



УДК 32.019.51

DOI 10.52575/2687-0967-2026-53-3-750-758

EDN LDEBUS

Оригинальное исследование

## Информационный суверенитет России: стратегии и технологии в условиях глобализационных вызовов

Евграфов В.И. 

Казанский (Приволжский) федеральный университет,  
Россия, 420008, Республика Татарстан, г. Казань, ул. Кремлёвская, д. 18

[Vladimirevgrafov01@gmail.com](mailto:Vladimirevgrafov01@gmail.com)

**Аннотация.** В статье рассматривается феномен информационного суверенитета Российской Федерации в контексте современных глобализационных вызовов. Раскрываются теоретико-методологические основы понятия информационного суверенитета и его связь с государственным суверенитетом. Проведен анализ глобализационных угроз информационной безопасности России после 2022 года, усиления информационной войны, кибератак и технологической зависимости. Изучены государственные стратегии и технологии обеспечения информационного суверенитета (нормативно-правовые акты, развитие национальной цифровой инфраструктуры, политика импортозамещения в ИТ-сфере, продвижение искусственного интеллекта, меры по кибербезопасности). Отдельное внимание уделено международному опыту, практике Китая и Ирана в обеспечении информационного суверенитета и возможности использования этих подходов в российских реалиях. В заключении формулируются выводы о значении информационного суверенитета для национальной безопасности и даны рекомендации по укреплению суверенитета России в информационной сфере.

**Ключевые слова:** информационный суверенитет, информационная безопасность, глобализация, цифровой суверенитет, кибербезопасность, импортозамещение, государственная политика

**Финансирование:** работа выполнена без внешних источников финансирования.

**Для цитирования:** Евграфов В.И. 2026. Информационный суверенитет России: стратегии и технологии в условиях глобализационных вызовов. *Via in tempore. История. Политология*, 53(3): 750–758. DOI: 10.52575/2687-0967-2026-53-3-750-758. EDN: LDEBUS

## The Information Sovereignty of Russia in the Context of Globalization: Strategic Approaches and Technological Solutions

Vladimir I. Evgrafov 

Kazan (Volga Region) Federal University,  
18 Kremlyovskaja St., Kazan 420008, Republic of Tatarstan, Russia

[Vladimirevgrafov01@gmail.com](mailto:Vladimirevgrafov01@gmail.com)

**Abstract.** The article explores the complex issue of information sovereignty in the Russian Federation in the context of contemporary global challenges. It delves into the theoretical foundations and methodological approaches that underlie the concept of information sovereignty and its relationship with the traditional notion of state sovereignty. The analysis examines post-2022 threats to Russia's information security, including the intensification of information warfare, cyberattacks, and technological dependence. It carefully examines government strategies and measures to protect information sovereignty, including regulations, development of national digital infrastructure, pursuit of import substitution in IT, promotion of artificial intelligence, and strong cybersecurity measures. Special attention is paid to the international experience and practices of countries such as China and Iran, with a focus on the potential to adapt these approaches to Russian

circumstances. The author draws a conclusion about the importance of information sovereignty for a country's national security and provide recommendations for enhancing Russia's information sovereignty.

**Keywords:** information sovereignty, information security, globalization, digital sovereignty, cybersecurity, import phase-out, state policy

**Funding:** the work was carried out without external sources of funding.

**For citation:** Evgrafov V.I. 2026. The Information Sovereignty of Russia in the Context of Globalization: Strategic Approaches and Technological Solutions. *Via in tempore. History and political science*, 53(3): 750–758 (in Russian). DOI: 10.52575/2687-0967-2026-53-3-750-758. EDN: LDEBUS

В современную эпоху цифровизации информационные технологии и глобальные коммуникационные сети стали важнейшим фактором, влияющим на суверенитет государств. Стремительное развитие информационно-коммуникационных технологий (ИКТ) в конце XX – начале XXI века ознаменовало наступление новой цифровой эпохи, ускорив процессы глобализации. Негативные факторы цифровой глобализации сделали приоритетной задачу обеспечения информационной безопасности как ключевого условия сохранения государственного суверенитета в новых реалиях.

### *Понятие информационного суверенитета*

В настоящее время ни одно государство не обладает абсолютным, полностью автономным информационным суверенитетом. Тем не менее степень защищенности информационного пространства существенно различается по странам, а информационный суверенитет становится критически важным компонентом национальной безопасности.

