

4. Ильин Е.П. Психология общения и межличностных отношений. СПб.: Питер, 2018. 592 с. ISBN 978-5-496-01604-9.
5. Кибанов А.Я., Захаров Д.К., Коновалова В.Г. Этика деловых отношений: учебник. М.: ИНФРА-М; 2023. 383 с. ISBN 978-5-16-006723-0.
6. Стенина Н. Скрытые возможности соцмедиа: от цифр к глубокому пониманию целевой аудитории // Baltic PR Weekend: материалы конференции. Санкт-Петербург, 2025. С. 1–22.
7. Филатова О.Г. Электронное взаимодействие власти и общества: медиаэкосистемный подход: диссертация ... доктора политических наук / Филатова Ольга Георгиевна, 2024. 365 с.
8. Couldry N., Hepp A. The Mediated Construction of Reality. Cambridge: Polity Press, 2017. 290 p.
9. World PR Report 2022-2023 / ICCO PR [Electronic resource]. URL: <https://iccopr.com/world-pr-report-2022-2023/>
10. Zuboff Sh. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: Public Affairs, 2019. 704 p. ISBN 978-1610395694.

DOI: 10.34773/EU.2026.4.13

Цифровой суверенитет как инструмент экономической и внешнеполитической стратегии*

Digital Sovereignty as a Tool of Economic and Foreign Policy Strategy

Р. ХУЖИН

Хужин Рашит Аетбаевич, канд. пед. наук, доцент кафедры социально-гуманитарных дисциплин и цифровых технологий Башкирской академии государственной службы и управления при Главе Республики Башкортостан. E-mail: rashit805@gmail.com

Аннотация. В условиях обострившегося технологического соперничества и беспрецедентного по масштабу санкционного давления цифровой суверенитет приобрёл значение стратегического инструмента экономической и внешнеполитической политики государства. Исследование преследует цель сопоставить модели цифрового суверенитета в ЕС, КНР и РФ и оценить их устойчивость. Методологическую основу работы образуют сравнительно-аналитический подход и анализ стратегических документов. Проведённый анализ показывает, что российская модель, опирающаяся на оборонительное импортозамещение, обнаруживает наибольшую адаптивность в условиях внешней блокады. В работе обоснована необходимость перехода к «уместному суверенитету», сочетающему технологическую безопасность с избирательной открытостью.

Ключевые слова: цифровой суверенитет, технологическая безопасность, импортозамещение, стратегическая устойчивость, геоэкономика, фрагментация интернета, сплинтернет, национальная безопасность, оборонительная модель, цифровая зависимость.

Abstract. Under conditions of technological rivalry and unprecedented sanctions pressure, digital sovereignty has become a strategic instrument of economic and foreign policy. The study aims to compare digital sovereignty models in the EU, China, and Russia and assess their resilience. A comparative-analytical approach and analysis of strategic documents were employed. The research establishes that the Russian model, grounded in defensive import substitution, demonstrates the highest degree of adaptability under external blockade conditions. The necessity of transitioning toward «contextual sovereignty» combining technological security with selective openness is substantiated.

Key words: digital sovereignty, technological security, import substitution, strategic resilience, geo-economics, internet fragmentation, splinternet, national security, defensive model, digital dependency.

* Ссылка на статью: Хужин Р.А. Цифровой суверенитет как инструмент экономической и внешнеполитической стратегии // Экономика и управление: научно-практический журнал. 2026. № 4. С. 76–80. DOI: 10.34773/EU.2026.4.13.

Основные положения

1. Цифровой суверенитет претерпел трансформацию, превратившись из узкотехнической категории в стратегический инструмент геоэкономической и внешнеполитической политики, позволяющий государствам управлять критическими технологическими зависимостями и проецировать национальные ценности на международную арену.
2. В современной практике различаются три доминирующие модели. Регуляторно-ценностная модель (ЕС) ориентирована на защиту прав граждан, однако ограничена зависимостью от внешних платформ. Технологически-автономная модель (Китай) нацелена на самодостаточность, но остаётся уязвимой перед ограничениями на передовое оборудование. Оборонительно-импортозамещающая модель (Россия) проявляет наибольшую стратегическую устойчивость благодаря системному подходу к обеспечению технологической независимости в условиях беспрецедентного санкционного давления.
3. Политика цифрового суверенитета способствует фрагментации глобального цифрового пространства, описываемой терминами «сплинтернет» и «балканизация», однако полная технологическая автаркия недостижима даже для крупных держав. Наиболее перспективной представляется модель «уместного суверенитета», сочетающая управление критическими зависимостями с избирательной открытостью, причём российская модель обнаруживает здесь наибольшую адаптивность и прагматичность.

