



А.П. КОЧЕТКОВ*

Цифровой суверенитет России в условиях формирования глобального цифрового общества

Индекс УДК 32
Код ГРНТИ 11.01.29
DOI: 10.22204/2587-8956-2026-124-01-23-32

В статье анализируются проблемы формирования цифрового суверенитета России в глобальном цифровом обществе. Рассмотрены угрозы цифровому суверенитету страны в процессе цифровизации и необходимые условия его обеспечения в новых исторических реалиях.

По итогам проведённого исследования сделан вывод, что для обеспечения российского цифрового суверенитета необходимы создание и развитие собственных цифровых ресурсов, активное и постоянное инвестирование в разработку отечественных ИТ-технологий, высокий уровень образования и подготовки кадров в этой сфере, крупные инвестиции в образование, наличие широкого рынка информационных услуг как стимула конкуренции в области развития ИТ-технологий.

Особое внимание обращается на то, что цифровой суверенитет России является главным условием национальной независимости страны в глобальном цифровом обществе, раскрывается практическая деятельность государства по обеспечению своего цифрового суверенитета.

Ключевые слова: цифровизация, цифровой суверенитет, национальная независимость России, глобальное цифровое общество, транснациональные ИТ-корпорации, национальные цифровые ресурсы, инвестиции в ИТ-технологии, государственная информационная политика, российское законодательство по регулированию Интернета, факторы успеха российской ИТ-отрасли

В условиях формирования глобального цифрового общества особо важное значение для России приобретают проблема цифрового суверенитета, независимость российских сервисов и ИТ-инфраструктуры от внешних влияний и воздействий, создание отечественного программного обеспечения, независимость от иностранных технологий (ил. 1). В этих условиях государ-

ственная политика должна быть нацелена на цифровую трансформацию экономики и общества. Определяющим становится способность государства осуществлять независимую внешнюю и внутреннюю политику в цифровом пространстве.

В эпоху становления глобального цифрового общества, прекращения экспорта в нашу страну западных ИТ-технологий и введения «коллективным Западом»

* **Кочетков Александр Павлович** — доктор философских наук, профессор кафедры российской политики факультета политологии Московского государственного университета им. М.В. Ломоносова.
E-mail: apkoch@mail.ru

Цифровой суверенитет страны — это способность страны быть самостоятельной и независимой в цифровом пространстве



Ил. 1. Структура цифрового суверенитета

санкций против наших IT-компаний доступ к технологиям для России становится намного важнее, чем доступ к деньгам, так как технологии позволяют контролировать деятельность пользователей в цифровой среде, формировать у них национально-ориентированные представления и привычки.

В научной литературе нет единого определения понятия «цифровой суверенитет». Существуют различные точки зрения на эту проблему [1, с. 90–99]. В узком смысле слова «цифровой суверенитет» сводится к информационному суверенитету как праву государства контролировать информацию, распространяемую на его территории [2, с. 201–215]. В широком смысле слова в понятии «цифровой суверенитет» акцент делается на использование отечественного IT-оборудования и приоритетную поддержку отечественных IT-корпораций; обеспечение безопасности национальной интернет-инфраструктуры и национального интернет-трафика; использование больших данных исключительно в интересах национального государства [3, с. 31–45, 90–99].

Некоторые исследователи к понятию «цифровой суверенитет» также относят управление Интернетом отечественными государственными структурами с учётом места и роли страны в глобальной интернет-сети, национальные особенности взаимодействия государства, гражданского общества и частных IT-компаний [4, с. 24].

Цифровой суверенитет может включать в себя две основные компоненты: возможность независимого применения цифровых технологий в собственных интересах и способность их использования [5]. При этом цифровое пространство должно регулироваться национальным законодательством в интересах суверенного государства [6]. Ряд исследователей справедливо отмечают, что цифровой суверенитет является неотъемлемой частью национальной безопасности государства [7].

Важное значение имеют работы Ш. Зубофф, в которых раскрываются механизмы подрыва государственного суверенитета транснациональными цифровыми корпорациями через присвоение и монетизацию данных, что стимулировало развитие регуляторных мер (в частности, локализацию

данных) как инструментов защиты цифрового суверенитета [8]. К числу других аналогичных работ необходимо отнести монографию Т. Ву «Проклятие технологических гигантов», в которой он анализирует монополизацию цифрового пространства и угрозы для государственного суверенитета, возникающие в данной сфере [9]. К схожим выводам приходит Я. Варуфакис в книге «Технофеодализм» [10].

