CC BY

http://dx.doi.org/10.35596/1729-7648-2026-32-1-5-11

УДК 338.2

ФАКТОРЫ ФОРМИРОВАНИЯ ЦИФРОВОГО СУВЕРЕНИТЕТА ГОСУДАРСТВА В УСЛОВИЯХ ГЕОПОЛИТИЧЕСКОЙ ТУРБУЛЕНТНОСТИ

Е. Ю. РАКОВА

Белорусский государственный экономический университет (Минск, Республика Беларусь)

Аннотация. По мере проникновения цифровых технологий в экономику, политику и повседневную жизнь концепция цифрового суверенитета приобретает все большее значение. Однако в литературе отсутствует универсальное определение. Научная новизна исследования заключается в систематизации основных концепций цифрового суверенитета и подходов различных стран к его реализации. Особый интерес представляет анализ внутренних и внешних факторов, определяющих степень стратегической цифровой автономии того или иного государства. Аргументы автора склоняются в пользу гибкой стратегии, направленной на достижение стратегической автономии в критических областях при одновременном использовании преимуществ международной технологической кооперации, а также усилении применения мягких образовательных и просветительных мер и инструментов.

Ключевые слова: цифровой суверенитет, цифровая безопасность, информационный суверенитет, информационная безопасность, интернет-суверенитет, суверенитет данных, информационно-коммуникационные технологии, искусственный интеллект.

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Для цитирования. Ракова, Е. Ю. Факторы формирования цифрового суверенитета государства в условиях геополитической турбулентности / Е. Ю. Ракова // Цифровая трансформация. 2026. Т. 32, № 1. С. 5–11. http://dx.doi.org/10.35596/1729-7648-2026-32-1-5-11.

FACTORS IN THE FORMATION OF STATE DIGITAL SOVEREIGNTY IN THE CONDITIONS OF GEOPOLITICAL TURBULENCE

ELENA RAKOVA

Belarus State Economic University (Minsk, Republic of Belarus)

Abstract. As digital technologies permeate the economy, politics, and everyday life, the concept of digital sovereignty is gaining increasing importance. However, a universal definition is lacking in the literature. The research's novelty lies in its systematization of the key concepts of digital sovereignty and the approaches various countries take to implementing it. Of particular interest is the analysis of the internal and external factors that determine the degree of strategic digital autonomy for each state. The author argues for the need for a flexible strategy aimed at achieving strategic autonomy in critical areas while simultaneously leveraging the benefits of international technological cooperation and strengthening the use of soft educational and awareness-raising measures and tools.

Keywords: digital sovereignty, digital security, information sovereignty, information security, internet sovereignty, data sovereignty, information and communication technologies, artificial intelligence.

Conflict of interests. The author declares that there is no conflict of interests.

For citation. Rakova E. (2026) Factors in the Formation of State Digital Sovereignty in the Conditions of Geopolitical Turbulence. *Digital Transformation.* 32 (1), 5–11. http://dx.doi.org/10.35596/1729-7648-2026-32-1-5-11 (in Russian).

Введение

Цифровой суверенитет определяется сложным балансом внутренних и внешних факторов. В настоящее время внешние факторы являются драйвером суверенизации и сегментации интернета. Однако важными представляются и внутренние факторы, на которые государство может и должно влиять.

Исходя из проведенного анализа, предложены некоторые меры государственной политики, которые будут способствовать развитию и укреплению цифрового суверенитета. Начало XXI в. было стартом деглобализации и распада мировых хозяйственных связей. По мере обострения экономических и политических противоречий набирает популярность концепция суверенитета как противоположность различным проявлениям гегемонизма, будь то гегемония США в международных отношениях или гегемония частных корпораций [1, с. 130]. Идеи суверенизации коснулись и цифровой сферы. По мере развития информационно-коммуникационных технологий (ИКТ) и глобального лидерства западных стран появляется интерес к защите собственного информационного пространства и суверенизации критической информационной инфраструктуры. Лидером становится Китай, первым начавший жестко и последовательно защищать свои «виртуальные» границы. Постепенно в научной литературе появляются концепции интернет-суверенитета, информационного и цифрового суверенитета.

