УДК 327.88+321.011(47)

В. И. Евграфов

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОГО СУВЕРЕНИТЕТА РОССИИ: ПРОТИВОСТОЯНИЕ КИБЕРУГРОЗАМ

Казанский федеральный университет, Казань, Россия
Поступила в редакцию 08.10.2025 г.
Принята к публикации 14.11.2025 г.
doi: 10.5922/vestnikhum-2025-4-10

Для цитирования: *Евграфов В.И.* Обеспечение информационного суверенитета России: противостояние киберугрозам // Вестник Балтийского федерального университета им. И. Канта. Сер.: Гуманитарные и общественные науки. 2025. №4. С. 121—132. doi: 10.5922/vestnikhum-2025-4-10.

Представлены результаты политологического анализа взаимосвязи между кибербезопасностью и информационным суверенитетом России с акцентом на роли отечественных цифровых технологий в обеспечении национальной безопасности. Раскрыты теоретические подходы к понятию информационного суверенитета, ключевые вызовы кибербезопасности для России в условиях глобальных угроз, а также значение развития собственных технологий и инфраструктуры для поддержания цифрового суверенитета государства. Рассмотрена современная законодательная и институциональная база кибербезопасности в Российской Федерации – охарактеризованы доктринальные документы и законы, направленные на защиту критической информационной инфраструктуры и укрепление «цифровых границ». Особое внимание уделено геополитическому измерению проблемы – сотрудничеству России с другими государствами в сфере международной информационной безопасности и конфликтам интересов в глобальном киберпространстве. Обоснован вывод о том, что укрепление киберзащиты и достижение информационного суверенитета требуют комплексного подхода, сочетающего технологическое развитие, эффективное регулирование и международное сотрудничество при одновременном обеспечении независимости национального цифрового пространства.

Ключевые слова: импортозамещение, информационная безопасность, информационный суверенитет, кибербезопасность, критическая информационная инфраструктура, международная информационная безопасность, суверенный Интернет

В эпоху глобальной цифровой трансформации информационно-коммуникационные технологии стали неотъемлемым фактором экономического развития и политических процессов, они во многом определяют конкурентоспособность и безопасность государств [6, с. 38; 7, с. 148—154]. Цифровое пространство превратилось в арену геополити-

ческого противоборства, а уровень цифровизации страны теперь в значительной мере обусловливает ее положение на международной арене и диапазон внешнеполитических возможностей [6]. Для современной России вопросы кибербезопасности и информационного суверенитета приобрели стратегическое значение, поскольку устойчивость национальной цифровой инфраструктуры и способность контролировать собственное информационное пространство рассматриваются как ключевые условия защиты государственного суверенитета и обеспечения национальной безопасности.

Информационный суверенитет: понятие и подходы

Понятие информационного суверенитета

В теории международных отношений суверенитет традиционно определяется как верховенство и независимость государственной власти внутри страны и в отношениях с другими государствами [5]. Возникшая в Вестфальскую эпоху концепция подразумевает, что государство обладает высшей властью на своей территории и не подчиняется внешним силам во внутренних делах. В XXI в. данная категория получила новое измерение — информационный суверенитет. Информационный суверенитет можно определить как способность государства самостоятельно формировать и реализовывать политику в информационной сфере, контролировать свое цифровое пространство и информационные потоки без вмешательства извне [6]. Иными словами, это независимость государства в управлении своей цифровой инфраструктурой, данными и контентом, ставшая одним из ключевых показателей государственной состоятельности, безопасности и технологической конкурентоспособности [Там же].

Следует отметить, что суверенитет никогда не был статичной категорией — со временем его содержание расширялось. С развитием информационного общества настала очередь и цифрового суверенитета — способности государства контролировать критически важные информационно-коммуникационные технологии и процессы. Если в 1990-е гг. Интернет воспринимался как глобальное пространство вне юрисдикций, то к настоящему времени государства всё настойчивее утверждают свое право регулировать национальные сегменты сети и устанавливать в них свои «цифровые границы» [5].

