ВОПРОСЫ ЭКОНОМИКИ

DOI 10.35775/PSI.2025.73.8.001
УДК 32.327

А.Б. ИНХЕЕВ
аспирант Дипломатической академии МИД России,
Россия, г. Москва
E-mail: inheev@yandex.ru

ЦИФРОВОЙ СУВЕРЕНИТЕТ: ИНСТИТУЦИОНАЛЬНЫЕ МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ В УСЛОВИЯХ ГЛОБАЛЬНЫХ ТЕХНОЛОГИЧЕСКИХ ТРАНСФОРМАЦИЙ В РОССИИ И США

Статья анализирует институциональные подходы к обеспечению цифрового суверенитета в России и США в условиях глобальных технологических трансформаций. Исследование основано на междисциплинарном анализе нормативных актов, стратегических документов и научных публикаций.

Рассмотрены ключевые механизмы формирования государственной политики в области цифрового суверенитета, включая деятельность государственных органов, взаимодействие с частным сектором и международными организациями. Выявлено, что обе страны применяют комплексное регулирование национальной инфраструктуры, контроля трансграничных данных и кибербезопасности, но отличаются по степени централизации и характеру государственного участия.

Российская модель ориентирована на сильное государственное регулирование, а американская – на участие частного сектора и гибкое правовое регулирование. Эффективность институциональных механизмов зависит от их адаптивности к технологическим изменениям и способности балансировать между национальной безопасностью и глобальной интеграцией.

Ключевые слова: *цифровой суверенитет, институциональные механизмы, кибербезопасность, трансграничные потоки данных, национальная безопасность, государственное регулирование, Россия, США.*

Введение. Цифровизация всех сфер общества привела к возникновению концепции «цифровой суверенитет», ставшей ключевым элементом национальной безопасности и независимости государств в XXI веке. Под цифровым суверенитетом обычно понимают способность государства осуществлять полный контроль над собственной цифровой инфраструктурой, данными и информационными потоками в пределах своей юрисдикции [7. С. 30-49]. Возрастание глобальной технологической взаимозависимости поставило перед государствами новую

задачу: обеспечить суверенитет в цифровой сфере без ущерба для развития цифровой экономики.

Следует подчеркнуть, что в работах российских авторов, опубликованных в последние годы, освещается широкий спектр вопросов близких к данной предметной области [1; 2; 4; 6; 9; 13; 14; 17; 20; 21; 26; 27].

Однако проблему обеспечения цифрового суверенитета различных государств в условиях глобальных технологических изменений нельзя назвать однозначно исчерпанной. В силу многих объективных обстоятельств изучение обозначенной темы продолжает сохранять высокий уровень актуальности.

Цель данной статьи – провести сравнительный анализ институциональных механизмов обеспечения цифрового суверенитета в России и США в условиях глобальных технологических изменений. Для этого анализ основывается на правовых актах, стратегических документах и научных публикациях.

Концепция цифрового суверенитета и глобальный технологический контекст. Термин «цифровой суверенитет» получил распространение в последние десятилетия и остается дискуссионным, имея разные интерпретации в разных странах. Классическое понятие государственного суверенитета подразумевает верховенство власти государства в пределах своей территории и независимость во внутренних делах [31. С. 98-105]. Однако с развитием глобальной сети Интернет встал вопрос, применимо ли традиционное понимание суверенитета к киберпространству. В международно-правовой доктрине сформировались по крайней мере три подхода: (1) нигилистический; (2) юрисдикционный; (3) государственнический [11. С. 99-108].

При реализации цифрового суверенитета государства строят институциональные механизмы на трех уровнях: инфраструктурном (контроль сетей), технологическом (отечественные ПО и шифрование) и информационном (регулирование контента) [10. С. 144-163].

Также необходимо отметить, что эффективность стратегии цифрового суверенитета в значительной степени определяется качеством правовой базы, которая регламентирует отношения, складывающиеся в процессе использования цифровых технологий.

Глобальные технологические трансформации подорвали монополию государств на контроль информации. Вместе с этим, рост киберугроз (хакерские атаки, кибершпионаж, информационные войны) стимулировали государства пересмотреть отношение к киберпространству [16. С. 5-15]. В следующем разделе рассмотрим, какими институциональными мерами обеспечивается цифровой суверенитет в Российской Федерации, а затем – в Соединенных Штатах Америки.

