

Научная статья

УДК 94:32:004(73)(470)(510)

DOI: 10.18384/2949-5164-2025-5-173-189

ЦИФРОВОЙ СУВЕРЕНИТЕТ В ГЛОБАЛЬНОЙ ПОЛИТИКЕ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ СТРАТЕГИЙ США, РОССИИ И КИТАЯ

Безрученко М. П., Ткачёва Т. О.

Кубанский государственный университет

г. Краснодар, Российская Федерация

** Корреспондирующий автор, e-mail: marina.telenga@gmail.com*

Поступила в редакцию 18.08.2025

После доработки 16.09.2025

Принята к публикации 26.10.2025

Аннотация

Цель. Выявление особенностей трактовки и реализации цифрового суверенитета в контексте национальных стратегий США, России и Китая, а также анализа влияния данных подходов на международные отношения и глобальное управление интернетом.

Процедуры и методы. Исследование опирается на концепцию фрейм-анализа для изучения научных публикаций и источников. Дополнительно применяется сравнительный анализ для сопоставления подходов к цифровому суверенитету в США, России и Китае с учётом исторических, культурных и политических особенностей. Качественный анализ текстов на русском, английском и китайском языках позволяет выявить ключевые нарративы и практики в данной области.

Результаты. Исследование демонстрирует доминирование США в цифровом пространстве. В свою очередь, Россия и Китай стремятся противостоять этой гегемонии. Россия фокусируется на защите национального сегмента интернета и снижении зависимости от западных технологий, в то время как Китай развивает автономную цифровую экосистему, опираясь на государственный контроль и культурно-историческую специфику.

Теоретическая и/или практическая значимость. Исследование расширяет понимание трансформации классического понятия суверенитета в цифровую эпоху. Результаты исследования предоставляют инструментарий для анализа национальных стратегий цифрового суверенитета и их влияния на международные отношения.

Ключевые слова: цифровая гегемония, цифровой суверенитет, информационный суверенитет, золотой щит, РФ, КНР, США

Для цитирования:

Безрученко М. П., Ткачёва Т. О. Цифровой суверенитет в глобальной политике: сравнительный анализ стратегий США, России и Китая // Вестник Государственного университета просвещения. Серия: История и политические науки. 2025. № 5. С. 173–189.

DOI: 10.18384/2949-5164-2025-5-173-189

Original research article

DIGITAL SOVEREIGNTY IN GLOBAL POLITICS: A COMPARATIVE ANALYSIS OF THE STRATEGIES OF THE USA, RUSSIA AND CHINA

M. Bezruchenko*, T. Tkachoyva

Kuban State University

Krasnodar, Russian Federation

* Corresponding author, e-mail: marina.telenga@gmail.com

Received 18.08.2025

Revised 16.09.2025

Accepted 26.10.2025

Abstract

Aim. The purpose of the study is to identify the specifics of the interpretation and implementation of digital sovereignty in the context of the national strategies of the United States, Russia and China, as well as to analyze the impact of these approaches on international relations and global Internet governance.

Methodology. The study relies on the concept of frame analysis to study scientific publications and sources. Additionally, comparative analysis is used to compare approaches to digital sovereignty in the United States, Russia and China, taking into account historical, cultural and political features. Qualitative analysis of texts in Russian, English and Chinese allows us to identify key narratives and practices in this area.

Results. The study demonstrates the dominance of the United States in the digital space. In turn, Russia and China seek to counter this hegemony. Russia focuses on protecting the national segment of the Internet and reducing dependence on Western technologies, while China is developing an autonomous digital ecosystem, relying on state control and cultural and historical specifics.

Research implications. The study expands the understanding of the transformation of the classical concept of sovereignty in the digital age. The results of the study provide tools for analyzing national digital sovereignty strategies and their impact on international relations.

Keywords: digital hegemony, digital sovereignty, information sovereignty, golden shield, Russian Federation, USA, PRC

For citation:

Bezruchenko, M. P. & Tkachoyva, T. O. (2025). Digital sovereignty in global politics: a comparative analysis of the strategies of the USA, Russia and China. In: *Bulletin of Federal State University of Education. Series: History and Political Sciences*, 5, 173–189.

DOI: 10.18384/2949-5164-2025-5-173-189

Введение

Глобальная цифровизация формирует «новое измерение», актуализируя исследование изменений роли государства в международных отношениях. Суверенитет, веками остававшийся основополагающим принципом, теперь сталкивается с вызовами, требующими его переосмысления [1; 2]. Традиционно суверенитет рассматривался как верховная власть государства, ограниченная лишь внутренним законодательством, и символизировал независимость. Однако цифровая эра с её отсутствием физических границ, множественностью акторов, пересекающимися юрисдикциями и децентрализованным взаимодействием размывает привычные рамки. Это ставит перед государствами задачу трансформации понимания суверенитета применительно к цифровой реальности.

Дискуссия о суверенитете в цифровом пространстве получила новый импульс пять лет назад благодаря работам американских учёных: в 2020 и 2021 гг. были опубликованы работы М. Мюллера и К. Дж. Хеллера. Эти работы стали отправной точкой для активных дебатов о роли и природе суверенитета в условиях цифровых технологий. Результатом данных публикаций стало зарождение понятия «цифровой суверенитет».

Идея цифрового суверенитета сформировалась в результате многоуровневых дебатов – международных, национальных и внутригосударственных. Несмотря на появление множества качественных исследований, консенсус о содержании, масштабах и значении этой концепции, а также её связи с традиционным суверенитетом, пока не достигнут.

Цифровой суверенитет декларируется как отдельными государствами, так и международными организациями. Однако последние, будучи лишены атрибутов суверенности, сталкиваются с ограничениями в его реализации. На практике цифровой суверенитет формируется через нарративы, политические стратегии,

технологические практики и правовые механизмы, которые, в свою очередь, черпают легитимность из самой концепции.

Группа европейских учёных предлагает подход «недумающего» цифрового суверенитета, основанный на идее Им. Валлерстайна [3, р. 24]. Этот подход предполагает отказ от устоявшихся представлений для создания новых теоретических основ. Его цель — не замена существующих интерпретаций, а критический анализ через нетрадиционные призм. Подход децентрирует понятие суверенитета от классической Вестфальской модели, предлагая новые перспективы его понимания.

Кроме того, «недумающий» подход подчёркивает, что исследователи цифрового суверенитета не остаются нейтральными аналитиками. Их работа активно влияет на формирование политик и практик, использующих эту концепцию для легитимации. Таким образом, подход выводит эпистемологические вопросы в центр дискуссий о цифровом управлении, призывая к рефлексивному осмыслению структур и академических нарративов.