В российском академическом дискурсе обычно используется термин «информационный суверенитет», позволяющий подчеркнуть, что речь идет не только о контроле над технической инфраструктурой, но и над трансграничными потоками контента [6]. Западные же исследователи чаще говорят о «цифровом суверенитете» или «киберсуверенитете», подразумевая в первую очередь юрисдикцию государства над интернет-инфраструктурой, программным обеспечением и данными, нередко без акцента на контроле контента [Там же]. Таким образом, российский подход шире и включает культурно-информационный аспект: защита ценностей, предотвращение внешнего информационного

влияния, способного привести к политической дестабилизации (так называемым «цветным революциям»). Показательно, что события «Арабской весны» 2011 г. в Москве были восприняты как подтверждение уязвимости национальных режимов перед внешним информационным вмешательством, после чего многие государства (включая РФ) усилили внимание к контролю социальных сетей и трансграничного информационного обмена [5]. Согласно этой точке зрения обеспечение информационного суверенитета требует способности государства фильтровать или ограничивать потоки информации из-за рубежа, если они несут угрозу политической стабильности или противоречат национальным интересам.

Компоненты цифрового суверенитета

Информационный суверенитет современного государства многогранен. Российские эксперты часто трактуют его как совокупность следующих элементов: технологическая независимость (наличие автономной программно-аппаратной базы, собственных технологий и развитого IT-сектора); контроль инфраструктуры (способность государства обеспечить безопасность и устойчивость своей информационно-телекоммуникационной инфраструктуры, включая критические объекты); контроль контента (возможность регулировать и при необходимости ограничивать распространение информации в целях защиты национальной безопасности и ценностей); международная правосубъектность в киберпространстве (признание принципа суверенного равенства государств в цифровой среде и закрепление права государства на управление своим сегментом сети в международных нормах) [5]. Информационный суверенитет тесно связан с понятием «технологический суверенитет» и подразумевает способность государства развивать ключевые технологии самостоятельно и защищать свои интересы без критической зависимости от внешних игроков [Там же].

Важнейший теоретический вопрос — границы применения суверенитета в киберпространстве. Международное право пока не дает четкого ответа, однако Россия последовательно продвигает на глобальной арене идею о том, что принцип невмешательства и суверенного равенства государств распространяется и на информационную сферу [Там же].

Вызовы кибербезопасности России в условиях глобальных угроз

Глобальный ландшафт киберугроз

Развитие информационного общества сопровождалось экспоненциальным ростом киберугроз, способных причинить ущерб национальной безопасности. Для России, как и для других государств, особую опасность представляют атаки на критически важную инфраструктуру — энергетические системы, транспорт, связь, финансовый сектор, системы государственного управления и обороны [7, с. 147—148]. Нарушение работы таких объектов может привести к тяжелым по-

следствиям для экономики, обороноспособности и жизни граждан. В последние годы наблюдается как количественный рост кибератак, так и усложнение их характера, злоумышленники используют методы социальной инженерии, вредоносные программы-вымогатели, уязвимости в программном обеспечении и даже элементы искусственного интеллекта для проведения целевых сложных атак. По данным Совбеза РФ, только за 2024 г. на российские объекты критической информационной инфраструктуры (КИИ) было совершено свыше 208 тыс. особо опасных компьютерных атак, нацеленных на подрыв ключевых систем [11]. Для сравнения, годом ранее фиксировалось около 202 тыс. подобных атак, что свидетельствует о нарастающей киберугрозе на фоне обострения международной обстановки [Там же].

Источниками кибератак признаются как негосударственные хакерские группировки (в том числе террористические и криминальные организации), так и подразделения иностранных разведок и военных структур. Российские официальные лица прямо указывают на роль «отдельных государств», стремящихся использовать свои возможности в киберпространстве для шпионажа, саботажа и вмешательства во внутренние дела России. В Доктрине информационной безопасности Российской Федерации главным информационным вызовом названы действия иностранных государств, стремящихся «использовать технологическое превосходство для доминирования в информационном пространстве», в том числе для дестабилизации обстановки внутри России [13].

Особенности российских вызовов

Исторически Россия испытывала определенное технологическое отставание в IT-сфере и зависимость от импортных решений, что прямо признавалось в официальных документах. Доктрина 2016 г. отмечала, что доля отечественной продукции в сфере информационных технологий недостаточна, российская наука в области кибербезопасности развивается медленно, а зависимость от зарубежного софта и оборудования создает риски «геополитического влияния зарубежных стран» [Там же]. Иными словами, технологическая зависимость рассматривается как угроза информационному суверенитету, где иностранные поставщики могут, следуя санкциям или своим государственным интересам, прекратить поддержку продуктов, встроить уязвимости в оборудование, либо отказаться поставлять критически важные компоненты. Примером стало прекращение обслуживания и обновления некоторого зарубежного программного обеспечения в России на фоне политических санкций, что потребовало срочного поиска альтернатив.

