, 13.04.2018. URL: https://www.reuters.com/article/russia-telegram-block-idUSKBN1HK10B (дата обращения: 01.09.2025 г.).

[16] См.: Stubbs J., Ostroukh A. Russia to ban Telegram messenger over encryption dispute // Reuters, 13.04.2018. URL: https://www.reuters.com/article/russia-telegram-block-idUSKBN1HK10B (дата обращения: 01.09.2025 г.).

[17] См.: О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26 июля 2017 г. № 187-ФЗ // Собрание законодательства РФ. 2017. № 31. Ст. 4736. Официальный интернет-портал правовой информации. URL: https://publication.pravo.gov.ru/Document/View/0001201707260023 (дата обращения: 01.09.2025 г.).

зи) инициировало программу по переходу критической инфраструктуры на отечественное программное и аппаратное обеспечение[18]. Предполагалось, что к 2021–2022 гг. операторы КИИ должны начать использовать исключительно российские или евразийские софты и оборудование. Хотя эти сроки оказались слишком оптимистичными и были скорректированы, курс на импортозамещение в сфере информационно-коммуникационных технологий получил нормативное закрепление и финансирование. Таким образом, к концу 2010-х сформировался комплекс мер, укрепляющих технологическую независимость российского сегмента Интернета и цифровой инфраструктуры.

Кульминацией нормативного оформления цифрового суверенитета стал Федеральный закон от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите информации"—широко известный как закон "о суверенном Рунете"»[19]. Этот закон прямо направлен на создание в России автономной инфраструктуры Интернет, способной поддерживать работоспособность российского сегмента в случае внешнего отключения, а также на введение механизмов централизованного управления российским сегментом сети. Закон вступил в силу 1 ноября 2019 г.

Основные положения закона о суверенном Интернете включают следующие меры[20]:

— На операторов связи возлагается обязанность устанавливать специальные технические средства противодействия угрозам (далее—ТСПУ) на точках обмена трафиком и линиях связи, пересекающих границу РФ. Эти устройства с функцией «Deep Packet Inspection»[21] (далее—DPI) позволяют анализировать и фильтровать трафик;

— Создается центр мониторинга и управления сетью связи общего пользования, через который Роскомнадзор получает возможность в случае угроз оперативно управлять маршрутизацией трафика. Проще говоря, государственный регулятор может при наступлении определенных условий перераспределять потоки данных, ограничивать или перенаправлять соединения на международных каналах[22];

— Вводится обязательная регистрация точек обмена трафиком (узлов подключения сетей друг к другу). Только внесенные в государственный реестр узлы могут использоваться операторами, а несоблюдение указаний регулятора грозит отключением оператора от точек обмена.

— Предусмотрено проведение учений по отработке действий в условиях угроз устойчивости Интернета, а также создание национальной системы доменных имен (далее—DNS)—копии корневых серверов DNS внутри страны, чтобы обеспечить разрешение доменных имен автономно.

Закон был мотивирован официально необходимостью защититься от гипотетического отключения России от глобального интернета извне. В пояснительной записке и заявлениях авторов указывалось, что США в своей киберстратегии допускают наступательные операции в киберпространстве, приведен пример отключения Сирии от Интернета в 2012 г. (предположительно вследствие действий Агентства Национальной Безопасности США)[23]. Соответственно, по замыслу законодателей, автономная инфраструктура (включая дублирующие корневые DNS-серверы) позволит сохранить

[18] Подробнее см.: Эмельянов А.А., Коршунов И.Л., Микадзе С.Ю. К вопросу о цифровом суверенитете России. Аналитическая статья Фонда «Росконгресс», 2022. URL: https://roscongress.org/materials/k-voprosu-o-tsifrovom-suverenitete-rossii-/ (дата обращения 01.09.2025 г.); Об утверждении Методических рекомендаций по переходу государственных компаний на преимущественное использование отечественного программного обеспечения, в том числе отечественного офисного программного обеспечения: Приказ Минкомсвязи России от 20 сентября 2018 г. № 486 [в ред. 10.09.2021] // КонсультантПлюс (официальная публикация: Минцифры, файл-релиз на официальном сайте). URL: https://digital.gov.ru/uploaded/files/metodicheskie-rekomendatsii-po-perekhodu-na-ispolzovanie-rossijskogo-programmnogo-obespecheniya.docx (дата обращения: 01.09.2025 г.); Сводная карточка. URL: https://www.consultant.ru/document/cons_doc_LAW_314283/ (дата обращения: 01.09.2025 г.); Об утверждении методических рекомендаций по переходу органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления на использование отечественного офисного программного обеспечения, в том числе ранее закупленного: Приказ Минкомсвязи России от 04 июля 2018 г. № 335 // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_303138/ (дата обращения: 01.09.2025 г.); Об утверждении Методических рекомендаций по переходу на использование российского программного обеспечения, в том числе на значимых объектах критической информационной инфраструктуры…: Приказ Минцифры России от 18.01.2023 № 21 // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_439904/ (дата обращения: 01.09.2025 г.).