Теоретические аспекты понятия «цифровой суверенитет»

Следует отметить, что хотя проблематика формулирования и реализации права государства на суверенитет в сфере ИКТ давно существует, в литературе отсутствует единое научное определение цифровой независимости или цифрового суверенитета. Каждый автор видит его по-разному, а суть понятия варьируется от цифрового до информационного суверенитета или безопасности, используя в определении комбинацию ключевых слов: суверенитет, технологии, инфраструктура и данные [1–6].

Представленные в статье концепции являются ответом на глобализацию и цифровизацию и направлены на усиление роли государства в управлении и контроле над различными аспектами цифрового пространства. Технологический суверенитет стоит в основании пирамиды, обеспечивая способность создавать «железо» и «софт». Суверенитет данных отвечает на вопрос «Что регулируется?». Информационный суверенитет отвечает на вопрос «Зачем?», а интернет-суверенитет – на вопрос «Как?». Обобщает все концепции понятие «цифровой суверенитет», включающее в себя все составляющие подлинной независимости: от верховенства права до контроля над данными и технологиями.

Рассмотрим более подробно различные виды концепций:

• технологический суверенитет – это способность государства проводить независимую политику в сфере высоких технологий [1, с. 90]. Он реализуется на базовом уровне, обеспечивающем физический контроль над сетями и инфраструктурой. Сюда относят владение ключевыми технологиями, которые считаются критически важными для обеспечения функционирования основных институтов государства и конкурентоспособности: контроль над магистральными каналами передачи данных, точками обмена интернет-трафиком (IXP), сетями мобильной связи (4G/5G); наличие и управление собственными дата-центрами; независимая работа энергосистем, финансовых сетей, транспорта, которые управляются цифровыми системами; национальные системы доменных имен (DNS), позволяющие интернету работать внутри страны, даже если связь с глобальными серверами прервана;

• суверенитет данных – контроль над хранением и обработкой данных, а также «рациональные действия национальных государств, направленные на установление контроля над потоками конфиденциальных данных внутри собственных границ и за их пределами» [8, с. 10]. Можно сказать, что это правовой принцип, согласно которому информация (особенно персональные данные) подчиняется законам и нормам страны, на территории которой она находится. Таким образом, объектом защиты являются данные, а инструментами защиты – законы о защите данных, требования локализации данных (хранения на территории страны), их шифрование. Этот подход зачастую является самым конкретным и юридически оформленным в национальных юрисдикциях. Ключевые элементы – рациональные действия национальных государств, направленные

на установление локализации и контроля над потоками, хранением и обработкой данных внутри собственных границ и за их пределами. Другими словами, суверенитет данных – это обеспечение юрисдикции государства над данными на своей территории, их защита от несанкционированного доступа иностранных государств и компаний. Негативным следствием сильного суверенитета данных может являться фрагментация интернета (распад единого информационного пространства на ряд самостоятельных подсистем), однако «сама по себе такая политика сопряжена со значительными издержками, возникающими вследствие цифровой и физической изоляции страны» [8, с. 10];

• информационный суверенитет. В этом подходе подчеркивается исключительное право государства на определение информационной политики, задается идеологическая и ценностная рамка регулирования. Фокус смещается на защиту информационного пространства от деструктивного влияния извне, ориентацию на национальные интересы, обеспечение доминирования национальной культуры и идеологии. Его инструменты – политические и правовые режимы обработки данных, суверенное право страны проводить собственную информационную политику, т. е. контроль не только над технологической инфраструктурой, но и над способами создания и передачи информации. Важность данной концепции можно подчеркнуть тезисом, что информационный суверенитет является разновидностью государственного суверенитета [7, с. 119];

