

ТЕОРЕТИЧЕСКИЕ И КОНЦЕПТУАЛЬНЫЕ ОСНОВАНИЯ ЦИФРОВОГО СУВЕРЕНИТЕТА

Индекс УДК 338.2, 327

Код ГРНТИ 06.54.31

DOI: 10.22204/2587-8956-2026-124-01-13-22

**И.В. ДАНИЛИН***

Современные проблемы, специфика и требования к цифровому суверенитету: анализ мирового опыта**

На основе анализа научной литературы и документов систематизированы проблемы и функциональные области цифрового суверенитета различных стран мира. В качестве первичных проблем выделены вопросы цифровой независимости, в том числе усиления собственного экономического и технологического потенциала, противодействия цифровому монополизму крупных платформенных корпораций США, а ныне — и КНР. В последние годы в этом же контексте реализуются меры по развитию национальных микроэлектронных комплексов. Далее, это проблема цифровых гражданских прав и их защиты (включая модельные законы и нормы Евросоюза, ставшие общепризнанными основами цифрового регулирования). Наконец, в числе основных проблем современного цифрового суверенитета выделяются безопасность (в широком определении термина, с учётом секьюритизации и вепонизации цифровых технологий) и геополитика. Анализ мирового опыта также позволяет выделить условия, требования и специфику его реализации. Помимо общих, системных вопросов, наибольшее значение для эффективной политики в сфере цифрового суверенитета имеют целеполагание, учёт и интеграция экономических, социальных, политических и иных задач, а также взаимосвязанный вопрос вовлечения различных внешних субъектов и заинтересованных. В условиях глобализации всё большее значение приобретает также экстернализация цифрового суверенитета, включая создание альянсов, глобализацию и гармонизацию норм и иные меры. Сформированы рекомендации в отношении российской политики в сфере цифрового суверенитета: рост национального диалога и государственно-частных партнёрств, формирование российского стека технологий и подходов цифрового суверенитета и диалог со странами-партнёрами, а также актуализация новых направлений цифрового суверенитета, включая культуру, сохранение идентичности коренных народов и пр.

* **Данилин Иван Владимирович** — кандидат политических наук, заместитель директора по научной работе Национального исследовательского института мировой экономики и международных отношений им. Е.М. Примакова РАН.
E-mail: danilin.iv@imemo.ru

** Статья подготовлена при поддержке гранта Министерства науки и высшего образования РФ на проведение крупных научных проектов по приоритетным направлениям научно-технологического развития № 075-15-2024-551 «Глобальные и региональные центры силы в формирующемся мироустройстве».

Ключевые слова: цифровой суверенитет, Европейский союз, США, Китай, Индия, развивающиеся страны, цифровые технологии, международные отношения в цифровой сфере

Цифровой суверенитет (ЦС) является одним из наиболее сложных и дискуссионных вопросов в исследованиях и реальной практике. Развитие цифровых технологий, процессы цифровизации экономики и осознание этих проблем элитами ведут к актуализации ЦС [1] и расширению его проблематики. Особенно это верно в условиях всплеска геополитической конфликтности и технологических изменений, включая «революцию» генеративного искусственного интеллекта (ИИ).

К настоящему времени накоплены существенный опыт и теоретические разработки в сфере ЦС. Их изучение важно как с научной, так и с практической точек зрения, в частности для уточнения российских подходов, определения глобального ландшафта реализации российской политики ЦС, в том числе для выстраивания диалога с дружественными странами. Этим задачам и посвящена данная статья. Основное внимание мы уделим функциональным аспектам феномена ЦС, специфике и требованиям к его обеспечению.

Цифровой суверенитет: генезис и содержание понятия

Истоки формирования дискурсов и практик ЦС можно отнести к середине 1990-х гг., хотя сам термин стал вводиться в оборот только со второй половины десятилетия (см. [2]). Мощный всплеск дискуссий и реальной деятельности в сфере ЦС приходится, однако, на 2010-е гг., когда этот термин появляется, например, в европейских документах [3]. Это было обусловлено новыми тенденциями и вызовами, начиная от развития интернет-экономики и реакций на формирование

охранительной китайской цифровой политики до громких разоблачений Э. Сноудена в 2013 г. [4].

