ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ
МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ (УНИВЕРСИТЕТ)
МИНИСТЕРСТВА ИНОСТРАННЫХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

На правах рукописи

ШИТЬКОВ Сергей Владимирович

ГОСУДАРСТВЕННЫЙ СУВЕРЕНИТЕТ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Специальность 5.5.4. Международные отношения, глобальные и региональные исследования

Диссертация на соискание ученой степени
доктора политических наук

Научный консультант:

доктор политических наук, профессор
Зиновьева Елена Сергеевна

Москва 2026

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

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 ИКТ. Несмотря на то, что данная категория стала популярной как в централизованных / авторитарных, так и в демократических странах, сама концепция «цифрового суверенитета» остается весьма спорной и пока не получила комплексного и всестороннего освещения в научной литературе. Вышеизложенное обуславливает *научную актуальность* данной тематики.

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

Внимание к проблемам обеспечения цифрового суверенитета возрастает не только на уровне научной литературы, аналитических докладов ведущих фабрик мысли[2], но и на уровне политических решений в различных странах мира. В 2020 году Германия в рамках своего председательства в Совете Европы провозгласила обеспечение «цифрового суверенитета» приоритетом цифровой повестки дня ЕС[3].

России к данной проблеме обращаются на уровне политических решений начиная со второй половины 2010х годов – так, в таких документах стратегического планирования, как Доктрина информационной безопасности от 2016 года[4] и Основы государственной политики в области международной информационной безопасности[5] 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 сообщества. Растущее политическое внимание к проблематике «цифрового суверенитета» в условиях отсутствия академической базы в данной области данной обуславливает *прикладную актуальность* выбранной темы исследования.

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

---

[2] См. напр.: Realpolitik в «цифре»: суверенитет, союзы и неприсоединение XXI века. Безруков А., Мамонов М., Ребро О., Сушенцов А. / Доклад клуба «Валдай». URL: https://ru.valdaiclub.com/a/reports/realpolitik-v-tsifre-suverenitet-soyuzy/

[3] https://www.eu2020.de/eu2020-en/eu-digitalisation-technology-sovereignty/2352828

[4] Доктрина информационной безопасности Российской Федерации. Утв. Указом Президента России 2016.

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

условием общей стратегической автономии государства. Эти официальные позиции формируют современный политический контекст исследования и требуют включения в научный анализ.

Понятие цифрового суверенитета тесно связано с более широким контекстом глобальной цифровой трансформации, которая затрагивает все аспекты жизни современного общества и мировой политики – социокультурные, 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 бизнеса[6], 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 аналогов[7]. Аналогичные тенденции наблюдаются в России, где с 2019 года проводится политика по развитию автономного сегмента интернета[8], а также в ЕС, где принятие General Data Protection Regulation

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

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

[8] 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

(GDPR)[9] стало шагом к усилению контроля над персональными данными граждан. Важной составляющей стало также принятие в ЕС Artificial Intelligence Act 2025, который закрепил стремление к стратегической автономии в сфере искусственного интеллекта[10].

При этом концепция цифрового суверенитета не сводится исключительно к вопросам кибербезопасности 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 автономии. В России проводится политика технологического суверенитета, которая включает в себя создание реестра отечественного программного обеспечения, политику импортозамещения в ИТ и электронике, контроль цифровой инфраструктуры, развитие национальных технологических разработок, в том числе в сфере искусственного интеллекта[11].

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

---

[9] 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

[10] Artificial Intelligence Act (Regulation (EU) 2024/1689), Official Journal version of 13 June 2024'. Interinstitutional File: 2021/0106(COD)

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

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.[12] или российские законы о «о фейках»[13], отражают политику по установлению контроля над цифровым пространством.

Вопросы цифрового суверенитета также тесно переплетаются с международным правом. Отсутствие универсальных норм, регулирующих киберпространство, приводит к конфликтам юрисдикций. Например, применение американского CLOUD Act, позволяющего властям США получать данные[14], хранящиеся на серверах за пределами страны, противоречит принципам GDPR[15] 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 фактором, усложняющим международное сотрудничество. 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

---

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

[13] 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

[14] Clarifying Lawful Overseas Use of Data (CLOUD) Act. US Department of Justice. Crimonal Division. 2018. URL: https://www.justice.gov/criminal/media/999391/dl?inline (дата обращения 27.11.2025)

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

научной литературе, что обуславливает *научную актуальность* темы диссертации.

Степень научной разработанности проблемы.

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. Кокошин[16], М.М. Лебедева[17], А.А. Сергунин[18], Ст. Краснер[19], Д. Лейк[20], А. Осиандер[21], и другие ученые. Особый акцент необходимо сделать на исследованиях С. Краснера, которые внесли фундаментальный вклад в концептуализацию суверенитета, предложив 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 принципа[22]. 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. Рогожина[23]. Прикладной анализ государственной состоятельности как опыта количественного анализа практики

[16] Кокошин А. А. Реальный суверенитет в современной мирополитической системе. – Европа, 2006.
[17] Лебедева М. М. Мировая политика //М.: Аспект пресс. – 2007.
[18] Сергунин А. А. Суверенитет: эволюция концепта //Политическая экспертиза: ПОЛИТЭКС. – 2010. – Т. 6. – №. 4.
[19] Krasner S. D. Sovereignty. – Princeton University Press, 1999.
[20] Lake D. A. The new sovereignty in international relations //International studies review. – 2003. – Т. 5. – №. 3. – С. 303-323.
[21] Osiander A. Sovereignty, international relations, and the Westphalian myth //International organization. – 2001. – Т. 55. – №. 2. – С. 251-287.
[22] Krasner S. D. Sovereignty: organized hypocrisy. – Princeton university press, 1999.
[23] 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.

государственного суверенитета в международной политике можно провести на основании проекта коллектива авторов МГИМО «Политический атлас современности»[24], а также проекта Консорциума МГИМО и ВШЭ: «Политический атлас современного мира 2.0»[25] под руководством Мельвиля А.Ю. Кроме того, нельзя не отметить концепцию инфраструктурной власти социолога М. Манна под которой понимается институциональная возможность государства реализовывать свои решения в пределах государственных границ[26]. 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 суверенитета подвергаются трансформации.

Вместе с тем, в современной научной изучение темы «цифрового суверенитета» носит фрагментарный характер и комплексных исследований, посвященных трансформации суверенитета и проблемам его обеспечения в условиях цифровой трансформации современной мировой политике автору найти не удалось. 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-

---

[24] 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 (дата обращения 27.11.2025)

[25] https://social.hse.ru/politatlas/ (дата обращения 27.11.2025)

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

технологий способствовало размыванию государственного суверенитета и снижению влияния государств[27]. Так, в этот период был опубликован целый ряд работ, посвященных вопросам размывания государственного суверенитета под воздействием информационной революции, в том числе российских авторов А.Н. Михеева[28], Д.Н. Пескова[29], а также зарубежных исследователей, таких как Д. МакЛин, В. Кляйнвахтер[30], Д. Най и Р. Кохейн[31], Д. Розенау[32] 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. Стрельцов[33] и М.М. Кучерявый[34], Е.С. Зиновьева[35] занимались международно-правовыми аспектами данной проблематики. Среди зарубежных авторов следует отметить М.Мюллера[36], Д. Поул и Т. Тьель[37], которые исследовали трансформацию суверенитета в демократических странах под

---

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

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

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

[30] 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

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

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

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

[34] Кучерявый М. М. Государственная политика информационного суверенитета России в условиях современного глобального мира //Управленческое консультирование. – 2014. – №. 9 (69).

[35] 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.

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

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

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. Плотникова[38], С.В. Шкодникого и А.М. Кушнира, Продченко И.А.[39], А.А. Афанасьева[40] 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. Шифедекхера[41], Ф. Креспи, С. Каравелла[42], Д. Элдера, К. Блайнда[43] и др. В последние годы также публикуются труды исследователей из КНР, Индии, Бразилии, посвященные данной проблематике[44].

Важный вклад в работу над диссертацией внесли труды, посвященные экономическим аспектам цифрового суверенитета, в частности, работы Ш. Зубофф[45], которые раскрыли механизмы подрыва

---

[38] 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.

[39] 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.

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

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

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

[43] 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.

[44] 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.

[45] 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.

государственного суверенитета транснациональными цифровыми корпорациями через присвоение и монетизацию данных, что стимулировало развитие регуляторных мер (в частности, локализацию данных) как инструментов защиты цифрового суверенитета. Её анализ показал, что доминирование цифровых платформ и ИТ гигантов 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»[46], 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»[47].

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»[48], в которой концептуализированы основные направления влияния новых технологий на мировую экономику и мировую политику. В 2025 году ЮНКТАД опубликовал доклад о технологиях и инновациях, в котором обозначил современные тенденции как начало 5 промышленной революции, основанной на нейроморфных системах и прямом человеко-компьютерном взаимодействии[49]. Другие зарубежные исследователи, занимающиеся данной темой, включают в себя Н. Негропонте[50], Э. Бруссо, Н. Кюри[51] и др. Кроме того, необходимо

[46] Wu T. The curse of bigness. – Penguin Random House, 2018.
[47] Варуфакис Я. Технофеодализм. М.: Ad Marginem, 2025.
[48] Клаус Ш. Четвертая промышленная революция. – Litres, 2016.
[49] Technology and innovation report. UNCTAD, 2025. URL: https://unctad.org/system/files/official-document/tir2025_en.pdf (дата обращения 27.11.2025)
[50] Negroponte N. Being digital. – Vintage, 2015.
[51] Brousseau E., Curien N. (ed.). Internet and digital economics: principles, methods and applications. – Cambridge University Press, 2007.

отметить работы российских авторов в области цифровизации мировой экономики, в том числе работы И.В. Сударушкиной, Н.А. Стефановой[52], О.Б. Пичкова и А.А. Уланова[53], Н.М. Борисова[54], З.М. Алиевой, М.М. Магомадовой, И.С. Разиной[55], а также экспертные доклады профильных структур по данной проблематике, в том числе экспертов АНО Цифровая экономика[56] и др.

Правовое измерение цифровой трансформации практики государственного суверенитета представлено в трудах юристов-международников Э.Л. Сидоренко[57], Т.А. Поляковой, А.А. Смирнова[58],

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

[53] 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.

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

[55] Алиева З. М., Магомадова М. М., Разина И. С. Цифровая трансформация и цифровая экономика: исследование основных технологий и их характеристик //Региональные проблемы преобразования экономики. – 2024. – №. 5. – С. 151-158.

[56] Белая книга цифровой экономики 2023 // АНО Цифровая экономика. 2024. URL: https://files.data-economy.ru/Docs/White_paper_2023_.pdf (дата обращения 27.11.2025) : Будущее искусственного интеллекта 2025 // АНО Цифровая экономика 2025. URL: https://files.data-economy.ru/Docs/AI_Future_2025.pdf (дата обращения 27.11.2025)

[57] 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.

[58] 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.

А.В. Минбалеева[59], А.А. Ефремова[60], А.А. Стрельцова[61], К.К. Лазаря[62] и др. Отдельно следует выделить сборник «Цифровое право», в котором обозначены ключевые тенденции развития данной новой отрасли права[63]. Среди зарубежных авторов, занимающихся данной проблематикой необходимо отметить Л. Лессига[64], Э. Тикк[65], М. Кертуннен[66], Е. Попа-Тахе[67]. 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

[59] 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; Минбалеев А. В. и др. Методы и подходы к регулированию формирующейся отрасли квантовых коммуникаций в условиях современного информационного общества //Информационное общество. – 2024. – №. 4. – С. 112-120.

[60] 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, Ефремов А. А. Перспективы развития экспериментального правового регулирования в сфере цифровых и технологических инноваций //Вестник Университета имени ОЕ Кутафина. – 2024. – №. 10 (122). – С. 133-140.

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

[62] Лазарь К. К. Кибербезопасность и суверенитет в киберпространстве: вызовы и перспективы международного права //Московский журнал международного права. – 2025. – №. 1. – С. 125-137.

[63] Цифровое право / Под ред. Э.Л.Сидоренко. — Москва: Юрлитинформ, 2024. — 720 с.

[64] 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.

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

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

[67] Popa Tache C. E., Săraru C. S. Evaluating today’s multi-dependencies in digital transformation, corporate governance and public international law triad //Cogent Social Sciences. – 2024. – Т. 10. – №. 1. – С. 237-245. DOI: 10.1080/23311886.2024.2370945

руководство 2.0» под редакцией авторитетного юриста М. Шмидта[68]. Конструктивистская трактовка норм применительно к цифровой сфере, в том числе в контексте обеспечения цифрового суверенитета представлена в трудах М. Финнемор и Д. Холлиса[69], М. Брауна[70], Г. Робертса[71]. 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 цифрового суверенитета. Их результаты были использованы в ходе написания 3 главы настоящей диссертации. В частности, Л. Белли возглавляет проект КиберБРИКС (CyberBRICS)[72], а также публикует значительное число работ по цифровому суверенитету Бразилии и стран Латинской Америки[73]. Исследованиями цифрового суверенитета или стратегической автономии ЕС в области данных и цифровых технологий занимаются А.Н Толстухина[74], Е.С. Зиновьева и В.И. Булва[75], А.В. Алейников, Д.А.

[68] 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.

[69] 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? Accuzations and International Law in Global Cybersecurity.”. – 2018.

[70] Braun M., Hummel P. Is digital sovereignty normatively desirable? //Information, Communication & Society. – 2025. – Т. 28. – №. 10. – С. 1721-1734.

[71] Roberts H. Digital sovereignty and artificial intelligence: a normative approach //Ethics and Information Technology. – 2024. – Т. 26. – №. 4. – С. 70.

[72] www.cyberbrics.com (дата обращения 27.11.2025)

[73] 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.

[74] Толстухина А. Технологический суверенитет Европейского союза и его границы // Дискуссионный клуб Валдай. Аналитические записки.№ 19. Октябрь, 2022. URL: https://ru.valdaiclub.com/files/42559/ (дата обращения 27.11.2025)

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

Мальцева[76], С.В. Володенков[77], С.Н. Федорченко[78], А.А. Ватулина[79], а также европейские авторы Л. Флориди[80], Э. Селесте[81], Р. Белланова[82] 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. Кожухова[83], И. Денисова[84], авторитетного зарубежного исследователя Р. Кримерса[85], а также авторов из КНР, в том числе Д. Ли[86], И. Хун[87], М. Джианг[88] и др. Опыт Индии и стран «Глобального юга» в практике цифрового суверенитета рассмотрен в работе М. Ксианг[89]. 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

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

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

[78] 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.

[79] Ватулина А. А. Трансформация нормативной силы Европейского союза и построение цифрового суверенитета под влиянием новых вызовов //Международные отношения. – 2025. – №. 2. – С. 178-189.

[80] 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.

[81] 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.

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

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

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

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

[86] Lee J. The CPC and Sovereignty in a Digitally Connected World. 2020

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

[88] 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.

[89] 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.

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. Смирнов[90], А.А. Ефремов[91]), международной информационной безопасности (Е.С. Зиновьева[92], И.О. Яникеева[93], В.И. Булва[94]), информационного противоборства (М.В. Кучерявый[95]) или региональных аспектов информационной безопасности (А.В. Макарычева[96]). 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 единого комплексного всестороннего и систематического осмысления в научной литературе по международным отношениям и политическим наукам. Настоящий пробел призвано восполнить предлагаемое исследование.

Теоретическая и методологическая основы исследования.

В качестве теоретической базы исследования использовано конструктивистское направление в международных исследованиях,

---

[90] 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

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

[92] Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности: проблемы, субъекты, перспективы : дисс. … доктора полит. Наук // ЕС Зиновьева – Москва – 2019. 350 с.

[93] 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

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

[95] 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.

[96] 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

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, государств[97]. 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 исследований[98]. Данный подход позволяет рассмотреть 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. Пулио[99]. Практический

---

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

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

[99] 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.

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, будет в качестве теории среднего уровне будет использована концепция суверенитета С. Краснера[100]. 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 эпоху этот аспект подвергается наиболее серьезным вызовам, учитывая трансграничную природу киберпространства.

2. Суверенитет взаимозависимости (Interdependence sovereignty) - способность государства контролировать трансграничные потоки

[100] Krasner S. D. Sovereignty. – Princeton University Press, 1999.

(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 ведете 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 конкрентных 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.

Исследовательский вопрос: как эволюционирует суверенитет государств в цифровую эпоху, в том числе под влиянием секьюритизации глобального информационного пространства?

Цель исследования: определить основные проблемы обеспечения и направления эволюции цифрового суверенитета в мировой политике.

Для достижения цели исследования были поставлены и решены 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.

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.

Объект исследования: государственный суверенитет в современной мировой политике.

Предмет исследования: проблема обеспечения «цифрового суверенитета» государств в современной мировой политике.

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.

Эмпирической базой для исследования послужили российские концепции по вопросам внешней политики (Концепция внешней политики Российской Федерации от 2023 года)[101], доктрины и стратегии Российской Федерации (Доктрина информационной безопасности Российской Федерации в редакции от 2016 года[102], Военная доктрина Российской Федерации от 2014[103], Стратегия национальной безопасности Российской Федерации от 2021 года[104],), официальные документы зарубежных государств (КНР, США и др)[105], документы международных

---

[101] 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/ (дата обращения 27.11.2025)

[102] Доктрина информационной безопасности Российской Федерации. Утв. Президентом РФ 5.12.2016. URL: http://www.scrf.gov.ru/documents/6/5.html (дата обращения 27.11.2025)

[103] Военная доктрина Российской Федерации. Утв. Президентом 25 декабря 2014 г., № Пр-2976. URL: http://www.scrf.gov.ru/security/military/document129/ (дата обращения 27.11.2025)

[104] Стратегия национальной безопасности Российской Федерации. Утверждена указом Президента Российской Федерации 02.07.2021 № 400. URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения 27.11.2025)

[105] 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,

правительственных организаций и форумов (Резолюции Генеральной Ассамблеи ООН[106], соглашения, подписанные в рамках ШОС[107], ОДКБ[108], АСЕАН[109], Меркосур[110] итоговые декларации БРИКС[111], Группы двадцати[112] и Группы восьми[113]).

Научная новизна.

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 суверенитете;

- выявлены ключевые характеристики цифровых границ, отличающие их от классических территориальных границ: виртуальность,

---

2022. URL: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf (дата обращения 27.11.2025); 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 (дата обращения 27.11.2025)

[106] 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.

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

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

[109] 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.

[110] Declaración presidencial sobre la integración digital en el MERCOSUR, 2021. URL: https://www.mercosur.int/documento/declaracion-presidencial-sobre-la-integracion-digital-en-el-mercosur/ (дата обращения 27.11.2025)

[111] Казанская декларация БРИКС. Казань, 2024

[112] 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 (дата обращения 27.11.2025)

[113] Окинавская Хартия глобального информационного общества. -- Окинава, 2000.

URL: http://www.ifap.ru/ofdocs/okinhar.htm (дата обращения 27.11.2025); G8 Background paper: International action against Cybercrime. Evian, 2003.

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 ЕС, 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 ЕС, 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.

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 России в цифровую эпоху.

Положения, выносимые на защиту:

1. На основе анализа современной практики реализации суверенитета доказано, что цифровой суверенитет не сводится исключительно к территориально ориентированным классическим трактовкам, а представляет собой многоуровневый и полицентричный 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.

2. 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 в качестве специфического политического института, трансформирующего традиционные представления о границах государства и формах его взаимодействия с глобальной цифровой средой.

3. 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 переосмысления 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.

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 и закрепления данных подходов в нормах международного публичного права.

5. Технологическое доминирование передовых держав, таких как США и Китай, создаёт новые формы неравенства в международных отношениях. Приоритетный 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. 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, платформами, данными и инфраструктурой.

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 2026 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.

Теоретическая значимость предлагаемого исследования обусловлена малой изученностью выбранной темы в современной научной литературе, однако, изучение трансформации данной аналитической категории, 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 вакуум, 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.

Практическая значимость исследования состоит 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 осмысления практики реализация государственного суверенитета в цифровую эпоху, а также позволяет сформулировать рекомендации в

целях практического укрепления позиций России в глобальном информационном пространстве.

Апробация исследования осуществлялась в рамках выступления на ведущих российских, зарубежных и международных научных и научно-практических конференциях. Результаты исследования нашли отражение в экспертно-аналитической деятельности для МИД России, Министерства обороны и Генштаба Российской Федерации, других заинтересованных министерств и ведомств

Основные положения диссертационной работы отражены в следующих публикациях:

Статьи, опубликованные в изданиях, рекомендованных Высшей аттестационной комиссией Министерства образования и науки Российской Федерации и входящие в Перечень 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.
2. 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.
3. 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.
4. 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.
5. 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.

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

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

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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. Шитьков С.В. Аннексия. Попытка историко-правового анализа / С.В. Шитьков. 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.

А также в других изданиях, в том числе:

1. Цифровые международные отношения В двух томах. Учебное пособие для вузов / Торкунов А.В., Шерстюк В.П., Крутских А.В., Зиновьева Е.С., Шитьков С.В., Волкова С.Г., Зинченко А.В., Булва В.И.,

Цветкова Н.А., Сытник А.Н., Смирнов А.И., Сурма И.В., Исаева Т.В., Мирошников Б.Н., Чернухин Э.В., Стрельцов А.А., Пичков О.Б., Патрунина К.А., Салыгин В.И., Григорьев Д.И. и др. // Под ред. С.В. Шитькова, Е.С. Зиновьевой. М.: Аспект-Пресс, 2023.

2. Цифровая трансформация мировой экономики Учебное пособие для программ бакалавриата и магистратуры / Пичков О.Б., Шитьков С.В., Уланов А.А., Патрунина К.А. Москва: Аспект-Пресс, 2022.

Структура работы.

Во введении диссертации обоснована актуальность представленного исследования, осветить степень разработанности проблемы, теоретической и методологической основы работы, сформулировать цели и задачи исследования, а также положения, выносимые на защиту.

В первой главе «Теоретико-методологические основания анализа государственного суверенитета в современной политической науке» планируется провести анализ теоретических аспектов и концептуальных основ анализа суверенитета в современной международной политике

Во второй главе «Мирополитическая концептуализация современной цифровой революции» предполагается проанализировать основные направления современной цифровой революции в контексте их влияния на современную мировую политику и обеспечение суверенитета государств.

В третьей главе «Цифровой суверенитет в практике современных международных отношений: опыт ведущих стран и международных структур» особое внимание планируется уделить опыту обеспечения цифрового суверенитета ведущих государств мира, а также ЕС как интеграционной структуры, которая проводит консолидированную политику на данном направлении.

В заключении диссертации обобщены результаты проведенного исследования, сформулировать основные выводы и рекомендации.

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

1.1. Эволюция подходов к концептуализации понятия «государственный суверенитет» в политической мысли

Категория государственного суверенитета восходит к античности и Римской империи, в рамках которой были заложены основы государственного управления, впоследствии сыгравшие ключевую роль в формировании концепции суверенитета в современном понимании. Правовые и философские традиции Римской империи положили начало идеям о праве, государственности и власти, хотя сам термин «суверенитет» появился значительно позже[114]. В античное время прото-суверенитет проявлялся через независимость городов-государств (полисов), но прежде всего, через централизованную власть Римской империи, самостоятельное проведение внешней политики, а также через законодательную и судебную систему. Античные государства демонстрировали элементы верховной власти и независимости, которые являются основополагающими для современной концепции суверенитета.

Римская империя с ее сложной системой управления и права установила фундамент, на котором строились последующие концепции государственного устройства. Император Римской империи, воплощавший в себе высшую исполнительную, законодательную и судебную власть, стал прототипом суверена. Кодификация римского права, осуществленная при Юстиниане I, укрепила основы правовой системы, которая оказала

[114] Леонов А. С. Государственный суверенитет: этимология и предыстория развития концепта / А.С. Леонов – Текст : электронный //Вестник Нижегородского университета им. НИ Лобачевского. – 2013. – №. 3-2. – С. 131-135. – URL: https://cyberleninka.ru/article/n/gosudarstvennyy-suverenitet-etimologiya-i-predystoriya-razvitiya-kontsepta (дата обращения: 18.02.2024).

значительное влияние на развитие европейского права и понятий политической власти и государственного суверенитета[115].

Практика суверенитета продолжила эволюционировать в Средневековой Европе, отражая изменения в политическом ландшафте. В Средние века суверенитет был размыт между множеством феодальных владений и католической церковью. Феодальная система, характеризующаяся раздробленной властью и взаимными обязательствами между сеньорами и вассалами, представляла собой отход от централизованной власти Римской империи, но в то же время способствовала развитию идей о локальном самоуправлении и автономии. В Средние века в Европе католическая церковь была одной из самых могущественных институций. Её влияние проникало в политические, экономические и социальные аспекты жизни, что значительно ограничивало суверенитет светских правителей. Церковь обладала огромным духовным авторитетом, который часто использовала для вмешательства в светские дела, ставя под вопрос самостоятельность и независимость князей. Папа Римский, как глава католической церкви, обладал верховной духовной властью над всей христианской Европой, которая позволяла вмешиваться во внутренние дела княжеств. Папа мог отлучить правителя или наложить интердикт на целое государство, что означало приостановление церковных служб и таинств. Духовная монополия папской власти подрывала легитимность правителя и его контроль над подданными, заставляя его подчиняться воле церкви. Церковь владела обширными землями и имуществом, что делало её крупным экономическим игроком. У церкви также была собственная автономная судебная система. Власть католической церкви в Средневековой Европе существенно ограничивала суверенитет светских

[115] Суверенитет. Трансформация понятий и практик : монография / М.В. Ильин, И.В. Кудряшова, Я.И. Ваславский [и др.] ; под ред. М.В. Ильина, И. В. Кудряшовой. – Москва : МГИМО-Университет, 2008. – 24, 93 с. – ISBN: 978-5-9228-0362-5 – Текст : непосредственный.

правителей через духовное, экономическое, судебное и политическое влияние. Папство играло ключевую роль в европейской политике, используя свою духовную власть для вмешательства в дела государств, контролируя значительные экономические ресурсы, создавая параллельную судебную систему и формируя политические союзы. Соперничество светской и духовной властей порождало конфликтность, и вызывало недовольство как со стороны подданных, так и князей и духовенства.

Реформация в Европе позволила разрешить конфликт между интересами церкви, князей и подданых. Проповедник Мартин Лютер, выступая против папской власти и утверждая идею «Sola Scriptura» (только Писание), способствовал тому, что светские власти стали восприниматься как независимые от религиозной власти. Одним из основных принципов Лютера было утверждение, что каждый человек имеет право на личную веру и непосредственное отношение с Богом, без посредничества церкви. Это подрывало авторитет церкви и укрепляло идею государственной концепции суверенитета, в рамках которой государства могли действовать независимо от внешних религиозных авторитетов. Лютер настаивал на разделении сфер светской и духовной власти, что государственная власть должна быть автономной и не подчиненной религиозным авторитетам. Результатом стало формирование секулярного государства в Европе, где суверенитет определяется независимостью светской власти от религиозных институтов. Реформация, начатая Мартином Лютером, существенно ослабила власть католической церкви и привела к укреплению национальных государств. Важной предпосылкой для формирования концепции суверенитета стал Аугсбургский мир, подписанный в 1555 году. Установив принцип «Cuius regio, eius religio»[116] («чья власть, того и вера»), он позволял князьям государств в составе

[116] Чья страна, того и вера.

Священной Римской империи выбирать лютеранство или католицизм в подвластных им владениях. Этот принцип позволил каждому князю в Священной Римской империи определять религию своих подданных, что способствовало укреплению их политической независимости и суверенитета, ограничив возможности вмешательства со стороны Церкви во внутренние дела государств[117]. Подданным, не пожелавшим подчиниться выбору князя, предоставлялся льготный период, в течение которого они могли свободно эмигрировать в регионы, где была принята желаемая религия[118]. Это соглашение фактически положило конец религиозной борьбе в Европе и стало основой для последующего правового воплощения принципа государственного суверенитета в рамках Вестфальского мира 1648 года.

Признание Аугсбургским миром принципа соответствия религии вероисповеданию правителя, а также исключения и защита, которые он предусматривал для определенных групп населения, стали поворотным моментом в признании и практике суверенной власти в Священной Римской империи, создав прецедент для последующего развития государственного устройства в Европе. Созданная им система, основанная на принципе суверенитета территориальных правителей над религиозными вопросами в пределах их владений, в конце концов рухнула в начале XVII века, что способствовало началу Тридцатилетней войны.

Концептуальное оформление суверенитета в научном дискурсе начало складываться в то же время, различные теории власти и государственности начали обретать четкие очертания. Вестфальский мир 1648 года положил начало современной системе международных отношений, основанной на принципах государственного суверенитета и

---

[117] Беляев, М.П. Аугсбургский религиозный мир 1555 года как конституционный акт священной Римской империи / М.П. Беляев. – Текст : электронный // История и археология. – 2020. – № 3. – С. 83. – URL: https://cyberleninka.ru/article/n/augsburgskiy-religioznyy-mir-1555-goda-kak-konstitutsionnyy-akt-svyaschennoy-rimskoy-imperii (дата обращения: 24.03.2024).

[118] Чье царство, того и религия

невмешательства во внутренние дела других государств. Как отмечает М.М. Лебедева, «Подписание Вестфальского мира в 1648 г. стало важнейшей в историческом и политическом развитии вехой, ознаменовавшей собой формирование политической системы, которая в дальнейшем распространилась по всему миру. Политическая система получила название по месту заключения мира – Вестфальской, и/или по основному принципу, который был положен в основу мирных договоров – государственно- центристской, поскольку идея национального государства, обладающего суверенитетом, явилась ключевой. Это была величайшая социальная инновация, позволившая преодолеть многочисленные конфессиональные, территориальные, этнические и другие противоречия, раздиравшие Европу середины 17 в.»[119]. В правовом отношении национальный суверенитет действительно уровнял все страны, независимо от их различных характеристик - формы правления, размеров, военной и экономической мощи и т.д. - и дал возможность выстроить основы международного права. В политической науке сложился консенсус, согласно которому суверенитет стал играть определяющее значение в мировой политике после 1648 года, когда был подписан Вестфальский мирный договор, заложивший основы Вестфальской политической системы мира, которая сохраняет свое значение до сих пор. Суверенитет, понимаемый как полнота власти государства внутри границ и независимость на международной арене, стал важнейшим общим знаменателем, определяющим равенство государств в мировой политике и международном праве[120]. И хотя дискуссии о трансформации и размывании суверенитета были популярны в 1990-х и 2000-х годах[121], в настоящее время бесспорно, что суверенитет является важнейшим и

[119] Лебедева М.М. Политическая система мира: проявления «внесистемности»: или новые акторы – старые правила / М.М. Лебедева // «Приватизация» мировой политики локальные действия – глобальные результаты // Под ред. М.М.Лебедевой. – М.: Голден Би, 2008. – С. 53-66.
[120] Лебедева М. М. Политическая система мира: ее размывание и поиск решений //Современные глобальные проблемы мировой политики. – 2009. – С. 229-254.
[121] Krasner S. D. Power, the state, and sovereignty: essays on international relations. – Routledge, 2009.

неотъемлемым свойством государства как международного актора. Успешное решение сложной научной задачи определения природы и функций суверенитета в цифровую эпоху невозможно без обращения к истории концептуализации данной проблематики в научной мысли и практического воплощения данной категории.

Исследования суверенитета восходят к работе Ж.Бодена «Шесть книг о республике» 1576 года, где он определяет суверенитет как наивысшую, абсолютную власть над гражданами и подданными, которой обладает монарх как представитель Бога на Земле. Изначально категория государственного суверенитета была тесно связана с контролем над определенной территорией, расположенной внутри государственных границ. Важный вклад в становление теории суверенитета в политической и юридической науках внесли труды Гуго Гроция, Т.Гоббса, Дж.Локка.

Важно отметить, что суверенитет никогда не был статичной категорией, эволюционировал и включает в себя не только территориальный суверенитет, но и суверенитет в области территориальных вод, воздушного пространства государства, валютный суверенитет и ряд других компонентов.

Однако, изначально суверенитет в самом широком смысле рассматривался как исключительная прерогатива монарха, возможность контролировать территорию, расположенную внутри определенных границ и проживающее на этой территории население. Вестфальский мир установил принцип «государь император в своих владениях», согласно которому верховная власть принадлежит князю и, таким образом, заложил основы для системы баланса сил в Европе. При этом концептуально категория суверенитета также эволюционировала в классической политической мысли, отражая изменяющиеся реалии. В частности, можно выделить такие термины, как государственный суверенитет, народный суверенитет, национальный суверенитет. Вышеуказанные термины отражают разные подходы к источнику легитимности государственной

власти. Еще один термин – экстратерриториальный суверенитет, отражает возможности выведения суверенитета за пределы государственных границ в исключительных случаях.

Так, например, Гуго Гроций в классическом труде «О праве войны и мира» в 1550 г. пишет, что «общим носителем власти является государство», однако полагает, что у государства могут быть различные формы правления, отмечая при этом, божественную природу монархической власти. Кроме того, он выделяет несуверенные государства, то есть колонии, на которые фактически распространялся суверенитет монополий[122]. Он заложил, таким образом, основы категории экстратерриториального суверенитета.

Политическая концепция суверенитета, понимаемая как власть, которой обладает руководящий орган управлять государством, без какого-либо вмешательства со стороны внешних источников власти, происходит от латинского слова «superanus», что означает «над» или «высший». В то время как традиционная теория суверенитета, предложенная в шестнадцатом веке французским политическим философом Жаном Боденом, касалась полномочий правителя принимать окончательные решения, Жан-Жак Руссо изменил концепцию так, чтобы она сосредоточилась на народном суверенитете, а не на монархическом суверенитете; со временем он стал все больше ассоциироваться с демократией, верховенством закона и территориальностью[123]. Сегодня суверенитет всегда в первую очередь означает независимость государства по отношению к другим государствам (внешний суверенитет), а также его верховную власть над всеми полномочиями на территории государства (внутренний суверенитет). Боден в своем труде «Шесть книг о

[122] Г. Гроций. О праве войны и мира. Книга 1. Электронный ресурс. URL: http://www.civisbook.ru/files/File/Groziy.Kn1.pdf
[123] Putterman E. Rousseau, Law and the Sovereignty of the People. – Cambridge University Press, 2010.

Республике»[124] впервые систематически обосновал концепцию суверенитета как абсолютного, полного, неограниченного и бессрочного авторитета сюзерена над его подданными, основанного на естественном праве. Данное учение французский философ создал как реакцию на большое количество видов господств над человеком: религиозное – господство церкви, ленное – феодальное господство, господство сюзерена над феодами, сословное – одних групп людей над другими и т. д.[125] Сфера власти и подчинения не была урегулирована.

Боден выделял четыре основных неотъемлемых признака суверенной власти: постоянство, абсолютность, неделимость и верховенство закона[126]. Под постоянством подразумевался непрерывный характер власти, сохраняющийся даже при переходе от одного правителя к другому через законные механизмы наследования или решения, принятые самим сюзереном. Если правитель менялся часто и процесс передачи власти не был институциализирован, то страна теряла свой суверенитет. Абсолютистский характер демонстрировался через верховенство данной власти над другими видами власти и ее неограниченность никакими условиями. Неделимость означала невозможность разделения суверенной власти между разными лицами или группами, если только это решение не принято самим сюзереном. Если власть начинала делиться, то есть появлялся более чем один суверен, то уже существующий суверен терял свой полномочный статус, без суверена терялся суверенитет. Верховенство закона предполагало, что суверен обладает способностью создавать, изменять и отменять законы, а также

---

[124] Субочев, В. В. Исчезновение суверенитета: теоретический анализ политико-правовых реалий / В. В. Субочев. – Текст : электронный // Правовая политика и правовая жизнь. – 2016. – № 2. – С. 13-21. URL: https://mgimo.ru/upload/iblock/0c7/Subochev-dissolution-of-sovereignty.pdf?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (дата обращения: 24.03.2024).

[125] Суверенитет. Трансформация понятий и практик : монография / М.В. Ильин, И.В. Кудряшова, Я.И. Ваславский [и др.] ; под ред. М.В. Ильина, И. В. Кудряшовой. – Москва : МГИМО-Университет, 2008. – 44 с. – ISBN: 978-5-9228-0362-5 – Текст : непосредственный.

[126] Сергунин, А. А. Суверенитет: эволюция концепта / А. А. Сергунин. – Текст : электронный // Политическая экспертиза: ПОЛИТЭКС. – 2010. – № Том 6, №4. – С. 7-8. – URL: https://clck.ru/3ANWf8 (дата обращения: 01.04.2024).

требовать их неукоснительного соблюдения всеми субъектами в пределах государства.

Помимо того, Боден подчеркивал, что суверенитет не подразумевает произвольное или деспотическое правление: суверен должен действовать в интересах общественного блага и соблюдать определенные моральные и естественно-правовые ограничения[127]. Несмотря на эти ограничения, суверен обладает исключительной властью решать, что является общественным благом, и какие средства для его достижения наиболее подходящие[128].

Исключительный характер суверенитета обуславливает наличие целого комплекса иммунитетов в правовой, экономической, юридической сферах. Исторически они нашли воплощение в таких концептуальных формулировках, как par in parem non habet imperium – равный над равным не имеет власти, par in parem non habet jurisdictionem – равный над равным не имеет юрисдикции, par in parem non habet potestas – равный над равным не имеет полномочий[129].

Д. Боден рассматривал главу государства как наместника Бога на земле, поэтому суверенитет был обусловлен божественной природой государственной власти. Решающим средством развертывания суверенитета становилась компетенция принятия решений. Таким образом, можно согласится с тезисом, что само появление доктрины суверенитета ставило своей задачей легитимизировать монархическую власть[130].

---

[127] Никитина, В. С. Теория суверенитета Жана Бодена / В. С. Никитина, Е. А. Чудаева. – Текст : электронный // Вестник Самарской гуманитарной академии. – 2019. – № 1. – С. 129-133. – URL: https://cyberleninka.ru/article/n/teoriya-suvereniteta-zhana-bodena (дата обращения: 24.03.2024).

[128] Осветимская, И. И. Государственный суверенитет: содержание и преобразование в условиях глобализации / И. И. Осветимская. – Текст : электронный // Актуальные вопросы публичного права: конституционное право – 2017. – С. 150-167. – URL: https://publications.hse.ru/pubs/share/direct/225697087.pdf (дата обращения: 24.03.2024).

[129] Романовская В. Б., Пужаев В. В. Проблема государственного суверенитета и ее отражение в творчестве Леона Дюги и Раймона Карре де Мальберга //Журнал российского права. – 2016. – №. 2 (230). – С. 26-38.

[130] Романовская В. Б., Пужаев В. В. Проблема государственного суверенитета и ее отражение в творчестве Леона Дюги и Раймона Карре де Мальберга //Журнал российского права. – 2016. – №. 2 (230). – С. 26-38.

В свою очередь, английский философ Т. Гоббс в труде «Левиафан, Материя, форма и власть государства церковного и гражданского» от 1651 года, развил идею суверенитета как основы социального договора и гаранта мира и порядка в обществе и сформулировал ответ на вопрос об источнике суверенитета. Теория государственного суверенитета Томаса Гоббса подразумевает, что в его «естественном состоянии» человек обладает агрессивностью, характерной для «войны всех против каждого». Переход человека в «общественное состояние» сопровождается заключением «общественного договора», который предполагает наличие механизма для гарантированного выполнения его положений и наказания нарушителей. Этот механизм должен быть реализован всеми членами общества через передачу своих полномочий суверену, который в свою очередь станет гарантом соблюдения положений договора[131]. На теоретические воззрения Гоббса серьезное влияние оказали исторические события, а именно Славная революция в Великобритании.

Гоббс утверждает, что форма правления, установленная посредством общественного договора, не может быть изменена подданными: люди, передавшие свою суверенность правителю, не могут передавать свои полномочия другому правителю. Источником суверенной власти является общественный договор, но само общество не является носителем суверенитета[132]. Носителем суверенитета является монарх.

Тем не менее, Гоббс указывает на ограниченность власти суверена. Так как его власть не распространяется за пределы его государства, он не может командовать другими странами или контролировать своих граждан в плену у иностранцев. В международных отношениях суверены находятся в состоянии «войны всех против каждого», поскольку не существует

---

[131] Гоббс, Т. Левиафан, или материя, форма и власть государства церковного и гражданского / Т. Гоббс. – Текст : электронный // Электронная библиотека. Гражданское общество в России : [сайт]. – С. 132-134. – URL: https://www.civisbook.ru/files/File/Gobbs_Leviafan.pdf (дата обращения: 01.04.2024).

[132] Суверенитет. Трансформация понятий и практик : монография / М.В. Ильин, И.В. Кудряшова, Я.И. Ваславский [и др.] ; под ред. М.В. Ильина, И. В. Кудряшовой. – Москва : МГИМО-Университет, 2008. – 44-45 с. – ISBN: 978-5-9228-0362-5 – Текст : непосредственный.

межгосударственного общественного договора. Кроме того, даже внутри страны действия суверена ограничены законами и конституцией, его задача – обеспечить мир и благосостояние. Наконец, при ограничении публичной свободы, граждане могут наслаждаться личной свободой в сфере предпринимательства, верований и личной жизни. Гоббс также подчеркивает, что поддержка частной собственности и развитие экономики являются ключевыми обязанностями суверена[133].

Параллельно с теоретическими осмыслениями суверенитета происходило постепенное воплощение концепции в реальной политической жизни: в 1648 году был заключен Вестфальский мир, который существенно повлиял на развитие суверенитета, закрепив принципы территориальности и невмешательства во внутренние дела других государств. Эта серия договоров, подписанных в вестфальских городах Мюнстер и Оснабрюк, положили начало государственной системе, лежащей в основе современных международных отношений, и ввели концепцию Вестфальского суверенитета. Этот принцип предполагает, что каждое национальное государство обладает суверенитетом над своей территорией и внутренними делами, исключая влияние внешних сил, и основывается на идее невмешательства во внутренние дела другой страны[134]. Кроме того, в нем подчеркивается, что каждое государство, независимо от его размера, равноправно в международном праве[135]. То есть западноевропейские государства признавались единицами, главенствующими на определенной территории

---

[133] Сергунин, А. А. Суверенитет: эволюция концепта / А. А. Сергунин. – Текст : электронный // Политическая экспертиза: ПОЛИТЭКС. – 2010. – № Том 6, №4. – С. 9. – URL: https://clck.ru/3ANWf8 (дата обращения: 01.04.2024).

[134] Куприянов А.В. “Вестфальский миф” и “вестфальский” суверенитет / А.В. Куприянов – Текст : электронный //Анализ и прогноз. Журнал ИМЭМО РАН. – 2019. – №. 4. – С. 11-23. – URL: https://cyberleninka.ru/article/n/vestfalskiy-mif-i-vestfalskiy-suverenitet (дата обращения: 01.04.2024).

[135] Евстафьев Д.Г. Поствестфальский суверенитет в постглобальном мире / Д. Г. Евстафьев, Н. М. Межевич. – Текст : электронный // Политическая наука. – 2022. – № 4. – С. 122. – URL: https://clck.ru/3ANWxh (дата обращения: 01.04.2024).

в политическом, экономическом и социальном плане, и, что еще более важно, они сами определили данный статус для себя[136].

В Новое время мир вновь обратился к идеям демократии, истоки которых можно найти в трудах античности, а Джон Локк и Жан-Жак Руссо заложили основы идеи народного суверенитета, предложив концепцию, отличавшуюся от абсолютной монархической суверенности. Возникновение и становление государственного суверенитета связано с эволюцией взглядов на природу государственной власти и постепенным признанием неотъемлемых политических прав и свобод народа[137].

Джон Локк отверг господствовавшие до него теории божественного права монархической власти и абсолютного суверенитета монарха и ввел концепцию народного суверенитета. В «Двух трактатах о правлении» он утверждал, что законная власть правителей проистекает из согласия управляемых. Народ соглашается на создание общества и правительства, чтобы защитить свои естественные права, включая право на жизнь, свободу и собственность. Если правительство не защищает эти права или нарушает их, народ имеет право сменить или свергнуть правительство[138]. Таким образом, по мнению Локка, суверенитет основан на договоре между правителями и управляемыми, а правительство можно рассматривать как условно выполняющее свои обязательства перед гражданами.

Концепция Жан-Жака Руссо, в свою очередь, рассматривала суверенитет как выражение общей воли народа, отличной от воли всех индивидов в обществе. Данная категория является основополагающей для

---

[136] Бусыгина И.М. Европейский Союз: новые измерения концепции суверенитета/ И.М. Бусыгина – Текст : электронный // Политическая наука. Россия, Москва: Федеральное государственное бюджетное учреждение науки «Институт научной информации по общественным наукам Российской академии наук». – 2005. – № 4. – 47–69 с. – URL: https://clck.ru/3ANX2E (дата обращения: 01.04.2024).

[137] Язов А.Н. Источники формирования идеи народного суверенитета в либеральной правовой мысли России второй половины XIX-начала XX века / А.Н. Язов – Текст : электронный //Философия права. – 2017. – №. 1 (80). – С. 38-44.– URL: https://cyberleninka.ru/article/n/istochniki-formirovaniya-idei-narodnogo-suvereniteta-v-liberalnoy-pravovoy-mysli-rossii-vtoroy-poloviny-xix-nachala-xx-veka (дата обращения: 01.04.2024).

[138] Жан-Жак Руссо и Джон Локк: некоторые идеи о суверенитете и естественном праве / С. П. Сальников, О. А. Клименко, Р. К. Мирзоев, и. Л. Третьяков. – текст : электронный // юридическая наука: история и современность. – 2016. – № 5. – С. 174. – URL: https://clck.ru/3ANX3y (дата обращения: 01.04.2024).

понимания политической философии Руссо и описана в его работе «Об общественном договоре». По мнению философа, суверенитет должен принадлежать не монарху, а народу, что означает выражение и реализацию его интересов. Эта идея была связана с демократическим правлением и легла в основу французской Декларации прав человека и гражданина 1789 года и Конституции Французской Республики 1791 года.

Концепция народного суверенитета доминировала в XIX веке. Однако мыслители, такие как Гегель, ставили под сомнение практическую реализацию этой модели. Подобные дискуссии подготовили почву для интеграции идеи народного суверенитета во все формы правления, не только в республики, но и в монархии[139].

Помимо этого, возникла проблема определения соотношения между суверенитетом и принципом разделения властей. Отвечая на этот вызов, представители немецкой школы права утверждали, что народный суверенитет не подразумевает суверенитета управляемых над управляющими, поскольку обе группы являются частью общей воли. Таким образом, народ является источником власти, но не обязательно источником административного контроля.

Эпоха национализма и демократических революций способствовала утверждению идей национального суверенитета. Великая французская революция (1789-1799) и американская революция были яркими примерами борьбы за суверенитет народа (1775-1783). Декларация прав человека и гражданина провозгласила идеи народного суверенитета и равенства перед законом. Принцип народного суверенитета был закреплён в Конституции США, установив республиканскую форму правления.

В начале XX века немецкий философ Макс Вебер, выражая принципы бюрократической организации государственной власти, в

---

[139] Суверенитет. Трансформация понятий и практик : монография / М.В. Ильин, И.В. Кудряшова, Я.И. Ваславский [и др.] ; под ред. М.В. Ильина, И. В. Кудряшовой. – Москва : МГИМО-Университет, 2008. – 46 с. – ISBN: 978-5-9228-0362-5 – Текст : непосредственный.

работе «Политика как призвание и профессия» определил государственную власть через присущую исключительно ей монополию на легитимное насилие[140]. Подобный подход вдохновил Карла Шмитта на формулирование децизионистской теории суверенитета. Согласно этой теории, суверенитет определяется как способность принимать решения в исключительных обстоятельствах, что включает в себя право нарушать существующий правовой порядок. Шмитт подчеркивал, что исключения из правил подтверждают суверенитет, а способность государства действовать вопреки собственным законам в критических ситуациях является неотъемлемой чертой его власти и гарантом безопасности в кризисной ситуации[141]

Точка зрения Шмитта была подвергнута критике французским исследователем, теоретиком права Леоном Дюги. В своих работах он выступал за понятие ограниченного суверенитета, адаптированного к реалиям международного взаимодействия и внутренних демократических процессов[142]. Дюги провозглашал идею всеобщего верховенства права как как норму социальной солидарности. Полемизируя с концепцией народного суверенитета и общественного договора, ученый делал особый акцент на роли государственного суверенитета в сфере международных отношений и международного права, утверждая, что в этой сфере суверенитет имеет четко определенное значение[143].

Теоретическая конструкция народного суверенитета развивалась и логическим следствием стала теория о самоопределении народов: если вся власть в государстве принадлежит народу, то это также означает, что если какая-либо группа, объединившаяся на какой-либо территории, признает

---

[140] Дюги Л. Конституционное право. Общая теория государства. М., 1908. С. 393 – 424.

[141] Гройсберг, А. И. Современные подходы к определению понятия «суверенитет» / А. И. Гройсберг. – Текст : непосредственный // Современное состояние российского законодательства: проблемы и пути совершенствования. – 2009. – № 1. – С. 20.

[142] Федерализм. Энциклопедия. / Отв. ред. Гаджиев К.С. – М.: Издательство Московского университета, 2000. – 531-532 с. – Текст : непосредственный.

[143] Романовская В. Б., Пужаев В. В. Проблема государственного суверенитета и ее отражение в творчестве Леона Дюги и Раймона Карре де Мальберга //Журнал российского права. – 2016. – №. 2 (230). – С. 26-38.

себя народом, то она также имеет право создать на этой территории независимое суверенное государство. Ранее, Гуго Гроций, будучи сторонником монархической формы правления, прямо отрицал такую возможность, полагая, что некоторые государства несуверенны, состоят в полном обладании, то есть с возможностью их отчуждения[144]. Однако, данный тезис был оспорен сторонникам народного суверенитета. Другими словами, каждый народ имеет право определять не только правительство, которым он хочет управлять, но и государство, к которому он хочет присоединиться.

Влияние этой идеи особенно выросло после русской революции 1917 года и трудов Ленина[145]. В работе «Государство и революция» Ленин критиковал концепцию ‘народного суверенитета’ как буржуазную фикцию, противопоставляя ей принцип диктатуры пролетариата. Он не развивал теорию суверенитета как политико-правовой категории в современном понимании, а подчинял её своей теории классовой борьбы. В свою очередь, последующее развитие международного права и создание Лиги Наций в 1919 году подчеркнули необходимость сотрудничества государств и признания определенных ограничений суверенных прав в интересах международного мира и безопасности[146].

После двух мировых войн суверенитет стал центральным принципом в международных отношениях. Создание ООН закрепило право народов на самоопределение и уважение суверенитета государств. Все эти процессы и концептуальные образования в совокупности привели к следующему важному этапу в практическом развитии суверенитета - включению права народов на самоопределение в качестве принципа в статью 1(2) Устава

---

[144] Г. Гроций. О праве войны и мира. Книга 1. Электронный ресурс. URL: http://www.civisbook.ru/files/File/Groziy.Kn1.pdf (дата обращения 27.11.2025)

[145] Ленин, В. И. Государство и революция / В. И. Ленин. – 2-е изд. – Москва : ООО «Издательство АСТ», 2020. – 136 С. – Текст : непосредственный.

[146] Ильинская, О. И. Защита прав человека в деятельности Лиги Наций / О. И. Ильинская. – Текст : электронный // Журнал российского права. – 2017. – № 11. – С. 96-110. – URL: https://clck.ru/3ANXiW (дата обращения: 01.04.2024).

Организации Объединенных Наций[147], на возникновение которой оказал сильное влияние Советский Союз. Этот принцип сыграл решающую роль в формировании международной системы после Второй мировой войны, способствуя процессу деколонизации и возникновению новых государств.

Включение положения о самоопределении в Устав ООН означало сдвиг в сторону международного признания легитимности стремления народов к независимости и самоуправлению. На международном уровне признавалось, что суверенитет принадлежит не только государствам, но и народам, составляющим эти государства. Это привело к росту поддержки движений за независимость и обеспечило правовую и легитимность для их борьбы. В середине XX века многие колонии добились независимости, что было признанием права народов на самоопределение и укреплением концепции национального суверенитета.

Категория государственного суверенитета также находит свое отражение в трудах современных философов. Карл Шмитт, немецкий политический теоретик и юрист, известен своими работами о суверенитете, праве и политической теории. Он оказал значительное влияние на политическую философию XX века, особенно в контексте авторитаризма и теории государства. Его взгляды на суверенитет играют ключевую роль в его понимании политики и правопорядка.

В работе «Политическая теология» (1922) Шмитт определяет суверенитет как способность принимать решение о введении исключительного состояния (чрезвычайного положения)[148]. Для Шмитта суверен – это тот, кто может временно приостановить действие норм права ради защиты государства.

---

[147] Организация Объединенных Наций. Устав Организации Объединенных Наций : подписан 26 июня 1945 года в Сан-Франциско по завершении Конференции Организации Объединенных Наций по международной организации – Текст : электронный // Организация Объединенных Наций : официальный сайт. – URL: https://www.un.org/ru/about-us/un-charter/full-text (дата обращения: 21.02.2024).

[148] Schmitt C. Political theology II: The myth of the closure of any political theology. – John Wiley & Sons, 2014.

Он подчеркивает, что суверенитет проявляется не в повседневных законах и процедурах, а именно в момент кризиса, когда необходимо принять исключительное решение, выходящее за пределы правовых норм.

Шмитт утверждает, что исключительное состояние – это основополагающая категория суверенитета. Это состояние является моментом, когда нормы права приостанавливаются, а власть суверена становится абсолютной. В исключительном состоянии суверен обретает неограниченную власть, чтобы защитить государство. По Шмитту, исключительное состояние – это ситуация, в которой истинная природа власти обнажается, и суверен принимает решения, руководствуясь политической целесообразностью, а не правовыми нормами[149].

Шмитт вводит понятие «политического», определяя его через различие между другом и врагом. Для него политика заключается в способности государства идентифицировать и управлять врагами. Суверенитет играет ключевую роль в этом процессе, так как именно суверен решает, кто является врагом и как с ним бороться. По мнению Шмитта, это различение определяет политическое сообщество и оправдывает исключительные меры, которые суверен может принять ради безопасности и единства государства. Шмитт критиковал либеральную демократию и парламентаризм за их неспособность справляться с кризисами. Он считал, что либеральные институты подчинены нормам, которые делают их слабыми перед лицом угроз и кризисов[150].

Суверенитет, по его мнению, требует сильного лидера или авторитета, способного принимать решительные меры в кризисных ситуациях, в отличие от медлительных и раздробленных демократических процессов. Шмитт рассматривал суверенитет как основу политического порядка, подчеркивая, что любая правовая система в конечном счете

[149] Bendersky J. W. Carl Schmitt: theorist for the Reich. – Princeton University Press, 2014. – T. 702.
[150] Там же.

зависит от возможности установления исключительного состояния, то есть от политической воли суверена.