Важным следствием такого подхода является понимание того, что развитие цифрового суверенитета нельзя рассматривать изолированно. Этот процесс вплетён в глобальную борьбу за контроль над цифровым пространством, которая тесно связана с геополитическим соперничеством и стремлением к гегемонии, часто принимающем жёсткие и конфликтные формы.

Дополнительной трудностью для учёных становится рост цифровой дипломатии как составной части публичной дипломатии. Это явление усложняет анализ цифрового суверенитета, поскольку включает в себя как технологические, так и коммуникативные аспекты, влияющие на международные отношения и глобальное управление [4, с. 147].

В этой статье авторы исследуют вопрос о том, что можно подразумевать

под суверенитетом в контексте данных и цифровых пространств. В качестве основы для этого исследования мы выделяем три концепции суверенитета – российскую, американскую и китайскую.

Соединённые Штаты Америки закрепили за собой положение гегемона на цифровой арене: согласно докладу клуба «Валдай», представленному в 2021 г., 92% данных местных властей и национальных правительств, а также данных социальных сетей западного мира хранятся на серверах, принадлежащих США¹.

Правительства России и Китая хотят добиться цифрового суверенитета, чтобы обеспечить безопасность своих стран. Но они используют разные подходы: Россия старается достичь этой цели через дипломатию и внешнеполитические инициативы, а Китай применяет меры по фильтрации контента внутри своего сегмента интернета².

Таким образом, мы видим государства, стремящиеся установить цифровой суверенитет, ввиду разного позиционирования и преследования отличающихся результатов.

Методология проведённого исследования

Авторы в соответствии с концепцией фрейм анализа сформулировали стратегию поиска и исследования источниковой базы и академического материала, в которых упоминается об информационном суверенитете. Так, помимо вышеупомянутого термина, наша стратегия включает четыре родственных и показавшихся релевантными понятия: «цифро-

вой суверенитет», «киберсуверенитет», «суверенитет данных» и «виртуальный суверенитет». Оговоримся, что мы не останавливали своё внимание на пяти категориях цифрового суверенитета: суверенитет киберпространства, цифровой суверенитет государства и правительства, цифровой суверенитет коренных народов, цифровой суверенитет и общественные движения, а также личный цифровой суверенитет [5]. Более того, данная статья не претендует на исчерпывающий обзор всех опубликованных по обозначенной тематике статей.

В качестве исследовательской базы были использованы публикации на русском, английском и китайском языках. Подобный выбор объясняется составом нашей исследовательской группы и профессиональной специализацией авторов, а также сформулированной задачей работы. Материал включался в исследование, если в нём упоминалось понятие суверенитета в связи с цифровыми, например, данными, оцифровкой, информационно-коммуникационными технологиями или цифровыми инфраструктурами.

Обратим внимание, что оценка качества понятий или аргументов, которые встречались в исследовательском материале, не обозначалась в качестве результата. Мы попытались отобразить использование понятий и выявить отличия.

Цифровой суверенитет: теоретический аспект

Суверенитет как категория, связанная с цифровизацией, стала предметом научного интереса относительно недавно – данной теме посвящён ряд обзорных статей и дискуссионных статей последних лет. В них даются конкретные концепции понимания, что именно охватывает суверенитет в отношении цифровых технологий и сред.

Первыми на цифровой суверенитет обращают внимание американские исследователи. В 2020 г. вышла статья М. Мюллера, которая была посвящена вопросу

¹ Цифровой суверенитет // Международный дискуссионный клуб «Валдай» [Электронный ресурс]. URL: <https://ru.valdaiclub.com/multimedia/infographics/tsifrovoy-suverenitet/> (дата обращения: 15.06.2025).

² Зиновьева Е., Яцзе Б. Практика цифрового суверенитета в России и КНР // Российский совет по международным делам [Электронный ресурс]. URL: <https://russiancouncil.ru/analytics-and-comments/analytics/praktika-tsifrovogo-suvereniteta-v-rossii-i-kr/> (дата обращения: 25.03.2025).

суверенитета в рамках сети Интернет [6, р. 784]. В следующей году была опубликована работа его коллеги К. Дж. Хеллера, в которой автор рассуждает о том, что такое суверенитет, и существует ли он в цифровом пространстве [7, р. 1444]. Именно с выхода этих трудов начинается дискуссия об исследуемом нами вопросе.

Данная тематика вызывает общемировой научный интерес в настоящий момент. Европейский научный сегмент, направленный на изучение цифрового суверенитета, принято делить на две группы [8, р. 2111]. Одно направление литературы рассматривает этот вопрос как политическую концепцию, пытаясь оценить его политическую полезность и нормативную желательность или картировать различных вариантов использования или понимания цифрового суверенитета [9].

Другое направление исследований фокусируется на политической роли или функции цифрового суверенитета, стремясь понять, что именно он «делает», т. е. как цифровой суверенитет влияет на политику в области цифровых технологий [10, р. 322]. Данное восприятие выражается в тезисе, что цифровой суверенитет – это не только нормативный проект, но и геополитический.

Британский учёный Л. Флориди исследует цифровой суверенитет через призму трансформации капитализма и демократии в информационную эпоху. Он отмечает, что данные принципиально отличаются от традиционных ресурсов, таких как нефть: они находятся преимущественно в частной собственности, контролируются рыночными силами и активно эксплуатируются транснациональными корпорациями.

По мнению Флориди, национальный суверенитет нуждается в дополнении наднациональными механизмами регулирования, которые становятся условием его реализации. Учёный подчёркивает важность гармонизации стандартов и улучшения координации между различ-

ными уровнями управления цифровым пространством для обеспечения равных прав участников [11, р. 25].

Коллектив соавторов из Германии отмечает, что «суверенитет данных обычно каким-то образом связан со значимым контролем, владением и другими претензиями на данные или инфраструктуры данных» [12, р. 141]. Их коллеги из Берлинского центра социальных наук Дж. Поле и Т. Тиль подчёркивают, что цифровой суверенитет «часто используется как сокращение для упорядоченной, ценностно-ориентированной, регулируемой и, следовательно, разумной и безопасной цифровой сферы» [13]. Далее учёные замечают, что он направлен на восстановление роли национального государства, включая национальную экономику и её граждан в качестве ключевых категорий в глобальном управлении цифровыми инфраструктурами и технологиями.

Эти два ключевых общих наблюдения приводят к следующему тезису: государство продолжает оставаться одним из значимых субъектов, которые декларируют и стремятся обеспечить формы суверенитета в цифровой сфере. Например, британский учёный К. Мартин детально рассматривает дискуссии о суверенитете государства в контексте использования цифровых инструментов частным сектором для гуманитарных целей [14]. Кроме основного аспекта контроля, субъекты связывают цифровой суверенитет с различными мерами и инструментами. Государства или наднациональные организации могут добиться контроля над цифровыми технологиями через усиление потенциала, инвестиции и регулирование. Эти подходы помогают им укреплять свою способность управлять и развивать цифровые технологии, что в конечном итоге способствует повышению уровня их цифрового суверенитета [8, р. 2112].