Серьезным вызовом признана также угроза информационно-психологического воздействия на население. Через соцсети и онлайн-СМИ внешние игроки могут влиять на общественное мнение, инспирировать протесты и подрывать ценностные основы общества. Для противодействия этому в доктринальных установках провозглашены

укрепление патриотических и духовно-нравственных ценностей, нейтрализация деструктивного информационного воздействия извне [13]. Таким образом, под вызовами кибербезопасности Россия понимает не только сугубо технические угрозы (хакинг, вирусные эпидемии, кибершпионаж), но и контентные угрозы (идеологические, политические), что отражает широту концепции информационной безопасности.

Глобальные тенденции

В мире в целом наблюдается тревожная динамика, растет число инцидентов на критических объектах, обостряется конкуренция великих держав в киберпространстве, включая взаимные обвинения в хакерских операциях против государственных учреждений и выборных систем, происходит фрагментация глобального Интернета. Последнее проявляется в том, что многие страны пытаются локализовать хранение данных, использовать национальные сети и даже разрабатывают сценарии функционирования интернета в отрыве от глобальной сети на случай чрезвычайных ситуаций [7, с. 154—162]. Противоположные идеологии столкнулись: западные демократии во главе с США провозглашают приверженность единому открытому Интернету, тогда как такие государства, как Китай и Россия, отстаивают принцип цифрового суверенитета, который на практике означает возможность введения национальных ограничений и правил в сети [Там же]. Данная тенденция часто называется «балканизацией» Интернета — дроблением глобальной сети на сегменты по государственным границам [Там же, с. 161]. Для России данная тенденция двояка: с одной стороны, она соответствует ее интересам в части контроля над Рунетом, с другой — грозит технологическими и экономическими издержками, связанными с ограничением доступа к мировым информационным ресурсам и разделением Интернета на изолированные части.

Наконец, к наиболее серьезным современным вызовам относятся и риски технологического неоколониализма. Российские специалисты указывают, что менее развитые в технологическом отношении страны рискуют оказаться в полной зависимости от лидеров цифровой экономики, превратившись в «периферию», потребляющую чужие технологии на чужих условиях [Там же, с. 162—163]. Технологически продвинутые державы, обеспечивая кибербезопасность своей критической инфраструктуры и локализуя производство ключевых компонентов, фактически бросают вызов остальным. В результате перед большинством стран встает дилемма: присоединиться к одному из центров технологической силы (и, возможно, пожертвовать частью суверенитета), либо пытаться развивать собственные аналоги критических технологий с нуля, что крайне ресурсозатратно. Для России, претендующей на роль одного из мировых центров силы, решение очевидно — добиваться технологической самостоятельности, опираясь на научный и промышленный потенциал, и выстраивать коалиции с теми державами, которые разделяют подход к суверенитету в цифровой сфере. Именно по-

этому курс на обеспечение информационного суверенитета в РФ тесно сопряжен с идеей ускоренного инновационного развития и импортозамещения технологий, что рассматривается в следующем разделе.

Роль отечественных технологий в обеспечении цифрового суверенитета

Одним из ключевых условий информационного суверенитета является наличие в государстве собственных высокотехнологичных решений, которые могут заменить иностранные аналоги. Технологическая автономность снижает уязвимость перед внешними санкциями, киберугрозами и политическим давлением. Россия начала осознавать эту необходимость еще в 2000-х гг.: одним из первых стратегических документов в данной области стала Доктрина информационной безопасности 2000 г., где был сделан акцент на развитие национальных информационно-коммуникационных технологий [2]. В последующие годы были достигнуты определенные успехи — так, к 2010-м гг. в России сформировались собственные поисковые системы, социальные сети и национальная платежная система. Все это рассматривалось как элементы цифрового суверенитета, укрепляющие независимость от западных платформ и финансовых инфраструктур. В Доктрине информационной безопасности 2016 г. прямо отмечена важность ликвидации зависимости отечественной промышленности от зарубежных технологий за счет создания и широкого внедрения отечественных разработок [13]. Таким образом, стратегический курс на импортозамещение в IT-сфере был закреплен на высшем уровне.