Он утверждал, что суверенитет – это не просто юридическая функция, но и основа легитимности власти. Суверен имеет право принимать решения, которые выходят за рамки закона, когда это необходимо для сохранения политического порядка. Шмитт видит суверенитет как неотъемлемую часть политической власти, которая выходит за пределы обычного правового регулирования и проявляется в условиях кризиса и исключения. Его теории оказали глубокое влияние на политическую философию, особенно в вопросах диктатуры, авторитаризма и правового порядка в условиях чрезвычайного положения[151]

Мишель Фуко, французский философ, внес значительный вклад в понимание концепции суверенитета, хотя его подход к этому вопросу отличается от традиционных теорий суверенитета, которые часто связываются с властью государства и закона. Фуко интересовался властью, но он сместил фокус с классического понимания суверенитета как верховенства на другие формы власти и их проявления в обществе[152].

Фуко утверждает, что в классических теориях власть рассматривалась как суверенная, то есть сосредоточенная в руках государя или правительства, которое имеет право наказывать и управлять подданными. Однако, начиная с XVIII века, по мнению Фуко, происходит переход к другим формам власти – дисциплинарной и биовласти. Дисциплинарная власть проявляется через институты, такие как тюрьмы, школы, больницы, армии, которые регулируют поведение людей через дисциплину и надзор[153].

---

[151] Gottfried P. Carl Schmitt: politics and theory. – New York : Greenwood Press, 1990. – С. 83-100.
[152] Foucault M. Power: the essential works of Michel Foucault 1954-1984. – Penguin UK, 2019.
[153] Foucault M. Discipline //Rethinking the subject. – Routledge, 2018. – С. 60-69.

Биовласть касается управления жизнью населения, включая здоровье, рождаемость, смертность и другие биологические аспекты, что позволяет государству контролировать жизнь общества в более тонкой и скрытой форме.

Фуко критикует классическое понятие суверенитета как недостаточное для объяснения современных форм власти. Он утверждает, что суверенитет – это только один из элементов более сложной сети властных отношений. В современном мире власть больше не ограничивается прямым и явным контролем над телами людей через законы и наказания. Вместо этого она функционирует через микромеханизмы контроля, которые проникли в повседневную жизнь[154].

По мнению Фуко, суверенная власть часто легитимизируется через право и закон, но в то же время власть не ограничивается только правовыми рамками. Закон становится лишь одним из инструментов для поддержания власти, но не её основой.

Важным становится то, как власть контролирует и управляет, выходя за пределы традиционных представлений о суверенитете, через нормы, правила и дисциплину. Фуко вводит понятие биополитики, которое описывает способы управления жизнями людей через регулирование биологических и социальных процессов. Биополитика рассматривается как новый способ реализации суверенитета в условиях современности, где акцент смещается с контроля территории на управление населением[155].

Фуко таким образом расширяет понятие суверенитета, показывая, что власть не ограничивается действиями государства или правовой системы, а присутствует повсеместно через множество механизмов и практик, направленных на контроль и управление людьми.

---

[154] Foucault M. Power: the essential works of Michel Foucault 1954-1984. – Penguin UK, 2019.
[155] Lemke T. Beyond Foucault: From biopolitics to the government of life //Governmentality. – Routledge, 2010. – С. 173-192.

Джорджио Агамбен, итальянский философ, известен своими работами о суверенитете, особенно через призму понятий власти, права и исключительного состояния. Основные идеи Агамбена о суверенитете можно рассмотреть через его концепции «исключительного состояния» и «голой жизни», которые занимают центральное место в его теоретическом подходе.

В книге «Homo Sacer: Суверенная власть и голая жизнь» Агамбен исследует связь между суверенитетом и исключительным состоянием. Он утверждает, что суверенитет заключается в способности решать, когда и где действуют законы, и когда они могут быть приостановлены[156].

Суверенитет проявляется через способность создавать исключительное состояние – ситуацию, в которой нормы права временно приостанавливаются, а власть действует вне правовых ограничений. Это позволяет суверену (лидеру или государству) принимать меры, которые считаются необходимыми для защиты государства, но которые могут противоречить существующим законам и правам.

Агамбен утверждает, что исключительное состояние, которое традиционно воспринимается как временная мера, в современной политике становится нормой. Современные государства всё чаще прибегают к таким состояниям, что ставит под угрозу основные права граждан и подрывает традиционные юридические структуры.

По мнению Агамбена, это ведет к ситуации, когда суверенитет постоянно поддерживается через исключение, а не через соблюдение правовых норм. Концепция «голой жизни» или Homo Sacer (священный человек) описывает фигуру, которая может быть убита, но не может быть принесена в жертву – она исключена из обоих, и юридического, и религиозного порядков. Это жизнь, которая исключена из политического

[156] Agamben G. The omnibus homo sacer. – Stanford University Press, 2017.

и юридического порядка, но при этом полностью подвержена власти суверена.

Агамбен использует этот образ для описания того, как суверенитет действует на границах законности, создавая зоны исключения, где граждане могут быть лишены своих прав, оставаясь при этом в рамках власти. Агамбен также развивает идеи биополитики, подчеркивая, что суверенитет связан с контролем над жизнью, телами и населением[157]. Суверенитет включает не только способность к принятию законов, но и власть над жизнью, особенно в кризисных ситуациях.

Агамбен рассматривает суверенитет как неотъемлемо связанный с исключением и властью над жизнью, подчеркивая, что современный суверенитет проявляется не только в праве управлять, но и в праве исключать. Его работы часто критикуются за пессимистическое видение современной политики, но они также подчеркивают важность критического анализа власти и прав в условиях современного мира.

Выводы по параграфу:

Базовые основы категории государственного суверенитета, заложенные в Римской империи, эволюционировали через идеи монархии и абсолютной власти. Параллельно с теоретическим осмыслением суверенитет институализировался в западноевропейских политических системах посредством Аугсбургского мира и Вестфальского мира, заложившие основы для современного понимания территориального суверенитета и невмешательства. Данные принципы отражены сегодня в Уставе ООН.

Развитие политической философии Нового времени углубило понимание суверенитета, подчеркнув его неотъемлемые признаки и взаимосвязь с гражданскими правами и народом. В XX веке Макс Вебер и Карл Шмитт дополнительно развили концепцию, вводя идеи легитимного

[157] Fitzpatrick P. Bare sovereignty: Homo Sacer and the insistence of law //Theory & Event. – 2001. – Т. 5. – №. 2.

насилия, подчеркивая роль государства как основного регулятора правопорядка и исключительного обладателя суверенной власти. В противовес этому Леон Дюги отмечал необходимость ограничения суверенитета через внешние международные институты и внутренние демократические процессы. Таким образом, суверенитет как концепт прошел путь от абсолютной монархической власти к сложной сети прав и обязанностей, учитывающей как внутренние, так и международные реалии, подтверждая свою адаптивность и важность в развитии государственной власти и международных отношений. Следовательно, суверенитет - подвижная концепция, меняющаяся под воздействием времени и окружающей его современности[158].

В современной трактовке государственный суверенитет – это принцип, согласно которому государство обладает верховной властью на своей территории и в своих внутренних делах, без вмешательства извне. Суверенитет включает в себя:

- Территориальный суверенитет: государство имеет полную власть над своей территорией и ресурсами.
- Политический суверенитет: государство самостоятельно определяет свою политическую систему и форму правления.
- Юридический суверенитет: государство издает законы и распоряжения, которые обязательны для исполнения на его территории.
- Экономический суверенитет: государство ведет самостоятельную экономическую политику и контролирует свои экономические ресурсы.

С развитием цифровых технологий формируется новая аналитическая и прикладная категория – цифровой суверенитет.

---

[158] Onuf N.G. Sovereignty: Outline of a conceptual history / N. G. Onuf – Текст : электронный //Alternatives. – 1991. – Т. 16. – №. 4. – С. 425-446. – URL: https://journals.sagepub.com/doi/abs/10.1177/030437549101600403?journalCode=alta (дата обращения: 01.04.2024).

1.2. Понятие и признаки государственного суверенитета в современной политической науке и теории международных отношений

По мысли авторитетного российского политолога Ильина М.В.[159] методологически понятийные категории можно разделить на два типа: зонтичные, расширяющие понятие вширь, и матрешечные, углубляющие его понимание. Многие концепции являются сложносоставными и включаются в более широкие категории при этом имея внутреннюю аналитическую иерархию (то есть являются и зонтичными, и матрешечными одновременно). Государственный суверенитет - пример именно такого понятия. По мере эволюции международных отношений категория государственного суверенитета расширялась, чтобы включить всех участников международных отношений, контролирующих территорию, но устанавливающих разный порядок. Кроме того, технологическое развитие привело к появлению различных типов и элементов государственного суверенитета - продовольственный, технологический культурный, экономический, налоговый, платежный, информационный, цифровой, киберсуверенитет, суверенитет данных и так далее. В большинстве случаев каждый из таких типов суверенитета используется как синоним независимости государства в определенной области в рамках существующего мирового порядка. Таким образом, эволюция суверенитета пошла по пути как расширения практики применения данного понятия, которое стало зонтичным, так и по пути увеличения числа функциональных сфер суверенитета, перестроив его как полисоставное понятие.

---

[159] Суверенитет. Трансформация понятий и практик : монография / М.В. Ильин, И.В. Кудряшова, Я.И. Ваславский [и др.] ; под ред. М.В. Ильина, И. В. Кудряшовой. – Москва : МГИМО-Университет, 2008. – 18-19 с. – ISBN: 978-5-9228-0362-5

Суверенитет – ключевая категория в современной теории международных отношений. В частности, в рамках классического реализма, к представителям которой можно отнести Д. Моргентау[160], Э.Х. Карра[161] и других авторов, суверенитет рассматривается как главный принцип, определяющий поведение государств в международной системе. В этом контексте суверенитет понимается как абсолютная власть государства в пределах своих границ, а также как способность государства защищать свои интересы на международной арене. Согласно классическому политическому реализму, международная система анархична, отсутствует централизованная власть, которая могла бы регулировать поведение государств. В таких условиях суверенитет становится критически важным для выживания и безопасности государства. Государства, действующие в условиях анархии, стремятся к максимизации своей мощи и защите своих национальных интересов. Суверенитет в этом контексте является важнейшим условием и средством обеспечения безопасности и независимости[162].

Научная школа идеализма в теории международных отношений, оппонируя реализму, признаёт важность суверенитета, но также подчеркивает значимость международного сотрудничества, институтов и норм. Представители данного подхода исходят из того, что международные институты могут ограничивать абсолютный суверенитет государств ради достижения коллективных целей, таких как мир, стабильность и процветание. Международные организации, такие как ООН, играют важную роль в регулировании международных отношений и отражают наличие ограничений суверенитету[163]. Либеральная теория также подчеркивает важность защиты прав человека. Согласно данному

[160] Morgentau Hans J. Politics among Nations, The Struggle for Power and Peace. – 1948.
[161] Carr E. H. The twenty years' crisis, 1919-1939: Reissued with a new preface from Michael Cox. – Springer, 2016.
[162] Бордачев Т.В., Зиновьева Е.С., Лихачева А.Б. Теория международных отношений в 21 веке. М.: МО, 2015.
[163] Там же.

подходу, в некоторых случаях международное сообщество может считать необходимым вмешательство во внутренние дела суверенного государства ради защиты прав человека, что ставит суверенитет в контексте глобальных норм и обязательств[164].

Однако вмешательство во внутренние дела под предлогом защиты прав человека является примером экстратерриториальной практики в праве и суверенитете, и является наиболее спорным. Подход экстратерриториальности в практике суверенитета берет начало в колониальную эпоху. Исторически, метрополии (колониальные державы) устанавливали свою юрисдикцию на подконтрольных территориях, в том числе через создание правовых систем, неподконтрольных местным законам. Колониальные державы создавали концессии и анклавы в стратегически важных местах. Например, в Китае в XIX и начале XX веков существовали иностранные концессии, где европейские державы и США обладали экстерриториальными правами, управляя этими территориями вне юрисдикции китайских законов. В некоторых колониальных соглашениях иностранные державы добивались права экстерриториальной юрисдикции над своими гражданами, проживающими в колониях. Это позволяло им избегать местного правосудия и подчиняться только законам своей страны[165].

Экстратерриториальный суверенитет – это концепция, которая описывает способность государства или другого суверенного образования осуществлять власть или юрисдикцию за пределами своих территориальных границ[166]. Эта концепция имеет важное значение в международном праве в XXI веке. Исследователи отмечают, что в международном праве наметилась тенденция к распространению

---

[164] Weiss T. G. Humanitarian intervention. – John Wiley & Sons, 2016.

[165] Амирова А. А. Колониальная клаузула в контексте экстерриториального применения международных договоров по правам человека //Электронное сетевое издание «Международный правовой курьер». – 2020. – №. 11. – С. 9-19.

[166] Kayaoglu T. The extension of Westphalian sovereignty: State building and the abolition of extraterritoriality //International Studies Quarterly. – 2007. – Т. 51. – №. 3. – С. 649-675.

экстратерриториальной юрисдикции, которая утрачивает значение «юрисдикции последнего уровня», ввиду возможности ее установления не только в отношении преступлений в сфере международного права, но и применительно к иным публично-правовым отношениям в сфере налогового, антимонопольного, информационного регулирования[167].

Отдельные элементы и примеры экстратерриториального суверенитета являются легитимными и обоснованными. Дипломаты и консульские служащие, находящиеся на территории другого государства, обладают иммунитетом от юрисдикции этого государства. Этот принцип закреплен в Венской конвенции о дипломатических сношениях (1961 год) и Венской конвенции о консульских сношениях (1963 год). Международные организации, такие как ООН, могут пользоваться определенными привилегиями и иммунитетами в странах, где они расположены, что позволяет им действовать независимо от местной юрисдикции.

Однако его другие элементы являются спорными с точки зрения международной безопасности и права. Например, США имеют военные базы в Германии, Японии и многих других странах, на которые не распространяется суверенитет принимающих государств. Налоговое законодательство США требует от граждан и резидентов декларировать и платить налоги с доходов, полученных за границей. США проводят операции по борьбе с терроризмом и коррупцией за пределами своих границ, что часто вызывает споры о нарушении суверенитета других стран. В числе примеров – операции США в Ираке в 2003 году и в Афганистане в 2001 году. Примером эстратерриториальной политики являются международные санкции (за исключением тех, которые легитимированы резолюцией СБ ООН) против иностранных граждан, организаций или

[167] Терентьева Л. В. Экстерриториальное проявление юрисдикции государства в условиях трансформации восприятия его пространственных границ //Право. Журнал Высшей школы экономики. – 2019. – №. 3. – С. 160-180.

государств, что включает замораживание активов и ограничения на торговлю, даже если эти меры применяются за пределами территории государства, налагающего санкции. Например, санкции США против Ирана касаются не только американских, но и иностранных компаний, взаимодействующих с иранским бизнесом. Аналогичной практикой является санкционная политика США в отношении России, которая по оценкам И.Н. Тимофеева насчитывает на апрель 2024 года более 14 тысяч[168].

Экстратерриториальная практика суверенитета вызывает множество правовых и этических вопросов. Односторонние действия без согласия другого государства не являются легитимными. Экстерриториальные санкции могут негативно повлиять на граждан стран, и способствовать деградации международной безопасности. Сегодня США и ЕС проводят политику экстратерриториального суверенитета, в том числе в рамках цифровой среды. GDPR, введённый Европейским Союзом в 2016 году, является ярким примером экстратерриториального цифрового суверенитета. Регламент применяется не только к компаниям, базирующимся в ЕС, но и ко всем организациям, которые обрабатывают данные граждан ЕС, независимо от их местоположения[169].

Закон о честности и правосудии в информационных вопросах (CLOUD Act), принятый в США в 2018 году, позволяет американским правоохранительным органам запрашивать данные у компаний, находящихся за границей, если эти компании управляют данными американских граждан или связаны с американской юрисдикцией[170].

Россия и Китай на международном уровне выступают за развитие категории цифрового суверенитета в праве и в практике международных

---

[168]Тимофеев И. Все шоковые санкции против России уже введены // РИА Новости. 04.04.2024 URL: https://ria.ru/20240404/timofeev-1937753263.html (дата обращения: 04.04.2024)

[169] Goddard M. The EU General Data Protection Regulation (GDPR): European regulation that has a global impact //International Journal of Market Research. – 2017. – Т. 59. – №. 6. – P. 703-705.

[170] Rojszczak M. CLOUD act agreements from an EU perspective //Computer Law & Security Review. – 2020. – Т. 38. – P. 105.

отношений, в том числе на уровне РГОС ООН[171]. Вместе с тем, экстратерриториальность в цифровых международных отношениях, в том виде как ее реализуют США и ЕС, рассматривается как вызов международной информационной безопасности и попытка распространить нормативные рамки и правила Запада на глобальном уровне, без учета подходов и интересов других стран.

Таким образом, традиционные подходы и трактовки к изучению и практике государственного суверенитета в значительной степени применимы к практике цифровой среды. Однако, для более полной и детализированной формулировки теоретико-методологической базы исследования представляется целесообразным рассмотреть также современные направления теории международных отношений. Современные направления в теории международных отношений, а именно неолиберальный и неореалистический подходы - предлагают различные интерпретации меняющейся динамики государственного суверенитета в контексте глобализации и международных отношений.

Представители неолиберального институционализма[172] подчеркивают важность международных институтов, законов и норм в формировании поведения и суверенитета государств. Согласно этой точке зрения, несмотря на свой национальный суверенитет, государства включены в плотную сеть глобальных взаимодействий и должны сотрудничать и соблюдать международные нормы. Неолибералы утверждают, что эта взаимосвязанность приводит к «сложной взаимозависимости», в которой государства не могут просто действовать

---

[171] UN GA. 2021. Open-ended working group on developments in the field of information and telecommunications in the context of international security.

[172] Sørensen G. Sovereignty: Change and continuity in a fundamental institution / G. Sørensen – Текст : непосредственный //Political Studies. – 1999. – Т. 47. – №. 3. – С. 590-604; Jackson R. Sovereignty in world politics: a glance at the conceptual and historical landscape / R. Jackson – Текст : непосредственный // Political Studies. – 1999. – Т. 47. – №. 3. – P. 431-456; Nye J. S., Keohane R. O. The Role of Transnational Forces. Transnational Relations and World Politics / J. S. Nye, R. O. Keohane // International Politics. Anarchy, Force, Imperialism / Ed. by R. J. Art, R. Jervis. Boston: Little, Brown and Company, 1973. P. 501–512; Haas R. N. Intervention. The Use of American Military Force in the Post-cold War World. / R. N. Haas – Текст : непосредственный // New York: The Carnegie Endowment Book, 1994.

независимо, не учитывая международные последствия и выгоды от сотрудничества[173]. Этот подход не рассматривает суверенитет как абсолютную власть, ограниченную территориальными границами. В рамках данной парадигмы суверенитет концептуализируется как объем полномочий, который можно разделить или объединить, особенно в тех областях, где необходимо глобальное сотрудничество для решения трансграничных проблем, таких как изменение климата, торговля и безопасность[174].

Неореалисты[175], напротив, считают государство главным действующим лицом в международных отношениях и полагают, что суверенитет и власть занимают центральное место в исследованиях поведения государства. Они рассматривают международную систему как анархическую. В ней нет доминирующей силы, способной диктовать действия государств, помимо национальных интересов и соображений безопасности. С этой точки зрения государства защищают свой суверенитет, чтобы сохранить автономию и контроль над собственными территориями. Однако даже с неореалистической точки зрения концепция суверенитета подвергается изменениям под воздействием новых глобальных реалий. Государствам становится все труднее в одностороннем порядке отстаивать традиционную концепцию суверенитета, не сотрудничая с другими государствами и международными структурами для эффективного управления вызовами и угрозами, с которыми они сталкиваются вместе. Такой подход

---

[173] Rana W. Theory of complex interdependence: A comparative analysis of realist and neoliberal thoughts //International journal of business and social science. – 2015. – Т. 6. – №. 2.

[174] Бордачев Т.В., Зиновьева Е.С., Лихачева А.Б. Теория международных отношений в 21 веке. М.: МО, 2015.

[175] Krasner, S. D. Sovereignty: Organized Hypocrisy / S. D. Krasner. – Текст : непосредственный. // Princeton : Princeton, 1999. – 280 с; Waltz K. Globalization and American power / K. Waltz – Текст : непосредственный. // The National Interest. 2000. Spring. P. 46–55; Gilpin R. The Challenge of Global Capitalism: the World Economy in the 21th Century. / R. Gilpin – Текст : непосредственный. // Princeton: Princeton University Press. – 2000; Escude C. An Introduction to Peripheral Realism and its Implication for the Interstate System // Argentina and the Condor II missile project International relations theory and the Third World / Ed. by S. Neuman. – Текст : непосредственный. // New York: St.Martin’s Press. – 1998. – P. 55–76; Gruber L. Ruling the World: Power Politics and the Rise of Supranational Institutions. // Princeton: Princeton University Press. – 2000.

соответствует неолиберальному акценту на сотрудничестве через международные институты и неореалистическому взгляду на защиту национальных интересов в условиях хаотичного мирового порядка.

Кроме того, в дискуссии о суверенитете есть еще одна плоскость: разногласия между постпозитивистами и неолибералами по поводу существования концептуальной категории «суверенитета» в принципе. Постпозитивизм как парадигма – это сложная совокупность идей, концепций и методов, объединяющая несколько традиций политической мысли, включая постструктурализм, постмодернизм, социальный конструкционизм, неомарксизм. Постпозитивизм ставит под сомнение кажущуюся самоочевидность таких традиционных понятий, как суверенитет, власть и политика. Парадигма критикует всю традицию западной политической мысли, начиная с эпохи Просвещения. Эта критика особенно направлена на неолиберализм, который теоретики рассматривают как наиболее последовательное проявление традиции, которую они оспаривают в интеллектуальном и политическом планах[176].

Постпозитивисты утверждают, что в эпоху глобализации понятие суверенитета теряет смысл. Государство постепенно передает свои полномочия субнациональным образованиям (субъектам федерации, регионам, провинциям), транснациональным институтам и частным акторам, которые находятся вне государственного контроля. Глобальные потоки финансов, медиаобразов, рисков, моделей потребления, населения и власти дестабилизируют традиционное представление о национальных пространственных границах[177]. Подобный подход предлагает убедительные интерпретации возросшей роли ТНК в цифровой среде, в

[176] Лебедев С. А. Проблема научного метода в постпозитивизме / Лебедев С. А. – Текст : электронный. // Гуманитарный вестник. – 2019. – №. 6 (80). – С. 1 - 21 – URL: https://cyberleninka.ru/article/n/problema-nauchnogo-metoda-v-postpozitivizme (дата обращения: 21.02.2024).

[177] Иванов В. Государство и суверенитет. Спор о суверенитете / В. Иванов – Текст : электронный. // Русский журнал. – 2009. 28 сентября – URL: http://www.russ.ru/Mirovaya-povestka/Gosudarstvo-i-suverenitet (дата обращения: 21.02.2024); Agamben G. Homo Sacer. Sovereign Power and Bare Life. / G. Agamben – Текст : непосредственный. // Stanford: Stanford University Press. – 1998; Outhwaite W., Ray L. Social Theory and Postcommunism. / W. Outhwaite , L. Ray – Текст : непосредственный. // Oxford: Balckwell. – 2005.

особенности, крупных платформенных компаний, которые по многим параметрам превосходят возможности «средних» государств и даже отдельных «региональных» держав.

Постпозитивисты, в частности, представители Копенгагенской школы, утверждают, что государства, используя концепцию суверенитета, зачастую искусственно относят большинство важнейших вопросов к сфере безопасности, секьюритизируя отдельные вопросы, в том числе в сфере цифровых технологий[178].

Однако, согласно неолиберальному институционализму, постпозитивистский аргумент о «конце суверенитета» в современном мире недостаточно обоснован. Политический институт суверенитета эволюционирует, адаптируясь к новым вызовам, и этот адаптационный процесс еще не завершен[179]. Хотя постпозитивизм получил определенное распространение в международных и некоторых национальных социальных науках, он не смог преодолеть доминирующую точку зрения на суверенитет как ключевую категорию практики и анализа международной политики и вряд ли сможет сделать это в обозримом будущем.

Теория социального конструктивизма, получившая популярность в конце XX – начале XXI веков[180] рассматривает суверенитет как социально сконструированное понятие, которое меняется в зависимости от исторического и социального контекста. Конструктивисты, в том числе А. Вендт, утверждают, что понятие суверенитета формируется и изменяется под воздействием социальных норм, коллективных идентичностей и дискурсов. Государства не действуют исключительно на основе материальных интересов, но также учитывают социальные конструкции и международные нормы. В отличие от реалистов и либералов,

[178] Buzan B., Wæver O., De Wilde J. Security: A new framework for analysis. – Lynne Rienner Publishers, 1998.
[179] Sørensen G. Sovereignty: Change and continuity in a fundamental institution / G. Sørensen – Текст : непосредственный //Political Studies. – 1999. – Т. 47. – №. 3. – С. 590-604.
[180] Wendt A. Social theory of international politics. – Cambridge university press, 1999. – Т. 67.

конструктивисты считают, что суверенитет не является фиксированной величиной. Он эволюционирует и адаптируется под влиянием международных практик и изменений в восприятии легитимности власти. Гринвуд в своей трактовке делает акцент на суверенитете как сложном и развивающемся понятии, которое реагирует на изменения в международном праве, поведении государств и глобальной политике[181]. Онуф представляет суверенитет как глубоко переплетенный с состоянием современности концепт, предполагая, что ясность и стабильность суверенитета считались само собой разумеющимися, когда современная государственная система была неоспоримой. Однако по мере того, как вопросы о современности становились все более явными, концепция суверенитета также стала подвергаться критической переоценке. Эта переоценка отражает постоянный диалог между историческими традициями и современными вызовами, делая суверенитет динамичной, а не статичной характеристикой международных отношений.

Николас Онуф отмечает, что современная концепция суверенитета по-прежнему признает верховную власть в рамках политического сообщества, но при этом адаптировалась к реалиям глобальной взаимозависимости и влиянию международных норм. Теперь суверенитет включает в себя не только контроль над территорией и людьми на ней, но и признание со стороны других государств, что необходимо для эффективного участия государства в международной системе[182].

Необходимо также обратить внимание на отдельные аспекты современного суверенитета в работах ряда отечественных исследователей. Согласно трактовке М.В. Ильина суверенитет под собой объединяет три взаимосвязанных понятия «суверен» «суверенность» и непосредственно

[181] Greenwood R. War and sovereignty in medieval Roman law //Law and History Review. – 2014. – Т. 32. – №. 1. – С. 31-63.
[182] Onuf N. G. Sovereignty: Outline of a conceptual history //Alternatives. – 1991. – Т. 16. – №. 4. – С. 425-446.

сам «суверенитет»[183]. Суверен уникален и представляет собой верховный авторитет, определяющий политический порядок внутри определенной территории, являясь таким образом предельной инстанцией власти. Суверенность контекстна и описывает совокупность условий и механизмов, которые позволяют данной инстанции исполнять роль суверена. Суверенитет же воспринимается как универсальный политический принцип, подкрепленный соответствующими институтами, которые не только определяют возможность существования суверенов, но и гарантируют их взаимное мирное сосуществование. Его применение в различных контекстах помогает уточнить статус и суверенность конкретных политических субъектов.

Для полного осмысления суверенитета как категории необходимо учитывать территориальность, границы, конституции, легитимацию и другие современные институты. Сувереном может считаться актор, действующий от имени государства, если он соответствует общему принципу суверенитета, важному в мировой политике. Однако суверенитет не формируется простым объединением суверенов или атрибутов. Политолог Стивен Краснер, основываясь на реалистическом анализе международной политики, развивает мысль о том, что суверенитет как концепция, которая формально признана на международной арене, на практике часто подвергается нарушениям в интересах государств. Эти нарушения обусловлены стремлением государств максимизировать свои интересы. Суверенитет, таким образом, является скорее «организованным лицемерием», чем абсолютной реальностью, которая непрерывно ограничивает или направляет поведение государств[184].

---

[183] Ильин М.В. Суверенитет: вызревание понятийной категории в условиях глобализации / М.В. Ильин - – Текст : электронный //Политическая наука. – 2005. – №. 4. – С. 10-28. – URL: https://cyberleninka.ru/article/n/suverenitet-vyzrevanie-ponyatiynoy-kategorii-v-usloviyah-globalizatsii (дата обращения: 21.03.2024).

[184] Krasner S. D. Power, the state, and sovereignty: essays on international relations. – Routledge, 2009.

В этой перспективе суверенитет разделяется на несколько аспектов: внутренний суверенитет, суверенитет взаимозависимости, вестфальский суверенитет и международно-правовой суверенитет. Под внутренним суверенитетом традиционно понимается организация публичной власти внутри государства. Суверенитет взаимозависимости означает способность суверена контролировать то, что пересекает границы государства. Вестфальский суверенитет подразумевает исключение внешних акторов из властных структур внутри территории государства. Международный юридический суверенитет - юридические способности государства действовать на международной арене, а также преимущества, проистекающие из взаимного признания государств.

Краснер утверждает, что, несмотря на долговременное существование и частое упоминание категории суверенитета, они не всегда оказывают значительное влияние на межгосударственное взаимодействие. Государства действуют в рамках международной системы, характеризующейся неравенством власти и существованием конкурирующих норм, что ведет к тому, что принципы суверенитета могут быть легко нарушены в борьбе национальных интересов. Следовательно, суверенитет не является непреложной основой международного порядка, а скорее удобной концепцией, которая может быть использована или отброшена государствами в зависимости от обстоятельств[185].

В.Л. Цымбурский также[186] делит суверенитет на ряд составляющих: внутренний суверенитет факта господства (суверенитет властителя), внутренний суверенитет признания (суверенитет народа), внешний суверенитет факта господства (суверенитет государства) и внешний суверенитет признания (суверенитет нации). Суверенитет властителя отражает способность государства оказывать воздействие и принуждение

[185] Krasner, S. D. Sovereignty: Organized Hypocrisy. // Princeton : Princeton, 1999. – 280 p.
[186] Цымбурский, В. Л. Идея суверенитета в посттоталитарном контексте. // Полис. – 1993. – № 1. – С. 1-15.

внутри общества, обеспечивая его независимость на международной арене. Суверенитет народа акцентирует внимание на признании во имя сохранения регионального статус-кво, отражая отношение к суверенитету личности в посттоталитарном контексте. Суверенитет государства связан с возможностью государства действовать как независимый субъект международного права, устанавливая дипломатические отношения и ведя внешнюю политику. Суверенитет нации основывается на признании и согласии как внутри страны, так и на международном уровне, подчеркивая важность признания для определения суверенитета.

Дэниел Филпотт[187] развивает тему суверенитета, предлагая комплексный взгляд на его многоаспектность и важность для понимания международных отношений. Суверенитет – это верховная легитимная власть в пределах определенной территории, что которая дает право властвовать и право того, что в рамках определенной территории эта власть будет беспрекословна. Филпотт подчеркивает, что легитимность суверенитета может базироваться на законе, традиции, согласии или божественном предписании, и она признается теми, кто находится под властью суверена[188].

Филпотт также разделяет суверенитет на внутренний и внешний. Внутренний суверенитет касается способности государства осуществлять авторитетное воздействие внутри своих границ, регулируя жизнь своих граждан без вмешательства извне, что включает в себя контроль над экономикой, обороной, внутренним порядком и другими аспектами внутренней политики. Внешний суверенитет относится к признанию государства как независимого субъекта на международной арене, способного вести внешнюю политику, устанавливать дипломатические

[187] Philpott, D. Sovereignty: An Introduction and Brief History // Journal of International Affairs. – 1995. – № Vol. 48, No. 2, Transcending National Boundaries. – pp. 353-368.
[188] Там же.

отношения и защищать свои интересы без вмешательства других государств[189].

В некоторых областях суверенная власть государства может быть ограничена международными договорами или обязательствами, такими как членство в международных организациях, которые могут налагать определенные обязанности или ограничения на действия государства.

Филпотт подчеркивает, что суверенитет не следует путать ни с властью (которая может быть силовой и нелегитимной), ни с законом (который может регулировать действия суверена, но не определяет его суверенитет). Легитимность и способность осуществлять суверенные функции делают суверенитет ключевым элементом международных отношений и мировой политики.

Современные трактовки суверенитета в теории международных отношений отражают также эволюцию международно-правового закрепления категории государственного суверенитета. Устав Организации Объединенных Наций[190] 1945 года является основополагающим документом, задающим тон признания суверенитета на международном уровне. Пункт 1 статьи 2 Устава упоминает принцип суверенного равенства всех его членов, устанавливая, что все государства-члены, независимо от размера или силы, имеют равные права и обязанности. Пункт 4 статьи 2 подкрепляет этот принцип, запрещая всем членам Организации применять силу против территориальной целостности или политической независимости любого государства или любым другим способом, несовместимым с целями Организации Объединенных Наций. Пункт 2 статьи 1 Устава ООН закрепляет уже упомянутый принцип самоопределения народов.

---

[189] Там же.

[190] Организация Объединенных Наций. Устав Организации Объединенных Наций : подписан 26 июня 1945 года в Сан-Франциско по завершении Конференции Организации Объединенных Наций по международной организации – Текст : электронный // Организация Объединенных Наций : официальный сайт. – URL: https://www.un.org/ru/about-us/un-charter/full-text (дата обращения: 21.02.2024).

Важно отметить, сложное противоречивое отношение между принципами самоопределения народов и территориальной целостности государств[191]. В правовом поле противоречие снимает Декларация о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами[192], принятая в 1970 году. Документ развивает принципы Устава, уделяя особое внимание поведению государств в международных отношениях. В документе поясняются принципы, установленные Уставом ООН. В части противоречия самоопределения и целостности дается пояснение о том, что действия государства не должны толковаться как санкционирование или поощрение любых действий, которые привели бы к дроблению, частичному или полному нарушению территориальной целостности или политического единства суверенных и независимых государств, придерживающихся принципа равноправия и самоопределения народов.

В 1965 году в Декларации о недопустимости вмешательства во внутренние дела государств и защите их независимости и суверенитета[193] было прямо заявлено, что ни одно государство или группа государств не имеют права прямо или косвенно, по какой бы то ни было причине, вмешиваться во внутренние или внешние дела любого другого государства. Этот принцип крайне важен для поддержания международного мира и предотвращения конфликтов, которые могут

---

[191] Буханова А.С. Коллизия принципов самоопределения народов, территориальной целостности государств и возможные пути ее решения / А.С. Буханова – Текст : электронный // Право и управление: XXI век. - 2011. - № 4(21). - С. 67-71. – URL: https://mgimo.ru/upload/iblock/ed7/ed70d38bfd1591ae84ae4b8b474cb40b.pdf (дата обращения: 01.04.2024).

[192] Организация Объединенных Наций. Декларация о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом Организации Объединенных Наций : принята резолюцией 2625 (XXV) Генеральной Ассамблеи ООН от 24 октября 1970 года – Текст : электронный // Организация Объединенных Наций : официальный сайт. – URL: https://www.un.org/ru/documents/decl_conv/declarations/intlaw_principles.shtml (дата обращения: 21.02.2024).

[193] Организация Объединенных Наций. Декларация о недопустимости вмешательства во внутренние дела государств, об ограждении их независимости и суверенитета : принята резолюцией 2131 (XX) Генеральной Ассамблеи от 21 декабря 1965 года – Текст : электронный // Организация Объединенных Наций : официальный сайт. – URL: https://www.un.org/ru/documents/decl_conv/declarations/inadmissibility_of_intervention.shtml (дата обращения: 21.02.2024).

возникнуть в результате внешнего вмешательства. В настоящее время данный принцип сохраняет свою актуальность применительно к цифровым международным отношениям.

Декларация о недопустимости интервенции и вмешательства во внутренние дела государств 1981 года[194] рассматривает более сложные формы вмешательства, такие как политические и экономические меры, которые могут подорвать государственный суверенитет. Эта декларация имела особое значение в период холодной войны, подчеркивая приверженность международного сообщества защите автономии государств от всех форм тайного и открытого вмешательства.

Хельсинкский акт 1975 года, хотя и не имел обязательной юридической силы, сыграл решающую роль в практическом применении принципов суверенитета, особенно в контексте европейской безопасности и сотрудничества. В нем подчеркивалось уважение суверенитета, территориальной целостности и политической независимости государств и утверждалось невмешательство во внутренние дела как норма поведения, которую согласились соблюдать все государства-участники. В дальнейшем он привел к созданию Организации по безопасности и сотрудничеству в Европе.

Данные нормативные акты в совокупности свидетельствуют о наличии устоявшейся[195] международно-правовой базы, поддерживающей государственный суверенитет в практике международных отношений. Они не только определяют права государств на самоуправление без вмешательства извне, но и декларируют приверженность установлению стабильного и сбалансированного международного порядка,

---

[194] Организация Объединенных Наций. Декларация о недопустимости интервенции и вмешательства во внутренние дела государств : принята резолюцией 36/103 Генеральной Ассамблеи от 9 декабря 1981 года – Текст : электронный // Организация Объединенных Наций : официальный сайт. – URL: https://www.un.org/ru/documents/decl_conv/declarations/internal_affairs_decl.shtml (дата обращения: 21.02.2024).

[195] Мигранян А. Саакашвили добивается независимости Абхазии и Южной Осетии / А. Мигранян – Текст : электронный. // Известия. – 17 сентября 2004 г. – URL: https://iz.ru/news/294263 (дата обращения: 18.03.2024).

способствующего мирному сосуществованию и сотрудничеству между странами.

Из всех юридических принципов суверенитет является наиболее политическим. Дело не только в прямой связи суверенитета с проблемой о сущности, носителе и пределах политической власти, но и в значении принципа суверенитета в международной политике и международном праве[196]. Теоретические и юридические споры вокруг суверенитета неизбежно обретают политическую окраску и тесно вписаны в международно-политические реалии.

Вывод по параграфу:

Оформление цифрового суверенитета в международном праве носит обрывочный и фрагментарный характер, при этом он выступает и как гарант безопасности государства, и как условие развития сотрудничества и как социальный конструкт. Государства стремятся защищать свои цифровые ресурсы, данные и инфраструктуру, разрабатывая национальные законы и участвуя в международных инициативах. Однако цифровой суверенитет сталкивается с множеством вызовов, включая влияние глобальных технологических компаний, трансграничные потоки данных и киберугрозы. В будущем баланс между глобальной интеграцией и национальным суверенитетом в цифровой сфере будет оставаться ключевым вопросом международных отношений. При этом цифровой суверенитет тесно вписан в актуальные международные реалии. Таким образом, без рассмотрения взаимодействия и влияния на суверенитет таких международных процессов как глобализация, регионализация и макрорегионализация не представляется возможным провести глубокий анализа суверенитета в цифровую эпоху.

1.3. Категория государственного суверенитета в контексте трансформации международного порядка

[196] Левин И. Суверенитет. – Litres, 2022.

Современные международные отношения представляют собой сложную систему взаимодействий между государствами, международными организациями, негосударственными акторами. Начало СВО на Украине в 2022 году способствовало формированию многополярного мироустройства. Как отмечается в Концепции внешней политики Российской Федерации от 2023 года «необратимо уходит в прошлое неравновесная модель мирового развития, которая столетиями обеспечивала опережающий экономический рост колониальных держав за счет присваивания ресурсов зависимых территорий и государств в Азии, Африке и Западном полушарии. Укрепляется суверенитет и увеличиваются конкурентные возможности незападных мировых держав и региональных стран-лидеров. Структурная перестройка мировой экономики, ее перевод на новую технологическую основу (в том числе внедрение технологий искусственного интеллекта, новейших информационно-коммуникационных, энергетических, биологических технологий и нанотехнологий), рост национального самосознания, культурно-цивилизационное разнообразие и другие объективные факторы ускоряют процессы перераспределения потенциала развития в пользу новых центров экономического роста и геополитического влияния, способствуют демократизации международных отношений»[197].

Многополярность проявляется и в цифровых международных отношениях. Растет влияние незападных центров силы, в рамках таких международных организаций как ШОС, БРИКС, ЕВРАЗЭС, МЕРКОСУР и ряд других получает институциональное оформление концепция незападного мирового большинства[198].

---

[197] Концепция внешней политики Российской Федерации. Утв. Указом Президента от 30.03.2023.

[198] Тимофеев И.Н. Россия: путь к мировому большинству. 5.04.2023. РСМД. URL: https://russiancouncil.ru/analytics-and-comments/analytics/rossiya-put-k-mirovomu-bolshinstvu/ (дата обращения 23.04.2025)

Программный директор клуба Валдай Т.В. Бордачев выделяет следующие характеристики, демонстрирующие конструктивные аспекты выстраивания нового мирового порядка: «Во-первых, становление демократической многополярности, символом которой является объединение БРИКС. Во-вторых, постепенное размывание монополии узкой группы государств в различных секторах мировой экономики. В-третьих, оживление внешнеполитической активности большинства стран, которые мы определяем как мировое большинство: совокупность государств, которые не ставят перед собой революционных задач, но стремятся к усилению своей самостоятельности в мировых делах и определению собственного будущего»[199].

Несмотря на рост геополитической напряженности сохраняют динамику транснациональные процессы, в том числе в цифровой сфере. В современных условиях суверенитет и суверенность уже не определяются лишь внутренней легитимацией и не существуют в отрыве от системы международных отношений. Рост националистической политики и пересмотр глобальных цепочек поставок, фундаментальные процессы глобализации - такие как движение информации, капитала, людей, информации и данных эволюционируют, адаптируясь к новым международным реалиям многополярного мира, технологическому прогрессу, росту международной конфликтности и великодержавной напряженности[200].

Со времен Ж. Бодена суверенитет считался центральной концепцией для понимания политики. Но в 1990-е годы это значение, казалось, уменьшилось, что привело к разговорам о пост-суверенном мире, в котором государства больше не будут самым важным и, в конечном счете,

---

[199] Т. Бордачев. Признаки нового мирового порядка. // Дискуссионный клуб Валдай. 2023. URL: https://ru.valdaiclub.com/a/highlights/priznaki-novogo-mezhdunarodnogo-poryadka/#masha_0=4:39,4:93 (дата обращения 23.04.2025)

[200] Там же.

высшим источником[201]. Важную роль в дискуссиях о конце суверенитета играли аргументы об особой природе информационных технологий и Интернета, которые фактические не «признавали» государственных границ[202]. Однако дебатам о конце суверенитета пришли на смену дебаты о конце глобализации[203], которые акцентируют возрастающую роль государств и непреходящую значимость государственного суверенитета в практике международных отношений. Особенно заметными дебаты о конце глобализации и возврату к классическим принципам Вестфальской политической системы мира стали в 2020-е гг[204]. Все более популярной в этих условиях становится и дискуссия о конце информационной глобализации, хотя аргументы, выдвигаемые авторами в пользу цифровой фрагментации, носят менее категоричный характер и апеллируют скорее к цифровой регионализации[205].

Дебаты о конце глобализации отражают сложное взаимодействие экономических, политических и технологических сил, которые меняют глобальный политический ландшафт. Более того, рост негосударственных акторов, таких как международные правительственные и неправительственные организации и ТНК[206], ставит под сомнение монополию государства на принятие решений и создают новый контекст для реализации государственного суверенитета[207].

В экономическом измерении глобализация обычно ассоциируется увеличением объемов перемещения товаров, услуг, капитала и рабочей

---

[201] Philpott D. Sovereignty: An introduction and brief history //Journal of international affairs. – 1995. – С. 353-368.
[202] Зиновьева Е. С. Формирование цифровых границ и информационная глобализация: анализ с позиций критической географии //Полис. Политические исследования. – 2022. – №. 2. – С. 8-21.
[203] См. напр.: Rugman A. The end of globalization. – Random House, 2012; James H., James H. The end of globalization: lessons from the Great Depression. – Harvard University Press, 2009.
[204] Hameiri S. COVID-19: Is this the end of globalization? //International Journal. – 2021. – Т. 76. – №. 1. – С. 30-41.
[205] Зиновьева Е. С., Булва В. И. Цифровой суверенитет Европейского союза //Современная Европа. – 2021. – №. 2. – С. 40-49.
[206] Юдин, Н. О. Роль ТНК в современной мировой политике / Н. О. Юдин // Обозреватель. – 2020. – № 9(368). – С. 83-92.
[207] Krasner S.D. Globalization and sovereignty / Krasner S.D. – Текст : непосредственный. // States and Sovereignty in the Global Economy. – Routledge, 1999. – 19 p.

силы через национальные границы[208]. В политическом измерении – с развитием международных и наднациональных институтов, которые размывают традиционное понятие вестфальского суверенитета, то есть абсолютной власти в рамках территориально определенного государства[209]. В культурном измерении – с распространением идей, ценностей и форм культурного самовыражения по всему миру, что приводит к таким явлениям, как культурная гибридизация и глобальное распространение социальных сетевых сервисов[210]. Сами процессы глобализации тесно связаны с развитием цифровых технологий, на современном этапе – с развитием трансграничных потоков данных и информационно-коммуникационных технологий.

Глобализация изменила контекст международной политики и количество акторов цифровых международных отношений. Результатом стала реконфигурация суверенитета, который стал более сложным и раздробленным между различными уровнями и институтами[211]. Поэтому государство сохраняет роль ключевого субъекта глобальной политики[212], но в рамках сложной сети международных институтов и соглашений.

Появление негосударственных субъектов привнесло новое измерение в международное сотрудничество. Появляются новые форматы международного сотрудничества, в которых наряду с государствами принимают участие негосударственные акторы[213]. Новые форматы получают распространение проявляются в различных областях, таких как

---

[208] Трифонов, Д. С. Глобализация: сущность и современные тенденции развития / // Вестн. Моск. Ун-та. Сер. 6. Экономика. . – 2006. – № 5. – С. 32.

[209] Held D. [и др.]. Global Transformations: Politics, Economics and Culture / под ред. C. Pierson, S. Tormey // London: Palgrave Macmillan UK. – 2000. – С.19, 28.

[210] Тангалычева Р.К. Теоретико-методологические основы социологического изучения межкультурной коммуникации. / Р.К. Тангалычева – Издательство: ООО «Скифия-принт» . – 2014. – с. 79-82 – Текст : непосредственный.

[211] Held D. [и др.]. Global Transformations: Politics, Economics and Culture / под ред. C. Pierson, S. Tormey – Текст : непосредственный // London: Palgrave Macmillan UK. – 2000. – p. 35.

[212]Гринин Л.Е. Глобализация и процессы трансформации национального суверенитета / Л.Е. Гринин – Текст : электронный // Век глобализации – №1 – 86-97 С. – URL: https://cyberleninka.ru/article/n/globalizatsiya-i-protsessy-transformatsii-natsionalnogo-suvereniteta (дата обращения: 10.03.2024).

[213] Юдин Н.О. Транснациональная корпорация как актор гуманитарной дипломатии // Социально-гуманитарные знания. – 2024. – № 2. – С. 147-150.

экономика, управление окружающей средой и глобальное здравоохранение, поскольку государства признают необходимость межрегионального сотрудничества для решения трансграничных проблем[214]. Вопросы управления интернетом и обеспечения международной информационной безопасности также обсуждаются в многоуровневом формате – с привлечением государств и негосударственных акторов.

Сложную многоуровневую динамику отношений между суверенитетом и транснациональными процессами и потоками, многоуровневый и неоднозначный характер глобализационных процессов продемонстрировала пандемия COVID-19, которая подчеркнула взаимосвязанность современного мира, показав, как быстро транснациональные вызовы могут стать угрозой глобальной безопасности. Эффективнее они могут быть решены за счет скоординированных действий со стороны всех государств. Пандемия, как глобальное потрясение, стала новым примером динамики государственного суверенитета. Ответственность за совершение этих скоординированных действия взяла на себя Всемирная организация здравоохранения (ВОЗ). Однако национальные власти сами решали, как и в каком объеме реализовывать рекомендации ВОЗ. Нужно также упомянуть и то, что у одних стран были ресурсы на то, чтобы справиться самим (Россия, Китай), другие – были вынуждены ждать помощи от мирового сообщества (Италия).

Начало пандемии, во-первых, привело к немедленному усилению пограничного контроля и ограничений на поездки со стороны государств по всему миру. Такое усиление является классической демонстрацией суверенитета, подчеркивающей традиционные для Вестфальского порядка

[214] Slaughter A New World Order / Slaughter, M. A. – Текст : непосредственный. // Princeton University Press. – 2005. – 368 с.

полномочия государства по контролю своих границ[215]. Закрытие границ, часто одностороннее и без международных консультаций, продемонстрировало, что государства действуют в режиме самопомощи, где национальные интересы превалируют над коллективными глобальными действиями[216].

Пандемия также высветила уязвимые места, связанные с глобализацией, в частности зависимость от международных цепочек поставок товаров первой необходимости, включая медицинские и фармацевтические препараты. Конфликты между государствами за доступ к маскам, аппаратам искусственной вентиляции легких, а затем и вакцинам показали, насколько государственный суверенитет подорван глобализацией. Государства, контролировавшие эти ресурсы, обладали значительной властью, оказывая влияние на мировую политику в соответствии с теориями динамики и баланса сил[217]. Коронакризис привел к возрождению националистических настроений, когда правительства стали уделять больше внимания внутренним, а не международным проблемам. Это проявилось в «вакцинном национализме», и в последующих «вакционных войнах», когда страны отдавали приоритет вакцинации своего населения, а не экспорту вакцин[218].

Эффективность международных организаций, таких как ВОЗ, во время пандемии показала свои уязвимые стороны. Очевидная неспособность этих организаций эффективно справиться с кризисом без полного сотрудничества с государствами еще больше иллюстрирует ограничения глобального управления, когда ни один центральный орган не

---

[215] Mearsheimer J. J. The tragedy of great power politics. / J. J. Mearsheimer – Текст : непосредственный. // WW Norton & Company. – 2001. – 362 с.
[216] Waltz K. N. Theory of international politics. / K. N. Waltz – Текст : непосредственный. // Waveland Press. – 2010. – 251 с.
[217] Baldwin R., Di Mauro B. W. Economics in the time of COVID-19/ R. Baldwin, B. W. Di Mauro – Текст : непосредственный. // Vox CEPR Policy Portal. – 2020. – Т. 2. – №. 3.
[218] Bollyky T. J., Bown C. P. The tragedy of vaccine nationalism: only cooperation can end the pandemic / T. J. Bollyky, C. P. Bown – Текст : непосредственный. // Foreign Aff. – 2020. – Т. 99. – С. 96.

может заставить суверенные государства действовать против своих интересов[219].

Таким образом, пандемия COVID-19 подчеркнула нелинейный, многомерный характер государственного суверенитета в условиях глобализации. Международные организации внесли свой вклад в преодоление кризиса, но действия, предпринятые государствами во время пандемии - от закрытия границ до складирования необходимых медицинских препаратов, - подчеркивают постоянное доминирование государства как основного актора международных отношений, имеющего ресурсы и руководствующегося национальными интересами и соображениями безопасности.

Ответом на «провалы» глобализации стал процесс регионализации поскольку в региональных организациях, как правило, меньше участников чем в глобальных, и они чаще более близки в плане культур и интересов, следовательно, им проще договориться, и они более эффективны[220].

В настоящем исследовании под регионализацией понимается процесс, в ходе которого регионы становятся центром управления, экономической деятельности и формирования идентичности, выходя за пределы национальных границ. Заключая региональные соглашения, государства также, как и на глобальном уровне, могут уступать определенные аспекты своего суверенитета региональным органам в обмен на экономические выгоды, безопасность или политическое влияние[221]. Такая уступка суверенитета, как и в случае с глобализацией, влияет на традиционное представление о государственной автономии, но

---

[219] Там же.

[220] Regionalism and the European Union – Текст : электронный. // E-International Relations – URL: https://www.e-ir.info/2022/05/21/regionalism-and-the-european-union/ (дата обращения: 14.03.2024).

[221] Кузнецов А.С. «Надкушенный суверенитет»: проблема категории «Суверенитет» при исследовании субнациональной дипломатии / А.С. Кузнецов – Текст: электронный. // Политическая экспертиза: ПОЛИТЭКС. – 2006. – Vol. 2, № 3. – С. 241–252. – URL: https://cyberleninka.ru/article/n/nadkushennyy-suverenitet-problema-kategorii-suverenitet-pri-issledovanii-subnatsionalnoy-diplomatii (дата обращения: 21.03.2024).

также может стать альтернативным механизмом управления региональными проблемами и, возможно, глобальными.

Предпосылки формирования регионализации появились на рубеже XIX - XX веков, когда геополитические стратегии привели к формированию региональных альянсов, главным образом с целью защиты собственных рынков сбыта и экономических интересов. Европейские государства создавали таможенные союзы, появился Бенилюкс. США и Франция предпринимали неудачные попытки организации взаимодействия в своих регионах[222].

Однако наиболее значительные усилия по регионализации возникли после Второй мировой войны под влиянием как проблем безопасности, так и экономических вопросов. В 1923 году 23 страны подписали Генеральное соглашение по тарифам и торговле (ГАТТ), что стало началом формирования международной торговой сети взаимодействий. С 1951 года по 1959 год формировались европейские экономических объединения нового типа. Параллельно с этим создание Организации Североатлантического договора (НАТО) в 1949 году и Организации Варшавского договора (ОВД) в 1955 году подчеркнуло роль региональных организаций в механизмах коллективной безопасности, в первую очередь, обусловленную геополитической напряженностью времен холодной войны.

Окончание холодной войны способствовало регионализации как органичной части глобализации. Региональное сотрудничество институционализировалось в рамках таможенных союзов (Южноамериканский общий рынок, Экономическое сообщество западноафриканских государств, Общий рынок для Восточной и Южной

[222] Спартак А.Н. Метаморфозы процесса регионализации: от региональных торговых соглашений к межрегиональным проектам. / А.Н. Спартак – Текст: электронный // Контуры глобальных трансформаций: политика, экономика, право. – 2017. – Vol. 10, № 4. – С. 13–37. – URL: https://cyberleninka.ru/article/n/metamorfozy-protsessa-regionalizatsii-ot-regionalnyh-torgovyh-soglasheniy-k-mezhregionalnym-proektam (дата обращения: 21.03.2024).

Африки, Западноафриканский экономический и валютный союз), Таможенного союза России – Беларуси – Казахстана. Появились Североамериканское соглашение о свободной торговле (NAFTA) в 1994 году и Ассоциация государств Юго-Восточной Азии (АСЕАН) в 1967 году. Подобные организации создавались для содействия экономическому росту за счет снижения торговых барьеров и расширения экономического сотрудничества[223]. Данный этап можно назвать «классической вариацией» регионализации.

К предпосылкам начала новой вехи регионализма относят разочарование стран-участниц в ВТО из-за отсутствия значимых результатов переговоров Дохийского раунда, снижение эффективности функционирования ЕС из-за вступления в Союз стран Центральной и Восточной Европы, а также отказ от наднационального формата интеграции из-за его негибкости. Однако возвращаться к двусторонним форматам взаимодействия уже не представлялось эффективным, что привело к расширению повестки региональных организаций, к увеличению их количества, а также к интенсификации их деятельности[224]. Регионализация стала в некотором роде оппозицией глобализации и рассматривалась как альтернатива для решения существовавших проблем, что позволило оформиться такому явлению как мегарегионализм.