Правовые аспекты государственного цифрового суверенитета рассмотрены в трудах Э.Л. Сидоренко [11], Т.А. Поляковой, А.А. Смирнова [12].

В последние годы вышел ряд работ, рассматривающих опыт КНР в защите своего цифрового суверенитета. Рассмотрению данной проблемы посвящены исследования К. Кожухова [13], И. Денисова [14], Р. Кримерса [15], И. Хун [16], М. Джианг [17] и др.

Однако многие аспекты этой важной и актуальной темы остаются недостаточно исследованными. В частности, чётко не сформулированы проблемы защиты цифрового суверенитета, средства и методы их возможных решений.

Целью данной статьи является определение основных средств и методов защиты цифрового суверенитета России в условиях формирования глобального цифрового общества.

Угрозы цифровому суверенитету России в глобальном цифровом обществе

В ст. 53 Стратегии Национальной безопасности России 2021 г. отмечается стремление транснациональных IT-корпораций закрепить своё монопольное положение

в сети Интернет и контролировать все информационные ресурсы путём введения по собственному усмотрению цензуры и блокировки альтернативных интернет-платформ, навязывания по политическим причинам пользователям сети Интернет искажённого взгляда на исторические факты, на события, происходящие в России и в мире¹.

В настоящее время основная часть интернет-пользователей в мире предпочитает интернет-продукты таких крупнейших западных IT-корпораций, как Microsoft, Google, Facebook, YouTube и др., которые доминируют на рынке информационных услуг². В руках владельцев этих компаний сосредоточились огромные богатства. Совокупный собственный капитал 20 самых богатых миллиардеров в области искусственного интеллекта превышает 500 млрд долларов³.

При этом особый интерес вызывает тот факт, что формальные владельцы ведущих мировых IT-гигантов (Илон Маск, Ларри Пэйж, Марк Цукерберг, Билл Гейтс и др.) не являются их основными собственниками. Так, например, крупнейший американский инвестиционный фонд Vanguard Group сконцентрировал в своём портфеле крупные пакеты акций Amazon, Microsoft, Apple, Facebook, Google, Visa и др.⁴ В целом, в 2023 г. под управлением Vanguard Group находились активы на сумму 7,6 трлн долларов. При этом имена конечных бенефициаров (основных акционеров) этого фонда официально не разглашаются⁵.

В число основных акционеров крупнейших мировых IT-корпораций входят также инвестиционные фонды BlackRock, име-

¹ Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации». 06.07.2021. URL: <http://www.kremlin.ru/acts/bank/47046/page/1> (дата обращения: 23.12.2025).

² Meta Platform Inc. (соцсети Facebook, Instagram) признана экстремистской, её деятельность запрещена на территории РФ.

³ 20 самых богатых ИИ-миллиардеров в мире. 27.07.2023. <https://mpost.io/ru/the-20-richest-ai-billionaires-in-the-world/> (дата обращения: 14.01.2026).

⁴ Meta Platform Inc. (соцсети Facebook, Instagram) признана экстремистской, её деятельность запрещена на территории РФ.

⁵ Edwards J. Who Owns Vanguard Group? 2023. URL: <https://www.investopedia.com/> (accessed 26.11.2023).

ющие в управлении средства в 12,5 трлн долл., и State Street Corporation с активами 5,1 трлн долл. Три крупнейших указанных выше мировых фонда параллельно владеют частью акций друг друга и на сегодняшний день аккумулируют более 20 трлн долларов, контролируют не только американскую, но и во многом мировую технологическую сферу¹.

Всё это ставит проблему формирования глобального цифрового общества, в котором правящая цифровая элита станет осуществлять цифровое управление, выйдя из-под контроля мирового сообщества и государств, так как ей никто не делегирует полномочия управлять на основе признаваемых в обществе процедур. Уже сегодня она стремится к переходу в перспективе на цифровые методы управления экономикой и обществом во всём мире в своих узкокорыстных интересах.

Как Россия защищает свой цифровой суверенитет

В этой ситуации Россия предпринимает значительные шаги для обеспечения своего цифрового суверенитета, защиты информационного пространства нашей страны, ограждения граждан от негативных информационных воздействий. Сейчас в России уже существуют IT-компании, находящиеся в российской юрисдикции и способные создавать собственные поисковики, видеохостинги, банковские сервисы, социальные сети и т.п. На развитие информационных технологий и коммуникаций в России

с 2026 по 2028 г. планируется направить более 981 млрд рублей².