Механизмы обеспечения цифрового суверенитета в Российской Федерации. Россия рассматривает цифровой суверенитет как ключевой элемент государственной безопасности, технологической независимости и сохранения политического суверенитета в условиях глобальной конкуренции. На институциональном уровне в России сформирована целая система мер – законодательных,

административных и технических – направленных на установление государственного контроля над национальным киберпространством и снижение зависимости от иностранных технологий [8. С. 11-20].

Основой любого институционального регулирования является нормативно-правовая база. В официальных документах цифровой суверенитет закреплен как один из приоритетов. Так, Доктрина информационной безопасности Российской Федерации [5] прямо называет обеспечение суверенитета в информационном пространстве одной из целей государственной политики. Также к важнейшим законам в данной сфере относятся: ФЗ «О персональных данных» (2015) [24] с требованием локального хранения данных российских граждан на серверах внутри страны, ФЗ «об информации» (т.н. «закон о суверенном интернете», 2019) [25], пакет законов о регулировании деятельности иностранных технологических компаний (2014-2021 гг.), включающий требования об открытии локальных представительств, удалении запрещенного контента и др.

Одним из ключевых институтов цифрового суверенитета России является Роскомнадзор, который контролирует интернет-контент и применяет технические меры против ресурсов, нарушающих законодательство. Также важную роль играют Министерство цифрового развития, связи и массовых коммуникаций, ФСБ и другие службы, отвечающие за информационную безопасность и технические средства оперативно-розыскных мероприятий (СОРМ). В результате в России сформировалась модель централизованного управления цифровой инфраструктурой, обусловленная историческим опытом сильной роли государства, восприятием киберугроз как международной конкуренции и стремлением защитить ключевые цифровые системы от внешних рисков.

Россия также развивает национальную систему доменных имен (НСДИ) для автономного управления интернетом, включая развертывание корневых DNS-серверов под контролем государства. В том числе, в условиях санкций развиваются отечественные технологии шифрования и программное обеспечение в целях повышения цифровой безопасности и снижения зависимости от иностранных технологий.

Цифровой суверенитет России имеет важное военно-политическое значение, рассматриваясь как условие обороноспособности и геополитического влияния. В официальных документах подчеркивается необходимость защиты информационного пространства от внешних вмешательств, кибератак и пропаганды. На международной арене Россия активно продвигает идею государственного суверенитета в информационной сфере, выступая на площадках ООН, БРИКС и ШОС с инициативами по формированию норм ответственного поведения в интернете и противодействию доминированию одной страны. Такой подход отражает стремление укрепить многополярность цифрового пространства и предотвратить монопольный контроль глобальной сети со стороны США.

Итак, российские механизмы обеспечения цифрового суверенитета можно обобщить следующим образом: комплекс нормативных и технических мер, направленных на государственное регулирование обращения данных и трафика

внутри страны; развитие автономной цифровой инфраструктуры (национальный сегмент сети, собственные сервисы); а также интеграцию вопросов цифровой безопасности в общую стратегию национальной безопасности. Такой комплексный подход повышает устойчивость и независимость российского сегмента интернета и позволяет минимизировать риски внешнего воздействия. Далее предлагается рассмотреть, каким образом обеспечивается цифровой суверенитет в США и в чем американский подход отличается от российского.

Механизмы обеспечения цифрового суверенитета в США. Соединенные Штаты Америки, будучи родиной интернета и крупнейших ИТ-корпораций, долгое время продвигали идею глобального, открытого и рыночно-ориентированного киберпространства. Традиционно американская цифровая политика опиралась на принципы свободы слова, минимального регулирования и ведущей роли частного сектора в инновациях. Тем самым обеспечение национальных интересов в цифровой сфере основывалось не на прямом контроле государства над сетью, а на экономическом и технологическом доминировании – через мощные корпорации (Google, Apple, Microsoft, Amazon, Facebook и др.), а также через влияние на международные нормы и институты интернет-управления [18]. Тем не менее, с усилением киберугроз и обострением конкуренции (прежде всего с Китаем и Россией), США также разработали ряд институциональных мер, направленных на защиту своего цифрового суверенитета. Важно отметить, что хотя сам термин «цифровой суверенитет» встречается нечасто, синонимичные понятия присутствуют в стратегиях в ряде нормативных актов.

