УДК 004.056.53

ЦИФРОВОЙ СУВЕРЕНИТЕТ ГОСУДАРСТВА И ЗАЩИТА НАЦИОНАЛЬНОГО КИБЕРПРОСТРАНСТВА В РОССИЙСКОЙ ФЕДЕРАЦИИ

Остpик К.С.,

Студент 4 курса направления государственная и муниципальная служба

КФ РАНХиГС

Калуга, Россия

Бобырев Д.Б.,

к.э.н., доцент

КФ РАНХиГС

Калуга, Россия

Аннотация

В данной статье проводится комплексный анализ концепции цифрового суверенитета Российской Федерации и мер по защите национального киберпространства в условиях современных геополитических вызовов и внешних санкций. Рассматриваются ключевые стратегические документы, такие как Доктрина информационной безопасности, а также законодательные инициативы, направленные на обеспечение технологической независимости и безопасности. Особое внимание уделяется практическим аспектам реализации цифрового суверенитета, включая создание национальной системы маршрутизации интернет-трафика, управление критической информационной инфраструктурой (КИИ) и формирование альтернативной отечественной цифровой экосистемы. Делается вывод о том, что предпринимаемые меры направлены на минимизацию внешних рисков, защиту данных граждан и обеспечение устойчивого развития цифровой экономики страны.

Ключевые слова: цифровой суверенитет, киберпространство, информационная безопасность.

DIGITAL SOVEREIGNTY OF THE STATE AND THE PROTECTION OF NATIONAL CYBERSPACE IN THE RUSSIAN FEDERATION

Ostrik K.S.,

4th year student of the direction of state and municipal service

CF RANHiGS

Kaluga, Russia

Bobyrev D.B.

Candidate of Economics, Associate Professor

CF RANHiGS

Kaluga, Russia

Abstract

The article provides a comprehensive analysis of the concept of digital sovereignty in the Russian Federation and the measures taken to protect national cyberspace in the context of modern geopolitical challenges and external sanctions. It examines key strategic documents, such as the Information Security Doctrine, as well as legislative initiatives aimed at ensuring technological independence and security. Particular attention is paid to the practical aspects of implementing digital sovereignty, including the creation of a national internet traffic routing system, the management of critical information infrastructure (CII), and the formation of an alternative domestic digital ecosystem. The conclusion is drawn that the measures taken are aimed at minimizing external risks, protecting citizens' data, and ensuring the sustainable development of the country's digital economy.

Keywords: digital sovereignty, cyberspace, information security, Information Security Doctrine, sovereign internet, critical information infrastructure (CII), cybersecurity, geopolitical challenges, Russian digital ecosystems, IT legislation.

Данная статья актуальна, так как в условиях стремительно развивающегося цифрового мира концепция цифрового суверенитета становится все более актуальной для государств, стремящихся защитить свои интересы в киберпространстве. Цифровой суверенитет подразумевает способность государства контролировать и управлять своим цифровым пространством, обеспечивая безопасность данных и информационных систем, а также защищая национальные интересы от внешних угроз. В последние годы, особенно на фоне геополитической напряженности и введения экономических санкций, Россия активно разрабатывает и внедряет меры, направленные на укрепление своего цифрового суверенитета.

Цифровой суверенитет представляет собой концепцию, основанную на принципе, что государство должно контролировать и защищать свою цифровую инфраструктуру, включая персональные данные граждан и киберпространство от внешних вмешательств и угроз. В условиях быстро развивающегося цифрового мира это понятие стало особенно актуальным для России, учитывая сложные вызовы, с которыми сталкивается страна на международной арене. Формирование цифрового суверенитета в России началось в начале 2000-х годов с принятия основных стратегических документов, таких как Доктрина информационной безопасности. Этот документ определил ряд приоритетов, включая развитие национальных систем и технологий, способствующих снижению зависимости от иностранных решений и продуктов [1].

Согласно данным, в последние несколько лет значение цифрового суверенитета в России возросло в ответ на санкционное давление и уход из

страны иностранных IT-компаний. Правительственные инициативы нацелены на создание условий для поддержки и развития отечественных технологий, а также укрепления кибербезопасности. Глава Минцифры РФ Максут Шадаев подчеркивает, что «цифровой суверенитет является защитой интересов граждан и национальной инфраструктуры в современных условиях» [2].