Несмотря на продолжительный период развития, понятие «цифровой суверенитет» не имеет чёткого определения, разделяемого большинством исследователей и практиков [2, 5, 6]. Существуют разные интерпретации — вплоть до иерархии функциональных «уровней» ЦС (ил. 1). Де-факто ЦС является «зонтичным» термином, объединяющим разные процессы, подходы, вызовы и пр. Причём содержание понятия, перечень вызовов и угроз, инструментарий и даже объекты и субъекты ЦС постоянно меняются вследствие как объективных изменений, так и конъюнктурных факторов (например, стремления Еврокомиссии расширить свои полномочия за счёт ранее чисто «национальной» сферы безопасности [7]). Ситуацию осложняет то, что не всегда мероприятия, подпадающие под определение «цифрового суверенитета», воспринимаются как таковые. И наоборот, не все действия, де-юре связанные с ЦС, относятся к цифровому суверенитету.

Тем не менее можно выделить несколько взаимосвязанных проблемных областей ЦС, сложившихся исторически, определяющих содержание и политические практики разных стран мира.

Первичной является проблема цифровой независимости, наиболее актуальной в качестве смыслового «ядра» ЦС едва ли не для всех стран мира, в том числе наиболее развитых [9, 10].

Истоком проблемы следует признать реакцию на вызов монополизации цифровых рынков со стороны американских цифровых корпораций. Рыночное доми-

нирование Microsoft, а позднее Google, Amazon, Apple, Facebook/Meta¹ и иных компаний, рассматривалось как риск для формирования национальных цифровых потенциалов, конкуренции и цифровых прав граждан разных стран [7]. В настоящее время, несмотря на сохраняющийся антиамериканский акцент (от ЕС и КНР до ряда стран АСЕАН), проблематика цифрового монополизма применяется и к китайским цифровым гигантам в развивающихся странах [1].

Меры противодействия везде различаются. Не считая РФ, попытки создать национальные противовесы американским корпорациям удалось только в КНР за счёт достаточно жёсткой политики ограничения доступа на национальные рынки. В ЕС попытки создать европейский аналог Google [11] или усилить потенциал в цифровой сфере за счёт масштабных программ НИОКР успеха не имели. Более результативной оказалась мировая практика рыночных ограничений: от ужесточения требований к обращению с данными и до блокировки приложений, как в случае с китайскими сервисами в Индии.

Актуальность этих мер росла благодаря совпадению с иными значимыми национальными задачами и идейно-идеологическими конструктами. С одной стороны, это цифровой протекционизм и импортозамещение, а также антимонопольное регулирование цифровых рынков. С другой – антиколониальные дискурсы (в цифровой реальности колонизируемыми оказались как развивающиеся, так и развитые государства), в частности вопросы «колониализма данных», ставшие значимыми в условиях развития интернет-монополий и ИИ. Расширились и границы понимания «цифровой независимости». Так, с началом технологического конфликта США с КНР и пандемии COVID-19 её важным



Ил. 1. «Иерархия» уровней цифрового суверенитета.

Составлено автором на основе схемы в [8]

элементом стал вопрос о выпуске высокопроизводительных чипов как физическом условии ЦС [3, 7].

«Цифровая независимость» сближает ЦС с традиционным суверенитетом: контроль над цифровым и информационным «пространством» (включая локализацию хранения данных и необходимой инфраструктуры) и недопущение подобного контроля со стороны третьей силы, государств или иностранных корпораций [12].

Другим значимым направлением современного ЦС является проблематика защиты гражданских цифровых прав, начиная от конфиденциальности (privacy) и до более широкого концепта личных данных как собственности и неотъемлемого права граждан.

Можно утверждать, что изначально этот аспект ЦС стал следствием европейского понимания суверенитета, связанного с традицией Ж.-Ж.Руссо, где народ, а не государство, выступает основным источником ЦС, и, шире, подхода ЕС к проблеме гражданских прав. Впрочем, были и отдельные экономические соображения (пресечение несправедливого и монопольного извлечения ренты из больших данных), сбли-

¹ Признана экстремистской и запрещена на территории Российской Федерации.

