

На правах рукописи

ШИТЬКОВ СЕРГЕЙ ВЛАДИМИРОВИЧ

ГОСУДАРСТВЕННЫЙ СУВЕРЕНИТЕТ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Специальность 5.5.4. Международные отношения, глобальные
и региональные исследования

АВТОРЕФЕРАТ

Диссертации на соискание ученой степени доктора политических наук

Москва – 2026

Диссертация подготовлена на кафедре мировых политических процессов
Факультета управления и политики ФГАОУ ВО «Московский государственный институт
международных отношений (университет) Министерства иностранных дел Российской
Федерации»

Научный консультант	Зиновьева Елена Сергеевна Доктор политических наук, профессор, профессор кафедры мировых политических процессов, Федеральное государственное автономное образовательное учреждение высшего образования "Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации"
Официальные оппоненты	Цветкова Наталья Александровна Доктор исторических наук, профессор, и.о. Директора, Федеральное государственное бюджетное учреждение науки Институт Соединенных Штатов Америки и Канады Российской академии наук Панцерев Константин Арсеньевич Доктор политических наук, доцент, профессор кафедры теории и истории международных отношений, Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет» Ахременко Андрей Сергеевич Доктор политических наук, доцент, профессор Департамента политики и управления Федерального государственного автономного образовательного учреждения высшего профессионального образования «Национальный исследовательский университет «Высшая школа экономики»"
Ведущая организация	Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет имени М.В.Ломоносова», Факультет политологии

Защита состоится «3» марта 2026 года в «15-00» часов на заседании диссертационного совета ПДС 1000.007 при ФГАОУ ВО «Российский университет дружбы народов имени Патриса Лумумбы» (РУДН) по адресу: 117198, Москва, ул. Миклухо-Маклая, д. 6, зал Ученого совета.

С диссертацией и авторефератом можно ознакомиться:

1. На сайте Российского университета дружбы народов имени Патриса Лумумбы.
2. В информационно-научном библиотечном центре (Научной библиотеке) Российского университета дружбы народов имени Патриса Лумумбы по адресу: 117198, г. Москва, ул. Миклухо-Маклая, д. 6.

Автореферат размещен на сайте Высшей аттестационной комиссии Министерства науки и высшего образования Российской Федерации: Автореферат разослан «3» февраля 2026 г.

Ученый секретарь диссертационного
совета ПДС 1000.007
кандидат политических наук, доцент

Казаринова Д.Б.

I. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Бурное развитие современных информационно-коммуникационных технологий ставит на международную повестку дня целый ряд вопросов, которые нуждаются в согласованных ответах со стороны международного сообщества, а также в осмыслении на уровне международных исследований и политической науки. Одной из таких проблем стало обеспечение государственного суверенитета в цифровую эпоху. Современный этап технологического развития в значительной степени опирается на достижения в сфере цифровых технологий, которые на современном этапе приобретают новые измерения, что находит свое воплощение в таких передовых направлениях, как развитие «Интернета вещей», Больших данных, технологий искусственного интеллекта и других, которые в российской и зарубежной науке чаще всего концептуализируются при помощи подхода К. Шваба о четвертной промышленной революции (Industrie 4.0)¹. В этих условиях трансформируются традиционные категории политической науки и политической практики, в том числе и категория государственного суверенитета.

За последнее десятилетие цифровой суверенитет стал центральным элементом политических дискуссий по вопросам международных аспектов развития **информационно-коммуникационных технологий**. Несмотря на свою популярность, концепция «цифрового суверенитета» остается весьма спорной и пока не получила комплексного и всестороннего освещения в научной литературе. Вышеизложенное обуславливает *научную актуальность* данной тематики.

В России к данной проблеме обращаются на уровне политических решений начиная со второй половины 2010-х гг. Так, в таких документах стратегического планирования, как Доктрина информационной безопасности² от 2016 года и Основы государственной политики в области международной информационной безопасности³ от 2021 года особое внимание уделяется вопросам обеспечения суверенитета в условиях новых вызовов и угроз, порождаемых стремительным развитием информационно-коммуникационных технологий. Соответствующие инициативы принимаются и большинством других стран международного

¹ Schwab K. The fourth industrial revolution. – Currency, 2017.

² Доктрина информационной безопасности Российской Федерации. Утв. Указом Президента России 2016.

³ Основы государственной политики Российской Федерации в области международной информационной безопасности. Утв. Указом Президента России 2021 г.

сообщества.

Отдельного внимания требует влияние Специальной военной операции РФ на Украине (2022–н.в.) на трансформацию суверенитета. СВО стала точкой ускорения процессов технологического и цифрового суверенитета, обострив конфликт между Россией и коллективным Западом. В 2022–2025 гг. Президент РФ и МИД РФ неоднократно подчеркивали, что цифровой и технологический суверенитет является условием общей стратегической автономии государства. Эти официальные позиции формируют современный политический контекст исследования и требуют включения в научный анализ.

Растущее политическое внимание к проблематике «цифрового суверенитета» в условиях отсутствия академической базы в данной области обуславливает *прикладную актуальность* выбранной темы исследования.

Понятие цифрового суверенитета тесно связано с более широким контекстом глобальной цифровой трансформации, которая затрагивает все аспекты жизни современного общества и мировой политики – социо-культурные, экономические, политические. В условиях, когда данные становятся ключевым ресурсом развития, а информационные потоки пересекают национальные границы в режиме реального времени, традиционные механизмы государственного контроля и регулирования сталкиваются с принципиально новыми вызовами. Исследование данных вызовов и анализ прикладных примеров обеспечения государственного суверенитета позволит выявить оптимальную модель сопряжения государственной политики и цифровой трансформации.

Одним из таких вызовов является фрагментация глобального интернет-пространства. Если в первые десятилетия развития Всемирной сети доминировала идея ее открытости и децентрализованности и неподконтрольности со стороны не только государства, но и крупного бизнеса⁴, то сегодня все больше стран принимают меры по локализации данных, ограничению доступа к иностранным цифровым платформам и созданию собственных технологических экосистем. Китай, например, реализует модель «суверенного интернета» через систему «Золотого щита», включающую блокировку зарубежных сервисов и продвижение национальных аналогов⁵. Аналогичные тенденции наблюдаются в России, где с

⁴ Mueller M. L. Against sovereignty in cyberspace //International studies review. – 2020. – Т. 22. – №. 4. – С. 779-801.

⁵ Creemers R. China's conception of cyber sovereignty //Governing cyberspace: Behavior, power and diplomacy. – 2020. – С. 107-145.

2019 года проводится политика по развитию автономного сегмента интернета⁶, а также в ЕС, где принятие General Data Protection Regulation (GDPR)⁷ стало шагом к усилению контроля над персональными данными граждан.

При этом концепция цифрового суверенитета не сводится исключительно к вопросам информационной безопасности или защиты данных. Она также включает в себя технологическую независимость, что особенно актуально в условиях глобальной конкуренции за лидерство в сфере искусственного интеллекта, квантовых вычислений и других прорывных направлений. Зависимость от иностранных технологий, будь то полупроводники, оборудование для 5G или облачные платформы, создает риски для национальной безопасности и экономической стабильности. В этой связи многие государства активно инвестируют в развитие собственных технологических компетенций. Например, инициатива ЕС по созданию «GAIA-X» – проекта облачной инфраструктуры, альтернативной американским и китайским решениям, – демонстрирует стремление к цифровой автономии⁸. В России проводится политика технологического суверенитета, которая включает в себя создание реестра отечественного программного обеспечения, политику импортозамещения в ИТ и электронике, локализацию цифровой инфраструктуры, развитие национальных технологических разработок, в том числе в сфере искусственного интеллекта⁹.

Еще одним важным аспектом цифрового суверенитета является регулирование контента и цифровых коммуникаций. Социальные сети, мессенджеры и поисковые системы становятся площадками не только для обмена информацией, но и для политической борьбы, что заставляет государства искать баланс между свободой слова и предотвращением дезинформации, экстремизма и вмешательства во внутренние дела. Законодательные инициативы, такие как немецкий «Закон о защите прав пользователей в социальных сетях» от 2017 г.¹⁰ или российские законы о «о фейках»¹¹, отражают политику по установлению

⁶ Федеральный закон № 90-ФЗ «О внесении изменений в Федеральный закон „О связи“ и Федеральный закон „Об информации, информационных технологиях и о защите информации“» Утв. 1 мая 2019 года

⁷ Regulation (EU) 2016/679 (General Data Protection Regulation) in the current version of the OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018

⁸ <https://gaia-x.eu>

⁹ Зиновьева Е. С., Шитьков С. В. Цифровой суверенитет в практике международных отношений //Международная жизнь. – 2023. – №. 3. – С. 38-51.

¹⁰ Румянцев А. Немецкий закон о социальных сетях: нормативное закрепление технологического отставания // Сравнительное конституционное обозрение. 2019. № 3 (130). С. 27–53.

¹¹ Федеральный закон № 32-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации». Утв от 4 марта 2022 года

суверенного контроля над цифровым пространством.

Вопросы цифрового суверенитета также тесно переплетаются с международным правом. Отсутствие универсальных норм, регулирующих международное ИКТ пространство, приводит к конфликтам юрисдикций. Например, применение американского CLOUD Act, позволяющего властям США получать данные¹², хранящиеся на серверах за пределами страны, противоречит принципам GDPR¹³ и вызывает протесты со стороны ЕС. Аналогичные трения возникают вокруг экстерриториального применения национального законодательства, как в случае с санкциями со стороны США против Huawei или TikTok.

Таким образом, цифровой суверенитет становится не только инструментом защиты национальных интересов, но и объектом выработки согласованных норм на международном уровне. В условиях, когда технологии развиваются быстрее, чем механизмы их регулирования, выработка согласованных подходов на глобальном уровне представляется одной из ключевых задач ближайшего будущего. При этом поиск баланса между суверенитетом и открытостью, безопасностью и инновациями, государственным контролем и цифровыми свободами останется центральной дилеммой современного цифрового мира, малоизученной в научной литературе, что обуславливает *научную актуальность* темы диссертации.