Становится очевидным, что текущие международные тенденции и вызовы требуют адаптации концепции цифрового суверенитета. О важности технологической независимости, как основы этого суверенитета, неоднократно говорил Президент РФ Владимир Путин: «Суверенитет немыслим без технологической независимости». В армии новейших угроз, включая киберугрозы и экономический шантаж, необходимо не только защищать существующие системы, но и развивать новые, создавая аналогичные отечественные решения, которые обеспечат технологическую независимость России. Это позволяет обойти последствия, которые могут возникнуть в случае отключения от международных точек обмена трафиком [3].

Актуальность концепции цифрового суверенитета в условиях глобальных угроз очевидна, поскольку она определяет не только безопасность информации, но и устойчивость всего государственного механизма в цифровую эпоху. Таким образом, создание системы национальной безопасности в киберпространстве становится приоритетной задачей в новых реалиях безопасности [4].

Сегодня человечество вступило в новый этап развития, где технологии позволяют нам решать такие задачи, о которых наши предки только мечтали. Однако в эпоху технологий рынок как таковой перестал осуществлять свою задачу регулятора, тогда как потребители в основном начали определять его состав.

В 2025 году Россия сталкивается с множеством геополитических вызовов, которые непосредственно влияют на формирование концепции цифрового суверенитета. Специальная военная операция на Украине, нестабильность в

постсоветском пространстве и нарастающее санкционное давление со стороны Запада становятся основными факторами, определяющими внутренние стратегии государства. Политолог Денис Денисов подчеркивает, что несмотря на давление, внутренняя политическая стабильность сохраняется и конфликт в Украине демонстрирует признаки стабилизации [5].

Экономическая ситуация в стране, наоборот, показывает тенденцию к росту — на фоне мировых экономических трудностей, связанных с повышенной геополитической напряженностью, Россия сумела не только удержать свои позиции, но и продемонстрировать лучшие результаты по темпам роста экономики по сравнению с другими странами [6]. Это становится возможным в том числе благодаря адаптации к новым условиям и поиску альтернативных источников развития, что активно поддерживается государством.

Осознание роли информационной и кибербезопасности выходит за рамки пассивного соблюдения существующих нормативов: государство акцентирует внимание на формировании проактивных подходов к цифровой защите, основанных на собственных технологических возможностях. В этом контексте геополитические вызовы и санкционное давление выступают как ускоряющие факторы трансформации, способствующие укреплению цифрового суверенитета и созданию благоприятных условий для устойчивого национального развития в информационно-технологической сфере.

Принятие новой Доктрины информационной безопасности Российской Федерации в 2019 году стало важным этапом в формировании основ цифрового суверенитета. Основные цели и задачи Доктрины сосредоточены на обеспечении комплексной защиты информации и информационных систем, а также на развитии отечественных технологий и систем управления информацией [7].

Доктрина указывает, что информационная безопасность охватывает не только защиту от внешних угроз, но и необходимость создания внутренней инфраструктуры, отвечающей современным вызовам. Формулирование

конкретных взглядов в области информационной безопасности позволяет не только отразить текущее состояние, но и предугадать возможные изменения в этой сфере.

Одной из задач, обозначенных в Доктрине, является развитие правовой базы и координация усилий различных государственных структур, предприятий и организаций, участвующих в обеспечении информационной безопасности. Это необходимо для формирования единой системы, которая учитывает интересы всех участников процесса [8].

Важно отметить, что национальными интересами в информационной сфере являются:

а) обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;

б) обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время;

в) развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной

безопасности, оказанию услуг в области обеспечения информационной безопасности.

Кроме того, осуществление мероприятий, предусмотренных Доктриной, направлено на создание и внедрение отечественных решений в области информационных технологий и систем. Это не только способствует повышению уровня безопасности, но и ведет к снижению зависимости от зарубежных технологий. При этом акцент ставится на важность разработки и поддержки инновационных решений, что делает страну более устойчивой к внешним рискам [9].

В последние годы Российская Федерация активно формирует нормативно-правовую базу, направленную на обеспечение безопасности национального киберпространства, что представляет собой ключевой элемент стратегии цифрового суверенитета. Существенным шагом в данном направлении стало издание Указа Президента Российской Федерации от 1 мая 2022 года № 250, предусматривающего введение дополнительных мер по обеспечению информационной безопасности. Документ возлагает на ответственные органы обязанность по оперативному реагированию на возникающие киберугрозы и реализации комплекса организационных и технических мероприятий, направленных на минимизацию рисков.