жающие этот блок проблем с доменом независимости и антиколониализма.

В части «цифровой независимости» наблюдалась проекция на сферу ЦС классических подходов и методов протекционизма, импортозамещения, суверенитета. «Гражданская» защита данных потребовала отдельной проработки. Полноценное регулирование было сформировано лишь в середине 2010-х гг. Драйвером стал ЕС, который с учётом мощных экономических практик и регуляторных наработок (с введения в 1995 г. Директивы по защите данных, DPD) создал набор модельных подходов и инструментов: от Общего регламента по защите данных (GDPR, утверждён в 2016 г., введён в действие в 2018 г.) и до Закона по ИИ 2023 г. Неудивительно, что безотносительно к идейно-политической базе «гражданского» ЦС элементы GDPR и иных документов ЕС определяют повестку разных стран мира в части защиты данных.

Традиционной проблематикой ЦС была и остаётся безопасность в широком смысле этого понятия. Помимо рисков для критических инфраструктур, угроз разведывательного характера, кибертерроризма и тому подобных условно-объективных проблем, это направление активно развивается вследствие секьюритизации ЦС. Наблюдается реактуализация и предельное расширение понимания информационных рисков и угроз, включая влияние на внутренние политические процессы, ценности, идеологию (вплоть до утери идентичности из-за злонамеренных действий Иного [12]). Одновременно происходят секьюритизация и вепонизация материальной базы ЦС, прилагаются усилия по развитию национальной цифровой инфраструктуры и системы ограничений против попыток стран-оппонентов получить доступ к национальным цифровым технологиям и компетенциям [14].

Наконец, американо-китайское противостояние, конфликт с Россией и рост трансатлантических противоречий расширили проблематику ЦС с учётом геополитиче-

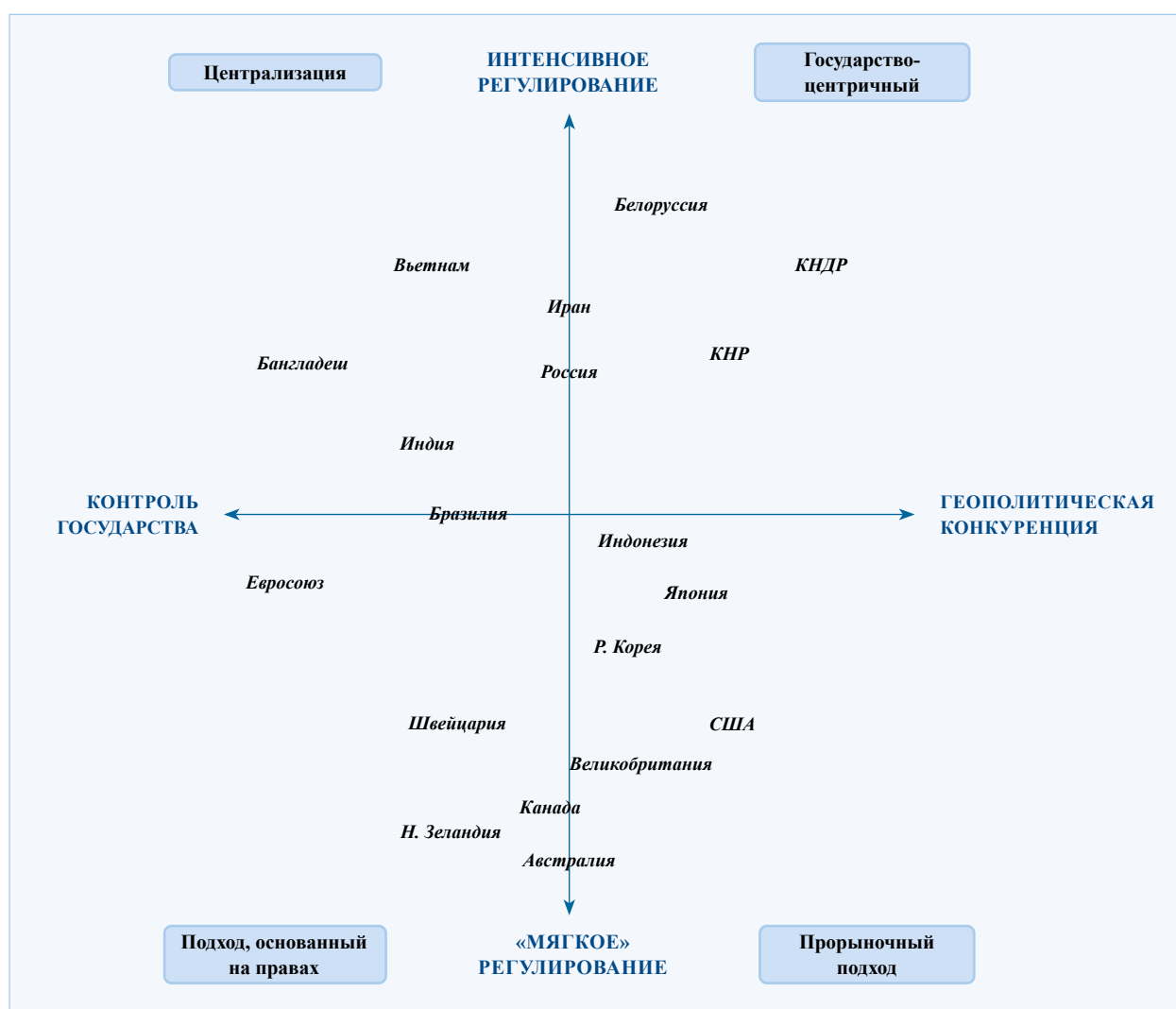
ских соображений [7]. Будучи формально частью более широких проблем безопасности, геополитика ЦС сформировала и новые задачи, включая «глобальное противодействие» усилиям тех или иных стран по захвату цифрового пространства и рынков.