Степень научной разработанности темы исследования. В научной литературе проблематика «цифрового суверенитета» пока не получила систематического освещения, хотя отдельные аспекты темы рассматриваются в работах российских и зарубежных ученых. В частности, изучением трансформации суверенитета государств на современном этапе мировой политики занимались А.А. Кокошин¹⁴, М.М. Лебедева¹⁵, А.А. Сергунин¹⁶, Ст. Краснер¹⁷, Д. Лейк¹⁸, А. Осиандер¹⁹, и другие ученые. Особый акцент необходимо сделать на

¹² Clarifying Lawful Overseas Use of Data (CLOUD) Act. US Department of Justice. Criminal Division. 2018. URL: <https://www.justice.gov/criminal/media/999391/dl?inline>

¹³ Regulation (EU) 2016/679 (General Data Protection Regulation) OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018

¹⁴ Кокошин А. А. Реальный суверенитет в современной мирополитической системе. – Европа, 2006.

¹⁵ Лебедева М. М. Мировая политика //М.: Аспект пресс. – 2007.

¹⁶ Сергунин А. А. Суверенитет: эволюция концепта //Политическая экспертиза: ПОЛИТЭКС. – 2010. – Т. 6. – №. 4.

¹⁷ Krasner S. D. Sovereignty. – Princeton University Press, 1999.

¹⁸ Lake D. A. The new sovereignty in international relations //International studies review. – 2003. – Т. 5. – №. 3. – С. 303-323.

¹⁹ Osiander A. Sovereignty, international relations, and the Westphalian myth //International organization. – 2001. – Т. 55. – №. 2. – С. 251-287.

фундаментальном вкладе С. Краснера, в концептуализацию суверенитета, который предложил теорию "суверенитета как организованного лицемерия" (organized hypocrisy), таким образом обосновав, что суверенитет в международных отношениях является не абсолютным, а контекстуальным феноменом, который государства выборочно соблюдают или нарушают в зависимости от политических интересов, деконструируя традиционное вестфальское понимание данного принципа²⁰. Важный вклад в осмысление истории концептуализации категории государственного суверенитета в политической мысли внесла книга «Интеллектуальные горизонты Жана Бодена» М.С. Бобковой, Т.В. Черниковой, А.А. Рогожина²¹. Прикладной анализ государственной состоятельности как опыта количественного анализа практики государственного суверенитета в международной политике можно провести на основании проекта коллектива авторов МГИМО «Политический атлас современности»²², а также проекта Консорциума МГИМО и ВШЭ: «Политический атлас современного мира 2.0»²³ под руководством Мельвиля А.Ю.

Нельзя не отметить концепцию инфраструктурной власти социолога М. Манна, под которой понимается институциональная возможность государства реализовывать свои решения в пределах государственных границ²⁴. Его исследования вносят важный вклад в осмысление государственного суверенитета, демонстрируя, что реальный суверенитет государства определяется не только формальным контролем над территорией, но и его способностью эффективно осуществлять власть через административные, экономические и социальные институты. Данная концепция подчеркивает, что суверенитет – это не статичный юридический принцип, а динамичный процесс, зависящий от способности государства проникать в общество и мобилизовывать ресурсы, что особенно актуально в условиях глобализации и цифровизации, когда традиционные границы

²⁰ Krasner S. D. Sovereignty: organized hypocrisy. – Princeton university press, 1999.

²¹ Интеллектуальные горизонты мира Жана Бодена / М.С.Бобкова, Т.В.Черникова, А.А.Рогожин [и др.]; общая редакция, предисловие и вступительная статья М.С.Бобковой; Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации, кафедра всемирной и отечественной истории; Российская академия наук, Институт всеобщей истории, Центр истории исторического знания. – Москва: МГИМО-Университет, 2023. – 644 с.

²² Политический атлас современности : Опыт многомерного статистического анализа политических систем современных государств. – М.: Изд-во «МГИМО-Университет», 2007. – 272 с., илл. URL: https://mgimo.ru/upload/docs_3/politatlas.pdf?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com

²³ <https://social.hse.ru/politatlas/>

²⁴ Mann M. Infrastructural power revisited //Studies in comparative international development. – 2008. – Т. 43. – С. 355-365.

суверенитета подвергаются трансформации.

Вместе с тем, в современной научной мысли изучение темы «цифрового суверенитета» носит фрагментарный характер и комплексных исследований, посвященных трансформации суверенитета и проблемам его обеспечения в условиях цифровой трансформации современной мировой политике не представлено. Важно отметить, что на различных исторических этапах подходы к научному осмыслению данной проблематики существенно отличались. В 1990-е годы преобладала концепция «интернет-оптимизма», согласно которой развитие интернет-технологий способствовало размыванию государственного суверенитета и снижению влияния государств²⁵. В этот период был опубликован целый ряд работ, посвященных вопросам размывания государственного суверенитета под воздействием информационной революции, в том числе российских авторов А.Н. Михеева²⁶, Д.Н. Пескова²⁷, а также зарубежных исследователей, таких как Д. МакЛин, В. Кляйнвахтер²⁸, Д. Най и Р. Кохейн²⁹, Д. Розенау³⁰ и др.

В 2010-е гг. в условиях возрастающего количества угроз кибер- и информационной безопасности, на уровне политических элит возрастает внимание к вопросам обеспечения цифрового суверенитета. В целом развитие информационно-коммуникационных технологий секьюритизировалось. Это нашло отражение и в научных трудах по данной тематике. В частности, такие авторы, как А.А. Стрельцов³¹ и М.М. КучерявыЙ³², Е.С. Зиновьева³³ занимались международно-правовыми аспектами данной проблематики. Среди зарубежных авторов следует отметить М.Мюллера³⁴, Д. Поул и Т. Тъель³⁵, которые

²⁵ См. напр.: Keohane R. O., Nye Jr J. S. Power and interdependence in the information age //Foreign Aff. – 1998. – Т. 77. – С. 81.

²⁶ Михеев А. Н. Информационно-коммуникационные технологии: глобальные проблемы и/или глобальные возможности? //Современные глобальные проблемы мировой политики/под ред. ММ Лебедевой. М. – 2009.

²⁷ Песков Д. Н. Интернет-пространство: состояние премодерна? //ПОЛИС. Политические исследования. – 2003. – №. 5. – С. 46-55.

²⁸ Kleinwaghter W. Internet co-governance: towards a multilayer multiplayer mechanism of consultation, coordination and cooperation. // E-learning and digital media. 2006. Vol. 3 #3. Pp. 473 - 487

²⁹ Keohane R. O., Nye Jr J. S. Power and interdependence in the information age //Foreign Aff. – 1998. – Т. 77. – С. 81.

³⁰ MacLean D. et al. Governing global electronic networks: International perspectives on policy and power. – MIT Press, 2008.

³¹ Стрельцов А. А. Суверенитет и юрисдикция государства в среде информационно-коммуникационных технологий в контексте международной безопасности //Международная жизнь. – 2017. – №. 2. – С. 87-106.

³² КучерявыЙ М. М. Государственная политика информационного суверенитета России в условиях современного глобального мира //Управленческое консультирование. – 2014. – №. 9 (69).

³³ Зиновьева, Е.С. Проблемы международного управления Интернетом в контексте цифрового суверенитета / Е.С.Зиновьева. – Текст: непосредственный // Международная жизнь. – 2020. – Специальный выпуск. Международная конференция «Киберстабильность: подходы, перспективы, вызовы» – С. 133-137.

³⁴ Mueller M. Will the internet fragment?: Sovereignty, globalization and cyberspace. – John Wiley & Sons, 2017.

³⁵ Pohle J., Thiel T. Digital sovereignty //Internet Policy Review. – 2020. – Т. 9. – №. 4. – С. 1-19.

исследовали трансформацию суверенитета в демократических странах под воздействием информационной революции и отмечали тенденцию к его укреплению, а также к усилению влияния «цифровых границ» государств в рамках глобального информационного пространства.

Отдельно следует отметить работы, посвященные технологическому суверенитету, как более широкой категории по отношению к исследованиям цифрового суверенитета. Важный вклад в осмысление данной категории внесли работы А.В. Плотникова³⁶, С.В. Шкодникого и А.М. Кушнира, Продченко И.А.³⁷, А.А. Афанасьева³⁸ и др. В России внимание к данной проблематике в последние годы существенно возросло. Зарубежные авторы, прежде всего, представители стран Западной Европы, включают в себя К. Марша, Э. Шифедекхера³⁹, Ф. Креспи, С. Каравелла⁴⁰, Д. Элдера, К. Блайнда⁴¹ и др. В последние годы также публикуются труды исследователей из КНР, Индии, Бразилии, посвященные данной проблематике⁴².

Важный вклад в работу над диссертацией внесли труды посвященные экономическим аспектам цифрового суверенитета, в частности, работы Ш. Зубофф⁴³, которые раскрыли механизмы подрыва государственного суверенитета транснациональными цифровыми корпорациями через присвоение и монетизацию данных, что стимулировало развитие регуляторных мер (в частности, локализацию данных) как инструментов защиты цифрового суверенитета. Анализ Зубофф

³⁶ Плотников А. В., Плотников В. А. О достижении технологического суверенитета в контексте обеспечения экономической безопасности России в условиях санкций //Экономика и управление. – 2024. – Т. 30. – №. 8. – С. 987-998.

³⁷ Шкодинский С. В., Кушнир А. М., Продченко И. А. Влияние санкций на технологический суверенитет России //Проблемы рыночной экономики. – 2022. – Т. 2. – №. 1. – С. 75-96.

³⁸ Афанасьев А. А. Технологический суверенитет как научная категория в системе современного знания //Journal of Economics. – 2022. – Т. 12. – №. 9. – С. 2377.

³⁹ March C., Schieferdecker I. Technological sovereignty as ability, not autarky //International Studies Review. – 2023. – Т. 25. – №. 2. – С. viad012.

⁴⁰ Crespi F. et al. European technological sovereignty: an emerging framework for policy strategy //Intereconomics. – 2021. – Т. 56. – №. 6. – С. 348-354.

⁴¹ Edler J. et al. Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means //Research Policy. – 2023. – Т. 52. – №. 6. – С. 104765.

⁴² Gu H. Data, big tech, and the new concept of sovereignty //Journal of Chinese political science. – 2024. – Т. 29. – №. 4. – С. 591-612; Jiang M. Models of State Digital Sovereignty From the Global South: Diverging Experiences From China, India and South Africa //Policy & Internet. – 2024. – Т. 16. – №. 4. – С. 727-738; Prasad R. People as data, data as oil: The digital sovereignty of the Indian state //Information, Communication & Society. – 2022. – Т. 25. – №. 6. – С. 801-815; Belli L. BRICS countries to build digital sovereignty //CyberBRICS: Cybersecurity regulations in the BRICS countries. – Cham : Springer International Publishing, 2021. – С. 271-280.