Научный сотрудник Центра цифровизации, демократии и инноваций Брюс-

сельской школы управления Й. Тумфарт отмечает, что страны Глобального Севера перешли от модели относительно нерегулируемого интернета к концепции цифрового суверенитета под влиянием ряда ключевых событий. Среди них: разоблачения Эдварда Сноудена в 2013 г., раскрывшие масштабы глобальной слежки со стороны США; скандал с Cambridge Analytica в 2016 г., связанный с использованием данных Facebook для манипулирования общественным мнением во время президентских выборов в США; Brexit, изменивший подходы к цифровой политике в Европе; а также кризис дезинформации, обострившийся во время пандемии COVID-19 в 2020–2021 гг. Эти события стали катализаторами усиления государственного контроля над цифровыми технологиями [15, р. 37].

В совместной статье Е. С. Зиновьевой и Б. Яцзе отмечается, что ключевые компоненты цифрового суверенитета включают развитие национальных поисковых систем и социальных сетей для снижения зависимости от зарубежных платформ, а также укрепление цифровой инфраструктуры национального сегмента интернета. Последнее подразумевает создание локализованных хранилищ данных и точек обмена трафиком, что обеспечивает большую автономность и безопасность информационной системы¹.

Китайский исследователь Ф. Биньсин выделил четыре основополагающих принципа цифрового суверенитета [16, р. 80]:

1. каждая страна должна самостоятельно регулировать и управлять своим национальным сегментом интернета;

2. государства обязаны обладать техническими и правовыми средствами для защиты своих цифровых ресурсов от внешних киберугроз;

3. необходимо обеспечить равные права всех стран на использование интернет-ресурсов без дискриминации или доминирования со стороны других государств;

4. иностранные акторы не должны контролировать корневые DNS-серверы, чтобы гарантировать независимость национальной цифровой инфраструктуры.

Е. Громова и Д. Брантес Феррейра выделяют четыре ключевых сегмента цифрового суверенитета: защиту данных, кибербезопасность, эффективное регулирование через эксперименты и создание благоприятных условий для развития технологий [17, р. 57]. При этом они подчёркивают, что последние два элемента не относятся к традиционным аспектам суверенитета, а роль стимулирующих мер особенно важна. По их мнению, государства должны активно продвигать цифровые технологии, используя специальные правовые режимы, такие как создание экономических зон или развитие государственно-частного партнёрства.

По мнению российских исследовательниц О. Устюжанцевой и Е. Поповой, в демократических государствах политика цифрового суверенитета формируется через многостороннее взаимодействие участников, что отражает ценности открытого общества. В авторитарных режимах, напротив, приоритет отдаётся централизованному контролю интернета, где ключевые полномочия находятся в руках государства [18, р. 77]. Это свидетельствует о том, что подходы к цифровому суверенитету определяются политической системой и распределением власти. В авторитарных странах концепция разрабатывается преимущественно государственными институтами без участия широкого круга заинтересованных сторон и практик совместного принятия решений.

Понятие цифрового суверенитета часто выступает как противовес доминированию США в управлении интернетом и влиянию транснациональных корпора-

¹ Зиновьева Е., Яцзе Б. Практика цифрового суверенитета в России и КНР // Российский совет по международным делам: [Электронный ресурс]. URL: <https://clcl.i/Pctua> (дата обращения: 14.03.2025).

ций (GAFAM: Google, Amazon, Facebook, Apple, Microsoft). Современные исследования всё больше фокусируются на роли крупных технологических компаний, хотя государство остаётся одним из ключевых, но не единственным субъектом в цифровой сфере. Здесь также активно действуют частные компании, граждане, бизнес-структуры и другие заинтересованные стороны, формируя сложное взаимодействие, где права и полномочия всех участников взаимосвязаны.

Анализ литературы позволяет сделать важные выводы. Во-первых, цифровой суверенитет принципиально отличается от традиционного государственного суверенитета, так как обусловлен спецификой цифровой среды. Во-вторых, он не отменяет и не заменяет существующую концепцию суверенитета, а дополняет её в условиях цифровизации общества. Наконец, цифровой суверенитет порождает новые правовые, политические и научные дискуссии, требующие переосмысления классических подходов к пониманию суверенитета.

Рассмотрим более подробно, как формируются концепции цифрового суверенитета в США, России и Китае.

Цифровая гегемония: взгляд из Вашингтона

США занимают доминирующее положение в цифровом пространстве, и их мощь основывается исключительно на собственных технологических возможностях, включая скрытые усилия по установлению глобального цифрового контроля.

В Стратегии кибербезопасности правительство США прямо заявляет, что лидерство в цифровой сфере является ключевым элементом для поддержания глобальной гегемонии страны¹. На практике это утверждение находит подтверждение в действиях американских властей.

¹ National Cybersecurity Strategy. March 2023 [Электронный ресурс]. URL: <https://clcl.i/pReBa> (дата обращения: 25.06.2025).

Цифровое доминирование США можно описать через пять ключевых аспектов. Во-первых, это массовое наблюдение, которое позволяет США собирать и контролировать огромные объёмы глобальных данных. Во-вторых, продвижение концепции общественного достояния, которая помогает стране захватывать значительную долю на мировом цифровом рынке. В-третьих, навязывание односторонних действий, направленных на противодействие установлению многосторонних правил в киберпространстве. В-четвёртых, монополизация критической инфраструктуры интернета, что усиливает контроль над глобальной сетью в интересах США. И, наконец, в-пятых, милитаризация киберпространства, включая проведение наступательных киберопераций для продвижения своих стратегических интересов.

Каждый из этих аспектов отражает стремление США укрепить своё цифровое превосходство, часто в ущерб международному сотрудничеству и безопасности других стран.

Анализ этих аспектов показывает, как США ставят свои гегемонистские цели выше безопасности и развития глобального киберпространства, нанося значительный ущерб его стабильности и процветанию².

В стремлении обеспечить собственную безопасность, Вашингтон без колебаний жертвует кибербезопасностью других государств. Это не только подрывает национальную безопасность других стран, но и ослабляет общую экосистему глобальной кибербезопасности, заставляя весь мир платить высокую цену.

Кроме того, США игнорируют киберсуверенитет других стран, преднамеренно вторгаясь в их цифровое пространство

² Liu Xuanjia, Sun Guangya (Сунь Гуаня). The US digital hegemony: characteristics, objectives and implications [Цифровая Гегемония США: Особенности, Цели И Последствия]. State and Municipal Management Scholar Notes, Russian Presidential Academy of National Economy and Public Administration. 2024. Vol. 2. P. 297–301.

