Научная статья
УДК 330.356
https://doi.org/10.17586/2713-1874-2025-4-30-40

РОЛЬ ЦИФРОВОГО СУВЕРЕНИТЕТА В ОБЕСПЕЧЕНИИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИИ В УСЛОВИЯХ ГЕОПОЛИТИЧЕСКОЙ НЕСТАБИЛЬНОСТИ

Ольга Владимировна Мамателашвили[1], Радмир Разитович Байбурин[2]✉

[1,2]Уфимский государственный нефтяной технический университет, г. Уфа, Россия
[1]mar3169@yandex.ru, https://orcid.org/0000-0002-7150-8237
[2]radmir.bajburin@mail.ru✉, https://orcid.org/0000-0001-2878-6821
Язык статьи – русский

Аннотация: В статье рассмотрена и проанализирована роль цифрового суверенитета в обеспечении экономической безопасности России в условиях геополитической нестабильности. Актуальность исследования обусловлена тем, что стремительный процесс цифровизации охватывает все сферы общественной жизни, из-за чего ключевым условием устойчивого развития становится обеспечение способности страны самостоятельно формировать и реализовывать политику в цифровом пространстве. Целью исследования является теоретико-аналитическое обоснование значимости цифрового суверенитета в качестве ключевого фактора, определяющего устойчивость экономической безопасности Российской Федерации. В качестве методологической базы использованы положения современной теории цифровой экономики, научные подходы к национальной безопасности, концепции суверенитета в условиях трансформирующегося глобального цифрового пространства. В содержании работы раскрывается сущностное содержание понятия «цифровой суверенитет», исследуются его структурные компоненты – технологическая независимость, контроль над данными, регуляторная автономия и сетевая инфраструктура, в контексте их влияния на экономическую безопасность. Особое внимание в работе уделяется правовым аспектам цифрового суверенитета. Сделан вывод о том, что Россия реализует стратегически обоснованный курс на укрепление суверенитета, который постепенно трансформируется в ключевой элемент политико-экономической субъектности государства. Актуальны перспективные направления дальнейших исследований, связанные с разработкой количественных индикаторов цифрового суверенитета и оценкой их влияния на макроэкономическую стабильность.

Ключевые слова: геополитическая нестабильность, глобальная цифровая трансформация, цифровизация, цифровой суверенитет, экономическая безопасность

Ссылка для цитирования: Мамателашвили О. В., Байбурин Р. Р. Роль цифрового суверенитета в обеспечении экономической безопасности России в условиях геополитической нестабильности // Экономика. Право. Инновации. – 2025. – Т. 13. – № 4. – С. 30–40. – https://doi.org/10.17586/2713-1874-2025-4-30-40

THE ROLE OF DIGITAL SOVEREIGNTY IN ENSURING RUSSIA'S ECONOMIC SECURITY IN THE CONTEXT OF GEOPOLITICAL INSTABILITY

Olga V. Mamatelashvili[1], Radmir R. Bayburin[2]✉

[1,2]Ufa State Petroleum Technological University, Ufa, Russia
[1]mar3169@yandex.ru, https://orcid.org/0000-0002-7150-8237
[2]radmir.bajburin@mail.ru✉, https://orcid.org/0000-0001-2878-6821
Article in Russian

Abstract: The article examines and analyses the role of digital sovereignty in ensuring Russia's economic security in conditions of geopolitical instability. This is due to the fact that the rapid process of digitalization is affecting all spheres of public life, making it essential for sustainable development that the country is able to independently formulate and implement policy in the digital space. The aim of the study is to provide a theoretical and analytical justification for the importance of digital sovereignty as a key factor determining the sustainability of the Russian Federation's economic security in such conditions. The methodological basis is provided by the provisions of modern digital economy theory, scientific approaches to national security, and concepts of sovereignty in the context of a transforming global digital space. The content of the work reveals the essential meaning of the concept of «digital sovereignty» and examines its

structural components – technological independence, data control, regulatory autonomy, and network infrastructure – in the context of their impact on economic security. Particular attention is paid to the legal aspects of digital sovereignty. Based on the results of the study, it is concluded that Russia is implementing a strategically sound course to strengthen sovereignty, which is gradually transforming into a key element of the state's political and economic subjectivity. Promising areas for further research related to the development of quantitative indicators of digital sovereignty and the assessment of their impact on macroeconomic stability are relevant.

Keywords: geopolitical instability, global digital transformation, digitalization, digital sovereignty, economic security

For citation: Mamatelashvili O. V., Bayburin R. R. The Role of Digital Sovereignty in Ensuring Russia's Economic Security in The Context of Geopolitical Instability. *Ekonomika. Pravo. Innovacii*. 2025. Vol. 13. No. 4. pp. 30–40. (In Russ.). https://doi.org/10.17586/2713-1874-2025-4-30-40.