Суверенитет как политико-правовая категория в классическом понимании означает верховенство государственной власти внутри страны и независимость государства на международной арене. Эта концепция сложилась в Вестфальской системе международных отношений (1648 г.) и с тех пор остается краеугольным принципом мировой политики и международного права [Зиновьева, Шитьков, 2023]. Однако на протяжении времени содержание суверенитета эволюционировало, включив новые измерения помимо территориального, такие как суверенитет в воздушном пространстве, суверенитет в области валютно-финансовой политики и др. [Зиновьева, Шитьков, 2023]. В XXI веке с распространением цифровых технологий возникло новое измерение суверенитета – информационное (цифровое) пространство.

Появились различные термины для отражения этого явления. В российском академическом дискурсе чаще используется термин «информационный суверенитет», подчеркивающий необходимость контроля не только над технической инфраструктурой, но и над трансграничными потоками контента. В западных исследованиях более популярны понятия «цифровой суверенитет» или «киберсуверенитет», акцентирующие юрисдикцию государства над инфраструктурой, программным обеспечением и данными при меньшем внимании к контролю содержания информации. Несмотря на терминологические разночтения, суть проблемы едина – способность государства самостоятельно определять политику в информационной сфере и защищать свой информационный простор от нежелательного внешнего вмешательства [Ustyuzhantseva, Popova, 2024].

В научной литературе нет единого общепризнанного определения информационного суверенитета [Холодная, 2024]. Тем не менее ряд исследователей предлагают формулировки, основывающиеся на классических признаках суверенитета, адаптированных к реалиям информационного общества. Так, М.М. Кучерявый [2014] определяет информационный суверенитет как «верховенство и независимость государственной власти при формировании и реализации информационной политики в национальном сегменте и глобальном информационном пространстве». В этом определении отражены два ключевых аспекта: внутренний (верховенство власти в своем информационном пространстве) и внешний (независимость от чужого диктата в

глобальной информационной среде). Близкой позиции придерживается и ряд других авторов. Например, Е.Н. Дубинина и Я.А. Хорошавина [2021] предлагают трактовать информационный суверенитет как способность государства с помощью современных технологий и правового регулирования обеспечивать и защищать конституционные права личности, интересы общества и государства в информационном пространстве, а также осуществлять эффективный контроль над происходящим в этом пространстве. Таким образом, информационный суверенитет можно рассматривать как частный аспект государственного суверенитета, относящийся к сфере информации и цифровых коммуникаций. В условиях цифровой эпохи устойчивость традиционного государственного суверенитета во многом зависит от уровня информационной безопасности страны. Недаром в стратегических документах РФ прямо подчеркивается, что «целью обеспечения информационной безопасности является укрепление суверенитета Российской Федерации в информационном пространстве».

Для более полного раскрытия содержания информационного суверенитета необходимо рассмотреть его структуру, или основные компоненты. Отечественные исследователи выделяют технические, содержательные и правовые составляющие суверенитета в информационной сфере. Так, В.В. Бухарин [2016] относит к ключевым техническим компонентам информационного суверенитета следующие элементы: собственная поисковая система, национальные социальные сети, отечественные операционные системы и программное обеспечение, независимая микроэлектронная база, сетевое телекоммуникационное оборудование, контролируемый государством национальный сегмент сети Интернет, суверенная система платежных карточек, отечественные средства защиты информации и криптографические протоколы, а также независимая навигационная спутниковая система. Наличие перечисленных компонентов создает материально-техническую основу для независимости страны в цифровой сфере. Содержательный компонент информационного суверенитета включает способность государства контролировать потоки информации (новостной, образовательный, культурный контент) в своих границах, ограждать общество от пропаганды, дезинформации, экстремистских материалов извне. Правовой компонент подразумевает наличие суверенной юрисдикции над национальным информационным пространством, т. е. развитие национального законодательства и институтов, регулирующих отношения в сфере информационной безопасности, СМИ, персональных данных, киберпреступности и т. д., а также отстаивание суверенных прав страны в международных нормах, касающихся интернета и информации.

Отдельно следует отметить, что категория информационного суверенитета эволюционирует вместе с научно-техническим прогрессом и трансформацией мирового порядка. Возникают новые вызовы – например, появление глобальных цифровых платформ колоссальной влияния, обладающих фактически наднациональной силой воздействия на аудиторию. Формируются метавселенные, распространяются криптоактивы – все это ставит вопросы, не вписывающиеся напрямую в традиционные рамки государственного суверенитета [Зиновьева, Шитьков, 2023]. Тем не менее, как отмечают исследователи, суверенитет остается базовым принципом, способным стать общим знаменателем для разработки новых международных правил ответственного поведения государств в цифровой среде [Зиновьева, Шитьков, 2023]. Обеспечение информационного суверенитета в таких условиях требует гибкого, динамического подхода, учитывающего и технологические изменения, и баланс между безопасностью и правами человека.