Так, в США принята Национальная стратегия кибербезопасности 2023 г. [34], которая определяет ключевые задачи по защите критически важной инфраструктуры, развитию наступательных кибервозможностей и укреплению технологического лидерства страны. Особое внимание уделяется обеспечению безопасности цепочек поставок и снижению зависимости от ненадежных иностранных поставщиков.

После ряда инцидентов, выявивших уязвимости сетей, президентским Указом № 14028 2021 г. [33. P. 26633-26647]. были введены жесткие требования к подрядчикам федерального правительства, включая обязательные стандарты безопасности программного обеспечения, проверку исходного кода и усиление мониторинга инцидентов. Эти меры направлены на повышение устойчивости государственных систем и предотвращение актов саботажа через эксплуатацию уязвимостей.

Другим направлением политики стала защита данных под американской юрисдикцией. В 2018 г. Конгресс принял закон CLOUD Act (Clarifying Lawful Overseas Use of Data Act) [32. P. 348-353], который наделил американские правоохранительные органы правом запрашивать данные пользователей у американских технологических компаний даже за пределами США. Фактически, этот закон экстерриториально распространил юрисдикцию США на облачные данные, вызывая дискуссии о конфликте с европейским законодательством (GDPR) и суверенитетом других стран [19. С. 20-51]. Как отмечает, в частности, Т. Кокрейн, с точки

зрения США CLOUD Act стал инструментом обеспечения доступа к информации для целей безопасности и правопорядка, несмотря на национальные границы – то есть элементом их «цифрового суверенитета» в глобальном масштабе [11. С. 99-108].

Кроме того, в последние годы США активно противодействуют проникновению иностранных (преимущественно китайских) технологий в критическую инфраструктуру, усматривая в них угрозу безопасности и суверенитету [3]. В 2019 г. в США был принят закон, запрещающий государственным структурам использовать бюджетные средства на закупку телекоммуникационного оборудования и сервисов у компаний, подконтрольных КНР. Ярким примером в данном ключе стал запрет на оборудование Huawei и ZTE. Также были введены ограничения на экспорт в Китай передовых полупроводников, технологий искусственного интеллекта и квантовых вычислений, которые могут использоваться в военных целях.

В США действует разветвленная система институтов, ответственных за цифровую политику. В сфере обороны ключевую роль играет US Cyber Command полноценно развернутое в 2018 г., занимающееся планированием наступательных и оборонительных кибероперацій. В рамках внутренней безопасности работает Агентство по кибербезопасности и безопасности инфраструктуры (CISA), созданное в 2018 г., координирующее защиту федеральных сетей и сотрудничество с частными операторами критической инфраструктуры [22]. Значительную роль играет Агентство национальной безопасности (NSA), осуществляющее киберразведку, контрразведку и защиту правительственной связи. В 2021 г. для улучшения координации между ведомствами и частным сектором была учреждена должность Национального директора по кибербезопасности при Белом доме.

Надо отметить, что система кибербезопасности США исторически развивалась фрагментарно. Исследователи указывают, что на протяжении 2000-х годов решения в области киберполитики нередко принимались ad hoc, разные ведомства дублировали функции, а единая вертикаль отсутствовала [15]. Лишь в последнее десятилетие, по мере роста кибератак США предприняли усилия по централизации этой сферы [23. С. 13]. Тем не менее, частный сектор по-прежнему владеет значительной частью критической цифровой инфраструктуры, и государство во многом зависит от сотрудничества с ним.

Американская модель цифрового лидерства опирается на рынок и инновации. Крупные технологические компании группы FAMGA (Microsoft, Google, Amazon, Facebook, Apple) не принадлежат государству, но обеспечивают значительное влияние США на глобальном уровне. Правительство выстраивает с ними сотрудничество, которое эволюционировало от секретного доступа АНБ к серверам фирм (программа PRISM) к открытому партнерству, включающему обмен информацией о киберугрозах и совместную разработку стандартов безопасности. По сути формируется государственно-частное партнерство, где бизнес предоставляет ресурсы и экспертизу, а государство – координацию и правовую базу.

Соединенные Штаты Америки на глобальном уровне реализуют модель многостейкхолдерского управления интернетом, в рамках которой значимую роль играют техническое сообщество, частный сектор и гражданское общество наряду с государственными структурами. Эта модель сформировалась исторически, в том числе через деятельность организаций, таких как ICANN и IETF. Также США активно участвуют в разработке международных норм по киберпространству, традиционно выступая против инициатив, направленных на изоляцию национальных сегментов интернета и значительные ограничения трансграничного обмена данными.