[19] См.: О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации»: Федеральный закон от 1 мая 2019 г. № 90-ФЗ // Официальный интернет-портал правовой информации. Номер опубликования: 0001201905010025. URL: https://publication.pravo.gov.ru/document/view/0001201905010025 (дата обращения: 01.09.2025 г.).

[20] См.: О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации»: Федеральный закон от 1 мая 2019 г. № 90-ФЗ // Официальный интернет-портал правовой информации. Номер опубликования: 0001201905010025. URL: https://publication.pravo.gov.ru/document/view/0001201905010025 (дата обращения: 01.09.2025 г.).

[21] См.: Об установке, эксплуатации и о модернизации в сети связи оператора связи технических средств противодействия угрозам…: Постановление Правительства РФ от 12 февраля 2020 г. № 126 (в ред. 28.02.2024) // Официальный интернет-портал правовой информации. URL: https://ips.pravo.gov.ru/?docbody=&link_id=8&nd=102677953&vkart=card (дата обращения: 01.09.2025 г.); Термин DPI не используется в тексте закона № 90-ФЗ и ПП № 126, там фигурирует обобщённое понятие «технические средства противодействия угрозам» (ТСПУ), однако DPI—технологическая основа для реализации функций фильтрации/ограничения доступа, предусмотренных законом.

[22] См.: Russia's «Sovereign Internet» Law // Internet Society—Internet Fragmentation Insights, 01.12.2023. URL: https://www.internetsociety.org/resources/internet-fragmentation/russias-sovereign-internet-law/ (дата обращения: 01.09.2025 г.).

[23] Подробнее см.: Пояснительная записка к проекту Федерального закона № 608767–7 (редакция на момент внесения): [PDF-копия на базе «КонсультантПлюс»] URL: https://storage.consultant.ru/ondb/attachments/201902/3/3tf4trm52rotdql6/Zakonoproekt_N_608767-7_Ux M.pdf (дата обращения: 01.09.2025 г.); Законопроект о «суверенном интернете» принят в первом чтении: Официальный портал Государственной Думы, 12.02.2019. URL: https://duma.gov.ru/news/29748/ (дата обращения: 01.09.2025 г.); The White House. National Cyber Strategy of the United States of America. Washington, DC, Sept. 2018. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения: 01.09.2025 г.); Ars Technica. Snowden: the NSA, not Assad, took Syria off the Internet in 2012, 13.08.2014. URL: https://arstechnica.com/tech-policy/2014/08/snowden-the-nsa-not-assad-took-syria-off-the-internet-in-2012/ (дата обращения: 01.09.2025 г.).

работу российских сайтов и онлайн-сервисов, даже если зарубежные центры отключат Россию от сети[24].

Однако закон «о суверенном Рунете» вызвал бурные дискуссии среди операторов связи, экспертов ИТ-отрасли и правозащитников еще на стадии проекта. Комиссия РСПП (Российский союз промышленников и предпринимателей) по телекоммуникациям в своем отзыве отмечала, что угроза внешнего отключения маловероятна, так как в России уже имеются копии корневых серверов DNS и архитектура Интернета децентрализована настолько, что одномоментно отключить страну от сети извне практически невозможно. С технической точки зрения подчеркивалось, что централизация управления трафиком создаст единую точку отказа: концентрация контроля в руках государственных органов может, напротив, снизить устойчивость. Также высказывались опасения, что установка ТСПУ повлечет замедление скорости доступа и удорожание обслуживания сетей—расходы в конечном счете лягут на операторов и пользователей. Счетная палата РФ тоже в своем заключении не поддержала проект, указав на недостатки обоснования и возможные риски для экономики[25].

Несмотря на критику, закон был принят и начал реализовываться. По данным Роскомнадзора, к 2021–2022 гг. оборудованием ТСПУ были оснащены основные магистральные сети связи. Глава Роскомнадзора А. Липов утверждал, что российский сегмент Интернета теперь на 100% защищен от внешних угроз[26]. В 2021–2023 гг. проводились учения по устойчивости Рунета, включая тестовые отключения от глобальной сети: например, 15 июля 2021 г. и 6 июля 2023 г. сообщалось о проверке способности российского Интернета автономно функционировать. По некоторым сообщениям, в феврале 2024 г. был проведен повторный эксперимент отключения, а в декабре 2024 г.—целый день изоляции Интернета в Чеченской Республике[27]. Эти мероприятия призваны выявить узкие места и улучшить готовность инфраструктуры.

Помимо защиты от внешнего отключения, закон 90-ФЗ существенно усилил цензурно-контрольные функции государства. Благодаря ТСПУ Роскомнадзор теперь технически способен фильтровать трафик на сети провайдеров, блокируя запрещенные ресурсы более эффективно и централизованно, чем прежняя система блокировок по IP-адресам. По сути, создана возможность «ручного управления» российским сегментом Интернета, что характеризуется экспертами как движение в сторону модели «китайской великой стены». На практике, после 2022 г. государственные органы заблокировали или ограничили доступ к ряду западных социальных сетей, новостных сайтов и сервисов—во многом опираясь на обновленные технические возможности и правовые механизмы суверенного Интернета[28]. Тем самым, юридическая база, заложенная законом о суверенитете, стала инструментом для проведения независимой информационной политики в кризисный период.