Особенности обеспечения современного цифрового суверенитета в мире

Учитывая подробное описание в литературе различных мероприятий и теоретических аспектов ЦС, а также систематизацию моделей обеспечения ЦС в разных странах (ил. 2), полезно выявить ключевые особенности формирования и реализации ЦС.

Самоочевидным вопросом является чётко прослеживаемая связь ЦС с национальным потенциалом, развитие которого оказывается важнейшей смежной задачей, и, прежде всего, с ролью субъектов ЦС. Так, если для КНР и США феномен ЦС всегда неразрывно связывался с усилением национальных цифровых корпораций и технологического сектора, то для ЕС была актуальна только «защитная» логика противодействия бесконтрольной экспансии американских и китайских компаний. В Африке и Латинской Америке в силу слабой способности в настоящее время сформировать собственных игроков, вопрос замыкается либо на выбор внешнего партнёра — от поставщиков решений до подходов к регулированию («агентная» логика обеспечения ЦС), либо на балансирование между центрами силы [1, 9]. Особняком стоят Индия [9, 15] и до 2022 г. — Россия, которые направленно формировали своих цифровых акторов и актантов (в случае с Индией — набор цифровых платформ, сервисов и инструментов, India Stack) без жёстких ограничений для компаний из третьих стран.

Очевидно также, что в каждом домене ЦС всё более тесно переплетаются политические, социальные и экономические, в том числе чисто коммерческие, вопросы. Как уже упоминалось, вопрос о данных рассматривается в категории не только



Ил. 2. Модели реализации цифрового суверенитета.

Источник: [4]

гражданственности, но и собственности, включая экономические эффекты, возникающие от использования «больших данных» [12]. Это указывает на уже существующие практику и требование учёта всех изложенных соображений, целей и интересов как в определении модели ЦС, так и в реализации мер по его обеспечению.

Последнее ещё раз подчёркивает значение проблемы агентности ЦС. Хотя органы власти де-юре остаются ключевыми игроками в данной сфере, только системный диалог между всеми заинтересованными сторонами оказывается гарантией оптимизации ЦС, его надёжного (вос)производства и обеспечения (так называемый *multistakeholderism* [4]).

Это особенно значимо, учитывая, что современное понимание ЦС, его носителей и источников выходит за рамки предельно агрегированных понятий (государство, народ и т.п.). Носителями «особых» форм ЦС могут выступать даже отдельные группы населения, например коренные народы (США, Австралия, Новая Зеландия [4, 9]).