⁴³ Zuboff S. Big other: surveillance capitalism and the prospects of an information civilization //Journal of information technology. – 2015. – Т. 30. – №. 1. – С. 75-89; Zuboff S. The age of surveillance capitalism //Social theory re-wired. – Routledge, 2023. – С. 203-213; Zuboff S. Surveillance capitalism and the challenge of collective action //New labor forum. – Sage CA: Los Angeles, CA : sage Publications, 2019. – Т. 28. – №. 1. – С. 10-29 и др.

показал, что доминирование цифровых платформ создаёт асимметрию экономической власти, вынуждающую государства развивать национальные цифровые экосистемы и ограничивать влияние глобальных технологических монополий. К числу других аналитических работ подобного рода необходимо отнести книгу Т. Ву «Проклятие технологических гигантов»⁴⁴, в которой он анализирует монополизацию цифрового пространства и угрозы для государственного суверенитета, возникающие в данной сфере. К схожим выводам приходит Я. Варуфакис в книге «Технофеодализм»⁴⁵.

Важный вклад в изучение трансформации практики цифрового суверенитета в цифровую эпоху вносят работы, посвященные исследованиям современной цифровой революции. Одной из ключевых книг в данной области является фундаментальный труд К. Шваба «Четвертая промышленная революция»⁴⁶, в котором концептуализированы основные направления влияния новых технологий на мировую экономику и мировую политику. Другие зарубежные исследователи, занимающиеся данной темой, включают в себя Н. Негропонте⁴⁷, Э. Бруссо, Н. Кюри⁴⁸ и др. Кроме того, необходимо отметить работы российских авторов в области цифровизации мировой экономики, в том числе работы И.В. Сударушкиной, Н.А. Стефановой⁴⁹, О.Б. Пичкова и А.А. Уланова⁵⁰, Н.М. Борисова⁵¹, а также экспертные доклады профильных структур по данной проблематике, в том числе экспертов АНО Цифровая экономика⁵² и др.

Правовое измерение цифровой трансформации практики государственного суверенитета представлено в трудах юристов-международников Э.Л. Сидоренко⁵³,

⁴⁴ Wu T. The curse of bigness. – Penguin Random House, 2018.

⁴⁵ Варуфакис Я. Технофеодализм. М.: Ad Marginem, 2025

⁴⁶ Клаус Ш. Четвертая промышленная революция. – Litres, 2016.

⁴⁷ Negroponte N. Being digital. – Vintage, 2015.

⁴⁸ Rousseau E., Curien N. (ed.). Internet and digital economics: principles, methods and applications. – Cambridge University Press, 2007.

⁴⁹ Сударушкина И. В., Стефанова Н. А. Цифровая экономика //Азимут научных исследований: экономика и управление. – 2017. – Т. 6. – №. 1 (18). – С. 182-184.

⁵⁰ Пичков О. Б., Уланов А. А. Риски и несовершенства развития цифровой экономики на современном этапе //Страховое дело. – 2017. – №. 11. – С. 3-8.; Пичков О. Б., Уланов А. А. Перспективы и возможности цифровой экономики на современном этапе развития //Страховое дело. – 2017. – №. 10. – С. 12-16.

⁵¹ Пичков О. Б., Борисов Н. М. Цифровизация и проблема обеспечения национальной экономической безопасности //Страховое дело. – 2021. – №. 5. – С. 44-54.

⁵² Белая книга цифровой экономики 2023 // АНО Цифровая экономика. 2024. URL: https://files.data-economy.ru/Docs/White_paper_2023_.pdf

⁵³ Сидоренко Э. Л. Адаптивные возможности российского права в условиях цифровой трансформации //Государственная служба. – 2020. – Т. 22. – №. 2 (124). – С. 56-63; Сидоренко А. И. Судебная защита интеллектуальных прав в цифровую эпоху //Журнал российского права. – 2019. – №. 8. – С. 136-147; Сидоренко Э. Л. Правовой статус криптовалют в Российской Федерации //Экономика. Налоги. Право. – 2018. – Т. 11. – №. 2. – С. 129-137 и др.

Т.А. Поляковой, А.А. Смирнова⁵⁴, А.В. Минбалеева⁵⁵, А.А. Ефремова⁵⁶, А.А. Стрельцова⁵⁷ и др. Среди зарубежных авторов, занимающихся данной проблематикой необходимо отметить Л. Лессига⁵⁸, Э. Тикк⁵⁹, М. Кертууннен⁶⁰. Вместе с тем, данная проблематика представляется весьма политизированной, в связи с чем, необходимо отдельно остановится на недопустимости академической легитимации вмешательства во внутренние дела государств и проведения кибер-операций, на что делается акцент в рамках трудов «Таллинское руководство» и «Таллинское руководство 2.0» под редакцией авторитетного юриста М. Шмидта⁶¹. Конструктивистская трактовка норм применительно к цифровой сфере, в том числе в контексте обеспечения цифрового суверенитета представлена в трудах М. Финнемор и Д. Холлиса⁶². Данный подход, также весьма популярный в трудах западных исследователей регуляторики и права в цифровой сфере представляется в большей степени соответствующим целям и задачам настоящего исследования.

В последние годы появляются исследовательские проекты, посвященные анализу опыта цифрового суверенитета в различных регионах, которые позволяют выявить региональную и макрорегиональную специфику практики реализации

⁵⁴ Смирнов А. А. Проблемы формирования системы правового обеспечения информационно-психологической безопасности //Труды Института государства и права Российской академии наук. – 2022. – Т. 17. – №. 5. – С. 82-107; Полякова Т. А., Смирнов А. А. Правовое обеспечение международной информационной безопасности: приоритеты для Союзного государства //Право. by. – 2023. – №. 5. – С. 84-92.

⁵⁵ Полякова Т. А., Минбалеев А. В., Кроткова Н. В. Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации //Государство и право. – 2020. – №. 5. – С. 75-87;

⁵⁶ Ефремов А. А. Формирование концепции информационного суверенитета государства //Право. Журнал Высшей школы экономики. – 2017. – №. 1. – С. 201-215; Ефремов А. А. Государственный суверенитет в условиях цифровой трансформации //Правоведение. – 2019. – Т. 63. – №. 1. – С. 47-61; Ефремов А. А. Единые цифровые пространства: в поиске баланса между интеграцией и суверенностью //Информационное право. – 2016. – №. 3. – С. 36-39; Ефремов А. А. Проблемы реализации государственного суверенитета в информационной сфере //Вестник УрФО. Безопасность в информационной сфере. – 2016. – №. 2 (20). – С. 54-60; Ефремов А. А. международная интеграция" цифровых" пространств и обеспечение государственного суверенитета //современное международное право: глобализация и интеграция. liber amicorum в честь профессора ПН БИРЮКОВА. – 2016. – С. 81-86. Ефремов А. А. Обеспечение государственного суверенитета Российской Федерации в информационном пространстве в документах стратегического планирования //Академический юридический журнал. – 2017. – №. 2. – С. 11-20.

⁵⁷ Стрельцов А. А. Основные направления развития международного права вооруженных конфликтов применительно к киберпространству //Право и государство: теория и практика. – 2014. – №. 3. – С. 75-88.

⁵⁸ Lessig L. Code: And other laws of cyberspace. – ReadHowYouWant. com, 2009; Lessig L. The law of the horse: What cyber law might teach //Harv. L. Rev. – 1999. – Т. 113. – С. 501; Lessig L. Code is law //Harvard magazine. – 2000. – Т. 1. – №. 2000.

⁵⁹ Tikk E. Ten rules for cyber security //Survival. – 2011. – Т. 53. – №. 3. – С. 119-132.

⁶⁰ Tikk E., Kerttunen M. (ed.). Routledge handbook of international cybersecurity. – London : Routledge, 2020.

⁶¹ Schmitt M. N. (ed.). Tallinn manual on the international law applicable to cyber warfare. – Cambridge University Press, 2013. Schmitt M. N. (ed.). Tallinn manual 2.0 on the international law applicable to cyber operations. – Cambridge University Press, 2017.

⁶² Finnemore M., Hollis D. B. Constructing norms for global cybersecurity //American Journal of International Law. – 2016. – Т. 110. – №. 3. – С. 425-479.; Finnemore M., Hollis D. B. Beyond naming and shaming: Accusations and international law in cybersecurity //European Journal of International Law. – 2020. – Т. 31. – №. 3. – С. 969-1003. Finnemore M., Hollis D. B. Naming without Shaming? Accusations and International Law in Global Cybersecurity.”. – 2018.

цифрового суверенитета. Их результаты были использованы в ходе написания 3 главы настоящей диссертации. В частности, Л. Белли возглавляет проект КиберБРИКС (CyberBRICS)⁶³, а также публикует значительное число работ по цифровому суверенитету Бразилии и стран Латинской Америки⁶⁴. Исследованиями цифрового суверенитета или стратегической автономии ЕС в области данных и цифровых технологий занимаются А.Н Толстухина⁶⁵, Е.С. Зиновьева и В.И. Булва⁶⁶, А.В. Алейников, Д.А. Мальцева⁶⁷, С.В. Володенков⁶⁸, С.Н. Федорченко⁶⁹, а также европейские авторы Л. Флориди⁷⁰, Э. Селесте⁷¹, Р. Белланова⁷² и др. Данная тематика весьма широко представлена в трудах европейских ученых. В последние годы существенно возросло количество работ, осмысливающих опыт КНР в данной области, в том числе российских авторов К. Кожухова⁷³, И. Денисова⁷⁴, авторитетного зарубежного исследователя Р. Кримерса⁷⁵, а также авторов из КНР, в том числе Д. Ли⁷⁶, И. Хун⁷⁷ и др. Опыт Индии и стран «Глобального юга» в практике цифрового суверенитета рассмотрен

⁶³ www.cyberbrics.com

⁶⁴ Belli L. CyberBRICS: A multidimensional approach to cybersecurity for the BRICS //CyberBRICS: Cybersecurity Regulations in the BRICS Countries. – 2021. – С. 1-33. Belli L. (ed.). CyberBRICS: Cybersecurity regulations in the BRICS countries. – Springer Nature, 2021.

⁶⁵ Толстухина А. Технологический суверенитет Европейского союза и его границы // Дискуссионный клуб Валдай. Аналитические записки. № 19. Октябрь, 2022. URL: <https://ru.valdaiclub.com/files/42559/>

⁶⁶ Зиновьева Е. С., Булва В. И. Цифровой суверенитет Европейского союза //Современная Европа. – 2021. – №. 2. – С. 40-49.