Современный мировой ландшафт характеризуется наличием нескольких значимых региональных и мегарегиональных объединений, каждое из которых играет огромную роль в формировании региональной экономической политики, политического сотрудничества и динамики безопасности.

---

[223] Там же.

[224] Спартак А. Н. Новый этап регионализации: основное содержание, вызовы для многосторонней торговой системы и постсоветской интеграции / Спартак А. Н. – Текст : электронный. //Международная торговля и торговая политика. – 2016. – №. 2 (6). – С. 8-27. – URL: https://cyberleninka.ru/article/n/novyy-etap-regionalizatsii-osnovnoe-soderzhanie-vyzovy-dlya-mnogostoronney-torgovoy-sistemy-i-postsovetskoy-integratsii (дата обращения: 18.02.2024).

Таким образом, приведенные выше примеры иллюстрируют динамичный и спорный характер суверенитета во взаимосвязанном мире. Суверенитет – это не только юридическая, но и глубоко политическая концепция, отражающая стремление граждан к автономии и самоопределению. Как и в случае с глобализацией, регионализация неоднозначна. Есть успешные региональные и мегарегиональные организации, но их эффективность вызывает вопросы.

Выводы по параграфу:

Под суверенитетом в данном исследовании подразумевается политическое состояние государства на определенной территории, имеющего признанные полномочия вести свои внутренние дела без вмешательства извне, проводить независимую внешнюю политику и контролировать взаимодействие в пределах своих границ, участвуя при этом в выгодных для себя случаях в международных механизмах. Суверенитет обладает такими характеристиками как гибкость, выражающаяся в функциональности и многоаспектности, уникальность, универсальность и контекстность. Следовательно, в мире нет одного одинакового суверенитета: суверенитет каждой страны уникален и в разной степени ограничен наднациональным уровнем, будь то региональным или глобальным.

Цифровая революция, произошедшая вслед за появлением Интернета и распространением цифровых коммуникационных технологий, положила начало новому этапу глобализации, который часто называют «цифровой глобализацией». Этот этап характеризуется беспрецедентными масштабами обмена информацией и возникновением цифровой экономической деятельности, которая преодолевает традиционные границы. Данные процессы привели к тому, что цифровизация, как и глобализация, за счет своего всеобъемлющего характера стала очередным испытанием для традиционного понимания

суверенитета и способствовала возникновению его нового «подвида» – цифрового суверенитета.

1.4. Подходы к изучению цифрового суверенитета в современной политической науке

В цифровом измерении концепция государственного суверенитета была оспорена академическим дискурсом о кибер-исключительности, согласно которому нормы, применимые к киберпространству не распространяются на классические международные отношения. Самую первую попытку определить полномочия государства в киберпространстве предпринял Джон Барлоу. В Декларации независимости киберпространства[225] он раскритиковал попытки правительств взять под контроль киберпространство. Главный аргумент состоял в нематериальности киберпространства: правительства управляют территорией, а у киберпространства ее нет, это новая сущность, где государствам нет места[226].

В 1990-е – начале 2000-х гг. появился целый ряд академических работ, преимущественной в научном сообществе США и стран Европы, которые критиковали применимость государственного суверенитета к цифровой среде. Используя схожие аргументы, антигосударственной точки зрения на управление Интернетом придерживается Мильтон Мюллер. По его мнению, в киберпространстве должен верховенствовать принцип «народного суверенитета». Суверенитет принадлежит пользователям Интернета, а не национальным государствам. Уникальная природа киберпространства делает традиционную модель суверенитета неуместной и потенциально вредной для существующих структур

[225] Barlow J. P. A Declaration of the Independence of Cyberspace./ J. P. Barlow – Текст : электронный. // 1996. – URL: https://www.eff.org/cyberspace-independence (дата обращения: 15.03.2024 г.).
[226] Там же.

управления Интернетом. Поэтому должна усиливаться роль и расшириться права и возможности отдельных лиц и многосторонних институтов, таких как Форум по управлению Интернетом и ICANN[227].

На современном этапе технологического развития важнейшее значение приобретает суверенитет в области цифровых технологий. Внимание к цифровому суверенитету обусловлено радикальной трансформацией экономического и технологического укладов, общественных отношений и политической жизни, вызванной глобальной цифровой трансформацией. Данные изменения были концептуализированы в работе К. Шваба «4 Промышленная революция»[228]. Следует подчеркнуть, что концепция К. Шваба подвергается широкой критике как в российской, так и зарубежной литературе. Ряд исследователей указывает на технократический и идеологизированный характер данного подхода, игнорирование социальных последствий цифровой трансформации, усиление влияния транснациональных корпораций и рисков цифрового неравенства. В условиях современной геополитической конфронтации эти риски особенно значимы для оценки влияния цифровой революции на государственный суверенитет.

В условиях, когда цифровое пространство стало полем геополитических противоречий, а уровень цифровизации становится важным фактором, определяющим положение страны на международной арене и спектр доступных ей внешнеполитических возможностей, в научном сообществе возросло внимание к проблематике цифрового суверенитета[229].

Исследования в области цифрового суверенитета тесно связаны с анализом технологического суверенитета, под которым понимается

---

[227] Mueller M. L. Against sovereignty in cyberspace / M. L. Mueller – Текст : непосредственный. // International studies review. – 2020. – Т. 22. – №. 4. – С. 779-801.
[228] Клаус Ш. Четвертая промышленная революция. – Litres, 2016.
[229] Цифра и искусственный интеллект на службе дипломатии. М.: МГИМО, 2024.

способность государства проводить независимую политику в сфере высоких технологий. Кроме того, многие авторы увязывают проблематику цифрового суверенитета с вопросами обеспечения информационной безопасности[230]. Отдельным вопросом стоит проблема цифрового вмешательства как нарушения суверенитета государств, причем эта проблематика рассматривается как российскими[231], так и зарубежными учеными. Также необходимо упомянуть взаимосвязь с исследованиями в области технологических укладов, которые проводятся в сфере экономических наук и подчеркивают экономический потенциал цифровых технологий в рамках перехода к Четвертой промышленной революции[232].

Существуют терминологические разночтения. Так, например, в российском академическом дискурсе чаще используется термин «информационный суверенитет», призванный подчеркнуть важность контроля не только над технической инфраструктурой в целях обеспечения суверенитета, но и над трансграничным контентом[233]. Западные авторы преимущественно оперируют термином «киберсуверенитет», которые рассматриваются через призму государственной юрисдикции над инфраструктурой, программным обеспечением и данными, и в меньшей степени затрагивают проблемы контроля над трансграничными потоками информации[234]. С развитием «больших данных» и технологий искусственного интеллекта наиболее употребимым становится термин «цифровой суверенитет».

---

[230] Виноградова Е. В., Полякова Т. А. О месте информационного суверенитета в конституционно-правовом пространстве современной России //Правовое государство: теория и практика. – 2021. – №. 1 (63). – С. 32-49.

[231] Зиновьева Е.С. Проблема «цифрового вмешательства» в российско-американских отношениях // РСМД. 23.10.2020. URL: https://russiancouncil.ru/analytics-and-comments/analytics/problema-tsifrovogo-vmeshatelstva-v-rossiysko-amerikanskikh-otnosheniyakh/

[232] Маслов В. И., Лукьянов И. В. Четвертая промышленная революция: истоки и последствия //Вестник московского университета. Серия 27. Глобалистика и геополитика. – 2017. – №. 2. – С. 38-48.

[233] Кучерявый М. М. Государственная политика информационного суверенитета России в условиях современного глобального мира //Управленческое консультирование. – 2014. – №. 9 (69). – С. 7-14.

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

Среди российских авторов проблему информационного суверенитета изучали М.М. Кучерявый[235], В.В. Бухарин[236]. Они рассматривали суверенитет через призму угроз в сфере информационной безопасности. Д.В. Винник связывает цифровой суверенитет с политическими и правовыми режимами обработки данных в Интернете[237]. М.М. Кучерявый определял информационный суверенитет как верховенство и независимость государственной власти при формировании и реализации информационной политики в национальном сегменте и глобальном информационном пространстве[238]. Российский автор В.В. Бухарин выделяет следующие компоненты информационного суверенитета России, технически обеспечивающие национальную безопасность: поисковую систему, социальные сети, операционную систему и программное обеспечение, микроэлектронику, сетевое оборудование, национальный сегмент сети Интернет, платежную систему, собственные средства защиты, криптографические алгоритмы и протоколы, навигационную систему[239].

Анализируя подходы европейских авторов, А.Н. Толстухина отмечает, что некоторые ученые полагают, что цифровой суверенитет можно интерпретировать как необходимость для страны развивать или сохранять в отношении ключевых технологий собственную автономию или же иметь как можно более низкий уровень структурной зависимости. Другие считают, что это способность страны (или группы стран) автономно генерировать технологические и научные знания или

---

[235] Кучерявый М. М. Государственная политика информационного суверенитета России в условиях современного глобального мира //Управленческое консультирование. – 2014. – №. 9 (69). – С. 7-14.
[236] Бухарин В. В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности //Вестник МГИМО университета. – 2016. – №. 6 (51). – С. 76-91.
[237] Винник Д. В. Цифровой суверенитет: политические и правовые режимы фильтрации данных //Философия науки. – 2014. – №. 2. – С. 95-113.
[238] Кучерявый М. М. Государственная политика информационного суверенитета России в условиях современного глобального мира //Управленческое консультирование. – 2014. – №. 9 (69). – С. 7-14.
[239] Бухарин В. В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности //Вестник МГИМО университета. – 2016. – №. 6 (51). – С. 76-91.

использовать технологические возможности, разработанные внешними игроками, за счет активизации надежных партнерских отношений[240].

Особенностью европейского академического дискурса также является концепция цифрового суверенитета личности. Под цифровым суверенитетом личности понимается безопасность персональных данных и защита от негативного информационного воздействия и дезинформации, а также защита от практики «надзорного капитализма» со стороны ИТ-гигантов, под которым понимается сбор персональных данных и их последующее использование в целях воздействия на предпочтения пользователей[241].

По инициативе исследователей из КНР в научный дискурс было введено понятие «интернет-суверенитет» – право государства устанавливать собственные правила функционирования интернет-пространства, отвечающие национальным интересам и традициям[242].

Необходимо отметить, что в научной литературе США долгое время критически относились к самой категории цифрового суверенитета, отмечая ее связь с цензурой [243]. Более того, исследователи США постоянно продвигали идею, согласно которой Интернет является общим пространством человечества по аналогии с открытым морем или космическим пространством, и на него не распространяется категория государственного суверенитета. Во внешнеполитическом дискурсе США такой подход до сих пор сохраняется. Однако в последние годы вопросы фрагментации Интернета и проблема вмешательства во внутренние дела США, тема смежная с проблематикой суверенитета, занимают важное

---

[240] Толстухина А. Технологический суверенитет Евросоюза и его границы // РСМД. 12.10.2022Г URL: https://russiancouncil.ru/analytics-and-comments/analytics/tekhnologicheskii-suverenitet-evrosoyuza-i-ego-granitsy/?sphrase_id=144471914

[241] Lewis J. A. Sovereignty and the evolution of internet ideology. – Center for strategic & international studies (CSIS), 2020.

[242] Zeng J., Stevens T., Chen Y. China's solution to global cyber governance: Unpacking the domestic discourse of “internet sovereignty” //Politics & Policy. – 2017. – Т. 45. – №. 3. – С. 432-464.

[243] Deibert R. J. The geopolitics of internet control: Censorship, sovereignty, and cyberspace //Routledge handbook of Internet politics. – Routledge, 2008. – С. 323-336.

место в академическом дискурсе США и политической риторике официальных лиц[244].

Таким образом, в научной литературе сложилось несколько различных подходов к определению содержания понятия «цифровой суверенитет», разнятся также и используемые термины. Во многом это обусловлено политическими противоречиями между странами, различиями в политических режимах и культурах государств, в уровнях развития цифровых технологий.

Важно также указать на ряд специфических особенностей цифровых технологий, которые не позволяют просто экстраполировать категорию суверенитета из реального в виртуальное пространство. К числу таких особенностей относятся трансграничный характер потоков информации и данных, высокая роль частных компаний и отдельных пользователей в создании контента. Сложность определения границ государственной юрисдикции в отношении данных и ряд других особенностей должны быть приняты во внимание при определении сущностных характеристик концепции цифрового суверенитета в международных отношениях и международном праве.

В отличие от других пространств, на которые ранее распространялась юрисдикция государств, цифровая сфера является рукотворной. Цифровые технологии развиваются очень быстро. В частности, актуальной тенденцией последних нескольких лет стало формирование метавселенных, развитие технологий виртуальной и дополненной реальности, а также широкое распространение криптовалют. В 2022 году возросшая напряженность вокруг независимости Тайваня поставила вопрос об автономном производстве компьютерных чипов на территории страны как важной составляющей технологического и

[244] Barrinha A., Renard T. Power and diplomacy in the post-liberal cyberspace //International Affairs. – 2020. – Т. 96. – №. 3. – С. 749-766. Fick N. et al. Confronting Reality in Cyberspace //Council for Foreign Relations [Official website] URL: https://www. cfr. org/report/confronting-reality-in-cyberspace/download/pdf/2022-07/CFR_TFR80_Cyberspace_Full_SinglePages_06212022_Final. Pdf

цифрового суверенитета. После начала специальной военной операции России на Украине в 2022 году западные интернет-платформы отказались предоставлять сбалансированную и объективную информацию о России и были заблокированы на территории страны, что показало важность наличия автономных интернет-платформ и контента как элементов информационного суверенитета.

В этих условиях представляется весьма релевантной концепция, согласно которой цифровой суверенитет по своей природе есть нестатичная, динамическая категория. [245].

Международное право уже содержит ряд положений относительно государственного суверенитета, которые если не по букве, то, по сути, вполне применимы к глобальному информационному пространству. Статья 2 Устава ООН 1945 года определяет принцип суверенного равенства государств как основополагающий принцип международного права. По смыслу Декларации о принципах международного права и Хельсинкского акта 1975 года каждое государство имеет право на обеспечение своей безопасности, не нанося ущерба безопасности других государств. Как представляется, данные права и обязанности, вытекающие из суверенитета, также в полной мере применимы к глобальному информационному пространству. Проявлением суверенного равенства государств является иммунитет каждого из них от юрисдикции другого государства. Однако пространственные пределы государственного суверенитета в сети Интернет в настоящее время не определены.

В современных условиях, когда угрозы безопасности, связанные с развитием ИКТ выходят на передний план политической повестки на мировом и национальном уровнях[246], проблематика обеспечения

[245] Зиновьева Е.С., Шитьков С.В. Цифровой суверенитет в практике международных отношений // Международная жизнь. 2021. № 3.
[246] Зиновьева Е.С. Международная информационная безопасность: проблемы многостороннего и двустороннего сотрудничества. М. МГИМО, 2021

суверенитета в цифровой сфере привлекает не только академическое внимание, но и прикладное.

При этом на современном этапе, когда тенденция к формированию многополярного мира сопровождается нарастающей международной конфликтностью, принцип государственного суверенитета играет важную роль. Как отметил Президент В.В. Путин, сегодня речь идет о переходе к «многополярному миру, основанному на подлинном суверенитете народов и цивилизаций»[247]. Директор департамента внешнеполитического планирования Д.В. Дробинин отмечает, что обеспечение технологического суверенитета – стратегическая задача государства, претендующего на самостоятельную роль в наступившую высококонкурентную эпоху[248]. При этом цифровой суверенитет является необъемлемой и важнейшей составляющей технологического суверенитета.

Дальнейшее развитие и уточнение принцип суверенного равенства государств получил в Декларации о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами 1975 года. Согласно Декларации, концепция суверенного равенства включает в себя следующие элементы:

1) государства юридически равны;

2) каждое государство пользуется правами, присущими полному суверенитету;

3) каждое государство обязано уважать правосубъектность других государств;

4) территориальная целостность и политическая независимость государства неприкосновенны;

---

[247] Путин заявил о начале слома мира с американскими правилами после старта СВО // Известия. 07.08.2022. URL: https://iz.ru/1361500/2022-07-07/putin-zaiavil-o-nachale-sloma-mira-s-amerikanskimi-pravilami-posle-starta-svo (дата обращения 23.04.2025)

[248] Дробинин А. Ю. Уроки истории и образ будущего: размышления о внешней политике России //Международная жизнь. – 2022. – Т. 3.

5) каждое государство имеет право свободно выбирать и развивать свои политические, социальные, экономические и культурные системы;

6) каждое государство обязано выполнять полностью и добросовестно свои международные обязательства и жить в мире с другими государствами.

Заключительный акт Хельсинской Конференции 1975 года указывает на ряд других элементов, в том числе: свободу и политическую независимость, право устанавливать свои законы и административные правила, определять и осуществлять по своему усмотрению отношения с другими странами в соответствии с международным правом, участвовать в международных организациях, двусторонних и многосторонних международных договорах, право на нейтралитет.

Авторитетный российский исследователь А.А. Стрельцов отмечает, что ИКТ-среда как объект международных отношений представляет собой юридическую фикцию, которая заключается в том, что соответствующая совокупность устройств и средств связи, локальных вычислительных сетей, информационных систем, существующих в пространстве цифровых идентификаторов и протоколов их взаимодействия, а также субъектов обеспечения согласованного функционирования выделенных устройств, средств, сетей и систем в составе глобальной ИКТ-среды, рассматривается как составляющая территории государства, что позволяет распространить на ИКТ-среду понятия «суверенитет государства» и «юрисдикция государства»[249]. Ряд технических возможностей современных цифровых технологий осложняет однозначное соотнесение данных, программного обеспечения и др. с территорией определенного государства и не позволяет дать конкретного определения этой категории. Демилитаризация

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

цифровых границ государства также затруднена в условиях значительного объема трансграничных данных[250].

Трансгранично передаваемая информация регулируется в рамках еще одной отрасли международного публичного права – права массовой информации. В частности, распространяемая трансгранично информация не должна представлять собой вмешательство во внутренние дела суверенных государств. При этом независимость средств массовой информации не должна отрицать принцип международной ответственности государств за деятельность своих национальных средств массовой информации на трансграничном уровне. Провозглашенное во Всеобщей декларации прав человека 1948 года право искать, получать и распространять информацию и идеи независимо от государственных границ (ст. 19) не является абсолютным и ограничено правом государства в законодательном ограничении свободы информации для охраны национальной безопасности, здоровья и нравственности населения, провозглашенным в ст. 19 Международного пакта о гражданских и политических правах 1966 года. Как представляется, подобный подход в полной мере применим к современным цифровым СМИ и, более того, может быть основой для обсуждения на международном уровне международных норм и правил, регламентирующих деятельность глобальных цифровых платформ и ИТ-гигантов. Однако данные нормы права не дают ответа на вопрос о проведении границ государства в цифровой среде.

Таким образом, в международном праве уже заложены основы для дальнейшего развития принципа государственного цифрового суверенитета в соотнесении с принципом невмешательства во внутренние дела и предотвращении международных конфликтов.

---

[250] Доклад о цифровой экономике. «Международные потоки данных и развитие: кому служат потоки данных. UNCTAD/DER/2021. Женева, 2021 г. (обзор)

Однако в последние годы расширяется практика вторжения в информационное пространство различных стран как со стороны других государств, так и со стороны негосударственных акторов, причем мотивы такого вмешательства (сбор информации, воздействие на информационную политику страны, нарушение работы информационных инфраструктур) достаточно сложно определить. В литературе подобная ситуация получила название «цифровой дилеммы безопасности» и широко представлена в трудах российских и зарубежных авторов[251]. В целом подобная ситуация способствует дестабилизации международной безопасности, усиливая взаимное недоверие государств и подталкивая их к односторонним действиям в информационной сфере, что, в свою очередь, актуализирует необходимость международного сотрудничества в области информационной безопасности, основанного на принципах уважения государственного суверенитета.

Несмотря на отдельные правовые лакуны и терминологические разночтения, цифровой суверенитет уже стал неотъемлемой частью политической и академической риторики, различные трактовки и подходы к данной категории находят отражение в официальных документах государств и международных организаций.

Российская Федерация первой обратила внимание международного сообщества на значимость обеспечения информационного суверенитета в контексте международной информационной безопасности. Россия с 1998 года продвигала на международной арене инициативу в области выработки правил ответственного поведения государств в области международной информационной безопасности, ориентировала международное сообщество на предотвращение информационных угроз в военно-

[251] Dunn Cavelty M. Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities //Science and engineering ethics. – 2014. – Т. 20. – P. 701-715.; Зиновьева Е. С. Киберсдерживание и цифровая дилемма безопасности в американском экспертном дискурсе //Международные процессы. – 2019. – Т. 17. – №. 3. – С. 51-65.

политической, террористической и преступной плоскостях при учете принципов равноправия и суверенного равенства государств[252].

В международных документах одно из первых упоминаний суверенитета государств в цифровой сфере было в итоговых документах Всемирной встречи на высшем уровне по вопросам информационного общества, которая прошла под эгидой ООН (женевский этап – в 2003 г., а тунисский – в 2005 г.). Тунисская программа для информационного общества 2005 года зафиксировала, что «политические полномочия по решению вопросов государственной политики, связанных с Интернетом, являются суверенным правом государств»[253]. Это был важный шаг к признанию того, что государственный суверенитет и права и обязанности из него вытекающие применимы к глобальному информационному пространству[254].

Однако в широкой практике международных отношений вопросы к обеспечению цифрового суверенитета стали привлекать пристальное внимание позднее. Важную роль сыграли события «арабской весны», в которой большое значение имели программы цифровой дипломатии США, опиравшиеся на использование социальных сетей, базирующихся в этой стране. Многие государства стали рассматривать их деятельность как вмешательство во внутренние дела и нарушение суверенитета. Кроме того, на этот же период приходятся атаки вируса «Stuxnet» на АСУП ТП АЭС в Иране, выведшие из строя АЭС в Натанзе, что дополнительно актуализировало стремление государств обеспечить свою информационную безопасность и укрепить границы в цифровом пространстве.

---

[252] Международная информационная безопасность: подходы России / Под ред А.В. Крутских, Е.С. Зиновьевой. М. МГИМО, 2021.

[253] Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-05/TUNIS/DOC/6(Rev.1)-R. Тунисская программа для информационного общества. – 18 ноября 2005 года.

[254] Цифровые международные отношения / Под ред Е.С. Зиновьевой, С.В. Шитькова. М.: Аспект-Пресс. 2023.

Весомый вклад в международно-правовое закрепление и развитие категории цифрового суверенитета внесла работа групп правительственных экспертов ООН (далее – ГПЭ) по международной информационной безопасности, которые неоднократно созывались для обсуждения международного сотрудничества в области предотвращения цифровых угроз. В докладе ГПЭ за 2015 год фиксируется, что на поведение государств в информационном пространстве распространяется государственный суверенитет и международные нормы, вытекающие из принципа государственного суверенитета[255]. Согласно документу, суверенитет также распространяется на юрисдикцию государств над ИКТ-инфраструктурой на их территории1. Схожие формулировки представлены и в других докладах ГПЭ.

На конец 2010-х - начало 2020-х годов приходится значительный рост объема данных, передаваемых посредством Интернета и других глобальных сетей, что позволило повысить экономический потенциал их использования и вывело процессы цифровой трансформации на новый уровень. Широкую популярность получила метафора «данные – это новая нефть», а во многих государствах были усилены инициативы в области обеспечения безопасности и контроля над данными, в целом вписывающиеся в контекст общей политики в области укрепления цифрового суверенитета.

В России в ноябре 2019 года был принят Закон о «суверенном Интернете» (неформальное название Федерального закона от 01.05.2019 №90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации»), который сформировал правовую базу для централизованного управления Интернетом в государственных границах.

[255] Доклад Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (Резолюция ГА ООН A/70/174 от 22 июля 2015 г.)

Кроме того, начало СВО России на Украине и обострение отношений со странами Запада актуализировали и форсировали политику России в области цифрового суверенитета. В 2022 году на территории России была запрещена деятельность ряда западных ИТ-платформ, что стало еще одним шагом на пути к укреплению цифрового суверенитета. При этом обеспечение суверенитета возможно «при открытости к самому широкому взаимообогащающему равноправному международному сотрудничеству и может гарантировать устойчивое развитие России и достойное место нашей страны в многополярном миропорядке».

Цифровой суверенитет – концепция, получившая широкое распространение в дискурсе, связанном с национальной безопасностью, управлением и международными отношениями в цифровую эпоху. Термин возник в связи с растущей обеспокоенностью по поводу контроля, осуществляемого транснациональными технологическими компаниями, базирующимися преимущественно в США и Китае, которые доминируют в глобальных потоках данных и инфраструктуре[256]. Европейская комиссия особенно активно выступала за цифровой суверенитет как средство восстановления контроля над данными и снижения зависимости от неевропейских технологий[257].

Несмотря на то, что цифровой суверенитет – это тоже суверенитет, он имеет ряд весомых отличий от традиционной концепции и представляет собой некую его адаптированную к уникальным вызовам и обстоятельствам, порожденным цифровой эпохой, версию.

Традиционный суверенитет, как уже было сказано, отличается двумя критическими в данном контексте признаками: территориальной

---

[256] Lambach D., Monsees L. Beyond sovereignty as authority: the multiplicity of European approaches to digital sovereignty / D. Lambach, L. Monsees – Текст : электронный. // Global Political Economy. – 2024. – С. 1-18. – URL: https://www.researchgate.net/publication/368837486_Beyond_Sovereignty_as_Authority_The_Multiplicity_of_European_Approaches_to_Digital_Sovereignty (дата обращения: 15.03.2024 г.).

[257] European, Commission Commission presents new initiatives for digital infrastructures of tomorrow / Commission European. – Текст : электронный // European Commission – URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_941 (дата обращения: 17.03.2024).

целостностью и политической независимостью государства, охватывающую способность регулировать внутренние дела и определять внешнюю политику. В свою очередь цифровой суверенитет имеет ряд существенных отличий от традиционного суверенитета.

Во-первых, в отличие от традиционного суверенитета, который четко очерчивает физические границы, цифровой суверенитет имеет дело с туманной и безграничной природой киберпространства. Оно динамично и поэтому быстрее других сфер внедряет инновации.

Во-вторых, в то время как традиционный суверенитет подчеркивает независимость от внешних сил, цифровой суверенитет должен бороться с реальностью глобальной взаимосвязанности и доминированием транснациональных корпораций в области технологий и управления данными. Эта зависимость осложняет попытки установить полный контроль над цифровыми ресурсами[258].

И в-третьих, в Интернете действуют совершенно другие социально-политическим правила[259]. Там нет политических институтов или государственных границ, нет людей: есть их цифровая «копия». Из-за анонимности и сложности привлечения к ответственности, отсутствия иерархии правила взаимодействия значительно отличаются от принятых в реальном мире.

В связи с этим возникают сложные вопросы, касающиеся регулирования, определения юрисдикции, контроля над данными, конфиденциальности и безопасности[260] и в целом определения концепции «цифрового суверенитета».

---

[258] Куманов Д. С. Цифровой суверенитет как инструмент национальной кибербезопасности / Д. С. Куманов – Текст : электронный. // Руссконгресс [Офиц. сайт]. – URL: https://roscongress.org/materials/tsifrovoy-suverenitet-kak-instrument-natsionalnoy-kiberbezopasnosti/ (дата обращения: 15.03.2024 г.).

[259] Choucri N., Goldsmith D. Lost in cyberspace: Harnessing the Internet, international relations, and global security / N. Choucri , D. Goldsmith – Текст : электронный. // Bulletin of the Atomic Scientists. – 2012. – Т. 68. – №. 2. – С. 70-77. – URL: https://www.researchgate.net/publication/254080130_Lost_in_cyberspace_Harnessing_the_Internet_international_relations_and_global_security (дата обращения: 15.03.2024 г.).

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

Трактовка цифрового суверенитета значительно варьируется в различных геополитических, культурных и технологических контекстах, отражая национальные приоритеты и традиции. Кроме того, есть определенного рода концептуальная путаница, поскольку информационный суверенитет, киберсуверенитет, Интернет-суверенитет и, наконец, сам цифровой суверенитет выступают, как правило, взаимозаменяемыми категориями. Однако представляется возможным выделить несколько направлений мысли в определении данного понятия.

Мюллеру в статье «В защиту чистого суверенитета в киберпространстве» отвечает Кевин Хеллер[261]. Он утверждает, принцип суверенитета применим и к киберпространству, поскольку государства должны иметь возможность осуществлять контроль над кибердеятельностью на своей территории, подобно традиционному территориальному суверенитету. Хеллер полагает, что любая несанкционированная кибер-операция, затрагивающая кибер-инфраструктуру другого государства, должна считаться нарушением суверенитета[262].

Бенджамин Браттон привнес в дискуссию о суверенитете еще одно измерение, используя концепцию «Stack». Stack – это глобальная вычислительная инфраструктура, которая нарушают традиционные представления о Вестфальском суверенитете. Вестфальская система - взаимодействие территориально определенных государств, у Stack принципиально иные механизмы развития, поэтому традиционный суверенитет в данном случае не применим.

Европейский исследователь Лучиано Флориди делает акцент на данных в цифровом суверенитете и трактует данный концепт как

---

https://www.researchgate.net/publication/343611573_The_Fight_for_Digital_Sovereignty_What_It_Is_and_Why_It_Matters_Especially_for_the_EU (дата обращения: 15.03.2024 г.).

[261] Heller K. J. In defense of pure sovereignty in cyberspace. / K. J. Heller – Текст : электронный. // SSRN. – 2021. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4081180 (дата обращения: 15.03.2024 г.).

[262] Там же.

способность государства управлять и контролировать цифровые данные своих граждан и учреждений, включая регулирование цифровых рынков, защиту личной информации, а также способность самостоятельно устанавливать и обеспечивать соблюдение правил, касающихся цифровой экономики[263]. Более того, цифровой суверенитет затрагивает не только специалистов и или активных пользователей Сети, а всех граждан, включая тех, кто не использует цифровые технологии активно. Флориди также отмечает, что борьба за цифровой суверенитет характеризуется асимметричным столкновением между государствами и корпорациями. Корпорации обладают способностью внедрять инновации и контролировать цифровые активы, в то время как государства обладают регулятивными полномочиями. Эти отношения динамичны и сложны, оба субъекта зависят друг от друга и влияют друг на друга.

Ряд западных ученых трактуют цифровой суверенитет исключительно как геополитический или националистический термин: автократические страны трактуют цифровой суверенитет как расширение государственного контроля над всеми цифровыми и информационными сферами. По мнению Мартина Калудиса[264] подобные страны используют цифровой суверенитет для оправдания строгого внутреннего регулирования и изоляционистской внешней политики, что часто приводит к форме цифровой автаркии или самодостаточности. Этот подход включает в себя технологическую изоляцию и строгий контроль над цифровой деятельностью граждан, направленный на поддержание и укрепление автократического правления. Джулия Поль и Торстен Тиль также считают, что цифровой суверенитет является политической и

[263] Floridi L. The fight for digital sovereignty: What it is, and why it matters, especially for the EU / L. Floridi – Текст : электронный. // Philosophy & technology. – 2020. – Т. 33. – С. 369-378. – URL: https://www.researchgate.net/publication/343611573_The_Fight_for_Digital_Sovereignty_What_It_Is_and_Why_It_Matters_Especially_for_the_EU (дата обращения: 15.03.2024 г.).

[264] Kaloudis M. Digital sovereignty–European Union's action plan needs a common understanding to succeed / M. Kaloudis – Текст : электронный. // History Compass. – 2021. – Т. 19. – №. 12. – С. 1-12. – URL: https://www.researchgate.net/publication/356271260_Digital_sovereignty-European_Union's_action_plan_needs_a_common_understanding_to_succeed (дата обращения: 15.03.2024 г.).

дискурсивной категорией, а не строго юридической или организационной концепцией, и его трактовка в значительной степени зависит от политической системы: в авторитарных государствах укрепление цифрового суверенитета предполагает «не только активное преодоление зависимости, но и создание инфраструктур для контроля и (возможно) манипулирования»[265].

Юкка Руохонен[266] придерживается мнения о том, что сначала нужно решить сложности и противоречия, возникающие при попытке применить традиционную, территориальную концепцию суверенитета к нетерриториальной, безграничной природе цифровых пространств. Руохонен критикует несоответствие классических определений суверенитета цифровому миру, подчеркивая их неотъемлемые различия, и выступает за переоценку и возможное переосмысление того, что означает суверенитет во все более взаимосвязанном цифровом мире. Однако автор не дает окончательного определения цифрового суверенитета, поскольку пока не будут решены несоответствия и проблемы, возможны концептные натяжки.

Зиновьева Е. С. определяет цифровой суверенитет в широком смысле как независимость государства в цифровой сфере, позволяющую ему автономно проводить информационную политику внутри страны и на международном уровне. Он включает в себя контроль над коммуникационной инфраструктурой и Интернетом в пределах национальных границ, независимость программного обеспечения и платформенную экономику, в том числе национальные поисковые системы, социальные сети и почтовые сервисы. Важным компонентом современного цифрового суверенитета является суверенитет данных.

---

[265] Pohle J., Thiel T. Digital sovereignty / J. Pohle, T. Thiel. – Текст : электронный. // Internet Policy Review. – 2020. - 9(4). – URL: https://ssrn.com/abstract=4081180 (дата обращения: 15.03.2024 г.).

[266] Ruohonen J. The treachery of images in the digital sovereignty debate / J. Ruohonen – Текст : электронный. // Minds and machines. – 2021. – Т. 31. – №. 3. – С. 439-456. – URL: https://link.springer.com/article/10.1007/s11023-021-09566-7 (дата обращения: 15.03.2024 г.).

Кроме того, эффективный цифровой суверенитет требует надежной правовой базы для регулирования цифрового взаимодействия и активного участия в международном сотрудничестве для формирования норм и принципов в этой области[267].

Коллектив авторов в статье «Категория «цифрового суверенитета» в современной мировой политике» тоже придерживается подобной точки зрения с некоторыми уточнениями[268]. Внешний суверенитет предполагает взаимодействие суверенных пространств, которые внутри стран будут образовываться с помощью системы коллегиального управления. Данная система будет создана при сотрудничестве государства и национальных негосударственных акторов, полномочия государства будут определяться сложившимися социально-культурными традициями.

Ряд российских[269] и китайских[270] исследователей также придерживается

трактовки цифрового суверенитета как независимости государства проводить собственную политику внутри и вне страны от своего имени с

---

[267] Зиновьева Е.С., Игнатов А.А. «Цифровой суверенитет» в повестке объединения БРИКС / Е.С. Зиновьева, А.А. Игнатов – Текст : электронный. // РСМД. – 2024. – URL: https://russiancouncil.ru/analytics-and-comments/analytics/tsifrovoy-suverenitet-v-povestke-obedineniya-briks/?sphrase_id=137399354 (дата обращения: 15.03.2024 г.).

[268] Ребро О., Гладышева А., Сучков М., Сушенцов А. Категория «Цифрового суверенитета» в современной мировой политике вызовы и возможности для России / О. Ребро, А. Гладышева, М. Сучков, А. Сушенцов – Текст : электронный. // Международные процессы. – 2021. – Т. 19. – №. 4. – С. 47-67. – URL: https://www.intertrends.ru/jour/article/view/266?locale=ru_RU (дата обращения: 15.03.2024 г.).

[269] Виноградова Е. В., Полякова Т. А. О месте информационного суверенитета в конституционно-правовом пространстве современной России / Е. В. Виноградова, Т. А. Полякова – Текст : непосредственный. // Правовое государство: теория и практика. – 2021. – №. 1 (63). – С. 32-49.

Володенков С. В. Феномен цифрового суверенитета современного государства в условиях глобальных технологических трансформаций: содержание и особенности / С. В. Володенков – Текст : непосредственный. // Журнал политических исследований. – 2020. – Т. 4. – №. 4. – С. 3-11.

Кочетков А. П., Маслов К. В. Цифровой суверенитет как основа национальной безопасности России в глобальном цифровом обществе / А. П. Кочетков, К. В. Маслов. – Текст : непосредственный. // Вестник Московского университета. Серия 12. Политические науки. – 2022. – №. 2. – С. 31-45.

Ромашкина Н. П. Информационный суверенитет в современную эпоху стратегического противоборства / Н. П. Ромашкина – Текст : непосредственный. // Информационные войны. – 2019. – №. 4. – С. 14-19.

[270] Jiang M. Authoritarian informationalism: China's approach to Internet sovereignty / M. Jiang – Текст : электронный. // SAIS Rev. Int'l Aff. – 2010. – Т. 30. – С. 71. – URL: https://www.researchgate.net/publication/236760988_Authoritarian_Informationalism_China's_Approach_to_Internet_Sovereignty (дата обращения: 15.03.2024 г.).

Shen Y. Cyber sovereignty and the governance of global cyberspace / Y. Shen – Текст : электронный. // Chinese Political Science Review. – 2016. – Т. 1. – С. 81-93.– URL: https://www.researchgate.net/publication/296632410_Cyber_Sovereignty_and_the_Governance_of_Global_Cyberspace (дата обращения: 15.03.2024 г.).

акцентом на важности реагирования на угрозы информационной безопасности и контроля этой сферы.

Отдельные ученые продолжают исследовать нюансы информационного суверенитета. А.В. Россошанский описывает информационный суверенитет как возможность и стремление политического субъекта создавать, распределять и использовать информацию согласно своим политическим интересам, а также применять ее как инструмент для политического влияния в объемах и масштабах, которые соответствуют его настоящим и стратегическим целям[271].

А.П. Кочетков и К.В. Маслов также разделяют цифровой и информационных суверенитеты: информационный суверенитет подразумевает контроль информационно-телекоммуникационных средств и систем государства, в свою очередь, цифровой суверенитет - контроль и защиту самой информации, цифровых ресурсов и цифровых платформ.

Из вышеуказанного следует, что в научных кругах устоявшегося определения цифрового суверенитета нет. Также он не находит однозначной трактовки на государственном уровне. Если Россия и Китай активно развивают эту концепцию в рамках своих юрисдикций, то США, например, трактуют этот термин с негативной точки зрения[272]. Декларируется, что цифровой суверенитет может привести к балканизации глобального Интернета, создавая барьеры на пути информационных потоков и потенциально приводя к разделению цифрового ландшафта[273]. Фрагментация может подорвать глобальную совместимость сетей, что

---

[271] Россошанский А. В. Информационная составляющая политического суверенитета / А. В. Россошанский – Текст : электронный. // Известия Саратовского университета. Новая серия. Серия Социология. Политология. – 2011. – Т. 11. – №. 4. – С. 88-92. – URL: https://cyberleninka.ru/article/n/informatsionnaya-sostavlyayuschaya-politicheskogo-suvereniteta (дата обращения: 15.03.2024 г.).

[272] Кутюр С., Софи Т. Что означает понятие» суверенитет» в цифровом мире? / С. Кутюр, Т. Софи – Текст : электронный. // Вестник международных организаций: образование, наука, новая экономика. – 2020. – Т. 15. – №. 4. – С. 48-69.– URL: https://www.researchgate.net/publication/349406229_Cto_oznacaet_ponatie_suverenitet_v_cifrovom_mire (дата обращения: 15.03.2024 г.).

[273] Mueller M. L. Against sovereignty in cyberspace / M. L. Mueller – Текст : непосредственный. // International studies review. – 2020. – Т. 22. – №. 4. – С. 779-801.

скажется на мировой торговле и коммуникациях[274]. К более подробному рассмотрению национального аспекта цифрового суверенитета будет необходимо вернуться позже.

Государственная власть в киберпространстве в первую очередь зависит от понятия юрисдикции, которая традиционно связана с географическими границами. При рассмотрении цифрового суверенитета важно также обратить внимание на концепции суверенитета данных и технологического суверенитета. Суверенитет данных – это концепция, согласно которой цифровые данные обрабатываются в соответствии с требованиями той страны, в которой они собираются или обрабатываются. Этот принцип гарантирует, что данные, независимо от места их физического хранения, подчиняются законодательным рамкам и нормам страны, откуда они происходят или где проживают их субъекты[275].

Основная идея суверенитета данных заключается в том, что государство осуществляет контроль и юридическую власть над данными на своей территории. Этот контроль охватывает хранение, передачу и обработку данных, обеспечивая соблюдение национального законодательства, особенно в отношении защиты данных, конфиденциальности и безопасности[276]. Ярким примером этих требований является принятый Европейским союзом Общий регламент по защите данных (GDPR).

В эпоху массовых утечек данных и киберугроз контроль над тем, как данные обрабатываются в пределах национальных границ, имеет решающее значение для защиты конфиденциальной информации,

---

[274] Chander A., Lê U. P. Data nationalism / A. Chander, U. Lê – Текст : непосредственный. //Emory LJ. – 2014. – Т. 64. – С. 677.

[275] Floridi L. The fight for digital sovereignty: What it is, and why it matters, especially for the EU / L. Floridi – Текст : электронный. // Philosophy & technology. – 2020. – Т. 33. – С. 369-378. – URL: https://www.researchgate.net/publication/343611573_The_Fight_for_Digital_Sovereignty_What_It_Is_and_Why_It_Matters_Especially_for_the_EU (дата обращения: 15.03.2024 г.).

[276] Кутюр С., Софи Т. Что означает понятие» суверенитет» в цифровом мире? / С. Кутюр, Т. Софи – Текст : электронный. // Вестник международных организаций: образование, наука, новая экономика. – 2020. – Т. 15. – №. 4. – С. 48-69. – URL: https://www.researchgate.net/publication/349406229_Cto_oznacaet_ponatie_suverenitet_v_cifrovom_mire (дата обращения: 15.03.2024 г.).

связанной с национальной безопасностью, экономической стабильностью и безопасностью граждан[277].

В выступлении на ПМЭФ-2022 Президент РФ В.В. Путин подчеркнул определяющую роль технологического суверенитета в политике России: «...сквозной, объединяющий нашу работу принцип развития – это достижение настоящего технологического суверенитета, создание целостной системы экономического развития, которая по критически важным составляющим не зависит от иностранных институтов»[278].

Концепция технологического суверенитета привлекает все больше внимания в политических и научных кругах, поскольку государства сталкиваются с проблемами, вызванными глобальной цифровой взаимосвязанностью, доминированием транснациональных технологических компаний и стратегической уязвимостью, связанной с иностранным контролем над технологиями.

Технологический суверенитет тесно связан с национальной безопасностью и экономической независимостью. Он подчеркивает способность страны самостоятельно разрабатывать, поддерживать и контролировать ключевые технологии без чрезмерной зависимости от внешних организаций[279]. Такая автономия рассматривается как ключ к сохранению целостности, конфиденциальности и доступности данных, что является одной из главных задач в цифровую эпоху[280].

---

[277] Lambach D., Monsees L. Beyond sovereignty as authority: the multiplicity of European approaches to digital sovereignty / D. Lambach, L. Monsees // Global Political Economy. – 2024. – P. 1-18. – URL: https://www.researchgate.net/publication/368837486_Beyond_Sovereignty_as_Authority_The_Multiplicity_of_European_Approaches_to_Digital_Sovereignty (дата обращения: 15.03.2024 г.).

[278] Путин: нужно достичь независимого от зарубежных институтов технологического суверенитета // ТАСС. 17.08.2022.URL: https://tass.ru/ekonomika/14954311

[279] Lambach D., Monsees L. Beyond sovereignty as authority: the multiplicity of European approaches to digital sovereignty / D. Lambach, L. Monsees – Текст : электронный. // Global Political Economy. – 2024. – С. 1-18. – URL: https://www.researchgate.net/publication/368837486_Beyond_Sovereignty_as_Authority_The_Multiplicity_of_European_Approaches_to_Digital_Sovereignty (дата обращения: 15.03.2024 г.).

[280] Mueller M., Schmidt A., Kuerbis B. Internet security and networked governance in international relations / M. Mueller, A. Schmidt, B. Kuerbis – Текст : электронный. // International Studies Review. – 2013. – Т. 15. – №. 1. – С. 86-104. – URL:

Несколько громких инцидентов, связанных с цепочками поставок телекоммуникационного оборудования и программных платформ, подчеркнули стратегическую важность технологического суверенитета. Например, споры вокруг использования оборудования Huawei в национальных сетях 5G подчеркивают геополитические аспекты технологической зависимости[281].

Хотя стремление к технологическому суверенитету стратегически оправдано, оно сталкивается с рядом проблем: стремление к полной технологической самодостаточности может привести к неэффективности и снизить конкурентоспособность национальных отраслей на мировом рынке. Кроме того, глобальный характер цепочек поставок технологий делает невозможным достижение абсолютного технологического суверенитета для большинства стран[282].

Технологический суверенитет остается сложной и развивающейся концепцией из-за необходимости балансировать национальную безопасность и национальные экономические интересы с реальностью технологической взаимозависимости. Поскольку технологии продолжают развиваться, стратегии достижения технологического суверенитета должны быть динамичными и адаптируемыми к цифровым угрозам и возможностям, которыми они стремятся управлять.

Характеристики киберпространства и цифровых технологий, такие как их трансграничный характер, часто проявляются при рассмотрении вопросов цифрового суверенитета, суверенитета данных и технологического суверенитета. Это неизбежно указывает на важность

---

https://www.researchgate.net/publication/264346180_Internet_Security_and_Networked_Governance_in_International_Relations (дата обращения: 15.03.2024 г.).

[281] Гемуева К. А. Huawei в странах ЕС: проблема участия в развитии сетей 5G / К. А. Гемуева– Текст : электронный. // Научно-аналитический вестник Института Европы РАН. – 2020. – №. 3. – С. 75-81. – URL: https://cyberleninka.ru/article/n/huawei-v-stranah-es-problema-uchastiya-v-razvitii-setey-5g (дата обращения: 15.03.2024 г.).

[282] Aaronson S. A. What are we talking about when we talk about digital protectionism? / S. A. Aaronson – Текст : электронный. // World Trade Review. – 2019. – Т. 18. – №. 4. – С. 541-577. – URL: https://www.researchgate.net/publication/326860989_What_Are_We_Talking_about_When_We_Talk_about_Digital_Protectionism (дата обращения: 15.03.2024 г.).

рассмотрения существующих подходов к международному регулированию этих вопросов.

Однако на международном уровне управление, например, данными сопряжено с многочисленными трудностями и проблемами, в первую очередь из-за сложного взаимодействия между глобальными потоками данных. Проблемы конфиденциальности и безопасности данных усугубляются различиями в национальном регулировании, что приводит к фрагментарному ландшафту, осложняющему международное сотрудничество, соблюдение требований и правоприменение.

Вывод по главе:

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[283].

[283] Ребро О., Гладышева А., Сучков М., Сушенцов А. Категория «Цифрового суверенитета» в современной мировой политике вызовы и возможности для России / О. Ребро, А. Гладышева, М. Сучков, А. Сушенцов – Текст : электронный. // Международные процессы. – 2021. – Т. 19. – №. 4. – С. 47-67. – URL: https://www.intertrends.ru/jour/article/view/266?locale=ru_RU (дата обращения: 15.03.2024 г.).

ГЛАВА 2. МИРОПОЛИТИЧЕСКАЯ КОНЦЕПТУАЛИЗАЦИЯ СОВРЕМЕННОЙ ЦИФРОВОЙ РЕВОЛЮЦИИ

2.1. Характеристики прорывных цифровых технологий Четвертой промышленной революции

2.1.1. Четвертая промышленная революция: цифровое измерение

Глобальная и повсеместная цифровая трансформация в экономической науке и в международных исследованиях концептуально осмысливается с позиций теории Четвертой промышленной революции (также используется вариант перевода – Индустрия 4.0), которая в значительной степени связана с президентом Всемирного экономического форума Клаусом Швабом. В 2016 году он опубликовал одноименную книгу, получившую высокие показатели цитирования и широкую академическую узнаваемость[284]. Термин «Четвертая промышленная революция» зародился раньше, еще в 2011 году в Германии на промышленной ярмарке в Ганновере, где демонстрировались достижения автоматизации производства; однако популярность он приобрел благодаря данной публикации. Согласно подходу Шваба, Четвертая промышленная революция представляет собой трансформационный период, характеризующийся слиянием физических, цифровых и биологических технологий, причем с точки зрения темпов развития и масштаба эти изменения носят исторический характер. Новая промышленная революция коренным образом изменяет экономику, политику и общественные структуры, прежде всего за счет развития цифровых технологий. На международному уровне технологические сдвиги в рамках революции

[284] Шваб К. Четвертая промышленная революция. М., 2017.

вносят значительные изменения в динамику власти, суверенитета, безопасности и глобального управления. Масштаб и глубина трансформаций позволяет изучать данный этап общественного развития в категориях революции, под которой понимается радикальный слом общественного устройства[285].

Клаус Шваб выделяет следующие особенности Четвертой промышленной революции, основанной на киберфизических системах, которые отличают ее от предшествующих, связанных с развитием парового двигателя, электричества и компьютерных технологий:

Темпы развития. В отличие от предыдущих, эта промышленная революция развивается не линейными, а скорее экспоненциальными темпами. Это является порождением многогранного, глубоко взаимозависимого мира, в котором мы живем, а также того факта, что новая технология сама синтезирует все более передовые и эффективные технологии.

Широта и глубина. Она основана на цифровой революции и сочетает разнообразные технологии, обусловливающие возникновение беспрецедентных изменений парадигм в экономике, бизнесе, социуме в каждой отдельной личности. Она изменяет не только то, «что» и «как» мы делаем, но и то, «кем» мы являемся.

Системное воздействие. Она предусматривает целостные внешние и внутренние преобразования всех систем по всем странам, компаниям, отраслям и обществу в целом»[286]. В российской академической литературе данный феномен осмысливается с позиций фазового перехода

[285] Щульц Э. Э. Революция: к вопросу об определении термина //Социологические исследования. – 2014. – №. 4. – С. 132-142.
[286] Шваб К. Четвертая промышленная революция. М., 2017. С. 8.

цивилизации или шестого технологического уклада[287], однако, российские авторы часто цитируют Шваба в целом согласны с его выводами[288].

Шваб выделяет следующие прорывные технологии, лежащие в основе цифрового измерения Четвертной промышленной революции:

- Искусственный интеллект (ИИ): под искусственным интеллектом в самом широком смысли понимаются программные алгоритмы и системы, способные выполнять интеллектуальные и творческие задачи, и показывать результаты сопоставимые или превосходящие результаты человеческого интеллекта.
- Большие данные (Big Data): анализ и обработка больших объемов данных для принятия решений и прогнозирования, а также для разработки технологий машинного обучения и искусственного интеллекта.
- Интернет вещей (IoT): данная технология позволяет при помощи датчиков соединять физические объекты по сети, собирать и обмениваться данными (например, технологии «умного дома», «умных энергосетей», а также роботизированных портов, беспилотных автомобилей и пр. основаны на Интернете вещей).
- Блокчейн и технологии распределенных реестров: использование распределенных реестров для безопасных и прозрачных транзакций и передачи информации[289].

Это не исчерпывающий перечень, в число значимых и прорывных направлений технологического развития входят биотехнологии, трехмерная печать, нано-технологии, космические системы и спутниковая связь и ряд других. При этом развитие технологий создает не только

---

[287] Глазьев С.Ю. Великая цифровая революция: вызовы и перспективы для экономики XXI века URL: https://glazev.ru/articles/6-jekonomika/54923-velikaja-tsifrovaja-revoljutsija-vyzovy-i-perspektivy-dlja-jekonomiki-i-veka

[288] См. напр.: Маслов В. И., Лукьянов И. В. Четвертая промышленная революция: истоки и последствия //Вестник московского университета. Серия 27. Глобалистика и геополитика. – 2017. – №. 2. – С. 38-48; Байнев В. Четвертая промышленная революция как глобальный инновационный проект //Наука и инновации. – 2017. – Т. 3. – №. 169. – С. 38-41.; Сафрончук М. В. Цифровая поступь революции (четвертая промышленная революция и цифровая трансформация) //Экономика и управление: проблемы, решения. – 2017. – Т. 5. – №. 11. – С. 52-56 и др.

[289] Там же.

возможности, но и новые вызовы международной и национальной безопасности и государственному управлению, открывает новые возможности дипломатии и сотрудничества, при этом способствуя усилению взаимозависимости государств, изменению динамики власти на международной арене и, в конечном итоге, трансформируя международно-политическое наполнение категории государственного суверенитета.

Для более полного и глубокого понимания природы влияния Четвертной промышленной революции на эволюцию государственного суверенитета в XXI веке. Рассмотрим подробнее характеристики и международно-политическое влияние прорывных цифровых технологий.

2.1.2. Интернет вещей

Интернет вещей (IoT, от англ. Internet of Things) представляет собой технологическую парадигму, в рамках которой объекты физического мира оснащены встроенными датчиками, программным обеспечением и другими технологиями для обмена данными с другими устройствами и системами по сети. Интернет вещей – это система взаимосвязанных вычислительных устройств, которые могут собирать и передавать данные по беспроводной сети без участия человека[290].

Устройства Интернета вещей могут подключаться к сети и взаимодействовать друг с другом посредством различных протоколов и технологий связи, как национальных, так и зарубежных. Для сбора данных об окружающей среде, такие как температура, влажность, свет, движение и другие параметры, устройства оснащены различными датчиками. Собранные данные могут обрабатываться локально (на уровне устройства) или передаваться в облачные хранилища для дальнейшего анализа и принятия решений. Использование алгоритмов машинного обучения и

[290]Что такое интернет вещей? Определение и описание // Касперский, официальный сайт. URL: https://www.kaspersky.ru/resource-center/definitions/what-is-iot (дата обращения: 23.04.2025)

искусственного интеллекта позволяет устройствам интернета вещей анализировать данные и принимать автономные решения, улучшая функциональность и адаптивность системы в целом. На практике данная технология нашла свое воплощение в широком спектре приложений и высокотехнологичных решений, от умных городов до промышленных автоматизированных систем, например, умных заводов, умных портов, умных энергосетей. В социальной сфере ярким примером использования технологии является умное здравоохранение.

В рамках цифровой экономики Интернету вещей отводится важная роль – так, например, система умного транспорта невозможна без технологий интернета вещей, формирующего сеть устройств, способных собирать данные об автобусах, трамваях, машинах и обмениваться ими через интернет. IP-камеры, сенсоры и датчики позволяют автоматически контролировать всё, что связано с транспортными средствами: от их местоположения до контроля давления в шинах. В частности, в Китае в рамках цифровизации транспортной инфраструктуры в соответствии с «Планом информатизации транспорта в 13 пятилетке» Министерства транспорта КНР используется технология интернета вещей для реализации проектов цифровой железнодорожной инфраструктуры, цифровой автодорожной инфраструктуры, в том числе путем подключения высокоскоростных автодорог к информационно-коммуникационным сетям, цифровизация водного транспорта, в том числе в рамках проектов «умные порты и судоходство», «умное морское дело», «портовый город», «умный крейсер», «умный водный путь»[291]. Способность различных устройств и систем взаимодействовать и обмениваться данными является ключевым аспектом интернета вещей. Она позволяет интегрировать различные элементы связных процессов и за счет синергии повысить их общую экономическую эффективность.

