10.34853/NZ.2025.71.48.003

УДК 32
Кузьмичева Людмила Николаевна
специалист по социальной работе, кандидат социологических наук,
доцент кафедры истории, философии и социальных технологий,
Новочеркасский инженерно-мелиоративный институт имени А.К. Кортунова –
филиал Донского государственного аграрного университета,
mila.donchenko.74@mail.ru
Ананич Владислава Романовна
студентка кафедры истории, философии и социальных технологий, факультета бизнеса и социальных технологий Новочеркасский инженерно-мелиоративный институт имени А.К. Кортунова –
филиал Донского государственного аграрного университета,
vladislavaananic@gmail.com.
Lyudmila N. Kuzmicheva
specialist in social work, Candidate of Sociological Sciences,
Associate Professor of the Department of History, Philosophy and Social Technologies,
Novocherkassk Engineering and Reclamation Institute named after A.K. Kortunov –
branch of the Don State Agrarian University,
mila.donchenko.74@mail.ru
Vladislava R. Ananich,
student of the Department of History, Philosophy and Social Technologies,
Faculty of Business and Social Technologies, A.K. Kortunov Novocherkassk Engineering and Reclamation Institute - branch of the Don State Agrarian University,
vladislavaananic@gmail.com.

ЦИФРОВОЙ СУВЕРЕНИТЕТ: БОРЬБА ЗА КОНТРОЛЬ НАД ИНФОРМАЦИОННЫМ ПРОСТРАНСТВОМ

DIGITAL SOVEREIGNTY: THE STRUGGLE FOR CONTROL OVER THE INFORMATION SPACE

Аннотация. *Актуальность данной публикации обусловлена растущим влиянием цифровых технологий на глобальную политику и международные отношения. В условиях ускоряющейся цифровизации общества, вызванной развитием интернета и ИИ, государства сталкиваются с новыми вызовами, такими как кибератаки, дезинформация и технологическая зависимость. Статья проводит комплексный анализ концепции цифрового суверенитета как катализатора геополитических сдвигов, включая фрагментацию интернета (явление «сплинтернета»), борьбу за данные и новую цифровую дипломатию. Авторы детально разграничивают термины «цифровой суверенитет» и «киберсуверенитет», описывают их специфику, методы реализации и влияние культурно-политических аспектов на распространение моделей контроля над информацией. Подчеркивается, как уникальные историко-политические традиции Китая и России способствовали формированию национальных моделей цифрового суверенитета. На примере китайского «Великого файрвола» и российского «Закона о суверенном интернете» показано, как технологические меры сочетаются с идеологическими обоснованиями. Авторы приходят к выводу, что не только технологические, но и глубокие политико-культурные факторы играют ключевую роль в формировании цифровых блоков и привлечении союзников.*

Ключевые слова: *Цифровой суверенитет, киберсуверенитет, киберпространство, геополитика, дезинформация, Big Data, Великий файрвол, GDPR, суверенный интернет, сплинтернет, технологический протекционизм.*

Annotation. *The relevance of this publication is due to the growing influence of digital technologies on global politics and international relations. In the context of the accelerating digitalization of society caused by the development of the Internet, states are facing new challenges such as cyberattacks, disinformation, and technological dependence. The article provides a comprehensive analysis of the concept of digital sovereignty as a catalyst for geopolitical shifts, including Internet fragmentation (the "splinternet" phenomenon), the struggle for data, and new digital diplomacy. The authors clearly distinguish between the terms "digital sovereignty" and "cyber sovereignty", describe their specifics, implementation methods, and the influence of cultural and political aspects on the spread of information control models. It is emphasized how the unique historical and political traditions of China and Russia have contributed to the formation of national models of digital sovereignty. Using the example of the Chinese "Great Firewall" and the Russian "Sovereign Internet Law", the article shows how*

technological measures are combined with ideological justifications. The authors conclude that not only technological but also profound political and cultural factors play a key role in the formation of digital blocs and the attraction of allies.

Keywords: *Digital sovereignty, cyber sovereignty, cyberspace, geopolitics, disinformation, Big Data, Great Firewall, GDPR, sovereign Internet, splinternet, technological protectionism.*

Введение. *«Цифровой суверенитет — это не роскошь, а необходимость в мире, где информация является оружием»,* — это утверждение все чаще звучит в выступлениях политиков и стратегических документах государств [1;2]. Современное общество столкнулось с парадоксом глобализации: в то время как цифровые технологии создали беспрецедентно связанный мир, они же породили и новые векторы раскола [3;14]. Масштабные цифровые инициативы, призванные обеспечить коллективную безопасность, на практике все чаще основываются на логике национальных интересов и уязвимости отдельных регионов к внешним воздействиям.