Практические шаги по импортозамещению в цифровой экономике особенно активизировались после 2014 г., в условиях санкций и охлаждения отношений с Западом. Уже к 2017 г. российское правительство запустило программу перехода государственных органов на отечественное программное обеспечение [10]. Однако по многим направлениям внедрение шло медленно, пока ситуация не обострилась еще сильнее в 2022 г. Массовый уход западных производителей и разработчиков из России после начала специальной военной операции вынудил ускоренно заместить иностранные IT- решения — в кратчайшие сроки компании и госструктуры начали переход на отечественный софт, искать альтернативы импортному оборудованию [8, с. 367—368]. Фактически то, на что планировалось потратить более десяти лет, произошло в сжатые сроки под давлением обстоятельств [Там же]. Данный вынужденный эксперимент продемонстрировал как наличие в стране определенного запаса собственных технологических решений, так и пробелы, особенно в сфере аппаратного обеспечения.

Эксперты подчеркивают, что импортозамещение — лишь первый шаг на пути к подлинному технологическому суверенитету [1]. Заменив внутри страны чужие продукты на свои, Россия все еще может зависеть от импорта ключевых компонентов (микропроцессоров, элементной базы, производственного оборудования). Поэтому задача мак-

симум — научиться разрабатывать собственные фундаментальные технологии. «Когда мы научимся создавать свои процессоры и радиоэлектронные компоненты, тогда сможем говорить о технологическом суверенитете», — отмечают представители отрасли [17]. Несмотря на сложности, наметился определенный прогресс: в России развиваются проекты по выпуску отечественных процессоров, наращивается производство средств криптозащиты информации. Государство стимулирует крупные IT-компании предлагать продукты взамен ушедших западных [5], расширяется функционал отечественных офисных пакетов, растет популярность российской ОС Astra Linux и др. По данным отраслевых исследований, в 2022—2023 гг. востребованность российского программного обеспечения существенно выросла, особенно в сфере информационной безопасности [Там же], что свидетельствует о готовности рынка переходить на местные решения при наличии качественных предложений.

Важный элемент технологической независимости — развитие собственной телекоммуникационной инфраструктуры. Под этим подразумевается не только наличие национальных операторов связи, но также собственные точки обмена интернет-трафиком, независимая система доменных имен, контролируемые государством каналы связи. Россия исторически интегрирована в глобальный Интернет, однако в последнее десятилетие предпринимала шаги к укреплению автономности Рунета. Например, с 2014 г. действуют требования по хранению персональных данных россиян на серверах, расположенных внутри страны (ФЗ-152 «О персональных данных») [15]. Эта мера, помимо целей защиты данных, имела и суверенный мотив — чтобы данные российских граждан не находились под юрисдикцией других государств. В 2019 г. был принят специальный закон, известный как закон о «суверенном Рунете» (ФЗ-90, вступил в силу в ноябре 2019 г.), который определил требования к тому, чтобы российский сегмент Интернета мог устойчиво функционировать, даже если будет отключен от глобальной сети [14]. В рамках этого закона у операторов связи появилась обязанность установить технические средства противодействия угрозам на сетях (специальное оборудование), а также была создана инфраструктура для централизованного управления трафиком. Таким образом, Россия подготовила техническую базу, чтобы при необходимости переключить Рунет в автономный режим, сохранив работоспособность основных услуг внутри страны. Этот шаг, хотя и раскритикован сторонниками свободного Интернета, рассматривается как важная веха на пути к цифровому суверенитету России.

Таким образом, развитие отечественных цифровых и телекоммуникационных технологий — краеугольный камень обеспечения информационного суверенитета. Без собственных технологических возможностей Россия была бы обречена на зависимость от импорта и, следовательно, от политической воли других стран. Инвестиции в науку, образование IT-кадров, стимулирование инноваций (через национальные проекты и программы) — неотъемлемые составляющие стратегии на-

циональной безопасности в информационном веке. Показательно, что в последние годы значительно возрос бюджет на поддержку IT-отрасли, создаются особые режимы (налоговые льготы для IT-компаний, технологические центры и инкубаторы). Одновременно Россия активизирует кооперацию с Китаем и другими странами БРИКС / ШОС в области технологий, пытаясь совместно вырабатывать альтернативы западным стандартам (например, сотрудничество в сфере 5G, микроэлектроники, операционных систем). Все это — элементы долгосрочной политики, направленной на достижение стратегической технологической автономии.