Помимо упомянутых ключевых законов, правовые основы цифрового суверенитета дополняются и другими актами, например: Доктрина информационной безопасности РФ (2016 г.)[29]—упомянутый нами ранее стратегический документ, в котором провозглашены цели уменьшения технологической зависимости, развития отечественной индустрии ИТ и защиты от информационно-технических угроз; Национальная стратегия безопасности—усилила акцент на обеспечение суверенитета в информационном пространстве и защите критических технологий, называя развитие национальной цифровой экономики одним из условий устойчивости государства[30]; Программы «Цифровая экономика» (2017) и «Цифровая трансформация»—содержат компоненты импортозамещения софта и оборудования, стимулирования отечественных разработок, создания независимой инфраструктуры (национальные центры обработки данных, собственные операционные системы, шифровальные стандарты и пр.)[31]; Отдельные законодательные инициативы 2020–2022 гг.: закон об обязательном присутствии иностранных IT-компаний (офис или представитель) на территории РФ для работы (2021), регулирование VPN и анонимайзеров (запрет предоставления доступа к запрещенным сайтам, 2017 и расширения в 2021), меры по поддержке российских

[24] См.: Эмельянов А.А., Коршунов И.Л., Микадзе С.Ю. К вопросу о цифровом суверенитете России. Аналитическая статья Фонда «Росконгресс», 2022. URL: https://roscongress.org/materials/k-voprosu-o-tsifrovom-suverenitete-rossii-/ (дата обращения 01.09.2025 г.).

[25] См.: Эмельянов А.А., Коршунов И.Л., Микадзе С.Ю. К вопросу о цифровом суверенитете России. Аналитическая статья Фонда «Росконгресс», 2022. URL: https://roscongress.org/materials/k-voprosu-o-tsifrovom-suverenitete-rossii-/ (дата обращения 01.09.2025 г.).

[26] См.: Эмельянов А.А., Коршунов И.Л., Микадзе С.Ю. К вопросу о цифровом суверенитете России. Аналитическая статья Фонда «Росконгресс», 2022. URL: https://roscongress.org/materials/k-voprosu-o-tsifrovom-suverenitete-rossii-/ (дата обращения 01.09.2025 г.).

[27] См.: Елена Зиновьева, Бай Яцзе. Практика цифрового суверенитета в России и КНР // Российский совет по международным делам (РСМД)—Аналитическая статья, 29.05.2023. URL: https://russiancouncil.ru/analytics-and-comments/analytics/praktika-tsifrovogo-suvereniteta-v-rossii-i-knr/ (дата обращения: 01.09.2025 г.).

[28] См.: Елена Зиновьева, Бай Яцзе. Практика цифрового суверенитета в России и КНР // Российский совет по международным делам (РСМД)—Аналитическая статья, 29.05.2023. URL: https://russiancouncil.ru/analytics-and-comments/analytics/praktika-tsifrovogo-suvereniteta-v-rossii-i-knr/ (дата обращения: 01.09.2025 г.).

[29] См.: Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 г. № 646) // Российская газета. 2016. № 8.

[30] См.: Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Официальный интернет-портал правовой информации. 02.07.2021. URL: https://publication.pravo.gov.ru/Document/View/0001202107020034 (дата обращения: 01.09.2025 г.).

[31] Подробнее см.: Распоряжение Правительства Российской Федерации от 28.07.2017 № 1632-р «Об утверждении программы "Цифровая экономика Российской Федерации" // Официальный интернет-портал правовой информации. 28.07.2017. URL: https://pravo.gov.ru/proxy/ips/?docbody=&nd=102440918 (дата обращения: 01.09.2025 г.); Паспорт национальной программы "Цифровая экономика Российской Федерации" // Правительство России (официальный сайт). 24.12.2018. URL: https://government.ru/info/35568/ (дата обращения: 01.09.2025 г.); Распоряжение Правительства Российской Федерации от 16.03.2024 № 637-р "Об утверждении стратегического направления в области цифровой трансформации государственного управления" // Официальный интернет-портал правовой информации. 20.03.2024. URL: https://publication.pravo.gov.ru/document/0001202403200032 (дата обращения: 01.09.2025 г.); Постановление Правительства Российской Федерации от 16.11.2015 № 1236 "Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» (с изм.) // Официальный интернет-портал правовой информации. 20.11.2015. URL: https://publication.pravo.gov.ru/Document/View/0001201511200006 (дата обращения: 01.09.2025 г.).

социальных сетей и онлайн-сервисов и др. Все они складываются в общую мозаику укрепления юрисдикционного контроля над цифровой средой[32].