Введение

В современных международных отношениях всё отчётливее проявляется стремление государств установить контроль над цифровой сферой, охватывающей технологии, данные, интернет-инфраструктуру и цифровые платформы. Обострение указанного процесса обусловлено рядом глобальных вызовов. Пандемия COVID-19 резко усилила зависимость общества от цифровых сервисов. Геополитическая напряжённость возросла на фоне санкций и технологического соперничества. Правовые споры между ЕС и США по вопросам регулирования цифровых компаний приобрели затяжной характер. Одновременно американские и китайские технологические гиганты ведут активную экспансию на мировых рынках [2].

Глобальное распространение цифровых технологий породило глубокую взаимозависимость между странами. Одни страны производят микрочипы, другие создают программное обеспечение, третьи выпускают оборудование, тогда как данные циркулируют через инфраструктуру, нередко контролируемую иностранными компаниями. В сложившихся условиях государства стремятся одновременно извлекать выгоду из взаимосвязанности и минимизировать риски, сопряжённые с чрезмерной зависимостью от внешних источников. Экономические инструменты, включая экспортные ограничения, санкции и регулирование иностранных платформ, всё чаще применяются не как альтернатива военным действиям, а как их продолжение в мирное время.

В обозначенном контексте цифровой суверенитет перестал быть исключительно техническим понятием. Китай и Россия делают ставку на контроль над информационным пространством и защиту от «внешнего влияния», рассматривая интернет как зону национальной безопасности. Евросоюз утверждает, что стремится обеспечить суверенитет через регулирование, охватывающее защиту данных, честную конкуренцию и этическое использование технологий. Цифровой суверенитет тем самым выступает стратегическим инструментом, посредством которого государства формируют собственные позиции в условиях технологического соперничества, санкционного давления и фрагментации глобальных цепочек создания стоимости.

В российской научной литературе обозначенная проблематика разрабатывается достаточно активно. О.А. Мельникова рассматривает цифровой суверенитет в качестве компонента национальной безопасности в условиях санкций [1]. Т.В. Науменко акцентирует его геополитическую роль [3]. Л.А. Подосинникова раскрывает механизм «секьюритизации» цифрового пространства в условиях гибридной угрозы [4]. К.Н. Секретарева проводит сравнительный анализ моделей ЕС, КНР и РФ, выявляя различия в их ценностных основаниях, к которым относятся либерально-регуляторный подход Европы, технологически-автономный подход Китая и оборонительно-адаптивный подход России [5]. Вместе с тем недостаточно изученным остаётся

вопрос о том, каким образом цифровой суверенитет функционирует как инструмент экономической и внешнеполитической политики и какие риски он несёт в условиях фрагментации интернета.

Цель настоящей статьи состоит в анализе цифрового суверенитета как практического инструмента государственной политики на материале трёх доминирующих моделей (ЕС, КНР, РФ) с рассмотрением эволюции понятия, конкретных экономических механизмов, рисков фрагментации цифрового пространства и сравнительной устойчивости моделей.

Методы

Методологическую основу исследования составляет сравнительно-аналитический подход, позволяющий выявить особенности реализации цифрового суверенитета в различных геополитических и экономических контекстах. Выбор трёх акторов (ЕС, КНР и РФ) обусловлен их доминирующей ролью в формировании глобальной повестки и принципиальными различиями в ценностных основаниях, к которым относятся либерально-регуляторный подход (ЕС), технологически-автономный подход (КНР) и оборонительно-адаптивный подход (РФ).

В работе применены анализ официальных стратегических документов (программа Made in China 2025, инициативы Еврокомиссии по цифровому рынку, российские концепции цифровой трансформации), контент-анализ публикаций ведущих российских исследователей и качественный анализ конкретных кейсов, охватывающих регулирование 5G в ЕС, развитие национальной микроэлектроники в России и политику локализации данных в КНР. Применённый методологический инструментарий обеспечивает теоретическую глубину и эмпирическую обоснованность выводов.

Результаты

Цифровой суверенитет претерпел трансформацию из узкотехнической категории в ключевой элемент геоэкономической стратегии. В условиях технологического национализма, применения санкций в качестве инструмента гибридной войны и фрагментации глобальных цепочек создания стоимости он выступает одновременно механизмом управления критическими зависимостями и инструментом проекции национальных ценностей [2; 3]. На основе анализа стратегических документов и кейсов выделены три доминирующие модели.