Введение. В условиях глобальной цифровой трансформации, характеризующейся экспоненциальным ростом объемов данных, всепроникающим распространением информационно-коммуникационных технологий и углубляющейся взаимозависимостью национальных экономик, проблемы обеспечения экономической безопасности приобретает качественно новые измерения. В этот период традиционные инструменты и механизмы обеспечения устойчивости оказываются недостаточными. В этой связи зародилась новейшая концепция цифрового суверенитета, приобретающая важное значение для любой страны мира.

С точки зрения теории безопасности, цифровой суверенитет выполняет превентивную функцию по предотвращению угроз, исходящих из трансграничной технологической зависимости и манипулятивных практик со стороны глобальных цифровых акторов (транснациональных корпораций и иностранных государств) [1, С. 33]. По той же концепции схематическое представление цифрового суверенитета государства отображено на рисунке 1.

Рисунок 1 – Схематическое представление цифрового суверенитета государства
Источник: составлено авторами

Технологическая независимость – это экосистема, которая должна быть способна к устойчивому воспроизведению технологических решений. Отсутствие автономии неизбежно ведет к формированию «цифровой зависимости», при которой ключевые узлы инфраструктуры находятся под внешним контролем. Такая зависимость снижает управляемость цифровизацией через физическое отключение инфраструктурных компонентов (как, например, санкционные механизмы) и, как следствие, ослабляется экономическая субъектность на международной арене. Контроль над данными в этом случае представляет собой стратегическую функцию государства. В этом контексте данные – особый нематериальный актив, обладающий высокой ценностью, утечка которых ведет к утрате управления в реальном секторе экономики из-за способности внешних субъектов формировать искаженные сценарии внутри государства. Вслед за контролем данных важна регуляторная автономия – фундаментальное условие правового обеспечения суверенитета. Она охватывает не только формальную нормотворческую деятельность, но и способность государства участвовать в международном правовом дискурсе на равных основаниях.

Сетевая инфраструктура – материальный каркас суверенитета, обеспечивающий физическую реализацию процессов передачи и хранения информации. В эту категорию

входит трафик, оптоволоконные линии связи, дата-центры, маршрутизаторы и многие другие продукты цифровизации. В условиях геополитической напряженности доступ к инфраструктурным мощностям может быть ограничен в любой момент, что потенциально приведет к цифровому параличу экономики. Чем больше собственных инфраструктурных ресурсов в государстве, тем выше вероятность формирования эффективной политики развития исходя из внутренних приоритетов.

Исследовательская проблема. Хотя представленная интегральная модель российского цифрового суверенитета и рассматривается как стратегическая парадигма, важно обозначить важность понятия в контексте современных реалий.

Гипотеза исследования состоит в том, что реализация стратегии цифрового суверенитета Российской Федерации является критически важным фактором обеспечения экономической безопасности государства в условиях нарастающей геополитической нестабильности. Предполагается, что усиление цифрового суверенитета способствует повышению устойчивости национальной экономики к внешним санкционным и другим воздействиям.

Целью исследования является теоретико-аналитическое обоснование роли цифрового суверенитета как системообразующего фактора обеспечения экономической безопасности России в условиях геополитической нестабильности.

Для выполнения поставленной цели необходимо решить ряд следующих **задач**.

1) Раскрыть сущностное содержание понятия «цифровой суверенитет» в контексте современной цифровой экономики и теории экономической безопасности государства.

2) Провести анализ структурных компонентов суверенитета.

3) Обосновать необходимость интеграции цифрового суверенитета в систему обеспечения экономической безопасности как элемента государственной цифровой политики.

Обзор литературы. В современных научных исследованиях наблюдается устойчивый рост интереса к проблематике цифрового суверенитета, что обусловлено ускоряющейся цифровизацией экономики, изменением конфигурации глобального цифрового пространства. Проанализировав множество определений понятия «цифровой суверенитет», в самом общем виде его можно представить как «…способность государства самостоятельно формировать и реализовывать политику в цифровом пространстве, включая контроль над цифровой инфраструктурой, данными, программным обеспечением (ПО) и сетями связи» [2]. Однако с точки зрения концептуального анализа, цифровой суверенитет следует рассматривать как часть более широкого феномена государственного суверенитета, адаптированного к реалиям цифровой эпохи. Если традиционное понятие предполагает контроль над территорией, населением и ресурсами в пределах национальных границ, то в новое время к ним добавляется необходимость контроля над виртуальной средой, в которой функционируют не только государственные институты, но повседневная жизнь граждан, коммерческие трансакции и принятие управленческих решений.