Мировая информационная среда в последние годы характеризуется повышенной турбулентностью и ростом конфликтного потенциала. Для Российской Федерации переломным моментом стал 2022 год, когда обострившееся противостояние с западными странами перешло и в информационно-цифровую плоскость. Рассмотрим основные вызовы и угрозы для информационного суверенитета и безопасности России, проявившиеся после 2022 года.

В связи с началом специальной военной операции (СВО) в 2022 г. беспрецедентно обострилась информационная война против России. Западные СМИ и интернет-платформы развернули масштабные кампании, зачастую сопровождаемые распространением дезинформации

и односторонней подачи событий. Российские государственные СМИ (RT, Sputnik и др.) были запрещены или ограничены в ряде стран, а аккаунты официальных российских источников информации подвергались блокировкам на глобальных платформах. Одновременно на территории России сами власти были вынуждены принимать меры реагирования, например, весной 2022 г. были ограничены (заблокированы) доступы к некоторым крупнейшим зарубежным соцсетям и онлайн-платформам, которые, по оценке российских органов, отказались предоставлять объективную и сбалансированную информацию о событиях и тем самым стали орудием информационного воздействия [Пашута и др., 2022; Зиновьева, Шитьков, 2023]. Вышеуказанные шаги фактически обозначили раскол глобального информационного пространства, где значительная часть мирового контента стала недоступна российским пользователям, и наоборот, российский информационный контент подвергся ограничениям за рубежом. В результате возникла угроза фрагментации интернета, когда национальный сегмент Рунета оказался в известной информационной изоляции от мирового. С одной стороны, такие меры рассматривались как вынужденная защита от враждебной пропаганды. С другой, они подчеркнули жизненную необходимость развития автономных отечественных информационных ресурсов и платформ, способных заменить иностранные сервисы и обеспечить устойчивость информационного обмена внутри страны. Фактически информационная конфронтация 2022 года показала, что наличие собственных социальных сетей, видеохостингов, новостных агрегаторов и т. п. является важным условием информационного суверенитета государства [Уртаева, 2024].

Одновременно внутри страны резко повысились требования к мониторингу и контролю информационных потоков во избежание распространения ложных сведений и панических слухов. Были оперативно приняты новые законодательные меры, ужесточена ответственность за «фейки» и дискредитацию Вооруженных сил РФ в условиях конфликта. Главной проблемой цифрового общества стала лавинообразная дезинформация – явление, которое Е.Н. Дубинина и Я.А. Хорошавина [2021] метко называет «информационной войной», отличающейся от традиционных военных действий тем, что главным оружием выступают средства массовой информации и интернет-сервисы. Через них сознанию граждан навязываются выгодные противнику интерпретации событий, подрывается доверие к государственным институтам. Таким образом, идеологические и психологические воздействия из внешних источников после 2022 г. приобрели характер постоянной угрозы информационной безопасности России.

Наряду с контентной агрессией Россия столкнулась с волной кибернетических атак на критически важную информационную инфраструктуру. Начиная с конца февраля 2022 г. активизировались как профессиональные хакерские группировки, ассоциируемые с иностранными спецслужбами, так и разрозненные группы «активистов», координирующиеся через соцсети и мессенджеры. В сумме происходит беспрецедентное по масштабу и интенсивности кибердавление на Россию. Российская Федерация в указанный период столкнулась с масштабным кибердавлением, включающим тысячи попыток воздействия на критически важную информационную инфраструктуру, что потребовало системных мер по её защите. По сути, киберфронт стал неотъемлемой частью общего противостояния, а информационная инфраструктура – объектом целенаправленного противоправного воздействия со стороны недружественных государств.