Геополитическое измерение: сотрудничество и противоборство в киберпространстве

Вопросы кибербезопасности и информационного суверенитета давно вышли за рамки внутренних дел государств, превратившись в важный фактор международных отношений. Для России геополитическое измерение киберпространства имеет двойственный характер. С одной стороны, Москва активно продвигает идеи международного сотрудничества и выработки универсальных правил ответственного поведения государств в информационной сфере. С другой — нарастает конфронтация с рядом стран (прежде всего с США и их союзниками) из-за различия подходов к управлению Интернетом, взаимных обвинений в кибератаках и вмешательстве во внутренние дела.

Сотрудничество и коалиции

Россия последовательно выступает инициатором диалога по вопросам международной информационной безопасности (МИБ) на различных площадках. Начиная с конца 1990-х гг. РФ выносит на рассмотрение ООН резолюции, призванные обеспечить мирное использование ИКТ и предотвращение киберконфликтов [4, с. 117; 16, с. 39]. Благодаря российским усилиям были созданы специализированные механизмы: с 2004 г. работала Группа правительственных экспертов (ГПЭ) ООН по вопросам информационной безопасности, а с 2019 г. функционирует Рабочая группа открытого состава ООН по безопасности в сфере ИКТ (инициатива РФ) [5]. В рамках этих форматов России удалось добиться частичного консенсуса: основы международного права были признаны применимыми в киберпространстве, сформулированы добровольные нормы ответственного поведения государств [7, с. 163]. Важнейшим достижением стало закрепление в документах принципа суверенного равенства государств в сфере ИКТ — цифровой суверенитет получил международное признание как легитимное понятие [5].

Россия не только сотрудничает с ООН, но и использует региональные организации. В рамках Шанхайской организации сотрудничества (ШОС) еще в 2009 г. был разработан проект Международного кодекса поведения в информационном пространстве, который Россия и Китай

совместно продвигали на международной арене [3]. Этот кодекс, в противоположность западному подходу, делал акцент на суверенитете, невмешательстве во внутренние информационные пространства и ответственности государств за действия в сети. В Организации Договора о коллективной безопасности (ОДКБ) Россия инициировала сотрудничество по линии кибербезопасности: в 2023 г. впервые прошла международная конференция государств — участников ОДКБ по вопросам кибербезопасности, где обсуждались совместные меры по защите цифрового суверенитета союзников [9]. На ней, в частности, было отмечено, что абсолютное большинство опасных кибератак исходило из-за рубежа, поэтому подчеркивалась необходимость обмена опытом между союзниками по отражению таких угроз.

Конфликт и противоборство

На противоположной стороне — Соединенные Штаты и их союзники, продвигающие концепцию «открытого и свободного Интернета». Противоречия носят как ценностный, так и конкретно-политический характер. Запад критикует Россию за цензуру в Интернете, ограничения в отношении иностранных интернет-компаний и СМИ, называя это нарушением прав человека. Россия же обвиняет западные страны в двойных стандартах: с одной стороны, они декларируют свободу Интернета, с другой — сами вводят ограничения (например, блокировка российских государственных медиаканалов в ЕС, санкции против российских IT-компаний). С апреля 2022 г. США и около 60 стран присоединились к Декларации о будущем Интернета, где закреплена приверженность идее единого глобального Интернета, уважения прав и конкуренции [12]. Эта декларация разделила мир по идеологическому признаку: есть страны, поддержавшие американский подход, и есть те, кто не согласен и строит собственный путь (Россия, Китай, Иран, Северная Корея и др. не приглашены к подписанию декларации). Москва расценила такой шаг как попытку изолировать «неугодные» режимы и навязать свою повестку в управлении Интернетом [7, с. 154—162].