Главным достижением России в IT-отрасли в 2025 г. стало её присоединение к странам «цифровой триады», т.е. к тем, которые обладают комплексом цифровых сервисов, включающим три элемента: собственную поисковую систему, свои социальные сети и мессенджер. До запуска в России в 2025 г. собственного мессенджера МАХ таким комплексом обладали всего три страны в мире: США с поисковиками Google и Bing, соцсетями Facebook, Instagram и X и мессенджерами iMessage и WhatsApp³; Китай с поисковиком Baidu, соцсетью Weibo и мессенджером WeChat; а также Южная Корея с поисковиком Naver, соцсетями Naver Cafe и Kakao Story и мессенджером KakaoTalk. С запуском в России мессенджера МАХ Россия стала четвёртой страной, обладающей такой триадой, с поисковиком «Яндекс», соцсетями «ВКонтакте» и «Одноклассники» и мессенджером МАХ⁴.

В настоящее время доля отечественного ПО в работе органов государственной власти составляет почти 80%. Кроме того, предполагается, что к 2030 г. не менее 95% российских компаний из ключевых отраслей экономики перейдут на использование базового и прикладного российского ПО в системах, которые обеспечивают основные производственные и управленческие процессы⁵.

Российские граждане зачастую сами не могут отделить правдивую информа-

¹ Cimerman A., Yalalov D. The 20 Richest AI Billionaires in the World. 2023. URL: <https://mpost.io/the-20-richest-ai-billionaires-in-the-world> (accessed 06.01.2026).

² В бюджет на три года заложили почти триллион рублей на развитие ИТ и связи. 2025. URL: <https://www.computerra.ru/325150/v-byudzheth-na-tri-goda-zalozhili-pochti-trillion-rublej-na-razvitie-it-i-svyazi/> (дата обращения: 07.01.2026).

³ Meta Platform Inc. (соцсети Facebook, Instagram) признана экстремистской, её деятельность запрещена на территории РФ.

⁴ Щит, меч и код: Три главные победы России в 2025 году, о которых говорит весь мир. 2025. URL: <https://life.ru/p/1822110> (дата обращения: 08.01.2026).

⁵ Доля отечественного ПО в работе госорганов приблизилась к 80%. 24.07.2025. URL: <https://realnoevremya.ru/news/345662-dolya-otechestvennogo-po-v-rabote-gosorganov-priblizilas-k-80> (дата обращения: 10.01.2026); Путин поручил к 2030 году довести до 95% долю использования российского ПО в госкомпаниях. 07.05.2024 URL: <https://tass.ru/ekonomika/20735947> (дата обращения: 04.01.2026).

цию от ложной. Отсюда одна из главных задач государства в информационной сфере — «фильтрация» неконтролируемого потока информации, обрушивающегося на российских граждан всех возрастов. В то же время правительство РФ в последние пять лет активно борется с антироссийскими действиями транснациональных IT-компаний. Так, например, в 2021 г. Роскомнадзор потребовал от Facebook¹ снять ограничения с трансляции, посвященной 60-летию полёта в космос первого космонавта Юрия Гагарина, назвав подобные действия американской социальной сети нарушением ключевых принципов свободного распространения информации, а также актом цензуры, который не даёт возможности широкой мировой общественности ознакомиться с достижениями России в космосе². Решением правительства с 1 апреля 2021 г. все планшеты и смартфоны с Android и iOS должны включать российские программы «Яндекс.Браузер», поисковик «Яндекс», «Почта Mail.ru», «Новости Mail.ru», «Госуслуги» и другие³.

Развитие отечественной IT-индустрии и нейтрализацию возможных негативных последствий цифровизации необходимо ввести, прежде всего, с опорой на российскую законодательную базу цифрового управления экономикой и обществом. В России действуют Федеральный закон «О персональных данных» от 27.07.2006 г. № 152-ФЗ (с поправками Федерального закона № 242-ФЗ 2015 г.), гарантирующий конфиденциальность персональных данных и право каждого на «цифровое забвение», Федеральный закон от 13.07.2015 г. № 264-ФЗ «О праве на забвение», согласно

которому граждане по заявлению и без решения суда могут требовать удаления из Интернета недостоверной информации о себе.