• интернет-суверенитет, или суверенный интернет, – способность государства обеспечивать устойчивое и независимое функционирование национального сегмента сети интернет, включая управление его критической инфраструктурой даже в условиях разрыва соединений с глобальной сетью [3, с. 78]. Именно поэтому иногда встречается такое определение, как сетевой суверенитет. Объектами регулирования являются интернет-инфраструктура и трафик. Это самый технически ориентированный вид суверенитета. Он направлен непосредственно на архитектуру и управление сетью интернет. Его цели – обеспечивать права государства устанавливать собственные правила функционирования интернет-пространства, отвечающие национальным традициям и интересам, гарантировать устойчивость и управляемость национального сегмента интернета, его защиту от внешних отключений и угроз. Инструментами государственной политики в данном случае являются национальное законодательство, контроль за интернет-провайдерами, фильтрация контента, ограничение доступа к ресурсам;

• цифровой суверенитет – самое широкое понятие. Объект регулирования в данной концепции – цифровая экосистема в целом, т. е. государство осуществляет контроль над коммуникационной инфраструктурой и интернетом в пределах национальных границ, обеспечивает независимость программного обеспечения и платформенной экономики, в том числе через национальные поисковые системы, социальные сети, почтовые сервисы, а также суверенитет данных. Главная цель – достижение технологической автономии, способности самостоятельно развивать и поддерживать критически важные цифровые технологии.

Таким образом, «цифровой суверенитет представляет собой способность государства самостоятельно, без вмешательства извне, определять порядок использования цифровых технологий, регулировать процессы сбора и обработки данных, а также обеспечивать безопасность и устойчивое функционирование национального сегмента информационно-коммуникационной сети интернет» [5, с. 40]. Можно сказать, что цифровой суверенитет – это стратегическая цель государства, тогда как другие концепции будут являться тактиками по ее достижению.

Правовые аспекты реализации цифрового суверенитета

В современном турбулентном мире каждая страна в меру своих возможностей и ограничений реализует концепцию информационного и цифрового суверенитета. Так, технологические компании США обязаны передавать данные о телефонных звонках, текстовых сообщениях и электронных письмах разведывательным службам США, включая ФБР, ЦРУ и АНБ. Тенденция последних лет – защита лидерства США в области критических технологий. Промышленный протекционизм и система ограничительных мер (например, на поставки высокотехнологичного оборудования в Китай в области искусственного интеллекта и облачных вычислений), а также масштабные инвестиции во внутренние исследования и стимулирование производства полупроводников в США призваны стимулировать внутреннее производство. То есть формально США стоят на принципах свободного интернета, однако в реальности все больше используют те или иные ограничительные и запретительные меры.

Европейский союз активно применяет различные нормативно-регуляторные меры защиты цифрового суверенитета. Основными инструментами являются Общий регламент по защите данных (General Data Protection Regulation, GDPR), который определяет порядок сбора, обработки, хранения и распространения персональных данных в странах Евросоюза, и Закон о цифровых услугах (EC) (Digital Services Act). На социальные сети, поисковые системы и торговые площадки, такие как Apple, Google, TikTok и Amazon, возложены дополнительные обязательства по борьбе с распространением незаконного контента, разжиганием ненависти, с дезинформацией и коммерческим мошенничеством (неправильный контент необходимо мониторить и немедленно уничтожать). Закон стал предметом судебных разбирательств между Европейской комиссией и американскими цифровыми компаниями, а также причиной огромных штрафов. В целом используется широкий набор мер и инструментов, направленных на защиту собственного цифрового суверенитета, иногда даже в ущерб глобальной конкурентоспособности. Таким образом, на Западе под цифровым суверенитетом понимают государственный контроль над инфраструктурой, программным обеспечением и данными.

В Китае на смену Великой китайской стены пришел Великий китайский файрвол (The Great Firewall of China). Одна из особенностей китайского файрвола – специальное программное обеспечение, закрывающее проникновение западных сервисов и заменяющее их местными аналогами. Другая особенность – создание аналогов западных платформ и мессенджеров. Так, китайцы переписываются в WeChat вместо Telegram, ищут информацию в Baidu, а не в Google, заказывают товары на Taobao, а не на Amazon. Страна активно развивается, у нее есть выбор всех западных программ, платформ и технологий, но на собственном технологическом базисе, с закрытием внешнего контура.