[291] Ма Хуатэн, Мэн Чжоли, Ян Дели, Ван Хуалей. Цифровая трансформация Китая. М.: Альпина, 2019. С. 47-49

На уровне политики и государственного управления данные технологии находят отражение в создании умных городов. Умные города основаны на технологиях интернета вещей, включают в себя системы управления уличным освещением, транспортом, парковками, мониторингом окружающей среды и инфраструктурой. Значительная часть решений умного города реализована в Москве[292], где в рамках технологий управления городом можно выделить следующие технологические решения:

- Информационная система ситуационного центра, позволяющая координировать работу городских служб и принимать решения на основе объективных и проверенных данных;
- «Цифровой двойник» города Москвы – это точная копия столицы в виртуальной реальности со всеми зданиями, сооружениями, инженерными и подземными коммуникациями. Она помогает планировать строительство жилых, промышленных и социальных объектов, принимать управленческие решения и контролировать ход реализации значимых городских проектов;
- Инвестпортал – многофункциональный инструмент столичных инвестиций и реализации городских объектов на торгах для инвесторов, предпринимателей и физических лиц;
- Система видеонаблюдения, позволяющая выявить нарушения в области ЖКХ с помощью нейронных сетей[293].

В 2018 году Москва стала лидером в рейтинге умных городов ООН, а согласно рейтингу 2022 года заняла 6 место (на первом месте Берлин)[294].

---

[292] Василенко И. А. Москва-»Умный город»: основные направления и перспективы смарт-стратегии развития столицы //Власть. – 2019. – №. 3. – С. 91-95.

[293] Умный город. Мультимедийная экспозиция Москвы. ULR: https://smartcity.mos.ru (дата обращения: 24.05.2025)

[294] UN E-Government Survey 2022. The future of e-government. URL: https://desapublications.un.org/sites/default/files/publications/2022-09/Web%20version%20E-Government%202022.pdf (дата обращения: 24.05.2025)

Популярные решения в рамках умных городов включают в себя «умные энергосети», которые предполагают создание «цифровых двойников» электросетевого комплекса за счет внедрения единого информационного пространства. Цифровизация электросетей весьма популярна в странах ЕС, дополнительную динамику развития получило в условиях масштабного энергоперехода и растущего внимания к проблемам энергетической безопасности в регионе[295]. Умные энергосети в последние годы становятся все более распространенными и в странах Азии – в Сингапуре, Южной Корее, Японии, КНР[296]. В России также развиваются соответствующие технологии. Цифровая трансформация энергетики в Российской Федерации является одной из важных стратегических задач в рамках реализации национальной программы «Цифровая экономика»[297], «Концепции цифровой трансформации 2030»[298] и «Стратегии развития электросетевого комплекса России»[299]. Постоянное усложнение энергосистемы, значительные объемы обрабатываемой информации при необходимости обеспечения надежного энергоснабжения обуславливают активное внедрение цифровых технологий в электроэнергетику в России[300] в рамках проектов и программ, направленных на сохранение и укрепление цифрового и технологического суверенитета страны.

Расширяется применения Интернета вещей в медицине и здравоохранении. В здравоохранении возможно использование носимых

---

[295] Proedrou F. Are smart grids the key to EU energy security? //Research handbook on EU energy law and policy. – Edward Elgar Publishing, 2017. – С. 450-459.

[296] Brown M. A., Zhou S. Smart-grid policies: an international review //Advances in Energy Systems: The Large-scale renewable energy integration challenge. – 2019. – С. 127-147;

[297] Федеральная целевая программа «Цифровая экономика Российской Федерации» Утверждена распоряжением Правительства Российской Федерации 28 июля 2017. URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf

[298] Концепция Цифровая трансформация 2030. Россети. Москва, 2018. URL: https://www.rossetivolga.ru/i/files/2019/2/7/kontseptsiya_tsifrovaya_transformatsiya_2030.pdf

[299] Стратегия развития электросетевого комплекса Российской Федерации. Распоряжение от 03.04.2013 № 511 – р. URL: http://static.government.ru/media/acts/files/0001201304080048.pdf

[300] Салыгин В.И., Маркин А.С. Цифровая трансформация объектов электросетевого комплекса (зарубежный опыт) // Электроэнергия: передача и распределение. Журнал для специалистов электросетевого комплекса. 2022. № 1. С. 110 – 117.

устройств для мониторинга здоровья пациентов, телемедицины и интеллектуальных систем управления медицинским оборудованием.

Однако наиболее экономически значимой практической сферой применения Интернета вещей является промышленное производство. Промышленный интернет вещей включает системы мониторинга и управления производственными процессами, предиктивного обслуживания оборудования и оптимизации цепочек поставок. При этом промышленный интернет вещей обладает существенным потенциалом экономического роста – согласно оценкам АНО «Цифровая экономика», в 2023 году Интернет вещей обеспечивал рост от 0.3 до 0.8 % национальных ВВП генерировал триллионы накопленного вклада в мировую экономику[301]. В докладе «Цифровой экономики» отмечается, что развитие интернета вещей тесно взаимосвязано с технологиями 5G, граничных вычислений, обработки больших данных, искусственного интеллекта, промышленной автоматизации и робототехники. И здесь у России есть большой потенциал для реализации масштабных проектов цифрового суверенитетов: разработаны несколько протоколов передачи данных, эксплуатируются и внедряются собственные платформы промышленного интернета вещей для отраслевых предприятий, имеются опыт масштабных городских проектов видеоаналитики, крупные частные игроки развивают собственные сети связи интернета вещей федерального охвата[302].

Страны, активно внедряющие интернет вещей, могут существенно повысить свою экономическую конкурентоспособность. Это стимулирует глобальную гонку за лидерство в области технологий, страны стремятся создать благоприятные условия для инноваций и инвестиций в технологии Интернета вещей, а также укреплять свой технологический суверенитет в

---

[301] АНО «Цифровая экономика» проанализировала развитие интернета вещей в России и Мире. 04.12.2023 URL: https://d-economy.ru/news/ano-cifrovaja-jekonomika-proanalizirovala-razvitie-interneta-veshhej-v-rossii-i-mire/ (дата обращения: 24.05.2025)

[302] Интернет вещей. Развитие технологий и оценка возможностей перехода на отечественные решения // АНО «Цифровая экономика», 2023. – URL: https://files.data-economy.ru/Docs/IoT-5.pdf

данной области. Интернет вещей трансформирует глобальные цепочки поставок, позволяя более эффективно управлять логистикой и отслеживать товаров, что в свою очередь способствует снижению издержек и повышению прозрачности в международной торговле.

Однако с увеличением числа подключенных устройств в системах Интернета вещей возрастает уязвимость, прежде всего, вследствие кибератак. Однако помимо развития национальных решений в данной области, цифровой суверенитет предполагает также внимание к вопросам безопасности. Большое количество подключенных устройств увеличивает уязвимость систем Интернета вещей к кибератакам и утечкам данных. В силу того, что большинство систем интернета вещей представляют собой интеграцию множества различных систем и технологий, работающих на различных программных решениях и операционных системах, уязвимость возрастает. Значительная часть данных хранится в облачных хранилищах и передается трансгранично[303] (за исключением государств, реализующих программы цифрового и технологического суверенитета). Трансграничная природа технологии диктует необходимость международного сотрудничества в области кибербезопасности для разработки стандартов и практик защиты данных в сфере Интернета вещей (подробнее об актуальных проблемах международной информационной безопасности см. в пп. 2.2).

С целью защиты цифрового технологического суверенитета многие страны стремятся снизить свою зависимость от иностранных технологий, разрабатывая собственные решения в области интернета вещей. Таким образом, в сфере интернета вещей также наблюдается тенденция укрепления технологического и цифрового суверенитета.

Однако, по ряду вопросов необходимо и укрепление международного сотрудничества. Необходимость разработки и принятия

[303] Наимиот Д.Е., Сухомлин В.А. О кибербезопасности систем интернета вещей // Международный журнал открытых информационных технологий. 2023. № 2. С. 85 – 95.

глобальных стандартов для обеспечения интероперабельности и совместимости устройств интернета вещей требует координации на международном уровне и создания общих технических стандартов, протоколов безопасности и норм защиты данных. В этом процессе ключевую роль могут сыграть международные организации, прежде всего, Международный союз электросвязи (ITU), который становится ключевой площадкой в координации усилий по разработке глобальных стандартов и регулированию интернета вещей[304].

2.1.3. Технологии распределенных реестров

Технологии распределенных реестров представляют собой инновационный подход к хранению, управлению и защите данных, в котором информация записывается, обновляется и сохраняется на множестве устройств или узлов в сети. Использование технологий распределенных реестров обеспечивает децентрализацию хранения данных, что позволяет обеспечить защищенность (за счет шифрования для подтверждения транзакций), неизменность (за счет того, что текущее состояние блокчейна зависит от предыдущих операций) и прозрачность (за счет публичного распределенного хранения) [305].

В распределенных реестрах отсутствует единая точка контроля или отказа, что делает систему более устойчивой к атакам и сбоям, а также создает дополнительные преимущества с точки зрения безопасности хранимых данных. Технология распределенных реестров создает механизм доверия на базе алгоритмов взаимного признания. Для обеспечения безопасности и целостности данных используются криптографические методы. Записи в распределенном реестре являются

---

[304] ITU Internet of Things Global Standards Initiative. URL: https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx (дата обращения: 24.05.2025)

[305] Клечиков А.В., Пряников М.М., Чугунов А.В. Блокчейн-технологии и их использование в государственной сфере // International Journal of Open Information Technologies. -2017. - №12. - С. 124.

неизменяемыми – после того как данные записаны и подтверждены, они не могут быть изменены или удалены, что обеспечивает высокий уровень доверия и прозрачности.

Блокчейн (Blockchain) – это наиболее известный вид распределенных реестров, в котором данные организованы в цепочки блоков. Каждый блок содержит список транзакций, хэш предыдущего блока и временную метку. Блокчейн получил широкое распространение благодаря криптовалютам, таким как Биткойн и Эфириум. Еще одним примером являются консорциумные и частные реестры, которые предназначены для использования в закрытых сетях, где доступ к реестру ограничен определенной группой участников. Консорциумные реестры управляются несколькими организациями, а частные реестры контролируются одной организацией[306].

Технология блокчейн широко применяется во многих отраслях экономики. Чаще всего это цифровая валюта, международные платежи, выпуск ценных бумаг, цифровые активы, финансирование цепочки поставок, взаимное страхование, отслеживание грузопотоков. В логистике технологии распределенных реестров обеспечивают прозрачность и отслеживаемость товаров на всех этапах цепочки поставок, что способствует борьбе с контрафактной продукцией и повышению эффективности и скорости логистических процессов. Блокчейн также широко используется для создания управления цифровыми активами и создания децентрализованных финансовых платформ (DeFi)[307]. DeFi призваны создать аналог традиционных финансовых институтов, таких как банки, биржи, инвестиционные фонды и прочие, основанный на принципе децентрализации. Как правило, у проектов открытый исходный код, и во

[306] Там же.
[307] Jensen J. R., von Wachter V., Ross O. An introduction to decentralized finance (defi) //Complex Systems Informatics and Modeling Quarterly. – 2021. – №. 26. – С. 46-54.

всех процессах задействованы специальные механизмы на основе блокчейн-технологий[308].

В финансовой сфере блокчейн предоставляет возможности для создания децентрализованных систем управления идентичностью, что позволяет пользователям контролировать свои персональные данные и снижает риск кражи идентификационной информации. Более того, данная технология обладает существенным потенциалом для дедолларизации современной мировой экономики, укрепляя таким образом финансовый суверенитет стран мирового большинства. В качестве примеров можно привести проект платежной платформы BRICS Pay, основанной на технологиях распределенных реестров. Планируется, что в ближайшем будущем появится специальная облачная платформа, соединяющая национальные платёжные системы государств БРИКС, и будет разработан онлайн-кошелек с доступом к этим платёжным системам, а также мобильное приложение по аналогии с Apple Pay, которое можно устанавливать на смартфон и оплачивать покупки в любой из пяти стран группы БРИКС вне зависимости от валюты средств на счёте покупателя[309].

В целях государственного управления технологии распределенных реестров могут использоваться для создания безопасных и прозрачных систем электронного голосования, обеспечивая защиту от фальсификаций и повышение доверия к результатам выборов. На международном уровне распределенные реестры могут применяться для отслеживания международной помощи, управления ресурсами международных организаций[310].

Биткойн и другие криптовалюты стали важным элементом международных финансовых систем, предоставляя альтернативные

---

[308] Harvey C. R., Ramachandran A., Santoro J. DeFi and the Future of Finance. – John Wiley & Sons, 2021.

[309] Лосев А. BRICS Pay – единая платёжная система стран БРИКС // Валдай. 05.03.2019. URL: https://ru.valdaiclub.com/a/highlights/brics-pay/

[310] JIU/REP/2020/7 Blockchain applications n the United Nations system: towards a state of readiness. Report of the joint inspection unit. United Nations, Geneva 2017. URL: https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2020_7_english.pdf (дата обращения: 24.05.2025)

средства для проведения трансграничных платежей и инвестиций. В частности, в России в 2024 году Государственной думой был рассмотрен законопроект, признающий криптовалюту определённого типа – «обеспеченные стейблкоины» – цифровым финансовым активом (ЦФА) и разрешающий использовать её во внешнеторговой деятельности[311]. Смарт-контракты могут использоваться для автоматизации и обеспечения выполнения международных соглашений, таких как торговые договоры и соглашения о климате. В России смарт-контракты на блокчейн-платформах использует крупнейший банк Сбер для взаимодействия с клиентами[312]. В ноябре 2023 года «Сбер» реализовал первую в России сделку по предоставлению банковской гарантии, где обычный договор был заменен смарт-контрактом на блокчейн-платформе[313].

Одной из основных проблем блокчейна является ограниченная масштабируемость. С увеличением числа пользователей и транзакций возникают сложности с обработкой большого объема данных в реальном времени. Развитие блокчейна сталкивается с правовыми и регуляторными вызовами, связанными с защитой данных, соблюдением правопорядка и налоговым регулированием. Для успешного внедрения технологии необходимо обеспечить совместимость различных систем и стандартов, что требует разработки и принятия общих протоколов и интерфейсов на международном уровне.

Блокчейн широко используется в рамках различных проектов интернета вещей, в том числе в промышленности, логистике, торговле, Использование смарт-контрактов позволяет автоматизировать и безопасно проводить торговые операции, снижая транзакционные издержки и риски мошенничества. Это способствует укреплению экономических связей

---

[311]В Госдуму внесён законопроект об использовании криптовалюты для внешней торговли // Цифровая Россия. 31.01.2024
URL https://d-russia.ru/v-gosdumu-vnesjon-zakonoproekt-ob-ispolzovanii-kriptovaljuty-dlja-vneshnej-torgovli.html

[312]«Сбер» впервые реализовал сделку с применением смарт-контракта // РБК: 14.11.2023.
URL https://www.rbc.ru/crypto/news/65532c8d9a794783cf239a59?from=copy

[313] Там же.

между странами и регионами. В частности, данная система лежит в основе цифровой интеграции ЕАЭС[314].

Несмотря на высокую степень надежности, данные технологии также сталкиваются с угрозами безопасности. Несмотря на то, что биткоин – самый известный пример применения технологии, с ним также возникают проблемы безопасности. Такие инциденты, как кражи на крупнейшей в мире бирже биткоинов Mt. Gox в 2011 году или хакерская атака на биржу Bitfinex в 2016 году показали уязвимость технологии. В 2016 году самый крупный в мире на тот момент продукт краудфандинга на базе криптовалюты Эфириум подвергся хакерской атаке, которая привела к краже 60 млн. долларов[315]. Это актуализирует обсуждение вопросов информационной безопасности и финансового суверенитета применительно к криптовалютам.

Несмотря на широкий спектр преимуществ технологий распределенных реестров, в российской и международной литературе существует серьезная критика блокчейна. Указывается, что механизм ‘доверия к коду’ не устраняет человеческий фактор: разработчики и участники консенсуса остаются источником возможных сбоев и манипуляций. Таким образом, блокчейн не столько устраняет проблему доверия, сколько трансформирует ее, перенося риски от традиционных институтов к разработчикам систем и майнерам.

Важнейшим элементом финансового суверенитета государства является право денежной эмиссии. Это становится не только вызовом в области финансового суверенитета, но и в сфере экономического развития. Согласно оценкам Банка России, распространение криптовалют приводит к выводу сбережений граждан за пределы российского финансового сектора, что сокращает возможности финансирования реального сектора и

---

[314] Еременко М. Ю. Цифровизация как драйвер экономической интеграции стран Евразийского экономического союза //Вестник университета. – 2021. – №. 3. – С. 32-37.

[315] Ма Хуатэн, Мэн Чжоли, Ян Дели, Ван Хуалей. Цифровая трансформация Китая. М.: Альпина, 2019. С. 47-49

потенциал экономического роста[316]. В самом широком смысле в академической литературе[317], экспертной[318] и политической среде[319] под данным термином понимается независимость финансовой, кредитно-денежной политики государства и устойчивость к внешним финансовым воздействиям. При этом развитие криптовалют по многим оценкам, несет вызовы не только цифровому и финансовому суверенитету государств, но и национальной и международной безопасности.

В докладе Банка России отмечаются следующие угрозы, связанные с развитием криптовалют:

- Угроза для благосостояния граждан в условиях высокой волатильности курсов;
- Угроза финансовой стабильности в силу возможности формирования пузырей на рынках криптовалют;
- Угроза противоправной деятельности в силу их анонимности и широкого использования мошенниками и преступными группировками[320].

Ответом на вызовы финансовому суверенитету и угрозы безопасности со стороны криптовалют стало создание цифровых валют центральных банков. В РФ реализуется пилотный проект о пробном использовании цифрового рубля. Он был запущен Центральным банком в августе 2023 года. В проекте принимают участие 12 банков, 600 физических лиц и 22 торгово-сервисных предприятия из 11 городов. Платформа в рамках «пилота» показала свою работоспособность и функциональность, уточнил президент. На 1 июля в этой системе, по его

---

[316] Криптовалюты: тренды, риски, меры. Доклад для общественных консультаций. Банк России, 2022. URL: https://www.cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf

[317] Дудин М. Н., Шкодинский С. В., Иванов М. О. Актуальные проблемы обеспечения финансового суверенитета России в условиях международных санкций //Финансы: теория и практика. – 2023. – Т. 27. – №. 1. – С. 185-194.

[318] Омелехина Н. В. Финансовый суверенитет государства: к постановке проблемы исследования правовой идентификации //Финансовое право. – 2017. – №. 4. – С. 12-21.

[319] Глава ЦБ перечислила критерии финансового суверенитета России // Коммерснт. 20.04.2023. URL: https://www.kommersant.ru/doc/5941603

[320] Криптовалюты: тренды, риски, меры. Доклад для общественных консультаций. Банк России, 2022. URL: https://www.cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf

словам, уже совершено более 27 тыс. переводов и свыше 7 тыс. оплат товаров и услуг[321]. Цифровая валюта – аналог национальной, который используют центральные банки разных стран для прозрачности расчетов. Лидер в этой сфере – Китай широко внедривший цифровой юань.

Розничные цифровые валюты центральных банков обладают всеми функциями бумажных наличных – могут использоваться как средство платежа, обращения, сбережений. Цифровые деньги предполагают намного меньшую анонимность, чем традиционные наличные (а при крупных сделках она практически исключена), их намного сложнее подделать и использовать в незаконных операциях, таким образом обеспечивается защита не только цифрового финансового суверенитета, но и международной безопасности. Цифровые валюты эмитируются Центробанком, они, в отличие от криптовалют, не являются децентрализованными[322].

В 2017 г. интерес к изучению потенциала цифровых денег в той или иной степени проявляли два из каждых трех центральных банков, в 2022 г. – 93%, причем половина уже перешла к стадии экспериментов или пилотных проектов. По оценкам Банка международных расчетов, к концу этого десятилетия в мире будет более двух десятков цифровых валют центральных банков[323].

---

[321] Строителева М., Нефедова А. Замайнить в сети: Путин рассказал о судьбе цифрового рубля и криптовалюты. Президент заявил о необходимости узаконить рынок добычи криптовалют // Известия. 17 июля 2024. URL: https://iz.ru/1728970/mariia-stroiteleva-alena-nefedova/zamainit-v-seti-putin-rasskazal-o-sudbe-tcifrovogo-rublia-i-kriptovaliuty

[322] Там же.

[323] Там же.

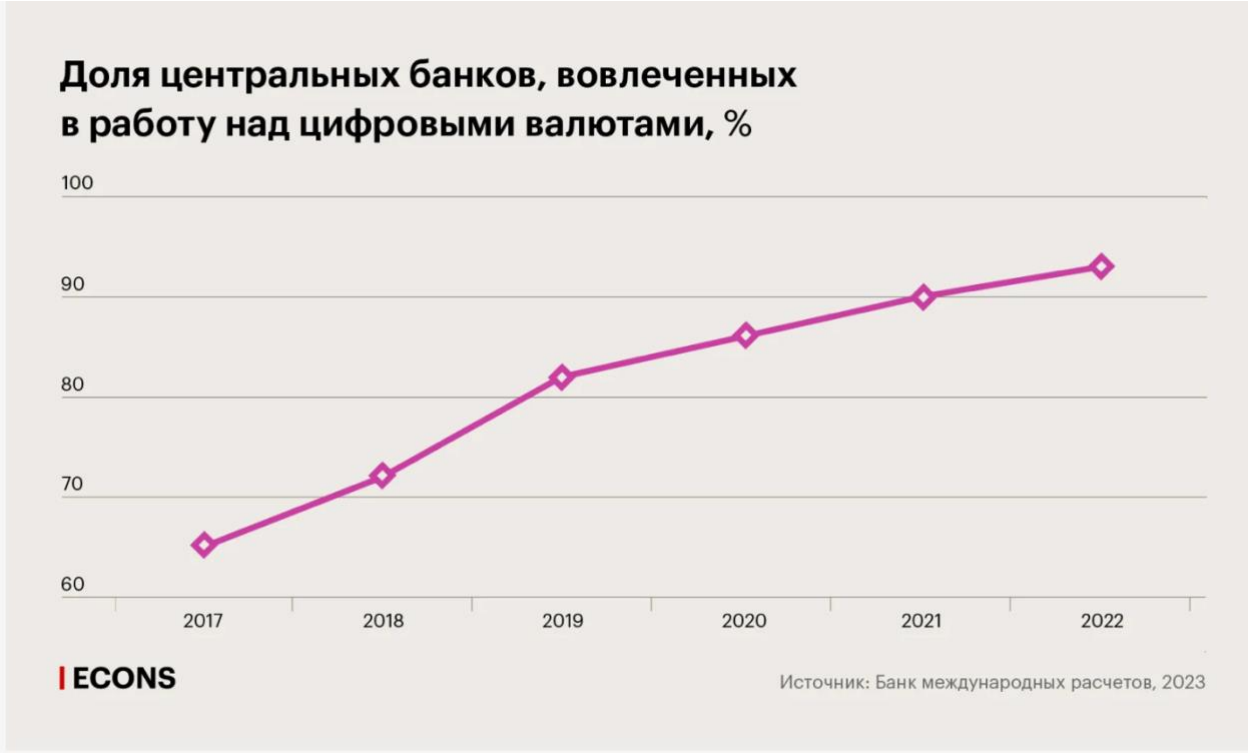

Рис. 1. Динамика роста числа цифровых валют центральных банков
Ист.: https://econs.online/articles/techno/mirovaya-tsifrovizatsiya-valyut/

В силу того, что доллар является доминирующей мировой резервной валютой, США жестко контролируют мировые финансовые платежи, что создает угрозу безопасности и экономического развития других стран. Так, международные транзакции банки проводят через систему SWIFT (Society for Worldwide Interbank Financial Telecommunications), которая вынуждена соблюдать санкции США, в том числе в отношении России, Ирана и других стран[324]. Отказ от данной системы, в том числе с опорой на технологии распределенных реестров является одним из возможных решений проблемы доминирования доллара в международных платежах и может сделать мировую финансовую систему более стабильной и безопасность.

Помимо международных финансов, на глобальном и региональном уровнях технологии распределенных реестров представляют новые

[324] Cipriani M., Goldberg L. S., La Spada G. Financial sanctions, SWIFT, and the architecture of the international payment system //Journal of Economic Perspectives. – 2023. – Т. 37. – №. 1. – С. 31-52.

инструменты для международного экономического сотрудничества, деятельности международных организаций и защиты прав человека. Однако успешное их внедрение требует решения множества вызовов, включая кибербезопасность, регулирование и стандартизацию. В этом контексте международное сотрудничество и координация усилий различных государств и организаций становятся ключевыми факторами для реализации потенциала распределенных реестров в глобальном масштабе.

2.1.4. Технологии искусственного интеллекта

Искусственный интеллект (ИИ) представляет собой область компьютерной науки, ориентированную на создание систем и алгоритмов, способных выполнять задачи, требующие когнитивных функций, характерных для человеческого интеллекта. На современном этапе благодаря искусственному интеллекту происходит рост мировой экономики, ускорение инноваций во всех областях науки, повышение качества жизни населения, доступности и качества медицинской помощи, качества образования, производительности труда и качества отдыха.

Термин искусственный интеллект используется с 1950-х гг. Первоначальной целью виделось создание неорганической копии человеческого интеллекта.

Термин «искусственный интеллект» (artificial intelligence) был предложен ученым Джоном Маккарти в рамках Дартмутского семинара в 1956 году, где обсуждались ключевые вопросы, связанные с разработкой ИИ. Теоретические основы искусственного интеллекта заложило большое количество людей, среди них Курт Гёдель, Алонзо Чёрч, Алан Тьюринг[325].

[325] Там же.

Основные направления развития технологий искусственного интеллекта включают в себя:

- Глубокое обучение и нейронные сети: Глубокое обучение стало основой для многих современных ИИ-систем. Нейронные сети позволяют ИИ обучаться на больших объемах данных и решать сложные задачи, такие как распознавание образов и обработка естественного языка.
- Большие языковые модели: ИИ значительно продвинулся в области обработки и генерации текста. Системы программирования языка могут понимать и генерировать текст на естественных языках, что нашло применение в чатах, переводах, автоматическом анализе текстов и многих других областях.
- Распознавание образов: Системы ИИ способны распознавать образы и объекты в фотографиях и видео, что нашло применение в автономных автомобилях, системах безопасности и медицинской диагностике.
- Робототехника: ИИ стимулирует развитие робототехники, включая автономных роботов, способных выполнять разнообразные задачи, от сортировки товаров на складах до хирургических операций[326].

Среди наиболее значимых современных цифровых технологий – искусственный интеллект. Как отметил Генеральный Секретарь ООН А. Гуттериш, скорость и масштабы распространения технологии искусственного интеллекта (далее ИИ) во всех его формах совершенно беспрецедентны. ИИ сравнивают с внедрением печатного станка, но потребовалось более пятидесяти лет, чтобы книги стали широко доступны по всей Европе, а ChatGPT получил 100 миллионов пользователей всего за

[326] Цифровые международные отношения / Под ред. Е.С. Зиновьевой, С.В. Шитькова. М.: Аспект-Пресс, 2023.

два месяца[327]. При этом в финансовой сфере к 2030 году вклад ИИ в мировую экономику может составить от 10 до 15 триллионов долларов[328].

Как отметил в 2023 году А. Гуттериш, ИИ способен причинить вред как отдельным людям, так и государствам и международной системе в целом. Терроризм, преступления, кибератаки – применение ИИ в этих целях будет иметь крайне серьезные последствия для глобальной безопасности[329].

Исследователи различают концепции сильного или общего искусственного интеллекта (artificial general intelligence) и слабого или специализированного искусственного интеллекта (narrow artificial intelligence)[330]. Примеры слабого ИИ широко представлены повседневной жизни: технологии «умного дома», онлайн-переводчики, распознавание изображений. Слабый ИИ может решать конкретные задачи, под которые он был создан. Если система была обучена, чтобы играть в шахматы, то без дополнительных усовершенствований она сможет играть только в эту игру. Термин «сильный ИИ» предполагает возможность самообучения и самосознания по аналогии с человеческим интеллектом. На современном этапе развития технологии большинство экспертов согласны, что сильный ИИ недостижим в краткосрочной и среднесрочной перспективе[331].

За свою историю технологии пережили несколько «зим», когда их считали недостаточно эффективными, и подъемов, когда инвестиции в отрасль возрастали. В частности, первые нейросети появились еще 1960-е гг., однако возложенные на них ожидания не оправдались. Это ознаменовало начало первой «зимы» в развитии искусственного интеллекта. Очередной виток роста внимания и инвестиций в технологии

---

[327] Генсек ООН – об искусственном интеллекте: «Это еще только начало…» // ООН, официальный сайт. 18.07.2023. URL: https://news.un.org/ru/story/2023/07/1442977

[328][328] Там же.

[329] Там же.

[330] Райков А. Н. Слабый vs сильный искусственный интеллект //Информатизация и связь. – 2020. – №. 1. – С. 81-88.

[331] Искусственный интеллект: время слабых. РСМД, 15.03.2018. URL: https://russiancouncil.ru/analytics-and-comments/analytics/iskusstvennyy-intellekt-vremya-slabykh/

приходится на 1990-е гг. Широко известен пример DeepBlue, программы, которая смогла выиграть партию в шахматы у Каспарова в 1997 году[332]. DeepBlue использовал брутфорс, то есть перебирал миллионы возможных комбинаций за несколько секунд[333]. Современный прорыв в области технологий искусственного интеллекта связан с возможностью программ обучаться самостоятельно, не следуя заранее установленным правилам. Такая цель ставилась с самого начала информатики, однако добиться удовлетворительных результатов не удавалось. Считается, что очередным прорывом в развитии ИИ стала победа ИИ в 2016 году в игре го у корейского профессионала Ли Сеголя[334]. Современный этап развития ИИ, основанных на нейросетевых моделях, связан с тремя факторами:

- Развитие технологий машинного обучения, основанных на анализе Больших данных
- Увеличение программного и аппаратного потенциала компьютерных технологий, в том числе развитие суперкомпьютеров
- Развитие технологий моделирования «нейронных сетей» - определенного способа конструирования информационных связей, при котором точки обработки данных в значительной степени независимы друг от друга, по аналоги с нейронами человеческого мозга.[335]

Таким образом, важнейшими элементами развития современных технологий искусственного интеллекта являются технологии машинного обучения и нейронных сетей. Остановимся подробнее на характеристиках каждой из них.

Машинное обучение фокусируется на разработке алгоритмов, позволяющих системам обучаться на основе данных. Основные методы машинного обучения включают: обучения с учителем (под контролем

---

[332] в 2024 г. признан в РФ иностранным агентом и включен в перечень террористов и экстремистов
[333] Eliseeva D. Y. et al. The evolution of artificial intelligence and the possibility of its application in cyber games //Amazonia Investiga. – 2020. – Т. 9. – №. 28. – P. 123-129.
[334] Там же.
[335] Jiang Y. et al. Quo vadis artificial intelligence? //Discover Artificial Intelligence. – 2022. – Т. 2. – №. 1. – P. 4.

программиста), обучение с подкреплением (алгоритмы обучаются на размеченных данных и способны делать предсказания или классифицировать новые данные на основе обученной модели), обучение без подкрепления (алгоритмы выявляют скрытые структуры в неразмеченных данных, такие как кластеры или ассоциации). Что же касается глубокого обучения, то речь идет о применении нейронных сетей для реализации трех упомянутых ранее техник[336].

Нейронные сети, вдохновленные биологическими нейронными системами, являются основой многих современных ИИ-систем. Глубокие нейронные сети с множеством слоев используются для решения сложных задач, таких как обработка изображений, распознавание речи и генерация текста.[337]

В 2022 - 2023 годах в мире произошел новый скачок в развитии технологий искусственного интеллекта благодаря совершенствованию больших генеративных моделей в области языка, изображений (включая видеоизображения) и звука. Большие фундаментальные модели уже сейчас способны писать программные коды по техническим заданиям, сочинять поэмы на заданную тему, давать точные и понятные ответы на тестовые вопросы различных уровней сложности, в том числе из образовательных программ. Большая языковая модель (или LLM, large language model) – это нейросеть с множеством параметров, которая тренируется на гигабайтах текста по принципу «обучения без учителя». По принципу LLM устроены практически все популярные генеративные нейросети, от GPT-4 до YandexGPT[338].

Лидерами в данной области являются США и КНР[339]. Наиболее известные большие модели от производителей США: GPT-4 от OpenAI

---

[336] Цифровые международные отношения / Под ред. Е.С. Зиновьевой, С.В. Шитькова. М.: Аспект-Пресс, 2023.
[337] LeCun Y., Bengio Y., Hinton G. Deep learning //nature. – 2015. – Т. 521. – №. 7553. – С. 436-444.
[338] Wang Y. et al. Exploring new frontiers of deep learning in legal practice: A case study of large language models //International Journal of Computer Science and Information Technology. – 2023. – Т. 1. – №. 1. – С. 131-138.
[339] Новая модель YandexGPT 5.1 Pro // Яндекс, официальный сайт. URL: https://ya.ru/ai/gpt-3

(может выполнять широкий спектр задач, включая составление текстов, перевод, обобщение, ответы на вопросы и многое другое); BERT от Google (может быть настроен для различных задач обработки естественного языка таких, как анализ настроения, распознавание объектов и классификация текста); Gato от DeepMind; трансформеры Hugging Face и ряд других. В Китае насчитывается более 130 крупных языковых моделей. Лидером считается Ernie 4.0 от компании Baidu[340].

В России разрабатывается большое количество больших языковых моделей под различные задачи, в частности:

- GigaChat от Сбера. Считается, что эта модель обогнала ChatGPT по качеству ответов на английском языке[341].
- FRED-T5 (Fullscale Russian Enhanced Denoisers T5) от SberDevices, стала лучшей в мире по пониманию текста в соответствии с результатами тестов главного русскоязычного бенчмарка Russian SuperGLUE.
- YandexGPT – генеративная языковая модель, которая создает тексты, генерирует идеи, дает советы.
- Jay CoPilot – инструмент для взаимодействия с нейросетями от российской компании Just AI[342].

В России была поставлена задача обеспечить технологический суверенитет в области технологий искусственного интеллекта, в том числе путем наращивания возможностей цифрового суверенитета:

Модели искусственного интеллекта за секунды создают изображения на любую тему по заданному текстовому описанию или

---

[340] Козюлин В.Б. Как обеспечить технологический суверенитет в сфере искусственного интеллекта и больших языковых моделей? // Индекс Безопасности. 2024. № 5. URL: https://pircenter.org/editions/5-2024-kak-obespechit-tehnologicheskij-suverenitet-v-sfere-iskusstvennogo-intellekta-i-bolshih-jazykovyh-modelej/

[341] GigaChat обогнал по качеству ChatGPT и расширил контекст до 32 тысяч токенов URL: https://habr.com/ru/companies/sberdevices/articles/790470/

[342] Козюлин В.Б. Как обеспечить технологический суверенитет в сфере искусственного интеллекта и больших языковых моделей? // Индекс Безопасности. 2024. № 5. URL: https://pircenter.org/editions/5-2024-kak-obespechit-tehnologicheskij-suverenitet-v-sfere-iskusstvennogo-intellekta-i-bolshih-jazykovyh-modelej/

наброску, что создает угрозу распространения запрещенной информации, нарушения авторских прав и генерации ошибочных сведений. Однако развитие данных технологий сопряжено с угрозами безопасности.

Разработка и внедрение ИИ поднимает важные этические и политические вопросы, связанные с конфиденциальностью данных, предвзятостью алгоритмов, ответственностью за действия ИИ и влиянием на рынок труда. Международные организации и исследовательские сообщества работают над созданием этических норм и стандартов для использования ИИ[343].

Искусственный интеллект трансформирует различные сферы человеческой деятельности, от медицины и транспорта до финансов и образования. Успешное внедрение ИИ требует решения множества технических, этических и социальных вызовов, чтобы обеспечить безопасное и справедливое использование этой технологии. Общемировой тренд - создание так называемого доверенного искусственного интеллекта. Доверенный ИИ отвечает требованиям прозрачности, подотчетности, объяснимости и воспроизводимости результатов работы ИИ. В России также большое внимание уделяется развитию доверенного ИИ, в частности, в Институте системного программирования РАН создан Центр технологий доверенного искусственного интеллекта[344]. Согласно Концепции развития технологий искусственного интеллекта Российской Федерации до 2030 года, доверенный ИИ – это технологии, отвечающие стандартам безопасности, разработанные с учетом принципов объективности, недискриминации, этичности, исключающие при их использовании возможность причинения вреда человеку и нарушения его основополагающих прав и свобод, нанесения ущерба интересам общества и государства[345].

---

[343] Цифра и искусственный интеллект на службе дипломатии / Под ред. Е.С. Зиновьевой. М.: 2024.
[344] Исследовательский центр доверенного ИИ // ИСП РАН. URL: https://www.ispras.ru/ai-center/
[345] Стратегия развития искусственного интеллекта в Российской Федерации до 2030 года. Утв. Указом Президента Российской Федерации. 2024.

В 2024 году Президент России Владимир Путин подписал указ о поправках к Национальной стратегии развития искусственного интеллекта на период до 2030 года. Согласно стратегии, объем оказанных услуг по разработке и реализации решений в области ИИ к 2030 году должен вырасти как минимум до 60 млрд руб. по сравнению с 12 млрд руб. в 2022 году. Также планируется, что вырастет количество выпускников высших учебных заведений в сфере нейросетей с 3000 до 15 500 человек. Доля приоритетных отраслей экономики с высокой готовностью к внедрению ИИ увеличится с 12 до 95%[346].

В документе делается акцент на развитие больших генеративных моделей искусственного интеллекта – это модели ИИ, способные интерпретировать (предоставлять информацию на основании запросов, например, об объектах на изображении или о проанализированном тексте) и создавать мультимодальные данные (тексты, изображения, видеоматериалы и тому подобное) на уровне, сопоставимом с результатами интеллектуальной деятельности человека или превосходящем их[347].

Российскими организациями создаются модели искусственного интеллекта мирового уровня, в том числе в области генерации изображений, генерации и обработки текстов на русском и английском языках, медицины, генетики. К проблемным областям можно отнести неразвитость аппаратной базы, что может быть преодолено международной научно-технической кооперацией. В частности, Россия уступает лидерам по числу и потенциалу суперкомпьютеров и вычислительных мощностей[348].

---

[346] Путин утвердил стратегию развития ИИ до 2030 года // Право, 2024. URL: https://pravo.ru/news/251592/

[347] Стратегия развития искусственного интеллекта в Российской Федерации до 2030 года. Утв. Указом Президента Российской Федерации. 2024.

[348] Зиновьева Е.С. Научный потенциал российских ИИ-компаний: на пути к технологическому суверенитету // РСМД, 13.07.2024. URL: https://russiancouncil.ru/analytics-and-comments/analytics/nauchnyy-potentsial-rossiyskikh-ii-kompaniy-na-puti-k-tekhnologicheskomu-suverenitetu/

Тем не менее наша страна остается региональным лидером в области языковых моделей. По оценкам Яндекс, свои языковые модели развивают всего 7 стран, и Россия в их числе. Вместе с тем на 2023 год всего 3% открытых данных для обучения языковых моделей были на русском языке (для сравнения на английский язык приходится 57%, на китайский – 6%)[349].

Технологии искусственного интеллекта являются областью международной конкуренции. Технологическое лидерство в области искусственного интеллекта может позволить государствам достичь значимых результатов по основным направлениям социально-экономического развития. К 2024 году времени более 60 стран разработали и утвердили собственные национальные стратегии развития искусственного интеллекта [350]. Можно выделить две страны лидера в данной области – США и КНР.

Искусственный интеллект оказывает существенное влияние на экономический рост в мире. По оценкам экспертов, дальнейшее развитие больших генеративных моделей может вызвать резкое повышение производительности труда, которое приведет увеличению мирового валового внутреннего продукта на 1 - 2 процента ежегодно и позволит повысить оплату труда специалистов во всех отраслях экономики за счет увеличения объема выпуска продукции (товаров, работ, услуг) и улучшения ее качества. Развитие технологий искусственного интеллекта, как показывает опыт государств - лидеров в области искусственного интеллекта (Китай, США), сопровождается существенным увеличением государственных инвестиций в их развитие, а также в разработку прикладных решений в области искусственного интеллекта[351].

Многие эксперты и ученые отмечают, что развитие ИИ вызовет колоссальные изменения в структуре занятости. Уходят в прошлое

---

[349] Стратегия развития искусственного интеллекта в Российской Федерации до 2030 года. Утв. Указом Президента Российской Федерации. 2024.
[350] Там же.
[351] Там же.

профессии, связанные с монотонными повторяющимися операциями, где мышление можно заменить вычислениями, они переходят к ИИ. При этом появляется множество новых рабочих мест, таких как специалисты в областях больших данных, автоматизации, контроля роботов и др. Для сохранения цифрового суверенитета в данной области необходим также научный, кадровый и образовательный суверенитет.

Однако помимо возможностей, сопряженных с развитием технологий искусственного интеллекта, возникают и новые угрозы безопасности на национальном и международном уровнях, что актуализирует потребность в выработки регуляторной базы в данной области.

В период с 2022 по 2023 год количество зарегистрированных инцидентов с ИИ увеличилось примерно на 1278%, что совпало с популяризацией генеративного ИИ[352].

Международное сообщество идет по пути выработки этических принципов регулирования ИИ. 26 октября в России был открыт для подписания национальный Кодекс этики в сфере ИИ. Документ был разработан профессиональным сообществом на площадке Альянса в сфере ИИ совместно с академическим сообществом и при поддержке Аналитического центра при Правительстве Российской Федерации и Минэкономразвития России. В обсуждении документа приняли участие сотни российских экспертов, а дискуссии по нему прошли на полях Общественной палаты и Совета Федерации, а также АНО «Цифровая экономика»[353].

2.1.5. Анализ Больших данных

[352]Artificial Intelligence. OECD AI policy observatoty. 2025. URL: https://www.oecd.org/en/topics/policy-issues/artificial-intelligence.html

[353] Незнамов А. Этика ИИ в авангарде мировой повестки // 29.01.2021. URL: https://russiancouncil.ru/analytics-and-comments/analytics/etika-ii-v-avangarde-mirovoy-povestki/

Большие данные (Big Data) представляют собой совокупность технологий и методов, направленных на сбор, хранение, обработку и анализ массивных, разнообразных и быстро изменяющихся наборов данных. Эти данные характеризуются значительным объемом, разнообразием форматов и высокой скоростью поступления, что делает их обработку и анализ сложной задачей для традиционных систем управления базами данных.

Основные характеристики больших данных:

- Объем (Volume): Большие данные характеризуются огромным объемом информации, который измеряется в терабайтах и петабайтах. Современные технологии позволяют собирать данные из множества источников, включая социальные медиа, сенсоры, лог-файлы, транзакционные записи и т.д.
- Скорость (Velocity): Скорость, с которой данные генерируются и поступают, является критическим аспектом больших данных. Это включает как потоковую обработку данных в реальном времени, так и пакетную обработку.
- Разнообразие (Variety): Данные могут быть представлены в различных форматах, таких как структурированные данные (таблицы, реляционные базы данных), неструктурированные данные (тексты, изображения, видео) и полуструктурированные данные (XML, JSON).
- Правдивость (Veracity): Достоверность и качество данных являются важными аспектами. Большие данные могут содержать шум и ошибки, что требует применения методов очистки и валидации для обеспечения надежности анализа[354].
- Ценность (Value): Одной из основных задач работы с большими данными является извлечение полезной информации и знаний,

[354] Demchenko Y., De Laat C., Membrey P. Defining architecture components of the Big Data Ecosystem //2014 International conference on collaboration technologies and systems (CTS). – IEEE, 2014. – С. 104-112.

которые могут быть использованы для принятия обоснованных решений и создания экономической ценности[355].

В 2017 году авторы британского журнала Экономист метафорично отметили, что «данные – это новая нефть», которая определяет лицо современного цифрового общества[356]. Данная фраза впоследствии стала расхожей, и широко использовалась в публицистических и академических трудах. Аргумент, выдвигаемый здесь, заключается в том, что цифровые данные вытеснили ископаемое топливо в качестве ключевого материала, определяющего современную социально-экономическую организацию. Утверждается, что Четвертая промышленная революция, основанная на возможностях Больших данных, имеет такое же историческое и социальное значение, как и промышленные революции XIX и XX веков[357].

Согласно статистике ЮНКТАД, количество данных, передаваемых по сетям возрастает экспоненциально. Как отмечают авторы доклада ЮНКТАД за 2021 год главным фактором, определяющим лицо современной цифровой революции, становится растущий объем данных, которые в свою очередь меняют и переговорную практику и становятся объектом международных договоренностей[358].

В цифровых международных отношениях есть две страны лидера – США и Китай. Согласно статистике ЮНКТАД за 2021 год на их долю приходится половина мировых гипермасштабных центров обработки данных, самые высокие темпы внедрения 5G в мире, 94 процента всего финансирования стартапов в области ИИ за последние пять лет, 70 процентов ведущих мировых исследователей ИИ и почти 90 процентов рыночной капитализации крупнейших мировых цифровых платформ[359].

---

[355] Цифра и искусственный интеллект на службе дипломатии /Под ред. Е.С. Зиновьевой.М.: МГИМО, 2024.
[356] Taffel S. Data and oil: Metaphor, materiality and metabolic rifts //New media & society. – 2023. – Т. 25. – №. 5. – С. 980-998.
[357] Там же.
[358] UNCTAD Digital Economy Report 2021.
[359] UNCTAD Digital economy Report. 2021. URL: https://unctad.org/system/files/official-document/der2021_overview_en_0.pdf

Анализ данных становится важным фактором цифровой экономики. Ключевым ее направлением является финтех. В финансовом секторе анализ больших данных помогает в управлении рисками, обнаружении мошенничества, оптимизации инвестиционных стратегий и повышении качества клиентского обслуживания. В научных исследованиях большие данные применяются для обработки и анализа результатов экспериментов, моделирования сложных систем и прогнозирования климатических изменений. Большие данные играют важную роль в управлении городскими инфраструктурами, оптимизации трафика, мониторинге окружающей среды и повышении качества жизни граждан[360].

Обработка больших данных поднимает вопросы защиты персональной информации и обеспечения безопасности данных. Именно в контексте безопасности персональных данных появляется новый термин – цифровой суверенитет личности[361]. Как правило, данная категория предполагает независимое право человека управлять персональными данными – и иметь возможности влиять на решение вопросов, связанных с их хранением, использованием и редактированием[362].

Государственный суверенитет, согласно классической доктрине, складывается из верховенства, независимости и полноты государственной власти на территории государства. Как указывает Конституционный суд РФ, «территориальное верховенство государственной власти выражается в том, что в пределах территории РФ не допускается иной власти, которая могла бы существовать наряду с нею или вне её контроля». В этом плане вполне органично включение в эту схему так называемого суверенного интернета[363].

---

[360] Цифровые международные отношения / Под ред. Е.С. Зиновьева, С.В. Шитькова. М.: Аспект-Пресс, 2023.

[361] Lawo D. et al. Human-Centred Digital Sovereignty: Explorative Conceptual Model and Ways Forward //International Conference on Computer-Human Interaction Research and Applications. – Cham : Springer Nature Switzerland, 2023. – С. 84-103.

[362] Федотов М. Неприкосновенность частной жизни и суверенитет личности в социальных сетях // Валдай. 03.06.2021. URL: https://ru.valdaiclub.com/a/highlights/neprikosnovennost-chastnoy-zhizni/

[363] Avila Pinto R. Digital sovereignty or digital colonialsim //SUR-Int'l J. on Hum Rts. – 2018. – Т. 15. – С. 15.

В научной литературе современное значение данных для мировой экономики осмысливается в категориях неоколониальной теории. Согласно данному подходу, в то время как промышленный капитализм эксплуатировал и получал прибыль от завоевания новых территорий, ресурсов и рабочей силы в колониях, сегодня информационный колониализм продолжается путем приобретения нового типа общего ресурса: данных, и предназначенных для прогнозирования и воздействия на поведение людей в маркетинговых и политических целях[364]. Цифровой неоколониализм рассматривается новый способ биополитического контроля со стороны цифровых гигантов, опирающихся на анализ данных планетарного масштаба, алгоритмы машинного обучения[365].

Анализ данных используется в дипломатии и работе международных организаций. В работе международных организаций Большие данные помогают оптимизировать распределение гуманитарной помощи, анализируя потребности пострадавших регионов и координируя действия международных организаций. Это способствует более эффективному реагированию на кризисные ситуации и снижению издержек[366].

Проект «Global Pulse» ООН использует большие данные для анализа глобальных тенденций в области здравоохранения, экономики и экологии. Целью проекта является выявление ранних признаков кризисов и разработка мер для их предотвращения. Деятельность проекта охватывает широкий спектр инноваций с использованием данных, цифровых технологий, поведенческой науки и методов стратегического прогнозирования – от расширения охвата цифровыми технологиями женщин в Индонезии до прогнозирования последствий стихийного

[364] UNCTAD Digital Economy Report 2021.
[365] Avila Pinto R. Digital sovereignty or digital colonialsim //SUR-Int'l J. on Hum Rts. – 2018. – T. 15. – C. 15.
[366] Big Data for Sustainable Development. UN, Global Issues. URL: https://www.un.org/en/global-issues/big-data-for-sustainable-development

бедствия на Филиппинах или разработки национальной стратегии данных в Уганде[367].

Международные организации и исследовательские институты используют анализ больших данных для мониторинга и прогнозирования конфликтов. Это включает анализ новостных источников, социальных медиа и данных о перемещении населения. Управление ООН по поддержке миростроительства поручило команде SIPA Capstone определить ключевые проблемы в области миростроительства, где технологии «больших данных» могут оказать наибольшее влияние. Команда определила три движущие силы конфликта:

- миграция населения,
- разжигание ненависти
- исключение и восприятие исключения.

При помощи анализа больших данных предлагается усилить работу ООН по миростроительству и раннему предотвращению конфликтов. Среди таких направлений работы – анализ социальных сетей для выявления «лексики разжигания ненависти» в сообществах, находящихся в группе риска, надежные системы для прогнозирования рисков и измерения сотового трафика для выявления групп населения, находящихся в движении[368].

На современном этапе отсутствуют международные стандарты и нормы, которые обеспечат защиту персональных данных и соблюдение этических принципов. Сотрудничество развивается не на глобальном, но на региональном уровне. Ярким примером является ЕС. Наиболее значимым документом ЕС на данном направлении является Европейский регламент в области данных, принятый в 2016 году и вступивший в силу в

[367] UN Global Pulse. Official site. URL: https://www.unglobalpulse.org/un-global-pulse/
[368] Using Big Data to Prevent Conflict // Columbia University. School of International and Public Affairs. URL: https://www.sipa.columbia.edu/using-big-data-prevent-conflict

2018 году[369]. На уровне ЕС важный акцент делается на обеспечении «цифрового суверенитета» на уровне интеграционной структуры (в качестве других терминов используется «стратегическая автономия» и «технологический суверенитет»). Важнейшими предпосылками формирования собственной инфраструктуры анализа и хранения больших данных на уровне ЕС как части политики цифрового суверенитета интеграционного объединения стали, с одной стороны, заинтересованность в обеспечении политики в области защиты персональных данных граждан стран ЕС, а с другой – растущая обеспокоенность со стороны ЕС доминированием зарубежных ИТ компаний и интернет-гигантов на европейских рынках. Наиболее заметным проектом в области Больших данных стал GAIA – X – европейская система облачного хранения данных, объединившая компании из Франции, Германии, США и ряда европейских стран. Первоначально инициаторами создания GAIA – X стали Франция и Германия[370].

В России также предпринимаются меры по обеспечению суверенитета данных на законодательном уровне. 1 сентября 2015 года вступил в силу Федеральный закон №242-ФЗ, предусматривающий локализацию баз персональных данных в России. Согласно тексту закона хранение и обработка персональных данных граждан РФ должна осуществляться на территории РФ[371]. Кроме того, с 2006 года действует закон о персональных данных[372]. Целью Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке

---

[369] Regulation (EU) 2016/679 (General Data Protection Regulation) 27.04.2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[370] https://gaia-x.eu

[371] Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья» от 29.07.2017 N 242-ФЗ (последняя редакция)

[372] Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ (последняя редакция)

его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.[373]

Именно с развитием технологий больших данных связана концепция «суверенитета данных». Суверенитет данных предполагает, что организации, правительства и отдельные лица могут контролировать свои данные. Этот контроль позволяет им определять, как данные собираются, хранятся, передаются и используются[374].

Вывод по параграфу:

Подводя итог рассмотрению основных направлений технологического развития в эпоху современного технологического уклада, необходимо отметить, что цифровой технологический суверенитет государства представляет собой не только основу «цифрового лидерства», но является также необходимым условием суверенитета политического и его национальной независимости[375]. «Цифровая вседозволенность» последних трёх десятилетий существенным образом стимулировала инновации, экономическое освоение новой среды и улучшение качества жизни населения. Вместе с тем она привела к размыванию регулирующей роли государства и осложнила выполнение такой ключевой функции, как обеспечение безопасности граждан. Сегодня перед государствами стоит непростая задача: найти эффективные механизмы обеспечения суверенитета в цифровом пространстве без ущерба для положительных аспектов цифровой революции, а также выработать оптимальную глобальную архитектуру, в рамках которой будет гарантировано равноправие и безопасность всех вовлечённых сторон[376].

Новые технологии – искусственный интеллект и анализ данных, с одной стороны, опираются на возможности глобальной связности

---

[373] Там же.
[374] UNCTAD Digital Economy Report 2021.
[375] Ребро О. Категория «Цифрового суверенитета» в современной мировой политике вызовы и возможности для России // Международные процессы. 2021. № 4. URL: https://www.intertrends.ru/jour/article/view/266?locale=ru_RU
[376] Там же.

цифровой инфраструктуры и диктуют необходимость международного сотрудничества. Однако национальный сегмент киберпространства зависит от физической инфраструктуры, полностью находящейся под суверенным контролем. Таким образом, прикладное применение цифрового суверенитета – сформировать общее понимание действий государства по расширению регулирования новых технологий таким образом, чтобы минимизировать ущерб глобальной связности при понимании различий в национальных интересах государств.

Формирование глобального цифрового пространства сопровождается глубокими изменениями в международной политике, которые отражают как потенциал, так и угрозы цифровой трансформации. С одной стороны, технологии открывают новые возможности для взаимосвязи, сотрудничества и экономического роста, усиливая глобализацию и расширяя доступ к информации. С другой стороны, растет обеспокоенность по поводу усиления неравенства, доминирования отдельных государств и транснациональных корпораций, а также угроз кибербезопасности, которые ставят под сомнение стабильность международного порядка.

Глобальное цифровое пространство становится ареной соперничества, где государственные и негосударственные акторы формируют свои стратегии, опираясь на технологические достижения. Развитие технологий четвертой промышленной революции, таких как искусственный интеллект, интернет вещей, облачные вычисления и блокчейн, меняет привычные подходы к управлению, безопасности и экономическому развитию. Эти технологии не только повышают эффективность процессов, но и создают новые линии разлома, влияя на распределение власти и ресурсов в международной системе.