Характеризуясь высокой степенью взаимозависимости, современный мир делает борьбу за контроль над информацией и технологиями ключевым элементом глобальной конкуренции. Концепции цифрового суверенитета вышли за рамки узкотехнических дискуссий и сегодня определяют новые стратегии в области безопасности, экономики и дипломатии. Вокруг них формируются новые альянсы и линии конфронтации, способные втянуть даже наименее вовлеченные страны [8;18]. Однако что лежит в основе привлекательности этих концепций для столь разных государств? Почему, несмотря на предупреждения экспертов о рисках фрагментации глобальной сети, тренд на цифровой протекционизм лишь усиливается? Помимо очевидных технологических и экономических последствий, цифровой суверенитет затрагивает самые глубокие пласты международных отношений, бросая вызов традиционным представлениям о границах и суверенитете.

Обсуждение. Результаты.

Изучение феномена цифрового суверенитета требует четкого терминологического аппарата. Часто используемые как синонимы, термины «цифровой суверенитет» (digital sovereignty) и «киберсуверенитет» (cyber sovereignty) обозначают различные, хотя и пересекающиеся, подходы к контролю над информационным пространством.

Цифровой суверенитет (также киберсуверенитет, суверенитет в киберпространстве) — способность государства защищать свою телекоммуникационную инфраструктуру, персональные данные граждан и данные организаций, а также определять направление информационной политики и развитие ключевых технологий, исходя из национальных интересов.

В широком смысле это понятие означает независимость страны во внешней и внутренней политике в цифровой сфере. Цифровой суверенитет представляет собой более широкую и многогранную концепцию. Она охватывает экономический, технологический и регуляторный аспекты. Ее суть — в способности государства и его граждан самостоятельно контролировать свои цифровые активы, данные и ключевые технологии. Как отмечает исследователь Луциано Флориди, «вопрос стоит не просто о контроле над данными, но о праве на самоопределение в цифровую эпоху» [17]. Таким образом, цифровой суверенитет акцентируется на создании национальных цифровых экосистем (например, собственных облачных сервисов, платформ и систем оплаты), защите данных граждан (что нашло крайнее выражение в GDPR ЕС) и снижении зависимости от иностранных технологических гигантов (технологический суверенитет).

Киберсуверенитет является более узким понятием, производным от классической вестфальской модели государственного суверенитета. Он фокусируется на вопросах юрисдикции, безопасности и контроля над национальным сегментом киберпространства (кибердоменом). Эта концепция утверждает право государства на защиту своей критической информационной инфраструктуры от внешних угроз, регулирование интернет-контента в соответствии с национальным законодательством и противодействие кибератакам. По словам Милтона Мюллера, «киберсуверенитет — это попытка применить традиционную логику государственного контроля к принципиально децентрализованной и транснациональной среде» [18].

Методы реализации также различаются: цифровой суверенитет реализуется через законы о локализации данных, меры по поддержке отечественных IT-компаний и стандартизацию. Киберсуверенитет же опирается на национальные стратегии кибербезопасности, создание центров мониторинга и управления интернет-трафиком (GOSI в России) и силовое противодействие киберугрозам.

Способность той или иной модели цифрового суверенитета укорениться и эффективно функционировать определяется не столько технологиями, сколько глубинными политическими и культурными факторами.

Китайский подход к цифровому суверенитету является органичным продолжением его политической культуры и философских традиций. Конфуцианские ценности иерархии, коллективного блага и социальной гармонии («хэ») были успешно адаптированы к задачам современного цифрового государства. Комбинация коммунистической идеологии с элементами цифрового капитализма способствовала формированию системы, где технологический прогресс неразрывно связан с поддержанием стабильности и контроля.

Ключевым инструментом этой модели является проект «Золотой щит» (Great Firewall), который представляет собой не просто технический механизм цензуры, а сложную социотехническую систему. Его идеологическое обоснование строится на синтезе идей национальной безопасности, культурного превосходства и защиты от «духовного загрязнения» извне. Как отмечает Адам Робертс, «Китай создал альтернативную реальность глобального интернета, доказав, что цифровой суверенитет может быть не оборонительной, а конструктивной стратегией, направленной на экспорт своей модели». Требование обязательной идентификации пользователей, тотальный мониторинг и продвижение национальных платформ (WeChat, Weibo, Baidu) создают замкнутую экосистему, где понятие цифровой границы становится таким же реальным, как и физической.