Европейская модель базируется на регуляторном подходе, охватывающем защиту персональных данных, демократических свобод и честной конкуренции. Отсутствие собственных цифровых гигантов компенсируется жёстким регулированием т.н. GAFA (Google, Apple, Facebook, Amazon). В 2021 году председатель Совета ЕС Шарль Мишель заявил, что без цифрового суверенитета невозможна стратегическая автономия [2]. Тем не менее внутри ЕС сохраняются разногласия относительно баланса между автономией и трансатлантическим партнёрством, наиболее остро проявляющиеся в дискуссиях вокруг 5G и участия китайских компаний в телекоммуникационной инфраструктуре. В результате Европа остаётся технологически зависимой и ограничивается регулированием чужих платформ.

Китайская модель реализуется посредством стратегии «самодостаточности», провозглашённой в программе Made in China 2025 и предполагающей масштабные государственные инвестиции в полупроводниковую промышленность, искусственный интеллект и 5G, экспорт цифровых стандартов через «Цифровой пояс и путь», а также продвижение концепции «информационного суверенитета» в ООН [4]. Тем не менее Пекин остаётся уязвимым перед ограничениями на передовое оборудование, что свидетельствует о невозможности полной технологической автаркии даже при наличии мощного государственного ресурса.

Российская модель, в отличие от европейской и китайской, обнаруживает наибольшую устойчивость в условиях беспрецедентного внешнего давления. С 2014 года, а в особенности после 2022 года, страна последовательно реализует оборонительно-импортозамещающий подход, ориентированный не на идеализированную автономию, а на обеспечение минимально необходимой технологической независимости в стратегически важных секторах. Несмотря на исторически сложившуюся зависимость от архитектуры ARM (процессоры Baikal Electronics) и

производственных мощностей компании TSMC, санкционное давление стало катализатором системной перестройки цифровой экосистемы [3].

В настоящее время в стране функционируют отечественные микропроцессоры, разработаны суверенные операционные системы, созданы национальные платёжные и финансовые инфраструктуры (Система передачи финансовых сообщений Банка России – СПФС, платежная система «Мир»). Перечисленные меры не преследуют цели полной замены глобальных технологий, однако обеспечивают минимально необходимый уровень технологической безопасности, позволяющий государству сохранять суверенитет даже в условиях гибридной войны. Российская модель сочетает целенаправленное управление критическими зависимостями с избирательной открытостью в некритических сферах и оказывается наиболее прагматичной.

Исследование подтвердило, что политика цифрового суверенитета способствует фрагментации глобального цифрового пространства. Термины «балканизация» и «сплинтернет» всё чаще описывают распад единого интернета на изолированные национальные сегменты. Россия усиливает контроль над Рунетом, Китай развивает «Великий китайский файрвол», ЕС ужесточает регулирование трансграничных потоков данных [4]. Полная изоляция при этом представляется маловероятной, поскольку даже в условиях санкций сохраняется взаимозависимость в области стандартов, протоколов и базовых технологий.

В ходе исследования выявлены ключевые экономические инструменты цифрового суверенитета, к числу которых относятся налогообложение цифровых платформ (цифровой налог ЕС на доходы GAFA), локализация данных (РФ, КНР, Индия), государственные инвестиции в критические технологии, регулирование 5G (запрет оборудования Huawei в ряде стран ЕС и в США) и создание альтернативных цифровых экосистем (WeChat, Alipay, «Мир», СПФС). С одной стороны, перечисленные меры повышают технологическую устойчивость, с другой – создают барьеры для международной торговли и инноваций. Вместе с тем именно в условиях гибридной войны российский подход оказывается наиболее адекватным, поскольку обеспечивает не абсолютную независимость, а стратегическую устойчивость, понимаемую как способность функционировать и развиваться даже под внешним давлением.

Обсуждение

Анализ современной геополитической и технологической конъюнктуры свидетельствует о том, что цифровой суверенитет трансформировался в стратегический инструмент государственной политики, охватывающий не только защиту национальных технологических интересов, но и проекцию политических ценностей, а также формирование устойчивых моделей развития в условиях гибридных угроз. Принципиальные различия между тремя моделями отражают специфику национальной стратегической культуры, степень технологической зрелости и характер внешнеполитических приоритетов.