и нарушая его стабильность. Несмотря на международную критику, они продолжают политику массового наблюдения.

За этими усилиями стоят мощные мотивы: массовый сбор данных предоставляет США бесценную разведывательную информацию, которая служит основой для стратегического принятия решений на глобальном уровне. По данным СМИ, Агентство национальной безопасности США собирает огромные объёмы данных через онлайн-ресурсы и предоставляет их для ежедневных брифингов президента¹. На протяжении длительного времени киберразведка составляла более половины информации, представленной главе государства.

Таким образом, несмотря на глобальное осуждение, США продолжают действовать в одностороннем порядке, используя передовые технологии для поддержания своей системы глобального наблюдения и укрепления своего цифрового доминирования.

Информационный суверенитет: концепция Москвы

Согласно National Cyber Power Index 2022, подготовленному Центром Белфера при Гарвардской школе, Россия занимает третье место в мире по уровню кибервливания после США и Китая². Это подчёркивает важность информационных технологий в обеспечении национальной безопасности РФ. В российском дискурсе информационная сфера рассматривается как ключевой элемент суверенитета, что нашло отражение в Доктрине информационной безопасности Российской Федерации, принятой в 2016 г. Под информационной сферой понимается комплексная система, включающая информацию, инфраструктуру, субъектов, осуществляющих сбор, формирование, распро-

странение и использование информации, а также механизмы регулирования общественных отношений. Этот подход акцентирует внимание не только на технических, но и на социальных, правовых и организационных аспектах цифровизации³.

Термин «информационный суверенитет» активно используется в российской научной литературе, в отличие от западного аналога — «цифровой суверенитет». Среди пионеров исследования этой темы выделяются такие учёные, как М. М. Кучерявый и Н. Н. Федотов. Последний считается одним из первых популяризаторов термина, тогда как президент компании «Крибрум», член Совета при президенте по развитию гражданского общества и правам человека, член правления РОЦИТ И. С. Ашманов предложил одно из первых определений. Однако единое толкование феномена до сих пор отсутствует, что связано с его многоаспектностью и динамичным развитием [19].

В отличие от зарубежных исследователей, использующих термин «цифровой суверенитет», российская научная школа склоняется к термину «информационный суверенитет», считая его более точным. Однако в данной статье авторы используют оба термина как синонимы.

Учёные предлагают различные определения «информационного суверенитета» – от самых широких до узко направленных. Российский исследователь А. А. Ефремов под ним понимает право государства контролировать информацию, распространяемую на его территории [20, с. 207].

Уже упомянутый нами отечественный учёный М. М. Кучерявый, выявляя основные составляющие государственного суверенитета, экономический, идеологический, военный, дипломатический,

¹ Schaake, M. *The tech coup: How to save democracy from Silicon Valley*. Princeton University Press. 2024. P. 152.

² National Cyber Power Index 2022 / J. Voo, I. Hemani, D. Cassady [Электронный ресурс]. URL: <https://clcli.stcnd> (дата обращения: 14.07.2025).

³ Доктрина информационной безопасности Российской Федерации // Совет Безопасности Российской Федерации [Электронный ресурс]. URL: <http://www.scrf.gov.ru/documents/6/5.html> (дата обращения: 07.06.2025).

юридический, предлагает добавить в структуру государственного суверенитета информационный суверенитет как ответ новым вызовам обеспечения национальной безопасности России [21, с. 11]. Информационный суверенитет он характеризует как «независимость государственной власти при формировании и реализации информационной политики в национальном сегменте и глобальном информационном пространстве» [22].

Кандидат политических наук, руководитель подразделения проблем информационной безопасности ЦМБ ИМЭМО РАН Н. Ромашкина рассматривает информационный суверенитет «как способность технологически и законодательно обеспечивать и защищать независимость государства и конституционные права граждан в информационном пространстве от внешних угроз, контролируя при этом происходящее в этом пространстве»¹.

Группа соавторов Московского государственного университета определяет информационный суверенитет как «эмергентное свойство современного государства как сложной системы» [23]. Это взаимодействие формируется за счёт сочетания технологических возможностей государства (таких как: развитие цифровой инфраструктуры и внедрение информационных технологий) с цифровыми компетенциями, навыками и способностями граждан, организаций и институтов в области эффективного использования цифровых ресурсов.

Таким образом, ключевым фактором становится не только наличие технологий, но и уровень подготовленности общества к их применению, что создаёт основу для устойчивого развития цифровой экосистемы.

Их коллега из Польши Ф. Брокиш, анализируя российский информационный суверенитет, отмечает, что он подразумевает использование отечественного IT-оборудования и оказание приоритетной поддержки российским IT-компаниям в сфере цифровых технологий. Особое внимание уделяется обеспечению безопасности национальной интернет-инфраструктуры и интернет-трафика, а также созданию национальной системы управления большими данными в рамках суверенного государства².

Если давать дальнейшую характеристику западному взгляду на случай России, то следует отметить, что такие исследователи, американские учёные Р. Смит и С. Отс, определяют подход к информационному суверенитету как «государственно-контролируемое повествование» [24, р. 287]. В силу авторитарной природы политической системы государство здесь характеризуется как отстранённое и деинституционализированное, стремящееся минимизировать точки взаимодействия с гражданским обществом.

Президент компании «Крибрум», член Совета при президенте по развитию гражданского общества и правам человека, член правления РОЦИТ И. С. Ашманов настаивает на необходимости цифрового суверенитета «потому что обычные виды суверенитета (политический, дипломатический, экономический, военный) сейчас под огромной угрозой из-за того, что у государства нет цифрового суверенитета, потому что цифровое пространство сейчас – это огромная дыра, через которую ломаются все остальные элементы суверенитета»³. По мнению И. С. Ашманова, цифровой суверенитет – это способность государства защищать своё информационное пространство и

¹ Ромашкина Н. Информационный суверенитет или почему России нужна стратегия информационной безопасности // Российский совет по международным делам. [Электронный ресурс]. URL: <https://clcl.i/yTpsa> (дата обращения: 06.08.2025).

² Brokeš F Russia's Sovereign Internet // Central European Financial Observer. 2018. September 24.

³ Ашманов И. Информационный суверенитет России: новая реальность // Россия навсегда: [сайт]. URL: <http://rossiyanavsegda.ru/read/948/> (дата обращения: 15.05.2025).

самостоятельно определять информационную политику, не завися от внешних факторов. Он связывает этот феномен с необходимостью противостояния в информационной войне, особенно с США, и акцентирует внимание на разработке инструментов защиты и обеспечения безопасности информационного суверенитета.