В ряде работ подчеркивается, что цифровой суверенитет становится неотъемлемой составляющей государственной суверенности в XXI веке, особенно в условиях обострения геополитической конкуренции. Так, в исследовании Кубанцевой Е. В. акцент сделан на угрозах цифровой зависимости, включая доминирование иностранных платформ, киберугрозы, что напрямую ставит под угрозу экономическую безопасность страны [3, С. 47]. В данном контексте актуализируется необходимость формирования национальных цифровых экосистем, способных функционировать автономно от внешних технологических центров влияния.

Также в научной литературе уделяется внимание вопросам институционального обеспечения цифрового суверенитета. В частности, в работе [4] подчеркивается необходимость интеграции усилий государства и частного сектора в разработке и внедрении отечественных цифровых решений. Анализируется роль цифровых платформ как инфраструктурных основ суверенитета, а также оценивается степень их независимости от зарубежных компонентов.

Часто связь между цифровым суверенитетом и экономической безопасностью

рассматривается в двух основных плоскостях. Первая – защитная: контроль над критической цифровой инфраструктурой рассматри- вается как средство предотвращения внешних шоков и информационного влияния, которые в нынешних условиях могут иметь прямые экономические последствия (как, например, разрыв логистики, утечка коммерческой тайны, паралич финансовых секторов). Вторая – стратегическая: политика цифрового суверенитета рассматривается как инструмент смягчения экономических последствий международных санкций посредством ограничения внешней зависимости в ключевых технологических звеньях. Лишь при грамотной реализации цифровой автономии снижается уязвимость экономики к внешним ограничениям [5].

Выделяют две точки зрения на определение цифрового суверенитета. Одна трактует его как необходимый элемент национальной безопасности – акцент делается на стимулировании импортозамещения, развитии национальных платформ, укреплении регуляторной автономии. Другая критически оценивает риски чрезмерной изоляции: снижение эффективности конкуренции, торможение инноваций, потенциальная трансформация суверенитета в инструмент репрессивного государственного контроля над информацией. Эта дихотомия прослеживается как в российских публикациях, так и в зарубежных исследованиях, где сравниваются практики «суверенизации» интернета в разных государствах и подчеркивается многообразие моделей (от более открытых к более закрытым) [1].

Эмпирические исследования последних лет дают неоднозначную картину эффективности мер цифрового суверенитета. Работы, анализирующие последствия закона о локализации и связанные с ним регуляторные новации, отмечают положительный эффект на формирование внутреннего рынка дата-центров, но указывают и на теневые издержки: усложнение трансграничных операций, рост трансакционных издержек, ухудшение условий для иностранных инвестиций в цифровую экономику. Анализ воздействия технологических санкций после 2022 года показывает, что меры по созданию отечественных заменителей (локальные операционные системы, российские апп-сторы, программы импортозамещения аппаратного обеспечения) частично компенсируют отсутствие поставок, но часто сталкиваются с проблемами масштабирования, качества и, самое главное, экономической целесообразности [6]

Тема статьи актуальна и тем, что с 2019 года, с принятием закона о «суверенном Интернете», Россия начала формировать правовую базу для централизованного управления Интернетом в государственных границах. Стратегия национальной безопасности Российской Федерации отражает стремление адаптировать и развивать модель с акцентом на безопасность.

Таким образом, обзор современной научной литературы показывает, что цифровой суверенитет рассматривается как ключевой фактор обеспечения экономической безопасности, при этом акцент смещается от абстрактных теоретических суждений к прикладным аспектам реализации соответствующей политики.

Материалы и методы исследования. В статье использованы научные методы анализа, синтеза и логического обобщения. В частности, применен комплексный методологический подход, сочетающий междисциплинарные теоретические и эмпирические методы анализа. Методологическую основу работы составляют положения современной теории цифровой экономики, теории национальной и экономической безопасности, а также концепции суверенитета в условиях трансформации глобального цифрового пространства.

Эмпирический анализ направлен на выявление текущего состояния и динамики формирования цифрового суверенитета РФ. На первом этапе осуществлялся сбор и систематизация фактических данных из открытых источников (официальные отчеты Роскомнадзора, Strategy Partners, Infowatch; нормативно-правовые акты (Федеральные законы № 90-ФЗ, № 236-ФЗ, № 242-ФЗ и др.); аналитические материалы отраслевых исследовательских центров, таких как ИТ-холдинг Fplus).