Наконец, вынужденно многосторонний характер современного ЦС имеет и международное измерение. Опустим важные, но очевидные примеры вепонизации технологий как фактора ослабления потенциала оппонента, которое воспринимается элитами как способ обеспечения собственного ЦС. Налицо системная экстернализация ЦС в условиях глобализированного мира.



Ил. 3. Современный открытый экстернализованный цифровой суверенитет (логическая схема).

Источник: составлено автором

Так, учитывая объективную ограниченность научно-технологического, производственного, инфраструктурного и компетенционного потенциала в сфере цифровых технологий, для большинства стран классические «вестфальские» подходы к обеспечению ЦС оказываются нерелевантны. Цена такого «закрытого» ЦС в условиях международного разделения труда и специализации становится неподъёмной даже для США.

Несмотря на периодические попытки роста «закрытости» ЦС, всё более выражена логика «стратегической автономии» и «открытого (техно)суверенитета». Изначально она была концептуализирована ЕС, но де-факто реализуется большинством стран мира [1, 3, 9, 10, 15, 16]. Данная логика предполагает опору (где возможно) на собственные силы с формированием широких международных партнёрств и иных способов гарантированного доступа к необходимым технологиям. Разумеется, не все области ЦС могут быть реализованы в этой логике. Например, сложно себе представить «партнёрское» хранение и защиту национальных данных. Однако,

например, уже создание системы ЦОД оказывается безальтернативно «открытым» процессом. В данной сфере даже наиболее развитые страны вынуждены полагаться на внешние технико-технологические ресурсы, как в случае с проектом GAIA-X в ЕС, где де-факто одну из ведущих ролей выполняют те самые цифровые гиганты США, которых Европа принуждает локализовать хранение данных [7, 13].

Не говоря об очевидности глобализации технических стандартов, важнейшим аспектом экстернализации оказывается гармонизация и/или глобализация норм ЦС. Опять же, показателен опыт ЕС. По сравнению с США и КНР Европа имеет несопоставимо более слабый цифровой сектор. Но за счёт превращения собственных норм в модельные и их глобализации ЕС частично компенсирует асимметричную цифровую зависимость от партнёров, попутно усиливая свою глобальную «нормативную» власть [7]. При всех различиях в акцентах другие игроки следуют этому же правилу. США — в части продвижения идеологии «свободной торговли»

и де-факто — своих норм регулирования цифровых рынков. КНР также продвигает глобализацию своих подходов: от двусторонних отношений по линии Цифрового Шёлкового пути и до Глобальной инициативы в сфере безопасности данных [1]. Свои подходы для развивающихся стран предлагает и Индия.

Заметим, что эти же факты говорят о том, что, несмотря на рост национального, суверенного начала в мировой цифровой экономике (т.е. развитие ЦС в классическом понимании термина «суверенитет»), определённая кооперативность оказывается неизбежной даже на уровне отношений центр—периферия (ил. 3).

Мировой опыт борьбы за цифровой суверенитет: уроки для России

Формально ЦС может быть описан через условно-универсальные решения (например, национальные ЦОД) и «базовое» понимание проблем независимости, прав и безопасности в контексте ЦС. Тем не менее его реальное обеспечение является своего рода равнодействующей вызовов, потенциала, национальных задач и прочих аспектов — вплоть до национальной культуры и юридической системы, но с учётом определённых подходов и принципов, а также международных условий.

С этой точки зрения мировой опыт позволяет сделать ряд обоснованных выводов о ЦС России.

Наша страна входит в число «парадоксальных лидеров» ЦС. Будучи экономикой среднего размера (по мировым меркам), имея сравнительно небольшой цифровой сектор и низкие затраты на НИОКР, Россия является одним из лидеров цифровизации в ряде секторов экономики — от финансов до ритейла, активно разрабатывает прорывные технологии, включая ИИ, а также имеет сильные международные цифровые корпорации (Яндекс, Mail.ru Group, Сбер, во всё большей мере также Wildberries, Ozon и пр.).