В России и Китае большое значение уделяется контролю над трансграничным контентом [1, 5]. То есть на первый план выходит концепция информационного суверенитета. Национальное законодательство страны создает правовую базу для централизованного управления интернетом в государственных границах. Большое внимание Россия уделяет строительству собственной инфраструктуры и созданию национальных программных продуктов и решений.

Беларусь также активно развивается в поиске своего места и возможностей в цифровом мире. Согласно Концепции обеспечения суверенитета Республики Беларусь в сфере цифрового развития до 2030 года, под суверенитетом в сфере цифрового развития понимается «неотъемлемое право государства управлять государственной информационно-коммуникационной инфраструктурой и информационными ресурсами, осуществлять над ними контроль, защищать свои интересы и проводить независимую внешнюю и внутреннюю государственную политику в сфере цифрового развития» [9]. В то же время Концепция не дает четкого и исчерпывающего определения цифрового суверенитета. Согласно Концепции, «суверенитет в сфере цифрового развития является частью обеспечения информационной безопасности Республики Беларусь». В числе приоритетов проекта стратегии – формирование в стране экономики данных, разработка цифровых сервисов, стимулирование разработки и перехода на собственные программные продукты и информационные технологии. Правительству и бизнесу предстоит большая работа по наполнению их конкретными проектами и программами.

Внутренние и внешние факторы, определяющие цифровой суверенитет

Цифровой суверенитет – это не статичное состояние, а динамический результат непрерывного взаимодействия различных факторов, определяющих амбиции и возможности страны. На уровень стратегической автономии в эпоху цифровых технологий оказывает влияние тонкий баланс между национальной безопасностью, экономической стабильностью и сохранением культурно-политической идентичности в условиях, когда большая часть жизни переместилась в онлайн, управляемый извне. Можно сказать, что цифровой суверенитет в глобальном мире – это возможность проводить сбалансированную экономическую политику, используя глобальные технологии и одновременно инвестируя в собственные технологии и образование, создавая гибкое законодательство и противодействуя внешним вызовам.

Факторы, влияющие на цифровой суверенитет, носят комплексный характер и охватывают технологическую, экономическую, правовую и геополитическую сферы. Их можно разделить на внутренние (зависящие от действий самого государства, на которые оно может влиять) и внешние (объективные вызовы и угрозы).

Внутренние факторы:

– технологические и инфраструктурные: уровень развития собственной IT-отрасли, состояние критической информационной инфраструктуры (КИИ – устойчивость сетей, энергосистем, финансового и банковского секторов к кибератакам и внешним воздействиям, зависимость от иностранного программного обеспечения и технологий, наличие и качество телекоммуникационных сетей);

– экономические (ВВП, объем инвестиций в НИОКР, конкурентоспособность IT-отрасли, доля электронного бизнеса и IT-технологий в ВВП);

– правовые и регуляторные: наличие и качество законодательства (законы о защите персональных данных, КИИ, о суверенном интернете, регулировании техкорпораций), качество и эффективность управления государства в цифровой среде (электронное правительство), борьба с киберпреступностью;

– кадровые и образовательные (качество и количество IT-специалистов, уровень цифровой грамотности населения, состояние системы образования);

– социокультурные (уровень доверия к государству в цифровой сфере, культурная, ментальная и языковая специфика, ценности).

Внешние факторы в настоящее время становятся главным драйвером фрагментации и суверенизации интернета, прочерчивая виртуальные национальные границы в ранее свободной и открытой сети. Именно они стимулируют государство к созданию замкнутых контролируемых цифровых систем. Среди основных внешних факторов можно отметить:

- геополитическую конкуренцию и санкционное давление;
- деятельность глобальных технологических корпораций (Big Tech);
- развитие ИКТ, под которыми понимаются весь спектр и комплекс объектов, действий и правил, связанных с подготовкой, переработкой, доставкой информации при персональной, массовой и производственной коммуникации, а также все технологии и отрасли, интегрально обеспечивающие перечисленные процессы. Следует подчеркнуть, что эти технологии могут как подрывать цифровой суверенитет (системы слежения, блокировки данных, использование параллельных транзакций и т. п.), так и, наоборот, помогать сохранять и шифровать данные, создавать альтернативные технологические решения и пр.