Федеральный закон от 4 ноября 2025 года № 404-ФЗ внёс коррективы в Кодекс Российской Федерации об административных правонарушениях, усилив ответственность за несоблюдение требований в сфере информационной безопасности. Принятие данного законодательного акта подчеркивает возросшее внимание государства к юридическому обеспечению защиты информации, в том числе в контексте утечки данных и обеспечения конфиденциальности.

Ключевую роль в формировании правового регулирования в информационно-коммуникационной сфере продолжает играть Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных

технологиях и о защите информации». Он охватывает широкий спектр вопросов – от терминологического аппарата до установления требований по защите информации и прав субъектов в цифровой среде, служа основой для регулирования процессов в области кибербезопасности.

Дополнительные нормативные положения, разрабатываемые и утверждаемые Федеральной службой безопасности Российской Федерации, направлены на обеспечение защиты персональных и конфиденциальных данных. Эти меры включают технические и организационные требования к безопасности информационных систем общего пользования, способствуя созданию условий для безопасного функционирования цифровой инфраструктуры государства и обеспечения информационной защищённости граждан [10].

Создание национальной системы маршрутизации интернет-трафика в России стало необходимым и важным шагом в обеспечении цифрового суверенитета. Эта система, направлена на защиту российского интернета от внешних угроз и обеспечения его устойчивости в случае сбоев. Основное внимание уделяется координации работы через Роскомнадзор, который берёт на себя функции по регулированию маршрутизации трафика и предотвращению потенциальных кибератак [11].

Главная задача новой сети заключается в создании устойчивой инфраструктуры, что предполагает структурирование всех звеньев коммуникационной системы в России. Это включает в себя создание точек обмена трафиком и определение номеров автономных систем. Подобная организация маршрутов не только защитит от внешних воздействий, но и предоставит возможность наряду с традиционными средствами фильтрации трафика реализовать технические средства противодействия угрозам (ТСПУ) [12].

Данные изменения должны привести к улучшению управления интернет-пространством внутри страны. Необходимо обеспечить возможность

доступности российских интернет-ресурсов даже при отключении от международных корневых DNS-серверов, что критически важно для защиты информации и соблюдения государственно-контрольного надзора в аффилированной сети [13].

6. Создание альтернативной цифровой экосистемы

Российская цифровая экосистема характеризуется динамичным развитием, направленным на формирование полноценных альтернатив западным цифровым платформам и услугам. По состоянию на 2025 год ведущими участниками данного сегмента остаются такие компании, как «Сбер», «Яндекс», VK, МТС и Т-Банк. Их экосистемы охватывают широкий спектр отраслей — от транспортных и финансовых услуг до образовательных и медийных платформ.

Параллельно с крупными игроками на рынке начинают формироваться новые экосистемные структуры, среди которых можно выделить «Инго», «Авито» и Ozon. Эти проекты сосредоточены преимущественно на предоставлении финансовых и торговых сервисов, демонстрируя потенциал для дальнейшего расширения.

Следует отметить снижающиеся темпы запуска новых цифровых сервисов в последние годы: если в 2022 году было запущено 37 новых продуктов, то в 2023 данный показатель составил 36, а в 2024 — снизился до 31. Такая динамика обусловлена необходимостью адаптации к изменяющемуся потребительскому спросу и влиянию внешнеэкономических факторов, включая санкционное давление и ограниченность ресурсной базы. В условиях нарастающей турбулентности крупные корпорации, такие как «Сбер» и «Яндекс», продолжают курс устойчивого развития, тогда как другие участники — VK и МТС — демонстрируют либо замедление инновационной активности, либо свёртывание отдельных проектов вследствие их низкой рентабельности.

Ключевыми направлениями для дальнейшего развития отечественных цифровых экосистем становятся внедрение технологий искусственного

интеллекта, развитие облачных решений и инфраструктур, а также активная диверсификация продуктового портфеля. Эти процессы отражают стремление к формированию устойчивых, конкурентоспособных цифровых решений, способных эффективно функционировать в условиях внешних технологических и политико-экономических вызовов.

Российская цифровая экосистема переживает этап формирования, и хотя она еще не достигла значительного воздействия на макроэкономику, успешные примеры таких сервисов, как RUSSPASS, свидетельствуют о потенциале.