Еще один серьезный вызов информационному суверенитету России, обнажившийся после 2022 г., это высокая зависимость отечественной цифровой экосистемы от зарубежных технологий, оборудования и программного обеспечения. Вследствие введения масштабных санкций и ухода из России многих западных технологических компаний в стране возникла угроза технологической изоляции. В 2022 году производство и обновление значительной части программных продуктов, используемых в государственных информационных системах и на предприятиях, было поставлено под угрозу из-за прекращения поддержки со стороны правообладателей. По оценке Минцифры РФ, на начало 2022 года лишь около 20 % программного обеспечения, применяемого на российских промышленных предприятиях, имели сопоставимые отечественные аналоги. Остальные 80 % зависели от импорта, что создавало критическую уязвимость [Воротилова, 2024]. Резкий отток иностранных ИТ-компаний усилил риск технологического отставания и даже возможной деградации отдельных сегментов Рунета.



Таким образом, санкционное давление высветило проблему импортозависимости в информационно-технологической сфере, которая прямо затрагивает информационный суверенитет. Уход иностранцев обнажил эти проблемы, но вместе с тем стимулировал рост собственных технологических проектов: уже в 2023 г. объем реализации российских ИТ-решений значительно вырос за счет резкого подъема внутреннего спроса [Оруч, 2024]. В целом вызов технологической независимости стал катализатором для переосмысления стратегии цифрового развития, где акцент сместился на достижение цифрового суверенитета к 2030 г., соответствующая цель зафиксирована в Указе Президента Российской Федерации от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» [Попкова, 2025].

Первым компонентом укрепления информационного суверенитета является формирование нормативно-правовой базы, закрепляющей суверенные права государства в информационном пространстве и устанавливающей правила обеспечения информационной безопасности. В России такой фундамент закладывается с конца 1990-х годов [Полякова, 2025]. Уже в 1998 году была принята Концепция государственной информационной политики РФ, определившая национальные интересы в информационной сфере и систему мер по их защите. В дальнейшем ключевые положения нашли отражение в доктринальных документах, в 2000 г. была утверждена первая Доктрина информационной безопасности, обновленная в новой редакции в 2016 году (Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации») [Шерашенкова, Федоскин, 2025].

Доктрина информационной безопасности РФ 2016 г. представляет собой систему официальных взглядов на обеспечение национальной безопасности в информационной сфере [Chislova, Sokolova, 2021]. Она исходит из признания информационной сферы неотъемлемой частью жизнедеятельности государства и фиксирует национальные интересы в этой области. Защита суверенитета названа среди ключевых целей обеспечения информационной безопасности. В Доктрине 2016 г. проанализированы основные угрозы и определены стратегические задачи, что задало рамки для государственной политики информационной безопасности, впоследствии конкретизированной в отраслевых стратегиях.

Важнейшим программным документом стал также Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации». В этой Стратегии значительно усилено внимание к вопросу информационного суверенитета. Отдельно выделен приоритет обеспечения суверенитета информационного пространства России и безопасности отечественной информационной инфраструктуры. В числе национальных интересов названы развитие безопасного информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия, защита инфраструктуры связи и критических информационных систем. Стратегия-2021 предписывает комплекс мер для достижения этих целей, от импортонезависимости цифровой базы до повышения устойчивости Рунета и продвижения российской позиции на международных площадках. Таким образом, признано, что информационная сфера – это поле конкуренции и потенциальной конфронтации, где Россия должна отстаивать свой суверенитет.

Усиление государственного регулирования информационного пространства в российских условиях обусловлено не идеологическими соображениями, а объективной необходимостью защиты национальной безопасности в условиях внешнего давления [Амелин, Плащенко, 2025]. Реализуемые меры направлены на обеспечение устойчивости цифровой инфраструктуры, предотвращение деструктивного информационного воздействия и сохранение функциональной целостности национального сегмента сети Интернет [Чернышова, 2022]. При этом государственная политика в данной сфере ориентирована на избирательное и пропорциональное применение регуляторных инструментов, исходя из характера и масштаба выявляемых угроз.

Отчасти показательна практика избирательного воздействия, где государство блокирует только те зарубежные сервисы, которые «ведут себя недружественно» и отказываются соблюдать российские законы. Так, продолжают работать иностранные сайты, не нарушающие норм, что

свидетельствует об осторожном подходе. Вместе с тем сохраняется возможность в любой момент ограничить любую площадку, если она станет инструментом информационной агрессии против РФ [Володенко, Федорченко, 2025]. Таким образом, создан необходимый инструментарий управления национальным сегментом сети, который может быть задействован пропорционально уровню угроз.