ПРАКТИКА РЕАЛИЗАЦИИ И ДИСКУССИОННЫЕ ВОПРОСЫ

Политика цифрового суверенитета в России привела к заметным изменениям в функционировании отечественного сегмента Интернета и отношениях государства с крупными технологическими компаниями. Реализация рассмотренных правовых норм сопровождается как успешными прецедентами, так и спорными моментами, выявившими ряд проблем.

С положительной стороны, можно отметить создание национальной инфраструктуры: развита Государственная система предотвращения атак (ГосСОПКА), функционируют центры мониторинга (ФСТЭК, ФСБ, Роскомнадзор курируют различные аспекты безопасности)[33]. Построена Национальная система платежных карт «Мир» (после ухода Visa/Mastercard в 2014), что снизило зависимость от западных платежных систем[34]. Ускорилось развёртывание отечественных корневых DNS-серверов[35] и точек обмена трафиком. Запущены отечественные аналоги популярных сервисов—например, видеохостинг RuTube, платформа Яндекс.Видео и VK. Видео, отечественные маркетплейсы приложений (RuStore) взамен Google Play и др[36]., и т.п. После введения западных санкций 2022 г. и исхода ряда иностранных ИТ-платформ наблюдается рост спроса на российское ПО и онлайн-сервисы: появились свои образовательные платформы (Stepik, Skillbox вместо Coursera)[37] и другие продукты[38].

Закон о безопасности КИИ стимулировал компании в важных секторах укреплять защиту. Хотя внедрение шло медленно, крупные игроки инвестировали в собственные системы киберзащиты. В 2022 г., столкнувшись с волной беспрецедентных кибератак на российские сайты и инфраструктуру (особенно в первые месяцы после начала специальной военной операции), государственные и частные структуры сумели в основном предотвратить фатальные сбои. По данным «Ростелекома», число кибератак весной 2022 выросло в 7 раз[39], но координированные действия по линии Минцифры, ФСБ и спецслужб позволили сохранить работоспособность критических систем. Этот опыт лишь укрепил аргументацию в пользу концепции цифрового суверенитета—как гаранта безопасности в условиях геополитической турбулентности.

Более того, Россия на площадках ООН последовательно продвигает идею суверенного равенства государств применительно к информационному пространству и принцип невмешательства. В 2021 г. в рамках ООН был достигнут консенсус, что международное право и, в частности, принцип суверенитета применим к ИКТ-среде, хотя остаются разногласия в трактовках[40]. Тем не менее, российская дипломатия (совместно с Китаем и др.) способствовала принятию резолюций о правилах ответственного поведения государств в киберпространстве,

[32] Подробнее см.: Федеральный закон от 01.07.2021 № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети Интернет на территории Российской Федерации» // Официальный интернет-портал правовой информации. 01.07.2021. URL: https://publication.pravo.gov.ru/Document/View/0001202107010059 (дата обращения: 01.09.2025 г.); Федеральный закон от 29.07.2017 № 276-ФЗ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации» (об обязанности анонимайзеров/VPN ограничивать доступ к запрещенным ресурсам) // Официальный интернет-портал правовой информации. 30.07.2017. URL: https://publication.pravo.gov.ru/Document/View/0001201707300002 (дата обращения: 01.09.2025 г.); Постановление Правительства Российской Федерации от 29.12.2021 № 2531 «Об утверждении Правил ведения перечня отечественных социально значимых информационных ресурсов» // Официальный интернет-портал правовой информации. 30.12.2021. URL: https://publication.pravo.gov.ru/Document/View/0001202112300210 (дата обращения: 01.09.2025 г.).

[33] Подробнее см.: Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Официальный интернет-портал правовой информации. 26.07.2017. URL: https://publication.pravo.gov.ru/document/view/0001201707260023 (дата обращения: 01.09.2025 г.); Справочно: «Правовые основания» ГосСОПКА // gossopka.ru (ФСБ России/НКЦКИ). URL: https://gossopka.ru/pravovye-osnovaniya/ (дата обращения: 01.09.2025 г.).

[34] См.: Банк России о НСПК // cbr.ru (официальный сайт). URL: https://cbr.ru/psystem/nspk/ (дата обращения: 01.09.2025 г.); «Национальная система платежных карт: история и развитие» // NSPK (официальный сайт). URL: https://nspk.ru/company/about/history/ (дата обращения: 01.09.2025 г.).

[35] Подробнее см.: Постановление Правительства Российской Федерации от 12.02.2020 № 127 «Об утверждении Правил централизованного управления сетью связи общего пользования» // Официальный интернет-портал правовой информации. 13.02.2020. URL: https://publication.pravo.gov.ru/document/0001202002130060 (дата обращения: 01.09.2025 г.); Приказ Роскомнадзора от 31.07.2019 № 229 «Об утверждении Положения о национальной системе доменных имен ...» (зарегистрирован Минюстом РФ 07.11.2019 № 56453) // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_337185/ (дата обращения: 01.09.2025 г.); Постановление Правительства Российской Федерации от 11.10.2019 № 1311 «Об утверждении Правил ведения реестра точек обмена трафиком интернет-трафика» // Официальный интернет-портал правовой информации (карточка). URL: https://publication.pravo.gov.ru/Document/View/0001201910140024 (дата обращения: 01.09.2025 г.).