На втором этапе были отобраны ключевые количественные индикаторы, отражающие степень реализации основных структурных компонентов цифрового суверенитета. В частности, для оценки использовались следу-

ющие индикаторы: рост рынка корпоративного ПО в России в 2023 и 2030 гг. (в млрд руб.), объем и структура российского IT-рынка до 2030 г. (в млрд руб.), число утечек информации и число утекших персональных данных в России за 2020–2024 гг. (в млн), утечки персональных данных по отраслям за 2023–2024 гг., (в %). На третьем этапе проводилась обработка и интерпретация полученных данных, которые сопоставлены с теоретической моделью цифрового суверенитета (рисунок 1), что позволило оценить степень ее реализации на практике.

Результаты исследования. Как было показано ранее, цифровой суверенитет выступает одним из ключевых детерминантов экономической безопасности государства, особенно в условиях нарастающей геополитической нестабильности. В Российской Федерации данный феномен приобретает не только технологическое измерение, но и становится политико-экономическим феноменом, тесно связанным с устойчивостью национального развития.

Прежде всего следует подчеркнуть, что в условиях геополитической конфронтации и растущей цифровой зависимости от зарубежных платформ, суверенитет трансформируется из факультативной составляющей цифровой политики в императивное условие функционирования ключевых секторов экономики – энергетики, финансов, логистики, промышленности [7]. Следовательно, представленная ранее интегральная модель с четырьмя базовыми элементами демонстрирует внутреннюю взаимосвязь между элементами и их кумулятивное влияние на уровень защищенности цифровой экосистемы страны. Для получения общей картины необходимо провести анализ каждого из 4-х компонентов.

По данным IT-холдинга Fplus, соотношение отечественных серверов к зарубежным в корпоративном канале в 2024 году составило 75% на 25%, а доля российской продукции (объем которой в 2024 году составил 100–110 млрд рублей), выросла на четверть [8]. Как утверждают некоторые авторы, ставку на производство отечественных серверов было решено сделать в интересах национальной безопасности [9]. Так, делая заказ российских серверов со связанным отечественным ПО, компании приобретали иммунитет к уходу иностранных вендоров, внедряли актуальные меры защиты от кибератак и быстрее реагировали на угрозы.

В целом, переход к преимущественному использованию отечественного аппаратного обеспечения явился ответной мерой на санкционное давление, что следует из проекта Федерального закона «О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» [10, п. 8]. Такая переориентация технологической инфраструктуры позволяет устранить риски технологического саботажа, внедрения скрытых уязвимостей, а также усилить возможности для локальной адаптации решений под национальные стандарты кибербезопасности. Дополнительным положительным эффектом является рост компетенций внутри страны: развитие отечественного производства серверов сопряжено с расширением научно-исследовательских центров и подготовкой квалифицированных инженеров. Это соответствует логике формирования инновационно-ориентированной модели экономики, к которой стремятся крупнейшие страны мира, включая Российскую Федерацию.

Согласно базовому прогнозу Strategy Partners [11], в течение ближайших пяти лет рынок корпоративного ПО в России будет расти в среднем (CAGR) на 24% в год и в 2030 году составит 727 млрд рублей. Рассмотрим прогнозные значения объема рынка в 2023 и 2030 годах с привязкой к сегменту рынка (рисунок 2).

Согласно этому же источнику, прогнозируется рост IT-рынка до 2030 года с темпами 8–13%, а сегмент ПО и услуг в 2030 году достигнет уровня в 2,8 трлн рублей в базовом сценарии (рисунок 3).

Таким образом, резкое увеличение доли российских серверов на корпоративном рынке в 2024 году и прогнозные значения исследовательских центров представляют собой не локальную тенденцию, а начало устойчивого курса на технологическую суверенизацию. На взгляд авторов, в дальнейшем критически важным направлением должно стать углубление производственной локализации.

Рисунок 2 – Рост рынка корпоративного ПО в России, 2023 и 2030 гг., млрд руб.
Источник: составлено авторами на основе данных [12]

Рисунок 3 – Объем и структура российского IT-рынка до 2030 г., млрд руб.
Источник: составлено авторами на основе данных [12]

Следующее ключевое значение в системе обеспечения цифрового суверенитета – контроль над данными. Несмотря на действующее правовое регулирование в России, направленное на локализацию персональных данных, прежде всего Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-коммуникационных сетях» от 21.07.2014 № 242-ФЗ [12], обязывающий операторов обеспечивать хранение и обработку персональных данных исключительно на территории Российской Федерации, на практике сохраняются значительные затруднения в обеспечении реального юрисдикционного контроля над цифровыми потоками. Так, материалы Роскомнадзора за 2024 год указывают на то, что трансграничные потоки данных продолжают функционировать как в рамках формальных исключений, так и посредством технических обходов, включая маршрутизацию через зарубежные облачные сервисы и CDN-сети [13]. С 1 марта по июнь 2023 года в его адрес поступило 733 уведомления о намерении осуществлять такую передачу, из-за чего Роскомнадзором было принято три решения о запрещении трансграничной передачи и шесть решений об ограничении.