В основе российской модели лежат два ключевых направления: «электронный щит» и «информационный щит». Первый направлен на снижение технологической зависимости от зарубежных решений. Он включает развитие отечественной аппаратной и программной базы, создание национальных систем (поисковые платформы, социальные сети, платёжные системы), импортозамещение микроэлектроники и внедрение криптографических средств защиты данных.

Однако реализация такого подхода остаётся уязвимой из-за недостаточной независимости в области цифровых технологий. В этой связи важно рассмотреть компоненты цифрового суверенитета, предложенные отечественным исследователем В. В. Бухариным:

- 1) собственная поисковая система для независимости в области поиска и обработки информации;
- 2) отечественные социальные сети для развития локального цифрового взаимодействия;
- 3) российскую операционную систему и программное обеспечение для снижения зависимости от зарубежных решений;
- 4) импортозамещение микроэлектроники для укрепления технологической независимости;
- 5) криптографические средства защиты информации для обеспечения безопасности данных;
- 6) глобальную навигационную систему для автономности в сфере геолокации;
- 7) национальную платёжную систему для поддержания финансовой независимости страны [19, с. 89].

Эти компоненты формируют основу цифровой инфраструктуры, способной противостоять внешним угрозам и обеспечивать устойчивое развитие государства в условиях глобальной цифровизации.

«Информационный щит» включает создание автономной интернет-инфраструктуры, контроль над медиасферой и распространением информации, разработку законодательной базы для защиты национальных интересов, а также продвижение государственной идеологии и противодействие внешним угрозам. Закон «О суверенном интернете», принятый в 2019 г., стал важным шагом в реализации этих подходов. Он предусматривает создание национальной системы маршрутизации трафика и централизованное управление критически важными элементами инфраструктуры¹.

В качестве контрмер по защите информационного суверенитета предлагается использовать так называемый «информационный меч», который представляет собой систему методов и линии поведения направленная на причинение ущерба информационному суверенитету противоборствующего государства. Они могут реализовываться в тех же плоскостях, что и стратегия «щита».

Несмотря на прогресс, Россия сталкивается с рядом трудностей. Ограниченный опыт высокотехнологичных компаний в разработке комплексных платформенных решений, зависимость от зарубежных технологий, особенно в области микроэлектроники, и необходимость более активного участия в международных дискуссиях о регулировании интернета остаются вызовами. Таким образом, информационный суверенитет становится ключевым элементом национальной безопасности, требующим комплексного подхода: технологического,

¹ Ашманов И. С. Информационный суверенитет. Лекция для специалистов ИТ [Электронный ресурс]. URL: https://vk.com/wall-82197743_656994 (дата обращения: 20.07.2025).

правового и социального. Россия последовательно движется к снижению зависимости от западных технологий, однако полная реализация этой стратегии требует дальнейших усилий, включая развитие собственной индустрии и участие в международном диалоге.

Золотой щит: цифровая политика Пекина

Изначально термин «цифровой суверенитет» появился в китайском дискурсе на рубеже XXI в. как ответ на расширение цифровой мощи США. В этот период Соединённые Штаты активно продвигали свою «мягкую силу» через информационные технологии, рассматривая их как инструменты демократизации и либерализации общества.

Эта геостратегия, основанная на принципах децентрализации интернета и нетерриториальных сетей, была воспринята китайскими учёными как западный гегемонистский проект. Ярким примером такого доминирования стало влияние США на инфраструктуру управления интернетом, включая ключевую роль Корпорации по управлению именами и номерами в интернете. Именно в противовес этой модели Китай начал развивать собственную концепцию киберсуверенитета, подчёркивающую важность государственного контроля над цифровым пространством [25, p. 11].

Инспирированное дискуссиями Нового мирового информационного и коммуникационного порядка, китайское социотехническое представление о цифровом суверенитете, направленное на укрепление национального контроля над цифровыми технологиями, начало формироваться ещё в 1990-х гг. Этот подход изначально опирался на стремление Пекина минимизировать зависимость от зарубежных технологий и создать автономную цифровую экосистему, что заложило основу для современной стратегии технологического суверенитета страны [13; 26]. Данное представление определя-

ется пятью ключевыми культурными и политическими факторами.

Первым фактором выступает геополитический контекст. После распада СССР Китай стал рассматриваться как стратегический и экономический конкурент США. Защита от попыток изменения политического режима через цифровые средства стала ключевой задачей китайской политики.

Вторым элементом можно выделить культурно-историческую самосознательность. Китай позиционирует себя как постколониальное государство, чувствительно относясь к действиям западных стран, особенно США. Антиколониальная риторика усилилась в 1990-х гг., что совпало с восстановлением суверенитета над Гонконгом в 1997 г. и Макао в 1999 г. Эти процессы повлияли на формирование представлений о цифровом суверенитете.

Третьим фактором является специфика политической системы. В рамках социалистической модели чёткое разделение частного и государственного секторов отсутствует. Государство активно контролирует ключевые технологические направления, следуя марксистскому подходу к управлению экономикой и технологиями для обеспечения национальных интересов [27].

Особое значение имеет конфуцианство и его влияние на общество и государство. Конфуцианская традиция, возрождённая при Дэн Сяопине, играет важную роль в формировании государственной идеологии. Несмотря на официальный атеизм, общество нельзя назвать светским в западном смысле. Конфуцианство подчёркивает гармонию и коллективное благо, что интегрируется в современные подходы к управлению обществом и цифровым суверенитетом.

Последней, но не по значению, составляющей является универсалистское понимание государственности. Китайская концепция суверенитета уходит корнями в конфуцианскую и имперскую мысль, выражаемую через идею 天下

(Tianxia, «всё под небом»). Это целостное представление о государстве связывает культурные и политические вопросы, подчёркивая их взаимозависимость. Осторожная позиция Китая в отношении цифровой гегемонии США обусловлена восприятием доминирования западной культурной парадигмы в интернете, что усиливает стремление к технологическому и культурному суверенитету.

Ещё в 1990-е-начале 2000-х гг. китайские учёные рассматривали доминирование английского языка в интернете как угрозу национальной культурной идентичности. Эти опасения побудили правительство Китайской Народной Республики уже в 2000 г. внедрить доменные имена, записанные китайскими иероглифами [28].

Идеологическую основу цифрового суверенитета Китая можно проследить с 1996 года [27, р. 444], а ключевым моментом стало эссе Гун Вэньсяна из Школы международных отношений Пекинского университета, опубликованное в 1998 г. под названием «Информационный суверенитет» (信息主权) [28].

Гун Вэньсян ссылаясь на дискуссии о Новом мировом информационном и коммуникационном порядке, критикуя культурное господство США как угрозу глобальному информационному равновесию. Он призывал к созданию «справедливых, равноправных и взаимовыгодных форм коммуникации», противопоставляя концепцию «информационного суверенитета» западной модели «глобализации информации».