Вместе с тем в экспертных кругах отмечается определенная двойственность позиции США: критикуя ограничительные меры в интернете в других странах, они сохраняют широкое институциональное влияние благодаря доминированию доллара в электронных расчетах и юрисдикции над ведущими цифровыми платформами и облачными сервисами. В научной литературе данное явление часто интерпретируется как проявление «цифровой гегемонии США», подчеркивающее выбор для многих государств – либо использовать глобальные сети, основанные на американской технологической и нормативной базе, либо стремиться к построению альтернативных национальных или региональных сегментов [30. С. 572-584].

Таким образом, американский подход к обеспечению национального контроля и безопасности в цифровой сфере базируется на сочетании: защиты открытого и глобального характера интернета, активного укрепления сетей и инфраструктуры против киберугроз, применения национальной юрисдикции к данным и международным компаниям, а также опоры на частный сектор как партнера в инновациях и кибербезопасности. Вместе с тем определенные механизмы косвенного регулирования также присутствуют в США – например, противодействие дезинформации через сотрудничество с социальными сетями, ограничительные меры в отношении иностранных ИТ-компаний, а также блокировка по решению суда незаконного контента.

Сравнительный анализ подходов России и США. Общие тенденции в подходах России и США заключаются в том, что обе страны признают стратегическую важность управления цифровой сферой для национальной безопасности и экономики. Для них характерно усиление военного компонента в киберпространстве: создание специализированных подразделений в вооруженных силах, разработка доктрин информационной безопасности. В этом контексте цифровой суверенитет рассматривается как часть более широкого понятия национального суверенитета, включающего способность государства обеспечивать безопасность собственной цифровой инфраструктуры.

Кроме того, и Россия, и США в определенной мере используют инструменты защиты национальной цифровой экономики. Россия в государственной политике подчеркивает необходимость технологической самодостаточности – разработки отечественного программного обеспечения и электроники, а также поддержки национальных цифровых платформ (например, «Яндекс»,

«VK», «RuTube») в качестве альтернатив зарубежным. США, декларируя приверженность принципам свободного рынка, на практике также применяют меры для защиты собственных производителей (например, ограничения на экспорт технологий или санкции против отдельных иностранных компаний). Оба государства стремятся минимизировать технологическую зависимость: Россия – от западных стран и Китая (в перспективе), США – от Китая. Таким образом, технологический суверенитет как элемент цифрового суверенитета становится приоритетом для обоих государств.

Главные различия связаны с уровнем государственного вмешательства. Российская модель характеризуется традицией централизованного государственного управления, при которой стратегические сферы, включая информационную, находятся под контролем федеральных органов. Она базируется на нормативном закреплении роли государства, в частности через законы «о суверенном интернете» и «о персональных данных». Институционально это отражается в развитии национального сегмента сети и участии Роскомнадзора в управлении информационными потоками и инфраструктурой. Эта совокупность исторических, правовых и технических факторов формирует основу российской стратегии цифрового суверенитета.

В США регулирование носит более опосредованный характер: через судебные механизмы, элементы саморегуляции индустрии, а также через применение санкционных и экспортных инструментов в вопросах национальной безопасности. Американское государство, как правило, устанавливает стандарты и создает стимулы, нежели ограничивает доступ к информации напрямую.

В международном контексте Россия позиционирует свой подход как альтернативу преобладающим западным моделям управления киберпространством. США, напротив, стремятся сохранить статус-кво, при котором архитектура интернета остается глобальной и распределенной, но значительная роль в ней продолжает принадлежать американским институтам. Таким образом, выявленные различия имеют и международное измерение: российская модель акцентирует внимание на укреплении киберсуверенитета отдельных государств, что сопровождается тенденцией к фрагментации глобального киберпространства, тогда как американская модель направлена на поддержание сетевой взаимозависимости и укрепление международного влияния США через технологические стандарты.

Заключение. Концепция цифрового суверенитета возникла как ответ на вызовы глобальной цифровой эпохи: зависимость от иностранных технологий, угроза кибератак и влияние транснациональных корпораций. Россия и США выбрали разные институциональные модели, отражающие их политические ценности и стратегические приоритеты.