Текущие тенденции демонстрируют, что цифровая революция переходит в стадию усиления национальных и региональных инициатив, таких как создание автономных интернет-платформ, внедрение защитных

мер для данных и регулирование потоков информации. Эти меры часто направлены на сохранение суверенитета в условиях глобальной взаимозависимости, но могут привести к фрагментации мирового цифрового пространства и созданию конкурирующих технологических экосистем. Государства стремятся адаптироваться к новым вызовам, одновременно пытаясь диктовать правила игры на глобальной арене.

Таким образом, формирование глобального цифрового пространства, ускоряемое технологиями четвертой промышленной революции, – это сложный, противоречивый и многослойный процесс. Он требует не только инновационных подходов к сотрудничеству и управлению, но и глубокого переосмысления традиционных концепций международной политики. В условиях стремительного технологического прогресса стабильность и безопасность цифрового пространства становятся важнейшими вызовами для будущего международных отношений.

2.2. Актуальные проблемы развития и управления глобальным цифровым пространством

2.2.1. Фрагментация Интернета и цифровой суверенитет

Распространение прорывных технологий изменяет все сферы жизни общества и государства. Важнейшей чертой современного этапа развития мировой политики является повсеместная цифровизация, сопровождающаяся нарастающей международной конфликтностью. Пандемия коронавирусной инфекции COVID-19 способствовала ускоренной цифровизации – в силу вынужденной самоизоляции, которая затронула и дипломатов, и сотрудников международных организаций, цифровые технологии в дипломатии стали использоваться более интенсивно.

Согласно статистике, на 2024 год общее количество пользователей Интернета составило порядка 70% общего населения планеты Земля, при этом пользователей социальных сетей – 63% от общего населения планеты. В среднем по миру люди проводят чуть менее 3х- часов в день в социальных сетях[377]. При этом широкое распространение мобильных телефонов, привело к тому, что люди проводят очень много времени в Интернете – в целом, согласно статистике, порядка 7 часов в день в различных приложениях[378].

В отдельных странах, например, в Исландии, Дании, Голландии, Норвегии и Кипре уровень проникновения интернета уже превысил 95%, то есть практически каждый житель является пользователем сети. По количеству пользователей лидируют страны с населением более 100 млн. человек: Китай, Индия, США, Бразилия, Индонезия, Япония и Россия[379]. В последние годы число пользователей быстрее всего растет в таких густонаселенных странах как Индия и Индонезия[380].

В Китае в настоящее время крупнейшей в мире базы пользователей Интернета – 513 миллионов человек, что более чем вдвое превышает 245 миллионов пользователей в США – Китай также имеет самую активную в мире среду для социальных сетей. Его используют более 300 миллионов человек: от блогов до социальных сетей, микроблогов и других онлайн-сообществ[381]. Это примерно эквивалентно совокупному населению Франции, Германии, Италии, Испании и Великобритании. Кроме того, онлайн-пользователи Китая проводят более 40 процентов своего времени в социальных сетях, и эта цифра продолжает быстро расти.

Пользователи социальных сетей Китая не только более активны, чем пользователи любой другой страны, но и в более чем 80 процентах всех

---

[377] We are social. Digital 2024. URL: https://wearesocial.com/uk/blog/2024/01/digital-2024/
[378] Там же.
[379] Internet usage and population statistics. URL: www.internetworldstats.com
[380] Internet Usage Statistics In 2024. Forbes. URL: https://www.forbes.com/home-improvement/internet/internet-statistics/
[381] Number of internet users in China from 2013 to 2023 // Statista. URL: https://www.statista.com/statistics/265140/number-of-internet-users-in-china/

случаев имеют несколько учетных записей в социальных сетях, в основном с местными игроками (по сравнению с 39 процентами в Японии)[382]. Использование мобильных технологий для доступа к социальным сетям также становится все более популярным в Китае: в 2013 году насчитывалось более 100 миллионов пользователей мобильных социальных сетей, и, по прогнозам, возрастало примерно на 30 процентов ежегодно[383].

Именно эти различия, которые накладываются на культурное и языковое разнообразие, обуславливают фрагментацию глобального информационного пространства Интернета. Важную роль играют и прорывные технологии 4 Промышленной революции, которые стали полем геополитической конкуренции, и межгосударственной конфликтности, что также усиливает фрагментацию Интернета. Современный этап развития информационно-коммуникационных технологий в академической литературе все чаще называют «цифровой революций», с целью подчеркнуть его отличие от более ранней информационной революции, которая датируется 1990-ми годами и характеризуется широким распространением пользовательских компьютеров и глобальной сети Интернет[384]. Цифровая же революция характеризуется растущим количеством данных, передаваемых по глобальным информационным сетям, в особенности по социальным сетям, таким как TikTok, Vkontakte. Именно данные и социальные сети оказывают трансформирующее влияние на мировую экономику, мировую политику, а также все сферы жизни личности, общества и государства. При этом в основе современных Больших данных лежат именно данные пользователей социальных сетей. Локализация персональных данных и

[382] Там же.
[383] Там же.
[384] См. напр.: Цифровые международные отношения / Под ред Е.С. Зиновьевой, С.В. Шитькова. М.: Аспект-Пресс, 2023.

формирование т.н. «эко-комнат» в цифровом пространстве усиливают фрагментацию и разобщенность в сети.

Фрагментация Интернета, пришедшая на смену информационной глобализации, становится новой реальностью. Протекционизм, пандемия, санкционные войны и нарастающая международная конфликтность способствовали сворачиванию процессов глобализации, как она формировалась начиная с 1980-х гг.[385] Схожая динамика наблюдается и в информационном пространстве. Видение глобального интернета, в котором нет государственных границ, характерное для 1990-х 2000-х гг.[386], не оправдало себя. Один из наиболее заметных глобальных форумов в области управления киберпространством, Форум по вопросам управления Интернетом ООН в Кении в 2022 году прошел под знаком обсуждения фрагментации интернета[387]. Эксперты Всемирного экономического форума еще в 2016 году выделили несколько уровней фрагментации – уровень государства, уровень технологических компаний и уровень пользователей[388]. С тех пор фрагментация глобальной сети только усиливается.

Государства и региональные организации проводят практику «огораживания» и выделения национальных и региональных сегментов глобальной сети. Особенно заметным является пример Китая, где с 1996 г. ведётся политика по укреплению цифрового суверенитета, символом и практической реализацией, в которой является Великий китайский файрволл. Китай выступает в роли первопроходца в данной области. На уровне ЕС в последние годы также активизируются инициативы, направленные на формирование технологического и цифрового суверенитета на уровне региона, ведется политика, направленная на

---

[385] Keohane R. O., Nye, Jr J. S. (ed.). Transnational relations and world politics. – Harvard University Press, 1972.
[386] Kurbalija J. An introduction to internet governance. – Diplo Foundation, 2016.
[387] Internet Governance Forum. Kenya, 2022. URL: https://kigf.or.ke
[388] Internet Fragmentation: An Overview. World Economic Forum, 2016. URL: https://www.weforum.org/publications/internet-fragmentation-an-overview/

укрепление стратегической автономии в цифровом пространстве. Важнейшей задачей на уровне государственной политики России является укрепление цифрового суверенитета страны. При этом Россия открыта к международному сотрудничеству в области управления интернетом на равноправной основе.

Внимание к вопросам обеспечения цифрового суверенитета в интернет-пространстве обусловлено значимостью технологий, которые не только определяют положение страны на международной арене, но и спектр доступных ей внешнеполитических возможностей. Цифровые технологии и Интернет являются важнейшим ресурсом влияния в современных международных отношениях и полем острейших геополитических противоречий, характеризующихся новым витком борьбы за глобальное лидерство в XXI веке между технологически развитыми державами. Формирование многополярного мира связано с ростом напряженности в отношениях между великими державами и цифровые технологии становятся важнейшей ставкой в глобальной борьбе за власть в условиях многополярного мира.

Балканизация Интернета, фрагментация интернета, «расколотый интернет» – такие термины используются в прессе и в академической литературе для обозначения нового качества международного информационного пространства. Однако, несмотря на набирающую силу фрагментацию интернета, масштабы охвата цифровых технологий на сегодняшний день беспрецедентны.

Как отмечает Д. Льюис, риск от расширения суверенного контроля – это не «балканизация» или технологическая фрагментация, не множество отдельных интернетов, а фрагментация руководящих концепций, при которой базовые технические протоколы все еще поддерживают глобальную связь, но на эту связь накладывается множество нескоординированных действий. Часто противоречивые правила в отношении данных, конфиденциальности и безопасности, определяемые

разными и конкурирующими национальные интересами, способствуют фрагментации[389].

Вопрос не в том, чтобы предотвратить эту «балканизацию», а в том, чтобы управлять ею. Текущие усилия, как частных и многосторонних институтов являются недостаточными. Проблема усугубляется нарастающей международной конфликтностью в условиях перестройки международной системы и складывания многополярности.

Начало специальной военной операции России в Украине обострило отношения России со странами запада и ускорило политику России в области укрепления цифрового суверенитета. При этом цифровая дипломатия в условиях фрагментированной цифровой реальности также сталкивается с рядом вызовов, в числе которых «культура отмены, кратное ускорение информационного цикла и алгоритмические фильтры соцсетей, формирующие у пользователей индивидуальные картины мира, далекие от объективных».

В современных условиях все чаще наблюдается усталость пользователей от социальных сетей, снижается объем размещаемой информации. При этом пользователей все больше заботят проблемы дезинформации и кражи персональных данных, что также снижает и потенциал использования социальных сетей в рамках цифровой дипломатии.

Геополитическая напряженность, в том числе обострение отношений между США и Китаем[390], в свою очередь способствовало снижению прибылей крупных ИТ-компаний, в том числе владеющих социальными сетевыми сервисами, которые в значительной степени формировали ландшафт глобального цифрового пространства. В этих условиях

---

[389] Lewis J. A. Sovereignty and the evolution of internet ideology. – Center for strategic & international studies (CSIS), 2020. URL: https://www.orfonline.org/public/uploads/posts/pdf/20230501094513.pdf#page=65

[390] Дегтерев Д. А., Рамич М. С., Пискунов Д. А. Подходы США и КНР к глобальному управлению киберпространством: «новая биполярность» в «сетевом обществе» // Вестник международных организаций: образование, наука, новая экономика. – 2021. – Т. 16. – №. 3. – С. 7-33.

социальные сети стремятся формировать замкнутые цифровые экосистемы. Социальные сети остаются площадками для информационного противоборства и продвижения внешнеполитических нарративов. По мере роста значимости цифровых технологий для политики, экономики, общества и культурной сферы возрастает и стремление к контролю данной области со стороны государств. При этом отсутствуют признанные на глобальном уровне международно-правовые нормы, регламентирующие глобальное цифровое пространство. Вероятно, фрагментация по линии цифровых гигантов будет менее значительной, чем фрагментации по линии государств.

Кроме того, наметилась фрагментация по линии предпочтений пользователей цифровых сетей. Исследователи фиксируют востребованность новых форматов цифровой дипломатии, в частности, в условиях фрагментированного пользовательского опыта широкую популярность приобретает дипломатия в Телеграмм каналах в силу того, что они позволяют настраивать подачу информации не исходя из алгоритмов социальных сетей, а исходя из предпочтений пользователей (подписываться на различные каналы по интересам).

Поляризация мнений и широкое использованию ботов в социальных сетях, что в свою очередь провоцирует усталость пользователей от коммуникации. Сегодня, как отмечают исследователи, пользователи социальных сетей в основном используют их для получения информации, но в меньшей степени вовлекаются в создание нарративов и реже размещают авторский контент[391]. В этих условиях цифровая дипломатия вынуждена подстраиваться под предпочтения пользователей и апеллировать к отдельным группам, предлагая различные нарративы и фреймы, что в свою очередь усиливает фрагментацию.

[391] Dhir A. et al. Antecedents and consequences of social media fatigue //International Journal of Information Management. – 2019. – Т. 48. – С. 193-202.

Страны Запада и либеральные демократии во всем мире ослабили свое принципиальное воздержание от регулятивных мер контроля онлайн-коммуникаций. Совсем недавно противодействие иностранным кибератакам и кампаниям по дезинформации стало важной тенденцией в стратегиях безопасности во всем мире, что подстегнуло фрагментацию интернета. Как подчеркивают субъекты управления, суверенитет стал доминирующей целью в легитимных стратегиях онлайн-контроля. Легитимные стратегии демократического суверенитета допускают сдвиги в регулировании в сторону мер в отношении онлайн-контента и участников на основе происхождения на нескольких уровнях (государственное регулирование, совместное регулирование и саморегулирование)[392].

2.2.2. Международное управление Интернетом

На сегодняшний день проблематика управления интернетом включает в себя более широкий круг вопросов и включает в себя вопросы защиты прав человека в глобальном информационном пространстве, преодоления цифрового разрыва, обеспечения информационной безопасности. Именно вопросы информационной безопасности на сегодняшний день занимают приоритетное место на глобальной повестке дня и играют важнейшую роль в международном сотрудничестве в области управления интернетом.

В условиях, когда цифровое пространство милитаризируется и использование цифровых инструментов является неотъемлемой частью войн и конфликтов, для дипломатов и дипломатических ведомств становится важным не столько использовать социальные сети для

[392] Schünemann W. J., Kneuer M. Do not disturb! Studying discourses of democratic sovereignty as potential drivers of Internet fragmentation through online control //ISA Annual Convention. – 2021. URL: https://www.researchgate.net/profile/Marianne-Kneuer/publication/353351837_Do_not_disturb_Studying_discourses_of_democratic_sovereignty_as_potential_drivers_of_Internet_fragmentation_through_online_control/links/60f71eee0c2bfa282aeeedbb/Do-not-disturb-Studying-discourses-of-democratic-sovereignty-as-potential-drivers-of-Internet-fragmentation-through-online-control.pdf

донесения информации до широкой международной аудитории, сколько формировать правила, управляющие цифровым пространством как таковым. При этом важнейшей задачей выработки подобных правил является предотвращение эскалации межгосударственных противоречий в цифровом пространстве. Россия исходит из необходимости мирного развития глобальной ИКТ среды, уважения государственного суверенитета, невмешательства во внутренние дела государств и предотвращения конфликтов в ИКТ-среде[393].

Сторонники суверенитета Интернета, напротив, подчеркивают примат национальных границ и автономию государств в регулировании Интернета внутри страны и в глобальном масштабе. Главным требованием суверенитета Интернета является то, что Интернет не отличается от других типов коммуникационных технологий и, как и в случае с радио или телевидением, конечная власть по управлению онлайн-доменом принадлежит национальному государству. Многосторонность – традиционные межправительственные структуры и форумы, такие как Международный союз электросвязи ООН – это модель, необходимая для устойчивого развития системы управления интернетом[394].

Можно говорить о складывающейся многополярной системе в глобальном информационном пространстве. Однако, современный международный режим управления интернетом не отражает ее ключевых характеристик. На сегодняшний день международный режим управления интернетом характеризуется непропорциональным влиянием США[395]. Фактически, функции управления пространством имен и адресов интернета осуществляются частной компанией, зарегистрированной в США. В 2022 году Украина обратилась в ICANN с предложением

---

[393] Зиновьева Е. С. Глобальное управление Интернетом: российский подход и международная практика //Вестник МГИМО Университета. – 2015. – №. 4 (43). – С. 111-118.
[394] Зиновьева Е. С. Глобальное управление Интернетом: российский подход и международная практика //Вестник МГИМО Университета. – 2015. – №. 4 (43). – С. 111-118.
[395] Зиновьева Е. С. Международное управление Интернетом: конфликт и сотрудничество. – М.: МГИМО, 2011.

отключить домен России от глобального интернета[396]. Это предложение было отвергнуто, однако показало политизированный характер современной системы управления интернетом.

Развитие Интернета и механизмов управления интернетом – это продукт либерального мирового порядка[397]. Россия выступает за передачу функций управления интернетом на уровень международной организации, в рамках которой решения принимаются по принципу – одна страна – один голос. При этом со стороны США актуализируется запрос на формирование закрытых форматов международного сотрудничества. В частности, США выступили с инициативой Декларации за будущее интернета[398], к которой на сегодняшний день присоединились порядка 60 стран, прежде всего, союзников США. Показательно, что Россию и КНР не пригласили к участию в данной инициативе. Руководитель недавно созданного в рамках Государственного департамента США Бюро по цифровой политике и кибер-дипломатии заявил, что нормы более эффективны для сплочения союзников, чем для сдерживания противников. Показательно, что в Стратегии кибер-безопасности США от 2023 года именно Россия и Китай названы в числе основных вызовов лидерству США в цифровом пространстве[399].

В этих условиях актуализируется вопрос выработки правил в области управления интернетом на международном уровне. Россия давно выступает в поддержку интернационализации международного управления интернетом и передачи соответствующих функций на уровень международной организации. Важно отметить, что на современном этапе эти правила будут включать в себя не только вопросы международной

---

[396] Украина требует отключить Россию от Интернета // CNews, 02.03.2022. URL: https://www.cnews.ru/news/top/2022-03-02_ukraina_prosit_vygnat_rossiyu

[397] Nanni R. The Rise of China, Internet Fragmentation, and the Future of Multistakeholderism: Implications for the Liberal International Order //Rising China and Internet Governance: Multistakeholderism, Fragmentation and the Liberal Order in the Age of Digital Sovereignty. – Singapore : Springer Nature Singapore, 2024. – C. 143-163.

[398] Declaration for the Future of `Internet. USA Department of State, 2022. https://www.state.gov/declaration-for-the-future-of-the-internet

[399] https://www.weforum.org/agenda/2023/03/us-national-cybersecurity-strategy/

информационной безопасности, но и регулирования новых перспективных технологий, в том числе Больших данных, искусственного интеллекта, машинного обучения и ряда других.

На сегодняшний день возрастает число международных инициатив, направленных на регламентацию перспективных направлений технологического развития, в том числе регулирования потоков больших данных. Показательно, что и в этой области управления интернетом мы наблюдаем скорее конкуренцию различных подходов. Так, в 2020 году МИД КНР выступил с глобальной инициативой в области безопасности данных, в которой отмечается важность защиты персональных данных, уважения государственного суверенитета в области данных, а также центральной роли ООН в международном сотрудничестве на данном направлении[400]. Россия поддержала видение КНР. Показательно, что в настоящее время страны Запада выступают с альтернативными инициативами, стремясь оспорить регуляторную инициативу Китая на данном направлении. в числе которых Рекомендации ОЭСР в области регулирования технологий искусственного интеллекта[401] и инициатива на уровне Группы семи в области регулирования трансграничных потоков данных[402]. Схожая конкуренция проектов в области управления передовыми технологиями наблюдается и в области технологий искусственного интеллекта, регулирования 5G – сетей связи нового поколения, а также регламентации технологий Интернета вещей и других.

При этом важно отметить, что международная политика даже в условиях многополярности и нарастающей международной конфликтности характеризуется высокой степенью взаимозависимости, в том числе в сфере цифровой безопасности. Это диктует необходимость

---

[400] Глобальная инициатива в области безопасности данных МИД КНР, 2020 (на английском языке) // Global Initiative on Data Security. MFA of PRC, 08 September, 2020.

[401] Recommendation of the Council on Artificial Intelligence, 2019 OECD/LEGAL/0449

[402] Дорожная карта «Группы семи» по сотрудничеству в области свободных потоков данных и доверия. Лондон, 2021 (на английском языке) - извлечение

диалога и выработки согласованных подходов регулирования передовых цифровых технологий. Важнейшую роль в обсуждении возможных направлений международного взаимодействия в данной области призван играть Форум по вопросам управления интернетом, в том числе в области перспективных технологий, таких как регулирование Больших данных и технологий искусственного интеллекта.

2.2.3. Цифровая экономика и цифровой суверенитет

Важнейшей составляющей цифровых международных отношений являются цифровые международные экономические отношения. Цифровая экономика охватывает экономические деятельности, основанные на цифровых технологиях и интернет-сервисах. Цифровое измерение экономики включает в себя электронную коммерцию, цифровые финансовые технологии (финтех), деятельность платформенных компаний, а также ряд других направлений. В целом же, необходимо отметить, что в настоящее время происходит размывание грани между реальной и виртуальной экономикой - «как не существует чистых интернет предприятий (интернет уже охватил всю социальную инфраструктуру), так и не существует чистых традиционных отраслей, потому что в них уже активно используется Интернет»[403]. Ярким примером использования продуктивного и конструктивного потенциала цифровых технологий является Китай. На 2019 год цифровой экономикой было охвачено 30% ВВП Китая, благодаря цифровизации удалось создать 2.8 млн. рабочих мест, обеспечить ежегодный рост занятости на 21%.[404]

---

[403] Ма Хуатэн, Мэн Чжоли, Ян Дели, Ван Хуалей. Цифровая трансформация Китая. М.: Альпина, 2019. С. 47-49

[404] China’s digital transformation. McKinsey and Company. URL: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/chinas-digital-transformation

Согласно оценкам McKinsey 2025 году интернет-приложения могут обеспечить до 22 процентов роста ВВП КНР[405], и в целом значимость экономического измерения цифрового суверенитета в экономике возрастает.

В основе современной цифровой экономики лежат платформенные решения, которые меняют природу современной экономики, как в национальном, так и в глобальном масштабе. Крупнейшие такие платформы – Apple, Microsoft, Amazon, Alphabet (Google), Tencent и Alibaba, а также российские Яндекс, Сбер и ряд других – все активнее инвестируют во все звенья глобальной цепочки создания стоимости данных: сбор данных с помощью сервисов платформы, ориентированных на пользователей; передача данных по подводным кабелям и спутникам; хранение данных (центры обработки данных); а также анализ, обработка и использование данных, например, с помощью ИИ.

Эти компании имеют конкурентное преимущество в области данных благодаря своему платформенному компоненту, но они больше не являются просто цифровыми платформами. Они стали глобальными цифровыми корпорациями с планетарным охватом; огромная финансовая, рыночная и технологическая мощь; и контроль над большими объемами данных о своих пользователях. И они увидели, что их размер, прибыль, рыночная стоимость и доминирующие позиции укрепились во время пандемии, поскольку цифровизация ускорилась[406].

Цифровые технологии облегчают трансграничную торговлю, расширяя рынки для бизнеса и потребителей. Важнейшим элементом цифровой торговли является онлайн банкинг, который предполагает использование цифровых платформ для банковских операций, включая переводы, кредиты и инвестиции. Новые технологии, такие как биткойн и

---

[405] Там же

[406] UNCTAD Digital Economy report. 2021. URL: https://unctad.org/system/files/official-document/der2021_overview_en_0.pdf

блокчейн, меняют финансовый ландшафт, предлагая альтернативные методы платежей и контрактов. Цифровые платформенные компании, такие как Uber и Airbnb, которые предоставляют новые модели бизнеса и занятости.

Особенностью современного этапа цифровой революции является широкое распространение мобильного интернета. В январе 2007 года компания Apple выпустила iPhone нового поколения и это событие стало рубежом в истории развития Интернета – заложило основу формирования постмобильного интернета. Это событие изменило бизнес-модель интернета и цифровой экономики – появились модели экономики совместного потребления.

В цифровой экономике наступила постмобильная эпоха. Большую отдачу от инвестиций приносят не инвестиции в мобильный интернет и инфраструктуру, а в технологии, которые могут работать на основании мобильного интернета[407].

Развитие национальной цифровой экономики предполагает реализацию государственной политики по защите суверенитета в данной области, В частности, защиту рынков путем регулирования деятельности иностранных компаний, в том числе цифровых платформ. Цифровой суверенитет в экономике также предполагает государственную поддержку стартапов и инноваций в рамках национальной экономики, с тем чтобы снизить зависимость от внешних технологий и способствовать экономическому росту.

Цифровая экономика и цифровой суверенитет являются важными элементами современной политики. Государства вынуждены балансировать между развитием цифровой экономики, поддержкой инноваций и защитой своих национальных интересов в цифровом пространстве, что проявляется в разработке комплексных стратегий,

[407] Ма Хуатэн, Мэн Чжоли, Ян Дели, Ван Хуалей. Цифровая трансформация Китая. М.: Альпина, 2019. С. 47-49

углублении сотрудничества с частным сектором и участия в международных инициативах и соглашениях.

Поскольку роль данных как экономического ресурса, а также роли трансграничных потоков данных стала более актуальной, появились новые измерения цифрового разрыва в связи с «цепочкой создания стоимости данных»[408]. Эта концепция является ключевой для оценки ценности данных. Ценность возникает в процессе преобразования необработанных данных – от сбора данных, анализа и обработки в цифровой интеллект – который можно монетизировать в коммерческих целях или использовать для социальных целей. Отдельные данные не имеют никакой ценности, если они не агрегированы и не обработаны. И наоборот, без необработанных данных не могут развиваться технологии машинного обучения и искусственного интеллекта.

По мере развития цифровой экономики, основанной на данных, усугубился цифровой разрыв. В этой новой конфигурации развивающиеся страны могут оказаться в подчиненном положении, поскольку данные и связанная с ними стоимость будут сосредоточены в руках нескольких глобальных цифровых корпораций и других транснациональных предприятий, которые контролируют данные. Они рискуют стать поставщиками необработанных данных для глобальных цифровых платформ, при этом им придется платить аналитику данных и другие цифровые услуги, основанные на данных, ими же поставляемых[409].

ИКТ дают возможности для предоставления высококачественных товаров и услуг, в том числе в здравоохранении, образовании, финансах, торговле, управлении, сельском хозяйстве и других важнейших областях. Они могут помочь в сокращении масштабов нищеты и голода, в повышении уровня здоровья, создании новых рабочих мест, смягчении

[408] UNCTAD Digital Economy Report 2021

[409] UNCTAD Digital Economy Report 2021. URL: https://unctad.org/system/files/official-document/der2021_overview_en_0.pdf

последствий изменения климата, повышении энергоэффективности и устойчивости городов и сообществ.

2.2.4. Международная информационная безопасность

Согласно Основам государственной политики Российской Федерации в области международной информационной безопасности от 2021 года, «Международная информационная безопасность представляет собой такое состояние глобального информационного пространства, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного партнерства обеспечивается поддержание международного мира, безопасности и стабильности»[410].

Документ выделяет шесть основных угроз международной информационной безопасности:

«а) использование информационно-коммуникационных технологий в военно-политической и иных сферах в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности государств, осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира, безопасности и стабильности;

б) использование информационно-коммуникационных технологий в террористических целях, в том числе для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

в) использование информационно-коммуникационных технологий в экстремистских целях, а также для вмешательства во внутренние дела суверенных государств;

---

[410] Основы государственной политики Российской Федерации в области международной информационной безопасности. Утверждены Указом Президента Российской Федерации от 12 апреля 2021 г. № 213. URL: http://www.scrf.gov.ru/security/information/document114/

г) использование информационно-коммуникационных технологий в преступных целях, в том числе для совершения преступлений в сфере компьютерной информации, а также для совершения различных видов мошенничества;

д) использование информационно-коммуникационных технологий для проведения компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру;

е) использование отдельными государствами технологического доминирования в глобальном информационном пространстве для монополизации рынка информационно-коммуникационных технологий, ограничения доступа других государств к передовым информационно-коммуникационным технологиям, а также для усиления их технологической зависимости от доминирующих в сфере информатизации государств и информационного неравенства[411].

Первоначально наиболее распространенным подходом к определению природы угроз международной информационной безопасности было выделение их триады по принципу выявления субъектов: военно-политические, террористические и преступные угрозы международной информационной безопасности. Данный подход впервые был сформулирован в резолюции ГА ООН 1999 года «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[412].

Цифровизация одномоментно уменьшила разрыв в военно-стратегических потенциалах государств мира, раньше казавшийся непреодолимым: теперь сравнительно низкозатратными кибернетическими средствами стало возможно нанести государству-

[411] Там же.
[412] Международная информационная безопасность: теория и практика / Под ред. А.В. Крутских. М.: Аспект-Пресс, 2019.

сопернику пусть и не критический, но существенный ущерб. Рост использования цифровых технологий в военном деле, таким образом, сместил акценты в военно-технологической конкуренции держав[413].

По причине политических противоречий существуют определенные терминологические разночтения в сфере международной информационной безопасности. Государства, а также международные организации на уровне официальных документов используют различные термины: «информационная безопасность», «кибербезопасность», «безопасность ИКТ», «безопасность использования ИКТ и самих ИКТ», «компьютерная безопасность». Разночтения существуют и на уровне научной литературы[414]. Термин «кибербезопасность» предполагает акцент на технологических угрозах, в то время как «информационная безопасность» ориентирована на учет и технических, и политико-идеологических аспектов. В прессе и публицистических материалах в России и за рубежом чаще используется «кибертерминология» в силу ее популярности и узнаваемости среди широкой аудитории. Кроме того, неизбежно ее использование для обозначения и описания подходов западных государств[415].

Однако трактовки того, что составляет объект информационной безопасности, существенно варьируются. Как правило, причина различий в терминологии кроется в особенностях национальных интересов государств.

Россия стала пионером в области международного сотрудничества по обеспечению информационной безопасности. Первые ее внешнеполитические инициативы на данном направлении были предложены еще в 1998 г. Изначально Россия на ориентировала

---

[413] Безруков А., Мамонов М., Ребро О., Сушенцов А. Реалполитик в цифре: суверенитет, союзы и неприсоединение в XXI веке // Валдай, 2021. URL: https://ru.valdaiclub.com/files/39047/

[414] См. напр.: Международная информационная безопасность: теория и практика / Под ред. А.В. Крутских. М.: Аспект-Пресс, 2019.

[415] Зиновьева Е., Мищишина Е. Формирование универсальной терминологии в сфере МИБ: политические аспекты // РСМД. 14.07.2022. URL: https://russiancouncil.ru/analytics-and-comments/analytics/formirovanie-universalnoy-terminologii-v-sfere-mib-politicheskie-aspekty/

международное сообщество на широкую трактовку термина «международная информационная безопасность»[416]. Схожий подход был представлен и в научной литературе российских авторов по данной теме[417]. Информационная безопасность рассматривалась комплексно, причем исследователи выделяли информационно-технологическое измерение (безопасность сетей, систем и данных) и политико-идеологическое измерение (проблемы воздействия на общественное мнение, прежде всего в контексте инспирирования «цветных революций» по информационным каналам). Вызовы информационной безопасности в политико-идеологическом контексте прежде всего связаны с внутренним суверенитетом государств и ставят под вопрос возможность правительств контролировать ход событий, обеспечивать общественную стабильность и безопасность. Именно это представляет собой ключевую угрозу информационной безопасности в ее социогуманитарном понимании. В условиях широкого распространения Интернета особое значение имеет работа с общественным мнением как внутри страны, так и на международной арене. Контроль над информационным пространством выступает в качестве инструмента «мягкой силы», то есть способности воздействовать на ценностные установки зарубежной аудитории и процессы восприятия.

Российское видение угроз МИБ столкнулось с неприятием со стороны стран Запада. В частности, США во внешнеполитическом дискурсе продвигали термин «кибербезопасность»[418]. Согласно данному подходу, на международном уровне регулированию подлежат исключительно технологические аспекты информационной безопасности, в то время как термин «информационная безопасность» предполагает

---

[416] Доктрина информационной безопасности Российской Федерации. Утв. указом Президента РФ в 2000 г.

[417] Федоров А.В., Зиновьева Е.С. Международная информационная безопасность: политическая теория и дипломатическая практика. М.: 2017.

[418] National Cybersecurity Strategy USA. White House, 2017. URL: https://www.whitehouse.gov/oncd/national-cybersecurity-strategy/

обеспечение не только технической безопасности информационных сетей и систем, но и информационно-психологическую безопасностью, регулирование контента. Общее в двух подходах – их ориентация на использование информационно-коммуникационных технологий, так как главные угрозы безопасности рассматриваются в качестве порожденных или усиленных в результате глобальной информатизации.

Современная научная литература западных исследователей сосредоточена на исследовании технических аспектов проблематики. Обеспечение информационно-технической безопасности включает в себя защиту, контроль и соблюдение правопорядка в телекоммуникационной сфере: защита от несанкционированного доступа, хакерских взломов компьютерных сетей и сайтов, логических бомб, компьютерных вирусов и вредоносных программ, несанкционированного использования частот, радиоэлектронных атак и пр. Безусловно, данная проблематика представляется крайне важной, на данном направлении необходимо развивать и углублять международное сотрудничество[419]. Прежде всего, в контексте технического измерения информационной безопасности выделяют угрозы критическим информационным инфраструктурам. Ключевой задачей государства и бизнеса в этом контексте является обеспечение безопасности ключевых информационных систем и инфраструктуры, таких как энергетические сети, банковская система и правительственные серверы. Однако угрозы международной безопасности, порождаемые развитием новых цифровых технологий, не ограничиваются исключительно технологическим измерением. В контексте международного сотрудничества западная академическая литература посвящена изучению вопросов международно-правовой

[419] Choucri N., Madnick S., Ferwerda J. Institutions for cyber security: International responses and global imperatives //Information Technology for Development. – 2014. – Т. 20. – №. 2. – С. 96-121.

регламентации кибер-безопасности, выработки социальных норм и стандартов в данной области[420].

Манипулирование общественным мнением в цифровую эпоху представляет значительный вызов для суверенитета государств. Цифровые платформы и социальные сети предоставляют новые возможности для влияния на общественное мнение, что может подрывать демократические процессы, стабильность и национальную безопасность. Использование социальных сетей и других цифровых платформ для распространения ложных новостей с целью ввести в заблуждение общественность и создать хаос.

Важнейшую роль в формировании режима информационной безопасности на глобальном уровне играет ООН, в рамках которой ведется обсуждение проблем МИБ на нескольких площадках. Так, в системе ООН данной проблематикой занимается созданная по инициативе России Рабочая группа открытого состава по международной информационной безопасности (РГОС). В рамках работы РГОС ведется обсуждение правил ответственного поведения государств в глобальном информационном пространстве[421]. Запущенная по инициативе России РГОС является единственным открытым и всеохватным переговорным механизмом по проблематике международной информационной безопасности (МИБ) под эгидой ООН. В ходе секций РГОС российские дипломаты дипломаты представили концепцию конвенции ООН об обеспечении МИБ, проект реестра контактных пунктов для обмена информацией о компьютерных инцидентах, а также видение будущего формата регулярного диалога по МИБ в ООН. Задача – формирование международно-правового режима

---

[420] См. напр.: Verhelst A. et al. Filling global governance gaps in cybersecurity: International and european legal perspectives //International Organisations Research Journal. – 2020. – Т. 15. – №. 2. – С. 105-124; 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.

[421] Об итогах четвертой сессии Рабочей группы открытого состава ООН по международной информационной безопасности // МИД России. Сообщение для СМИ. 13.03.2023. URL: https://www.mid.ru/ru/foreign_policy/news/1857793/?TSPD_101_R0=08765fb817ab2000522cf443de94605ea9dcff02ff9ef7e64e25653cff399ec217cab25640ec211f08edae8ec01430009ad98ca41fa59b9036feb15d12831d421893c57d819cf241aaee168f699a6336f8cb087c4d577e76b92a0193895c4780

регулирования сферы ИКТ и укрепление практического сотрудничества государств по линии компетентных ведомств в данной области[422].

С 2019 года в системе ООН также действует Специальный комитет ООН по выработке конвенции в области противодействия киберпреступности, на которой был представлен российский проект Конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях[423]. Данный комитет также был создан по инициативе Российской Федерации.

В Китае обеспечение информационной безопасности является одним из приоритетов. Кибербезопасность стала ключевой областью регулирования в цифровом обществе, экономике и государстве Китая[424]. Это обусловлено необходимостью обеспечить гарантии безопасности для реализации амбициозной политики «информатизации», символом которой стало принятие Закона о кибербезопасности в 2016 году[425]. Кибербезопасность также стала интегрированной в общую национальную безопасность и рассматривается как важнейшая компонента цифрового суверенитета[426].

В академической литературе информационно-психологический аспект противостояния, в том числе в контексте зарубежной пропаганды в последние годы все чаще осмысливается в категориях когнитивного противоборства.

С конца 1990-х годов Китай проводит политику «информатизации», которая влечет за собой внедрение цифровых технологий во всех значимых сферах экономической и социальной жизни, а также в деятельности

---

[422] Там же.
[423] Под статью подвели не все // Коммерсант. 12.01.2024. URL: https://www.kommersant.ru/doc/6452715
[424] Cheung T. M. The rise of China as a cybersecurity industrial power: Balancing national security, geopolitical, and development priorities //Journal of Cyber Policy. – 2018. – Т. 3. – №. 3. – С. 306-326.
[425] Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017) URL: https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/#:~:text=Any%20person%20and%20organization%20using,interests%3B%20they%20must%20not%20incite
[426] Creemers R. Cybersecurity Law and regulation in China: Securing the smart state //China Law and Society Review. – 2023. – Т. 6. – №. 2. – С. 111-145.

правительства. В 2014 году создание Центральной ведущей группы по кибербезопасности и информатизации под председательством президента Си Цзиньпина вывело цифровую политику на высший приоритетный уровень и способствовало развитию «стратегии кибервласти»[427]. В 2020 году руководство обозначило данные как новый фактор производства, наравне с землей, капиталом и трудом. Четырнадцатый пятилетний план (2021–2025 годы) содержал несколько амбициозных планов по информатизации в целом, цифровому государственному управлению, цифровой экономике и финансовым технологиям. В этом контексте обеспечение безопасности данных и информационной безопасности стало приоритетом для КНР.

Си Цзиньпин заявил, что кибербезопасность неотделима от национальной безопасности, и этот вопрос быстро стал приоритетным, о чем свидетельствует принятие Закона о национальной безопасности[428] и создания Совета национальной безопасности[429]. К 2016 году Пекин опубликовал Национальную стратегию кибербезопасности[430], Стратегию международного сотрудничества в киберпространстве[431] и Закон о кибербезопасности[432], которые сформировали основу комплексного режима кибербезопасности, построение которого все еще продолжается. Этот режим состоит из ряда административных и ведомственных постановлений, изданных Государственным советом, Управлением киберпространства Китая и соответствующими министерствами, а также

---

[427] Being a Cyberpower – China's Ambitions in Cyberspace // TechPress.com. 12.02.2023. URL: https://www.techpolicy.press/being-a-cyberpower-chinas-ambitions-in-cyberspace/

[428] Опубликован перевод 14-го пятилетнего плана социально-экономического развития (2021-2025) // Российско-китайский деловой совет. URL: https://cset.georgetown.edu/publication/china-14th-five-year-plan/

[429] Там же.

[430] China announces cybersecurity strategy // Xinhua. 27.12.2016. URL: https://english.www.gov.cn/state_council/ministries/2016/12/27/content_281475526667672.htm

[431] China International Strategy of Cooperation on Cyberspace URL: http://news.xinhuanet.com/english/china/2017-03/01/c_136094371_5.htm

[432] Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017) URL: https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/#:~:text=Any%20person%20and%20organization%20using,interests%3B%20they%20must%20not%20incite

технических стандартов и соглашений о саморегулировании отраслевых ассоциаций и торговых организаций[433].

Сходных с Китаем позиций придерживается Российская Федерация. По словам заместителя Министра иностранных дел России О. Сыромолотова, с начала специальной военной операции на Украине атаки на российские интернет-ресурсы (в том числе госструктуры и СМИ) участились и стали более заметными. 20 мая 2022 г. под председательством Владимира Путина состоялось заседание Совета Безопасности Российской Федерации, на котором обсуждались вопросы повышения устойчивости и безопасности функционирования информационной инфраструктуры. Российский президент акцентировал внимание на актуальности этой темы, назвав ее «важнейшей для нашего суверенитета и безопасности, для экономики и для государственного управления, для общественной стабильности».

В России с апреля 2022 года действует межведомственная комиссия Совета безопасности по обеспечению технологического суверенитета России в IT-сфере[434].

2.2.5. Цифровая дипломатия

Цифровая дипломатия представляет собой эволюцию традиционных дипломатических методов и инструментов, адаптированных к реалиям цифрового мира. Цветкова Н.А. определяет ее как правительственный механизм влияния на поведение пользователей социальных сетей и концептуализирует как использование социальных сетей и иных цифровых инструментов для достижения внешнеполитических целей государства[435].

---

[433] Creemers R. Cybersecurity Law and regulation in China: Securing the smart state //China Law and Society Review. – 2023. – Т. 6. – №. 2. – С. 111-145.

[434] Путин поручил обеспечить сетевой суверенитет в рамках цифровой трансформации // ТАСС. 7.05.2924. URL: https://tass.ru/obschestvo/20736063

[435] Цветкова Н. А. Феномен цифровой дипломатии в международных отношениях и методология его изучения //Вестник РГГУ. Серия: Политология. История. Международные отношения. – 2020. – №. 2. – С. 37-47.

На современном этапе важным инструментом цифровой дипломатии становится искусственный интеллект. Искусственный интеллект оказывает значительное влияние на эту область, внося как новые возможности, так и новые вызовы – с одной стороны, ИИ позволяет дипломатам анализировать большие объемы данных из различных источников, включая социальные сети, новости и официальные документы, чтобы выявлять тренды и потенциальные кризисы, но при этом создает новые угрозы, связанные с информационной безопасностью, защитой данных и возможной алгоритмической предвзятостью.

Чат-боты и виртуальные ассистенты, работающие на базе ИИ, могут автоматизировать рутинные дипломатические задачи, такие как ответ на запросы граждан, координация встреч и предоставление информации. Чаще всего подобные инструменты используются в консульской работе и кризисной дипломатии.

Важнейшим инструментом современной цифровой дипломатии является использование социальных сетей. Социальные сети стали важным фактором во всех сферах жизни общества и государства, и одним из важнейших источников новостей и информации. Их использование определяет то, как люди общаются, работают и совершают покупки, и получают услуги. При этом, динамика и тенденции использования социальных сетей, в свою очередь, влияют на направления и тенденции развития цифровой дипломатии. Дипломаты и сотрудники международных организаций не могут игнорировать новую цифровую реальность и расширяют свое присутствие в интернете на различных площадках социальных сетей. В 2020 году рекордно быстрыми темпами росла сеть коротких-видео сообщений TikTok, соответственно, дипломаты и сотрудники международных организаций расширяли свое присутствие в этой сети.

Сегодня дипломатические ведомства управляют целыми «империями» социальных сетей. Послы при ООН используют

мессенджеры для координации голосования по различным вопросам на повестке дня организации, а пресс-атташе государств при международных организациях публикуют информацию о международных договоренностях на своих страницах в социальных сетях и используют их для общения с журналистами[436]. Цифровая дипломатия применялась во время переговоров по ядерной сделке с Ираном в 2013–2015 гг. [437], после воссоединения Крыма с Россией в 2014 г. [438], а затем во время пандемии COVID-19[439]. Весной 2020 г. был проведен ряд виртуальных встреч на высшем уровне с использованием средств видеоконференцсвязи лидеров «Группы двадцати», ООН, БРИКС.

Протекционизм, пандемия, санкционные войны и нарастающая международная конфликтность способствуют сворачиванию процессов глобализации, как она формировалась и осмысливалась начиная с 1980-х годов. Схожая динамика наблюдается и в глобальном информационном пространстве. Видение глобального интернета, в котором нет государственных границ не оправдало себя. Государства и региональные организации проводят практику «огораживания» и выделения национальных и региональных сегментов глобальной сети. Особенно заметным является пример Китая, где с 1996 года ведется политика по укреплению цифрового суверенитета, наиболее заметным символом и воплощением которой является Великий китайский файрволл. На уровне ЕС в последние годы также активизируются инициативы, направленные на формирование технологического и цифрового суверенитета государства.

Широкое распространение получает практика кибер- дипломатии – то есть использования информационно-коммуникационных технологий, прежде всего, социальных сетей в дипломатической работе и

[436] Manor I. Digitalization of public diplomacy. Springer, 2019.
[437] Duncombe C. Twitter and the challenges of digital diplomacy //SAIS Review of International Affairs. – 2018. – Т. 38. – №. 2. – С. 91-100.
[438] Bjola C., Pamment J. Introduction: the ‘dark side’of digital diplomacy //Countering Online Propaganda and Extremism. – Routledge, 2018. – С. 1-10.
[439] Bramsen I., Hagemann A. The missing sense of peace: diplomatic approachment and virtualization during the COVID-19 lockdown //International Affairs. – 2021. – Т. 97. – №. 2. – С. 539-560.

международных переговорах, а также вопросы выработки правил, регулирующих современную цифровую сферу. Это особенно важно, поскольку изначально цифровая дипломатия рассматривалась исключительно как инструмент продвижения мягкой силы, однако на современном этапе она становится важным фактором информационного противоборства.

Вывод по параграфу:

Формирование глобального цифрового пространства сопровождается глубокими изменениями в международной политике, которые отражают как потенциал, так и угрозы цифровой трансформации. С одной стороны, технологии открывают новые возможности для взаимосвязи, сотрудничества и экономического роста, усиливая глобализацию и расширяя доступ к информации. С другой стороны, растет обеспокоенность по поводу усиления неравенства, доминирования отдельных государств и транснациональных корпораций, а также угроз кибербезопасности, которые ставят под сомнение стабильность международного порядка.

Глобальное цифровое пространство становится ареной соперничества, где государственные и негосударственные акторы формируют свои стратегии, опираясь на технологические достижения. Развитие технологий четвертой промышленной революции, таких как искусственный интеллект, интернет вещей, облачные вычисления и блокчейн, меняет привычные подходы к управлению, безопасности и экономическому развитию. Эти технологии не только повышают эффективность процессов, но и создают новые линии разлома, влияя на распределение власти и ресурсов в международной системе.

Текущие тенденции демонстрируют, что цифровая революция переходит в стадию усиления национальных и региональных инициатив, таких как создание автономных интернет-платформ, внедрение защитных мер для данных и регулирование потоков информации. Эти меры часто

направлены на сохранение суверенитета в условиях глобальной взаимозависимости, но могут привести к фрагментации мирового цифрового пространства и созданию конкурирующих технологических экосистем. Государства стремятся адаптироваться к новым вызовам, одновременно пытаясь диктовать правила игры на глобальной арене.

Таким образом, формирование глобального цифрового пространства, ускоряемое технологиями четвертой промышленной революции, – это сложный, противоречивый и многослойный процесс. Он требует не только инновационных подходов к сотрудничеству и управлению, но и глубокого переосмысления традиционных концепций международной политики. В условиях стремительного технологического прогресса стабильность и безопасность цифрового пространства становятся важнейшими вызовами для будущего международных отношений.

2.3. Концептуализация цифровой революции в современной науке о международных отношениях

Теория международных отношений изучает природу международной системы, а также ее субъектов – прежде всего, государств, однако, в последние десятилетия, также и негосударственных акторов. Развитие цифровых технологий и складывание цифровых международных отношений также осмысливается в теоретических трудах в области международных отношений. При этом каждое теоретическое направление в международных отношениях предлагает уникальное видение суверенитета государства и ее роли в международной системе.

В то время как реализм и неореализм подчеркивают значимость военной и экономической мощи, либерализм акцентирует внимание на взаимозависимости и роли международных институтов. Конструктивизм фокусируется на социальных конструкциях и дискурсах, а марксизм – на

экономических структурах и классовых отношениях. Феминизм и постколониализм вносят важные перспективы, анализируя власть через призму гендерных и постколониальных аспектов. Все это позволяет лучше понять категорию цифрового суверенитета и выявить ее функциональное и концептуальное наполнение.

2.3.1. Институционализм о природе цифровых международных отношений

Институционализм в теории международных отношений – это направление, которое акцентирует внимание на роли международных институтов и организаций в формировании и поддержании международного порядка и сотрудничества между государствами. Существуют научные школы в рамках подхода институционализма, каждая из которых делает акцент на разных аспектах международного взаимодействия.

Неолиберальный институционализм исходит из того, что международные институты и организации играют ключевую роль в содействии сотрудничеству между государствами, снижении транзакционных издержек и преодолении проблем коллективного действия[440]. Согласно данному подходу в условиях комплексной взаимозависимости возрастает влияние институтов, которые в свою очередь размывают суверенитет, который, тем не менее, не исчезает полностью[441]. В цифровой сфере данный подход делает акцент на усиление трансграничных связей и транзакций, которые действительно имеют место быть. Статистика подтверждает рост объема трансгранично передаваемых

[440] Keohane R. O., Nye Jr J. S. Power and interdependence //Survival. – 1973. – Т. 15. – №. 4. – С. 158-165; Keohane R. O., Nye J. Globalization: what's new? What's not?(And so what?) //Foreign Policy. – 2003. – Т. 118.

[441] Nye J. S. The information revolution and the paradox of American power //Proceedings of the ASIL Annual Meeting. – Cambridge University Press, 2003. – Т. 97. – С. 67-75.

данных, что в свою очередь усиливает взаимозависимость государств, в том числе в сфере информационной безопасности, регулирования цифровой экономики и др. Согласно данному подходу, решение общих вызовов лежит в плоскости международного сотрудничества, как на уровне международной системы, так и отдельных регионов и субрегиональных структур.

Кроме того, данный подход представляется полезным для анализа динамики цифрового суверенитета в рамках интеграционных структур[442]. Согласно институционализму, в условиях взаимозависимости, сотрудничая, государства передают часть суверенитета на уровень интеграционных объединений, с тем чтобы более эффективно решать общие задачи. Именно данный подход хорошо объясняет феномен политики «цифрового суверенитета ЕС»[443].

Социологический институционализм фокусируется на культурных и идеологических аспектах международных институтов, утверждая, что институты формируют идентичности и нормы поведения государств[444]. Во многом данный подход смыкается с конструктивизмом, анализируя нормы поведения государств как социально сконструированные факторы, влияющие на их поведения, в том числе в цифровой среде[445].

В целом институционализм утверждает, что международные институты создаются государствами как рациональные акты для решения конкретных проблем и увеличения их выгод через сотрудничество. Институты упрощают процессы взаимодействия между государствами, снижая издержки на переговоры и заключение соглашений. Международные организации помогают следить за соблюдением договоренностей и обеспечивать выполнение обязательств.

---

[442] Lake D. A. Delegating divisible sovereignty: Sweeping a conceptual minefield //The Review of International Organizations. – 2007. – Т. 2. – С. 219-237.

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

[444] Цыганков П.А., Цыганков А.П. Социология международных отношений. М.: Аспект-Пресс, 2007.

[445] Powell W. W., DiMaggio P. J. (ed.). The new institutionalism in organizational analysis. – University of Chicago press, 2012.

Международные институты разрабатывают и продвигают стандарты и нормы поведения, которые способствуют предсказуемости и стабильности международных отношений. Институты способствуют распространению идей и ценностей, таких как права человека, демократическое управление и устойчивое развитие. Международные организации предоставляют платформы для мирного разрешения споров между государствами через переговоры, арбитраж и судебные разбирательства.

Некоторые критики утверждают, что международные институты часто не способны эффективно решать глобальные проблемы из-за недостатка полномочий и ресурсов. Институты могут отражать интересы мощных государств и усиливать неравенство в международной системе, пренебрегая интересами менее влиятельных стран. Механизмы и процедуры международных организаций могут становиться излишне сложными и бюрократическими, что снижает их эффективность и адаптивность.

2.3.2. Неомарксизм и цифровые международные отношения

Неомарксизм фокусируется на анализе глобального капитализма, классовой борьбы и неравенства в контексте международных отношений[446]. В эпоху цифровой трансформации неомарксисты исследуют, как цифровые технологии влияют на глобальные экономические и политические структуры, подчеркивая вопросы эксплуатации, контроля и доминирования.

Неомарксисты утверждают, что цифровые технологии способствуют концентрации капитала в руках небольшого числа глобальных

[446] Budd A. Transnationalist Marxism: a critique //Contemporary Politics. – 2007. – Т. 13. – №. 4. – С. 331-347; Linklater A. The changing contours of critical international relations theory //Critical theory and world politics. – 2001. – С. 23-44.

корпораций, таких как Google, Amazon, и Apple[447]. Анализ условий труда в таких платформах, как Uber и Deliveroo, показывает высокую степень эксплуатации и отсутствие социальных гарантий для работников.

Развитие цифровых технологий усиливает экономическое неравенство как внутри стран, так и между ними, способствуя доминированию развитых стран и транснациональных корпораций. Переход к цифровой экономике изменяет характер труда, увеличивая долю нестабильной и низкооплачиваемой занятости, особенно в таких секторах, как гиг-экономика. Цифровые платформы контролируют огромные объемы информации и данных, что позволяет им влиять на общественное мнение и политические процессы. Глобальные цифровые компании распространяют культурные нормы и ценности, которые поддерживают существующую систему капиталистического доминирования и нормы капитализма потребления, но в области данных[448].

Неомарксисты подчеркивают, что государство играет ключевую роль в поддержании капиталистической системы, регулируя цифровые технологии в интересах правящего класса. Государства стремятся контролировать цифровую инфраструктуру и данные для защиты национальных интересов, но часто оказываются под влиянием транснациональных корпораций. Цифровые компании собирают и монетизируют данные пользователей, что вызывает вопросы о приватности и защите данных[449].

Исследования показывают, что цифровой разрыв между развитыми и развивающимися странами увеличивается, усиливая глобальное экономическое неравенство. Инвестиции в развитие ИИ и других передовых технологий для поддержания технологического лидерства.

---

[447] Gabrys J. et al. Reworking the political in digital forests: The cosmopolitics of socio-technical worlds //Progress in Environmental Geography. – 2022. – Т. 1. – №. 1-4. – С. 58-83.
[448] Смит Д. Империализм в XXI веке М.: Горизонталь, 2022.
[449] Kucuk S. U. Consumerism in the digital age //Journal of Consumer Affairs. – 2016. – Т. 50. – №. 3. – С. 515-538.

Неомарксизм предлагает ценный аналитический инструмент для понимания цифровых международных отношений, подчеркивая вопросы власти, контроля и неравенства в контексте глобального капитализма. Цифровые технологии открывают новые возможности, но также создают серьезные вызовы, требующие комплексного подхода к их регулированию и использованию в интересах всех слоев общества. Международное сотрудничество, справедливые экономические модели и защита прав трудящихся являются ключевыми аспектами для достижения устойчивого и справедливого цифрового будущего.

2.3.3. Неореализм о природе суверенитета государства в цифровых международных отношениях

Неореализм, также известный как структурный реализм, является одной из ведущих теорий международных отношений. Он акцентирует внимание на структурных аспектах международной системы и утверждает, что поведение государств определяется не столько внутренними характеристиками, сколько структурой самой международной системы. Основным вкладом в теорию неореализма является работа Кеннета Уолтца, особенно его книга «Теория международной политики»[450]. Кеннет Уолтц внес значительный вклад в теорию международных отношений, предложив системный подход к пониманию международной политики. Его работа фокусируется на структурных факторах, определяющих поведение государств, и на важности системного уровня анализа для объяснения международных явлений.

Международная система анархична, не имеет верховного управляющего органа. Государства существуют в среде, где нет центральной власти, способной обеспечивать безопасность и порядок.

[450] K Waltz. Theory of International Politics. Reading, 1979

Государства рассматриваются как основные участники международных отношений, и они действуют как рациональные единицы, стремящиеся к выживанию и безопасности в условиях анархии[451].