На отрицательную тенденцию контроля данных указывает и число утечек персональных данных граждан Российской Федерации за последние годы. К сведению: объемы утекших данных оцениваются только как количество записей и применяются только к персональным данным, платежной информации. Объемы утечек других видов данных не учитываются из-за отсутствия сведений (рисунок 4).

Рисунок 4 – Число утечек информации и число утекших персональных данных в России, 2020–2024 гг., млн.

Источник: составлено авторами на основе данных [14]

Как видно из рисунка 4, в 2023 году зафиксировано 786 случаев против 778 в 2024 году. Чаще всего утекают данные отраслей торговли, телекоммуникаций и государственных служб (рисунок 5).

Как было отмечено, энергетика, финансы, логистика и промышленность являются отраслями, утечка данных в которых наиболее сильно способна оказать влияние на цифровой суверенитет страны. Однако в первую тройку входит утечка данных государственных учреждений, что также говорит о недостаточности действующих механизмов регулирования. В этом контексте необходимо наращивать государственные инвестиции в отечественные решения по управлению данными и развивать международное сотрудничество с дружественными юрисдикциями в части трансграничного обмена данными при соблюдении принципов взаимного цифрового уважения.

Рисунок 5 – Утечки персональных данных по отраслям, 2023–2024 гг., %

Источник: составлено авторами на основе данных [14]

С рядом системных вызовов сталкивается и цифровая регуляторная автономия. В России действует Федеральный закон № 236-ФЗ от 1 июля 2021 года о «приземлении» иностранных ИТ-компаний, обязывающий зарубежные цифровые платформы, чья деятельность направлена на российских пользователей, создавать официальные представительства на территории страны [15]. Однако практика реализации данных норм демонстрирует значительное расхождение между регулированием и фактическим исполнением. Как заявил председатель правления РОЦИТ Антон Горелкин, требования закона «о приземлении» сейчас выполняют многие зарубежные ИТ-компании, но ряд иностранных хостинг-провайдеров их демонстративно игнорирует [16]. Феномен частичной или декларативной имплементации свидетельствует о наличии институциональных барьеров, связанных с экстерриториальностью цифровых услуг и доминирующем положением глобальных BigTech-компаний. Компании, обладающие существенными рыночными преимуществами (Apple, Goggle), в ряде случаев предпочитают игнорировать требования локального законодательства или формально соответствовать им, минимизируя фактическое подчинение российской юрисдикции. В остальном российское правительство старается адаптировать существующее законодательство под цифровые реалии.

Важнейшей компонентой модели цифрового суверенитета является сетевая инфраструктура, к которой относятся центры обработки данных (ЦОД), точки обмена интернет-трафиком, кабельные системы, маршрутизаторы и каналы сетевого взаимодействия. В ответ на ограничения в доступе к зарубежным технологическим решениям, Россия предприняла комплексные меры по ускоренной локализации сетевой инфраструктуры. В частности, был инициирован ряд национальных проектов, направленных на развертывание региональных и федеральных ЦОДов, развитие отечественных маршрутизаторов и коммутаторов, а также создание устойчивых каналов связи, не зависящих от инфраструктуры недружественных государств. В 2023–2024 годах в эксплуатацию было введено рекордное количество стойко-мест в коммерческих ЦОДах: темпы запусков составили 10 тыс. стойко-мест в год. При этом из 22,4 тыс. стоек, запущенных годом ранее, более 13 тыс. были построены девелоперскими компаниями, которые ранее не занимались подобным бизнесом ввиду технологической сложности [17]. Однако несмотря на достигнутый процесс, степень критической импортозависимости в данной сфере остается значительной и превышает допустимые пороговые значения. Так, в 2024 году более 78% рынка сетевых коммутаторов в России составляет продукция зарубежных производителей [18].