⁶⁷ Мальцева Д. А., Алейников А. В. Эффекты цифровизации публичного управления современной России: трансформация модели в условиях глобальной политической конфронтации. – ООО Издательский дом «Сциентия». Конференция: XVII Ковалевские чтения Санкт-Петербург, 16–18 ноября 2023 года.

⁶⁸ Володенков С. В. и др. Цифровой суверенитет современного государства в условиях технологических трансформаций: содержание и особенности //Полилог. – 2021. – Т. 5. – №. 1.

⁶⁹ Володенков С. В., Федорченко С. Н., Печенкин Н. М. Возможности и особенности формирования мировоззрения в цифровой коммуникационной среде: по материалам экспертного исследования //Политическая экспертиза: ПОЛИТЭКС. – 2023. – Т. 19. – №. 1. – С. 58-79.

⁷⁰ Floridi L. The fight for digital sovereignty: What it is, and why it matters, especially for the EU //Philosophy & technology. – 2020. – Т. 33. – С. 369-378.

⁷¹ Celeste E. Digital sovereignty in the EU: challenges and future perspectives //Data protection beyond borders: Transatlantic perspectives on extraterritoriality and sovereignty. – 2021. – С. 211-228.

⁷² Bellanova R., Carrapico H., Duez D. Digital/sovereignty and European security integration: an introduction //European security. – 2022. – Т. 31. – №. 3. – С. 337-355.

⁷³ Кожухова К. Е. Политика Китая в области обеспечения цифрового суверенитета //Вестник академии военных наук. – 2020. – №. 4. – С. 171-176.

⁷⁴ Денисов, И.Е. Китайская стратегия «больших данных»: реформа управления, инновации и глобальная конкуренция. М.: Издательство «МГИМО-Университет», 2023. 28 с.

⁷⁵ Creemers R. China's conception of cyber sovereignty //Governing cyberspace: Behavior, power and diplomacy. – 2020. – С. 107-145.:

⁷⁶ Lee J. The CPC and Sovereignty in a Digitally Connected World. 2020

⁷⁷ Yun H. China's data sovereignty and security: Implications for global digital borders and governance //Chinese Political Science Review. – 2024. – С. 1-26.

в работе М. Ксианг⁷⁸. Опыт цифрового суверенитета России также привлекает существенное внимание, однако комплексных исследований с позиций теории международных отношений настоящей проблематике не было представлено в научной литературе, большая часть вопросов рассмотрена фрагментарно в рамках уже описанных выше научно-исследовательских трудов.

В МГИМО и других вузах уже был защищен ряд кандидатских и докторских диссертаций, посвященных различным аспектам цифрового суверенитета, в том числе затрагивающих данную тематику с позиций международного права (А.А. Смирнов⁷⁹, А.А. Ефремов⁸⁰), международной информационной безопасности (Е.С. Зиновьева⁸¹, И.О. Яникеева⁸², В.И. Булва⁸³), информационного противоборства (М.В. КучерявыЙ⁸⁴) или региональных аспектов информационной безопасности (А.В. Макарычева⁸⁵). Однако, несмотря на наличие научных работ, докторских и кандидатских диссертаций и аналитических докладов по теме трансформации суверенитета в цифровую эпоху, выбранная тема исследования не получила систематического осмыслиения в научной литературе по международным отношениям и политическим наукам. Настоящий пробел призвано восполнить предлагаемое исследование.

Проведенный анализ научной литературы позволяет сделать вывод о том, что, несмотря на значительное количество исследований, посвященных различным аспектам цифрового суверенитета, данная тема остается недостаточно систематизированной в рамках теории международных отношений и политической науки.

Существующие работы сосредоточены на отдельных аспектах цифрового

⁷⁸ Jiang M. Models of State Digital Sovereignty From the Global South: Diverging Experiences From China, India and South Africa //Policy & Internet. – 2024. – Т. 16. – №. 4. – С. 727-738.

⁷⁹ Смирнов А.А. Формирование системы правового обеспечения информационной безопасности Российской Федерации : дис.... д-ра юрид. наук // Москва, 2021. 418с. <http://www.igpran.ru/nauka/Автореферат%20диссертации%20%20Смирнов%20А.А.pdf>

⁸⁰ Ефремов А. А. Информационно-правовой механизм обеспечения государственного суверенитета Российской Федерации: дис.... д-ра юрид. наук //АА Ефремов–Москва–2020.–418с. – 2020.

⁸¹ Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности: проблемы, субъекты, перспективы : дис. ... доктора полит. Наук // ЕС Зиновьева – Москва – 2019. 350 с.

⁸² Яникеева И.О. Фактор международной информационной безопасности в двусторонних отношениях России и США в XXI веке дис.... канд. полит. наук //–Москва–2023. <https://mgimo.ru/science/diss/yanikeeva-i-o.php>

⁸³ Булва В.И. Международная информационная безопасность в деятельности ООН (1998-2021): проблемы и перспективы дис.... канд. полит. наук //–Москва–2023

⁸⁴ КучерявыЙ М.М. Информационное измерение политики национальной безопасности России в условиях современного глобального мира : дисс. на соискание ученой степени доктора политических наук : специальность 23.00.04 / КучерявыЙ Михаил Михайлович ; С.-Петерб. гос. ун-т. - Санкт-Петербург, 2014.

⁸⁵ Макарычева А.В. Подходы к преодолению традиционных и новых вызовов безопасности в Латинской Америке (на примере территориальных споров и информационных угроз) дис.... канд. полит. наук //–Москва–2020

суверенитета (правовых, экономических, технологических, региональных), однако отсутствует комплексный междисциплинарный анализ, интегрирующий эти направления в единую теоретическую рамку. Большинство исследований носит прикладной характер, тогда как концептуальные основания цифрового суверенитета (его природа, критерии, механизмы реализации) требуют более глубокой теоретической проработки.

Традиционные же теории суверенитета не в полной мере учитывают вызовы цифровизации, такие как трансграничность данных, влияние технологических корпораций. Концепции государственного суверенитета требуют адаптации к условиям цифровой среды, где суверенитет становится не столько территориальным, сколько функциональным и технологически обусловленным. Вопросы цифрового суверенитета часто рассматриваются через призму национальных или региональных интересов (ЕС, КНР), что затрудняет выработку универсальных теоретических подходов. Правовые исследования цифрового суверенитета не всегда учитывают политico-экономические факторы, влияющие на реализацию цифрового суверенитета. Несмотря на растущее внимание к цифровому суверенитету в России, большинство работ носит фрагментарный характер, а комплексных исследований, анализирующих российский опыт в контексте глобальных трендов, практически нет.

Таким образом, актуальность диссертационного исследования обусловлена необходимостью преодоления теоретической разрозненности, разработки целостной концепции цифрового суверенитета и анализа его трансформации в условиях глобальной цифровизации. Данная работа призвана восполнить существующий пробел, предложив системный подход к изучению цифрового суверенитета как нового измерения государственного суверенитета в XXI веке.

Цель исследования состоит в том, чтобы определить основные направления трансформации государственного суверенитета под влиянием цифровизации.

В соответствии с поставленной целью были поставлены следующие **задачи**:

- провести критический анализ существующих теоретических подходов (реализм, либерализм, конструктивизм, критическая теория) к пониманию суверенитета в условиях цифровой эпохи и выявить их эвристический потенциал и ограничения;
- сформулировать теоретико-методологические основания исследования – оценить аналитический потенциал теории социального конструктивизма

применительно к современной цифровой революции;

– охарактеризовать основные направления развития современных цифровых технологий в контексте мировой политики и международных отношений;

– выявить современные факторы, влияющие на политику ведущих стран мира в области обеспечения цифрового суверенитета;

– оценить влияние угроз международной информационной безопасности и секьюритизации информационного пространства на общую тенденцию к укреплению цифрового суверенитета в мировой политике;

– выявить соотношение понятий «Вестфальский суверенитет», «внутренний суверенитет», «внешний суверенитет», «суверенитет взаимозависимости», «цифровой суверенитет»;

– дать оценку концепции «пост-вестфальской» модели суверенитета и ее применимость к цифровому пространству;

– раскрыть политическую роль международного права и возможность формирования новых норм, регулирующих цифровой суверенитет и государственное поведение в киберпространстве;

– концептуализировать процесс секьюритизации цифровой сферы: как и кем киберугрозы конструируются как экзистенциальные вызовы национальной безопасности, требующие чрезвычайных мер;

– определить роль современных цифровых технологий в трансформации государственного суверенитета на современном этапе;

– сформулировать авторское видение реализации политики Российской Федерации в области обеспечения цифрового суверенитета.

Объект исследования – государственный суверенитет в современной мировой политике.

Предмет исследования – проблема обеспечения суверенитета государств в современной мировой политике под влиянием цифровизации.

Хронологические рамки исследования – с 1969 г. по настоящее время. Выбор отправной точки исследования обусловлен тем фактом, что 1969 г. исторически считается «датой рождения» Интернета, когда была осуществлена первая передача данных по сети. Цифровая революция, ставшая основой трансформации суверенитета, начинается в 1969 году и продолжается по сей день. Подобное определение хронологических рамок позволяет проследить

трансформацию категории государственного суверенитета под воздействием цифровой революции и современных информационно-коммуникационных технологий.

Область исследования соответствует требованиям следующих пунктов паспорта ВАК для специальности 5.5.4. Международные отношения, глобальные и региональные исследования, в частности следующим областям исследований политической науки: п. 2. Субъекты международных отношений. Деятельность государственных и негосударственных акторов. Формальные и неформальные институты в международных отношениях и в мировой политике. Формирование и реализация внешнеполитических стратегий, концепций и доктрин; п. 7. Международная безопасность. Системы глобальной и региональной безопасности. Военная сила в международных отношениях. Международный терроризм и борьба с ним. Разоружение и контроль над вооружениями. Вызовы, риски, опасности и угрозы.; п. 17. Информационные, когнитивные, био- и другие новые технологии в международных отношениях и мировой политике.

Методологическая и теоретическая база исследования.

В качестве теоретической базы исследования использовано конструктивистское направление, которое позволяет изучать государственную политику в области формирования «цифрового суверенитета» как социально обусловленную, при этом важную роль играет восприятие и идентичность. Одним из основоположников социального конструктивизма является А. Вендт, который отмечает, что мировая политика представляет собой социальный конструкт, и такие ключевые категории как «суверенитет» также являются социально сконструированными, то есть зависят от идентичностей и представлений субъектов мировой политики, прежде всего, государств⁸⁶. Современное развитие информационно-коммуникационных технологий меняет идентичности государств и их восприятие своих интересов и угроз, усиливая цифровую составляющую в указанных категориях, что обосновывает выбор конструктивизма и его применимость к анализу категории «цифрового суверенитета».