Это эссе стало важным шагом в формировании китайского подхода к цифровому суверенитету, подчёркивая необходимость защиты национальных интересов в условиях глобализации технологий.

В период правления Цзян Цзэминя Китай сделал значительные инвестиции, опираясь на концепцию «конкурентного преимущества позднего старта», чтобы вывести страну в лидеры в новейших и сложных отраслях информационно-коммуникационных технологий (ИКТ) [29,

р. 114]. Благодаря этой стратегии и масштабным вложениям Китай превратился в одну из ведущих экономик мира, заняв прочные позиции во многих секторах ИКТ.

В то время как на Западе интернет воспринимался как площадка для либерализации и продвижению прав и свобод человека и гражданина, китайское правительство воспринимало интернет иначе – прежде всего как инструмент для достижения экономических целей. В то же время оно стремилось предотвратить распространение американского понимания интернета, которое могло бы нанести ущерб существованию и легитимности Коммунистической партии Китая. Так, важным поворотным моментом в этой последовательной политики стало формирование системы, известной как «Великий китайский файрвол». Она призвана блокировать информацию по чувствительным для Китая темам — включая вопросы, связанные с тибетским и уйгурским вопросами, а также события июня 1989 г. [30, р. 444].

Один из самых простых способов контроля нежелательного контента — его полная блокировка. Именно эта логика легла в основу китайского «Проекта Золотого щита», который считается одной из самых сложных систем блокировки и фильтрации контента в мире. Проект был разработан в 1996 г., но официально запущен только лишь в 2006 г. Другими словами, «Проект Золотого щита» представляет собой технологическую реализацию законодательных норм, направленных на регулирование интернета [31, р. 171].

С момента полного запуска проекта «Золотой щит» в 2006 г. были заблокированы десятки веб-страниц, IP-адресов и URL-адресов, включая популярные социальные сети – Twitter, Facebook и Instagram¹.

¹ WhatsApp, Facebook и Instagram – принадлежат компании Meta Platforms Inc. (признана экстремистской организацией, и её деятельность запрещена на территории РФ). Реализация Facebook и Instagram на территории РФ запрещена.

Согласно исследованию 2020 г., развитие проекта можно разделить на четыре фазы. Первая фаза началась с блокировки определённых доменных имён и IP-адресов внутри страны. Система также использовалась для выявления нарушителей. Для этого китайские власти обязали все интернет-кафе установить одобренное шпионское программное обеспечение и регистрировать пользователей по удостоверениям личности. Это позволило государству контролировать активность в интернет-кафе и оперативно наказывать нарушителей [30, p. 446].

В этом контексте под руководством Си Цзиньпина Китай начал активно продвигать собственное видение киберсуверенитета. Это понятие основано на принципах государственного контроля, сосредоточено на роли государства и подчёркивает обязанности отдельных лиц, а не их права [29, p. 116]. Идея китайского «киберсуверенитета» получила новое развитие в Белой книге 2010 г. под названием «Интернет в Китае». В документе было чётко обозначено, что «на территории Китая интернет находится под суверенитетом Китая». Белая книга также подчёркивала, что все лица и организации, действующие в Китае, обязаны соблюдать местные законы и правила, регулирующие использование интернета.

Культурные элементы цифровой политики нельзя сводить лишь к ограничениям сверху. Они включают и продуктивные практики, возникающие снизу вверх. Одним из ярких примеров является развитие формы «цифрового национализма» в китайском обществе, где пользователи интернета осознанно поддерживают государственную повестку и участвуют в её распространении [31, p. 168].

На Будапештской конференции по киберпроблемам в 2012 г. Китай представил пять принципов международного сотрудничества в киберпространстве. Первый и ключевой принцип – суверенитет – был определён как право каждого государства самостоятельно формулиро-

вать свою политику и законодательство с учётом своей уникальной истории, традиций, культуры и языка [30, p. 462].

Этот подход подчёркивает важность уважения национальной специфики в регулировании интернета и противостоит универсализму, который часто ассоциируется с западными моделями управления киберпространством.

Заключение

Анализ показывает, что США укрепляют цифровое доминирование через 5 ключевых аспектов: массовый сбор данных, продвижение концепции общественного достояния, односторонние решения, контроль над критической интернет-инфраструктурой и милитаризацию киберпространства. Эти шаги, направленные на обеспечение глобальной гегемонии, подрывают международную кибербезопасность, игнорируют суверенитет других стран и ставят национальные интересы выше принципов многостороннего сотрудничества.

В России и Китае цифровой суверенитет рассматривается как элемент национальной безопасности, но подходы к его реализации различаются в зависимости от исторических, культурных и политических особенностей. Россия фокусируется на защите национального сегмента интернета и снижении зависимости от западных технологий. Закон «О суверенном интернете» направлен на создание автономной инфраструктуры и централизованное управление трафиком, однако слабая развитость высокотехнологичных компаний и необходимость участия в международных дискуссиях остаются вызовами.

Китайская модель основана на государственном контроле и создании автономной цифровой экосистемы. Через систему «Золотого щита» страна блокирует западные сервисы, развивает собственные платформы и продвигает идеологию коллективного блага. Особую роль играет «цифровой национализм», усиливающий

лояльность граждан. Культурно-историческая специфика и технологическое импортозамещение поддерживают эту стратегию.

Общие тенденции включают восприятие цифрового суверенитета как инструмента противодействия доминированию США и западных технологических корпораций. Обе страны стремятся к созданию автономных цифровых экосистем, снижению зависимости от зарубежных решений и укреплению национальной безопасности. При этом культурные и идеологические факторы, особенно в Китае, играют ключевую роль в легитимации государственной стратегии.

На глобальном уровне подходы России и Китая ставят под сомнение универсальные модели управления интернетом, предлагаемые западными странами. Эти государства выступают за многосторонний подход, учитывающий национальные особенности, но их усилия могут усугубить фрагментацию интернета и создать новые барьеры для международного сотрудничества. Таким образом, цифровой суверенитет становится не только технической, но и политической категорией, отражающей стремление государств сохранить контроль над своим цифровым будущим в условиях глобализации и технологической конкуренции.