Дополнительную угрозу представляет географическая и логистическая конфигурация глобальных каналов связи, особенно подводных магистралей, значительная часть которых контролируется консорциумами, аффилированными участниками санкционных режимов. Подобные зависимости могут быть использованы как инструмент давления, в том числе посредством временной изоляции от мирового интернета, как ранее практиковалось в отношении отдельных государств (Иран, Северная Корея). В целях снижения этих рисков Россия активизировала создание независимого национального сегмента интернета (Рунета) в рамках реализации Федерального закона № 90-ФЗ от 01.05.2019 г. «О внесении изменений в Федеральный закон «О связи» и Федерального закона «Об информации, информационных технологиях и о защите информации» [19]. Согласно его положению, разрабатываются отечественные DNS-серверы и маршрутизирующее ПО, создаются защищенные каналы для органов государственной власти. Тем не менее, полноценное технологическое импортозамещение требует не только финансовых вливаний, но и стратегического партнерства с нейтральными странами в рамках Евразийского экономического союза, БРИКС и ШОС.

Выводы. Результаты проведенного анализа подтверждают, что цифровой суверенитет является необходимым условием устойчивого социально-экономического развития в условиях внешнего давления и неопределенности. Наращивание технологической независимости, в частности, увеличение доли отечественных серверов и ПО, напрямую способствует снижению уязвимости националь-

ной экономики перед санкционными рисками.

Данные о росте числа утечек и ограниченности контроля над трансграничными потоками данных продемонстрировали, что без эффективного механизма защиты невозможно обеспечить управление ключевыми секторами экономики, а значит, сохранить безопасность экономики.

Изучение регуляторной практики (включая действие законов о «суверенном интернете» и «приземлении» иностранных ИТ-компаний) показало, что правовая автономия государства является фундаментом цифрового контроля. Исследование сетевой инфраструктуры выявило высокий уровень импортозависимости в производстве оборудования, что подтверждает необходимость ускоренного развития отечественных ЦОДов.

Таким образом, ключевые составляющие суверенитета – технологическая независимость, контроль над данными, регуляторная автономия и развитие суверенной сетевой инфраструктуры – находятся в состоянии технологического и институционального становления. Тем не менее, реализуемый государством курс представляет собой стратегически выверенное направление развития, отвечающее вызовам геоэкономической среды.

Список источников

1. Кочетков А. П., Маслов К. В. Цифровой суверенитет как основа национальной безопасности России в глобальном цифровом обществе // Вестник Московского университета. Политические науки. – 2022. – № 2. – С. 31–44. – URL: https://cyberleninka.ru/article/n/tsi frovoy-suverenitet-kak-osnova-natsionalnoy-bezopa snosti-rossii-v-globalnom-tsifrovom-obschestve (дата обращения: 12.11.2025). – Текст: электронный.

2. Strategy Partners: российский рынок корпоративного ПО в 2024 году вернулся к докризисному показателю и составил 199 млрд руб. [Электронный ресурс]. – URL: https://ict.dev.ict.moscow/news/strategy-partners-rossiiskii-rynok-korporativnogo-po-v-2024-godu-vernulsia-k-dokrizisnomu-pokazateliu-i-sostavil-199-mlrd-rub/ (дата обращения: 22.05.2025). – Текст: электронный.

3. Кубанцева Е. В. Цифровая трансформация государственного управления как фактор достижения цифрового суверенитета в Российской Федерации // Общество: политика, экономика, право. – 2023. – № 9. – С. 45–52. – URL: https://cyberleninka.ru/article/n/tsifrovaya-transformatsiya-gosudarstvennogo-upravleniya-kak-faktor-dostizheniya-tsifrovogo-suvereniteta-v-rossiyskoy-federatsii (дата обращения: 12.11.2025). – Текст: электронный.

4. Караваева Е. В., Байбурин Р. Р. Роль государственно-частного партнерства в условиях цифровизации экономики // Вестник Алтайской академии экономики и права. – 2023. – № 10-3. – С. 316–321.

5. Чечин О. П. Цифровая трансформация в концепции экономической безопасности // Экономические науки. – 2019. – № 7 (176). – С. 92–97. – DOI: 10.14451/1.176.92. – Текст: электронный.

References

1. Kochetkov A. P., Maslov K. V. Digital Sovereignty as the Basis of National Security of Russia in the Global Digital Society. *Vestnik Moscovskogo Universiteta. Politicheskie Nauki*. 2022. No. 2. pp. 31–44. Available at: https://cyberleninka.ru/article/n/tsifrovoy-suverenitet-kak-osnova-natsionalnoy-bezopasnosti-rossii-v-globalnom-tsifrovom-obschestve (Accessed: 12.11.2025). (In Russ.).

2. Strategy Partners: Russian Market of Corporate Software in 2024 Returned to the Pre-Crisis Indicator and Totalled 199 Billion Rubles. Available at: https://ict.dev.ict.moscow/news/strategy-partners-ros siiskii-rynok-korporativnogo-po-v-2024-godu-ver nulsia-k-dokrizisnomu-pokazateliu-i-sostavil-199-mlrd-rub/ (Accessed: 22.05.2025). (In Russ.).