Таким образом, внешние факторы не просто ослабляют или усиливают цифровой суверенитет, они качественно его меняют. Во-первых, этому способствовали сами IT-гиганты, и в первую очередь – развитие цифровых платформ, которые стали использовать информацию и личные данные пользователей как собственный ресурс для генерации новых услуг и прибыли, тем самым вызывая на себя давление с целью защиты персональных данных. Во-вторых, активное развитие новых информационных технологий и нейросетей приводит к возможности реального вмешательства и манипулирования политическим выбором – от Румынии до Мадагаскара. В-третьих, существующие практики отмены и санкционирования программных продуктов и технологий ставят страны, не владеющие ими, в реально уязвимое положение. В результате происходит системная трансформация подходов к управлению в области цифрового суверенитета. Смещается фокус контроля: вместо контроля над каналами связи (сетями) нужен контроль над данными, алгоритмами и точками их обработки. Становятся важными новые компетенции, которые надо создавать. Государству для эффективного контроля критично важно иметь своих специалистов по искусственному интеллекту и алгоритмам нейросетей, анализу больших данных, криптографии и блокчейну. Все это требует значительных финансовых и человеческих ресурсов и специальной государственной политики.

В то же время в цифровую эпоху невозможно просто «закрыться». Стратегия полной автаркии не только не реалистична, но и контрпродуктивна. Цифровой суверенитет в современном мире – это не столько технологический, сколько управленческий вызов. Соответственно, каждой стране нужно быть гибкой и адаптивной, находить тонкий баланс между импортозамещением и использованием современных технологий, между запретами и экономической эффективностью, гибкостью, стимулированием, а не принуждением. Необходимо найти свое место в глобальной конкурентоспособности, обеспечивая суверенитет лишь в критически важных сегментах (КИИ, оборона, госуправление и т. п).

Заключение

1. Систематизированы и проанализированы различные концепции, лежащие в основе цифрового суверенитета, такие как суверенитет данных, информационный и технологический суверенитет. Рассмотрена их взаимная обусловленность и связанность. Выполнен анализ внутренних и внешних факторов, определяющих возможности и границы цифрового суверенитета каждой страны. Именно внешние факторы выступают основным драйвером фрагментации интернета во многих странах, не являющихся технологическими лидерами в IT-отрасли. В то же время государствам необходимо сосредоточить основные усилия на развитии внутренних факторов.

2. В настоящее время большинство регуляционных мер, обеспечивающих реализацию информационного или цифрового суверенитета, так или иначе касаются правовых и технологических рамок. Сюда относятся меры, обеспечивающие безопасность цифровой среды, а также меры запретов и контроля. Однако все они требуют колоссальных ресурсов и имеют отложенный эффект. Изменение подхода и смещение фокуса с регуляторных и контролирующих мер, которые могут только задавать направление и рамки, к более мягким образовательным и просветительным мерам и инструментам, создающим кадровый и технологический потенциал, качественный национальный контент, устойчивую культурную среду и медиаграммотность, позволят существенно укрепить как цифровой, так и общенациональный суверенитет.