[36] Подробнее см.: RuStore—официальный релиз (совместный проект VK и Минцифры) // Минцифры России. 25.05.2022. URL: https://digital.gov.ru/ru/events/50671/ (дата обращения: 01.09.2025 г.); RUTUBE (о сервисе; обновления платформы в 2022 г.) // Газпром-Медиа. 05.04.2022. URL: https://www.gazprom-media.com/ru/media/rutube-obnovil-dizayn-platformy-i-dobavil-vozmozhnost-kommentirovaniya (дата обращения: 01.09.2025 г.).

[37] Подробнее см.: «Coursera прекращает сотрудничество с российскими организациями» // РБК. 05.03.2022. URL: https://www.rbc.ru/politics/05/03/2022/6222fef29a79476cc5afeb6f (дата обращения: 01.09.2025 г.); Skillbox—«О компании» (официально) // Skillbox. URL: https://skillbox.ru/company/ (дата обращения: 01.09.2025 г.); Stepik—«О нас» (официально) // Stepik. URL: https://welcome.stepik.org/ru/about (дата обращения: 01.09.2025 г.).

[38] См.: Динамика ИТ-рынка РФ и импортозамещение (обзор) // CNews Analytics. 21.07.2025. URL: https://www.cnews.ru/reviews/rynok_it_itogi_2024/articles/-_1 (дата обращения: 01.09.2025 г.).

[39] См.: Количество кибератак на сервисы и структуры России в 2022 году выросло в семь раз // ТАСС. 21.03.2023. URL: https://tass.ru/ekonomika/17327093 (дата обращения: 02.09.2025 г.); Число кибератак на российские предприятия увеличилось в 10 раз в апреле–июне [Электронный ресурс] // Ведомости. 25.08.2022. URL: https://www.vedomosti.ru/technology/news/2022/08/25/937640-chislo-kiberatak-uvelichilos-v-10-raz? (дата обращения: 02.09.2025 г.).

[40] Подробнее см.: United Nations. Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. A/76/135. 14.07.2021. URL: https://docs.un.org/A/76/135 (дата обращения: 02.09.2025 г.); United Nations. Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. A/75/816. 18.03.2021. URL: https://docs.un.org/en/A/75/816 (дата обращения: 02.09.2025 г.).

где косвенно признается суверенное право государств на свою информационную инфраструктуру[41]. Это создает определенную легитимацию и для внутренних мер по суверенизации российского сегмента Интернета.

Вместе с тем, существует ряд противоречивых моментов. Критики указывают, что под предлогом цифрового суверенитета в России расширяется цензура интернета. Блокировка десятков тысяч сайтов (включая оппозиционные СМИ, иностранные соцсети), преследование за репосты и высказывания—все это стало возможным технически благодаря новым законам. Международные организации (Human *Rights Watch, Freedom *House и др.) отмечают усиление интернет-цензуры в РФ, снижающее рейтинги свободы интернета[42]. Возникает вопрос о балансе между суверенитетом и соблюдением конституционных прав на доступ к информации и свободное выражение мнения.

Бизнес-сообщество частично разделяет опасения. Если Россия пойдет по пути жесткого суверенного интернета, изолированного от глобальных потоков, это может затормозить внедрение новых технологий, отпугнуть зарубежные инвестиции в ИТ-сектор, сузить возможности для отечественных компаний на внешних рынках[43]. Пока этого не произошло в полной мере—мы по-прежнему связаны с глобальной сетью, и многие зарубежные платформы остаются доступными—однако перспектива усиления протекционизма в цифровой сфере беспокоит инновационный бизнес. Например, требования локализации данных и строгого соблюдения российских правил создают дополнительные расходы для международных сервисов; некоторые компании (Netflix, Spotify и др.) свернули работу в РФ, что сужает конкуренцию на рынке[44].

Практика показала, что построение полностью независимой инфраструктуры—сложная и дорогостоящая задача. Несмотря на успехи, Россия все еще зависит от импорта значительной части высокотехнологичного оборудования (серверы, сетевые процессоры и т.п.) и программного обеспечения. Санкции осложнили поставки, но стимулировали развитие собственных производств. Еще одна проблема—квалификация кадров: для обеспечения суверенитета нужны высококлассные специалисты в кибербезопасности, разработке софта, администрировании сетей. Отток ИТ-кадров за рубеж в 2022 г. и общее снижение притока молодых специалистов могут затруднить достижение поставленных целей. Государство пытается решать это за счет образовательных программ, привлечения талантов, однако эффект будет ощутим лишь в долгосрочной перспективе[45].