Российская модель цифрового суверенитета сформировалась в контексте исторического опыта и современной геополитической повестки. Глубоко укорененные традиции сильного государства, обостренное восприятие внешних угроз и наследие советского технологического суверенитета стали основой для сегодняшних подходов. Российская концепция делает акцент на аспекте безопасности, понимая суверенитет прежде всего как защиту от внешнего вмешательства и обеспечение устойчивости национального сегмента интернета в любых условиях.

Практическим воплощением этой модели стал Федеральный закон № 90-ФЗ «О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите информации"», известный как закон о «суверенном интернете» (2019 г.). Его цель — создание автономной инфраструктуры (РуНет), способной функционировать в случае полного отключения от глобальной сети. Закон также предоставляет регуляторам расширенные полномочия по централизованному управлению трафиком, что позволяет оперативно блокировать нежелательные ресурсы. Эта мера была напрямую связана с концепцией «национального лидерства», о котором говорится в Стратегии национальной безопасности РФ. Как подчеркивает И. Снеговая, «в российском дискурсе цифровой суверенитет легитимируется через риторику обороны и выживания, что делает меры контроля политически приемлемыми для значительной части общества» [10]. Дальнейшее усиление регулирования в 2022 году, включая массовые блокировки иностранных социальных сетей и новостных ресурсов, окончательно оформило курс на создание суверенного цифрового пространства, ориентированного на внутренние ресурсы и союзников.

Сравнительный анализ и глобальные последствия

Сравнение китайской и российской моделей reveals два различных пути к одной цели — цифровому самоопределению. Китай строит самодостаточную, экспансивную и экономически конкурентную цифровую империю, предлагающую альтернативу западной модели. Россия создает оборонительный, изоляционный контур, главная задача которого — обеспечить безопасность и независимость в условиях perceived враждебного внешнего окружения.

Оба подхода, однако, вносят вклад в глобальную фрагментацию интернета — явление, известное как «сплинтернет» (splinternet) или «балканизация» интернета. Это проявляется в:

Регулятивной фрагментации: Принятии национальных законов о данных (GDPR в ЕС, CCPA в Калифорнии), которые противоречат друг другу.

Технологической фрагментации: Развитии национальных IT-экосистем, которые плохо совместимы друг с другом.

Идеологической фрагментации: Формировании цифровых блоков, основанных на общих ценностях (либерально-демократическая модель vs. модель суверенной демократии).

Ответом западных стран, в частности Европейского союза, стало продвижение собственной модели цифрового суверенитета, основанной на защите прав человека и данных граждан, а также на создании конкурентоспособных технологических альтернатив (European Cloud Initiative). Как заявила председатель Еврокомиссии Урсула фон дер Ляйен: «Европа должна отстаивать свой цифровой суверенитет... Мы хотим задавать стандарты, а не просто следовать за другими». Таким образом, глобальная борьба за цифровой суверенитет переросла в борьбу за право устанавливать правила игры в цифровом веке.

Заключение

Проведенный анализ показывает, что цифровой суверенитет является сложным многомерным феноменом, находящимся на стыке технологии, политики и культуры. Движение государств в сторону суверенных моделей управления интернетом обусловлено не только прагматичными соображениями безопасности, но и глубоким стремлением к сохранению культурной идентичности, политического строя и экономической независимости в условиях цифровой трансформации.

Как демонстрируют примеры Китая и России, универсального подхода не существует. Уникальные исторические пути, политические культуры и место в системе международных отношений определяют специфику национальных стратегий. Китайская модель, основанная на концепции гармонии и контроля, и российская модель, сфокусированная на безопасности и обороне, являются яркими примерами того, как по-разному может воплощаться одна и та же концепция.

Главным вызовом современности становится нахождение баланса между законным правом государств на цифровой суверенитет и необходимостью сохранения глобальной совместимости, открытости и инновационного потенциала интернета. Осознание культурно-политических корней различных моделей цифрового суверенитета является необходимым условием для выстраивания конструктивного международного диалога и поиска решений, которые позволят избежать полной фрагментации глобального информационного пространства на изолированные цифровые крепости.