Опустим очевидные вопросы по микроэлектронике, иные критические уязвимо-

сти отечественной цифровой экономики и технологического суверенитета, как и объективную потребность роста инвестиций в инновационно-технологический сектор, науку и производство. Представляется, что как минимум несколько аспектов мирового опыта ЦС имеют для нашей страны принципиальное значение.

Прежде всего, речь идёт об умеренной коррекции подходов к формированию политики в сфере ЦС. С одной стороны, это рост качества целеполагания и — шире — интеграции подходов ЦС с долгосрочными задачами развития страны. Особенно это важно с учётом тесного переплетения экономики, политики, социально-культурных аспектов в современном ЦС. С другой стороны, реализация этого процесса требует расширения коммуникации между ключевыми интересантами, включая бизнес, научное и экспертное сообщества. Наряду с форсайтом или тому подобными партисипативными практиками управления можно говорить о более активной работе отраслевых ассоциаций, государственно-частных партнёрствах и мероприятиях по совместной разработке полноценного регулирования, стандартов и технологий как основы российского «стека» ЦС.

Очевидно, требуются и существенные усилия по экстернализации отечественного ЦС. За пределами частично очень общего, частично, напротив, очень специализированного диалога в рамках БРИКС, в иных международных форматах и в рамках двусторонних отношений российские практика и подходы к ЦС требуют роста коммуникации и кооперации. Наряду с лучшим пониманием позиции РФ важна гармонизация интересов и подходов — вплоть до совместных НИОКР для реализации «открытого» ЦС, отработки совместных «стеков» ЦС и иных инициатив. Это тем более верно, что на глобальном уровне российская позиция по ЦС достаточно спорна и воспринимается или как исключительно «внутренняя» проблема, или как фрагментарный набор надёжных решений в идеологии «третьего поставщика».

Заметим, что с учётом постоянного расширения границ феномена ЦС, России есть что предложить для развития его идей. Например, это касается этнокультурной сферы, которая пока даже не воспринимается как важная часть российского «гражданского» ЦС. Это цифровое сохранение и воспроизводство культурно-исторических памятников, нематериального наследия, поддержка коренных народов и многие иные направления.

Наконец, отметим компетенционный вопрос. Защита ЦС, цифровых прав и свобод, доступность данных как одна из интерпретаций ЦС включают в себя способность индивида реализовывать свои цифровые интересы [12]. Опуская фундаментальный

вопрос о кадрах ЦС [4, 10], сделать это без роста массовых цифровых компетенций граждан, включая таргетированный подход к отдельным группам населения, невозможно. Как невозможно реализовать ЦС в условиях ограничений цифровизации для компаний реального сектора экономики вплоть до малых и средних предприятий.

Только комплексный и инновационный подход к ЦС, отказ от шаблонных мер и интерпретаций ЦС через боденовско-вестфальские фильтры или практики XX в., а также более глубокое международное измерение способны обеспечить истинный цифровой суверенитет России и глобализацию её подходов в интересах как самой РФ, так и стран-партнёров.