Кроме этого, в процессе быстрого наращивания регулирования не все нормы оказались согласованными. Например, режим блокировок сайтов по разным основаниям регулируется сразу несколькими законами (149-ФЗ «Об информации», 90-ФЗ «о суверенном Рунете», законами о противодействии экстремизму и фейкам и др.), что создает сложности правоприменения. Бизнес жалуется на неопределенность требований: в разных ситуациях регуляторы могут по-разному трактовать обязанности операторов связи или владельцев платформ. Это повышает регуляторные риски и требует совершенствования законодательства, устранения дублирующих или противоречивых положений[46].

Стоит подчеркнуть, что российский опыт цифрового суверенитета развивается в русле общемировых трендов, но имеет свою специфику. Для сравнения, в Китае действует самая масштабная система государственного контроля интернета, что обеспечило рост собственных ИТ-гигантов, хотя и ценой полной фильтрации внешнего контента[47]. Россия, напротив, долгое время стремилась не ограничивать доступ к глобальным платформам, ограничиваясь точечными блокировками запрещенного контента. Лишь с недавних пор, под влиянием геополитического противостояния, курс начал смещаться к более изоляционистскому. При этом российская политика делает акцент на международном сотрудничестве: Москва продвигает инициативы о международных правилах поведения в информационном пространстве, пытаясь легитимировать принцип невмешательства (здесь Китай поддерживает Россию)[48]. Таким образом, Россия пытается укрепить цифровой суверенитет не только внутри страны, но и формируя новые нормы международного права в этой сфере.

[41] См.: UNODA. International ICT-security at the United Nations. URL: https://disarmament.unoda.org/ict-security/ (дата обращения: 02.09.2025 г.).

[42] См.: Моржакова М. Суверенитет в Сети: российский путь // Новый проспект, 21.05.2024. URL: https://newprospect.ru/news/articles/suverenitet-v-seti-rossiyskiy-put/ (дата обращения: 01.09.2025 г.).

[43] См.: Счётная палата увидела риски для бюджета из-за закона о суверенном Рунете // РБК. 07.02.2019. URL: https://www.rbc.ru/technology_and_media/07/02/2019/5c5c640a9a7947c571f5abb2 (дата обращения: 02.09.2025 г.); Savelyev A. Russia's New Personal Data Localization Regulations: A Step Forward or a Self-Imposed Sanction? // HSE Working Papers. 2016. URL: https://pravo.hse.ru/data/2017/03/22/1169832328/2015%20Savelyev%20AI%20Russian%20New%20Personal%20Da..ward%20or%20a%20Self-Imposed%20Sanction.pdf (дата обращения: 02.09.2025 г.).

[44] См.: Netflix приостановил работу в России // РБК. 07.03.2022. URL: https://www.rbc.ru/technology_and_media/07/03/2022/62251da49a7947899dd17b63 (дата обращения: 02.09.2025 г.); Spotify уйдет из России из-за закона о фейках // Вести. 25.03.2022. URL: https://www.vesti.ru/article/2694359 (дата обращения: 02.09.2025 г.).

[45] См.: Правительство разрешило операторам не хранить сетевой трафик в условиях дефицита оборудования // Ведомости. 30.03.2022. URL: https://www.vedomosti.ru/technology/news/2022/03/30/915877-pravitelstvo-ne-hranit-trafik (дата обращения: 02.09.2025 г.); Минцифры заявило о росте числа ИТ-специалистов в 2023 г.; ранее Шадаев оценивал отток 2022 г. в 100 тыс. Человек // РБК. 05.04.2024. URL: https://www.rbc.ru/rbcfreenews/660fbd0b9a79478544d69596 (дата обращения: 02.09.2025 г.).

[46] См.: Шахова О.А., Федотова М.Н. Блокировка интернет-ресурсов: судебная и внесудебная практика // Теория и практика государственного управления (НИУ ВШЭ). 2021. URL: https://tis.hse.ru/article/download/13049/13063/ (дата обращения: 02.09.2025 г.); Размытость полномочий при блокировках. Верховный суд меняет практику по прокурорским блокировкам веб-сайтов // Zakon.ru (блог). 13.06.2018. URL: https://zakon.ru/Blogs/verhovnyj_sud_menyaet_praktiku_po_prokurorskim_blokirovkam_veb-sajtov/74078 (дата обращения: 02.09.2025 г.).

[47] См.: Shi-Kupfer, K.; Ohlberg, M. China's Digital Rise: Challenges for Europe (MERICS Papers on China, No. 7). Berlin: MERICS, April 2019. 58 p. URL: https://merics.org/sites/default/files/2020–04/MPOC_No.7_ChinasDigitalRise_web_final_2.pdf? (дата обращения: 02.09.2025 г.); Freedom House. China: Freedom on the Net 2024 Country Report. 2024. URL: https://freedomhouse.org/country/china/freedom-net/2024? (дата обращения: 02.09.2025 г.).

[48] См.: Елена Зиновьева, Бай Яцзе. Практика цифрового суверенитета в России и КНР // Российский совет по международным делам (РСМД)—Аналитическая статья, 29.05.2023.—URL: https://russiancouncil.ru/analytics-and-comments/analytics/praktika-tsifrovogo-suvereniteta-v-rossii-i-knr/ (дата обращения: 01.09.2025 г.).