В России цифровой суверенитет реализуется через государственное регулирование с развитой законодательной базой, контролем национального сегмента интернета и техническими средствами управления трафиком. Такой подход снижает уязвимость страны перед внешними воздействиями.

В США внимание сосредоточено на рыночных механизмах и сотрудничестве с частным сектором – существенную роль играют антикитайские санкции и законы, такие как CLOUD Act, а также развитие профильных агентств, обеспечивающих защиту от цифровых угроз.

Несмотря на различия, цифровой суверенитет становится ключевой задачей обеих стран в контексте цифровой трансформации и усиливающихся вызовов безопасности. Для международного сообщества это ставит задачу поиска баланса между уважением легитимных интересов государств в сфере кибербезопасности и обеспечением безопасности собственных цифровых сетей. В условиях ситуационной киберосведомленности долгосрочная цель может заключаться в формировании такого порядка, который участники принимают на основе согласованных интересов, а не под давлением гегемона [29. С. 35-53].

Таким образом, исследование институциональных механизмов России и США отражает два различных подхода к цифровому суверенитету. Российская модель обеспечивает высокий уровень государственного контроля, что связано с определенными ограничениями развития интернет-сегмента. Американская модель опирается на развитие инновационной экосистемы, при этом сталкивается с вызовами в области защиты данных и противодействия иностранному влиянию. Комбинация лучших практик с учетом национальной специфики может быть полезна для улучшения текущих стратегий развития в условиях глобальных технологических изменений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Авдеев М.А., Собакарева Е.В., Шевченко А.В., Григорян Д.К.** Цифровизация государственного и муниципального управления на территории РФ // Евразийский Союз: вопросы международных отношений. 2025. № 2.
2. **Афонин М.В., Тиханов Р.С., Кривова А.Л., Полежайкина Е.В.** Риски избирательных кампаний в контексте цифрового политического участия // Вопросы политологии. 2025. № 2.
3. **Браттон Б.** Х. Стек: о программном обеспечении и суверенитете. (Software studies). Кембридж (Массачусетс): MIT Press, 2016.
4. **Гавров С.Н., Еремкин М.П.** Использование технологий искусственного интеллекта в политической рекламе // Вопросы политологии. 2025. № 4.
5. Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 5 декабря 2016 г. № 646 // Собрание законодательства РФ. 2016. № 50, ст. 7074.
6. **Дронов А.И.** Политическая коммуникация выборных элит с населением посредством социальных медиа при принятии управленческих решений // Вопросы политологии. 2025. № 4.
7. **Дудин М.Н., Шкодинский С.В., Усманов Д.И.** Цифровой суверенитет России: барьеры и новые траектории развития // Проблемы рыночной экономики. 2021. № 2.

8. **Ефремов А.** Обеспечение государственного суверенитета Российской Федерации в информационном пространстве в документах стратегического планирования // Академический юридический журнал. 2017.
9. **Жбанов А.М.** Практика государственно-частного партнерства в системе обеспечения политики кибербезопасности США// Вопросы национальных и федеративных отношений. 2024. № 6.
10. **Зиновьева Е.С., Шитьков С.В.** БРИКС на пути обретения цифрового суверенитета? // Проблемы национальной стратегии. 2024. № 2 (83).
11. **Капустин А.Я.** Суверенитет государства в киберпространстве: международно-правовое измерение // Журнал зарубежного законодательства и сравнительного правоведения. 2022. Т. 18. № 6.
12. **Кокрейн Т.** В укрытии в самом центре облака: как соглашения по Закону CLOUD расширяют экстерриториальные полномочия США в расследованиях // Duke Journal of Comparative & International Law. 2021. Т. 32. № 1.
13. **Колесников А.И.** Технократическая легитимация и цифровизация в современной России // Вопросы национальных и федеративных отношений. 2024. № 7.
14. **Кубанцева Е.В.** Динамика цифрового доминирования: роль больших данных в усилении глобальной зависимости // Вопросы политологии. 2025. № 4.
15. **Кукутаи Т., Тейлор Дж.** Суверенитет данных: к формированию повестки // ANU Press. 2016. Т. 382.
16. **Литвиненко А.** Переопределение границ в сети: стратегический нарратив России о суверенитете интернета // Media and Communication. 2021. Т. 9. № 4.
17. **Медведева В.К., Медведев Н.П.** Информационная политика государства: современные вызовы и направления совершенствования (Часть 2) // Вопросы национальных и федеративных отношений. 2025. № 1.
18. **Розенцвейг П.** Организация правительства США и частного сектора для достижения киберсдерживания // SSRN Electronic Journal. 2010.
19. **Свайр П. и др.** Риски для кибербезопасности от локализации данных, классифицированные по методам, тактикам и процедурам // Journal of Cyber Policy. 2024. Т. 9. № 1.
20. **Слизовский Д.Е., Медведев Н.П.** Информационные, гибридные и прокси-войны: обзор новейших исследований // Вопросы политологии. 2024. № 12.
21. **Сурма И.В.** Международно-правовые особенности обеспечения кибербезопасности в условиях развития высокотехнологичной преступности // Вопросы национальных и федеративных отношений. 2024. № 7.
22. **Такачел Э.** Снижение рисков и сдерживание: две стороны одной медали // Homeland Security Affairs. 2021. Т. 17. Ст. 3.
23. **Такачел Э.** Риск, сдерживание и теория перспектив: влияние когнитивных искажений на эффективность количественного сдерживания при снижении рисков // Homeland Security Affairs. 2022. Дек. Т. 18.