ЛИТЕРАТУРА

1. Kissinger H. *World Order*. Penguin, 2014. 432 p.
2. Digital transformation: A multidisciplinary reflection and research agenda / P. C. Verhoef, T. Broekhuizen, Y. Bart, A. Bhattacharya, et al. // *Journal of Business Research*. 2021. Vol. 122. Pp. 889–901.
3. Pohle J., Nanni R., Santaniello M. *Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices* // *Policy & Internet*. 2024. Vol. 16. № 3. P. 666–671. DOI: 10.1002/poi3.437
4. Кривохиж С. В., Теленьга М. П. Трансформация цифровой дипломатии в условиях новых вызовов: взгляд из Вашингтона и Пекина // *Вестник Санкт-Петербургского университета. Международные отношения*. 2024. Т. 17. Вып. 2. С. 143–163. DOI: 10.21638/spbu06.2024.203
5. Кутюр С., Тоупин С. Что означает понятие «суверенитет» в цифровом мире? // *Вестник международных организаций*. 2020. № 15. С. 48–69.
6. Mueller M. L. *Against Sovereignty in Cyberspace* // *International Studies Review*. 2020. № 22. P. 779–801. DOI: 10.1093/isr/viz044
7. Heller K. J. *In Defense of Pure Sovereignty in Cyberspace* // *International Law Studies*. 2024. № 97. P. 1432–1499.
8. Digital sovereignty – Rhetoric and reality / G. Falkner, S. Heidebrecht, A. Obendiek, T. Seidl // *Journal of European Public Policy*. 2024. № 31. P. 2099–2120. DOI: 10.1080/13501763.2024.2358984
9. Obendiek A. *Take back control? Digital sovereignty and a vision for Europe* // *Hertie School – Jacques Delors Center*. 2023. P. 341–345. DOI: 10.1080/13501763.2024.2358984
10. Digital sovereignty: From narrative to policy? / D. Broeders, R. Csernatoni, K. Irion, M. Kaminska, et al. 2022. 18 p.
11. Floridi L. *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU* // *Philos Technol*. 2020. № 33. P. 369–378. DOI: 10.1007/s13347-020-00423-6
12. Data sovereignty: A review / P. Hummel, M. Braun, M. Tretter, P. Dabrock // *Big Data & Society*. 2021. № 8. DOI: 10.1177/2053951720982012
13. Pohle J., Thiel T. *Digital sovereignty* // *Internet Policy Review*. 2020. № 9. DOI: 10.14763/2020.4.1532
14. Martin C. *Geopolitics and Digital Sovereignty*. In: *Perspectives on Digital Humanism*. Springer, Cham / Werthner H., et al., eds. Springer, 2023. P. 227–231. DOI: 10.1007/978-3-030-86144-5_30
15. Thumfart J. *The norm development of digital sovereignty between China, Russia, the EU and the US: From the late 1990s to the Covid-crisis 2020/21 as catalytic event* // *Data Protection and Privacy: Enforcing Rights in a Changing World* / D. Hallinan, et al., eds. Hart Publishing, 2021. P. 1–44.
16. Binxing F. *Cyberspace Sovereignty*. Springer Singapore, 2018. 521 p.
17. Gromova E., Brantes Ferreira D. *On the Way to BRICS+ Digital Sovereignty: Opportunities and Challenges of a New Era* // *BRICS Law Journal*. 2024. № 11. P. 54–69. DOI: 10.21684/2412-2343-2024-11-3-54-69

18. Ustyuzhantseva O., Popova E. *Shaping Digital Sovereignty in Russia: Actors and Debates // Problems of Post-Communism*. 2024. № 72. P. 76–87. DOI: 10.1080/10758216.2024.2346202
19. Бухарин В. В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестник МГИМО-Университета. 2016. № 6. С. 76–91.
20. Ефремов А. А. Формирование концепции информационного суверенитета государства // Право: Журнал Высшей школы экономики. 2017. № 1. С. 201–215.
21. Кучерявый М. М. Государственная политика информационного суверенитета России в условиях современного глобального мира // Управленческое консультирование. 2015. № 2. С. 11–12.
22. Зорина Е. Г. Информационный суверенитет современного государства и основные инструменты его обеспечения // Известия Саратовского университета. Серия: Социология. Политология. 2017. Т. 17. Вып. 3. 345–348.
23. Цифровой суверенитет современного государства в условиях технологических трансформаций: содержание и особенности / С. В. Володенков, А. С. Воронов, Л. С. Леонтьева, М. Сухарева // Polylogos. 2021. № 5. DOI: 10.18254/S258770110014073-2
24. SMYTH R., OATES S. MIND THE GAPS: MEDIA USE AND MASS ACTION IN RUSSIA // EUROPE-ASIA STUDIES. 2015. № 67. P. 285–305. DOI: 10.1080/09668136.2014.1002682
25. Pierucci F. Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace // Digital Society. 2025. № 4. DOI: 10.1007/s44206-025-00189-4
26. Cong W., Thumfart J. A Chinese Precursor to the Digital Sovereignty Debate: Digital Anti-Colonialism and Authoritarianism from the Post-Cold War Era to the Tunis Agenda // *Global Studies Quarterly*. 2022. Vol. 2. Iss. 4. P. 1–13. DOI: 10.1093/isagsq/ksac059
27. Zeng J., Stevens T., Chen Y. China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty" // *Politics and Policy*. 2017. № 45. P. 432–464. DOI: 10.1111/polp.12202
28. Creemers R. China's Conception of Cyber Sovereignty: Rhetoric and Realization // *Governing Cyberspace: Behaviour, Power and Diplomacy* / D. Broeders, B. Berg, eds. London: Rowman & Littlefield, 2020. P. 107–142. DOI: 10.1007/978-3-319-60405-3
29. The Golden Shield Project of China: A Decade Later An in-depth study of the Great Firewall / S. Chandel, J. Zang, Y. Yu, J. Sun, Zhipen Zhang // *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*. 2020. P. 111–119. DOI: 10.1109/CyberC.2019.00027
30. Zeng J., Tim S., Yaru C. China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty" // *Politics and Policy*. 2017. № 45. P. 432–464. DOI: 10.1111/polp.12202
31. Schneider F. A. China's digital nationalism // *The Routledge handbook of nationalism in East and Southeast Asia* / Z. Lu, ed. New York: Routledge, 2023. P. 167–180. DOI: 10.4324/9781003111450-14

REFERENCES

1. Kissinger, H. (2014). *World Order*. Penguin.
2. Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., et al. (2021) Digital transformation: A multidisciplinary reflection and research agenda. In: *Journal of Business Research*, 122, 889–901.
3. Pohle, J., Nanni, R. & Santaniello, M. (2024). Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices. In: *Policy & Internet*, 16-3, 666–671. DOI: 10.1002/poi3.437
4. Krivokhizh, S. V. & Telenga, M. P. (2024). Transformation of digital diplomacy in the face of new challenges: a look from Washington and Beijing. In: *Bulletin of St. Petersburg University. International relations*, 17-2, 143–163. DOI: 10.21638/spbu06.2024.203 (in Russ.).
5. Couture, S. & Toupin, S. (2020). What does the concept of "sovereignty" mean in the digital world? In: *Bulletin of International Organizations*, 15, 48–69 (in Russ.).
6. Mueller, M. L. (2020). Against Sovereignty in Cyberspace. In: *International Studies Review*, 22, 779–801. DOI: 10.1093/isr/viz044
7. Heller, K. J. (2024). In Defense of Pure Sovereignty in Cyberspace. In: *International Law Studies*, 97, 1432–1499.
8. Falkner, G., Heidebrecht, S., Obendiek, A. & Seidl, T. (2024). Digital sovereignty – Rhetoric and reality. In: *Journal of European Public Policy*, 31, 2099–2120. DOI: 10.1080/13501763.2024.2358984
9. Obendiek, A. (2023). Take back control? Digital sovereignty and a vision for Europe. In: *Hertie School – Jacques Delors Center*, 341–345. DOI: 10.1080/13501763.2024.2358984