Список литературы

1. Шитьков, С. В. Подходы к изучению цифрового суверенитета в современной политической науке / С. В. Шитьков // Международная жизнь. 2025. № 5. С. 90–100.
2. Антонов, Д. Е. Цифровой суверенитет современного государства: от контроля до коммуникации / Д. Е. Антонов // Полилог. 2022. Т. 6, № 2. С. 1–14.
3. Бухарин, В. В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности / В. В. Бухарин // Вестник МГИМО-Университета. 2016. Т. 6, № 51. С. 76–91. https://doi.org/10.24833/2071-8160-2016-6-51-76-91.
4. Володенков, С. В. Феномен цифрового суверенитета современного государства в условиях глобальных технологических трансформаций: содержание и особенности / С. В. Володенков // Журнал политических исследований. 2020. Т. 4, № 4. С. 3–11. DOI: 10.12737/2587-6295-2020-3-11.
5. Зиновьева, Е. С. Цифровой суверенитет в публикации о международных отношениях / Е. С. Зиновьева, С. В. Шитьков // Международная жизнь. 2023. № 3. С. 38–51.
6. Кутюр, С. Что означает понятие «суверенитет» в цифровом мире? / С. Кутюр, С. Тоупин // Журнал исследований международных организаций. 2020. Т. 15, № 4. С. 48–69.
7. Шахновская, И. В. Информационный суверенитет государства и личности: опыт Республики Беларусь и зарубежных стран / И. В. Шахновская // Вестник ЮУрГУ. Серия «Право». 2024. Т. 24, № 2. С. 117–123.
8. Creemers, R. China's Conception of Cyber Sovereignty: Rhetoric and Realization / R. Creemers // Governing Cyberspace. 2020. P. 107–142.
9. Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. Режим доступа: https://pravo.by/document/?guid=12551&p0=C22401074. Дата доступа: 10.11.2025.

Поступила 22.12.2025 Принята в печать 22.01.2026 Доступна на сайте 10.04.2026

References

1. Shitkov S. V. (2025) Approaches to the Study of Digital Sovereignty in Modern Political Science. *The International Affairs*. (5), 90–100.
2. Antonov D. E. (2022) Digital Sovereignty of the Modern State: From Control to Communication. *Polylogos.* 6 (2), 1–14.
3. Bukharin V. V. (2016) The Russian's Digital Sovereignty as a Technical Basis of Information Security. *MGIMO Review of International Relations*. 6 (51), 76–91. https://doi.org/10.24833/2071-8160-2016-6-51-76-91.
4. Volodenkov S. V. (2020) The Phenomenon of Contemporary State's Digital Sovereignty in the Context of Global Technological Transformations: Content and Features. *Journal of Political Research*. 4 (4), 3–11. DOI: 10.12737/2587-6295-2020-3-11.
5. Zinovieva E. S., Shitkov S. V. (2023) Digital Sovereignty in International Relations. *The International Affairs*. (3), 38–51.

6. Couture S., Toupin S. (2020) What Does the Notion of "Sovereignty" Mean When Referring to the Digital? *International Organizations Research Journal*. 15 (4), 48–69.
7. Shakhnovskaya I. V. (2024) Information Sovereignty of the State and Individuals: The Experience of the Republic of Belarus and Foreign Countries. *Bulletin of the South Ural State University. Series "Law"*. 24 (2), 117–123.
8. Creemers R. (2020) China's Conception of Cyber Sovereignty: Rhetoric and Realization. *Governing Cyberspace*. 107–142.
9. *National Legal Internet Portal of the Republic of Belarus*. Available: https://pravo.by/document/?guid=12551&p0=C22401074 (Accessed 10 November 2025).

Received: 22 December 2025 Accepted: 22 January 2026 Available on the website: 10 April 2026

Сведения об авторе

Ракова Е. Ю., канд. экон. наук, доц. каф. коммерческой деятельности и управления недвижимостью, Белорусский государственный экономический университет

Адрес для корреспонденции

220038, Республика Беларусь,
Минск, ул. Свердлова, 7
Белорусский государственный
экономический университет
Тел.: 375 29 659-10-02
E-mail: rakova2025@gmail.com
Ракова Елена Юрьевна

Information about the author

Rakova E., Cand. Sci. (Econ.), Associate Professor at the Department of Commercial Activity and Real Estate Management, Belarus State Economic University

Address for correspondence

220038, Republic of Belarus,
Minsk, Sverdlova St., 7
Belarus State
Economic University
Tel.: 375 29 659-10-02
E-mail: rakova2025@gmail.com
Rakova Elena