24. Федеральный закон от 27 июля 2006 г. № 152-ФЗ (в ред. Федерального закона от 21 июля 2014 г. № 242-ФЗ) // Собрание законодательства РФ. 2006. № 31 (ч. 1), ст. 3451.
25. Федеральный закон от 27 июля 2006 г. № 149-ФЗ (в ред. Федерального закона от 1 мая 2019 г. № 90-ФЗ) // Собрание законодательства РФ. 2006. № 31 (ч. 1), ст. 3448.
26. **Филатов О.В.** Подходы НАТО к обеспечению информационной безопасности: от общих киберугроз до злонамеренного использования искусственного интеллекта // Вопросы политологии. 2023. № 2.
27. **Форостянный Н.С., Тёмкина А.М.** Политический потенциал БРИКС в трансформации системы международной безопасности // Евразийский Союз: вопросы международных отношений. 2024. № 7.
28. **Хеммингс Дж., Шринивасан С., Суайр П.** Определение сферы «владения, хранения или контроля» в вопросах конфиденциальности и Закон CLOUD // Journal of National Security Law & Policy. 2020. Т. 10.
29. **Хили Дж.** Кибервоздействие в войне: классификация по месту, объекту и причинам // Texas National Security Review. 2020. Т. 3.
30. **Цзян С., Сунь Ч.** Система правовой охраны цифрового суверенитета государств-членов Шанхайской организации сотрудничества // Вестник Санкт-Петербургского университета. Право. 2025. Т. 16. № 2.
31. **Шестопал С.С., Мамычев А.Ю.** Суверенитет в глобальном цифровом измерении: современные тренды // Балтийский гуманитарный журнал. 2020. Т. 9. № 1 (30).
32. Clarifying Lawful Overseas Use of Data Act (CLOUD Act): Public Law 115-141, div. V, Mar. 23, 2018 // U.S. Statutes at Large. Vol. 132.
33. Executive Order 14028, Improving the Nation's Cybersecurity: May 12, 2021 // Federal Register. Vol. 86, No. 93. May 17, 2021.
34. National Cybersecurity Strategy of the United States of America. Washington, D.C.: The White House, 2023.

A.B. INKHEEV
Postgraduate student at the Diplomatic
Academy of the Russian Foreign Ministry,
Moscow, Russia

DIGITAL SOVEREIGNTY: INSTITUTIONAL MECHANISMS FOR ITS ASSURANCE IN THE CONTEXT OF GLOBAL TECHNOLOGICAL TRANSFORMATIONS IN RUSSIA AND THE UNITED STATES

The article analyzes institutional approaches to digital sovereignty in Russia and the United States amid global technological changes. It uses an interdisciplinary framework based on legal acts, strategic documents, and scholarly sources. The study examines key policy mechanisms, including government roles, private sector involvement, and international cooperation. Both countries employ comprehensive regulation of infrastructure, cross-border data flows, and cybersecurity, yet differ in management centralization and state-business relations. The Russian model emphasizes strong state control, while the U.S. relies more on private sector participation and flexible legal frameworks. The effectiveness of these mechanisms depends on adaptability to technological change and balancing national security with global integration.

Key words: *digital sovereignty, institutional mechanisms, cybersecurity, cross-border data flows, national security, state regulation, Russia, USA.*