3. Kubantseva E. V. Digital Transformation of Public Administration as a Factor in Achieving Digital Sovereignty in the Russian Federation. *Obshchestvo: politika, ekonomika, parvo*. 2023. No. 9. pp. 45–52. Available at: https://cyberleninka.ru/article/n/tsifrovaya-transformatsiya-gosudarstvennogo-upravleniya-kak-faktor-dostizheniya-tsifrovogo-suvereniteta-v-rossiyskoy-federatsii (Accessed: 12.11.2025). (In Russ.).

4. Karavaeva E. V., Bayburin R. R. The Role of Public-Private Partnerships in the Context of the Digitalisation of the Economy. *Vestnik Altayskoy akademii ekonomiki i prava*. 2023. No. 10-3. pp. 316–321. (In Russ.).

5. Chechin O. P. Digital Transformation in the Concept of Economic Security. *Ekonomicheskiye nauki*. 2019. No. 7 (176). pp. 92–97. DOI: 10.14451/1.176.92. (In Russ.).

6. Цифровизация под санкциями: 8 проблем, с которыми столкнулись ИТ-службы российских банков [Электронный ресурс]. – URL: https://www.prbank.ru/articles/site/article-29032022 (дата обращения: 06.10.2025). – Текст: электронный.
7. Габитова З. Р., Нигматуллина Р. А., Байбурин Р. Р. Инновационная среда России на современном этапе развития экономики // Экономика. Право. Инновации. 2024. № 1. С. 17–23. – DOI: 10.17586/2713-1874-2024-1-17-23. – Текст: электронный.
8. Серверное сияние: на каждый проданный зарубежный сервер приходится три российских [Электронный ресурс]. – URL: https://www.forbes.ru/tekhnologii/536481-servernoe-sianie-na-kazdyj-prodannyj-zarubeznyj-server-prihoditsa-tri-rossijskih (дата обращения: 22.05.2025). – Текст: электронный.
9. Спасение рядового сервера: какая поддержка нужна российским производителям «железа» [Электронный ресурс]. – URL: https://www.forbes.ru/tekhnologii/534099-spasenie-radovogo-servera-kakaa-podderzka-nuzna-rossijskim-proizvoditelam-zeleza (дата обращения: 22.05.2025). – Текст: электронный.
10. Федеральный закон от 07.04.2025 № 58-ФЗ «О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. – URL: http://www.kremlin.ru/acts/bank/51814 (дата обращения: 12.11.2025). – Текст: электронный.
11. Мухамадиева Э. Ф., Шабанов Н. И. Цифровой суверенитет и безопасность в эпоху информации: вызовы и стратегии развития России // Экономика и управление: научно-практический журнал. – 2024. – № 4. – С. 10–15. – DOI: 10.34773/EU.2024.4.2. – Текст: электронный.
12. Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» от 21.07.2014 № 242-ФЗ (последняя редакция) [Электронный ресурс]. – URL: http://www.kremlin.ru/acts/bank/38728 (дата обращения: 12.11.2025). – Текст: электронный.
13. Реформа трансграничной передачи данных: первые итоги [Электронный ресурс]. – URL: https://zakon.ru/blog/2024/08/05/reforma_transgranichnoj_peredachi_dannyh_pervye_itogi (дата обращения: 22.05.2025). – Текст: электронный.
14. Россия: утечки информации ограниченного доступа, 2023-2024 [Электронный ресурс]. – URL: https://www.infowatch.ru/analytics/analitika/utechki-informatsii-v-rossii-otchet-za-proshedshiy-god (дата обращения: 22.05.2025). – Текст: электронный.

6. Digitalisation Under Sanctions: 8 Problems Faced by IT Services of Russian Banks. Available at: https://www.prbank.ru/articles/site/article-29032022 (Accessed: 06.10.2025). (In Russ.).

7. Gabitova Z. R., Nigmatullina R. A., Bayburin R. R. Innovation Environment of Russia at the Current Stage of Economic Development. *Ekonomika. Pravo. Innovatsii*. 2024. No. 1. pp. 17–23. DOI: 10.17586/2713-1874-2024-1-17-23. (In Russ.).

8. Server Glow: For Every Foreign Server Sold There are Three Russian Servers. Available at: https://www.forbes.ru/tekhnologii/536481-servernoe-sianie-na-kazdyj-prodannyj-zarubeznyj-server-prihoditsa-tri-rossijskih (Accessed: 22.05.2025). (In Russ.).