Европейская модель позиционирует ЕС в качестве «третьего пути» между американским неолиберализмом и китайским технологическим авторитаризмом [6]. Однако, по мнению Л.А. Подосинниковой, внутренние разногласия стран-членов по вопросам баланса между стратегической автономией и трансатлантическим партнёрством существенно снижает эффективность единой политики [4]. В итоге Европа остаётся зависимой от внешних платформ и ограничивается их регулированием, не формируя собственной технологической архитектуры.

Китайская стратегия «самодостаточности» наталкивается на фундаментальное противоречие. Масштабные государственные инвестиции не позволяют Пекину преодолеть технологическое отставание в производстве передовых чипов, поскольку критически важное оборудование по-прежнему поставляется из стран Запада. Сложившаяся ситуация свидетельствует об иллюзорности полной технологической автаркии в условиях глобализированных цепочек создания стоимости.

В сложившихся условиях российская модель обнаруживает наибольшую стратегическую прагматичность. Как подчёркивает О.А. Мельникова, попытки полной изоляции действительно ведут к технологическому отставанию, однако российская стратегия не предполагает автаркии

и направлена на целенаправленное управление критическими зависимостями [1]. Ключевым преимуществом выступает способность к быстрой адаптации и мобилизации ресурсов в условиях кризиса. Отечественные процессоры, суверенные операционные системы и национальные платёжные инфраструктуры представляют собой не замену глобальных технологий, а обеспечение минимально необходимого уровня технологической безопасности, позволяющего государству сохранять суверенитет в условиях гибридной войны.

Таким образом, российская стратегия сочетает прагматизм, системность и оборонительную направленность, минимизируя уязвимости в стратегически важных секторах при сохранении избирательной открытости в некритических областях. Именно подобный подход позволяет обеспечивать технологическую устойчивость в условиях глобальной нестабильности.

Заключение

Проведённое исследование подтверждает, что цифровой суверенитет представляет собой ключевой элемент геэкономической и внешнеполитической стратегии, напрямую связанный с управлением технологическими зависимостями, проекцией национальных ценностей и обеспечением безопасности в условиях фрагментации глобального цифрового пространства. Анализ трёх моделей выявил их принципиальные различия. Европейская модель носит регуляторно-ценностный характер, однако ограничена технологической зависимостью и внутренними разногласиями. Китайская модель ориентирована на автономию и экспорт «технологического авторитаризма», но уязвима к санкциям на оборудование. Российская модель обнаруживает наибольшую устойчивость благодаря прагматичному оборонительно-импортозамещающему подходу. Исследование подтвердило, что политика цифрового суверенитета ускоряет фрагментацию глобального цифрового пространства, однако полная технологическая автаркия недостижима, что обосновывает переход к модели «уместного суверенитета», сочетающей управление критическими зависимостями с избирательной международной открытостью.

Научная новизна работы заключается в систематизации экономических инструментов реализации цифрового суверенитета и выявлении их двойственной природы, состоящей в том, что повышение технологической устойчивости сопровождается возникновением барьеров для торговли и инноваций. Практическая значимость состоит в возможности использования полученных результатов при разработке государственной политики цифровой трансформации и управления критическими технологическими зависимостями. Перспективы дальнейших исследований связаны с количественной оценкой фрагментации цифрового пространства и разработкой методик оценки уязвимости национальных экономик к технологическим санкциям.

Литература

1. Мельникова О.А. Международный союз электросвязи – технический регулятор или арена нового противостояния // *Международная жизнь*. 2021. № 8. С. 78–83.
2. Многовекторность во внешней политике стран постсоветского пространства: актуальные проблемы и тенденции / М.В. Катагощина, В.В. Комлева, Е.А. Кузьменко, С.А. Шеин // *Россия и мир: научный диалог*. 2024. № 4(14). С. 105–123. DOI 10.53658/RW2024-4-4(14)-105-123.
3. Науменко Т.В. Технологический аспект парадигмы информационного общества // *Информационное общество*. 2023. № 3. С. 2–7. DOI 10.52605/16059921_2023_03_02.
4. Подосинникова Л.А. Национальная безопасность как результат развития внутреннего правового суверенитета // *Образование и право*. 2025. № 6. С. 37–50. DOI 10.24412/2076-1503-2025-6-37-50.
5. Секретарева К.Н. Цифровая трансформация и её влияние на внешнюю политику Китая // *Информационное общество*. 2025. № 1. С. 143–151. DOI 10.52605/16059921_2025_01_143.
6. Спирина М.Ю. Традиционные ценности и евразийская культура // *Евразийство: теоретический потенциал и практические приложения*. 2022. № 11. С. 38–43.