Перспективы развития цифровых платформ в России на горизонте 3–5 лет (до 2030 гг.) будут определяться несколькими ключевыми факторами — государственной политикой, государственной поддержкой, технологическим суверенитетом, цифровизацией экономики, а также неизбежной трансформацией бизнес-моделей. С учетом принятого политического курса, действующего законодательства, с большой долей вероятности можно утверждать, что в ближайшие несколько лет Россия будет двигаться к дальнейшей цифровой изоляции. Что в совокупности с невозможностью возвращения на национальный рынок крупнейших западноевропейских игроков создаст дополнительные стимулы для активного развития российских цифровых платформ. Это коснется как технологий (ИИ, большие данные, блокчейн, IoT и т.д.) так и так и различных отраслей экономики. При этом ключевыми двигателями изменений останутся государство и крупный бизнес.

Концепция цифрового суверенитета России в условиях современных вызовов представляет собой многогранный и динамичный процесс, требующий комплексного подхода и взаимодействия различных государственных и частных структур. Важно понимать, чтобы все меры, принимаемые в этой области, были направлены на защиту интересов государства и его граждан, а также на создание безопасного и эффективного цифрового пространства. В условиях глобализации и быстрого развития технологий, защита национального киберпространства

становится не только вопросом безопасности, но и важным фактором экономического и социального развития страны.

Библиографический список

1. Доктрина информационной безопасности Российской Федерации : утв. Указом Президента Рос. Федерации от 5 дек. 2016 г. № 646 // Рос. газ. – 2016. – 6 дек. – URL: https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 12.12.2025).
2. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» (в ред. от 13.06.2024) // Собр. законодательства Рос. Федерации. – 2022. – № 18. – Ст. 3060. – URL: https://www.consultant.ru/document/cons_doc_LAW_416198/(дата обращения: 12.12.2025).
3. Федеральный закон от 01.05.2019 № 90-ФЗ «О внесении изменений в Федеральный закон “О связи” и Федеральный закон “Об информации, информационных технологиях и о защите информации”» // Собр. законодательства Рос. Федерации. – 2019. – № 18. – Ст. 2213. – URL: https://www.consultant.ru/document/cons_doc_LAW_323815/ (дата обращения: 12.12.2025).
4. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (в действ. ред.) // Собр. законодательства Рос. Федерации. – 2006. – № 31 (ч. 1). – Ст. 3448. – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 12.12.2025).
5. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (в действ. ред.) // Собр. законодательства Рос. Федерации. – 2017. – № 31 (ч. 1). – Ст. 4736. – URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 12.12.2025).
6. Шадаев М. И. Цифровой суверенитет – защита пользователей и интересов государства : интервью // Рос. газ. – 2025. – 22 мая. – URL: https://rg.ru/2025/05/22/shadaev-cifrovoj-suverenitet-zashchita-polzovatelej-i-interesov-gosudarstva.html (дата обращения: 12.12.2025).
7. Путин В. В. Послание Президента Российской Федерации Федеральному Собранию : 29 февр. 2024 г. // Президент России : офиц. сайт. – URL: http://www.kremlin.ru/events/president/news/73585 (дата обращения: 12.12.2025).

8. Исследование: крупнейшие российские цифровые экосистемы 2024-2025 // Spektr.team. – 2025. – URL: http://spektr.team/tpost/g8cbrog5l1-issledovanie-krupneishie-rossiiskie-tsif (дата обращения: 12.12.2025).
9. Цифровые экосистемы в России // TAdviser. – 2025. – URL: https://www.tadviser.ru/index.php/Статья:Цифровые_экосистемы_в_России (дата обращения: 12.12.2025).
10. Подходы к пониманию цифрового суверенитета России / П. В. Степанов // Журнал российского права. – 2024. – № 4. – С. 45–58.
11. Закон о «суверенном Рунете»: ответы на главные вопросы // Гос. Дума Федер. Собр. Рос. Федерации : офиц. сайт. – URL: http://duma.gov.ru/news/51194/ (дата обращения: 12.12.2025).
12. Практика цифрового суверенитета в России и КНР // Рос. совет по междунар. делам (РСМД). – URL: https://russiancouncil.ru/analytics-and-comments/analytics/praktika-tsifrovogo-suvereniteta-v-rossii-i-knr/ (дата обращения: 12.12.2025).