Для К. Уолтца суверенитет означает что государство определяет само, как оно будет внутренние и внешние проблемы, включая то, будет ли оно искать помощи у внешних государств и через принятие обязательств ограничить свою свободу. Суверенные государства сами формируют свою стратегию, свой курс и все остальное на, что направлена их деятельность[452]. Он также подвергал сомнению концепцию глобализма, популярную в академической литературе в 1990-е гг., отмечая, что чем сильнее взаимозависимость, темы выше роль государства в международной системе. Отечественный исследователь В.Н. Конышев отмечает, что в данном контексте суверенитет не предполагает полной независимости государства[453]. Современные тенденции в цифровых международных отношениях в целом подтверждают данный тезис.

Другой видный неореалист Ст. Краснер отмечает, что суверенитет на практике всегда изменяется, будучи одновременно и инструментом контроля, и правовым принципом юридической независимости государств[454].

В условиях анархии государства стремятся к обеспечению своей безопасности через создание баланса сил. Это может включать военное наращивание, формирование союзов и стратегические альянсы для предотвращения доминирования одного государства.

Согласно неореалистам, важнейшим фактором в международных отношениях является мощь государства, которая определяется его военными, экономическими и технологическими ресурсами. Поведение

---

[451] Telbami S. Kenneth Waltz, neorealism, and foreign policy //Security Studies. – 2002. – Т. 11. – №. 3. – С. 158-170.
[452] K Waltz. Theory of International Politics. Reading, 1979
[453] Конышев В. Н. Американский неореализм о проблеме суверенитета //Политическая экспертиза: ПОЛИТЭКС. – 2010. – Т. 6. – №. 4. – С. 68-88.
[454] Krasner S. D. Sovereignty: An institutional perspective //Comparative political studies. – 1988. – Т. 21. – №. 1. – С. 66-94.

государств и их взаимодействие объясняются структурными характеристиками международной системы, такими как распределение мощи среди государств (полярность системы). Это может быть многополярная, биполярная или однополярная система.

Эрозия суверенитета в 1990-е гг. – не более чем кратковременная флуктация[455]. С точки зрения Краснера, очень немногие государства обладают всеми атрибутами суверенитета: более слабые государства регулярно подвергаются нарушению своей внутренней власти со стороны более могущественных государств, а международное признание не соответствует четко установленным нормам[456].

Неореализм который стал продолжением классической версии политического реализма, унаследовал от него отношение к суверенитету как объективному и главному свойству государства. Сами реалисты мало изучают суверенитет в связи с теорией государства, так как их внимание сосредоточено на свойствах международной системы. Суверенитет предполагается как очевидное качество государств в качестве элементов международной системы[457]. При этом представители данного направления не склонны сомневаться в сохранении системообразующей роли государственного суверенитета в международной системе, при этом они не могут игнорировать новые трактовки и динамику процесса эволюции государственного суверенитета в условиях глобальной цифровой трансформации.

Хотя суверенитет является глобальной нормой, ни глобализация, ни международные институты не накладывают реальных ограничений на великие державы просто потому, что государства обладают достаточной властью, чтобы интерпретировать суверенитет так, как он отвечает их

---

[455] Конышев В. Н., Сергунин А. А. Теория международных отношений: канун новых «великих дебатов» //Полис. – 2013. – №. 2. – С. 66-78.

[456] Krasner S. D. Sovereignty: An institutional perspective //Comparative political studies. – 1988. – Т. 21. – №. 1. – С. 66-94.

[457] Конышев В. Н. Американский неореализм о проблеме суверенитета //Политическая экспертиза: ПОЛИТЭКС. – 2010. – Т. 6. – №. 4. – С. 69.

интересам. Власть – это обязательное условие международных отношений, используемое для защиты своего суверенитета (или для нарушения чужого суверенитета), но это не концепция, которую следует интерпретировать. Суверенитет обеспечивает жизненно важную защиту от эрозии государственных интересов[458].

Реализм предполагает, что великие державы высоко ценят компоненты суверенитета – свободу международных действий, включая ведение войны, исключительную власть над внутренними делами и признание в качестве законного международного игрока. Реалистический подход воспринимает суверенитет как данность точно так же, как национальные интересы. Суверенитет не зависит от конкретных социальных или культурных интерпретаций, а скорее является международно-признанной концепцией. На протяжении веков великие державы ревностно охраняли свой суверенитет в анархическом мире, полагаясь на военную мощь, чтобы гарантировать, что никакое другое государство не посягнет на их свободу действий на международном уровне или на их исключительное право управлять внутри страны так, как они считают нужным. Реализм признает, что государственный суверенитет может быть ограничен на международной арене, но эти ограничения накладываются уравновешивающим эффектом других крупных держав, а не глобальными институтами.

Поскольку основной задачей государства является обеспечение государственной безопасности, они стремятся к максимальной свободе действий и поэтому избегают участия в международных структурах, предполагающих ограничение суверенитета. Согласно реалистской трактовке, цифровой суверенитет – это право государства управлять своей национальным сегментом цифровой сети для защиты национальных

[458] Цветкова Н. А. Феномен цифровой дипломатии в международных отношениях и методология его изучения //Вестник РГГУ. Серия: Политология. История. Международные отношения. – 2020. – №. 2. – С. 37-47.

интересов, наиболее важными из которых являются информационная безопасность и цифровая экономика.

Интернет и его базовая архитектура по своей сути являются глобальными, что создает вызовы для системы суверенитета и контроля границ[459]. Сложная сеть коммерческих связей и технических зависимостей лежит в основе того, что мы называем киберпространством. Именно поэтому, цифровой суверенитет в практике современных международных отношений – еще один пример «организованного лицемерия», в терминах С. Краснера, так как полнотой суверенитета обладают лишь сильные государства, слабые же находятся в зависимом и подчиненном положении.

Согласно реалистским оценкам, сфера технологий стала одной из ключевых в борьбе за власть в XXI веке. К началу третьего десятилетия очевидно оформление двух основных «технологических экосистем» – американской и китайской. Американская система старейшая, наиболее развитая и опирается на безусловное технологическое лидерство США. Китайская техноэкономическая платформа скромнее американской. КНР первые в мире поэкспериментировали с автономизацией ряда сервисов и услуг, выстроив «Великую Китайскую цифровую стену». Кроме КНР и США, к числу лидеров в области цифровых технологий относят Россию, цифровым суверенитетом на уровне интеграционной структуры (чаще используется термин «стратегическая автономия» обладает также ЕС).

2.3.4. Конструктивизм о природе цифрового суверенитета

Конструктивизм внес значительный вклад в теорию международных отношений, предложив новый способ понимания динамики международной политики. Конструктивисты утверждают, что многие аспекты международной политики являются социально

[459] Зиновьева Е. С. Формирование цифровых границ и информационная глобализация: анализ с позиций критической географии //Полис. Политические исследования. – 2022. – №. 2. – С. 8-21.

сконструированными, а не объективно данными, к их числу относится и категория государственного суверенитета.

Реальность международных отношений формируется через взаимодействия и дискурсы между различными акторами, являясь, таким образом интерсубъективной.

Идеи и нормы играют ключевую роль в определении поведения международных акторов. Они помогают формировать восприятие акторов, их идентичности и интересы. Нормы определяют, что считается допустимым и недопустимым поведением в международной системе. Конструктивизм рассматривает взаимодействие между агентами (государствами, индивидами) и структурами (нормами, институтами). Они взаимно конституируют друг друга: агенты формируют структуры, а структуры формируют агентов.

Конструктивизм расширил спектр объектов анализа в международных отношениях, включая идеи, идентичности, нормы, дискурсы и культурные практики. Это позволило анализировать феномены, которые трудно объяснить в рамках реализма и либерализма, такие как изменение норм, распространение идей и культурные взаимодействия. Примеры включают изменения в нормах, касающихся суверенитета государств в условиях современной цифровой революции.

Конструктивисты изучают, как понятие безопасности и суверенитета меняется в зависимости от контекста и социальных взаимодействий. Это включает исследования по «секьюритизации» – процессу, через который вопросы переводятся в область безопасности. Примеры включают секьюритизацию киберугроз, данный подход весьма популярен в российской академической литературе[460].

Один из ведущих теоретиков конструктивизма, известный своей работой «Социальная теория международной политики». Вендт

[460] Зиновьева Е.С. Международная информационная безопасность: проблемы, субъекты, перспективы. Дисс. … доктора полит. Наук. М.: МГИМО, 2019.

утверждает, что «анархия – это то, что делают из нее государства», подчеркивая социальную природу международной системы[461].

Марта Финнемор известна своими исследованиями международных норм и роли международных организаций. Она исследует, как международные нормы формируются и распространяются, и как они влияют на государственное поведение[462]. Она также исследовала нормативные основы режима кибер-безопасности, совместно с юристом-международником Д. Холлисом[463].

Конструктивистский подход объединяет три основных уровня анализа в международной политике – структурный уровень, уровень подразделений и когнитивный уровень. На структурном уровне международная система переживает фундаментальную трансформацию концепции и практики государственного суверенитета, которую невозможно адекватно вписать в реалистическую парадигму. Ограничения и стимулы системного уровня постоянно меняются, что приводит к появлению новых условий для легитимного осуществления власти. На уровне единиц отдельные государства делятся на те, которые защищают постмодернистские формы суверенитета, основанные на гуманитарной интервенции, превосходящей суверенные права государств, и другие, которые энергично защищают традиционные вестфальские представления об абсолютном суверенитете. Наконец, на уровне элиты внутри одного государства могут иметь разные взгляды на суверенитет и могут стремиться переформулировать вопросы суверенитета ради политической выгоды[464].

---

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

[462] Finnemore M. Norms, culture, and world politics: insights from sociology's institutionalism //International organization. – 1996. – Т. 50. – №. 2. – С. 325-347.

[463] Finnemore M, Hollis DB. Constructing Norms for Global Cybersecurity. American Journal of International Law. 2016;110(3):425-479. doi:10.1017/S0002930000016894

[464] Litvinenko A. Re-Defining Borders Online: Russia’s Strategic Narrative on Internet Sovereignty //Media and Communication. – 2021. – Т. 9. – С. 5-15.

Питер Катценштейн исследует влияние культурных факторов и национальных идентичностей на международные отношения, особенно в контексте безопасности и политической экономии. Согласно данному подходу, Подход России к суверенитету отражает тесную связь между проектом рецентрализации внутри страны и укреплением позиции России как великой державы на международной арене[465]. Конструктивистский подход оказывается полезным при рассмотрении суверенитета – он направляет наше внимание на проблему развития новой постсоветской идентичности, но роль культуры и исторической интерпретации во внешней политике, российские концепции Запада как значимого и враждебного Другого – все это критически важные факторы в понимании российского внешнеполитического поведения. Основная идеологическая конструкция посткоммунистического периода – суверенная демократия – утверждает, что и суверенитет, и демократия социально и культурно детерминированы и, следовательно, противоречат западным интерпретациям этих концепций. Появление нового, постмодернистского набора глобальных норм, ограничивающих суверенитет (в том числе концепцию «ответственность по защите» и «суверенитет личности») Россия трактует как инструменты культурного и дискурсивного доминирования Запада, что также связано с сохраняющейся напряженностью между Россией и Западом[466].

Конструктивизм внес значительный вклад в теорию международных отношений, предложив новый способ анализа и понимания международной политики, который учитывает важность идей, норм, идентичностей и социальных взаимодействий. Этот подход предложил новые объяснения многих явлений в международных отношениях. Большинство аналитических течений в рамках общего подхода

[465] Litvinenko A. Re-Defining Borders Online: Russia’s Strategic Narrative on Internet Sovereignty //Media and Communication. – 2021. – Т. 9. – С. 5-15.
[466] Там же.

политического конструктивизма признают государства в качестве центральной единицы анализа, но утверждают, что суверенитет является социально сконструированным и, следовательно, изменчивым и дискурсивно обусловленным[467].

С конструктивистской точки зрения суверенитет можно понимать как ключевую статью конституций международного общества, определяющую государственную власть. Таким образом, вопрос заключается в том, соблюдаются ли такие международные нормы как обязательные правила, соблюдение которых обеспечивается каким-либо наднациональным органом, или просто как удобные соглашения, которые государства соблюдают до тех пор, пока они не ограничивают национальные интересы. Действительно, реалистический аргумент Краснера заключается в том, что суверенитет – это не набор обязательных норм, а удобный принцип действия, который на практике часто нарушается могущественными государствами[468]. Несмотря на то, что суверенитет по-прежнему очень важен и высоко ценится государствами, он зависит от национальной власти и интересов государств, и их поведение, как правило, определяется скорее этими интересами, чем международными нормами.

Как отмечает Эмануэль Адлер: «Навязывание смыслов материальному миру – это одна из высших форм власти…»[469] . Суверенитет и национальные интересы не являются данностью, а, скорее, вытекают из социального контекста – они представляют собой сконструированные концепции, которые получают свое истинное воплощение в правилах и нормах: нормы составляют социальную идентичность и придают национальным интересам их содержание и значение[470]. Территория, население, власть и признание являются

[467] Biersteker T. J., Weber C. (ed.). State sovereignty as social construct. – Cambridge University Press, 1996.
[468] Krasner S. D. Recognition: organized hypocrisy once again //International Theory. – 2013. – Т. 5. – №. 1. – С. 170-176.
[469] Adler E. Seizing the middle ground: Constructivism in world politics //European journal of international relations. – 1997. – Т. 3. – №. 3. – С. 319-363.
[470] Там же.

важными аспектами государственного суверенитета, и каждый из этих компонентов социально сконструирован на основе нормативной концепции, которая связывает эти элементы уникальным образом и в определенном месте – государстве[471].

2.3.5. Постпозитивизм и неоколониализм о природе цифрового суверенитета

Постпозитивизм в теории международных отношений включает множество школ и исследовательских направлений, которые объединяет критика методологического и эпистемологического подхода господствующих теорий. Постпозитивисты подчеркивают важность критического анализа, интерпретации и понимания социальных и политических явлений, в том числе природы суверенитета. С позиций постпозитивизма реальность международных отношений воспринимается как конструируемая через язык, дискурсы и социальные практики[472]. Значения и значения политических явлений, таких как глобальная цифровая трансформация, Четвертая промышленная революция и государственный суверенитет также формируются через дискурсы, которые отражают характер властных отношений в обществе.

Постпозитивисты утверждают, что исследование международных отношений всегда обусловлено ценностями и интересами. Невозможно полностью отделить факты от интерпретации, и любое знание является социально и исторически детермированным. В этом контексте весьма показательна популярная постколониальная теория международных отношений[473]. В частности, исследователи В. Конг из Университета

---

[471] Biersteker T. J., Weber C. (ed.). State sovereignty as social construct. – Cambridge University Press, 1996. – Т. 46.
[472] Wullweber J. Post-positivist political theory //The Encyclopedia of Political Thought. Chichester: Wiley. – 2015. – С. 2932-2942.
[473] Kapoor I. Capitalism, culture, agency: dependency versus postcolonial theory //Third World Quarterly. – 2002. – Т. 23. – №. 4. – С. 647-664.

Гонконга и Д. Тхумфарт из Свободного Университета Брюсселя прослеживают неоколониальный дискурс в академических публикациях авторов КНР, с 1994 по 2005 годы, в которых используются такие понятия, как «сетевой/кибер-суверенитет» и «информационный суверенитет»[474]. Реконструируя геополитическую, экономическую, культурную, идеологическую, и нормативную составляющую контекста рассматриваемых публикаций, авторы выделяют академический дискурс КНР как часть социотехнической конструкции цифрового суверенитета, который включает в себя критику киберколониализма Запада и при этом принятие неизбежности цифровизации и ее возможностей[475].

Постколониальная теория анализирует наследие колониализма и его влияние на современные международные отношения. Она акцентирует внимание на неравенствах, возникших в результате колониальной истории. В частности, отмечается, что базовые концепции теории, такие как суверенитет, неприложимы к объяснению политики стран третьего мира. Нормативные основы безопасности и суверенитета на практике не экстраполируются напрямую из западного опыта, а всякий раз адаптируются к локальным условиям, порождая многообразие вариантов развития. Многообразие делает невозможным полный универсализм в понимании природы безопасности и суверенитета[476]. Таким образом, и практика цифрового суверенитета в России, Индии, Китае и его дискурсивное осмысление будет отличаться от западных концепций и западного опыта.

Разные взгляды на цифровой суверенитет проявляются в разных нарративах. Цифровой суверенитет формируется такими нарративами. Это

---

[474] Cong W., Thumfart J. A Chinese Precursor to the Digital Sovereignty Debate: Digital anti-Colonialism and Authoritarianism from the post–Cold war era to the Tunis Agenda //Global Studies Quarterly. – 2022. – Т. 2. – №. 4. – С. ksac059.

[475] Cong W., Thumfart J. A Chinese Precursor to the Digital Sovereignty Debate: Digital anti-Colonialism and Authoritarianism from the post–Cold war era to the Tunis Agenda //Global Studies Quarterly. – 2022. – Т. 2. – №. 4. – С. ksac059.

[476] Конышев В. Н. Незападный взгляд на мировую политику //Мировая экономика и международные отношения. – 2020. – Т. 64. – №. 3. – С. 130-135.

позволяет идентифицировать, сравнивать и противопоставлять различные репрезентации цифрового суверенитета в дискурсе. В дискурсе различных стран вопросы развития, безопасности, защиты данных соотнесены с историческим опытом, политической культурой, уровнем экономического развития. Поэтом сходные нарративы получают различное политическое и юридическое оформление. С точки зрения нарративного анализа, именно расплывчатость и двусмысленность цифрового суверенитета способствует межтекстовым и межнарративным связям, позволяя различным нарративам цифрового суверенитета резонировать сильнее и с более широкой аудиторией, чем в противном случае.

Авторы из Германии выделяют следующие составляющие нарративов о цифровом суверенитете ЕС:

1) Цифровой суверенитет как необходимое условие экономического процветания – защита цифровых рынков является необходимым условием экономического процветания и глобальной конкурентоспособности – как правило этот дискурс подчеркивает значительный социо-экономический потенциал цифровых технологий, выделяет несколько критических цифровых технологий, необходимых для экономического роста, с неоколониальных позиций данный дискурс предостерегает от чрезмерной зависимости от внешних поставщиков цифровых технологий, услуг и решений, которые монополизировали глобальные рынки, главной угрозой видится потеря цифровых рынков и переход их в руки внешних, влиятельных игроков. Как правило подобный нарратив призывает к партнерству крупного бизнеса и государства;

2) Цифровой суверенитет как условие информационной безопасности - призван защитить государство и общество от широкого спектра внутренних и внешних угроз безопасности в киберпространстве. Цифровизация трактуется как источник угроз, конфликтов и нестабильности и фактор уязвимости современных обществ.

3) Цифровой суверенитет как выбор собственного пути – данный нарратив ориентирован на защиту ценностей, идей, образа жизни государства, которые подвергаются размыванию в условиях цифрового общества. Этот нарратив переосмысливает нарративы экономического процветания и безопасности через призму ценностей и норм национальной идентичности каждого государства.

4) Цифровой суверенитет как необходимый атрибут современного государства - цифровым суверенитетом понимается способность государственных органов принимать независимые решения о поставщиках и использовании ИТ-технологий, в частности программного обеспечения, в государственном управлении. Это рассматривается как часть более широких усилий по модернизации государственного управления и формирования «умного государства».

5) Цифровой суверенитет как условие защиты данных - идеи о защите данных, защите потребителей и защите персональных данных тесно связаны с категорией государственного суверенитета.

Исследователи отмечают, что гибкость интерпретации этой концепции делают ее привлекательным центром внимания для политических проектов участников из самых разных политических областей и политических лагерей[477].

Критическая теория, в частности Франкфуртская школа[478], критикует капитализм, империализм и другие формы неравенства. Постпозитивизм расширил аналитические рамки международных отношений, включив в них культурные, социальные и дискурсивные аспекты. Это позволило более глубоко понять сложные и многослойные феномены международной политики. Постпозитивистские теории способствовали включению маргинализированных голосов и перспектив в

[477] Lambach D., Oppermann K. Narratives of digital sovereignty in German political discourse //Governance. – 2023. – Т. 36. – №. 3. – С. 693-709.
[478] Wiggershaus R. The Frankfurt School: Its history, theories, and political significance. – mit Press, 1994.

анализ международных отношений. Это позволило учесть опыт и взгляды тех, кто традиционно был исключен из мейнстримных теорий, в том числе представителей «мирового большинства» и «глобального юга», рассмотреть их оценки процессов цифровизации и ее влияния на практику суверенитета. Говоря о потенциале постпозитивизма применительно к исследованию цифрового суверенитета, необходимо выделить несколько доминирующих и взаимопересекающихся нарративов цифрового суверенитета, в том числе изучить различия в интерпретациях цифрового суверенитета стран Запада и Востока. Также необходимо отметить, что постколониализм позволяет применить концепцию множественности модерна к изучению практики цифрового суверенитета[479].

Вывод по параграфу:

Концептуализация цифрового суверенитета в современной науке о международных отношениях отражает стремление соединить традиционные теории с новыми вызовами эпохи цифровой трансформации. Эта категория становится ключевым понятием в дискуссиях о том, как государства адаптируют свои суверенные функции к условиям глобальной взаимозависимости и технологической взаимосвязанности. В то время как реалистический подход акцентирует внимание на укреплении контроля над национальными цифровыми ресурсами, либеральные теории подчеркивают необходимость создания транснациональных институтов, способных обеспечить баланс между национальными интересами и глобальными нормами.

Важной частью концептуализации становится признание цифрового суверенитета как многоуровневого феномена, который включает в себя правовые, технологические и политические аспекты. В центре внимания оказываются такие темы, как кибербезопасность, контроль над потоками

[479] Об идее множественности модерна см. напр.: Кобылин И. И. « Провинциализация» революции: цивилизационный подход на постколониальном повороте //Неприкосновенный запас. Дебаты о политике и культуре. – 2017. – №. 5. – С. 97-111.

данных, регулирование платформенных корпораций и развитие цифровой инфраструктуры. Конструктивистский подход выделяет роль идентичностей и дискурсов в формировании национальных стратегий, подчеркивая, что цифровой суверенитет не только защищает национальные интересы, но и становится частью коллективного представления о государственности в условиях цифровой эпохи.

Современные теоретические модели цифрового суверенитета также сталкиваются с вызовами глобализации, которая размывает границы между внутренней и внешней политикой. Постпозитивистские исследования критикуют концепцию суверенитета, утверждая, что в условиях доминирования транснациональных корпораций и сетевых структур государства теряют способность контролировать свои цифровые пространства. Однако, несмотря на эту критику, цифровой суверенитет продолжает оставаться актуальной категорией, адаптируясь к новым реалиям и предлагая государствам гибкие инструменты для защиты своих интересов.

Таким образом, цифровой суверенитет в международных отношениях – это не статичная, а динамическая концепция, которая одновременно укрепляет национальные границы и подчеркивает неизбежность глобального взаимодействия. Его концептуализация требует синтеза теоретических подходов, способных отразить сложность современных вызовов и предложить пути их эффективного преодоления.

Вывод по главе:

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.

Развитие цифровых технологий 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.

Современная цифровая революция радикально трансформирует международные отношения, привнося новые вызовы и возможности для глобального управления. Концептуализация этих процессов демонстрирует, 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

3.1. Цифровой суверенитет в практике международных организаций

3.1.1. Цифровой суверенитет в повестке ООН

ООН, будучи организацией со всеобщим членством и неоспоримой легитимностью является ключевым международным институтом, занимающимся созданием норм и стандартов, которые будут способствовать справедливому и безопасному развитию цифрового пространства в интересах всех стран международного сообщества.

Важный вклад в становление дискуссии о цифровом суверенитете в ООН внесли предложенные по инициативе России резолюции «Достижения в сфере телекоммуникаций и информатизации в контексте международной безопасности», впервые представленные в рамках 1 комитета ГА ООН в 1998 году[480] и с тех пор принимающиеся ежегодно.

Впервые проблематика цифрового суверенитета на площадке ООН нашла отражение в итоговых документах Всемирного форума по вопросам информационного общества, который прошел в два этапа в Женеве и в Тунисе в 2003 и 2005 гг. Всего по итогам ВВУИО было принято четыре документа Женевская и Тунисская Программы действий и Женевские и Тунисские Обязательства в рамках каждого из этапов, соответственно за 2003 и 2005 гг.[481] В документах подчеркивается необходимость

[480] Резолюция ГА ООН A/53/70 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 4 декабря 1998 г.

[481] Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-03/GENEVA/DOC/4-R. Декларация принципов. - 12 декабря 2003 года; Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-03/GENEVA/DOC/5-R. План действий. – 12 декабря 2003 года; Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-05/TUNIS/DOC/6(Rev.1)-R. Тунисская программа для информационного

обеспечения государствами суверенного права на управление своим сегментом интернета, включая разработку национальных политик в области кибербезопасности, защиты данных и цифровой экономики. Согласно итоговым документам ВВУИО, управление интернетом должно быть основано на многоуровневом подходе, с участием государств, частного сектора, гражданского общества и международных организаций[482]. Акцентируется внимание на важности защиты персональных данных и конфиденциальности пользователей, что является неотъемлемой частью цифрового суверенитета. Также рассматривается баланс между суверенитетом государств и правами пользователей на доступ к информации и свободу выражения в интернете. Страны призваны защищать цифровые права граждан, уважая при этом национальные и международные нормы[483].

В развитие ВВУИО был создан Форум по вопросам управления Интернетом, который проходит ежегодно с 2006 года, а также имеет целый ряд региональных подразделений, в числе которых РИГФ – Российский Форум по вопросам управления Интернетом. Динамика переговорного процесса в рамках ФУИ и РИГФ показывают постепенный переход от многоуровневой к многосторонней системе управления Интернетом, которая характеризуется приоритетной ролью государств в принятии

общества. – 18 ноября 2005 года; Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-05/TUNIS/DOC/7-R. Тунисское обязательство. – 18 ноября 2005 года.

[482] Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-03/GENEVA/DOC/4-R. Декларация принципов. - 12 декабря 2003 года; Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-03/GENEVA/DOC/5-R. План действий. – 12 декабря 2003 года; Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-05/TUNIS/DOC/6(Rev.1)-R. Тунисская программа для информационного общества. – 18 ноября 2005 года; Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-05/TUNIS/DOC/7-R. Тунисское обязательство. – 18 ноября 2005 года.

[483] Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-03/GENEVA/DOC/4-R. Декларация принципов. - 12 декабря 2003 года; Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-03/GENEVA/DOC/5-R. План действий. – 12 декабря 2003 года; Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-05/TUNIS/DOC/6(Rev.1)-R. Тунисская программа для информационного общества. – 18 ноября 2005 года; Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-05/TUNIS/DOC/7-R. Тунисское обязательство. – 18 ноября 2005 года.

решений и переговорном процессе, что знаменует рост влияния принципа суверенитета в переговорном процессе в сфере управления интернетом.

Проблематика управления интернетом сохраняет важную роль на повестке ФУИ, ВВУИО и ООН в целом. Так, в 2019 году Генеральный Секретарь ООН А. Гуттериш объявил о созыве Саммита будущего в сентябре в 2024 году и представил документ Повестка дня для будущего в 2019 году. Глобальный цифровой договор ООН направлен на создание единого глобального соглашения, которое регулирует вопросы цифровой экономики, кибербезопасности, защиты данных и прав человека в интернете. Глобальный цифровой договор ставит своей задачей установить нормы и правила для управления цифровыми платформами, в том числе связанные с регулированием крупных технологических компаний, борьбой с дезинформацией и защитой прав пользователей. Договор предусматривает меры для повышения безопасности цифровой инфраструктуры, защиты данных и предотвращения кибератак. Важной частью договора является защита прав человека в цифровом пространстве, включая право на частную жизнь, свободу выражения мнений и доступ к информации. Договор также затрагивает вопросы наращивания потенциала развивающихся стран и преодоления цифрового разрыва в целях обеспечения равного доступа к цифровым технологиям для всех стран. Это включает в себя поддержку развивающихся стран в наращивании их цифровой инфраструктуры и навыков. Глобальный цифровой договор подчеркивает важность международного сотрудничества и координации в области цифровых технологий[484]. Однако данный документ не уделяет достаточного внимания вопросам цифрового суверенитета. В частности, регулирование платформ предлагается осуществлять путем реализации соглашений с пользователями, а не путем их «приземления» и определения правил на уровне государств. Таким

[484] Резолюция принятая ГА ООН A/Res/79/1. «Пакт во имя будущего» от 22 сентября 2024. URL: https://documents.un.org/doc/undoc/gen/n24/272/24/pdf/n2427224.pdf

образом, ГЦД и ряд других инициатив в области глобального цифрового управления, провозглашающие универсальные нормы, зачастую игнорируют фундаментальный для современной мирополитической архитектуры принцип государственного суверенитета, что находит свое прямое отражение в позиции Российской Федерации. Россия последовательно отстаивает модель управляемого и безопасного цифрового пространства, в которой верховная власть государства в определении правил, норм и юрисдикции в пределах своих национальных границ является неоспоримой. Российский подход, акцентирующий необходимость «приземления» цифровых платформ и защиты критической информационной инфраструктуры в рамках национального правового поля, представляет суверенную реакцию на вызовы цифровой трансформации, направленную на обеспечение международной информационной безопасности, культурно-цивилизационной идентичности и стратегической стабильности в условиях нарастающей конкуренции цифровых моделей мирового развития.

Важную роль на повестке ООН играет вопрос обеспечения международной информационной безопасности. Именно секьюритизация цифрового пространства стала важнейшим фактором укрепления цифровых границ и развития политики цифрового суверенитета. С 1998 года Российская Федерация инициативно продвигает обсуждение данной проблематики на уровне ООН, в частности, с 1998 года ежегодно принимаются резолюции «Достижения в области информационных и телекоммуникационных технологий в контексте международной безопасности»[485]. В 2018 году данная резолюция была дополнена сводом из 13 необязательных норм ответственного поведения государств в ИКТ

[485] Резолюция ГА ООН A/53/70 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 4 декабря 1998 г.

среде, в том числе основанных на принципе уважения государственного суверенитета[486].

С начала запуска переговорного процесса в ООН было созвано 6 Групп правительственных экспертом по международной информационной безопасности, из которых 4 приняли итоговые доклады, в которых, среди прочего отмечалась важность защиты государственного суверенитета в ИКТ среде[487]. Итоговые доклады являются важными документами, отражающими достигнутый международный консенсус по ключевым вопросам международной информационной безопасности и цифрового суверенитета. Одним из центральных вопросов всех докладов было признание того, что международное право, включая Устав ООН, применимо к действиям государств в киберпространстве. В силу того, что одним из центральных принципов Устава ООН является суверенное равенство государств, данные доклады внесли важнейший вклад в прикладную концептуализацию категории государственного суверенитета в цифровом пространстве.

Россия выступает за формирование универсального режима информационной безопасности. В частности, Россией было предложен проект Концепции международной информационной безопасности[488]. Конвенция настаивает на недопустимости включения недекларируемых возможностей в ИКТ-продукты, а также на обязательности раскрытия информации об уязвимостях в продуктах, производимых другими странами. Это необходимо для обеспечения прозрачности и защиты государств от возможных угроз их цифровому суверенитету. Документ подчеркивает недопустимость монополизации ИКТ-рынков отдельными государствами или компаниями, которые могут ограничивать доступ

---

[486] 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.

[487] Международная информационная безопасность: подходы России / Под ред. Е.С. Зиновьевой, А.В. Крутских. М.: МГИМО, 2023

[488] Концепция Конвенции международной информационной безопасности ООН. Совет Безопасности Российской Федерации. 2023.

других стран к передовым технологиям. Это ведет к усилению технологической зависимости и цифрового неравенства, что угрожает суверенитету государств, особенно в контексте их способности обеспечивать независимый контроль и безопасность своих информационных ресурсов[489].

Согласно официальной позиции России, использование ИКТ не должно нарушать основные права и свободы человека, такие как право на частную жизнь и свободу выражения мнений. Государства обязаны защищать эти права в своем национальном информационном пространстве и уважать их на международном уровне, соблюдая принципы международного права. Конвенция предполагает, что суверенные права государств в цифровом пространстве должны сочетаться с международным сотрудничеством в целях противодействия угрозам и вызовам международной информационной безопасности. Конвенция настаивает на недопустимости включения недекларируемых возможностей («закладок») в ИКТ-продукты, а также на обязательности раскрытия информации об уязвимостях в продуктах, производимых другими странами. Государства должны работать вместе над предотвращением кибератак, обмениваться опытом и информацией, а также участвовать в разработке стандартов и норм, которые укрепляют цифровой суверенитет и безопасность на глобальном уровне. Таким образом, цифровой суверенитет в рамках предложенного Россией проекта Конвенции ООН по ИКТ-безопасности охватывает широкий спектр мер, направленных на защиту национальных интересов государств, предотвращение вмешательства в их внутренние дела и развитие безопасного и стабильного международного информационного пространства[490].

---

[489] Там же.
[490] Там же.

Еще одним важным направлением международного сотрудничества в области информационной безопасности на повестке ООН, инициированным Россией, является противодействие преступному использованию ИКТ. С 2019 года в рамках 3 Комитета Генеральной Ассамблеи ООН (занимающегося пунктами повестки дня, которые касаются социальных и гуманитарных вопросов и вопросов прав человека)[491]. После долгого обсуждения проект резолюции был принят в 2024 году, что является важным дипломатическим успехом России. В отличие от Будапештской конвенции 2001 года, принятой в рамках Совета Европы, которая исходит из экстратерриториальной концепции государственного суверенитета[492], наиболее выгодной странам, желающим распространить свои правовые рамки на глобальном уровне, предложенный Россией проект предполагает уважение государственного суверенитета и реализацию принципа «либо выдавай, либо суди». Статья 3 Конвенции специально посвящена проблематике защиты суверенитета в цифровом пространстве: «1. Государства-участники осуществляют свои обязательства согласно настоящей Конвенции в соответствии с принципами государственного суверенитета, суверенного равенства государств и невмешательства во внутренние дела других государств; 2. Настоящая Конвенция не наделяет компетентные органы Государство-участника правом осуществлять на территории другого Государства-участника юрисдикцию и функции, которые относятся к исключительной компетенции органов этого другого государства, если иное не предусмотрено в настоящей Конвенции в соответствии с его внутренним законодательством»[493].

---

[491] Проект Конвенции ООН о сотрудничестве в сфере противодействия информационной преступности от 11 октября 2017 г. URL: http://www.mid.ru/foreign_policy/international_safety/regprla/-/asset_publisher/YCxLFJnKuD1W/content/id/3025418

[492] Convention on Cybercrime Budapest, 23.XI.2001 European Treaty Series - No. 185 URL: https://rm.coe.int/1680081561

[493] Проект Конвенции ООН о сотрудничестве в сфере противодействия информационной преступности от 11 октября 2017 г. URL: http://www.mid.ru/foreign_policy/international_safety/regprla/-/asset_publisher/YCxLFJnKuD1W/content/id/3025418

Вообще, проблематика применимости международного права к ИКТ среде, в том числе в контексте уважения государственного суверенитета и поддержки мирного развития глобальной цифровой сферы, является одной из важнейших на повестке ООН. По результатам работы Группы правительственных экспертов последнего созыва 2021 был принят итоговый доклад, который отмечает, что Устав ООН и основные нормы и принципы международного права применимы к ИКТ среде[494].

Важной составляющей современной работы ООН является регулирование технологий искусственного интеллекта. Причем, данная проблематика в повестке организации включает в себя широкий круг проблем, в том числе выработку этических принципов регулирования технологий искусственного интеллекта, запрет и выработка регуляторики в отношении САС (смертоносных автономных систем вооружений). В числе основных документов в данной области следует отметить «Руководящие принципы автономных систем летального оружия», принятые в рамках Конвенции о конкретных видах обычного оружия[495], или «Рекомендации по этике искусственного интеллекта», принятые ЮНЕСКО в 2021 году[496].

Генсек ООН в 2023 году принял решение о создании нового органа Организации Объединенных Наций для поддержки коллективных усилий по управлению ИИ - Консультативный совет высокого уровня по искусственному интеллекту с участием многих заинтересованных сторон, который к концу 2023 года представит доклад о вариантах глобального управления ИИ[497]. При этом видится что регулировании ИИ будет призвано дополнить уже поставленные задачи не только обеспечения его

---

[494] A/76/135 Group of `governmental Experts on Advancing Responsible States Behaviour in Cyberspace in the Context of International Security. 2021. URL: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf

[495] Конвенция о конкретных видах обычного оружия. ООН. 1983. URL: https://www.un.org/ru/documents/decl_conv/conventions/pdf/conweapons.pdf

[496] Recommendation on the Ethics of Artificial Intelligence UNESCO SHS/BIO/PI/2021/1 URL: https://unesdoc.unesco.org/ark:/48223/pf0000381137

[497] В ООН представили план по управлению искусственным интеллектом 19.09.2024 URL: https://news.un.org/ru/story/2024/09/1456466

безопасного использования, но и достижения ЦУР. Цифровые технологии уже активно используются в деятельности организаций семьи ООН, в частности, МСЭ для достижения ЦУР и ИИ призван дополнить цифровые инициативы МСЭ.

На уровне политики ООН опирается на такие инициативы, как Доклад Генерального секретаря «Наше общее цифровое будущее»[498] и работу специализированных агентств, включая ЮНЕСКО и Международный союз электросвязи (МСЭ). ЮНЕСКО, например, разработала первую в мире глобальную этическую рекомендацию по ИИ, которая акцентирует внимание на принципах транспарентности, подотчётности и недопущения дискриминации. Эти нормы создают основу для гармонизации подходов стран к разработке и применению ИИ.

Однако проблематика цифрового суверенитета становится серьёзным вызовом для реализации таких инициатив. Многие государства опасаются, что универсальные подходы могут ограничить их способность самостоятельно регулировать использование ИИ в соответствии с национальными интересами. Развитые страны, обладающие технологическим лидерством, часто защищают модели открытого и глобального регулирования, которые сохраняют их конкурентные преимущества. В то же время развивающиеся государства настаивают на праве на цифровой суверенитет, подразумевающем возможность локализации данных, регулирования трансграничного обмена информацией и создания собственных технологических экосистем.

Противоречия между принципом глобальной координации и национальными интересами приводят к сложностям в достижении консенсуса. Например, дискуссии в рамках ООН затрагивают такие вопросы, как необходимость предотвращения милитаризации ИИ и защита

[498] Доклад Генерального Секретаря ООН «Дорожная карта по цифровому сотрудничеству: осуществление рекомендаций Группы высокого уровня по цифровому сотрудничеству». Резолюция Генеральной Ассамблеи ООН A/74/821 от 29 мая 2020 г.

прав человека в условиях автоматизации. В то же время каждая страна по-своему интерпретирует, что именно представляет угрозу её цифровому суверенитету, будь то утечка данных, контроль над критической инфраструктурой или зависимость от иностранных технологий.

Ключевой вызов для ООН заключается в создании баланса между универсальными нормами и национальной автономией. Организация стремится предложить рамочные соглашения, которые позволят государствам адаптировать регулирование к своим нуждам, сохраняя при этом приверженность основным этическим стандартам. Этот компромисс становится основой для долгосрочной цели – обеспечить, чтобы ИИ развивался в интересах всего человечества, а не отдельных технологических гигантов или государств.

На последние несколько лет пришлось усиление внимания к вопросам цифрового суверенитета в официальных документах международных организаций, прежде всего ООН. В частности, согласно докладу Рабочей группы ООН открытого состава по международной информационной безопасности 2021 года (далее - РГОС)[499], созданной по инициативе России, «использование ИКТ, противоречащее нормам международного публичного права… создает угрозу… суверенитету государств». Особый акцент сделан на нужды развивающихся стран, отмечено, что «помощь в укреплении потенциала должна быть реализована при уважении принципа государственного суверенитета». ГПЭ ООН по международной информационной безопасности, созданная по инициативе США, опубликовала итоговый доклад, в котором подтверждается, что «суверенитет и международные нормы и принципы, вытекающие из него, применимы к нормам ответственного поведения

[499] Доклад Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (A/AC.290/2021/CRP.2 от 10 марта 2021 г.) (на английском) // Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substanive Report (A/AC.290/2021/CRP.2 10 March 2021)

государств в ИКТ-среде, и государственная юрисдикция распространяется на ИКТ-инфраструктуру, находящуюся на территории государства», а также «уважение государственного суверенитета, основных прав и свобод человека, и устойчивое цифровое развитие» лежат в основе усилий ООН в области регулирования цифровых технологий[500].

Организация Объединенных Наций и её специализированные учреждения (такие как МСЭ, ЮНЕСКО, UNCTAD) играют центральную, но внутренне противоречивую роль в попытке легитимизировать и нормативно закрепить концепцию цифрового суверенитета в качестве новой нормы международных отношений. С одной стороны, ООН выступает единственной универсальной площадкой для выработки консенсусных подходов, где суверенное равенство государств-членов является фундаментальным принципом. Именно в рамках ООН инициируются ключевые процессы, такие как Рабочая группа по открытому составу (РГОС) по вопросам безопасности в сфере использования ИКТ и идущие параллельно переговоры по Конвенции о противодействии киберпреступности, которые de facto являются ареной для борьбы за содержание цифрового суверенитета. Через призму функциональных организаций, ООН продвигает его отдельные аспекты: МСЭ помогает странам наращивать технологический потенциал, ЮНЕСКО отстаивает суверенитет в сфере культурного разнообразия и цифрового образования, а ЮНКТАД анализирует и концептуализирует данные как стратегический экономический актив.

Однако политика ООН в области глобального нормотворчества в цифровом пространстве наталкиваются на системные ограничения, проистекающие из глубокого раскола между политическими позициями основных групп государств. Переговоры в ООН часто заходят в тупик, что

[500] A/76/135 Group of `governmental Experts on Advancing Responsible States Behaviour in Cyberspace in the Context of International Security. 2021. URL: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf

приводит к принятию расплывчатых резолюций, где консенсус достигается ценой самых общих формулировок, а любые попытки создать юридически обязывающие документы блокируются. Как следствие, центр тяжести практического сотрудничества и реального нормотворчества закономерно смещается на региональный и макрорегиональный уровень, где достижение договоренностей политически и ценностно более осуществимо.

3.1.2. Цифровой суверенитет в повестке БРИКС

БРИКС, представляющий собой международное объединение ведущих стран Глобального Юга, играет все более значимую роль в развитии цифровых технологий и защите цифрового суверенитета. В рамках БРИКС цифровой суверенитет можно определить как стремление государств-участников к независимости и контролю над национальными цифровыми инфраструктурами, данными и интернет-ресурсами. Это понятие отражает не только растущую значимость данных в глобальной экономике, но и связанные с ними вызовы безопасности.

Страны БРИКС – Бразилия, Россия, Индия, Китай и Южная Африка – представляют 42% населения мира, что составляет 3,2 млрд человек, и обладают колоссальным объемом персональных данных[501]. Цифровые услуги, предоставляемые транснациональными корпорациями, в действительности оплачиваются ценнейшим ресурсом – данными, что ставит под угрозу национальный суверенитет стран[502]. Исследование проекта CyberBRICS демонстрирует, что страны-участницы разрабатывают нормативно-правовые и кибербезопасностные стратегии

[501] www.internetworldstats.com
[502] Min Jiang & Luca Belli. Contesting Digital Sovereignty: Untangling a Complex and Multifaceted Concept. Jiang M. & Belli L. (Eds) Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance. Cambridge University Press. (2024)

для восстановления своего цифрового суверенитета, включая принятие законов о защите данных[503].

Китай реализует наиболее амбициозную программу цифрового развития среди стран БРИКС, инвестируя значительные ресурсы в 5G, искусственный интеллект и высокотехнологичное производство, что способствует закреплению его позиций как глобальной технологической державы. Бразилия начала цифровую трансформацию позднее, но достигла успехов в автоматизации государственных услуг и приняла ключевые законы, такие как Marco Civil da Internet 2014[504]. Схожее значение имеет Закон о защите данных в КНР от 2018 года, которые открыли новые возможности для экономического роста[505].

Индия находится на стадии завершения законодательного процесса по защите данных, а Южная Африка разрабатывает национальные стратегии для извлечения преимуществ Четвертой промышленной революции, что стало одной из центральных тем Декларации БРИКС в Йоханнесбурге в 2018 году[506].

На саммитах БРИКС особое внимание уделяется развитию информационно-коммуникационных технологий (ИКТ) и созданию безопасной цифровой среды. Акцент делается на взаимосвязанности, надежности и устойчивости цифровых систем для экономического роста[507].

Важным элементом стратегии БРИКС является создание нормативно-правовой базы для обеспечения кибербезопасности и практического сотрудничества в области ИКТ. Страны работают над разработкой «дорожных карт» и поддерживают инициативы по созданию всеобъемлющей международной конвенции для противодействия

---

[503] Там же.
[504] Marco Civil Law of the Internet in Brazil / Presidency of the Republic. Civil House, Legal Affairs. LAW No. 12.965, APRIL 23RD 2014.
[505] Там же.
[506] Там же.
[507] Зиновьева Е.С., Игнатов А.А. Повестка ИКТ безопасности в БРИКС // Международные процессы. 2023. №4.

киберпреступности[508]. Особо значимой инициативой является BRICS Pay – международная платежная система, основанная на технологии блокчейна, которая способна обойти западные санкции и усилить экономическую независимость БРИКС[509]. В настоящее время данная инициатива еще в полной мере не реализована, но она призвана внести важный вклад в цифровое измерение экономического суверенитета стран БРИКС.

В Казанской декларации подчеркивается важность роли БРИКС в глобальной валютно-финансовой системе и обязательства по защите суверенитета в сфере ИКТ. В декларации также осуждаются односторонние действия, которые могут нарушить цепочки поставок, в частности киберсанкции, введенные Соединенными Штатами[510].

Кроме того, финансовые соглашения, достигнутые в Казани, предусматривают создание расчетно-депозитарной инфраструктуры BRICS Clear на основе технологии распределенного реестра. Это решение укрепит финансовую независимость стран БРИКС, позволяя им вести учет ценных бумаг внутри сообщества и развивать собственные механизмы финансового сотрудничества[511].

На фоне обостряющейся технологической конкуренции и геополитической нестабильности обеспечение цифрового суверенитета становится приоритетной задачей стран БРИКС. Этот вопрос приобретает еще большую актуальность в свете глобальных вызовов и растущей зависимости от передовых цифровых технологий[512].

Как убедительно свидетельствуют решения саммита в Казани, цифровой суверенитет эволюционирует от защиты информационной инфраструктуры и данных к утверждению финансово-экономической

---

[508] Шитьков С.В., Зиновьева Е.С. БРИКС на страже цифрового суверенитета // РИСИ, 2023.
[509] https://www.brics-pay.com
[510] Казанская декларация БРИКС. Казань, 2024.
[511] Там же
[512] Там же

независимости как своей ключевой составляющей. Осуждение односторонних киберсанкций и создание собственной расчетно-депозитарной инфраструктуры BRICS Clear на основе блокчейна являются стратегическими шагами по декарбонизации финансовых потоков и построению суверенных цифровых экосистем, минимизирующих уязвимость от действий отдельных государств. Подход БРИКС, таким образом, представляет суверенную и коллективную реакцию на вызовы цифровой трансформации, направленную на обеспечение международной информационной безопасности, и формирование технологически и финансово независимых контуров многополярного мира в условиях нарастающей конкуренции цифровых моделей мирового развития.

3.1.3. Цифровой суверенитет ШОС

Шанхайская организация сотрудничества (ШОС) играет ключевую роль в укреплении международного сотрудничества в сфере цифровых технологий и обеспечения информационной безопасности. Именно в рамках ШОС Российская Федерация впервые подняла вопрос о необходимости защиты цифрового суверенитета по постсоветском пространстве после событий Арабской весны. Проблематика цифрового суверенитета на уровне организации поднимается прежде всего в контексте международной информационной безопасности.

В 2011 году и впоследствии в 2015 году страны члены ШОС представили на рассмотрение ГА ООН проекты правил ответственного поведения государств в ИКТ среде, которые впоследствии были распространены как официальные документы ГА ООН на соответствующих сессиях[513]. Данные документы делали особый акцент на

[513] Международная информационная безопасность: подходы России / под ред А.В. Крутских, Е.С. Зиновьевой М.: МГИМО, 2021.

уважение государственного суверенитета, равноправное и мирное развитие ИКТ среды.

Одним из основополагающих документов, определяющих политику ШОС в области цифрового суверенитета, является Соглашение о сотрудничестве в области обеспечения международной информационной безопасности, подписанное 16 июня 2009 года[514].

Этот документ закладывает основы для предотвращения угроз и обеспечения устойчивости в цифровом пространстве, направлен на создание безопасной международной информационной среды, в которой соблюдаются права человека, обеспечивается мир и поддерживается международная стабильность.

Согласно Соглашению, информационная безопасность определяется как состояние защищенности личности, общества и государства от деструктивных воздействий в информационном пространстве[515]. Документ выделяет основные категории угроз, подрывающих международную информационную безопасность, включая разработку и применение информационного оружия, информационный терроризм, информационную преступность и цифровое неравенство. Особое внимание уделяется рискам, связанным с использованием доминирующего положения в глобальном информационном пространстве в ущерб интересам менее развитых стран.

Для эффективного противодействия этим вызовам Соглашение подчеркивает необходимость укрепления сотрудничества между странами-участницами. Совместные меры включают разработку международных правовых норм, ограничивающих распространение и использование информационного оружия, создание систем мониторинга и реагирования на новые угрозы, а также содействие развитию

---

[514] Соглашение между правительствами государств – членов Шанхайской организации сотрудничества в области обеспечения международной информационной безопасности. 2009 г.
[515] Там же.

международного сотрудничества в области кибербезопасности и противодействие информационному терроризму[516]. ШОС призывает к созданию более прозрачных и инклюзивных механизмов управления глобальной сетью Интернет, что должно способствовать её стабильному функционированию.

Отдельное внимание в документе уделено защите критически важных информационных инфраструктур государств. В условиях высокой взаимосвязанности глобальных сетей обеспечение устойчивости этих инфраструктур становится приоритетной задачей. Документ устанавливает строгие правила защиты информации, передаваемой между странами, и подчеркивает, что данные, составляющие государственную тайну, не могут быть переданы без соответствующих двусторонних или многосторонних договоренностей. Это положение способствует сохранению суверенитета стран и предотвращению утечек информации, угрожающих национальной безопасности.

Концепция цифрового суверенитета, закреплённая в документах ШОС, акцентирует внимание на праве государств самостоятельно управлять своими цифровыми системами и информационными ресурсами. В эпоху информационной глобализации это предполагает не только защиту от внешних угроз, но и активное развитие собственных технологий и нормативно-правовых механизмов, способствующих устойчивому экономическому и социальному развитию. Цифровой суверенитет становится инструментом защиты национальных интересов в условиях доминирования крупных технологических держав, стремящихся контролировать глобальные информационные потоки и инфраструктуры.

ШОС вносит значительный вклад в создание правовой базы для устойчивого цифрового развития своих государств-членов. Соглашение по международной информационной безопасности, подписанное в 2009 году

[516] Там же7

и вступившее в силу в 2012 году, стало важным шагом к выработке скоординированных подходов к цифровой безопасности. На фоне растущей зависимости от цифровых технологий страны-участницы обязуются сотрудничать для минимизации рисков, защиты данных и создания безопасного информационного пространства, способствующего процветанию и устойчивому развитию общества. ШОС выступает как площадка для обмена опытом, координации усилий и разработки совместных инициатив в ответ на вызовы информационной эпохи, что подчеркивает её важную роль в современных цифровых международных отношениях. Особенность подхода ШОС – в его жесткой привязке к традиционным понятиям государственного суверенитета и безопасности.

3.1.4. Цифровой суверенитет в повестке Лиги арабских государств

Лига арабских государств (ЛАГ), основанная в 1945 году, является региональной межправительственной организацией, объединяющей 22 арабских государства, включая Саудовскую Аравию, Египет, Объединенные Арабские Эмираты, Ирак, Алжир, Марокко и другие страны Ближнего Востока и Северной Африки. ЛАГ играет ключевую роль в укреплении сотрудничества между арабскими странами в политической, экономической, культурной и социальной сферах, что делает её важным фактором стабильности и развития в регионе.

В последние годы ЛАГ активно вовлечена в вопросы цифровой трансформации и регулирования информационно-коммуникационных технологий (ИКТ). Организация признает, что технологические инновации и цифровизация играют значительную роль в международных отношениях, оказывая влияние на безопасность, экономическое развитие и социальную стабильность. В этом контексте ЛАГ стремится способствовать интеграции цифровых инициатив среди государств-

членов, а также координирует меры по обеспечению кибербезопасности и регулированию цифрового суверенитета.

Согласно официальным отчетам ЛАГ, кибербезопасность стала одной из приоритетных тем в повестке организации после нескольких крупных инцидентов, угрожающих стабильности региона. К примеру, атаки на нефтяные объекты Саудовской Аравии, такие как инцидент с вредоносным программным обеспечением Shamoon[517], продемонстрировали, насколько уязвима энергетическая инфраструктура, которая имеет решающее значение для глобальной экономики. ЛАГ реагирует на эти вызовы через поддержку законодательных инициатив, направленных на усиление защиты критически важных данных и информационных систем. В рамках организации был создан Совет министров арабских государств по кибербезопасности[518].

Кроме того, ЛАГ активно сотрудничает с международными организациями, такими как Международный союз электросвязи (МСЭ) и Организация Объединенных Наций, для разработки глобальных стандартов в области цифрового регулирования. Взаимодействие с международными партнерами позволяет странам ЛАГ получать доступ к передовым технологиям и знаниям, обеспечивая их интеграцию в национальные стратегии цифровизации. При этом ЛАГ подчеркивает важность сохранения суверенитета и защиты культурной идентичности арабских государств в условиях глобальной цифровой трансформации.

Одним из примеров таких инициатив является принятие «Арабской стратегии по кибербезопасности»[519], которая предусматривает создание общих подходов к управлению интернет-пространством, разработку механизмов реагирования на киберугрозы и координацию усилий в

---

[517] Вредоносное ПО Shamoon и Kwampirs – дело рук одних и тех же хакеров15.03.2022. URL: https://www.itsec.ru/news/vredonosniye-po-shamoon-i-kwapirs-delo-ruk-odnih-i-teh-zhe-hakerov

[518] https://www.forbesmiddleeast.com/innovation/cybersecurity/arab-league-establishes-council-of-arab-ministers-of-cybersecurity-to-combat-growing-threats

[519] Arab cybersecurity strategy 2023 – 2027. Url: https://www.mtc.gov.tn/fileadmin/user_upload/Arab_Cybersecurity_Strategy_2023-2027_White_Paper.pdf

области цифрового образования. Страны ЛАГ работают над развитием собственной инфраструктуры, включая создание дата-центров и национальных облачных платформ, что помогает сократить зависимость от иностранных поставщиков и снизить риски утечек данных.