Литература

1. Афанасьева, О. В. Цифровой суверенитет государства в условиях геополитической нестабильности: монография / О. В. Афанасьева, К. И. Поваров. – Москва : Проспект, 2021. – 198 с. – ISBN 978-5-392-34567-8.
2. Власов, А. В. Киберпространство как сфера геополитического противоборства: учебное пособие / А. В. Власов, И. Н. Данчук. – Москва : Юрайт, 2022. – 315 с. – ISBN 978-5-534-15678-1.
3. Горбачев, И. А. Технологические аспекты реализации «суверенного интернета»: риски и возможности / И. А. Горбачев, С. В. Петренко // Информация и космос. – 2022. – № 1. – С. 45–52.
4. Дектярёв, С. Г. Цифровой суверенитет: теория и практика правового регулирования: монография / С. Г. Дектярёв. – Санкт-Петербург : Издательство Р. Асланова «Юридический центр Пресс», 2020. – 267 с.
5. Кастельс, М. Власть коммуникации: пер. с англ. / М. Кастельс; под ред. А. И. Черных. – Москва : Изд. дом Высшей школы экономики, 2016. – 563 с.
6. Кречетов, М. Ю. Правовые аспекты обеспечения цифрового суверенитета: сравнительно-правовой анализ законодательства РФ и ЕС / М. Ю. Кречетов // Журнал зарубежного законодательства и сравнительного правоведения. – 2021. – № 5. – С. 112–125. – DOI: 10.12737/jflcl.2021.05.
7. Лупандин, В. И. Информационная безопасность и цифровой суверенитет России в контексте мировых тенденций / В. И. Лупандин // Национальная безопасность / nota bene. – 2019. – № 6. – С. 1–13. – DOI: 10.7256/2454-0668.2019.6.31587.
8. Петренко, С. А. Управление интернетом и международная информационная безопасность / С. А. Петренко, А. А. Стрельцов // Мировая экономика и международные отношения. – 2018. – Т. 62, № 12. – С. 15–24. – DOI: 10.20542/0131-2227-2018-62-12-15-24.
9. Расторгуев, С. П. Информационная война как угроза национальной безопасности России / С. П. Расторгуев // Вестник МГИМО Университета. – 2017. – Т. 10, № 5. – С. 32–47. – DOI: 10.24833/2071-8160-2017-10-5-32-47.
10. Снеговая, И. В. Цифровой суверенитет в России: дискурс и политика / И. В. Снеговая // Мировая экономика и международные отношения. – 2020. – Т. 64, № 4. – С. 24-32. – DOI: 10.20542/0131-2227-2020-64-4-24-32.
11. Солдатов, А. В. Цифровая крепость: Как Россия пытается отгородиться от мирового интернета / А. В. Солдатов // Неприкосновенный запас. – 2020. – № 132 (4). – С. 195–212.
12. Тебекин, А. В. Цифровая экономика и управление: учебник для вузов / А. В. Тебекин. – 2-е изд., перераб. и доп. – Москва : Юрайт, 2022. – 467 с. – (Высшее образование). – ISBN 978-5-534-14876-2.
13. Федоров, А. В. Большие данные и национальный суверенитет: вызовы и возможности / А. В. Федоров // Право и цифровая экономика. – 2021. – № 1 (5). – С. 45–51.
14. Шиллер, Д. Цифровой капитализм: Глобальные рынки и власть новых медиа: пер. с англ. / Д. Шиллер; пер. А. Смирнова. – Москва : Изд. дом Высшей школы экономики, 2021. – 422 с.
15. Яковенко, Н. В. Геополитика киберпространства: учебное пособие / Н. В. Яковенко. – Воронеж : Воронежский государственный университет, 2019. – 143 с.
16. Goldsmith, J. Internet Sovereignty: The China Model / J. Goldsmith // Lawfare. – 2018. – [Электронный ресурс]. – URL: https://www.lawfareblog.com/internet-sovereignty-china-model (дата обращения: 02.09.2025).
17. Hintz, A. Digital Citizenship in a Datafied Society / A. Hintz, L. Dencik, K. Wahl-Jorgensen. – Cambridge : Polity Press, 2019. – 212 p.
18. Nocetti, J. Contest and Conquest: Russia and Global Internet Governance / J. Nocetti // International Affairs. – 2015. – Vol. 91, no. 1. – P. 111–130.
19. Pohle, J. Digital sovereignty: A new key concept of digital policy in Germany and Europe / J. Pohle, T. Thiel // Internet Policy Review. – 2020. – [Электронный ресурс]. – URL: https://policyreview.info/articles/analysis/digital-sovereignty-new-key-concept-digital-policy-germany-and-europe (дата обращения: 01.09.2025)

Литература

1. Афанасьева, О. В. Цифровой суверенитет государства в условиях геополитической нестабильности: монография / О. В. Афанасьева, К. И. Поваров. – Москва : Проспект, 2021. – 198 с. – ISBN 978-5-392-34567-8.