ЛИТЕРАТУРА

1. Bu Q. Data sovereignty in Africa: steering digital transformation between China and the West // International Cybersecurity Law Review. 2025. Pp. 1–15. DOI: 10.1365/s43439-025-00165-1.
2. Popova E., Ustyuzhantseva O., Gao H. Constructing Digital Sovereignty in Russian and Chinese Media: Big Data Analysis // Вестник РУДН. Серия: Международные отношения. 2025. Vol. 25 (2). Pp. 251–266. DOI: 10.22363/2313-0660-2025-25-2-251-266.
3. Романова Т.А. Эволюция концепции «цифровой суверенитет» в Евросоюзе: константы и дихотомии // Современная Европа. 2023. № 4. С. 62–76. DOI: 10.31857/S0201708323040022.
4. Fratini S., Hine E., Novelli C., Roberts H., Floridi L. Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models // Digital Society. 2024. № 3 (59). Pp. 1–27. DOI: 10.1007/s44206-024-00146-7.
5. Hummel P., Braun M., Tretter M., Dabrock P. Data sovereignty: A review // Big Data & Society. 2021. № 8 (1). Pp. 1–17. DOI: 10.1177/2053951720982012.
6. Jansen B., Kadenko N., Broeders D., van Eeten M., Borgolte K., Fiebig T. Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions // Government Information Quarterly. 2023. Vol. 40. Pp. 1–13. DOI: 10.1016/j.giq.2023.101862.
7. Broeders D., Cristiano F., Kaminska M. In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions // Information, Communication and Society. 2025. 28 (10). Pp. 1721–1734. DOI: 10.1080/1369118X.2024.2332624.
8. The Evolution of Digital Sovereignty: Moving Beyond Data and Cloud // International Data Corporation. 2023. Jan. 13 [Электронный документ]. URL: <https://www.idc.com/resource-center/blog/the-evolution-of-digital-sovereignty-moving-beyond-data-and-cloud/> (дата обращения: 02.02.2026).
9. 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. DOI: 10.1002/poi.3427.
10. Симонова Л.Н., Пономарев Е.А. Цифровой суверенитет, вызовы и риски цифровизации в Латинской Америке // Латинская Америка. 2023. № 11. С. 6–22. DOI: 10.31857/S0044748X0028265-0.
11. Germans pull out of European bid to rival Google // The Guardian. 2006. 28 Dec. [Электронный документ]. URL: <https://www.theguardian.com/technology/2006/dec/28/news.germany> (дата обращения: 02.02.2026).

12. Braun M., Hummel P. Is digital sovereignty normatively desirable? // Information, Communication & Society. 2025. № 28 (10). Pp. 1721–1734. DOI: 10.1080/1369118X.2024.2332624.
13. Santaniello M. Attributes of Digital Sovereignty: A Conceptual Framework // Geopolitics. 2025. Pp. 1–22. DOI: 10.1080/14650045.2025.2521548.
14. Данилин И.В. Экономическая безопасность цифровых технологий на примере полупроводников // Пути к миру и безопасности. 2025. № 1 (68). С. 26–39. DOI: 10.20542/2307-1494-2025-1-26-39.
15. Устюжанцева О.В. Особенности управления цифровой экономикой на примере истории вопроса о локализации данных в Индии // Азия и Африка сегодня. 2025. № 2. С. 42–50. DOI: 10.31857/S0321507525020054.
16. Данилин И., Сидорова Е.А. Концепция технологического суверенитета в меняющемся мире // Журнал Новой экономической ассоциации. 2024. № 3 (64). С. 238–243. DOI: 10.31737/22212264_2024_3_238-243.

Contemporary Problems, Specifics, and Requirements of Digital Sovereignty: Analysis of Global Experience

Danilin Ivan Vladimirovich — Candidate of Political Sciences, Deputy Director for Research at Primakov National Research Institute of World Economy and International Relations of the Russian Academy of Sciences.

E-mail: danilin.iv@imemo.ru

Based on the analysis of scientific sources and policy documents, this study systematizes the challenges and functional aspects of digital sovereignty across different countries. The primary issues identified include: digital independence (i.e., strengthening domestic economic and technological capacity, countering the digital monopolism of large U.S. platform corporations, and more recently, those based in China). In this context, in recent years measures aimed at developing national microelectronics complexes have also been implemented. The second major issue concerns digital civil rights and their protection, including the model laws and standards of the European Union, which have become broadly accepted foundations of digital regulation. Lastly, among the key contemporary challenges of digital sovereignty are security (understood broadly, accounting for the securitization and weaponization of digital technologies) and geopolitics. The analysis of global experience further reveals specific conditions, requirements, and contextual nuances for implementing digital sovereignty. Beyond general systemic issues, effective digital sovereignty policy critically depends on clear goal-setting, the integration of economic, social, political, and other objectives, and the related challenge of engaging diverse external actors and stakeholders. In the context of globalization, the externalization of digital sovereignty, along with building alliances, globalization, harmonization of norms, and other mechanisms, is gaining increasing importance. Based on these findings, the article offers recommendations regarding the Russian digital sovereignty policy: strengthening national dialogue and public-private partnerships; developing a domestic stack of technologies and digital sovereignty frameworks; maintaining dialogue with partner countries; and updating emerging areas of digital sovereignty, including culture and the preservation of indigenous identities, among others.