В качестве теории среднего уровня использована концепция секьюритизации, разработанная представителями Копенгагенской школы международных исследований⁸⁷. Данный подход позволяет рассмотреть

⁸⁶ Wendt A. Anarchy is what states make of it: the social construction of power politics //International organization. – 1992. Т. 46. №. 2. – С. 391-425.

⁸⁷ См. напр.: Buzan B. et al. Security: A new framework for analysis. – Lynne Rienner Publishers, 1998.

трансформацию международной повестки дня в области информационной безопасности, как фактор укрепления цифрового суверенитета государств. Растущая секьюритизация информационных технологий ведет к тому, что государства воспринимают данные угрозы как непосредственный вызов суверенитету и, в свою очередь, усиливают программы, направленные на обеспечение цифрового суверенитета.

Кроме того, важный вклад в осмысление цифрового суверенитета в современных международных отношениях внесли труды в рамках «практического поворота» в теории международных отношений, в том числе таких авторов как Е. Адлер, Д. Биго, В. Пулио⁸⁸. Практический поворот в теории международных отношений смещает фокус с на конкретные действия, рутинные практики и материальные аспекты мировой политики. Он подчеркивает, как акторы – государства, корпорации, экспертные сообщества – не просто следуют предписанным правилам, а активно формируют международный порядок через повседневные решения, технические стандарты и адаптацию к неформальным нормам. Этот подход позволяет изучать международные отношения через анализ того, как власть и суверенитет реально осуществляются в цифровых инфраструктурах, регуляторных режимах и даже в коде алгоритмов.

Такой взгляд помогает раскрыть, как государства на практике – а не только в доктринах и официальных документов – отстаивают контроль над данными и сетями в цифровой сфере. Практический поворот позволяет изучить цифровой суверенитет как совокупность материальных решений: от серверной инфраструктуры до протоколов шифрования, которые и создают реальные границы в киберпространстве.

Кроме того, в качестве теории среднего уровня использована концепция суверенитета С. Краснера⁸⁹. Краснер предлагает многомерную типологию, выделяя четыре взаимосвязанных, но концептуально различных вида суверенитета:

1. Вестфальский суверенитет (Westphalian sovereignty) – традиционное понимание суверенитета как исключительного права государства на контроль в пределах своей территории без вмешательства внешних акторов. В цифровую

⁸⁸ Bigo D. Pierre Bourdieu and international relations: Power of practices, practices of power //International political sociology. – 2011. – Т. 5. – №. 3. – С. 225-258. Adler E., Pouliot V. International practices //International theory. – 2011. – Т. 3. – №. 1. – С. 1-36.

⁸⁹ Krasner S. D. Sovereignty. – Princeton University Press, 1999.

эпоху этот аспект подвергается наиболее серьезным вызовам, учитывая трансграничную природу киберпространства.

2. Суверенитет взаимозависимости (Interdependence sovereignty) – способность государства контролировать трансграничные потоки (товаров, капиталов, информации). Применительно к цифровой сфере это предполагает анализ возможностей государств регулировать потоки данных и технологий.

3. Внутренний суверенитет (Domestic sovereignty) – эффективность государственных институтов в осуществлении власти на своей территории. В цифровом контексте это включает вопросы контроля над национальным сегментом интернета и цифровой инфраструктурой.

4. Международно-правовой суверенитет (International legal sovereignty) – признание государства другими акторами международной системы. В киберпространстве это проявляется в участии в международных регуляторных режимах.

Концепция Краснера особенно ценна для данного исследования, поскольку позволяет избежать редукционизма при анализе цифрового суверенитета, но при этом выявить асинхронность трансформации разных аспектов суверенитета и оценить, какие измерения суверенитета подвергаются наибольшей эрозии в условиях цифровизации. Кроме того, данный подход дает возможность проанализировать, как государства компенсируют ослабление одних видов суверенитета усилением других в цифровой сфере. Такой многомерный подход особенно актуален для изучения российской политики цифрового суверенитета, где можно наблюдать ослабление вестфальского суверенитета в цифровой сфере, но при этом усиление суверенитета взаимозависимости через меры технологического протекционизма и контроля цифровых границ, укрепление внутреннего суверенитета посредством развития национальной ИТ-инфраструктуры. При этом на международном уровне Россия ведет активную борьбу за международно-правовой суверенитет в рамках кибердипломатии.

Методы исследования включают конструктивистский подход, методы анализа политических нарративов и секьюритизационный анализ, позволяющие выявить способы конструирования цифрового суверенитета в международной политике. Эмпирическая часть основана на сравнительном изучении стратегических документов государств и международных организаций, а также на анализе конкретных примеров регулирования цифровой среды и практики обеспечения цифрового суверенитета.

Опираясь на социальный конструктивизм, цифровой суверенитет исследуется как социально обусловленный феномен, формирующийся под влиянием идентичности государств, их представлений об угрозах и нормативных ожиданий международного сообщества. Конструктивистская методология позволила проследить, как понятие цифрового суверенитета институционализируется в государственных стратегиях, концепциях кибербезопасности и международных проектах регулирования данных.

Методы анализа политических нарративов применялись для выявления ключевых смысловых рамок, с помощью которых государства и международные организации конструируют цифровой суверенитет — от европейского нарратива «цифровой автономии» до китайского «киберсуверенитета», российского акцента на информационной безопасности и американского дискурса технологической открытости.

Секьюритизационный анализ позволил реконструировать процесс превращения цифровой сферы в объект национальной безопасности, выявить акторов секьюритизации (государства, международные организации, цифровые регуляторы), референтные объекты (данные граждан, критическая инфраструктура) и меры (локализация данных, экспортный контроль технологий).

Эмпирическая часть исследования основана на сравнительном изучении стратегических документов государств и международных организаций, нормативно-правовых актов, концепций цифрового развития, а также анализе конкретных примеров регулирования цифровой среды: локализации данных, контроля цифровых платформ, развития автономной инфраструктуры, мер технологического импортозамещения, политики в области ИИ, кибербезопасности и регулирования трансграничных потоков данных.

Сравнительный анализ стратегий России, ЕС, США, Китая, позволил выявить разнообразие национальных моделей цифрового суверенитета и формирование цифровых макрорегионов. Анализ кейсов цифрового регулирования позволил установить зависимость реализации цифрового суверенитета от уровня технологической автономии и степени секьюритизации цифровой сферы.

Эмпирической базой для исследования послужили российские концепции по вопросам внутренней и внешней политики (Концепция внешней политики

Российской Федерации от 2023 года)⁹⁰, доктрины и стратегии Российской Федерации (Доктрина информационной безопасности Российской Федерации в редакции от 2016 года⁹¹, Военная доктрина Российской Федерации от 2014⁹², Стратегия национальной безопасности Российской Федерации от 2021 года⁹³), официальные документы других стран (КНР, США и др)⁹⁴, документы международных правительственные организаций и форумов (Резолюции Генеральной Ассамблеи ООН⁹⁵, соглашения, подписанные в рамках ШОС⁹⁶, ОДКБ⁹⁷, АСЕАН⁹⁸, Меркосур⁹⁹ итоговые декларации БРИКС¹⁰⁰, Группы двадцати¹⁰¹ и Группы восьми¹⁰²).

Научная новизна диссертационного исследования .

1. Концептуализация цифровых границ как нового политического института.

- впервые в отечественной политической науке цифровые границы рассмотрены не только как технологический или правовой феномен, но и как институт, трансформирующий традиционные представления о государственном

⁹⁰ Концепция внешней политики Российской Федерации. Утверждена Президентом Российской Федерации В.В.Путиным 31 марта 2023 г. URL: <https://www.mid.ru/ru/detail-material-page/1860586/>

⁹¹ Доктрина информационной безопасности Российской Федерации. Утв. Президентом РФ 5.12.2016. URL: <http://www.scrf.gov.ru/documents/6/5.html>

⁹² Военная доктрина Российской Федерации. Утв. Президентом 25 декабря 2014 г., № Пр-2976. URL: <http://www.scrf.gov.ru/security/military/document129/>

⁹³ Стратегия национальной безопасности Российской Федерации. Утверждена указом Президента Российской Федерации 02.07.2021 № 400. URL: <http://www.kremlin.ru/acts/bank/47046>

⁹⁴ National Cyber Strategy of the USA. White House, September, 2018. URL: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf> ; National Security Strategy of the USA. White House, 2022. URL: <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf> ; International Strategy of Cooperation on Cyberspace. Ministry of Foreign Affairs of the People's Republic of China. Beijing, 2017. URL: http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm

⁹⁵ Резолюция ГА ООН A/C.1/73/L.27/Rev.1 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 29 октября 2018 г.; Резолюция ГА ООН A/53/70 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 4 декабря 1998 г.

⁹⁶ Соглашение между правительствами государств – членов Шанхайской организации сотрудничества в области обеспечения международной информационной безопасности. 2009 г.

⁹⁷ Соглашение о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 г.

⁹⁸ Заявление Российской Федерации и АСЕАН о сотрудничестве в области обеспечения безопасности использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий от 14 ноября 2018 г.

⁹⁹ Declaración presidencial sobre la integración digital en el MERCOSUR, 2021. URL: <https://www.mercosur.int/documento/declaracion-presidencial-sobre-la-integracion-digital-en-el-mercadosur/>

¹⁰⁰ Казанская декларация БРИКС. Казань, 2024

¹⁰¹ Communiqué: G20 Finance Ministers and Central Bank Governors Meeting. Baden-Baden, 2017. URL: <https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/Communique+G20+Finance+Ministers+and+Central+Bank+Governors+Meeting+3-18-2017.pdf>

¹⁰² Окинавская Хартия глобального информационного общества. -- Окинава, 2000.

URL: <http://www.ifap.ru/ofdocs/okinhar.htm>; G8 Background paper: International action against Cybercrime. Evian, 2003.

суворенитете;

- выявлены ключевые характеристики цифровых границ, отличающие их от классических территориальных границ: виртуальность, динамичность, зависимость от инфраструктурного контроля и нормативных режимов;
- осуществлена концептуализация цифровых границ как специфического политического института, трансформирующего традиционные представления о границах государства и формах его взаимодействия с глобальной цифровой средой.

2. Систематизация нормативной конкуренции в цифровой сфере.

- Проведен сравнительный анализ экстерриториальных практик цифрового регулирования (GDPR EC, CLOUD Act США, китайский закон о данных и др.), что позволило выделить их ключевые противоречия (в том числе конфликт между территориальным суверенитетом государств и экстерриториальным действием правовых норм GDPR, противоречие интересов транснациональных платформ и государственных регуляторов, баланс между инновациями и безопасностью) и влияние на цифровой суверенитет государств .