Россия уделяет большое внимание информационной безопасности, защите персональных данных пользователей. Наша страна присоединилась к Конвенции 1981 г. о защите физических лиц при автоматизированной обработке персональных данных, которую подписала 51 страна (именно на этом документе основан и обязан ему своим появлением отечественный федеральный закон о персональных данных)⁴.

Однако российское законодательство в сфере регулирования Интернета ещё нуждается в совершенствовании. Так, в России до сих пор нет закона об ответственности должностных лиц или организаций за утечку персональных данных российских граждан. Необходимо также законодательное закрепление гражданского контроля за развитием процесса цифровизации и внедрением искусственного интеллекта в управление экономикой и обществом, чтобы цифровизация осуществлялась в интересах всех граждан, а не только отдельных социальных страт, например государственной бюрократии.

Для обеспечения цифрового суверенитета России сегодня необходимо избавляться от влияния транснациональных IT-гигантов. Поэтому в соответствии с Федеральным законом № 236-ФЗ от 01.07.2021 г. «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации», вступившим в силу с 1 января 2022 г., Роскомнадзор обязал 13 зару-

¹ Meta Platform Inc. (соцсети Facebook, Instagram) признана экстремистской, её деятельность запрещена на территории РФ.

² Роскомнадзор требует от Facebook снять ограничения с трансляции про Юрия Гагарина. 2021. URL: <https://www.kp.ru/online/news/4253742/> (дата обращения: 12.01.2026); ФАС возбудила дело против Google. 2021. URL: <https://www.interfax.ru/russia/762066> (дата обращения: 08.01.2026).

³ «Ведомости»: российские программы для предустановки появятся на устройствах Apple. 2021. URL: https://tass.ru/ekonomika/10909671?utm_source=yxnews&utm_medium=desktop (дата обращения: 05.01.2026).

⁴ Борьба за персональные данные, или последний рубеж обороны. 2019. URL: <https://aftershock.news/?q=node/770010> (дата обращения: 25.12.2025).

бежных IT-компаний, в том числе Google, Telegram, Twitter и Meta (бывшая Facebook) до 1 января 2022 г. открыть представительства в России¹. Перечисленные компании обязали размещать на сайте специальную форму для обратной связи с российскими пользователями, завести личный кабинет на сайте Роскомнадзора и установить на сайте счётчик посещаемости. Кроме того, они должны ограничивать доступ к информации, признанной нарушающей российское законодательство, а при их нежелании подчиняться российским законам, у них станут удалять неприемлемый контент, замедлять или блокировать сервисы таких IT-компаний. За нарушение закона IT-компаниям грозит запрет на рекламу, ограничение приёма платежей на территории РФ, запрет на поисковую выдачу, на сбор и передачу за рубеж личных данных, блокировка².

В отличие от развитых западных стран процесс становления в нашей стране цифрового общества находится под значительным контролем государства. В 2018 г. в России было создано министерство цифрового развития, которое координирует деятельность в этом направлении. Это обусловлено, во-первых, тем, что отечественные IT-компании сегодня не в состоянии конкурировать с транснациональными IT-корпорациями; во-вторых, тем, что государство понимает важность процесса развития цифровых технологий и управления, не хочет выпускать этот процесс из-под контроля.

Всё это свидетельствует о том, что российское государство ведёт борьбу за обеспечение своего цифрового суверенитета и имеет твёрдое намерение его укреплять.

Проблемы на пути обеспечения Россией своего цифрового суверенитета

Вместе с тем у России остаётся ещё ряд проблем на пути формирования собственного цифрового суверенитета. Из-за угроз отключения РФ от системы международных расчётов SWIFT в 2025 г. Китай создал собственную систему международных расчётов³. России же пока не удалось создать альтернативную SWIFT платёжную систему на новой технологической основе.

Крупные российские IT-корпорации сегодня стараются делать ту же самую работу меньшим, чем раньше, числом сотрудников, что привело к сокращению доступных вакансий для приёма новых сотрудников.

Уход западных IT-компаний с российского рынка заставил российские фирмы переходить на отечественное программное обеспечение. Теперь вместо Oracle они стали применять PostgreSQL, вместо SAP — 1C. Однако не все российские специалисты умеют работать с отечественными продуктами. Поэтому повысился спрос на тех, кто хорошо знает эти системы. Возникла необходимость срочной перестройки системы образования для обучения молодых специалистов работе на российском оборудовании⁴.