Keywords: digital sovereignty, European Union, USA, China, India, developing economies, digital technologies, international relations in the digital sphere

REFERENCES

1. Bu Q. Data sovereignty in Africa: steering digital transformation between China and the West // International Cybersecurity Law Review. 2025. Pp. 1–15. DOI: 10.1365/s43439-025-00165-1.
2. Popova E., Ustyuzhantseva O., Gao H. Constructing Digital Sovereignty in Russian and Chinese Media: Big Data Analysis // Vestnik RUDN. Seriya: Mezhdunarodnye otnosheniya. 2025. Vol. 25 (2). Pp. 251–266. DOI: 10.22363/2313-0660-2025-25-2-251-266 (in Russian).
3. Romanova T.A. Evolyutsiya kontseptsii «tsifrovoy suverenitet» v Evrosoyuze: konstanty i dikhoto-mii // Sovremennaya Evropa. 2023. № 4. С. 62–76. DOI: 10.31857/S0201708323040022 (in Russian).
4. Fratini S., Hine E., Novelli C., Roberts H., Floridi L. Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models // Digital Society. 2024. № 3 (59). Pp. 1–27. DOI: 10.1007/s44206-024-00146-7.
5. Hummel P., Braun M., Tretter M., Dabrock P. Data sovereignty: A review // Big Data & Society. 2021. № 8 (1). Pp. 1–17. DOI: 10.1177/2053951720982012.
6. Jansen B., Kadenko N., Broeders D., van Eeten M., Borgolte K., Fiebig T. Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions // Government Information Quarterly. 2023. Vol. 40. Pp. 1–13. DOI: 10.1016/j.giq.2023.101862.
7. Broeders D., Cristiano F., Kaminska M. In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions // Information, Communication and Society. 2025. 28 (10). Pp. 1721–1734. DOI: 10.1080/1369118X.2024.2332624.
8. The Evolution of Digital Sovereignty: Moving Beyond Data and Cloud // International Data Corporation. 2023. Jan. 13 [Elektronnyi dokument]. URL: <https://www.idc.com/resource-center/blog/the-evolution-of-digital-sovereignty-moving-beyond-data-and-cloud/> (data obrashcheniya: 02.02.2026).
9. 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. DOI: 10.1002/poi.3427.
10. Simonova L.N., Ponomarev E.A. Tsifrovoy suverenitet, vyzovy i riski tsifrovizatsii v Latinskoi Amerike // Latinskaya Amerika. 2023. № 11. С. 6–22. DOI: 10.31857/S0044748X0028265-0 (in Russian).
11. Germans pull out of European bid to rival Google // The Guardian. 2006. 28 Dec. [Elektronnyi dokument]. URL: <https://www.theguardian.com/technology/2006/dec/28/news.germany> (data obrashcheniya: 02.02.2026).
12. Braun M., Hummel P. Is digital sovereignty normatively desirable? // Information, Communication & Society. 2025. № 28 (10). Pp. 1721–1734. DOI: 10.1080/1369118X.2024.2332624.
13. Santaniello M. Attributes of Digital Sovereignty: A Conceptual Framework // Geopolitics. 2025. Pp. 1–22. DOI: 10.1080/14650045.2025.2521548.
14. Danilin I.V. Ekonomicheskaya bezopasnost' tsifrovyykh tekhnologii na primere poluprovodnikov // Puti k miru i bezopasnosti. 2025. № 1 (68). С. 26–39. DOI: 10.20542/2307-1494-2025-1-26-39 (in Russian).
15. Ustyuzhantseva O.V. Osobennosti upravleniya tsifrovoy ekonomikoi na primere istorii voprosa o lokalizatsii dannykh v Indii // Aziya i Afrika segodnya. 2025. № 2. С. 42–50. DOI: 10.31857/S0321507525020054 (in Russian).
16. Danilin I., Sidorova E.A. Kontseptsiya tekhnologicheskogo suvereniteta v menyayushchem-sya mire // Zhurnal Novoi ekonomicheskoi assotsiatsii. 2024. № 3 (64). С. 238–243. DOI: 10.31737/22212264_2024_3_238-243 (in Russian).