- Разработана типология стратегий государств в условиях нормативной конкуренции: от жесткого протекционизма до гибридной адаптации к глобальным цифровым режимам.

- в диссертации впервые в отечественной политической науке нормативная конкуренция и экстерриториальные практики цифрового регулирования (GDPR EC, CLOUD Act США и подобные акты) представлены как ключевые системные вызовы для реализации государственного цифрового суверенитета.

- аналитически выделены и систематизированы феномены цифровых границ и цифрового суверенитета, а также разработаны авторские предложения по совершенствованию международно-правовых норм и дипломатических практик в целях минимизации их негативного воздействия на цифровой суверенитет государств.

3. Эмпирическое подтверждение трансформации суверенитета в цифровую эпоху.

- На основе анализа конкретных примеров (ЕС, США, КНР, Россия) доказано, что цифровой суверенитет реализуется не через абсолютный контроль, а через избирательное регулирование критических инфраструктур и данных.

- выявлена зависимость цифрового суверенитета от технологической автономии

государства, что подтверждается анализом санкционных режимов и ограничений в сфере высоких технологий. Зависимость цифрового суверенитета от технологической автономии состоит в том, что способность государства контролировать цифровую инфраструктуру, данные и критические технологии напрямую определяется доступом к высокотехнологичным компонентам — микроэлектронике, облачным сервисам, телекоммуникационным сетям и технологиям искусственного интеллекта. Анализ санкционных режимов и ограничений в сфере высоких технологий показывает, что государства, лишённые такого доступа, оказываются ограничены в способности обеспечивать устойчивость цифровой инфраструктуры, защищать данные, развивать национальные ИИ-системы и противостоять экстерриториальным правовым требованиям других стран. Таким образом, технологическая автономия является ключевым структурным условием цифрового суверенитета.

Положения, выносимые на защиту:

1. Цифровая трансформация не только меняет традиционные представления о суверенитете, но и трансформирует саму его сущность, переводя акцент с территориального контроля на управление данными, цифровыми ресурсами и инфраструктурой. Эти изменения требуют переосмыслиния фундаментальных принципов международного права и пересмотра роли государства в глобальном управлении. Международное право нуждается в выработке новых норм, учитывающих специфику цифровых технологий и цифрового суверенитета, в том числе трансграничный характер и множественность акторов. Приоритетной площадкой для выработки такого рода норм является ООН как организация с универсальным членством и неоспоримой легитимностью.

2. На основе анализа современной практики реализации суверенитета доказано, что цифровой суверенитет не сводится исключительно к территориально ориентированным классическим трактовкам, а представляет собой многоуровневый и поликентричный сетевой феномен, формируемый в процессе взаимодействия государств, международных организаций и глобальных технологических компаний, выступая в качестве самостоятельного и многосубъектного явления международной политики. Процессы цифровой трансформации государственного суверенитета происходят неравномерно и характеризуются асинхронностью, при которой ослабление вестфальского аспекта

суверенитета сопровождается одновременным укреплением внутреннего суверенитета и суверенитета взаимозависимости.

3. Впервые в российской политической науке предложено рассматривать «цифровые границы» как институционально-нормативные и технологические механизмы, посредством которых государство обеспечивает контроль и регулирование потоков данных, платформенной экономики и критической цифровой инфраструктуры. Цифровые границы могут быть концептуализированы как специфического политического института, трансформирующего традиционные представления о границах государства и формах его взаимодействия с глобальной цифровой средой.

4. В условиях цифровой трансформации мировой экономики данные становятся стратегическим ресурсом, равнозначным природным богатствам. Государства, способные эффективно контролировать потоки данных и защищать цифровую инфраструктуру, приобретают преимущества в международной политике, что усиливает их позиции на глобальной арене. Контроль над данными, так же как и инфраструктурой их хранения и участие в выработке норм их регулирования и защиты на национальном и международном уровне является одним из важнейших элементов цифрового суверенитета в эпоху искусственного интеллекта. Усиление контроля над данными должно сопровождаться внедрением этических стандартов, гарантирующих соблюдение прав человека и недопущение дискриминации в цифровой среде. Это направление требует дальнейшей проработки на международном уровне, в том числе в контексте недопущения цифрового колониализма и колониализма данных.

5. Технологическое доминирование передовых держав, таких как США и Китай, создаёт новые формы неравенства в международных отношениях. доступ к передовым технологиям искусственного интеллекта и большими данным укрепляет влияние этих стран, в то время как другие государства вынуждены адаптироваться к внешним стандартам, что подрывает их суверенитет. Данный феномен представляет собой новую форму цифрового неоколониализма, реализуемого через практику экстерриториального цифрового суверенитета ведущих держав, распространяющих свои нормы, технологии и правовые рамки на менее развитые страны. Доминирующее положение транснациональных цифровых платформ (Google, Facebook, Alibaba и др.) способствует возникновению новых форм эрозии государственного суверенитета и формирует предпосылки для распространения

цифрового протекционизма.

6. Выявлена тенденция секьюритизации цифрового пространства как глобальная тенденция: проведенный анализ показал, что в XXI веке национальные стратегии цифрового суверенитета в значительной степени сосредоточены на секьюритизации киберпространства. Ведущие страны мира рассматривают киберугрозы как первоочередную проблему национальной безопасности, что приводит к укреплению государственного контроля над цифровыми коммуникациями.

7. Существующие международные нормы недостаточно учитывают вызовы цифровой эпохи. Это открывает перспективу для выработки новых механизмов международного сотрудничества, направленных на обеспечение равных условий для всех участников глобального цифрового пространства и защиту суверенитета слабых государств. Одной из перспективных международных площадок в данной области может стать создаваемый в 2025 году постоянный институциональный диалог ООН по международной информационной безопасности, который с одной стороны предполагает участие всех государств-членов ООН и возможность выработки обязательных соглашений, а с другой – допускает возможность консультативного участия бизнеса и неправительственных организаций.

8. Сравнительный анализ стратегий ЕС, России, Китая и США выявил их уникальные подходы к регулированию цифровой среды. Эти различия объясняются как внутренними политическими приоритетами, особенностями политической культуры, а также и степенью зависимости от международных технологических гигантов, что подчеркивает важность локальных особенностей в развитии глобальных стратегий цифрового управления. ЕС делает акцент на нормативном регулировании платформ и ИИ, защите персональных данных; Россия фокусируется на проблемах обеспечения информационной безопасности и технологической независимости; США делает ставку на доминирование через частные цифровые платформы и корпоративное лидерство; Китай стремится обеспечить строгий контроль над цифровым пространством и развитие национальных платформенных компаний.

9. На основе сравнительного анализа стратегий реализации цифрового суверенитета в Европейском союзе, ЕврАзЭС, АСЕАН и других региональных объединениях выявлено существование цифровых макрорегионов, характеризующихся сходными подходами к нормативно-правовому

регулированию цифровой среды и совместной защитой цифрового пространства от внешних вызовов. Процесса цифровой регионализации как важнейшего элемента современной архитектуры международных отношений.

Обоснованность и достоверность научных результатов, положений и выводов, содержащихся в диссертационной работе, обеспечивается широкой теоретической, нормативно-правовой и информационной базой и определяется полученным теоретическим научным знанием, которое обобщает, развивает и дополняет существующие научные представления о конструктивистском подходе к изучению государственной политики в области формирования «цифрового суверенитета» как социально обусловленной, при этом важную роль играет восприятие и идентичность. Практический поворот позволяет изучить цифровой суверенитет как совокупность материальных решений: от серверной инфраструктуры до протоколов шифрования, которые и создают реальные границы в киберпространстве.

Теоретическая значимость результатов диссертационной работы обусловлена малой изученностью выбранной темы в современной научной литературе, однако, изучение трансформации данной аналитической категории, которая происходит под влиянием процессов цифровизации, а также практических подходов государств к обеспечению цифрового суверенитета способны расширить не только понимание категории суверенитета государства в научной литературе, но и осмыслить тенденции трансформации мировой политики в условиях информационной революции. Классические теории суверенитета продолжают оперировать категориями территории и монополии на насилие, однако в цифровую эпоху реальная власть смещается в сферу контроля над информационными потоками, алгоритмами принятия решений и цифровой идентичностью граждан. Российские исследователи, включая специалистов в области кибербезопасности и цифровой экономики, уже начали заполнять этот концептуальный вакuum, однако системного осмысления происходящего сдвига в балансе сил между государствами и технологическими корпорациями пока недостаточно. Именно этот пробел в академической литературе и призвано восполнить настоящее исследование, что обуславливает теоретическую значимость выбранной темы исследования и полученных научных результатов.

Таким образом, исследование вносит вклад в теорию международных отношений и политическую науку, предлагая новую концептуальную рамку для

анализа цифрового суверенитета, а также практические рекомендации для укрепления регуляторных и дипломатических стратегий государств в цифровую эпоху.

Практическая значимость результатов исследования заключается в том, что оно может быть использовано органами государственной власти России в ходе реализации политики в области информационной безопасности и обеспечения государственного суверенитета в глобальном информационном пространстве. В условиях, когда санкционное давление на Россию включает в себя и технологические ограничения, вопросы цифрового суверенитета переходят в область национальной безопасности. Опыт последних лет наглядно демонстрирует, как зависимость от иностранных цифровых платформ и технологий может превратиться в уязвимость в моменты геополитической турбулентности. Разработка национальных технологических решений, создание альтернативных систем идентификации и платежей, формирование независимой цифровой инфраструктуры – все это становится факторами государственного суверенитета в XXI веке.

При этом Россия находится в уникальной позиции – с одной стороны, государства сталкивается с теми же вызовами цифровой трансформации, что и другие государства, с другой – наш опыт технологического суверенитета в условиях санкций может стать ценным кейсом для международного сообщества. Изучение этого опыта, анализ успехов и неудач, выявление оптимальных моделей регулирования цифрового пространства – все это открывает новые перспективы теоретического осмыслиения практики реализации государственного суверенитета в цифровую эпоху, а также позволяет сформулировать рекомендации в целях практического укрепления позиций России в глобальном информационном пространстве.

Полученные автором результаты исследования получили широкое внедрение в учебный процесс МГИМО МИД России, в частности, в рамках различных дисциплин преподаваемых на факультетах Международных отношений, Международных экономических отношений, Международной журналистики Факультете управления и политики в качестве базовой и дополнительной литературы используется учебное пособие «Цифровые международные отношения», «Цифровая трансформация мировой экономики», а также научные статьи, подготовленные автором в целях апробации научных

результатов проведенного исследования.