Сегодня в российской IT-отрасли существует дефицит специалистов по информационной безопасности, требуются DevOps-инженеры, потому что компании пытаются перевести свою инфраструктуру на внутренние решения, нужны аналитики и специалисты по данным, потому что бизнес хочет лучше понимать происходящие процессы и принимать решения на основе информации.

¹ Meta Platform Inc. (соцсети Facebook, Instagram) признана экстремистской, её деятельность запрещена на территории РФ.

² Федеральный закон от 01.07.2021 № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации». 2021. URL: <http://publication.pravo.gov.ru/Document/View/0001202107010014?index=37&rangeSize=1> (дата обращения: 28.12.2025).

³ Как Китай стал технологической сверхдержавой. 2025. URL: <https://trends.rbc.ru/trends/innovation/67c8297d9a794709eac7f155> (дата обращения: 08.01.2026).

⁴ Кризис в российском IT-секторе: почему всё одновременно и сразу. 2025. URL: <https://dzen.ru/a/aHVV6ie4QxCta0KC> (дата обращения: 09.01.2026).

Молодые специалисты часто предъявляют завышенные требования по зарплате. В действительности только опытные специалисты, которые способны действительно дать конкретный результат, предложить интересное, конкурентоспособное решение той или иной проблемы, могут рассчитывать на высокие зарплаты. И здесь возникает разрыв: молодёжь хочет получать много, но не способна решать реальные задачи. Работодатели не хотят платить больше, чем позволяет рынок. Всё это приводит к конфликтам и появлению многих незанятых мест.

IT-сектор зависит не только от людей, но и от технической базы. Центры обработки данных перегружены, места в дата-центрах стали дефицитом. Это ограничивает масштабирование проектов и увеличивает стоимость услуг. Кроме того, не все частные пользователи и компании согласны менять привычные инструменты на отечественные аналоги, так как российские продукты зачастую уступают западным по функционалу, интерфейсу, скорости работы и поддержке. Это снижает доверие и желание использовать их постоянно.

В результате российские IT-компании не получают достаточной поддержки от своей целевой аудитории. Это тормозит развитие отрасли и снижает инвестиционную привлекательность. Определённые сложности создаёт и то обстоятельство, что до 2026 г. отечественное ПО из реестра Минцифры продавалось с нулевой ставкой НДС. С 2026 г. она становится рыночной (22%). В 2026 г. в IT-компаниях также повысятся страховые взносы на сотрудников с 7,6% до 15%¹.

Действия российского государства для обеспечения цифрового суверенитета

Однако, по нашему мнению, изложенные выше проблемы российской IT-отрасли со временем могут быть решены. Для

этого необходимы постоянная, последовательная поддержка со стороны государства, создание не только благоприятных условий для развития отечественной IT-отрасли, но и активное инвестирование в информационные технологии, в том числе и в отечественные технологии искусственного интеллекта, робототехники и других перспективных направлений. В этом случае российские IT-компании активно смогут использовать ИИ для оптимизации бизнес-процессов, улучшения пользовательского опыта и создания новых продуктов.

Одним из ключевых факторов, который может способствовать успеху российской IT-отрасли, является поднятие на высокий уровень образования и подготовки кадров в этой сфере, крупные инвестиции в образование, особенно в области STEM (наука, технологии, инженерия и математика). Такая политика в области образования создаст благоприятную среду для развития стартапов, будет мотивировать молодёжь не только получать образование в сфере информационных технологий, но и направлять её на работу в отечественной IT-отрасли.

Важную роль в развитии российской IT-отрасли играет расширение рынка информационных услуг. Такой рынок, отличающийся высокой конкуренцией, заставит компании постоянно совершенствовать свои продукты и услуги, что усилит стимулирование инноваций и будет способствовать быстрому развитию технологий.

В условиях санкций со стороны США и «коллективного Запада», которые ограничивают доступ России к ключевым технологиям и рынкам, важно сделать всё необходимое для создания собственных технологий — например, наладить производство чипов и процессоров, снижая зависимость от западных поставщиков (ил. 2).

¹ Маржа утекает из IT. 2025. URL: <https://www.tbank.ru/invest/social/profile/Investokrat/182e99ff-8c34-4a27-833d-4e55431f0680/?author=profile> (дата обращения: 12.01.2026).