С учетом роли ЛАГ в международных отношениях особое значение приобретает и использование искусственного интеллекта (ИИ) в военных и оборонных целях. В последние годы такие страны, как ОАЭ и Саудовская Аравия, стали мировыми лидерами в использовании ИИ для обеспечения национальной безопасности[520]. ЛАГ поддерживает обмен информацией и передовыми технологиями среди своих членов, способствуя разработке ИИ-систем для кибероборонны и создания автономных вооружений, что становится все более актуальным в условиях современных конфликтов.

ЛАГ также активно продвигает концепцию цифрового суверенитета, подчеркивая, что государства должны сохранять контроль над данными своих граждан и критически важной инфраструктурой. Региональные инициативы, поддерживаемые ЛАГ, включают в себя меры по защите персональных данных, создание национальных центров киберугроз и разработку региональных стандартов для обработки информации.

Еще в 2010 году была принята Арабская конвенция по противодействию вредоносному использованию ИКТ[521]. Статья 4 Конвенции посвящена проблематике защиты суверенитета – “каждое государство-участник обязуется, с учетом своих собственных законов или конституционных принципов, выполнять свои обязательства, вытекающие из применения настоящей Конвенции, в соответствии с двумя принципами равенства регионального суверенитета государств и невмешательства во внутренние дела других государств. Ничто в настоящей Конвенции не

[520] UAE's International Stance on Artificial Intelligence Policy URL: https://uaelegislation.gov.ae/en/policy/details/uae-s-international-stance-on-artificial-intelligence-policy

[521] Arab Convention on Combating Information Technology Offences. League of Arab States General Secretariat & 2010. URL: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf

позволяет государству-участнику осуществлять на территории другого государства юрисдикцию или функции, осуществление которых является исключительным правом властей этого другого государства в силу его внутреннего права”[522].

Таким образом, Лига арабских государств играет ключевую роль в формировании цифровой повестки дня в регионе, обеспечивая координацию усилий стран-членов в противодействии киберугрозам, содействуя технологической интеграции и обеспечивая устойчивое развитие в условиях цифровой эры. В условиях стремительно меняющегося мирового порядка ЛАГ остается важным игроком, определяющим политику в сфере информационной безопасности и цифрового сотрудничества на международной арене.

Роль ЛАГ в цифровых международных отношениях заключается, прежде всего, в создании условий для скоординированного ответа региона на современные вызовы и угрозы в цифровой сфере. Организация проводит регулярные встречи на уровне министров связи и информации для обсуждения совместных стратегий и внедрения общих стандартов в области кибербезопасности, защиты данных и развития цифровой экономики. Эти мероприятия способствуют обмену опытом между странами, что критически важно для противодействия кибератакам и защите цифровой инфраструктуры.

Вывод по параграфу:

Современная цифровая революция радикально трансформирует международные отношения, привнося новые вызовы и возможности для глобального управления. Концептуализация этих процессов демонстрирует, что цифровая среда становится не просто технологической, но и политической ареной, где пересекаются интересы государств, транснациональных корпораций и международных

[522] Там же.

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.

Однако сама природа этого пространства, характеризующаяся глубокой взаимозависимостью и трансграничностью, парадоксальным

образом означает, что абсолютный цифровой суверенитет, достижимый исключительно односторонними действиями, является иллюзией. Подлинная технологическая независимость и безопасность в глобальном масштабе не могут быть обеспечены через изоляцию и фрагментацию, но лишь через сложный и многополярный диалог, направленный на установление четких «правил игры».

Такой диалог должен признавать легитимность стремления государств к защите своего цифрового пространства, но одновременно предотвращать его превращение в инструмент бесконтрольного протекционизма или цифрового авторитаризма. Ключевая задача международного сотрудничества на площадках ООН, БРИКС, ШОС и других форумов заключается в том, чтобы найти тонкий баланс между принципом невмешательства во внутренние дела и необходимостью соблюдения фундаментальных прав и свобод человека в цифровую эпоху, между правом на технологическое развитие и обязательствами по обеспечению международной безопасности. Только через переговоры и взаимное признание интересов можно создать инклюзивный и стабильный режим глобального цифрового управления, который, обеспечивая необходимый уровень суверенитета для отдельных государств, одновременно сохранял бы глобальную связность и инновационный потенциал цифровой среды, предотвращая её распад на изолированные и враждебные друг другу кибер-анклавы.

3.2. Цифровой суверенитет в практике региональной интеграции: ЕврАзЭс, ЕС, АСЕАН, Меркосур

3.2.1. Цифровой суверенитет на повестке ЕС

Подход Европейского Союза (ЕС) к политике в области цифрового суверенитета отличается и многоуровневостью, что отражает стремление создать независимую цифровую экосистему, способную защищать

интересы европейских граждан и бизнеса в глобальной технологической среде. При этом нельзя не отметить неоколониальные устремления ЕС, которые отражаются в желании усилить свои позиции в цифровых международных отношениях[523]. Значимость анализа ЕС обусловлена его статусом нормативного лидера в сфере цифрового регулирования и масштабностью правовой базы (GDPR, DSA, DMA, AI Act 2025), что требует более детального рассмотрения по сравнению с другими интеграционными объединениями.

Как и в КНР, особый акцент делается на суверенитет в области данных. Проект «European Cloud Initiative Gaia-X» был объявлен совместно Германией и Францией и предполагает создание с 2020 года федеративной инфраструктуры данных на европейском уровне, которая рассматривается как важная составляющая цифрового суверенитета. Как отмечает А.Н. Толстухина, практика обеспечения цифрового суверенитета ЕС на уровне региона в настоящее время смещается в сторону «стратегической автономии»[524]. Под стратегической автономией имеется в виду прежде всего технологическая независимость и безопасность, в том числе в сфере цифровых технологий.

Впервые цифровые технологии были определены в качестве ключевого фактора в достижении целей европейской интеграции в 2010 году в Цифровой повестке для Европы (2010-2020). Первая цифровая повестка была ориентирована на улучшение доступа к цифровым товарам и услугам для потребителей и предприятий по всей Европе, а также на формирование институтов правового регулирования цифровой экономики.

Европейский Союз (ЕС) уже на протяжении нескольких десятилетий уделяет особое внимание обеспечению цифрового суверенитета, поскольку его зависимость от импортных информационно-

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

[524] Толстухина А. Цифровой суверенитет Европейского Союза и его границы. Валдайская записка. 2022. URL: https://ru.valdaiclub.com/files/42559/

технологических решений, как программных, так и аппаратных, стремительно увеличивается. Эта зависимость представляет собой вызов, учитывая растущую значимость цифровых технологий для обеспечения государственной дееспособности и, в конечном счете, для сохранения государственного суверенитета.

Одним из центральных элементов этого подхода является нормативная власть ЕС, направленная на распространение своих ценностей и стандартов, таких как защита данных. В этом контексте такие законодательные инициативы, как Общий регламент по защите данных (GDPR)[525], Закон о цифровых услугах (Digital Services Act)[526] и Закон о цифровых рынках (Digital Markets Act)[527], демонстрируют стремление ЕС оказывать влияние на глобальные цифровые стандарты.

Важнейшей чертой этой политики является её интеграция с общей стратегией ЕС по обеспечению стратегической автономии, что включает развитие собственных технологических решений и снижение зависимости от внешних поставщиков. Стремление ЕС к независимости поддерживается значительными инвестициями в ключевые технологии, такие как искусственный интеллект, квантовые вычисления и производство полупроводников, а также созданием единого цифрового рынка и европейского рынка данных.

Зависимость от иностранных технологий, прежде всего от американских и китайских компаний, подталкивает ЕС к разработке целостной стратегии по защите и развитию своей цифровой экосистемы.

---

[525] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

[526] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)

[527] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance)

Важной вехой стало принятие в 2020 году новой Цифровой повестки для Европы (2020-2030)[528]. Повестка ставит цели достижения и поддержания глобального технологического лидерства ЕС, обеспечения стратегической автономии в сфере цифровых технологий и защиты цифрового суверенитета ЕС, а также распространения технологических стандартов ЕС в других регионах. Она сфокусирована на развитии прорывных технологий, в том числе: квантовых вычислений, использовании блокчейна в сфере торговли, искусственного интеллекта, широкополосных сетей связи нового поколения 5G и 6G. Стратегической целью является формирование единого европейского пространства данных и общего рынка данных и развития общеевропейской цифровой инфраструктуры, а также обеспечение кибер-безопасности ЕС. Внимания заслуживает Европейский закон о чипах 2023 года, который призван создать условия для развития европейской производственной базы в сфере полупроводников, привлечения инвестиций, поддержки исследований и инноваций, а также для подготовки ЕС к возможным перебоям с поставками чипов в будущем[529].

В рамках цифровой повестки ЕС значительный акцент сделан на развитие технологий искусственного интеллекта. В феврале 2020 года была опубликована Белая книга ЕС по искусственному интеллекту[530]. 21 апреля 2021 года Европейская комиссия опубликовала предложение по новому Закону об искусственном интеллекте (COM (2021) 0206), закрепив в законодательстве ЕС технологически нейтральное определение искусственного интеллекта. Более того, в сентябре 2022 года Европейская

---

[528] Digital agenda for Europe. URL: https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe#:~:text=The%20European%20digital%20agenda%20for,twin%20digital%20and%20green%20transitions.

[529] В ЕС принят закон о европейских чипах для развития собственной полупроводниковой отрасли https://d-russia.ru/v-es-prinjat-zakon-o-evropejskih-chipah-dlja-razvitija-sobstvennoj-poluprovodnikovoj-otrasli.html#:~:text=European%20Chips%20Act%20подразумевает%20привлечение,мере%2020%25%20к%202030%20году.

[530]White Paper on Artificial Intelligence – a European approach to excellence and trust URL: https://digital-strategy.ec.europa.eu/en/consultations/white-paper-artificial-intelligence-european-approach-excellence-and-trust

Комиссия опубликовала предложение по директиве об адаптации внедоговорных норм гражданской ответственности к искусственному интеллекту («Директива об ответственности ИИ»), чтобы гарантировать, что люди, пострадавшие от систем ИИ, пользуются тем же уровнем защиты, что и те, кто пострадал от других технологий.

1 августа 2024 года вступил в силу Закон Европейского Союза об искусственном интеллекте (ИИ), ставший первым в мире комплексным нормативным актом, регулирующим использование ИИ-систем. Этот закон классифицирует системы ИИ по степени риска и устанавливает соответствующие требования для их разработки и применения. Закон вводит четыре категории риска: неприемлемый, высокий, ограниченный и минимальный. Системы, относящиеся к категории неприемлемого риска, полностью запрещены, в то время как для высокорисковых систем предусмотрены строгие требования к безопасности, прозрачности и качеству. Системы с ограниченным и минимальным риском подлежат менее строгому регулированию[531].

Кроме того, закон запрещает использование ИИ-систем, которые манипулируют поведением людей, нарушают их права или представляют угрозу безопасности. Особое внимание уделяется системам распознавания лиц и социального рейтинга, которые ограничены или запрещены в определенных контекстах. Закон также предусматривает создание Европейской комиссии по ИИ, которая будет отвечать за надзор за соблюдением норм закона и координацию действий между государствами-членами ЕС. Ожидается, что этот орган начнет свою работу в ближайшие месяцы.

[531] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)
PE/24/2024/REV/1

Кроме того, ЕС активно развивает сотрудничество с НАТО в области кибербезопасности и противодействия гибридным угрозам, что подчеркивает важность коллективной безопасности и устойчивости в цифровую эпоху. Координация с НАТО помогает ЕС укрепить защиту критически важной инфраструктуры и создать механизмы быстрого реагирования на киберугрозы.

Таким образом, подход ЕС к цифровому суверенитету сочетает защиту внутреннего цифрового пространства с экспортом европейских ценностей и стандартов в глобальной цифровой среде. Л. Монсес и Д. Ламбах выделяют три аспекта цифрового суверенитета ЕС «5G, Gaia-X и полупроводниковая промышленность. Эта эмпирическая перспектива позволяет лучше понять, как представления о цифровом суверенитете помогают утверждать определенную европейскую идентичность, как определенные геополитические представления появляются в этих проектах цифрового суверенитета. Слабые цифровые отрасли Европы считаются проблемой безопасности. Китай и, в меньшей степени, Соединенные Штаты рассматриваются не только как экономические соперники, но и как угрозы безопасности, когда речь идет о таких вопросах, как шпионаж и защита данных. Проекты цифрового суверенитета ЕС способствуют особой идентичности ЕС как гибкого, ориентированного на будущее глобального игрока в оцифрованной экономике»[532].

В свете обострения глобальной технологической конкуренции и геополитических вызовов ЕС стремится укрепить свою автономию через инициативы, направленные на развитие собственных технологических решений, что соответствует общей стратегии, изложенной в документах Европейской комиссии и Европейского совета.

[532] Monsees L., Lambach D. Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity //European Security. – 2022. – Т. 31. – №. 3. – С. 377-394.

Значительной частью этих усилий является создание единого цифрового рынка и европейского рынка данных. Стратегия единого цифрового рынка ЕС нацелена на устранение цифровых барьеров между государствами-членами, что позволит бизнесу и потребителям получать выгоду от бесперебойного доступа к цифровым услугам и товарам по всей Европе. Основные элементы этой стратегии включают упрощение трансграничной торговли цифровыми товарами и услугами, защиту потребителей в онлайн-среде и обеспечение честной конкуренции между цифровыми платформам.

Регулирование трансграничных потоков данных является основной осью, на которой основана новая европейская цифровая повестка дня. Законодательные инициативы ЕС последних лет ориентированы на поиск баланса между свободой передачи данных и сохранением конфиденциальности, безопасности, безопасности и этических стандартов в области обработки данных. В феврале 2020 года была опубликована Европейская стратегия в области данных[533], ориентированная на формирование общеевропейского рынка данных. Стратегия направлена на повышение доступности данных, возможности их повторного использования и развития обмена данными. 23 февраля 2022 года Европейская Комиссия опубликовала предложение о гармонизированных правилах справедливого доступа к данным и их использования (Закон о данных). Документ рассматривает данные как важный ресурс экономического роста, конкурентоспособности, инноваций и создания рабочих мест. Развитие Европейского пространства данных является одним из приоритетов на 2019-2025 годы и включает девять секторов: здравоохранение, окружающая среда, энергетика, сельское хозяйство, мобильность, финансы, производство, общественная деятельность.

[533]Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance) URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

администрирование и навыки. ЕС создаст европейское облачное хранилище данных в рамках плана NextGenerationEU на основе Gaia-X[534].

Европейская стратегия данных (European Data Strategy), представленная в 2020 году, предполагает создание пространства общих данных, где компании и государственные учреждения смогут безопасно обмениваться информацией. Цель состоит в том, чтобы увеличить объем данных, доступных для использования в интересах общества и бизнеса, укрепляя позиции ЕС в глобальной экономике данных и позволяя странам-членам лучше контролировать использование своих данных (European Commission, 2020).

Эти инициативы предполагают разработку регулирующей базы, которая обеспечит соблюдение стандартов конфиденциальности и безопасности данных, соответствующих европейским ценностям. В этом контексте важным шагом стало принятие Закона о данных (Data Act), направленного на стимулирование обмена данными между секторами экономики, защиту прав пользователей на свои данные и ограничение доминирования крупных международных игроков в сфере данных[535].

Таким образом, формирование единого цифрового рынка и европейского рынка данных является стратегическим приоритетом ЕС, что подчеркивает стремление Союза создать независимую и инновационную цифровую экосистему, способную конкурировать на глобальном уровне и обеспечивать защиту интересов европейских граждан и бизнеса.

В целях создания безопасного и открытого общеевропейского цифрового рынка, защищающего права пользователей и создающего равные условия для бизнеса в 2022 году были приняты две

[534] Проект GAIA X был заявлен в 2019 году как едина общеевропейская платформа облачных вычислений, куда вошли 22 компании из Франции и Германии.
[535] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance)

законодательные инициативы: Закон о цифровых услугах (DSA)[536] и Закон о цифровых рынках (DMA)[537]. Законы устанавливают правила ответственности и подотчетности для поставщиков цифровых услуг, в особенности, крупных онлайн-платформ и социальных сетей, прежде всего, из-за рисков, которые они представляют при распространении незаконного и вредоносного контента. Закон о цифровых рынках (DMA) определяет, при каких условиях крупная интернет-платформа может быть отнесена к «привратникам». Привратники – это цифровые платформы, которые «предоставляют важный канал связи между коммерческими пользователями и потребителями, чьё положение может позволить им действовать в качестве субъектов нормотворчества, приводя таким образом к возникновению ограничивающего фактора» в условиях цифровой экономики[538]. Согласно документам, технологические платформы, занимающие ключевые позиции на рынке, должны соблюдать ряд правил, например:

- персональные данные (ПД) пользователей могут быть использованы для целевой рекламы только если субъект ПД дал на это свое согласие;
- запрет на навязывание пользователям приложений или настроек по умолчанию;
- сервисы обмена сообщениями должны будут обеспечить их совместимость с небольшими приложениями;
- техногигантам нельзя оценивать свои услуги выше, чем услуги конкурентов.

---

[536] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)
PE/30/2022/REV/1

[537] Digital Services Act and Digital Markets Act. EU, 2021. URL: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

[538] Вступил в действие новый закон ЕС о цифровых рынках https://d-russia.ru/vstupil-v-dejstvie-novyj-zakon-es-o-cifrovyh-rynkah.html https://d-russia.ru/vstupil-v-dejstvie-novyj-zakon-es-o-cifrovyh-rynkah.html

Помимо борьбы с деструктивным контентом данная законодательная инициатива ориентирована на снижение влияния американских цифровых гигантов в странах ЕС и поддержку европейского цифрового бизнеса[539].

В 2022 году высокий представитель опубликовал совместное сообщение о Политике ЕС в области киберзащиты. Новая политика киберзащиты увеличит инвестиции в данную область, тем самым укрепляя сотрудничество между военными и гражданскими киберсообществами. Инициатива направлена на снижение стратегической зависимости ЕС от важнейших ИТ-технологий США, одновременно укрепляя Европейскую оборонно-технологическую промышленную базу. При этом преимущественно проблематика кибер-безопасности входит в сферу компетенции НАТО.

ЕС и НАТО обмениваются информацией, проводят совместные учения по реагированию на киберугрозы и разрабатывают механизмы быстрого реагирования на инциденты. Например, Европейское агентство по кибербезопасности (ENISA) и Центр передового опыта НАТО по киберзащите (NATO Cooperative Cyber Defence Centre of Excellence) активно взаимодействуют для разработки и тестирования совместных стратегий защиты критически важной цифровой инфраструктуры[540].

ЕС и НАТО сотрудничают в создании механизмов раннего предупреждения и координации ответных мер, а также в обеспечении совместной информационной осведомлённости о потенциальных гибридных угрозах. Это особенно актуально в контексте возросшей геополитической напряжённости, когда такие угрозы могут быть направлены на подрыв политической стабильности и экономической безопасности в Европе[541].

---

[539] Толстухина А. Big Tech vs регуляторы: долгосрочный глобальный тренд. Рабочая тетрадь РСМД. 2022. URL: https://russiancouncil.ru/papers/BigTech-RIAC-WorkingPaper-71.pdf

[540] Vilnius Summit Communiqué
Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Vilnius 11 July 2023

[541] The European Union and NATO intensify cooperation on addressing cyber threats. 2023. URL: https://www.eeas.europa.eu/eeas/european-union-and-nato-intensify-cooperation-addressing-cyber-threats_en

Понятие цифрового суверенитета ЕС охватывает стремление государств-членов к независимости и контролю над своими цифровыми ресурсами, технологиями и данными, что становится стратегическим приоритетом в условиях глобальной технологической конкуренции. Зависимость от иностранных технологий, прежде всего от американских и китайских компаний, подталкивает ЕС к разработке целостной стратегии по защите и развитию своей цифровой экосистемы.

В настоящее время ЕС разработал наиболее проработанный в мире комплекс нормативно-правовых инструментов и институтов в области управления цифровой интеграцией. Несмотря на значительные инвестиции и внимание к данной области, по уровню развития цифровых технологий ЕС уступает США и Китаю. В этих условиях значительный акцент в рамках цифровой интеграции ЕС делается на ограничение возможностей цифровых гигантов, большая часть которых базируется в США и КНР и создание условий для формирования конкурентоспособного европейского цифрового бизнеса. Европейские регуляторы стремятся остановить монополизацию рынка со стороны неевропейских корпораций, защитить персональные данные своих граждан, предотвратить распространение дезинформации и деструктивного контента в Интернете, а также обеспечить прозрачность работы алгоритмов[542]. Глобальное распространение технологических и правовых стандартов ЕС также видится как важный инструмент стратегической автономии и глобального лидерства ЕС в цифровом пространстве.

3.2.2. Цифровой суверенитет АСЕАН

[542]Толстухина, А. Ю. Big Tech vs регуляторы: долгосрочный глобальный тренд: рабочая тетрадь №71 / 2022 [А. Ю. Толстухина, К. Н. Мат веенков ; под ред. Е. О. Карпинской, А. Ю. Толстухиной, С. М. Гавриловой]; Российский совет по международным делам (РСМД). — М.: НП РСМД, 2022. — 56 с. URL: https://russiancouncil.ru/papers/BigTech-RIAC-WorkingPaper-71.pdf

Основанная в 1967 г., АСЕАН первоначально сосредоточилась на экономическом сотрудничестве и урегулировании конфликтов. Однако со временем она превратилась в многогранную организацию, занимающуюся безопасностью, социально-культурными проблемами и региональной дипломатией. Такие принципы, как невмешательство во внутренние дела, уважение суверенитета и принятие решений на основе консенсуса, сыграли важную роль в поддержании стабильности и укреплении позиций АСЕАН на мировой арене[543].

Цифровой суверенитет в контексте Ассоциации государств Юго-Восточной Азии (АСЕАН) охватывает аспекты, связанные с управлением цифровыми технологиями и данными в странах региона.

Многие страны АСЕАН принимают меры для укрепления контроля над данными и защиты киберпространства. Это может включать в себя разработку национальных законов и регуляторных стандартов для защиты данных, предотвращения кибератак и обеспечения безопасности цифровой инфраструктуры.

В 1997 г. был принят первый документ, направленный на укреплении цифрового измерения интеграции в АСЕАН «Видение АСЕАН – 2020»[544]. В АСЕАН, в частности, наблюдается быстрое распространение цифровых технологий. В регионе АСЕАН произошел резкий рост числа интернет-пользователей – на 100 млн за четыре года с 2015-го и еще на 100 млн с 2019-го. К 2022 г. насчитывалось уже 460 млн интернет-пользователей. С началом интернет-бума мессенджеры, социальные сети, мобильные приложения служб доставки, интернет-банкинг и многие другие «цифровые продукты» стали неотъемлемой частью жизни большинства людей в Юго-Восточной Азии. Распространенность онлайн-покупок подкрепляется доступностью и использованием цифровых устройств. Это

[543]Титов А. и др. Цифровое завтра: как АСЕАН стимулирует рост цифровой экономики// Современная мировая экономика. 2024. Том 2. №1(5). URL: https://cwejournal.hse.ru//titov-1-2024
[544] ASEAN VISION 2020 June 28, 2012. URL: https://asean.org/asean-vision-2020/

стало очевидным на фоне пандемии COVID-19, когда произошел существенный сдвиг в ретейле – из традиционных магазинов в онлайн. В 2022 г., когда пандемия все еще вызывала беспокойство в некоторых отраслях, валовая выручка цифровой экономики Юго-Восточной Азии достигла почти 200 млрд долларов[545].

АСЕАН – крупнейшая межгосударственная политико-экономическая организация региона: по данным на 2018 г., численность населения составила 642,4 млн человек, совокупный ВВП 2,7 трлн долларов, внешнеторговый оборот – 2,5 трлн долл. Поставлена цель к 2030 г. стать четвертой экономикой мира[546]. Цифровая трансформация, рассматриваемая как важнейший инструмент достижения целей интеграции АСЕАН, находится в центре внимания уже более двух десятилетий с момента подписания Рамочного соглашения об электронной АСЕАН в ноябре 2000 года. Цифровизация в рамках АСЕАН направлена на ускорение развития цифровой экономики за счет формирования единого цифрового рынка, порождающего «эффект масштаба» и «сетевые эффекты», а также обеспечивающего усиление притока инвестиций в цифровую сферу АСЕАН[547]. Показательно, что Ассоциации удалось добиться 100% реализации всех 87 проектов, отмеченных в Генеральном плане АСЕАН по развитию ИКТ до 2015 г.[548]

В 2018 году в ходе председательства Сингапура в АСЕАН было принято Соглашение АСЕАН об электронной торговле. Рамочная программа комплексного восстановления АСЕАН после пандемии Covid-19 2021 года определила ускорение инклюзивной цифровой

---

[545]Титов А. и др. Цифровое завтра: как АСЕАН стимулирует рост цифровой экономики// Современная мировая экономика. 2024. Том 2. №1(5). URL: https://cwejournal.hse.ru//titov-1-2024

[546] ЕАЭС и АСЕАН обменялись опытом в сфере цифровой трансформации // ЕЭК URL: https://eec.eaeunion.org/news/eaes-i-asean-obmenyalis-opytom-v-sfere-tsifrovoy-transformatsii-/

[547] Васина А.М., Демина Ю.А. Политика в целях развития в плановых и стратегических документах АСЕАН // Азиатско-Тихоокеанский регион: экономика, политика, право. 2022. № 4. 49 – 68.

[548] Канаев Е. А., Королев А. С. ЕАЭС и АСЕАН: результаты и перспективы сотрудничества //Мировая экономика и международные отношения. – 2020. – Т. 64. – №. 1. – С. 64-72. https://www.imemo.ru/index.php?page_id=1248&file=https://www.imemo.ru/files/File/magazines/meimo/01_2020/08-KANAEV.pdf

трансформации как одну из пяти широких стратегий по выводу АСЕАН из кризиса.

Пандемия COVID-19 ускорила темпы цифровизации в АСЕАН. В 2020 году 40 миллионов человек в шести крупнейших экономиках Юго-Восточной Азии впервые перешли на цифровые технологии по сравнению со 100 миллионами новых пользователей за предыдущие пять лет, что укрепило позиции АСЕАН как самого быстрорастущего интернет-рынка в мире[549]. Быстрые темпы проникновения новых технологий обусловили растущий интерес к полноценному доступу и использованию цифровых технологий гражданами стран АСЕАН, среди которых цифровые технологии развиты неравномерно. В числе лидеров – Сингапур и Малайзия, при этом отдельные страны, такие как Камбоджа, Лаос, Мьянма, характеризуются значительно более низкими уровнями проникновения цифровых технологий. Без решения проблемы цифрового разрыва невозможно укрепление цифровой связности региона и решение задач интеграции.

В числе вызовов цифровой интеграции АСЕАН: недостаточно широкое распространение цифровой грамотности, различие в доступе к интернету между странами и регионами, неравномерность развития цифровой инфраструктуры, а также недостаточное развитие систем трансграничных электронных платежей и цифрового банкинга (на 2023 год его использовали только порядка 30% населения стран АСЕАН), что тормозит развитие трансграничной электронной торговли[550]. Например, в Индексе сетевой готовности 2023 г. Сингапур занял 2-е место из 131 страны мира, Малайзия заняла 40-е место, Индонезия – 59-е, а Филиппины – 69-е. Камбоджа и Лаосская Народно-Демократическая Республика,

[549] The bandar Seri Begawan roadmap: an ASEAN digital transformation agenda to accelerate ASEAN's economic recovery and digital economy integration URL: https://asean.org/wp-content/uploads/2021/10/Bandar-Seri-Begawan-Roadmap-on-ASEAN-Digital-Transformation-Agenda_Endorsed.pdf

[550] Цифровизация ММСП в странах АСЕАН / Министерство экономики и развития РФ/ URL: https://www.economy.gov.ru/material/file/b261c8ad088c0dc63e28d37a5aa47524/cifrovizaciya_mmsp_v_rossii_i_stranah_asean.pdf

напротив, имеют низкий рейтинг – 108-е и 109-е места соответственно. Это говорит о том, что прогресс стран АСЕАН в области цифровизации пока неоднородный[551].

Однако, несмотря на вызовы, страны АСЕАН находятся в числе лидеров в области цифровой трансформации и опыт АСЕАН в данной области рассматривается как весьма успешный. АСЕАН работает над разработкой политики и стандартов, касающихся цифрового суверенитета, чтобы обеспечить гармонизацию подходов и выработку общих решений для стран региона. Это может включать в себя создание рамок для защиты данных и регулирования цифровых платформ. В целом, страны АСЕАН стремятся сбалансировать национальный контроль над цифровыми технологиями с необходимостью сотрудничества на региональном и глобальном уровнях для стимулирования роста и устойчивого развития цифровой экономики.

3.2.3. Формирование единого цифрового пространства ЕАЭС и проблемы обеспечения цифрового суверенитета

Евразийский экономический союз (ЕАЭС) активно развивает политику в области цифрового суверенитета, направленную на укрепление независимости и конкурентоспособности своих государств-членов в цифровой сфере.

Старт цифровой повестке ЕАЭС был дан 26 ноября 2015 года в Минске на первом заседании президиума Делового совета Евразийского экономического союза (ЕАЭС). В 2016 году ЕАЭС были выработаны и представлены Предложения по формированию цифрового пространства[552].

---

[551] Титов А. и др. Цифровое завтра: как АСЕАН стимулирует рост цифровой экономики// Современная мировая экономика. 2024. Том 2. №1(5). URL**:** https://cwejournal.hse.ru//titov-1-2024

[552] Преложения по формированию цифрового пространства ЕАЭС. URL: https://eec.eaeunion.org/upload/medialibrary/ccc/Predlozheniya-po-formirovaniyu-tsifrovogo-prostranstva.pdf

В предложениях было отмечено, что за счет объединения усилий и ресурсов стран ЕАЭС при создании общего цифрового пространства возможно достижение синергетического эффекта, что расширит возможности и преимущества ЕАЭС в области экономического развития.[553].

В принятом в 2017 году Заявлении о цифровой повестке ЕАЭС заявлена приверженность формирования условий развития цифровой повестки ЕАЭС. Важнейшим документом на данном направлении стали принятые в 2017 году Стратегические направления развития цифровой повестки ЕАЭС до 2025 года[554]. Стратегические направления включают в себя шесть сфер сотрудничества: цифровую прослеживаемость товаров, услуг и цифровых активов, цифровую торговлю, транспортные коридоры и промышленную кооперацию, а также регулирование оборота данных ЕАЕС[555].

Россия является лидером в области цифровой интеграции ЕАЭС и на уровне государственной политики оказывает поддержку цифровой повестке. Указом Президента Российской Федерации от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» Правительству Российской Федерации установлено обеспечить в 2024 году решение задачи по разработке и внедрению национального механизма осуществления согласованной политики государств-членов ЕАЭС при реализации планов в области развития цифровой экономики[556].

С целью интенсификации цифрового измерения интеграционных процессов 8 июня 2023 года главы правительств приняли доклад о

---

[553] Там же.

[554] Стратегические направления формирования и развития цифрового пространства Евразийского экономического союза в перспективе до 2025 года (проект) URL: https://eec.eaeunion.org/upload/medialibrary/343/Strategicheskie-napravleniya-formirovaniya-tsifrovogo-prostranstva-EAES-_proekt_.pdf

[555] Ефремов А.В. Цифровая интеграция ЕАЭС: в тупике или на распутье? // Россия в глобальной политикею 2023. URL: https://globalaffairs.ru/articles/czifrovaya-integracziya-eaes/

[556] О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 // Указ Президента Российской Федерации от 07.05.2018 г. № 204 URL: http://kremlin.ru/acts/bank/43027

дальнейшем развитии интегрированной информационной системы ЕАЭС и цифровой повестки Союза, а также распоряжение, предусматривающее дальнейшие шаги по цифровой трансформации сфер сотрудничества, определённых Договором о ЕАЭС. Евразийская экономическая комиссия утвердила Целевую программу развития интегрированной системы (ИИС) Союза до 2027 года[557]. 2 августа 2023 года было принято решение о взаимном признании электронных цифровых подписей (ЭЦП) трансграничных B2G (Business-to-Government) взаимодействиях на территории Евразийского экономического союза. Это снимает необходимость для бизнеса получать отдельные ЭЦП для каждой страны.

Значительное внимание в рамках цифровой повестки ЕАЭС сделано на цифровом суверенитете стран-участниц, что предполагает снижение зависимости от западных цифровых технологий и стратегическую автономию в цифровой сфере. В 2022 году началось обсуждение возможности разработки межгосударственной программы развития полупроводниковой промышленности в странах–членах Евразийского экономического союза. В настоящее время обсуждаются также вопросы сотрудничества ЕАЭС и в других высокотехнологичных областях, однако, эксперты отмечают слабость технологической базы ЕАЭС и высокую зависимость от иностранных поставщиков в сфере высоких технологий[558].

В числе вызовов на пространстве ЕАЭС - различие в уровнях развития цифровой инфраструктуры и доступе к интернету. Недостаточно высокие темпы цифровой интеграции на пространстве ЕАЭС также связаны с межстрановыми различиями в нормативно-правовой базе. Цифровизация интеграционных процессов ЕАЭС позволит повысить экономические преимущества от сотрудничества, получить доступ к

[557]В ЕАЭС началось переформатирование цифровой повестки URL: https://eec.eaeunion.org/news/v-eaes-nachalos-pereformatirovanie-tsifrovoy-povestki-/

[558]Кооперацию с ЕАЭС полупроводят в жизнь // Коммерсант, 22.09.2022 URL: https://www.kommersant.ru/doc/5571902 (дата обращения 27.11.2025)

новым цифровым рынкам, а также реализовывать программы снижения зависимости от западных онлайн-платформ и технологических решений.

В политическом измерении ставится задача укрепления ЕАЭС как центра силы и в современной глобальной цифровой политике, при этом Россия выступает в роли лидера в интеграционных процессах на постсоветском пространстве. Для достижения данной цели необходимо развитие сотрудничества с третьими странами и интеграционными структурами и включение в повестку данного взаимодействия вопросов цифровизации в целях обмена опытом, получения доступа к технологиям и лучшим практикам.

Одной из тенденций международного сотрудничества в цифровой сфере является трансрегионализм – сотрудничество между интеграционными объединениями различных регионов. ЕАЭС стремится играть возрастающую роль в экономическом сотрудничестве на евразийском континенте, для достижения данной цели необходимо трансрегиональное экономическое сотрудничество и расширение сети партнерского взаимодействий. В Концепции внешней политики Российской Федерации от 2023 года отмечается необходимость формирования широкого интеграционного контура – Большого Евразийского партнерства – посредством объединения потенциалов всех государств, региональных организаций и объединений Евразии с опорой на ЕАЭС, ШОС и Ассоциацию государств Юго-Восточной Азии (АСЕАН), сопряжение планов развития ЕАЭС и китайской инициативы «Один пояс – один путь» при сохранении возможности участия в этом партнерстве всех заинтересованных государств и многосторонних объединений Евразийского континента и, как следствие, формирование сети партнерских организаций в Евразии[559].

---

[559] https://www.mid.ru/ru/detail-material-page/1860586/?TSPD_101_R0=08765fb817ab2000840b10c00f2a27fe8113ede6067ae204444cc9d87c960ec35a800b00db02ddb7084cee901c143000d6dd18af471e8a3fbae3d8ddcaaf6e0ae7c8e3a60dfa0ff3ddd28f4df2f55d6894cd8700de0a40d40c067f4c31acf057 (дата обращения 27.11.2025)

В условиях конфронтации со странами Запада возрастает значимость сотрудничества с Китаем. Россия и другие страны ЕАЭС с 2019 года участвуют в программе «Цифровой шелковый путь», которая предполагает создание цифровой и телекоммуникационной инфраструктуры, в том числе сетей связи нового поколения 5G. Кроме того, «Цифровой шелковый путь» направлен на установление общественных связей через он-лайн платформы и приложения для электронной коммерции, финансовых и образовательных технологий, а также продвижение китайского цифрового оборудования. Сопряжение «Цифрового шёлкового пути» и интеграции ЕАЭС позволяет странам ЕАЭС снизить зависимость от западных онлайн-платформ и технологий.

Россия, как один из ключевых участников ЕАЭС, активно продвигает инициативы по укреплению цифрового суверенитета Союза. Премьер-министр Михаил Мишустин подчеркнул необходимость использования отечественных разработок для обеспечения независимости в цифровой сфере.

Однако, несмотря на достигнутые успехи, ЕАЭС сталкивается с вызовами, связанными с высокой зависимостью от иностранных цифровых технологий. Для достижения реального технологического суверенитета необходима усиленная технологическая кооперация между государствами-членами, что может стать основой для глубокой цифровой интеграции. Таким образом, политика ЕАЭС в области цифрового суверенитета направлена на создание единого цифрового пространства, повышение конкурентоспособности и обеспечение независимости Союза в условиях глобальной цифровой трансформации.

3.2.4. Цифровые технологии и цифровой суверенитет Меркосур

Подход МЕРКОСУР к обеспечению цифрового суверенитета выделяется своим акцентом на коллективных усилиях и уважении к

внутренним особенностям государств-членов. Этот южноамериканский интеграционный блок, включающий Аргентину, Бразилию, Парагвай и Уругвай, рассматривает цифровой суверенитет как неотъемлемую часть региональной независимости. Страны региона осознают, что глобальные технологические гиганты, предоставляя платформы и сервисы, в то же время могут угрожать национальным интересам, контролируя данные и информационные потоки. Именно поэтому вопрос цифрового суверенитета становится одновременно экономическим, политическим и культурным вызовом.

Важнейшим элементом концепции суверенитета стран Латинской Америки является колониальное прошлое. Исследователи отмечают стремление региона к практической реализации концепции «нового неприсоединения» и укреплению суверенитета и не зависимости на международной арене[560]. 2020-е гг. с их горькими уроками пандемии и санкционных войн побудили политиков наращивать усилия в направлении разного вида суверенитета – медицинского, продовольственного, энергетического, причем в масштабах всего региона, о чем, к примеру, говорят соответствующие документы[561] и планы[562] в рамках CELAC[563]. Если говорить о политической рамке для «неприсоединения», то ее можно проассоциировать с интеграцией – в виде формирования в Южной, Латинской Америке структур для отображения коллективной воли, голоса стран[564]. Это находит отражение и в практике цифрового суверенитета в регионе.

---

[560] Fortín, C., Heine J., Ominami C. El no alineamiento activo y América Latina: una doctrina para el nuevo siglo, Santiago de Chile, Editorial Catalonia, 2021, 383 pp.

[561] https://www.sela.org/media/3226666/vii-cumbre-celac-declaracion-de-buenos-aires.pdf (дата обращения 27.11.2025)

[562] https://www.pv-magazine-mexico.com/2024/03/07/apostar-por-la-autosuficiencia-energetica-en-america-central-y-el-caribe/ (дата обращения 27.11.2025)

[563] Коновалова К. Концепция «нового неприсоединения» и Латинская Америка // РСМД, 13.05.2024. URL: https://russiancouncil.ru/analytics-and-comments/analytics/kontseptsiya-novogo-neprisoedineniya-i-latinskaya-amerika/ (дата обращения 27.11.2025)

[564] Там же.

Технологическое развитие и сокращение технологического разрыва между членами Меркосур являлось важной задачей интеграционного блока с момента образования в 1992 г. Однако работа над общей правовой и технологической базой была включена в его повестку лишь после 1998-2000 гг. В 2004 году в Меркосур была внедрена система обмена информацией по таможенному учету «Индира» (Intercambio de Información de los Registros Aduaneros, INDIRA). Она позволила объединить системы таможенного управления государств-членов, предоставляя консультации по составлению импортной и экспортной документации[565]. Развитие электронной торговли стимулировало создание проекта «Цифровой Меркосур» с целью поддержки цифровой трансформации в государствах и развития цифровой интеграции. В период с 2008 по 2013 г. целью проекта было развитие компетенций и знаний производителей в области применения информационно-коммуникационных технологий при развитии внешней торговли[566]. В рамках цифровой интеграции также был предпринят ряд инициатив, направленных на развитие электронной торговли, в том числе создание единой инфраструктуры распознавания цифровых подписей.

Однако, несмотря на ряд успешных инициатив цифровая интеграция сталкивалась с существенными проблемами, прежде всего, обусловленными неравномерностью доступа к интернету и недостаточным развитием цифровой инфраструктуры в некоторых странах – членах Меркосур.

Темпы роста электронной торговли в рамках Меркосур превышают аналогичные показатели других стран Латинской Америки, таким образом интеграционная структура удерживает цифровое лидерство в Латинской Америке. Так, например, в 2018 г. по сравнению с 2017 г. прирост

[565] Сысоева А. ЕАЭС, Меркосур и интеграция // РСМД 28.01.2019. URL: https://russiancouncil.ru/analytics-and-comments/analytics/eaes-merkosur-i-integratsiya/ (дата обращения 27.11.2025)
[566] Там же.

электронных розничных продаж в регионе составил около 18%[567]. Цифровая трансформация повлияла на способы коммуникации, осуществления сделок купли-продажи и проведения банковских операций, что привело к распространению онлайн-торговли товарами и услугами. Однако большая часть электронной торговли в Меркосур по-прежнему осуществляется на уровне внутренних рынков стран-членов и сталкивается с большими трудностями на пути к переходу к региональным и глобальным рынкам[568]. Серьёзным вызовом также является отсутствие достаточного уровня кибер-безопасности, недостаточный уровень цифровой грамотности населения. Однако, несмотря на асимметрию развития цифровых технологий (наиболее отстающим государством является Парагвай), Меркосур является лидирующей интеграционной структурой в Южной Америке в области цифрового развития.

Особенностью подхода МЕРКОСУР является сочетание попыток унификации стратегий и сохранения права на национальные исключения. Например, Бразилия активно развивает свои национальные облачные платформы и стремится к локализации данных, мотивируя это необходимостью защиты своей промышленной и социальной инфраструктуры. В то же время Аргентина больше сосредоточена на вопросах обеспечения прав граждан в цифровой среде, включая прозрачность алгоритмов и усиление контроля за обработкой персональных данных.

В рамках МЕРКОСУР цифровой суверенитет не сводится лишь к защите информации. Региональные инициативы активно поднимают вопросы о необходимости разработки собственных стандартов цифровой безопасности и создания совместимых платформ для государственных нужд. Это позволяет минимизировать зависимость от внешних

---

[567] Школяр Н. Цифровая трансформация Латинской Америки // РСМД. 21.03. 2022. URL: https://russiancouncil.ru/analytics-and-comments/analytics/tsifrovaya-transformatsiya-latinskoy-ameriki/?sphrase_id=102533716 (дата обращения 27.11.2025)

[568] Там же.

поставщиков технологий, сохраняя конкурентоспособность на глобальном уровне. Однако государства-члены сталкиваются с трудностями в координации таких усилий, поскольку каждая страна имеет собственный уровень технологической зрелости и уникальные потребности.

МЕРКОСУР также основывается на идее региональной солидарности. Вместо того чтобы конкурировать друг с другом, страны блока делают ставку на обмен опытом и совместное обучение. Эта стратегия особенно проявляется в проектах, направленных на развитие цифровой грамотности и поддержку стартапов, создающих локальные технологические решения. Таким образом, МЕРКОСУР стремится не только защитить свои цифровые границы, но и создать условия для устойчивого развития в условиях новой технологической эпохи.

В академической литературе практика цифрового суверенитета в МЕРКОСУР рассматривается с позиций неолониального дискурса[569]. Как показывает деколониальный поворот в изучении данных и технологий, технологии с интенсивным использованием данных особенно актуальны, когда речь идет о поддержании колониальности. По мнению Коулдри и Мехиаса, капитализм и колониализм вступают в новую фазу, отмеченную извлечением жизни людей посредством данных[570]. Как либеральные, так и государственные рыночные общества, такие как США и Китай соответственно, участвуют в колониализме данных. По мнению Паолы Рикаурте, эта форма насильственного извлечения распространяется на другие сферы общественной жизни и насильственно исключает альтернативные способы мышления и бытия, хотя сопротивление оказывается активистскими группами, заставляющими системы данных работать на социальную справедливость[571]. Рассматривая работников

[569] Lehuedé S. An alternative planetary future? Digital sovereignty frameworks and the decolonial option //Big Data & Society. – 2024. – Т. 11. – №. 1. – С. 20539517231221778.
[570] Couldry N, Mejias UA (2019) The Costs of Connection: How Data Is Colonising Human Life and Appropriating It for Capitalism. Stanford, California, USA: Stanford University Press.
[571] Ricaurte P (2019) Data epistemologies, the coloniality of power and resistance. Television & New Media 20(4): 350–365.

данных в Венесуэле, Хулиан Посада утверждает, что компенсация труда, задействованного в работе с данными, представляет собой двойную форму колониальности, охватывающую материальное извлечение и эпистемологическое навязывание[572]. В исследовании управления астрономическими данными в Чили показано, как использование огромных объемов данных может привести к появлению новых форм эпистемического подчинения и вступить в конфликт с традиционными для коренных народов формами отношения к природе[573].

3.2.5. Цифровой суверенитет в повестке Африканского союза

Цифровой суверенитет Африканского союза (АС) стал важным элементом развития континента в эпоху цифровой трансформации. Африка, несмотря на сложные стартовые условия, стремится выстроить свою цифровую инфраструктуру, снизить зависимость от глобальных технологических гигантов и создать условия для устойчивого развития собственного IT-сектора. Эти амбициозные цели сопровождаются множеством вызовов, включая цифровое неравенство между странами, недостаток инвестиций и нехватку квалифицированных кадров. Африка является вторым по масштабу рынком мобильных услуг и техники после Азии. Только государственный сектор рынка по адаптации цифровых технологий в странах Африки южнее Сахары оценивается в десятки млрд. долларов и расценивается как одно из наиболее перспективных направлений для инвестиций, в том числе со стороны компаний США и КНР. Российские ИТ-компании также представлены на африканских рынках.

---

[572] Posada J (2022) The Coloniality of Data Work: Power and Inequality in Outsourced Data Production for Machine Learning. PhD Dissertation, University of Toronto, Canada. Available at: https://tspace.library.utoronto.ca/handle/1807/126388

[573] Lehuedé S (2022) Territories of data: Ontological divergences in the growth of data infrastructure. Tapuya: Latin American Science, Technology and Society 5: 1–18.

Африканский союз (АС) активно продвигает цифровую трансформацию как ключевой элемент социально-экономического развития континента. В рамках стратегии «Повестка дня 2063» союзе стремится создать интегрированное, процветающее и мирное африканское сообщество, где цифровые технологии играют решающую роль в достижении этих целей[574].Однако, несмотря на значительные усилия, Африка сталкивается с серьезными вызовами на пути цифровой трансформации. Среди них ограниченный доступ к электричеству, низкий уровень развития интернет-инфраструктуры и значительный гендерный разрыв в использовании цифровых технологий. Эти проблемы препятствуют развитию цифровой экономики в регионе[575].

Одной из ключевых основ для достижения цифрового суверенитета стала Конвенция АС о кибербезопасности и защите данных (Malabo Convention), принятая еще в 2014 году[576]. Этот документ заложил правовые рамки для регулирования защиты персональных данных и обеспечения конфиденциальности. Конвенция регламентирует деятельность в следующих сферах: проведение электронных транзакций, защита персональных данных, обеспечение кибербезопасности и противодействие киберпреступности. Однако процесс ратификации идет медленно, что подчеркивает сложность внедрения общеконтинентальных норм в условиях значительных различий между странами.

Одновременно с этим Африканский союз сосредоточился на развитии инфраструктуры, инвестируя через такие проекты, как Программа развития инфраструктуры в Африке (PIDA)[577]. Целью стало не

---

[574] Повестка дня Африканского Союза-2063 и перспективы российско-африканского сотрудничества. Сборник научных статей IX Международной научно–практической конференции «Африка в контексте формирования новой системы международных отношений» / Под редакцией А.М. Васильева, Д.А. Дегтерева, А.С. Буторова. Москва: Российский университет дружбы народов 2019.

[575] Там же.

[576] Колесникова М. Обеспечение информационной безопасности в странах Африки: основные детерминанты // Международная жизнь. URL: https://interaffairs.ru/jauthor/material/2690 (дата обращения 27.11.2025)

[577] Там же.

просто расширение доступа к интернету, но и ликвидация цифрового разрыва между городскими и сельскими районами.

Особое место в стратегии АС занимает идея создания единого цифрового рынка, которая нашла отражение в инициативе Стратегия цифровой трансформации Африки 2030 (Digital Transformation Strategy for Africa) (2020–2030)[578]. Этот амбициозный проект предполагает не только гармонизацию законодательства стран-членов в области электронной коммерции, но и координацию усилий в сфере кибербезопасности и повышения цифровой грамотности населения. Акцент сделан на поддержку местных IT-стартапов и развитие локальных технологических решений, что позволяет Африке утверждать свою независимость в цифровой сфере.

Искусственный интеллект также стал важной частью этой трансформации. В 2021 году Африканский союз принял Континентальную стратегию по искусственному интеллекту[579] (AI Continental Strategy for Africa), которая отражает стремление региона использовать ИИ для достижения устойчивого развития. В документе подчеркивается, что технологии должны быть адаптированы к африканским условиям и нести пользу местным сообществам. АС намерен сосредоточиться на создании исследовательских центров ИИ, которые смогут разрабатывать локальные решения в таких областях, как здравоохранение, сельское хозяйство и образование. Например, в сельском хозяйстве ИИ уже помогает оптимизировать процессы выращивания культур с учетом климатических данных, а в здравоохранении – проводить диагностику заболеваний в регионах, где доступ к врачам ограничен[580].

---

[578] Русакова Е.П. Эволюция цифрового судопроизводства в Африке на примере Египта, Кении и ЮАР // Вестник РУДН. Серия юридические науки. 2024. № 2. DOI: https://doi.org/10.22363/2313-2337-2024-28-2-424-435

[579] https://au.int/sites/default/files/documents/44004-doc-EN-_Continental_AI_Strategy_July_2024.pdf

[580] Там же.

Однако на пути реализации этой стратегии стоят серьезные барьеры. Некоторые страны континента все еще испытывают острую нехватку базовой инфраструктуры. Интернет недоступен миллионам африканцев, что ставит под угрозу равенство доступа к цифровым возможностям. Кроме того, цифровая грамотность населения остается на низком уровне, что ограничивает потенциал использования новых технологий. Несмотря на это, такие инициативы, как Альянс «Умная Африка» (Smart Africa Alliance), помогают укреплять международное сотрудничество и привлекать инвестиции для решения этих проблем.

Африканский союз демонстрирует прогресс в направлении своего цифрового суверенитета. Регион делает акцент на развитие собственных решений, которые соответствуют его реалиям. Хотя вызовов остается немало, эта стратегия открывает Африке путь к укреплению ее позиций на глобальной арене и созданию цифрового будущего, где контроль над ключевыми ресурсами будет принадлежать самому континенту.

Вместе с тем, континент оказывается зависимым от внешних технологий. В Африке американские цифровые транснациональные корпорации осуществляют имперский контроль над цифровой архитектурой, а частные инициативы представляются как филантропические, несмотря на их экстрактивный характер.

Вывод по параграфу:

Подводя итог рассмотрению опыта региональных структур необходимо отметить, что современные интеграционные объединения, такие как МЕРКОСУР, ЕС, ЕАЭС и АСЕАН, все чаще делают цифровой суверенитет неотъемлемой частью своей стратегии. Это связано с необходимостью минимизации зависимости от глобальных технологических монополий, укрепления кибербезопасности и защиты персональных данных граждан. Цифровой суверенитет позволяет государствам-членам контролировать критически важную

инфраструктуру, поддерживать устойчивую цифровую экономику и обеспечивать независимость в вопросах цифровой трансформации.

Подходы к цифровому суверенитету зависят от уровня технологического развития объединений. Например, ЕС сделал акцент на разработке и внедрении нормативно-правовых актов, таких как Регламент по защите персональных данных и Закон об ИИ, чтобы защитить данные своих граждан и стимулировать развитие внутреннего цифрового рынка. МЕРКОСУР, в свою очередь, сосредоточен на ликвидации цифрового неравенства внутри блока, развитии трансграничной электронной торговли и продвижении собственных инициатив в области кибербезопасности[581].

Основной вызов для интеграционных объединений в достижении цифрового суверенитета – это цифровой разрыв и неравномерность в доступе и уровне развития цифровых технологий. Например, страны МЕРКОСУР сталкиваются с неравномерным развитием инфраструктуры, что препятствует созданию единого цифрового рынка.

В осложненных геополитических условиях интеграционные объединения стремятся к укреплению цифрового суверенитета через трансрегионализм. Например, сотрудничество МЕРКОСУР с ЕС в рамках программы eLAC позволило региону получить доступ к передовым технологиям и экспертным знаниям, несмотря на риск зависимости от внешних акторов[582]. Однако для достижения суверенитета требуется увеличение инвестиций в локальные разработки и укрепление координации внутри объединений.

Интеграционные объединения обладают значительным потенциалом для укрепления цифрового суверенитета через развитие локальных технологических решений, гармонизацию законодательств и координацию цифровых стратегий на глобальных форумах. Современные тренды,

[581] Decisiones del Consejo del Mercado Común, MERCOSUR/CMC/DEC. N° 19/17
[582] eLAC Action Plan, 2018-2020

включая трансрегионализм, открывают новые возможности для обмена опытом между блоками, такими как МЕРКОСУР и ЕАЭС, что способствует созданию глобального цифрового пространства, основанного на принципах суверенитета и устойчивости.

3.3. Цифровой суверенитет в практике ведущих государств

3.3.1. Цифровой суверенитет КНР

Особенности внешней политики Китая во многом определяются приверженностью пяти принципам мирного сосуществования, сформулированным в 1954 году. Эти принципы – взаимное уважение суверенитета и территориальной целостности, взаимное ненападение, невмешательство во внутренние дела, равенство и взаимная выгода, а также мирное сосуществование – стали основой китайского подхода к международным отношениям[583].

Китайское руководство рассматривает суверенитет как фундаментальный элемент международного порядка. Это проявляется в его настойчивой позиции по вопросам территориальной целостности, включая Тайвань, Тибет и Синьцзян. Принцип невмешательства, в свою очередь, стал ключевым в отношениях с развивающимися странами, особенно в Африке и Латинской Америке, где Китай избегает критики внутренней политики своих партнеров, концентрируясь на экономическом сотрудничестве.

Принцип равенства и взаимной выгоды на практике отражается в стремлении Китая создавать взаимовыгодные экономические и торговые связи. Таким образом, пять принципов мирного сосуществования остаются

[583] В Пекине прошло торжественное собрание по случаю 70-летия провозглашения «Пяти принципов мирного сосуществования» // Посольство КНР в России. 28.06.2024 URL: http://ru.china-embassy.gov.cn/rus/zgxw/202406/t20240630_11444664.htm#:~:text=В%20тот%20момент%20китайское%20руководство,и%20взаимная%20выгода%2С%20мирное%20сосуществование. (дата обращения 27.11.2025)

краеугольным камнем китайской внешней политики, определяя её подход к взаимодействию с миром, в том числе и в цифровых международных отношениях. При этом их реализация отражает как традиционные ценности Китая, так и прагматические интересы современного государства, стремящегося укрепить своё влияние на глобальной арене.