Апробация результатов исследования. Основные положения и результаты исследования были апробированы в монографических научных работах, а также опубликованы в качестве научных статей в рецензируемых научных изданиях, индексируемых в отечественных и международных библиометрических системах, рекомендуемых ВАК при Минобрнауки России и входящих в Перечень научных изданий РУДН. Результаты исследования нашли отражение в экспертно-аналитической деятельности для Министерства иностранных дел, Министерства обороны и Генштаба Российской Федерации, а также других заинтересованных министерств и ведомств.

Наиболее значимые результаты работы были представлены автором на российских и международных конференциях, симпозиумах, открытых выступлениях в том числе: Международная научно-практическая конференция «Тарлевские чтения. К новой архитектуре многополярного мира» (Москва, 2025), VII научная конференция «История отечественной культуры в архивных документах» Российской национальной библиотеки (Санкт-Петербург, 2024), Петербургский международный экономический форум (Санкт-Петербург, 2024), III Международный Алтайский форум «Алтайский вектор евразийской интеграции: в интересах укрепления межнационального и межрелигиозного согласия» (Горно-Алтайск, 2024), III международная научно-практическая конференция «Цифровые международные отношения 2024» (Москва, 2024), II международная научно-практическая конференция «Цифровые международные отношения 2023» (Москва, 2023), I международная научно-практическая конференция «Цифровые международные отношения 2022» (Москва, 2022).

Публикации по теме исследования. По теме исследования опубликованы 23 научные работы общим объемом более 135,25 п.л., в том числе 15 в изданиях, рекомендованных ВАК при Минобрнауки России и перечнем РУДН имени Патриса Лумумбы (общим объемом 16,5 п.л.), 4 монографии и главы в монографиях (общим объемом 45,75 п.л.) и 2 учебных пособия для вузов (общим объемом 73 п.л.). Общий объем публикаций более 150 п.л., авторский вклад 82,4%.

Структура диссертационной работы определена логикой исследования, его целью и задачами. Диссертация состоит из введения, трех глав, заключения. Основной текст изложен на 289 страницах. Список литературы включает 269 наименований. Цифровой и графический материал представлен 1 рисунком.

II. ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

ГЛАВА 1. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВАНИЯ ИССЛЕДОВАНИЯ КАТЕГОРИИ «ГОСУДАРСТВЕННЫЙ СУВЕРЕНИТЕТ» В УСЛОВИЯХ ГЛОБАЛЬНОЙ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

В параграфе «Эволюция подходов к концептуализации понятия «государственный суверенитет» в политической мысли» рассмотрена история изучения данной научной категории в исторической ретроспективе. Во втором параграфе «Понятие и признаки государственного суверенитета в современной политической науке и теории международных отношений исследованы современные подходы. Затем в рамках параграфа Категория государственного суверенитета в контексте трансформации международного порядка» исследованы современные вызовы, связанные с формированием многополярности. Четвертый параграф «Подходы к изучению цифрового суверенитета в современной политической науке» сосредоточен на категории цифрового суверенитета. Для целей данного исследования цифровой суверенитет будет определяться в неореалистской традиции российских ученых: как способность государства утверждать свое независимое управление и обеспечивать соблюдение собственных законов и правил в цифровом пространстве на фоне глобализации и взаимосвязи цифровой среды. Это важное условие политического суверенитета и национальной независимости государства в современном мире.

Обеспечение независимости в цифровом пространстве неизбежно затрагивает обеспечение безопасности информационных ресурсов и инфраструктур государства (технологический суверенитет в части информационно-коммуникационной инфраструктуры), контроль над потоками данных, защиту прав и безопасности граждан от цифровых угроз (суверенитет данных), а также взаимодействие государственных институтов по данным вопросам внутри и вне государства.

Цифровой суверенитет подразумевает поиск эффективных механизмов установления такого контроля без ограничения преимуществ цифровизации, таких как инновации и экономическое развитие. Кроме того, он позволяет сбалансировать национальный контроль с международным сотрудничеством для управления цифровой сферой таким образом, чтобы обеспечить равные права и

безопасность для всех участников.

ГЛАВА 2. МИРОПОЛИТИЧЕСКАЯ КОНЦЕПТУАЛИЗАЦИЯ СОВРЕМЕННОЙ ЦИФРОВОЙ РЕВОЛЮЦИИ

В параграфе «Характеристики прорывных цифровых технологий Четвертой промышленной революции» отмечается, что развитие прорывных цифровых технологий порождает новые угрозы международной безопасности, но и создает новые возможности для роста и развития. Цифровые технологии существенно влияют на международные отношения, изменяя динамику взаимодействий между государствами, международными организациями и негосударственными акторами.

Цифровые технологии также изменяют дипломатию и международные переговоры. Государства могут использовать социальные сети, веб-сайты и онлайн-платформы для общения с международной аудиторией, продвижения своих интересов и формирования имиджа. Цифровые инструменты позволяют оперативно реагировать на международные события и кризисы, обеспечивая быструю передачу информации и координацию действий. Цифровые технологии создают новые угрозы в виде кибератак на государственные структуры, критическую инфраструктуру и частные компании, что требует международного сотрудничества в сфере кибербезопасности.

Как показано во втором параграфе «Актуальные проблемы развития и управления глобальным цифровым пространством», современная цифровая революция радикально трансформирует международные отношения, привнося новые вызовы и возможности для глобального управления. В третьем параграфе «Концептуализация цифровой революции в современной науке о международных отношениях» отмечается, что цифровая среда становится не просто технологической, но и политической ареной, где пересекаются интересы государств, транснациональных корпораций и международных институтов. Технологии четвертой промышленной революции – искусственный интеллект, большие данные, интернет вещей и блокчейн – усиливают сложность мировой политики, переопределяя привычные категории, такие как суверенитет, безопасность и власть.

Цифровой суверенитет, являясь ключевым элементом адаптации государств к цифровой эпохе, интегрирует в себя различные аспекты управления данными,

кибербезопасности и технологической независимости. Секьюритизация цифрового пространства подчеркивает важность этого понятия, демонстрируя, как государства пытаются защитить свои интересы, усиливая контроль над трансграничными потоками данных и локализуя цифровую инфраструктуру. Однако односторонние подходы часто приводят к фрагментации глобального цифрового пространства, создавая напряженность между национальными приоритетами и необходимостью международного сотрудничества.

Научные подходы к цифровому суверенитету, варьирующиеся от реалистических до конструктивистских, показывают, что он является одновременно инструментом укрепления национальной идентичности и фактором, формирующим новый мировой порядок. В условиях глобальной взаимозависимости эта концепция становится индикатором изменений в международной системе, балансируя между стремлением государств к автономии и давлением глобализации, которая требует новых форм регулирования и согласованных действий.

Таким образом, цифровая революция и цифровой суверенитет не только отражают изменения в технологиях, но и представляют собой ключевые точки трансформации мировой политики. Эти процессы требуют пересмотра теоретических и практических подходов, способных обеспечить стабильность, безопасность и справедливость в быстро меняющемся мире.

ГЛАВА 3. ЦИФРОВОЙ СУВЕРЕНИТЕТ В ПРАКТИКЕ СОВРЕМЕННЫХ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ: ОПЫТ ВЕДУЩИХ СТРАН И МЕЖДУНАРОДНЫХ СТРУКТУР

Цифровой суверенитет проявляется как инструмент, через который государства стремятся одновременно укрепить свои внутренние позиции и адаптироваться к новым вызовам международной политики. В современных условиях он перестал быть просто механизмом защиты от внешних угроз, превратившись в способ переосмыслиения основ цифровой экономики, безопасности и глобального управления. Именно через призму этого понятия государства и международные организации формируют свои стратегии на пересечении технологий, прав человека и национального суверенитета.

Данная тенденция, однако, не носит абсолютного характера. Многие цепочки поставок на глобальном уровне сохраняют свою связность и играют

важную роль в формировании не только глобальной инфраструктуры интернета, но и программного обеспечения и контента. Так, например, важным элементом цифрового суверенитета, активно обсуждаемым в СМИ, является независимость в производстве чипов и микросхем, они также играют важное значение в создании и поддержании функциональности цифровой инфраструктуры. Более того, многие государства заявляют о том, что суверенизация не означает закрытости.

Первый параграф «Цифровой суверенитет в практике международных организаций» сосредоточен на исследовании международных площадок и организаций. ООН, как ведущая международная платформа, сталкивается с необходимостью сбалансировать суверенные интересы государств и потребность в универсальных правилах. Документы, разрабатываемые в рамках инициативы Глобального цифрового договора, отражают попытки объединить разрозненные подходы к управлению данными и технологиями. Однако внутренние противоречия между развитыми и развивающимися странами, особенно в части доступа к цифровым технологиям, ставят под сомнение возможность достижения полного консенсуса.

Второй параграф «Цифровой суверенитет в практике региональной интеграции: ЕврАзЭс, ЕС, АСЕАН, Меркосур» констатирует, что роль региональных объединений в продвижении цифрового суверенитета значительно возросла. БРИКС, объединяющий крупнейшие страны Глобального Юга, активно вырабатывает решения, направленные на снижение зависимости от транснациональных корпораций. Инициативы, такие как BRICS Pay, не только укрепляют финансовую независимость, но и формируют альтернативные подходы к управлению данными, противостоящие западным моделям. Вместе с тем у таких объединений остается проблема технологического отставания, что делает их усилия менее эффективными.

Европейский Союз демонстрирует системный и амбициозный подход к цифровому суверенитету. ЕС активно экспортирует свои ценности через разработку норм и стандартов, таких как GDPR или Закон об искусственном интеллекте. Тем не менее, даже такой продуманный механизм сталкивается с вызовами глобальной зависимости, особенно в производстве чипов и программного обеспечения. Несмотря на это, Евросоюз остается лидером в создании законодательных моделей, способных определять правила цифровой игры на мировой арене.

АСЕАН, напротив, сосредотачивается на преодолении цифрового разрыва, который особенно заметен в рамках этого региона. Быстрое развитие интернета и цифровой инфраструктуры стало важным шагом для повышения экономической активности и интеграции. Однако страны региона по-прежнему сталкиваются с вызовами, связанными с неравномерным распределением технологий и различиями в цифровой грамотности. Несмотря на это, опыт АСЕАН в цифровой трансформации может служить примером для других регионов с аналогичными проблемами.