Цифровой суверенитет достигается совместными усилиями и наличием собственных сервисов

 Разработчики и IT-специалисты

 Бизнес и компании

 Государство

 Пользователи



Ил. 2. Как достигается цифровой суверенитет

Проведённое исследование показало, что для обретения цифрового суверенитета России необходимы создание и развитие собственных национальных цифровых ресурсов, а также использование цифровых технологий всеми акторами российского общества и государства в собственных национальных интересах. В глобальном цифровом обществе высокий уровень отечественных IT-технологий становится необходимым и критически важным условием всестороннего, успешного развития

России в новых исторических реалиях, её национальной независимости.

В случае отсутствия возможностей обеспечения собственного цифрового суверенитета современное российское государство окажется перед существенными угрозами и рисками стратегического поражения в глобальном противостоянии с технологически развитыми государствами «коллективного Запада», потерей независимости уже не только в цифровой сфере.

ЛИТЕРАТУРА

1. Шитьков С.В. Подходы к изучению цифрового суверенитета в современной политической науке // Международная жизнь. 2025. № 5. С. 90–99.
2. Ефремов А.А. Формирование концепции информационного суверенитета государства // Право. Журнал Высшей школы экономики. 2017. № 1. С. 201–215.
3. Brokes F. Russia's sovereign internet // Central European Financial Observer. 2018. URL: <https://financialobserver.eu/cse-and-cis/russias-sovereign-internet> (дата обращения: 25.12.2025).
4. Сморгун Л.В. Институты публичного управления Интернетом: сравнительный анализ России, Белоруссии и Казахстана // Управленческое консультирование. 2020. № 12. С. 24–39.
5. Володенков С.В. Феномен цифрового суверенитета современного государства в условиях глобальных технологических трансформаций: содержание и особенности // Журнал политических исследований. 2020. № 4. С. 3–11.
6. Никонов В.А., Воронов А.С., Сажина В.А., Володенков С.В., Рыбакова М.В. Цифровой суверенитет современного государства: содержание и структурные компоненты (по материалам

- экспертного исследования) // Вестник Томского государственного университета. Философия. Социология. Политология. 2021. № 60. С. 206–216.
7. Кочетков А.П., Маслов К.В. Цифровой суверенитет как основа национальной безопасности России в глобальном цифровом обществе // Вестник Московского университета. Серия 12. Политические науки. 2022. № 2. С. 31–45.
 8. Zuboff S. The age of surveillance capitalism // Social theory rewired. Routledge, 2023. Pp. 203–213.
 9. Wu T. The curse of bigness. Penguin Random House, 2018.
 10. Варуфакис Я. Технофеодализм. М.: Ad Marginem, 2025.
 11. Сидоренко Э.Л. Адаптивные возможности российского права в условиях цифровой трансформации // Государственная служба. 2020. Т. 22. № 2 (124). С. 56–63.
 12. Полякова Т.А., Смирнов А.А. Правовое обеспечение международной информационной безопасности: приоритеты для Союзного государства // Право. 2023. № 5. С. 84–92.
 13. Кожухова К.Е. Политика Китая в области обеспечения цифрового суверенитета // Вестник академии военных наук. 2020. № 4. С. 171–176.
 14. Денисов И.Е. Китайская стратегия «больших данных»: реформа управления, инновации и глобальная конкуренция. М.: Издательство «МГИМО-Университет», 2023.
 15. Creemers R. China's conception of cyber sovereignty // Governing cyberspace: Behavior, power and diplomacy. 2020. Pp. 107–145.
 16. Yun H. China's data sovereignty and security: Implications for global digital borders and governance // Chinese Political Science Review. 2024. Pp. 1–26.
 17. Jiang M. Models of State Digital Sovereignty From the Global South: Diverging Experiences From China, India and South Africa // Policy & Internet. 2024. Vol. 16. № 4. Pp. 727–738.

Russia's Digital Sovereignty in the Context of Global Digital Society

Kochetkov Alexander Pavlovich — Doctor of Philosophy, Professor of the Department of Russian Politics, Faculty of Political Science, Lomonosov Moscow State University.
E-mail: apkoch@mail.ru

This article analyzes the challenges associated with the formation of Russia's digital sovereignty within the global digital society. It examines threats to the country's digital sovereignty arising from the process of digitization, as well as the necessary conditions for ensuring such sovereignty given the new historical realities.