Китайская Народная Республика считается пионером в области практической реализации государственного суверенитета в интернете. Еще в начале 2000-х Китай выстроил масштабную систему контроля над национальным сегментом сети – так называемый проект «Золотой щит», неофициально именуемый «Великим файрволом Китая». Цензурой и фильтрацией интернет-трафика в КНР занимается специальное подразделение Министерства общественной безопасности, а доступ граждан к зарубежным сайтам жестко регламентирован. Теория китайского подхода была изложена одним из архитекторов этой системы Фан Биньсином, которого называют «отцом китайского файрвола». В 2011 г. на симпозиуме по информационной безопасности в Чанше он сформулировал четыре принципа «интернет-суверенитета» [Мельникова, 2022; Зиновьева, Шитьков, 2023]:

1. Каждая страна должна обладать полным контролем над своим национальным сегментом Интернета.

2. Государство имеет право защищать свой сегмент сети от любых внешних атак.

3. Все страны равны в правах на использование ресурсов интернета.

4. Ни одно государство не должно контролировать корневые DNS-серверы, через которые осуществляется доступ к чужому национальному сегменту.

Вышеуказанные принципы отражают стремление Китая утвердить равноправие и независимость государств в киберпространстве, аналогично их суверенитету в офлайн-мире. Реализуя данный подход, Пекин последовательно создавал полноценные отечественные аналоги ключевых интернет-сервисов, что позволило минимизировать зависимость от иностранных ИТ-гигантов. Сегодня в Китае есть свои поисковые системы, социальные сети и мессенджеры, видеохостинги, онлайн-энциклопедии и т. д. [Мельникова, 2022]. Благодаря развитию этих собственных платформ «китайский Интернет» смог функционировать в относительно автономном режиме внутри цифровых границ государства. При этом китайские компании получили огромный внутренний рынок, что стимулировало рост национальной ИТ-индустрии.

В законодательном плане Китай также закрепил принципы цифрового суверенитета. В 2017 году был принят Закон КНР о кибербезопасности, легитимировавший практику контентной фильтрации и хранения данных внутри страны. В 2021 году введены Закон о безопасности данных и Закон о персональной информации, согласно которым данные признаются национальным стратегическим ресурсом, подлежащим защите [Зиновьева, Шитьков, 2023]. Экспорт значимых данных теперь возможен только с разрешения властей. Таким образом, Китай институционализировал контроль над данными вплоть до того, что в официальных документах данные названы наряду с землей, капиталом и технологиями новым фактором производства.

Для России китайский опыт подтверждает, что суверенное развитие цифровых технологий приносит плоды. Китай сумел защитить свое интернет-пространство от внешнего влияния, одновременно добившись технологического рывка и лидерства в ряде направлений. Конечно, прямое копирование китайской модели в России вряд ли оправдано ввиду иных политических и социальных условий. Китай представляет собой более закрытую политическую систему, что облегчает жесткую цензуру. Тем не менее некоторые элементы вполне коррелируют с российскими целями. Для России сотрудничество с Китаем в сфере кибербезопасности и интернет-управления также полезно, а совместные инициативы (в ООН, БРИКС, ШОС) повышают шансы продвинуть международные нормы, опирающиеся на принцип суверенитета.

Исламская Республика Иран – пример страны, которая ради защиты национальных ценностей и безопасности пошла на значительную изоляцию своего сегмента интернета. С начала 2010-х Иран активно строит так называемый «национальный интернет». Проект официально стартовал в 2013 году и предусматривал создание внутренней государственно контролируемой сети, параллельной глобальному интернету. Уже к сентябрю 2012 г. иранские власти сообщили о тестовом подключении всех государственных структур к этой внутренней сети, не имеющей выхода в глобальный интернет [Цветкова и др., 2022]. Планировалось, что на втором этапе (к 2013 г.) к



национальному интернету будут подключены университеты и впоследствии – рядовые граждане. Официально заявлялось, что национальный интернет будет сосуществовать с глобальным, обеспечивая более быстрое и надежное прохождение внутреннего трафика. При этом власти отрицали цель полностью изолировать иранских пользователей от Всемирной паутины, называя полное отключение «нелогичным» и сравнивая его с санкцией против самого себя [Рябцева, 2024].

Иранский опыт во многом схож с китайским в части строгой фильтрации контента, но отличается по техническим возможностям. Эксперты отмечали, что полностью изолировать Ирану себя сложно из-за ограниченности ресурсов и санкций (затрудняющих доступ к технологиям) [Рябцева, 2024]. Тем не менее государство добилось значительного контроля: иранский сегмент интернета может функционировать как интернет с разрешенным набором ресурсов. Главное обоснование – это защита религиозных и национальных ценностей от чуждого влияния и противодействие кибератакам [Цветкова и др., 2022].