9. Salvation of an Ordinary Server: What Support Russian Hardware Manufacturers Need. Available at: https://www.forbes.ru/tekhnologii/534099-spasenie-radovogo-servera-kakaa-podderzka-nuzna-rossijskim-proizvoditelam-zeleza (Accessed: 22.05.2025). (In Russ.).

10. Federal Law No. 58-FZ dated 07.04.2025 «On Amending the Federal Law «On the Security of Critical Information Infrastructure of the Russian Federation». Available at: http://www.kremlin.ru/acts/bank/51814 (Accessed: 12.11.2025). (In Russ.).

11. Mukhamadieva E.F., Shabanov N.I. Digital Sovereignty and Security in the Era of Information: Challenges and Strategies for the Development of Russia. *Ekonomika i upravleniye: nauchno-prakticheskiy zhurnal*. 2024. No. 4. pp. 10–15. DOI: 10.34773/EU.2024.4.2. (In Russ.).
12. Federal Law «On Amending Certain Legislative Acts of the Russian Federation to Clarify the Procedure for Processing Personal Data in Information and Telecommunications Networks» dated 21.07.2014 N 242-FZ (latest version). Available at: http://www.kremlin.ru/acts/bank/38728 (Accessed: 12.11.2025). (In Russ.).

13. Reform of Cross-Border Data Transfer: First Results. Available at: https://zakon.ru/blog/2024/08/05/reforma_transgranichnoj_peredachi_dannyh_pervye_itogi (Accessed: 22.05.2025). (In Russ.).
14. Russia: Limited Access Information Leaks, 2023-2024. Available at: https://www.infowatch.ru/analytics/analitika/utechki-informatsii-v-rossii-otchet-za-proshedshiy-god (Accessed: 22.05.2025). (In Russ.).

15. Закон о приземлении иностранных IT-компаний [Электронный ресурс]. – URL: https://www.garant.ru/article/1482938/?ysclid=mazb7xi7w8295345792 (дата обращения: 22.05.2025). – Текст: электронный.
16. Эксперты РОЦИТ обсудили вопросы «приземления» иностранных хостингов [Электронный ресурс]. – URL: https://news.rambler.ru/politics/52840307-eksperty-rotsit-obsudili-voprosy-prizemleniya-inostrannyh-hostingov/ (дата обращения: 22.05.2025). – Текст: электронный.
17. Благодаря девелоперам в России запустили рекордное количество стойко-мест [Электронный ресурс]. – URL: https://www.cnews.ru/reviews/rynok_tsod_2024/articles/blagodarya_developeram_v_rossii_zapustili (дата обращения: 22.05.2025). – Текст: электронный.
18. Анализ рынка сетевых коммутаторов в России – 2025. Показатели и прогнозы [Электронный ресурс]. – URL: https://marketing.rbc.ru/research/49339/ (дата обращения: 22.05.2025). – Текст: электронный.
19. 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» [Электронный ресурс]. – URL: http://www.kremlin.ru/acts/bank/44230 (дата обращения: 12.11.2025). – Текст: электронный.

15. Law on Landing of Foreign IT-Companies. Available at: https://www.garant.ru/article/1482938/?ysclid=mazb7xi7w8295345792 (Accessed: 22.05.2025). (In Russ.).

16. ROCIT Experts Discussed the Issues of «Landing» Foreign Hosting. Available at: https://news.rambler.ru/politics/52840307-eksperty-rotsit-obsudili-voprosy-prizemleniya-inostrannyh-hostingov/ (Accessed: 22.05.2025). (In Russ.).

17. Thanks to Developers in Russia Launched a Record Number of Rack Places. Available at: https://www.cnews.ru/reviews/rynok_tsod_2024/articles/blagodarya_developeram_v_rossii_zapustili (Accessed: 22.05.2025). (In Russ.).

18. Analysis of the Network Switches Market in Russia – 2025. Indicators and Forecasts. Available at: https://marketing.rbc.ru/research/49339/ (Accessed: 22.05.2025). (In Russ.).

19. Federal Law No. 90-FZ dated 01.05.2019 «On Amendments to the Federal Law «On Communications» and the Federal Law «On Information, Information Technologies and Information Protection». Available at: http://www.kremlin.ru/acts/bank/44230 (Accessed: 12.11.2025). (In Russ.).

Статья поступила в редакцию 11.06.2025; одобрена после рецензирования 12.11.2025; принята к публикации 12.12.2025.
The article was submitted 11.06.2025; approved after reviewing 12.11.2025; accepted for publication 12.12.2025.