Based on the findings of the research, it is concluded that ensuring Russia's digital sovereignty requires the development of domestic digital resources, active and sustained investment in domestic IT, a high level of education and professional training in this field, substantial investment in education, and the existence of a broad market for information services to stimulate competition in the development of IT.

Particular attention is paid to the fact that Russia's digital sovereignty constitutes the primary condition for the country's national independence in the global digital society. The article also outlines the practical activities undertaken by the state to ensure its digital sovereignty.

Keywords: digitalization, digital sovereignty, Russia's national independence, global digital society, transnational IT corporations, national digital resources, investment in IT technologies, state information policy, Russian legislation on Internet regulation, success factors of the Russian IT industry

REFERENCES

1. Shit'kov S.V. Podkhody k izucheniyu tsifrovogo suvereniteta v sovremennoi politicheskoi nauke // Mezhdunarodnaya zhizn'. 2025. № 5. С. 90–99 (in Russian).
2. Efremov A.A. Formirovanie kontseptsii informatsionnogo suvereniteta gosudarstva // Pravo. Zhurnal Vysshei shkoly ekonomiki. 2017. № 1. С. 201–215 (in Russian).
3. Brokes F. Russia's sovereign internet // Central European Financial Observer. 2018. URL: <https://financialobserver.eu/cse-and-cis/russias-sovereign-internet> (data obrashcheniya: 25.12.2025).
4. Smorgunov L.V. Instituty publichnogo upravleniya Internetom: sravnitel'nyi analiz Rossii, Belorussii i Kazakhstana // Upravlencheskoe konsul'tirovanie. 2020. № 12. С. 24–39 (in Russian).
5. Volodenkov S.V. Fenomen tsifrovogo suvereniteta sovremennogo gosudarstva v usloviyakh global'nykh tekhnologicheskikh transformatsii: sodержanie i osobennosti // Zhurnal politicheskikh issledovaniy. 2020. № 4. С. 3–11 (in Russian).
6. Nikonov V.A., Voronov A.S., Sazhina V.A., Volodenkov S.V., Rybakova M.V. Tsifrovoy suverenitet sovremennogo gosudarstva: sodержanie i strukturnye komponenty (po materialam ekspertnogo issledovaniya) // Vestnik Tomskogo gosudarstvennogo universiteta. Filosofiya. Sotsiologiya. Politologiya. 2021. № 60. С. 206–216 (in Russian).
7. Kochetkov A.P., Maslov K.V. Tsifrovoy suverenitet kak osnova natsional'noi bezopasnosti Rossii v global'nom tsifrovom obshchestve // Vestnik Moskovskogo universiteta. Seriya 12. Politicheskie nauki. 2022. № 2. С. 31–45 (in Russian).
8. Zuboff S. The age of surveillance capitalism // Social theory rewired. Routledge, 2023. Pp. 203–213.
9. Wu T. The curse of bigness. Penguin Random House, 2018.
10. Varufakis Ya. Tekhnofeodalizm. M.: Ad Marginem, 2025 (in Russian).
11. Sidorenko E.L. Adaptivnye vozmozhnosti rossiiskogo prava v usloviyakh tsifrovoy transformatsii // Gosudarstvennaya sluzhba. 2020. T. 22. № 2 (124). С. 56–63 (in Russian).
12. Polyakova T.A., Smirnov A.A. Pravovoe obespechenie mezhdunarodnoi informatsionnoi bezopasnosti: priority dlya Soyuznogo gosudarstva // Pravo. 2023. № 5. С. 84–92 (in Russian).
13. Kozhukhova K.E. Politika Kitaya v oblasti obespecheniya tsifrovogo suvereniteta // Vestnik akademii voennykh nauk. 2020. № 4. С. 171–176 (in Russian).
14. Denisov I.E. Kitaiskaya strategiya «bol'shikh dannykh»: reforma upravleniya, innovatsii i global'naya konkurentsia. M.: Izdatel'stvo «MGIMO-Universitet», 2023 (in Russian).
15. Creemers R. China's conception of cyber sovereignty // Governing cyberspace: Behavior, power and diplomacy. 2020. Pp. 107–145.
16. Yun H. China's data sovereignty and security: Implications for global digital borders and governance // Chinese Political Science Review. 2024. Pp. 1–26.
17. Jiang M. Models of State Digital Sovereignty From the Global South: Diverging Experiences From China, India and South Africa // Policy & Internet. 2024. Vol. 16. № 4. Pp. 727–738.