Цифровая интеграция на пространстве ЕАЭС развивается медленнее, хотя ее потенциал остается значительным. Программы, такие как создание единой цифровой платформы и цифровая маркировка товаров, иллюстрируют стремление стран-членов снизить технологическую зависимость. Однако отсутствие унифицированных правовых подходов и различия в уровнях цифровизации остаются серьезными препятствиями. В этих условиях политика цифрового суверенитета приобретает характер долгосрочной стратегии, нацеленной на структурное развитие интеграционных процессов.

Третий параграф «Цифровой суверенитет ведущих государств» посвящен анализу опыта России, КНР и США. Показано, что цифровой суверенитет сегодня – это не только вопрос безопасности или экономической независимости, но и средство формирования новой архитектуры глобального управления. Сочетание национальных интересов с необходимостью международной координации становится ключевым вызовом, особенно в условиях усиливающейся геополитической конкуренции. В долгосрочной перспективе только через диалог и поиск гибких решений удастся избежать фрагментации мирового цифрового пространства и обеспечить его устойчивое развитие.

ЗАКЛЮЧЕНИЕ

В заключении диссертации сформулированы основные итоги проведенного исследования и представлены выводы, обобщающие результаты работы. Проведённое исследование показало, что цифровая трансформация фундаментально меняет природу государственного суверенитета, смещая акцент с территориального контроля на управление данными, цифровыми ресурсами и критической инфраструктурой. Сравнительный анализ опыта ведущих стран подтвердил асинхронность и многоуровневость процессов цифровой

суверенизации, где ослабление вестфальских аспектов сопровождается усилением внутреннего суверенитета и суверенитета взаимозависимости. Исследование внесло вклад в развитие теории международных отношений, предложив концептуализацию цифровых границ и систематизацию нормативной конкуренции, а также сформулировав прикладные рекомендации для укрепления политики России в сфере цифрового суверенитета.

Цифровая трансформация не только расширяет инструментарий государств, но и изменяет фундаментальные параметры международной политики. Государственный суверенитет перестаёт быть исключительно территориальным феноменом и приобретает многослойный, функциональный характер, основанный на способности контролировать цифровые инфраструктуры, данные и технологические платформы.

Проведённый сравнительный анализ политик ЕС, США, Китая, России, стран Юго-Восточной Азии и интеграционных объединений выявил, что цифровой суверенитет формируется как результат взаимодействия внутренних стратегических приоритетов и внешних ограничений глобального цифрового порядка. При всём многообразии подходов прослеживается общая тенденция к секьюритизации цифровой сферы, росту внимания к технологической зависимости и стремлению к автономии в ключевых сегментах цифровой экономики. Одновременно фиксируется расширение пространства нормативной конкуренции, где государства используют право, стандарты и цифровые режимы для распространения собственного влияния за пределы национальных границ. В результате цифровое пространство всё более структурируется как политическое поле, в котором сталкиваются разные модели развития и ценностные ориентиры.

На основе полученных результатов формулируются выводы о необходимости выработки сбалансированной международной архитектуры цифровой безопасности, способной сочетать признание государственного суверенитета с поддержанием глобальной взаимосвязанности. Для России цифровой суверенитет становится не только элементом национальной безопасности, но и ресурсом укрепления международных позиций в условиях технологической конкуренции и санкционного давления. Дальнейшее развитие политики цифрового суверенитета требует комплексного подхода, включающего развитие собственных технологий, активное участие в выработке международных норм и расширение сотрудничества с государствами, заинтересованными в

формировании более справедливого и многополярного цифрового порядка.

III.СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ АВТОРОМ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в рецензируемых научных изданиях, рекомендованных перечнем ВАК РФ, и в изданиях из перечня, рекомендованного Аттестационной комиссией РУДН:

1.Шитьков С.В. Подходы к изучению цифрового суверенитета в современной политической науке / С.В. Шитьков // Международная жизнь. 2025. № 5. С. 90-99. EDN EGLHNH.

1. Шитьков С.В. Цифровые технологии в практике публичной дипломатии: потенциал метавселенных в музейной дипломатии / С.В. Шитьков // Вопросы национальных и федеративных отношений. 2025. Т. 15, № 2(119). С. 286-293. DOI 10.35775/PSI.2025.119.2.010. EDN TRNKKD.

2. Шитьков С.В. Искусственный интеллект и большие данные в цифровых международных отношениях / С.В. Шитьков // Проблемы постсоветского пространства. 2025. Т. 12, № 2. С. 102-113. DOI 10.24975/2313-8920-2025-12-2-102-113.

3. Шитьков С.В. Практический поворот в теории международных отношений и цифровой суверенитет России / С.В. Шитьков // Вопросы национальных и федеративных отношений. 2025. Т. 15, № 8(125). С. 1898-1905. – DOI 10.35775/PSI.2025.125.8.016.

4. Шитьков С.В. Концептуальные основания анализа государственного суверенитета в цифровую эпоху / С.В. Шитьков // Вестник Дипломатической академии МИД России. Россия и мир. 2025. № 2(44). С. 6-21. EDN LVHNKW.

5. Шитьков С.В. Мирopolитическая концептуализация современной цифровой революции / С.В. Шитьков // Обозреватель. 2025. № 4(411). С. 6-18. DOI 10.48137/2074-2975_2025_4_6.

6. Шитьков С.В. Цифровой суверенитет в повестке ШОС и БРИКС / С.В. Шитьков // Социально-гуманитарные знания. 2025. № 6. С. 343-347. EDN VYQEXQ.

7. Шитьков С.В. Суверенитет данных и инфраструктурная сила: российский подход в сравнительной перспективе / С.В. Шитьков // Вопросы

политологии. 2025. Т. 15, № 8(120). С. 3262-3269. DOI 10.35775/PSI.2025.120.8.017.

8. Шитьков С.В. Развитие цифрового суверенитета в рамках Евразийского экономического союза: стратегические приоритеты и институциональные механизмы / С.В. Шитьков // Евразийский Союз: вопросы международных отношений. 2025. Т. 14, № 5(70). С. 1318-1325. DOI 10.35775/PSI.2025.70.5.012.

9. Шитьков С.В. Цифровой суверенитет «мирового большинства»: практики, нормы и коалиции нового типа / С.В. Шитьков // Социально-гуманитарные знания. 2025. № 8. С. 386-390. EDN EBOFYY.

10. Шитьков С.В. Цифровой суверенитет Африки: региональное и страновое измерение / С.В. Шитьков // Вопросы политологии. 2025. № 7(119). С. 2444-2451. DOI 10.35775/PSI.2025.119.7.038.

11. Шитьков С.В. Суверенитет данных и инфраструктурная сила: российский подход в сравнительной перспективе / С.В. Шитьков // Евразийский союз: вопросы международных отношений. 2025. № 7(72) С. 1779-1789. DOI: DOI 10.35775/PSI.2025.72.7.008.

12. Шитьков С.В. Формирование международного режима в области информационной безопасности / С.В. Шитьков, Т.А. Полякова, А.А. Смирнов // Вестник МГИМО-Университета. 2025. Т. 18, № 5. С. 79-99. DOI 10.24833/2071-8160-2022-olf6.

13. Шитьков С.В. БРИКС на пути обретения цифрового суверенитета? / Е.С. Зиновьева, С.В. Шитьков // Проблемы национальной стратегии. 2024. № 2 (83). С. 144-163. DOI 10.52311/2079-3359_2024_2_144. – EDN PPEDMU.

14. Шитьков С.В. Цифровой суверенитет в практике международных отношений / Е.С. Зиновьева, С.В. Шитьков // Международная жизнь. 2023. № 3. С. 38-51. EDN HBTQYT.

Монографии:

1. Шитьков С.В. Цифровой поворот в международных отношениях : как новые технологии меняют мировую политику и науку о ней / М.А. Сучков, К.В. Воронцов, Н.Ю. Силаев [и др.]. М.: Московский государственный институт международных отношений (университет), 2023. 232 с. ISBN 978-5-9228-2808-6. – EDN IZLQNM.

2. Shitkov S.V. Sovereignty as Practice in Digital Age / E.S. Zinovieva, S.V. Shitkov // Digital International Relations. Singapore : Palgrave Macmillan, 2023. P. 75-90. – DOI 10.1007/978-981-99-3467-6_5. – EDN SNVHEF.
3. Шитков С.В. Аннексия. Попытка историко-правового анализа / С.В. Шитков. Тамбов : ТГУ им. Г.Р. Державина, 2016. 104 с. ISBN 978-5-00078-081-7. – EDN DGQOAG.
4. Shitkov S.V. Navigating the nexus of international order and artificial intelligence regulation: Divergent approaches and global governance implications / Zinovieva E.S., Shitkov S.V. // Digital Transformation in Artificial Systems / Ed. by M. Farina, P. Ciancarini, X.Yu, J. Chen. Elseveir, 2026. P. 78 – 116.

Шитков Сергей Владимирович
(Российская Федерация)
«Государственный суверенитет в условиях цифровизации»

Диссертация посвящена комплексному анализу феномена государственного суверенитета в условиях глобальной цифровой трансформации и выявлению проблем, связанных с обеспечением цифрового суверенитета, а также осмыслению их в теоретической и практической перспективе.

Предложено впервые в российской политической науке рассматривать «цифровые границы» как институционально-нормативные и технологические механизмы, посредством которых государство обеспечивает контроль и регулирование потоков данных, платформенной экономики и критической цифровой инфраструктуры.

Доказано, что доступ к передовым технологиям искусственного интеллекта и большим данным укрепляет влияние этих стран, в то время как другие государства вынуждены адаптироваться к внешним стандартам, что подрывает их суверенитет.

Полученные основные теоретические и практические результаты могут быть использованы как для академического сообщества, так и для разработчиков национальных и международных стратегий в области цифрового управления и безопасности.

Shitkov Sergey Vladimirovich
(Russian Federation)
“State Sovereignty in the Context of Digitalization”

The dissertation is devoted to a comprehensive analysis of the phenomenon of state sovereignty in the context of global digital transformation and the identification of problems associated with ensuring digital sovereignty, as well as understanding them in theoretical and practical perspectives.

It is proposed for the first time in Russian political science to consider “digital borders” as institutional, normative and technological mechanisms through which the state ensures control and regulation of data flows, platform economy and critical digital infrastructure.

It is proven that access to advanced artificial intelligence technologies and big data strengthens the influence of these countries, while other states are forced to adapt to external standards, which undermines their sovereignty.

The main theoretical and practical results obtained can be used both for the academic community and for developers of national and international strategies in the field of digital governance and security.