10. Broeders, D., Csernaton, R., Irion, K., Kaminska, M., et al. (2022). *Digital sovereignty: From narrative to policy?*
11. Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. In: *Philos Technol*, 33, 369–378. DOI: 10.1007/s13347-020-00423-6
12. Hummel, P., Braun, M., Tretter, M. & Dabrock, P. (2021). Data sovereignty: A review. In: *Big Data & Society*, 8. DOI: 10.1177/2053951720982012
13. Pohle, J. & Thiel, T. (2020). Digital sovereignty. In: *Internet Policy Review*, 9. DOI: 10.14763/2020.4.1532
14. Martin, C. (2023). Geopolitics and Digital Sovereignty. In: Werthner H., et al., eds. *Perspectives on Digital Humanism*. Springer, Cham. Springer, 227–231. DOI: 10.1007/978-3-030-86144-5_30
15. Thumfart, J. (2021). The norm development of digital sovereignty between China, Russia, the EU and the US: From the late 1990s to the Covid-crisis 2020/21 as catalytic event. In: Hallinan D., et al., eds. *Data Protection and Privacy: Enforcing Rights in a Changing World*. Hart Publishing, 1–44.
16. Binxing, F. (2018). *Cyberspace Sovereignty*. Springer Singapore.
17. Gromova E. & Brantes Ferreira D. (2024). On the Way to BRICS+ Digital Sovereignty: Opportunities and Challenges of a New Era. In: *BRICS Law Journal*, 11, 54–69. DOI: 10.21684/2412-2343-2024-11-3-54-69
18. Ustyuzhantseva, O. & Popova, E. (2024). *Shaping Digital Sovereignty in Russia: Actors and Debates*. In: *Problems of Post-Communism*, 72, 76–87. DOI: 10.1080/10758216.2024.2346202
19. Bukharin, V. V. (2016). Components of the digital sovereignty of the Russian Federation as the technical basis of information security. In: *Bulletin of MGIMO University*, 6, 76–91 (in Russ.).
20. Efremov, A. A. (2017). Formation of the concept of information sovereignty of the state. In: *Law: Journal of the Higher School of Economics*, 1, 201–215 (in Russ.).
21. Kucheryav, M. M. (2015). State policy of information sovereignty of Russia in the context of the modern global world. In: *Management consulting*, 2, 11–12 (in Russ.).
22. Zorina, E. G. (2017). Information sovereignty of the modern state and the main tools for its provision. In: *Izvestia Saratov University. Series: Sociology. Political science*, 17-3, 345–348 (in Russ.).
23. Volodenkov, S. V., Voronov, A. S., Leontyeva, L. S. & Sukhareva, M. (2021). Digital sovereignty of the modern state in conditions of technological transformations: content and features. In: *Polylogos*, 5. DOI: 10.18254/S258770110014073-2 (in Russ.).
24. SMYTH, R. & OATES, S. (2015). MIND THE GAPS: MEDIA USE AND MASS ACTION IN RUSSIA. In: *EUROPE-ASIA STUDIES*, 67, 285–305. DOI: 10.1080/09668136.2014.1002682
25. Pierucci, F. (2025). Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace. In: *Digital Society*, 4. DOI: 10.1007/s44206-025-00189-4
26. Cong, W. & Thumfart, J. (2022). A Chinese Precursor to the Digital Sovereignty Debate: Digital Anti-Colonialism and Authoritarianism from the Post-Cold War Era to the Tunis Agenda. In: *Global Studies Quarterly*, 2-4, 1–13. DOI: 10.1093/isagsq/ksac059
27. Zeng, J., Stevens, T. & Chen, Y. (2017). China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty". In: *Politics and Policy*, 45, 432–464. DOI: 10.1111/polp.12202
28. Creemers, R. (2020). China's Conception of Cyber Sovereignty: Rhetoric and Realization. In: Broeders, D., Berg, B., eds. *Governing Cyberspace: Behaviour, Power and Diplomacy*. London: Rowman & Littlefield, 107–142. DOI: 10.1007/978-3-319-60405-3
29. Chandel, S., Zang, J., Yu, Y., Sun, J., Zhang Zhipen (2020). The Golden Shield Project of China: A Decade Later An in-depth study of the Great Firewall. In: *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, 111–119. DOI: 10.1109/CyberC.2019.00027
30. Zeng, J., Tim, S. & Yaru, C. (2017). China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty". In: *Politics and Policy*. 2017. № 45. P. 432–464. DOI: 10.1111/polp.12202
31. Schneider, F. A. (2023). China's digital nationalism. In: Lu, Z., ed. *The Routledge handbook of nationalism in East and Southeast Asia*. New York: Routledge, 167–180. DOI: 10.4324/9781003111450-14

ИНФОРМАЦИЯ ОБ АВТОРАХ

Безрученко Марина Павловна (г. Краснодар) – кандидат исторических наук, доцент кафедры зарубежного регионоведения и востоковедения факультета истории, социологии и международных отношений Кубанского государственного университета;

e-mail: marina.telenga@gmail.com; ORCID: 0009-0006-2221-5792;

Ткачёва Татьяна Олеговна (г. Краснодар) – кандидат исторических наук, доцент кафедры зарубежного регионоведения и востоковедения факультета истории, социологии и международных отношений Кубанского государственного университета;

e-mail: totkacheva2002@gmail.com

INFORMATION ABOUT THE AUTHORS

Marina P. Bezruchenko (Krasnodar) – Cand. Sci. (History), Assoc. Prof., Department of Foreign Regional Studies and Oriental Studies, Faculty of History, Sociology and International Relations, Kuban State University;

e-mail: marina.telenga@gmail.com; ORCID: 0009-0006-2221-5792;

Tatyana O. Tkacheva (Krasnodar) – Cand. Sci. (History), Assoc. Prof., Department of Foreign Regional Studies and Oriental Studies, Faculty of History, Sociology and International Relations, Kuban State University;

e-mail: totkacheva2002@gmail.com