Для России в подобной ситуации особенно важно укреплять альянсы единомышленников, которые тоже заинтересованы в более справедливом информационном порядке. Одновременно Россия стремится снизить зависимость от инфраструктуры, контролируемой оппонентами. Так, уже с 2010-х гг. обсуждалось создание альтернативных маршрутов передачи данных (например, проложен подводный кабель связи между Россией и Китаем, планируются маршруты через Арктику для диверсификации от европейских каналов). Все это элементы более широкой геополитической игры, где предметом обсуждения является информационный суверенитет наций против глобального кибердоминирования.

Стоит подчеркнуть, что геополитическое измерение кибербезопасности для России сводится к тому, чтобы отстоять право на самостоятельный путь развития цифрового общества и защиту своего информационного пространства, не став изгоем мирового Интернета. Для

этого требуется тонкий баланс между конфронтацией (там, где затрагиваются принципиальные вопросы суверенитета) и сотрудничеством (там, где общие угрозы — киберпреступность, терроризм — требуют коллективных действий). Россия пытается сформировать новые нормы игры в киберпространстве, отвечающие ее национальным интересам, и продвигает идею многополярного и «субъектного» Интернета, где ни одна сила не монополизирует глобальную сеть, а каждая страна имеет гарантированные права и обязанности по обеспечению безопасности в цифровой сфере.

Заключение

В итоге проведенного анализа можно сделать ряд выводов. Кибербезопасность и информационный суверенитет для современной России являются взаимодополняющими целями, от достижения которых во многом зависит ее национальная безопасность и самостоятельная роль в мире. Киберпространство перестало быть нейтральной средой — оно превратилось в арену борьбы государств за влияние, и Россия как одна из великих держав выстраивает собственную модель защиты интересов в этой сфере. Модель кибербезопасности опирается на идею информационного суверенитета, и в ее рамках технологии играют первостепенную роль — от отечественных программ и микрочипов до суверенных сетевых инфраструктур. Такая стратегия позволяет минимизировать внешние риски и шоки, однако требует значительных ресурсов и может приводить к определенной фрагментации глобального информационного обмена.

Опыт России в обеспечении киберзащиты и информационного суверенитета демонстрирует, что технологическая мощь становится синонимом государственности в XXI в. Страны, которые неспособны защитить свой цифровой домен и обеспечить независимость в информационной сфере, рискуют утратить часть суверенитета и стать объектом технологического неоколониализма. Россия намерена не допустить этого, делая ставку на собственные силы, но при этом декларируя открытость к сотрудничеству на принципах равноправия. Как показывает политическая практика последних лет, прочный цифровой щит страны складывается из синергии передовых технологий, продуманной политики и консолидации общества вокруг идеи суверенитета в новом, цифровом измерении.

Список литературы

1. *Гайдукова М.О., Шушунова Т.Н., Челноков В.В., Аверина Ю.М.* Актуальные направления импортозамещения в сфере информационного обеспечения для цифровой трансформации наукоемких производств в РФ // Успехи в химии и химической технологии. 2022. №13 (262). С. 100—104.

2. *Доктрина* информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. №Пр-1895) // Парламентская газета. 2000. Ст. 187.

3. *Еникеев Ш.М., Лукин А.В., Новиков Д.П.* Шанхайская организация сотрудничества в новых геополитических условиях // Вестник международных организаций: образование, наука, новая экономика. 2024. №1. С. 129—148. doi: 10.17323/1996-7845-2024-01-06.

4. *Загайнов М.Р.* Вопросы развития сотрудничества США и России в сфере международной информационной безопасности // Социально-политические науки. 2024. №3. С. 115—124. doi: 10.33693/2223-0092-2024-14-3-115-124.

5. *Зиновьева Е.В., Бай Я.* Практика цифрового суверенитета в России и КНР // Российский Совет по международным делам (РСМД). 2023. 29 мая. URL: https://russiancouncil.ru/analytics-and-comments/analytics/praktika-tsifrovogo-suverenitета-v-rossii-i-knr/ (дата обращения: 05.08.2025).

6. *Зиновьева Е.В., Шитьков С.В.* Цифровой суверенитет в практике международных отношений // Международная жизнь. 2023. №3. С. 38—51.

7. *Карасев П.А., Стефанович Д.В.* Кибербезопасность критически важной инфраструктуры: новые вызовы // Россия в глобальной политике. 2022. Т. 20, №6. С. 147—164.