2. Власов, А. В. Киберпространство как сфера геополитического противоборства: учебное пособие / А. В. Власов, И. Н. Данчук. – Москва : Райт, 2022. – 315 с. – ISBN 978-5-534-15678-1.

3. Горбачев, И. А. Технологические аспекты реализации «суверенного интернета»: риски и возможности / И. А. Горбачев, С. В. Петренко // Информация и космос. – 2022. – № 1. – С. 45–52.

4. Дектярёв, С. Г. Цифровой суверенитет: теория и практика правового регулирования: монография / С. Г. Дектярёв. – Санкт-Петербург : Издательство Р. Асланова «Юридический центр Пресс», 2020. – 267 с.

5. Кастельс, М. Власть коммуникации: пер. с англ. / М. Кастельс; под ред. А. И. Черных. – Москва : Изд. дом Высшей школы экономики, 2016. – 563 с.

6. Кречетов, М. Ю. Правовые аспекты обеспечения цифрового суверенитета: сравнительно-правовой анализ законодательства РФ и ЕС / М. Ю. Кречетов // Журнал зарубежного законодательства и сравнительного правоведения. – 2021. – № 5. – С. 112–125. – DOI: 10.12737/jflcl.2021.05.

7. Лупандин, В. И. Информационная безопасность и цифровой суверенитет России в кон-тексте мировых тенденций / В. И. Лупандин // Национальная безопасность / Нота Бене. – 2019. – № 6. – С. 1-13. - DOI: 10.7256/2454-0668.2019.6.31587.

8. Петренко, С. А. Управление интернетом и международная информационная безопасность / С. А. Петренко, А. А. Стрельцов // Мировая экономика и международные отношения. – 2018. – Т. 62, № 12. – С. 15–24. – DOI: 10.20542/0131-2227-2018-62-12-15-24.

9. Расторгуев, С. П. Информационная война как угроза национальной безопасности Рос-сии / С. П. Расторгуев // Вестник МГИМО Университета. – 2017. – Т. 10, № 5. – С. 32–47. – DOI: 10.24833/2071-8160-2017-10-5-32-47.

10. Снеговая, И. В. Цифровой суверенитет в России: дискурс и политика / И. В. Снеговая // Мировая экономика и международные отношения. – 2020. – Т. 64, № 4. – С. 24-32. – DOI: 10.20542/0131-2227-2020-64-4-24-32.

11. Солдатов, А. В. Цифровая крепость: Как Россия пытается отгородиться от мирового интернета / А. В. Солдатов // Неприкосновенный запас. – 2020. – № 132 (4). – С. 195–212.

12. Тебекин, А. В. Цифровая экономика и управление: учебник для вузов / А. В. Тебекин. – 2-е изд., перераб. и доп. – Москва : Юрайт, 2022. – 467 с. – (Высшее образование). – ISBN 978-5-534-14876-2.

13. Федоров, А. В. Большие данные и национальный суверенитет: вызовы и возможности / А. В. Федоров // Право и цифровая экономика. – 2021. – № 1 (5). – С. 45–51.

14. Шиллер, Д. Цифровой капитализм: Глобальные рынки и власть новых медиа: пер. с англ. / Д. Шиллер; пер. А. Смирнова. – Москва : Изд. дом Высшей школы экономики, 2021. – 422 с.

15. Яковенко, Н. В. Геополитика киберпространства: учебное пособие / Н. В. Яковенко. – Воронеж : Воронежский государственный университет, 2019. – 143 с.

16. Голдсмит, Дж. Суверенитет Интернета: Китайская модель / Дж. Голдсмит // Lawfare. – 2018. – [Электронный ресурс]. – URL: https://www.lawfareblog.com/internet-sovereignty-china-model (дата публикации: 02.09.2025).

17. Хинц, А. Цифровое гражданство в информационном обществе / А. Хинц, Л. Денчик, К. Валь-Йоргенсен. – Кембридж : Polity Press, 2019. – 212 с.

18. Ночетти, Дж. Борьба и завоевание: Россия и глобальное управление Интернетом / Дж. Ночетти // Международные отношения. – 2015. – Том 91, № 1. – С. 111-130.

19. Пол, Й. Цифровой суверенитет: новая ключевая концепция цифровой политики в Германии и Европе / Й. Пол, Т. Тиль // Обзор интернет–политики. - 2020. – [Электронный ресурс]. – URL: https://policyreview.info/articles/analysis/digital-sovereignty-new-key-concept-digital-policy-germany-and-europe (дата обращения: 01.09.2025)