* Human Rights Watch, Inc. («Защита Прав Человека»), США признана нежелательной организацией на территории Российской Федерации.
* Freedom House, Inc. («Фридом Хаус») (США) признана нежелательной организацией на территории Российской Федерации.

ЗАКЛЮЧЕНИЕ

Правовые основы цифрового суверенитета в РФ к 2025 г. представляют собой разветвленную систему законодательных и стратегических актов, нацеленных на защиту национального цифрового пространства. Анализ показал, что за последнее десятилетие в России сложился комплекс мер: от локализации персональных данных и защиты критической инфраструктуры до создания технической возможности автономной работы российского сегмента интернета. Эти меры подкреплены соответствующими законами (242-ФЗ, 187-ФЗ, 90-ФЗ и др.), подзаконными актами, а также идеологически обоснованы в доктринальных документах (Доктрина информационной безопасности, национальные стратегии развития).

Курс на цифровой суверенитет продиктован объективными вызовами эпохи—ростом киберугроз, необходимостью защищать данные граждан, стремлением обеспечить технологическую независимость. Российская Федерация, обладая значительным научно-техническим потенциалом, стремится не допустить критической зависимости от внешних центров силы в цифровой сфере. В то же время, опыт применения новых норм выявил и ряд острых вопросов. Главный из них—как найти баланс между безопасностью и свободой: между правом государства управлять своим сегментом интернета и правами граждан в этом сегменте. Другой вопрос—эффективность и соразмерность принимаемых мер: оправданы ли экономические и социальные издержки ради гипотетической защиты от редких сценариев внешнего отключения? Дискуссии по этим поводам продолжаются как внутри страны, так и на международном уровне.

В заключение следует отметить, что правовое обеспечение цифрового суверенитета будет и дальше развиваться. По мере появления новых технологий (5G/6G-сетей, интернета вещей, искусственного интеллекта) будут возникать новые зоны для регулирования в интересах национальной юрисдикции. Вероятно усиление требований к иностранным технологическим компаниям, развитие отечественных стандартов и альтернативных глобальным систем (например, собственная система корневых сертификатов, операционные системы, поисковые сервисы). Одновременно Россия, вероятно, продолжит участвовать в формировании международных правил поведения государств в цифровой среде, отстаивая принцип цифрового суверенитета как неотъемлемую часть государственной независимости. Таким образом, эволюция правовых основ цифрового суверенитета РФ будет происходить на стыке внутренних потребностей безопасности и внешних факторов глобальной цифровой политики.

ЛИТЕРАТУРА

1. *Авдийский В.И., Иванов А.В., Царегородцев А.В.* Взаимосвязь цифрового суверенитета и цифрового пространства: новые вызовы и перспективы // Вестник Евразийской науки. 2024. Т. 16, № 3. 19 с. URL: https://esj.today/PDF/21FAVN324.pdf (дата обращения: 02.09.2025 г.).
2. *Зиновьева Е., Бай Я.* Практика цифрового суверенитета в России и КНР // Российский совет по международным делам (РСМД) аналитическая статья, 29.05.2023. URL: https://russiancouncil.ru/analytics-and-comments/analytics/praktika-tsifrovogo-suvereniteta-v-rossii-i-knr/ (дата обращения: 01.09.2025 г.).
3. *Зульфугарзаде Т.Э., Першина Ю.О.* Развитие правового обеспечения цифрового суверенитета современного государства на примере России // Экономика. Право. Общество. 2024. Т. 9, № 3. С. 128–133.
4. *Моржакова М.* Суверенитет в Сети: российский путь // Новый проспект. 21.05.2024. URL: https://newprospect.ru/news/articles/suverenitet-v-seti-rossiyskiy-put/ (дата обращения: 01.09.2025 г.).
5. Практика цифрового суверенитета в России и КНР // Российский совет по международным делам (РСМД) аналитическая статья, 29.05.2023. URL: https://russiancouncil.ru/analytics-and-comments/analytics/praktika-tsifrovogo-suvereniteta-v-rossii-i-knr/ (дата обращения: 01.09.2025 г.).
6. *Савельев А.* Russia's New Personal Data Localization Regulations: A Step Forward or a Self-Imposed Sanction? // HSE Working Papers. 2016. URL: https://pravo.hse.ru/data/2017/03/22/1169832328/2015%20Savelyev%20AI%20Russian%20New%20Personal%20Da..ward%20or%20a%20Self-Imposed%20Sanction.pdf (дата обращения: 01.09.2025 г.).