Для России иранская модель является крайним примером изоляционистского подхода. Преимущество – высокая степень контроля и сложность внешнего воздействия (кибератак, информационных операций). Но минусы очевидны, из-за ограниченного доступа к глобальным знаниям страдает развитие экономики, наука, общество. Иранские граждане испытывают постоянные трудности в коммуникациях, бизнес – в подключении к мировым рынкам. В итоге Иран остается во многом технологически отсталым и зависимым. Для России такой путь нежелателен. Однако некоторые элементы иранского опыта учитываются, например, создание закрытых сегментов связи для критических структур, развитие национальных сервисов. Главный вывод из иранской ситуации – надежность резервного интернета, ведь Иран показал, что при угрозе способен поддерживать ключевые сервисы даже без глобальной сети.

Исследование информационного суверенитета России в условиях современных глобальных вызовов позволяет сделать вывод, что информационный суверенитет выступает неотъемлемой частью общего государственного суверенитета в XXI веке. Цифровая трансформация всех сфер жизни привела к тому, что без контроля над национальным информационным пространством невозможно гарантировать ни политическую независимость, ни безопасность, ни устойчивое развитие государства. Российская Федерация на высшем уровне признала эту взаимосвязь, отразив приоритет защиты информационного суверенитета в стратегических документах безопасности. Обеспечение информационного суверенитета – длительный, многоплановый процесс. Россия уже прошла значительную часть пути, отразив первые мощные удары и заложив основу собственной цифровой независимости. Дальнейшие усилия должны быть направлены на укрепление достигнутого, устранение оставшихся «узких мест» и формирование такой информационно-технологической экосистемы, которая надежно защитит национальные интересы и в то же время станет драйвером развития в условиях новой полицентричной цифровой эпохи. Только располагая суверенными информационными ресурсами, Россия сможет уверенно противостоять глобальным вызовам и обеспечить свою безопасность, культурно-ценностную самобытность и конкурентоспособность в мире.

### **Благодарность**

Автор выражает искреннюю благодарность научному руководителю, доктору юридических наук Зазнаеву Олегу Ивановичу, за ценные рекомендации.

### **Список литературы**

- Амелин В.Н., Плашенков Д.Д. 2025. Механизмы обеспечения государственного суверенитета в многополярном мире. Социально-гуманитарные знания, 5: 559–565.
- Бухарин В.В. 2016. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности. Вестник МГИМО-Университета, 6(51): 76–91.
- Володенко С.В., Федорченко С.Н. 2025. Суверенитет цифрового пространства общественно-политических коммуникаций в современной России и его ключевые компоненты: по материалам экспертного исследования. Вестник Российского университета дружбы народов. Серия: Политология, 27(3): 520–542.