8. *Морозова Н.В., Мамчуев А.К., Хатуаев Т.А.* Импортозамещение программного продукта в России // Естественно-гуманитарные исследования. 2022. №6 (44). С. 367—370.

9. *Прошла* встреча глав государств — членов ОДКБ в узком составе. URL: https://odkb-csto.org/news/news_odkb/proshla-vstrecha-glav-gosudarstv-chlenov-odkb-v-uzkom-sostave/#loaded (дата обращения: 12.08.2025).

10. *Об утверждении* программы «Цифровая экономика Российской Федерации : распоряжение Правительства Российской Федерации от 28.07.2017 №1632-р // Собрание законодательства Российской Федерации. 2017. №32. Ст. 5138.

11. *Россия* отразила более 200 тысяч кибератак в 2024 году // Газета.ру. URL: https://www.gazeta.ru/tech/news/2025/06/19/26069870.shtml (дата обращения: 10.08.2025).

12. *США* и еще более 55 стран подписали «Декларацию о будущем интернета» // ТАСС. URL: https://tass.ru/obschestvo/14505635 (дата обращения: 12.08.2025).

13. *Об утверждении* Доктрины информационной безопасности Российской Федерации : указ Президента Российской Федерации от 05.12.2016 №646 // Собрание законодательства Российской Федерации. 2016. №50. Ст. 7074.

14. *О внесении* изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» : федер. закон Российской Федерации от 01.05.2019 №90-ФЗ // Собрание законодательства Российской Федерации. 2019. №18. Ст. 2214.

15. *О персональных* данных: Федеральный закон Российской Федерации от 27.07.2006 №152-ФЗ // Собрание законодательства Российской Федерации. 2006. №31. Ст. 3451.

16. *Чернявская К.Ю.* Деятельность ООН в информационном пространстве: история и документальная база организации в сфере борьбы с киберпреступностью // Русская политология. 2022. №4 (25). С. 38—42.

17. *Эксперты* назвали главные вызовы кибербезопасности страны // РБК. URL: https://ekb.rbc.ru/ekb/14/07/2023/64b1478e9a79479172b7e5bc (дата обращения: 12.08.2025).

Об авторе

Владимир Игоревич Евграфов — асп., Институт социально-философских наук и массовых коммуникаций, Казанский федеральный университет, Казань, Россия.

ORCID ID: 0009-0001-3607-9860

E-mail: vladimirevgrafov01@gmail.com

V. I. Evgrafov

CYBERSECURITY AND INFORMATION SOVEREIGNTY: THE ROLE OF TECHNOLOGY IN PROTECTING RUSSIA'S INTERESTS

Kazan Federal University, Kazan, Russia
Received 8 October 2025
Accepted 14 November 2025
doi: 10.5922/vestnikhum-2025-4-10

To cite this article: Evgrafov V.I. 2025, Cybersecurity and information sovereignty: the role of technology in protecting Russia's interests, *Vestnik of Immanuel Kant Baltic Federal University. Series: Humanities and social science*, №4. P. 121—132. doi: 10.5922/vestnikhum-2025-4-10.

The article presents the results of a political science analysis of the relationship between cybersecurity and Russia's information sovereignty, with a focus on the role of domestic digital technologies in ensuring national security. Theoretical approaches to the concept of information sovereignty are outlined, along with key cybersecurity challenges facing Russia in the context of global threats, as well as the importance of developing indigenous technologies and infrastructure to maintain the state's digital sovereignty. The contemporary legislative and institutional framework of cybersecurity in the Russian Federation is examined, including doctrinal documents and laws aimed at protecting critical information infrastructure and strengthening "digital borders." Particular attention is paid to the geopolitical dimension of the issue — Russia's cooperation with other states in the field of international information security and conflicts of interest in global cyberspace. The article substantiates the conclusion that strengthening cyber defense and achieving information sovereignty require a comprehensive approach that combines technological development, effective regulation, and international cooperation, while simultaneously ensuring the independence of the national digital space.

Keywords: cybersecurity, information sovereignty, critical information infrastructure, import substitution, sovereign internet, information security, international information security

The author

Vladimir I. Evgrafov, PhD Student, Institute of Philosophy, Social Sciences and Mass Communication, Kazan Federal University, Kazan, Russia.
ORCID ID: 0009-0001-3607-9860
E-mail: vladimirevgrafov01@gmail.com