REFERENCES

1. *Avdiyskiy V.I., Ivanov A.V., Tsaregorodtsev A.V.* Interr elation of digital sovereignty and digital space: new challenges and prospects. *Bulletin of Eurasian Science*. 2024. Vol. 16, No. 3. 19 p. URL: https://esj.today/PDF/21FAVN324.pdf (accessed: 02.09.2025).
2. *Zinovieva E., Bai Ya.* Practice of digital sovereignty in Russia and China. *Russian International Affairs Council (RIAC) analytical article*, 29.05.2023. URL: https://russiancouncil.ru/analytics-and-comments/analytics/praktika-tsifrovogo-suvereniteta-v-rossii-i-knr/ (accessed: 01.09.2025).
3. *Zulfugarzade T.E., Pershina Yu. O.* Development of legal support for digital sovereignty of the modern state using the example of Russia. *Economics. Law. Society.* 2024. Vol. 9, No. 3. Pp. 128–133.
4. *Morzhakova M.* Sovereignty on the Web: the Russian way. *New Prospect*. 21.05.2024. URL: https://newprospect.ru/news/articles/suverenitet-v-seti-rossiyskiy-put/ (accessed: 01.09.2025).
5. Practice of digital sovereignty in Russia and China. *Russian International Affairs Council (RIAC) analytical article*, 29.05.2023. URL: https://russiancouncil.ru/analytics-and-comments/analytics/praktika-tsifrovogo-suvereniteta-v-rossii-i-knr/ (accessed: 01.09.2025).
6. *Savelyev A.* Russia's New Personal Data Localization Regulations: A Step Forward or a Self-Imposed Sanction? *HSE Working Papers*. 2016. URL: https://pravo.hse.ru/data/2017/03/22/1169832328/2015%20Savelyev%20AI%20Russian%20New%20Personal%20Da..ward%20or%20a%20Self-Imposed%20Sanction.pdf (accessed:

щения: 02.09.2025 г.).
7. *Couture S., Toupin S.* What does the notion of «sovereignty» mean when referring to the digital? // New Media & Society. 2019. Vol. 21, No. 10. Pp. 2305–2322. URL: https://journals.sagepub.com/doi/full/10.1177/1461444819865984 (дата обращения: 02.09.2025 г.).
8. *Obradovic D.* Russia's «Sovereign Internet» Law. // Internet Society Internet Fragmentation Insights, 01.12.2023. URL: https://www.internetsociety.org/resources/internet-fragmentation/russias-sovereign-internet-law/ (дата обращения: 01.09.2025 г.).
9. *Stubbs J., Ostroukh A.* Russia to ban Telegram messenger over encryption dispute // Reuters, 13.04.2018. URL: https://www.reuters.com/article/russia-telegram-block-idUSKBN1HK10B (дата обращения: 01.09.2025 г.).
10. *Walker S.* Russia blocks access to LinkedIn over foreign-held data // The Guardian. 17.11.2016. URL: https://www.theguardian.com/world/2016/nov/17/russia-blocks-access-to-linkedin-over-foreign-held-data (дата обращения: 01.09.2025 г.).

02.09.2025).
7. *Couture S., Toupin S.* What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*. 2019. Vol. 21, No. 10. Pp. 2305–2322. URL: https://journals.sagepub.com/doi/full/10.1177/1461444819865984 (accessed: 02.09.2025).
8. *Obradovic D.* Russia's "Sovereign Internet" Law. *Internet Society Internet Fragmentation Insights*, 01.12.2023. URL: https://www.internetsociety.org/resources/internet-fragmentation/russias-sovereign-internet-law/ (accessed: 01.09.2025).
9. *Stubbs J., Ostroukh A.* Russia to ban Telegram messenger over encryption dispute. *Reuters*, 13.04.2018. URL: https://www.reuters.com/article/russia-telegram-block-idUSKBN1HK10B (accessed: 01.09.2025).
10. *Walker S.* Russia blocks access to LinkedIn over foreign-held data. *The Guardian*. 17.11.2016. URL: https://www.theguardian.com/world/2016/nov/17/russia-blocks-access-to-linkedin-over-foreign-held-data (accessed: 01.09.2025).

Рецензент: Северин В.А., д-р юрид. наук, профессор кафедры правовой информатики, информационного и цифрового права юридического факультета. Московский государственный университет имени М.В. Ломоносова, г. Москва, Российская Федерация.

Статья проверена программой «Антиплагиат». Оригинальность текста 94,16%.

Статья поступила в редакцию 06.09.2025, принята к публикации 26.09.2025
The article was received on 06.09.2025, accepted for publication 26.09.2025

СВЕДЕНИЯ ОБ АВТОРЕ

Спартак Сергей Андреевич, канд. полит. наук, доцент кафедры философии языка и коммуникации Философского факультета; Московский государственный университет имени М.В. Ломоносова; г. Москва, Российская Федерация, ORCID: 0009-0007-3494-6127, SPIN-код: 9147-1725, AuthorID: 1273402, e-mail: sspartak@yandex.ru

ABOUT THE AUTHOR

Sergey A. Spartak, Cand. Sci. (Polit.), Associate Professor of the Department of Philosophy of Language and Communication, Faculty of Philosophy; Lomonosov Moscow State University; Moscow, Russian Federation, ORCID: 0009-0007-3494-6127, SPIN-code: 9147-1725, AuthorID: 1273402, e-mail: sspartak@yandex.ru