- Воротилова М.Ю. 2024. Анализ текущего состояния импортозамещения в сфере программного обеспечения в России. Экономика и бизнес: теория и практика, 1–1(107): 40–43.
- Дубинина Е.Н., Хорошавина Я.А. 2021. Информационный Суверенитет Российской Федерации. *Advances in Law Studies*, 3: 66–70.
- Зиновьева Е.С., Шитков С.В. 2023. Цифровой суверенитет в практике международных отношений. *Международная жизнь*, 3: 38–51.
- Кучерявый М.М. 2014. Государственная политика информационного суверенитета России в условиях современного глобального мира. *Управленческое консультирование*, 9: 7–14.
- Мельникова О.А. 2022. Опыт Китая в защите национального киберсуверенитета. *Международная жизнь*, 12: 106–119.
- Оруч Т.А. 2024. Исследование роли цифровых технологий в обеспечении национального технологического суверенитета России. *Вестник Поволжского государственного университета сервиса. Серия: Экономика*, 20, 4(79): 5–10.
- Пашута В.Л., Поярков А.А., Оточкин В.В. 2022. Информационная война как высокотехнологичное оружие против России. *Актуальные проблемы физической и специальной подготовки силовых структур*, 2: 188–194.
- Полякова Т.А. 2025. Правовое обеспечение национального суверенитета в информационной сфере: стратегические задачи и проблемы в условиях цифровой трансформации в Российской Федерации. *Вестник Гродненского государственного университета имени Янки Купалы. Серия 4. Правоведение*, 15, 1: 25–35.
- Попкова А.А. 2025. Информационная безопасность в политическом дискурсе современной России. *Известия высших учебных заведений. Социология. Экономика. Политика*, 18, 3: 33–47.
- Рябцева Е.Е. 2024. Защита национального суверенитета в Интернет-пространстве (опыт Исламской Республики Иран). *Парадигмы истории и общественного развития*, 30: 10–15.
- Уртаева Э.Б. 2024. Влияние социальных сетей на развитие политических коммуникаций в новой цифровой реальности. *Общество: политика, экономика, право*, 3: 40–49.
- Холодная Е.В. 2024. Об информационном суверенитете. *Вестник Университета имени О.Е. Кутафина*, 10, 122: 85–90.
- Цветкова Н.А., Сытник А.Н., Гришанина Т.А. 2022. Цифровая дипломатия и digital international relations: вызовы и новые возможности. *Вестник Санкт-Петербургского университета. Международные отношения*, 15, 2: 174–196.
- Чернышова Е. Зачем власти создают «суверенный Рунет»: от чего он защитит и чем грозит. РБК URL: <https://trends.rbc.ru/trends/industry/609a52329a79471fba0f0837?from=copy> (дата обращения: 31.01.2026).
- Шерашенкова Е.А., Федоскин Н.Н. 2025. Проблемы и перспективы правового регулирования информационной политики. *Образование и право*, 7: 44–51.
- Chislova O., Sokolova M. 2021. Cybersecurity in Russia. *International Cybersecurity Law Review*, 2: 245–251.
- Ustyuzhantseva O., Popova E. 2024. Shaping Digital Sovereignty in Russia: Actors and Debates. *Problems of Post-Communism*, 72, 4: 76–87.

## References

- Amelin V.N., Plashenkov D.D. 2025. *Mehanizmy obespechenija gosudarstvennogo suvereniteta v mnogopoljarnom mire* [Mechanisms for Ensuring State Sovereignty in a Multipolar World]. *Social'no-gumanitarnye znaniya*, 5: 559–565.
- Buharin V.V. 2016. *Komponenty cifrovogo suvereniteta Rossijskoj Federacii kak tehnikeskaja osnova informacionnoj bezopasnosti* [Components of the Digital Sovereignty of the Russian Federation as a Technical Basis for Information Security]. *Vestnik MGIMO-Universiteta*, 6(51): 76–91.
- Volodenko S.V., Fedorchenko S.N. 2025. *Suverenitet cifrovogo prostranstva obshhestvenno-politicheskikh kommunikacij v sovremennoj Rossii i ego ključevye komponenty: po materialam jekspertnogo issledovanija* [The Sovereignty of the Digital Space of Social and Political Communications in Modern Russia and its Key Components: Based on the Materials of an Expert Study]. *Vestnik Rossijskogo universiteta družby narodov. Serija: Politologija*, 27, 3: 520–542.
- Vorotilova M.Ju. 2024. *Analiz tekushhego sostojanija importozameshhenija v sfere programmnogo obespechenija v Rossii* [Analysis of the Current State of Import Substitution in the Software Sector in Russia]. *Jekonomika i biznes: teorija i praktika*, 1–1(107): 40–43.
- Dubinina E.N., Horoshavina Ja.A. 2021. *Informacionnyj Suverenitet Rossijskoj Federacii* [Information Sovereignty of the Russian Federation]. *Advances in Law Studies*, 3: 66–70.



- Zinov'eva E.S., Shit'kov S.V. 2023. Cifrovoy suverenitet v praktike mezhdunarodnyh otnoshenij [Digital Sovereignty in the Practice of International Relations]. *Mezhdunarodnaja zhizn'*, 3: 38–51.
- Kucherjavij M.M. 2014. Gosudarstvennaja politika informacionno suvereniteta Rossii v usloviyah sovremennogo global'nogo mira [State Policy of Information Sovereignty of Russia in the Context of the Modern Global World]. *Upravlencheskoe konsul'tirovanie*, 9: 7–14.
- Mel'nikova O.A. 2022. Opyt Kitaja v zashhite nacional'nogo kibersuvereniteta [China's Experience in Protecting National Cyber Sovereignty]. *Mezhdunarodnaja zhizn'*, 12: 106–119.
- Oruch T.A. 2024. Issledovanie roli cifrovyyh tehnologij v obespechenii nacional'nogo tehnolo-gicheskogo suvereniteta Rossii [A Study of the Role of Digital Technologies in Ensuring Russia's National Technological Sovereignty]. *Vestnik Povolzhskogo gosudarstvennogo universiteta servisa. Seriya: Jekonomika*, 20, 4(79): 5–10.
- Pashuta V.L., Pojarkov A.A., Otochkin V.V. 2022. Informacionnaja vojna kak vysokotekhnologichnoe oruzhie protiv Rossii [Information Warfare as a High-Tech Weapon against Russia]. *Aktual'nye problemy fizicheskoy i special'noj podgotovki silovyh struktur*, 2: 188–194.
- Poljakova T.A. 2025. Pravovoe obespechenie nacional'nogo suvereniteta v informacionnoj sfere: strategicheskie zadachi i problemy v usloviyah cifrovoy transformacii v Rossijskoj Federacii [Legal Support for National Sovereignty in the Information Sphere: Strategic Tasks and Problems in the Context of Digital Transformation in the Russian Federation]. *Vestnik Grodnenskogo gosudarstvennogo universiteta imeni Janki Kupaly. Seriya 4. Pravovedenie*, 15, 1: 25–35.
- Popkova A.A. 2025. Informacionnaja bezopasnost' v politicheskom diskurse sovremennoj Rossii [Information Security in Political Discourse in Modern Russia]. *Izvestija vysshih uchebnyh zavedenij. Sociologija. Jekonomika. Politika*, 18, 3: 33–47.
- Rjabceva E.E. 2024. Zashhita nacional'nogo suvereniteta v Internet-prostranstve (opyt Islam-skoj Respubliki Iran) [Protecting National Sovereignty in the Internet Space (the Experience of the Islamic Republic of Iran)]. *Paradigmy istorii i obshhestvennogo razvitiya*, 30: 10–15.
- Urtaeva Je.B. 2024. Vlijanie social'nyh setej na razvitie politicheskikh kommunikacij v novoj cifrovoy real'nosti [The Impact of Social Media on the Development of Political Communications in the New Digital Reality]. *Obshhestvo: politika, jekonomika, pravo*, 3: 40–49.
- Holodnaja E.V. 2024. Ob informacionnom suverenitete [On Information Sovereignty]. *Vestnik Universiteta imeni O.E. Kutafina*, 10, 122: 85–90.
- Cvetkova N.A., Sytnik A.N., Grishanina T.A. 2022. Cifrovaja diplomatija i digital international relations: vyzovy i novye vozmozhnosti [Digital Diplomacy and Digital International Relation: Challenges and New Opportunities]. *Vestnik Sankt-Peterburgskogo universiteta. Mezhdunarodnye otnoshenija*, 15, 2: 174–196.
- Chernyshova E. Zachem vlasti sozdajut «suverennyj Runet»: ot chego on zashhitit i chem grozit [Why are the Authorities Creating a "Sovereign RuNet": What Will it Protect against and What Are the Threats?]. *RBK URL*: <https://trends.rbc.ru/trends/industry/609a52329a79471fba0f0837?from=copy> (data ob-rashhenija: 15.08.2025).
- Sherashenkova E.A., Fedoskin N.N. 2025. Problemy i perspektivy pravovogo regulirovaniya in-formacionnoj politiki [Problems and Prospects of Legal Regulation of Information Policy]. *Obrazovanie i pravo*, 7: 44–51.
- Chislova O., Sokolova M. 2021. Cybersecurity in Russia. *International Cybersecurity Law Review*, 2: 245–251.
- Ustyuzhantseva O., Popova E. 2024. Shaping Digital Sovereignty in Russia: Actors and Debates. *Problems of Post-Communism*, 72, 4: 76–87.

**Конфликт интересов:** о потенциальном конфликте интересов не сообщалось.

**Conflict of interest:** no potential conflict of interest related to this article was reported.

Поступила в редакцию 20.05.2026

Received 20.05.2026

Поступила после рецензирования 10.06.2026

Revised 10.06.2026

Принята к публикации 20.06.2026

Accepted 20.06.2026

## ИНФОРМАЦИЯ ОБ АВТОРЕ

## INFORMATION ABOUT THE AUTHOR

**Евграфов Владимир Игоревич**, аспирант кафедры политологии, Казанский (Приволжский) Федеральный университет, г. Казань, Россия

**Vladimir I. Evgrafov**, Postgraduate Student, Department of Political Science, Kazan (Volga region) Federal University, Kazan, Russia

 [ORCID: 0009-0001-3607-9860](https://orcid.org/0009-0001-3607-9860)