Инициатива «Один пояс, один путь» (Belt and Road Initiative, BRI) – стратегическая инициатива, направленная на укрепление экономического и инфраструктурного сотрудничества с другими странами через создание новых торговых путей и инвестиционных проектов, что также отражает внешнеполитические цели КНР.

Инициатива «Один пояс – один путь», задуманная как проект объединения стран через инфраструктурные сети, давно вышла за пределы физических дорог и портов. Сегодня она включает в себя развитие цифрового измерения – так называемого «цифрового шелкового пути». Этот проект охватывает телекоммуникации, спутниковую связь, искусственный интеллект и другие современные технологии. Китай видит в этом не только возможность модернизации экономики, но и способ укрепить свои позиции на мировой арене. Как отмечает Лю Ижу «Китайская цифровая экосистема включает уникальные технологические разработки Китая («Интернет +», «Золотой щит» и др.), которые одновременно выступают основой создания китайских цифровых стандартов. Эффективное продвижение «Цифрового Шелкового пути» в сторону глобальной цифровой экосистемы возможно за счет постоянного совершенствования механизма внешней экспансии, для которого предложена и охарактеризована совокупность практических инструментов: опыта применения технологий (искусственного интеллекта, блокчейна, «умного города» и пр.), стратегий экспансии цифровых стандартов, платформ для экспансии (торговых площадок, систем мобильных платежей и пр.), стратегий торговой экспансии на основе моделей маркетплейсов и маркетспейсов. Темпы цифровизации

национальной экономики и стратегии «Цифрового Шелкового пути» в совокупности позволяют Китаю обоснованно претендовать на ведущую роль в формировании глобального цифрового будущего»[584].

Одним из ключевых направлений цифрового развития КНР стало строительство телекоммуникационных сетей. Китайские компании, такие как Huawei и ZTE, активно прокладывают оптоволоконные кабели и развивают сети 5G в странах Азии, Африки и Европы.

Китай активно продвигает свою спутниковую систему BeiDou. Она уже конкурирует с GPS и используется в логистике, сельском хозяйстве и транспорте. Успех BeiDou в странах, участвующих в инициативе, усиливает влияние Пекина в ключевых секторах экономики.

Значительное внимание уделяется и цифровизации торговли. Компании вроде Alibaba помогают создавать платформы электронной коммерции, что ускоряет процессы импорта и экспорта. Появляются технологические хабы, исследовательские центры, технопарки.

Многие страны коллективного Запада, в особенности США, настороженно относятся к такой экспансии Китая, обвиняя в кибершпионаже и политическом влиянии.

Инициатива «Один пояс – один путь» - символ цифровой эпохи, где технологии становятся инструментом глобального влияния. Китай прокладывает не только новые маршруты, но и новые стандарты взаимодействия, основанного на уважении государственного суверенитета.

Китай стал государством-первопроходцем в области суверенного развития цифровых технологий. Концепцию суверенного Интернета выдвинул Фан Биньсин, известный как «отец китайского файрвола», выступая в 2011 году на Международном симпозиуме по информационной безопасности в Чанше. В основе идей интернет-суверенитета лежат четыре

[584] Лю Ижу «Цифровой Шелковый путь» как инновационная основа глобального проекта «Один пояс, один путь» // Инновации и инвестиции. 20207 № 12. С. 278 – 282.

принципа: каждая страна должна обладать полным контролем над своим сегментом Интернета; государство должно иметь возможность защищать свой сегмент Интернета от любых внешних атак; все страны должны иметь равные права на использование ресурсов в Интернете; другие страны не должны контролировать корневые DNS-серверы, через которые осуществляется доступ к национальному сегменту Интернета[585].

Подход Китая к обеспечению цифрового суверенитета исходит из того, что цифровые технологии и Интернет представляют собой значимые элементы, необходимые для достижения геополитического лидерства. Следствием этого является внимание к государственной поддержке цифровой отрасли, направленной на обеспечение технологического лидерства, и защита безопасности данных как ключевого ресурса современной цифровой экономики.

Особенности модели развития КНР заключаются в том, что, имея все собственные аналоги привычных в остальном мире ИТ-гигантов, таких как «Google», «WhatsApp», «Wikipedia», «Quora», «Youtube» и т. д., «китайский Интернет» смог развиваться внутри цифровых границ государства.

В последние годы Китай продемонстрировал готовность защищать суверенитет в области данных, которые рассматриваются как ключевой ресурс цифровой экономики. В декабре 2017 года Китай выпустил документ «Реализация национальной стратегии Больших данных и ускорения строительства цифрового Китая»[586], который регламентирует вопросы цифрового суверенитета на национальном уровне. В Китае в 2021 году был принят Закон КНР «О безопасности данных»[587] и Закон КНР «Об охране личных данных пользователей»[588]. Согласно этим законам, данные

[585] Денисов, И.Е. Китайская стратегия «больших данных»: реформа управления, инновации и глобальная конкуренция. М.: Издательство «МГИМО-Университет», 2023. 28 с.
[586] Там же
[587] Там же
[588] Там же

рассматриваются как национальное достояние, очередной фактор производства наряду с трудом, землей, капиталом и технологиями.

Внешнеполитические приоритеты КНР в отношении цифровой среды отражены в Глобальной инициативе в области безопасности данных, опубликованной МИД КНР в 2020 году, согласно которой «государства должны уважать суверенитет, юрисдикцию и управление в области данных со стороны других государств». Как отмечает научный сотрудник ИМИ И.Е. Денисов, правительство Китая прилагает значительные усилия для разработки и внедрения комплексных мер по обеспечению безопасности инфраструктуры данных, и эту политику можно в полной мере назвать суверенизацией данных[589].

Нужно отметить, что быстрый рост технологических компаний КНР способствовал вниманию к проблемам обеспечения технологического и цифрового суверенитета со стороны США. Первоначально США, будучи страной, которая разработала Интернет и способствовала его распространению в мире, активно поддерживали видение глобального цифрового пространства, свободного от государственных границ, а стремление государств к обеспечению информационного суверенитета приравнивали к актам цензуры. Показательным с этой точки зрения является «Международная стратегия для киберпространства» 2011 года[590], в которой термин «суверенитет» не упоминается, но делается акцент на свободный характер Интернета и недопустимость усиления государственного контроля в данной области.

Китай реализует строгий контроль над интернетом через «Великий китайский файрвол», блокируя доступ к иностранным веб-сайтам и приложениям, которые не соответствуют требованиям правительства.

---

[589] Global Initiative on Data Security. MFA of CPR. URL: https://documents.unoda.org/wp-content/uploads/2022/03/Position-paper-Global-Initiative-on-Data-Security-submitted-by-China.pdf (дата обращения 27.11.2025)

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

Контент в интернете жестко регулируется, а компании обязаны соблюдать строгие правила цензуры и хранения данных[591].

Цифровой суверенитет Китая основывается на принципах самообеспечения, защиты национальной безопасности и продвижения китайских технологий и стандартов на глобальном уровне. Эта стратегия помогает Китаю сохранять контроль над своей цифровой экосистемой и укреплять свои позиции в мировой экономике.

3.3.2. Цифровой суверенитет США

Именно США стояли у истоков рассмотрения цифровых технологий как пространства вне суверенитета. Продвигаемая правительствами США на форумах по управлению интернетом, таких как Международный союз электросвязи, эта парадигма господствовала в девяностых годах и была связана с идеей о том, что протоколы и архитектура интернета делают эту сеть непроницаемой для внешнего регулирования, а государственный суверенитет не распространяется на пространство Интернета.

Однако впоследствии данная парадигма была поставлена под сомнение, а затем доказала свою несостоятельность. Знаковым событием в этом отношении стали разоблачения Сноудена, которые обнажили сложную систему массового и целенаправленного наблюдения, осуществляемого американскими спецслужбами и компаниями. Параллельно с этим ранее децентрализованный интернет начал все больше концентрироваться в руках горстки технологических компаний, базирующихся в США. После этих событий и тенденций неудивительно, что либертарианская парадигма цифрового управления начала терять свою привлекательность, поскольку, как казалось, она приносила пользу в основном США. Сегодня же США сталкиваясь с растущей угрозой своему

---

[591] International strategy for cyberspace. White House, 2011. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (дата обращения 27.11.2025)

цифровому лидерству со стороны КНР также все более активно внедряют практику цифрового суверенитета, сохраняя на уровне риторике приверженность трансграничности цифрового пространства.

Ключевые приоритеты современной цифровой политики США представлены в основополагающих документах стратегического планирования, среди которых особое место занимает Стратегия национальной безопасности США (National Security Strategy, NSS) – основной документ, который определяет ключевые угрозы, цели и приоритеты внешней политики и национальной безопасности США. Стратегия национальной безопасности публикуется Администрацией президента и обновляется каждые несколько лет, отражая изменения в международной обстановке и внутренние приоритеты. В Стратегии национальной безопасности США 2022 года развитие цифровых технологий и обеспечение кибер-безопасности рассматривается как важный аспект национальной безопасности и экономического процветания[592]. США стремятся защитить свой суверенитет путем укрепления кибербезопасности, защиты критических технологий и продвижения принципов свободного и открытого интернета.

Документ подчеркивает важность международного лидерства США в укреплении глобального порядка, основанного на правилах. США стремятся формировать международные правила и нормы, в том числе в области технологий и киберпространства, чтобы обеспечить безопасность в условиях глобальной конкуренции, особенно с Китаем и Россией.

Национальная киберстратегия США 2018 (National Cyber Strategy) – направлена на защиту цифрового суверенитета США, предотвращение кибератак и обеспечение безопасности критической инфраструктуры[593]. США активно инвестируют в развитие кибербезопасности, защиту государственных сетей, а также в усиление оборонительных и

[592] National Security Strategy 2022. USA, White House
[593] National Cyber Strategy, USA, Ministry of Defense, 2018

наступательных кибероперациий через специализированные структуры, такие как Киберкомандование США (USCYBERCOM).

США работают над ограничением влияния иностранных технологий на свою инфраструктуру. Примером является запрет на использование оборудования китайских компаний, таких как Huawei и ZTE, в американских сетях 5G, что объясняется опасениями относительно национальной безопасности.

США поддерживают свои крупные технологические компании (Google, Apple, Microsoft, Amazon и другие). США продвигают свои стандарты в международной торговле, стремясь защитить свои компании и технологии. Защита интеллектуальной собственности является ключевым элементом этой стратегии, и США активно борются с кражей технологий и данных. Контроль экспорта технологических решений направлен на предотвращение попадания американских технологий в руки потенциальных противников. Как отмечается в Стратегии национальной безопасности США от 2022 года, «многие из союзников и партнеров США, особенно в Индо-Тихоокеанском регионе, находятся на передовой линии принуждения КНР и справедливо настроены стремиться к обеспечению собственной автономии, безопасности и процветания. Мы поддержим их способность принимать суверенные решения в соответствии с их интересами и ценностями, без внешнего давления, и будем работать над предоставлением высококачественных и масштабных инвестиций, помощи в развитии и рынков»[594].

Цифровой суверенитет США сосредоточен на сохранении и укреплении своего доминирующего положения в мировой цифровой экосистеме, защите своих данных и технологий, а также на формировании глобальных правил цифровой торговли и взаимодействия.

---

[594] USA National Security Strategy. 2022. URL: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf (дата обращения 27.11.2025)

Особенность подхода США заключается в делегировании значительных полномочий и задач в области безопасности и управления данными частному сектору. В том числе американские ИТ-компании при поддержке Госдепа выступают с международными инициативами в области кибербезопасности, такими как «Женевские киберконвенции»[595], предложенные «Майкрософт» для государств, и «Крайстчерчский призыв»[596], ориентированный на сотрудничество ИТ-платформ на международном уровне для противодействия кибертерроризму.

При этом на уровне риторики подчеркивается нецелесообразность активного государственного участия в цифровой сфере, в том числе в контексте обеспечения цифрового суверенитета.

Однако США готовы принимать меры в области защиты цифрового сектора экономики на государственном уровне. При администрации Д.Трампа в ответ на широкое присутствие социальных сетей и технологических компаний из КНР в США было принято решение в 2020 году запретить жителям США «вести дела» с приложением «TikTok» и мессенджером «WeChat» под предлогом защиты технологического суверенитета страны. В США также запретили продажу телеком-оборудования «Huawei», «ZTE» и еще трех китайских компаний под предлогом защиты национальной безопасности страны. Кроме того, США стали оказывать давление на партнеров с тем, чтобы они отказались от использования технологии 5G «Huawei»[597].

В настоящее время в США сложился новый подход к управлению глобальным информационным пространством, согласно которому в растущей конкуренции со стороны высокотехнологичных компаний КНР, а также фрагментированной цифровой реальности необходимо

---

[595] «Женевская конвенция» для киберпространства. 2017. URL: https://tcinet.ru/press-centre/technology-news/4728/ (дата обращения 27.11.2025)

[596] https://www.christchurchcall.org (дата обращения 27.11.2025)

[597] США стали оказывать давление на партнеров с тем, чтобы они отказались от использования технологии 5G «Huawei» // ТАСС, 28 сентября 2020. URL: https://tass.ru/ekonomika/9571633 (дата обращения 27.11.2025)

придерживаться норм и правил только в отношении дружественных государств, при этом вести максимально жесткую позицию в отношении соперников и конкурентов. США во все большей степени ориентируются на односторонние меры, в том числе меры сдерживания и демонстрации силы в цифровой сфере, а нормы «порядка, основанного на правилах» для цифровой сферы распространяют лишь на союзников. Данный подход нашел отражение в Декларации о будущем Интернета 2022 года, к которой присоединилось около 60 государств[598]. Согласно декларации, действия России и КНР в глобальном информационном пространстве представляют собой угрозу для безопасности США и киберпространства в целом. Показательно, что и в этом документе также не употребляется термин «суверенитет». Это может объясняться в том числе желанием распространить нормы и практики внутренней политики США на своих союзников.

При этом нельзя не отметить, что среди союзников США нет единства во взглядах на проблематику цифрового суверенитета. Так, в последние годы Евросоюз все более активно продвигает идею цифрового суверенитета ЕС на уровне региона. Во многом это является ответом на растущую зависимость ЕС от американских ИТ-гигантов и невысокие показатели европейского сектора цифровой экономики. В частности, в 2024 году представитель ЕС по технологическому суверинетету высказался в пользу ограничения присутствия социальной сети X на территории стран ЕС[599].

3.3.3. Цифровой суверенитет Российской Федерации

Согласно Конституции России, суверенитет Российской Федерации распространяется на всю её территорию, суверенитет проявляется в

[598] Declaration for the Future of the Internet. USA, 2020. URL: https://www.state.gov/declaration-for-the-future-of-the-internet (дата обращения 27.11.2025)

[599] Elon Musk faces potential personal hit in EU X probe // Euronews, 18.10.2024. URL: https://www.euronews.com/next/2024/10/18/e (дата обращения 27.11.2025)

верховенстве государственной власти, её единстве и независимости, также суверенитет подразумевает обеспечение целостность и неприкосновенность территории Российской Федерации.

Носителем суверенитета и единственным источником власти в Российской Федерации является её многонациональный народ. Народ осуществляет свою власть непосредственно, а также через органы государственной власти и органы местного самоуправления. Высшим непосредственным выражением власти народа являются референдум и свободные выборы.

Декларация о государственном суверенитете России была принята 12 июня 1990 года народными депутатами[600]. Суть принципа государственного суверенитета, закрепленного статье 4 Конституции РФ, состоит в верховенстве и единстве государственной власти и распространении её на всю территорию Россию. Этот принцип означает обязательность исполнения законодательных актов федеральных органов власти для всех субъектов права на территории Российской Федерации, иными словами устанавливается Верховенство центральной (федеральной) власти по отношению к власти субъектов федерации[6].

Правовым выражением верховенства суверенитета Российской Федерации является верховенство Конституции РФ и федеральных законов на всей территории РФ. Конституция обязательна для исполнения всеми субъектами права на территории России, она обладает высшей юридической силой по отношению к федеральным законам, законам субъектов федерации и любым подзаконным актам органов государственной власти[1].

Президент России, будучи главой государства, наделяется Основным Законом страны полномочиями «по охране суверенитета

---

[600] Декларация о государственном суверенитете РСФСР. от 12 июня 1990 г. № 22-1. URL: http://ips.pravo.gov.ru/?docbody=&prevDoc=102063718&backlink=1&&nd=102629766 (дата обращения 27.11.2025)

Российской Федерации, её независимости и государственной целостности» (статья 80 Конституции РФ). Вступая в должность, в своей торжественной присяге Президент РФ клянется «защищать суверенитет и независимость, безопасность и целостность государства»[601].

В Концепции внешней политики от 2023 России подход к государственному суверенитету характеризуется как принципиальный и незыблемый элемент международных отношений. Россия подчеркивает важность уважения суверенитета и территориальной целостности всех государств, а также невмешательства во внутренние дела других стран. Этот подход основан на ключевых нормах международного права, включая Устав ООН[602].

Россия считает, что каждый народ имеет право самостоятельно определять свою внешнюю и внутреннюю политику без внешнего давления или вмешательства. В рамках своей внешней политики Россия активно выступает против односторонних санкций, принуждения или действий, подрывающих суверенитет других государств. Таким образом, защита и укрепление государственного суверенитета рассматриваются как центральные элементы стабильности и безопасности в мире.

Цифровой суверенитет России представляет собой стратегию по обеспечению независимости и контроля над цифровыми ресурсами, инфраструктурой и данными в условиях растущей глобальной цифровизации и геополитической напряженности. Можно выделить элементы внутреннего и внешнего цифрового суверенитета России. К внешнему контуру цифрового суверенитета относятся инициативы России в рамках ООН, других глобальных и региональных структур, направленные на закрепление суверенитета как нормы права в цифровом пространстве. Кроме того, особое место в данной области занимают двусторонние отношения. 25 сентября 2020 г. президент России В. Путин

[601] Конституция Российской Федерации. 1992
[602] Концепция внешней политики Российской Федерации. Утв. Указом Президента. 13.03.2023

выступил с инициативой по нормализации российско-американских отношений в киберпространстве, которая в том числе, предполагает обмен «гарантиями невмешательства во внутренние дела, включая избирательные процессы, с использованием ИКТ и высокотехнологичных методов». Данная инициатива была обусловлена, среди прочего, растущим числом обвинений со стороны различных политических сил США о вмешательстве России в выборы в США в 2020 г. Причем Россия саму возможность такого вмешательства отрицает. Американская сторона эту инициативу отвергла, выдвинув новые обвинения в адрес Москвы по вмешательству во внутренние дела не только США, но и ряда других стран[603].

Россия развивает свою национальную цифровую инфраструктуру, включая создание независимой от глобального интернета сети. В 2019 году был принят закон о «суверенном интернете», который позволяет стране изолироваться от глобальной сети в случае угроз. Это обеспечивает возможность контролировать интернет-трафик внутри России и защитить его от внешнего вмешательства[604]. Усиление мер кибербезопасности является приоритетом для России. Создаются национальные системы мониторинга и защиты, а также повышаются требования к кибербезопасности государственных и частных организаций. Власти внедряют стратегии по защите критически важных объектов, таких как энергетика, транспорт и связь, от кибератак.

Россия активно развивает свои собственные технологические компании и платформы, такие как поисковик Яндекс, социальные сети ВКонтакте и Одноклассники, платежные системы Мир и облачные сервисы. Эти компании получают поддержку от государства в виде

---

[603] Зиновьева Е.С. Проблема «цифрового вмешательства» в российско-американских отношениях // РСМД. 23.10.2020. URL: https://mgimo.ru/about/news/experts/problema-tsifrovogo-vmeshatelstva-v-rossiysko-amerikanskikh-otnosheniyakh/?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (дата обращения 27.11.2025)

[604] http://publication.pravo.gov.ru/Document/View/0001201905010025?index=0&rangeSize=1 (дата обращения 27.11.2025)

налоговых льгот, грантов и субсидий, что способствует снижению зависимости от иностранных технологий. Россия стремится развивать собственное программное обеспечение и производить оборудование, включая операционные системы, системы управления базами данных и серверное оборудование. Программа импортозамещения направлена на то, чтобы заменить иностранные технологии российскими аналогами, особенно в государственных и стратегических секторах. В России принимаются законы, обязывающие иностранные IT-компании соблюдать местные правила, включая требования по локализации данных, удалению запрещенного контента и открытию представительств в стране. Законодательство направлено на усиление контроля над деятельностью глобальных технологических гигантов на российском рынке. Россия разрабатывает национальные стандарты и системы сертификации цифровых технологий и оборудования. Это позволяет контролировать качество и безопасность используемых в стране технологий, а также снижает риски, связанные с использованием иностранных решений. В условиях санкционного давления Россия развивает суверенные финансовые и платежные системы, такие как национальная платежная система «Мир» и альтернативные решения для межбанковских расчетов, в том числе продвигает новые и поддерживает существующие инициативы на уровне БРИКС и БРИКС +, с целью снизить зависимость от западных финансовых институтов и систем.

Цифровой суверенитет России направлен на обеспечение технологической независимости, защиту данных и цифровой инфраструктуры, а также на снижение зависимости от зарубежных технологий в условиях политических и экономических вызовов. В России сегодня взят курс на обеспечение цифрового суверенитета и укрепление технологической независимости страны.

Вывод по параграфу:

Практика обеспечения цифрового суверенитета в ведущих государствах – Китае, США и России – демонстрирует различные подходы, отражающие их уникальные политические, экономические и стратегические приоритеты. Китай активно развивает концепцию «суверенитета данных», основанную на строгом контроле над внутренними информационными потоками, создании национальных технологий и инфраструктуры, а также ограничении влияния иностранных компаний на цифровую среду. Это позволяет стране укреплять внутреннюю стабильность, защищать свои интересы и проецировать технологическую мощь на международной арене.

США, напротив, делают акцент на продвижении открытого цифрового пространства, одновременно усиливая свои позиции в глобальном технологическом секторе. Через доминирующие платформенные компании, такие как Google, Amazon и Microsoft, США формируют правила цифрового взаимодействия, продвигая свои нормативы и стандарты как универсальные. При этом политика США в области кибербезопасности направлена на защиту критически важной инфраструктуры и контроль за трансграничными потоками данных, что часто вызывает напряженность в отношениях с другими странами.

Россия стремится укрепить цифровой суверенитет через разработку национальных технологий, защиту своего информационного пространства и формирование независимой инфраструктуры. Государственная политика акцентирует внимание на локализации данных, развитии отечественных платформ и борьбе с внешними киберугрозами. При этом Россия активно участвует в международных инициативах, продвигая идею равноправного участия всех стран в управлении глобальным цифровым пространством.

Таким образом, подходы Китая, США и России к цифровому суверенитету отражают их различные геополитические цели и внутренние приоритеты. Эти стратегии формируют многоуровневую и конкурентную структуру глобального цифрового управления, где каждая из стран

стремится максимально защитить свои интересы, одновременно влияя на правила и нормы в мировой цифровой среде.

Вывод по главе:

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 переосмысления 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.

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.

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.

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

Настоящее исследование было посвящено комплексному анализу феномена государственного суверенитета в условиях глобальной цифровой трансформации. Основной целью работы стало выявление проблем, связанных с обеспечением цифрового суверенитета, а также осмысление их в теоретической и практической перспективе. Проведённый анализ позволил сформулировать ключевые выводы, которые тесно связаны с каждой из глав работы. В первой главе была рассмотрена эволюция понятия государственного суверенитета и его адаптация к меняющимся историческим условиям, что позволило выявить основополагающие концептуальные сдвиги. Во второй главе акцент сделан на воздействии цифровой революции на суверенитет, где технологии искусственного интеллекта и больших данных формируют новые вызовы и возможности. В третьей главе исследованы практические аспекты цифрового суверенитета через анализ политик ведущих держав, что позволило показать разнообразие подходов и общую тенденцию к укреплению национального контроля над цифровыми ресурсами.

В первой главе работы рассмотрены теоретико-методологические основания анализа государственного суверенитета. Особое внимание уделено исторической эволюции этой категории, начиная с античных представлений о власти, через Вестфальский мир, концепцию народного суверенитета и до современных подходов, включая реализм, либерализм и конструктивизм. Эволюция суверенитета отражает изменения в международных и внутригосударственных отношениях: от монархического абсолютизма к народному суверенитету и далее – к глобализованным формам власти, в которых государственные границы перестают быть абсолютным критерием суверенитета. Показано, что суверенитет остаётся ключевой категорией международных отношений, хотя его содержание и формы изменяются под воздействием глобальных

изменений. Особо выделен вклад теории социального конструктивизма, которая подчёркивает, что суверенитет является не статичной характеристикой, а социально сконструированным понятием, отражающим доминирующие нормы и представления своего времени. К числу таких изменений можно отнести сдвиг от абсолютного монархического суверенитета к народному суверенитету, сформированному идеями Просвещения, а также усиление роли международных норм и институтов в XX веке, что подчёркивает важность глобальных взаимозависимостей. В цифровую эпоху доминирующие нормы также изменяются, включая признание данных и цифровых технологий как ключевых ресурсов власти, что требует переосмысления роли государства в управлении этими процессами. Современные вызовы, включая глобализацию и цифровую трансформацию, ставят под сомнение традиционные трактовки суверенитета, что требует их пересмотра и адаптации.

Вторая глава была посвящена анализу влияния цифровой революции на мировую политику. Исследование показало, что такие технологии, как искусственный интеллект, большие данные, блокчейн и Интернет вещей, создают качественно новые вызовы и возможности для государств. Цифровая среда становится ареной для новых форм взаимодействия и конфликта, где традиционные представления о границах и власти размываются. Например, использование транснациональными корпорациями больших данных и алгоритмов искусственного интеллекта позволяет им влиять на общественное мнение и политические процессы в разных странах, что ставит под сомнение суверенитет государств над своей внутренней политической повесткой. Кибератаки, проводимые с территории одного государства и поражающие критическую инфраструктуру другого, являются ещё одним примером того, как цифровая среда устраняет географические границы и меняет традиционные подходы к защите суверенитета. В то же время,

секьюритизация цифрового пространства усиливается, так как государства стремятся минимизировать угрозы, связанные с кибератаками, трансграничными потоками данных и доминированием транснациональных корпораций. Особое внимание уделено концепции цифрового суверенитета, которая становится центральным элементом политики таких государств, как США, ЕС, Китай и Россия. Исследование подтвердило гипотезу о том, что цифровая трансформация не только усиливает конкуренцию между государствами, но и требует международной координации для выработки общих правил.

Третья глава сосредоточена на практических аспектах обеспечения цифрового суверенитета. Примеры политик США, ЕС, Китая и России демонстрируют различные подходы к этой проблеме. Так, США делают упор на доминировании своих технологий и экстерриториальности законодательства, тогда как ЕС стремится защитить права граждан и создать нормативную базу, ограничивающую влияние глобальных корпораций. Китай, напротив, активно развивает собственную цифровую инфраструктуру и концепцию «суверенитета данных», тогда как Россия акцентирует внимание на национальной безопасности и защите критической информационной инфраструктуры. Работа выявила, что хотя подходы государств различаются, все они стремятся усилить контроль над цифровыми ресурсами, что подтверждает гипотезу о глобальном характере этого процесса. Например, США используют закон CLOUD Act для получения доступа к данным, хранящимся за пределами их юрисдикции, что подчёркивает их стремление к экстерриториальному регулированию. ЕС, в свою очередь, внедрил Общий регламент по защите данных (GDPR), который распространяет свои нормы на компании, работающие с данными граждан ЕС независимо от их местонахождения. Китай активно развивает собственные технологии и инфраструктуру, продвигая концепцию «суверенитета данных», что позволяет ему минимизировать зависимость от иностранных поставщиков. Россия фокусируется на защите

критической инфраструктуры и разработке национальных платформ для хранения и обработки данных, что подчёркивает её стремление к цифровой автономии. Кроме того, роль международных организаций и региональных структур, таких как ООН и ЕС, становится всё более значимой в выработке глобальных норм цифровой среды.

Анализ позволяет сделать вывод, что в условиях цифровой революции суверенитет перестаёт быть исключительно территориальной категорией. Он трансформируется в многомерное понятие, включающее контроль над данными, киберпространством и цифровой инфраструктурой. Государства сталкиваются с необходимостью сочетания национальных интересов с международной координацией, что создаёт новые дилеммы для мировой политики. В то же время, цифровая трансформация открывает возможности для усиления роли государств в глобальном управлении.

Перспективы дальнейших исследований данной темы многочисленны. Особое внимание следует уделить влиянию технологий искусственного интеллекта, которые, с одной стороны, усиливают потенциал для развития национальных экономик и управления, а с другой – создают новые угрозы для безопасности и приватности. Искусственный интеллект может стать инструментом для обеспечения суверенитета, но также и фактором международной конфликтности, так как он усиливает асимметрию между государствами, обладающими передовыми технологиями, и теми, кто вынужден их заимствовать.

Эволюция суверенитета продолжает демонстрировать свою адаптивность в условиях меняющегося мира. Современная трактовка включает в себя множество аспектов, начиная от внутреннего контроля над территориями и населением до признания в международном сообществе. Однако, в цифровую эпоху традиционные подходы подвергаются серьёзным испытаниям. Данные становятся новым ресурсом, равнозначным природным богатствам, а их контроль – важнейшим

элементом государственного суверенитета. Традиционные представления о суверенитете, базирующиеся на территориальной власти, трансформируются, так как управление данными не ограничивается национальными границами. Контроль над данными позволяет государствам не только обеспечивать безопасность, но и влиять на экономическое развитие, политические процессы и информационное поле. Например, государства, обладающие мощной цифровой инфраструктурой, могут эффективно защищать свои интересы, тогда как страны, зависимые от иностранных технологий, теряют значительную часть своей автономии в глобальной системе. Кроме того, усиление цифровой зависимости приводит к пересмотру подходов к экономическому и технологическому суверенитету, формируя новые международные конфликты и альянсы.

Кроме того, нарастающая международная конфликтность, связанная с конкуренцией за технологическое лидерство, требует глубокого анализа. В условиях геополитической напряжённости цифровая среда становится ареной для гибридных конфликтов, включающих кибератаки, информационные войны и манипуляции общественным мнением. Исследование взаимодействия технологий и политики в таких условиях представляет собой важное направление для дальнейшего изучения.

Таким образом, цифровой суверенитет – это современная концепция, отражающая право и способность государства или организации контролировать свою цифровую инфраструктуру, данные и информационные потоки без зависимости от внешнего влияния. Он включает технические, политические и экономические аспекты, такие как: контроль над данными (хранение и обработка в национальных дата-центрах); разработка национального ПО и аппаратного и сетевого оборудования (например, российские ОС Astra Linux, платформа «ГосТех»); защита от кибератак и внешнего вмешательства (например, через законы о локализации данных, международное сотрудничество, продвижение инициатив в области информационной безопасности в ООН).

Отличия от классического суверенитета, сформулированного в работы Жана Бодена, Гуго Гроция, Томаса Гоббса коренятся в различиях в объекте контроля - классический суверенитет (XVI–XVII вв.) фокусировался на территориальной верховной власти государства (Боден), монополии на легитимное насилие (Вебер) и независимости в международных отношениях (Гроций), цифровой же суверенитет охватывает виртуальное пространство: данные, интернет-инфраструктуру, программное обеспечение, что усложняется отсутствием четких границ и трансграничной природой цифровых технологий. Классические теории предполагали физический контроль границ и территорий, а цифровой суверенитет сталкивается с транснациональными корпорациями (Google, Microsoft) и глобальными сетями, которые сложно регулировать .

Традиционный суверенитет опирался на армию, законы и дипломатию, в то время как цифровой требует технологической автономии (собственные ЦОД, криптография) и международной кооперации (например, альянсы в рамках БРИКС). Кроме того, классические теории не учитывали культурный суверенитет, который сегодня включает защиту от информационного доминирования (например, через регулирование соцсетей).

Таким образом, настоящее исследование не только подтверждает актуальность темы цифрового суверенитета, но и подчёркивает необходимость её дальнейшего изучения в контексте глобальных изменений. Предложенные выводы и рекомендации могут быть полезны как для академического сообщества, так и для разработчиков национальных и международных стратегий в области цифрового управления и безопасности.

Категория цифрового суверенитета носит сложный, многокомпонентный характер и ее наполнение в академической литературе и в практике международных отношений в значительной степени зависит от национальных интересов, особенностей

государственной политики и политической культуры, внешнеполитических ориентиров и приоритетов государства. При этом она эволюционирует вместе с развитием международной системы и научно-техническим прогрессом.

В последние годы в условиях масштабной перестройки международной системы наметилась тенденция к нарастающей напряженности между ведущими игроками в глобальном информационном пространстве. Фрагментация интернет-пространства при наличии различных подходов к управлению цифровыми технологиями и обеспечению безопасности в данной сфере порождает цифровую неопределенность, которая прежде всего выгодна США как наиболее сильному игроку в глобальном информационном пространстве. Однако неопределенность, как правило, чревата конфликтностью и угрозой непреднамеренной эскалации, особенно принимая во внимание растущую милитаризацию информационного пространства.

В этих условиях очень востребованными являются нормы и правила поведения государств в глобальном информационном пространстве, опирающихся на основополагающие нормы и принципы международного права, такие как невмешательство во внутренние дела, уважение государственного суверенитета, недопущение использования силы и угрозы силой в международных отношениях. Как в 1648 году, когда был подписан Вестфальский мир, категория суверенитета стала важнейшим общим знаменателем, снявшим неопределенность в отношениях между церковью и государствами, так и на современном этапе категория цифрового суверенитета в международном праве способна очертить «красные линии» и стабилизировать отношения в данной области.

Цифровые технологии трансграничны, но в политической сфере мир разбит на суверенные государства. Важным условием для развития диалога по цифровой проблематике являются взаимное уважение и признание его субъектов, в первую очередь суверенных государств. В этих

условиях суверенитет может выступить в роли общего знаменателя, необходимого для дальнейшего развития международного сотрудничества в сфере обеспечения информационной безопасности при уважении интересов всех государств.

Таким образом под суверенитетом в данном исследовании подразумевается политическое состояние государства на определенной территории, имеющего признанные полномочия вести свои внутренние дела без вмешательства извне, проводить независимую внешнюю политику и контролировать взаимодействие в пределах своих границ, участвуя при этом в выгодных для себя случаях в международных механизмах. Суверенитет обладает такими характеристиками как гибкость, выражающаяся в функциональности и многоаспектности, уникальность, универсальность и контекстность. Следовательно, в мире нет одного одинакового суверенитета: суверенитет каждой страны уникален и в разной степени ограничен наднациональным уровнем.

Проблематика информационной безопасности и цифрового суверенитета играет важную роль в работе региональных организаций. В частности, в рамках ШОС и ОДКБ были приняты документы, подтверждающие значимость данной категории к цифровой среде. Итоговый документ Самаркандского саммита ШОС 2022 года специально отмечает, что «принципы взаимного уважения суверенитета, независимости, территориальной целостности государств… являются основой устойчивого развития международных отношений», при этом особый акцент сделан на двух измерениях цифрового суверенитета: суверенитет в контексте выработки правил ответственного поведения государств в информационном пространстве и важность обеспечивать равные для всех стран права на регулирование сети Интернет и суверенное право государств на управление ею в своем национальном сегменте.

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Источники

Официальные документы Российской Федерации

1. Военная доктрина Российской Федерации. Утв. Президентом 25 декабря 2014 г., № Пр-2976. URL: http://www.scrf.gov.ru/security/military/document129/ (дата обращения 27.11.2025)

2. Доктрина информационной безопасности Российской Федерации. Утв. Президентом РФ 5.12.2016. URL: http://www.scrf.gov.ru/documents/6/5.html (дата обращения 27.11.2025)

3. Концепция безопасного функционирования и развития сети «Интернет» от 27.07. 2017. URL: https://digital.gov.ru/uploaded/files/prilozheniekontseptsiikonventsiioon.docx

4. Концепция участия Российской Федерации в объединении БРИКС. Утв. Президентом РФ 21.03.2013. URL: http://static.kremlin.ru/media/events/files/41d452a8a232b2f6f8a5.pdf (дата обращения 27.11.2025)

5. Программа «Цифровая экономика Российской Федерации». Утв. распоряжением Правительства РФ 28.07.2017. URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения 27.11.2025)

6. Проект Конвенции ООН о сотрудничестве в сфере противодействия информационной преступности от 11 октября 2017 г. URL: http://www.mid.ru/foreign_policy/international_safety/regprla/-/asset_publisher/YCxLFJnKuD1W/content/id/3025418 (дата обращения 27.11.2025)

7. Стратегия национальной безопасности Российской Федерации. Утверждена указом Президента Российской Федерации 02.07.2021 № 400. URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения 27.11.2025)

8. 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/ (дата обращения 27.11.2025)

9. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы. Утв. Президентом РФ 09.05.2017. № 203. URL: http://kremlin.ru/acts/bank/41919 (дата обращения 27.11.2025)

10. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» N 187-ФЗ 26.07.2016. URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 27.11.2025)

11. Основы государственной политики Российской Федерации в области международной информационной безопасности (утверждены Указом Президента РФ от 12 апреля 2021 г.)

12. Указ Президента Российской Федерации от 1 мая 2022 г. № 250 О дополнительных мерах по обеспечению информационной безопасности Российской Федерации

13. ФЗ от 27 июля 2006 г. № 152 «О персональных данных»

14. Концепция Конвенции международной информационной безопасности ООН. Совет безопасности. 2023.

Официальные документы США

15. Assessing Russian Activities and Intentions in Recent US Elections. The US Intelligence Community Assessment. 6 January 2017. URL: https://www.dni.gov/files/documents/ICA_2017_01.pdf (дата обращения 27.11.2025)

16. Countering America’s Adversaries Through Sanctions Act. Public Law No: 115-44. H.R.3364 – 115th Congress (2017-2018). URL: https://www.congress.gov/bill/115th-congress/house-bill/3364 (дата обращения 27.11.2025)

17. Executive Order 13694 Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities. Washington, April, 2015. URL: https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf (дата обращения 27.11.2025)

18. Foreign Economic Espionage in Cyber Space // National Counterintelligence and Security Center, 2018. URL: https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf (дата обращения 27.11.2025)

19. IT Strategic Plan. Digital Diplomacy: Fiscal Years 2011-2013 // US Department of State. September 1, 2010. URL:http://www.state.gov/m/irm/rls/148572.htm (дата обращения 27.11.2025)

20. National Cyber Strategy of the USA. White House, September, 2018. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения 27.11.2025)

21. 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 (дата обращения 27.11.2025)

22. US Department of Homeland Security Cybersecurity Strategy. Department of Homeland Security, May, 2018. URL: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf (дата обращения 27.11.2025)

23. A Declaration for the Future of the Internet // The White House 2022.

24. Non-Paper. Discussion Purposes Only. The Alliance for the Future of the Internet // Politico, 2021.

25. Efforts to Counter Ransomware The White House. 13 oct, 2021.

Официальные документы Китайской Народной Республики

26. 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 (дата обращения 27.11.2025)

27. China's Military Strategy. The State Council Information Office of the People's Republic of China. Beijing, 2015. URL: http://english.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm (дата обращения 27.11.2025)

28. Global Initiative on Data Security. MFA of PRC, 08 Septemeber, 2020.

29. Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 года

30. Made in China 2025. State Council, July 7, 2015., 中国制造2025

31. Cybersecurity Law of the People's Republic of China, 中华人民共和国网络安全法)

32. Data Security Law of the People's Republic of China, 中华人民共和国数据安全法

Официальные документы Франции

33. Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace. November 12, 2018. URL: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in (дата обращения 27.11.2025)

Документы международных правительственных организаций и форумов

Организация Объединенных Наций (ООН)

34. 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.

35. Резолюция ГА ООН A/53/70 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 4 декабря 1998 г.

36. Резолюция ГА ООН A/54/49 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 1 декабря 1999 г.

37. Резолюция ГА ООН A/C.3/73/L.9/Rev.1 «Противодействие использованию информационно-коммуникационных технологий в преступных целях» от 2 ноября 2018 г.

38. Резолюция ГА ООН A/73/505 «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности» от 22 декабря 2018 г.

39. Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (Доклад Генерального секретаря ООН A/60/202 от 5 августа 2005 г.)

40. Доклад Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (Резолюция ГА ООН A/65/201 от 30 июля 2010 г.)

41. Доклад Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (Резолюция ГА ООН A/68/98 от 24 июня 2013 г.)

42. Доклад Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (Резолюция ГА ООН A/70/174 от 22 июля 2015 г.)

43. Письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций на имя Генерального секретаря от 12 сентября 2011 года (A/66/359 от 14 сентября 2011 г.)

44. Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций на имя Генерального секретаря от 9 января 2015 года (A/69/723 от 9 января 2015 г.)

45. Резолюция ГА ООН A/57/239 «Создание глобальной культуры кибербезопасности» от 20 декабря 2002 г.

46. Резолюция ГА ООН A/58/199 «Создание глобальной культуры кибербезопасности и защита важнейших информационных инфраструктур» от 23 декабря 2003 г.

47. Резолюция ГА ООН A/64/211 «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур» от 21 декабря 2009 г.

48. «Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 года». Резолюция Генеральной Ассамблеи ООН A/RES/70/1 от 25 сентября 2015 г.

49. Стратегия Генерального секретаря по новым технологиям. 18-14875 (R). Июнь, 2018 г.

50. «Эпоха цифровой взаимозависимости»: доклад учрежденной Генеральным секретарем Группы высокого уровня по цифровому сотрудничеству. Июнь, 2019 г.

51. «Использование информационно-коммуникационных технологий в целях устойчивого развития». Резолюция Генеральной Ассамблеи ООН A/RES/74/197 от 10 января 2020 г.

52. Доклад Генерального Секретаря ООН «Дорожная карта по цифровому сотрудничеству: осуществление рекомендаций Группы высокого уровня по цифровому сотрудничеству». Резолюция Генеральной Ассамблеи ООН A/74/821 от 29 мая 2020 г.

53. Доклад Генерального Секретаря ООН «Наша общая повестка дня» Март, 2021 г.

54. Доклад Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (A/AC.290/2021/CRP.2 от 10 марта 2021 г.) (на английском) // Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substanive Report (A/AC.290/2021/CRP.2 10 March 2021)

55. Доклад Группы правительственных экспертов ООН по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности (Резолюция ГА ООН A/76/135 от 14 июля 2021 г.)

Международный союз электросвязи (МСЭ)

56. Всемирная ассамблея по стандартизации электросвязи МСЭ ВАСЭ-08 − Резолюция 50 – Йоханнесбург, 2008. URL:http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-R.pdf (дата обращения 27.11.2025)

57. World Telecommunication and Standartization Assembly Resolution. Non-discriminatory access and use of Internet resources. – Johannesburg, 2008. URL: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.69-2008-PDF-E.pdf (дата обращения 27.11.2025)

58. World Telecommunication Development Conference Resolution 69. Facilitating creation of national computer incident response teams, particularly for developing countries1, and cooperation between them. – Buenos-Aires, 2017. URL: https://www.itu.int/en/action/cybersecurity/Documents/Resolutions/69BuenosAires.pdf (дата обращения 27.11.2025)

59. World Telecommunication Standardization Assembly Resolution 50. Cybersecurity. - Hammamet, 2016. URL: https://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2016-PDF-E.pdf (дата обращения 27.11.2025)

Всемирная встреча на высшем уровне по вопросам информационного общества (ВВУИО)

60. Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-03/GENEVA/DOC/4-R. Декларация принципов. - 12 декабря 2003 года.

61. Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-03/GENEVA/DOC/5-R. План действий. – 12 декабря 2003 года.

62. Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-05/TUNIS/DOC/6(Rev.1)-R. Тунисская программа для информационного общества. – 18 ноября 2005 года.

63. Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-05/TUNIS/DOC/7-R. Тунисское обязательство. – 18 ноября 2005 года.

ЮНЕСКО

64. Программный документ ЮНЕСКО «Связанные с Интернетом вопросы, включая доступ к информации и знаниям, свободу выражения мнений, конфиденциальность и этические аспекты информационного общества» от 7 ноября 2013 г.

65. Рекомендация ЮНЕСКО об этических аспектах искусственного интеллекта. Резолюция Генеральной конференции ЮНЕСКО 41 C/23 от 24 ноября 2021 г.

66. Рекомендация ЮНЕСКО об открытых образовательных ресурсах // Резолюция Генеральной конференции ЮНЕСКО. 41 C/22 от 25 ноября 2019 г.

67. Рекомендации ЮНЕСКО по открытой науке // Резолюция Генеральной конференции ЮНЕСКО. CL/4319 от 8 сентября 2021 г.

ЮНКТАД

68. Доклад о цифровой экономике ЮНКТАД. «Создание стоимости и получение выгод: последствия для развивающихся стран». UNCTAD/DER/2019. Женева, 2019 г. (обзор)

69. Доклад о цифровой экономике. «Международные потоки данных и развитие: кому служат потоки данных. UNCTAD/DER/2021. Женева, 2021 г. (обзор)

70. UNCTAD Digital Economy Report 2024. URL: https://unctad.org/publication/digital-economy-report-2024 (дата обращения 27.11.2025)

«Группа двадцати»

71. 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 (дата обращения 27.11.2025)

72. G20 Leaders Communique. Antalya, 2015. URL: https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/G20+Leader%E2%80%99s+Communiqu%C3%A9+11-16-2015.pdf (дата обращения 27.11.2025)

«Группа восьми» / «Группа семи»

73. Окинавская Хартия глобального информационного общества. -- Окинава, 2000. URL: http://www.ifap.ru/ofdocs/okinhar.htm (дата обращения 27.11.2025)

74. G8 Background paper: International action against Cybercrime. Evian, 2003.

URL: http://www.diplomatie.gouv.fr/actual/evenements/cybercrim/fiche3.gb.html (дата обращения 27.11.2025)

75. G7 Declaration on Responsible State Behavior in Cyberspace. Lucca, 2017. URL: https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/G7+Declaration+on+Responsible+States+Behavior+in+Cyberspace+4-11-2017.pdf (дата обращения 27.11.2025)

76. G7 Principles and Actions on Cyber. Ise-Shima, 2016. URL: https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/G7+Principles+and+Actions+on+Cyber+5-27-2016.pdf (дата обращения 27.11.2025)

77. Joint Declaration by G7 ICT Ministers (Action Plan on implementing the Charter) of 30 April 2016

Совет Европы (СЕ)

78. Council of Europe Convention on cybercrime. ETSNo: 108. – Budapest, 2001.

URL:http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (дата обращения 27.11.2025)

Европейский союз (ЕС)

79. Artificial Intelligence Act (Regulation (EU) 2024/1689), Official Journal version of 13 June 2024

80. Cyber Security strategy of the European Union: An open, safe and secure Cyberspace. JOIN (2013). European Commission. Brussels, 7.02.2013. URL: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security (дата обращения 27.11.2025)

81. European Union Action Plan on Promoting Safer Use of the Internet. 276/1999/EC.

URL: http://europa.eu.int/ISPO/iap/decision/en.html. (дата обращения 27.11.2025)

82. Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities («Cyber Diplomacy Toolbox») of 19 June 2017

83. European Union General Data Protection Regulation (GDPR) of 27 April 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (дата обращения 27.11.2025)

Содружество Независимых Государств (СНГ)

84. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности от 23 ноября 2013 г.

Шанхайская организация сотрудничества (ШОС)

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

БРИКС

86. Казанская декларация БРИКС. Казань, 2024.

Организация безопасности и сотрудничества в Европе (ОБСЕ)

87. PC.DEC/1202. Решение № 1202. Меры укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий. 10.03.2016. URL: http://www.osce.org/ru/pc/228521?download=true (дата обращения 27.11.2025)

88. PC.DEC/1106. Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий. 3.12. 2013. URL: http://www.osce.org/ru/pc/109648?download=true (дата обращения 27.11.2025)

Организация договора о коллективной безопасности (ОДКБ)

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

Региональный форум Ассоциации государств Юго-Восточной Азии по безопасности (АСЕАН – АРФ)

90. 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.

Организация североатлантического договора (НАТО)

91. Заявление по итогам встречи НАТО на высшем уровне в Брюсселе от 11 июля 2018 г.

92. Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. Warsaw, 2016. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm (дата обращения 27.11.2025)

93. NATO Cyber Defense Pledge. Brussels, 2016. URL: https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/NATO+Cyber+Defence+Pledge+7-8-2016.pdf (дата обращения 27.11.2025)

94. NATO Whales Summit Declaration. Brussels, 2014. URL: https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/Wales+Summit+Declaration+9-5-2014.pdf (дата обращения 27.11.2025)

Африканский союз

95. African Union Convention on Cyber Security and Personal Data Protection. Malabo, 27.06.2014. URL: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (дата обращения 27.11.2025)

96. Continental Artificial Intelligence Strategy. African Union. 09.08.2024. URL: https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy (дата обращения 27.11.2025)

Двусторонние межправительственные соглашения и межгосударственные договоренности, совместные заявления

97. Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 г.

98. Совместное заявление президентов Российской Федерации и Соединенных Штатов Америки о новой области сотрудничества в укреплении доверия от 17 июня 2013 г.

99. Соглашение между Правительством Российской Федерации и Правительством Федеративной Республики Бразилии о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности от 14 мая 2010 г.

100. Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности от 25 декабря 2013 г.

101. Соглашение между Правительством Российской Федерации и Правительством Республики Индии о сотрудничестве в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий от 15 октября 2016 г.

102. Соглашение между Правительством Российской Федерации и Правительством Южно-Африканской Республики о сотрудничестве в области обеспечения международной информационной безопасности от 4 сентября 2017 г.

103. Совместное заявление Российской Федерации и Китайской Народной Республики о дальнейшем углублении отношений всеобъемлющего партнерства и стратегического взаимодействия от 4 июля 2017 г.

Библиография

Монографии, сборники научных трудов

На русском языке

104. Актуальные военные аспекты обеспечения международной информационной безопасности. / Под ред. С.В. Короткова. - М.: ГШВС России, 2008. - 92 с.

105. Балуев Д.Г. Информационная революция и современные международные отношения. – Н.Новгород: ННГУ, 2001. - 107 с.

106. Белл Д. Грядущее постиндустриальное общество: опыт социального прогнозирования: пер. с англ. - М.: Academia, 1999. - 788 с.

107. Варуфакис Я. Технофеодализм. М., 2025.

108. Кастельс М. Информационная эпоха: экономика, общество и культура: пер. с англ. / под научн. ред. О.И. Шкаратана. - М.:ГУ-ВШЭ, 2000. - 608 с.

109. Курбалиа Й. Управление Интернетом / пер. с англ. - М.: Координационный центр национального домена сети Интернет, 2010. - 208 с.

110. Ларина Е.С. Кибервойны XXI века. О чем умолчал Эдвард Сноуден / Е.С. Ларина, В.М. Овчинский. - М.: Книжный мир, 2014. - 352 с.

111. Лебедева М.М. Мировая политика. - М.: Аспект-пресс, 2013. - 256 с.

112. Международные отношения России в «новых политических пространствах»: космос, приполярные зоны, воздушные и морские пространства, глобальная информационная сфера. - М.: URSS, 2011. - 272 с.

113. Роговский Е.А. Кибер-Вашингтон: глобальные амбиции. - М.: Международные отношения, 2014. - 846 с.

114. Современное состояние и перспективы развития военного сотрудничества Российской Федерации в области международной информационной безопасности / Под общ. ред. С.А. Комова. - М.: Министерство обороны, 2014. – 332 с.

115. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. - М., 2004. URL: http://www.iisi.msu.ru/UserFiles/File/publications/Streltsov.pdf

116. Федоров А.В. Информационная безопасность в мировом политическом процессе. - М.: МГИМО, 2006. - 218 с.

117. Федоров А.В. Международная информационная безопасность: политическая теория и дипломатическая практика / А.В. Федоров, Е.С. Зиновьева. - М.: МГИМО, 2017. – 360 с.

118. Цифровая трансформация мировой экономики Учебное пособие для программ бакалавриата и магистратуры / Пичков О.Б., Шитьков С.В., Уланов А.А., Патрунина К.А. Москва: Аспект-Пресс, 2022.

119. Цифровое право / Под ред Э.Л. Сидоренко. М., 2024.

120. Цифровые международные отношения В двух томах. Учебное пособие для вузов / Торкунов А.В., Шерстюк В.П., Крутских А.В., Зиновьева Е.С., Шитьков С.В., Волкова С.Г., Зинченко А.В., Булва В.И., Цветкова Н.А., Сытник А.Н., Смирнов А.И., Сурма И.В., Исаева Т.В., Мирошников Б.Н., Чернухин Э.В., Стрельцов А.А., Пичков О.Б., Патрунина К.А., Салыгин В.И., Григорьев Д.И. и др. // Под ред. С.В. Шитькова, Е.С. Зиновьевой. М.: Аспект-Пресс, 2023.

121. Шаклеина Т.А. Россия и США в мировой политике. М.: МГИМО, 2018. – 336 с.

122. Шваб К. Четвертая промышленная революция. - М.: ЭКСМО, 2017. - 208 с.

На иностранных языках

123. Anderson B. I. C. Imagined communities: Reflections on the Origin and Spread of Nationalism. London: 1983. – 160 p.

124. Betz D. Cyberspace and the State: Toward a Strategy for Cyber-Power / D.Betz, T. Stevens. - London: Routledge, 2011. – 158 c.

125. Braun M., Hummel P. Is digital sovereignty normatively desirable? //Information, Communication & Society. – 2025. – Т. 28. – №. 10. – С. 1721-1734.

126. Brenner J. America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare. - NY: Penguin Press, 2014. – 320 p.

127. Buzan B. International systems in world history: remaking the study of international relations / B. Buzan, R. Little. – Oxford: Oxford University Press, 2000. – 452 p.

128. Buzan B. Security: a new framework for analysis / B.Buzan, O.Wæver, J.De Wilde. - Lynne Rienner Publishers, 1998. - 239 p.

129. Buzan B. The United States and the great powers: world politics in the twenty-first century. - Cambridge: Polity Press, 2004. - 227 p.

130. Castells M. The Rise of the Network Society: The Information Age: Economy, Society, and Culture. – NY: John Wiley & Sons, 2011. - 594 p.

131. Cavelty M. The Resurgence of the State: Trends and Processes in Cyberspace Governance / M.Cavelty, M.Dunn, S.Krishna-Hensel, V.Mauer. - Asghate: Ashgate Publishing, Ltd., 2007. - 165 p.

132. China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain /Ed. by J. Lindsay, T. Cheung, D. Reveron. New York: Oxford University Press, 2015. – 375 p.

133. Choucri N. Cyberpolitics in International Relations. - MIT Press, 2012. - 320 p.

134. Cyber Analogies / Ed. by e. Glodmann, J. Arquilla. – Monterey CA: Naval postgraduate School, 2014. – 119 p.

135. Cyber warfare and cyber terrorism. / Ed. by L. Janczewski, A. Colarick. - NY: IGI Global, 2007. - 565 p. URL:

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.670.9033&rep=rep1&type=pdf

136. Cyberprotest: new media, citizens and social movements / Ed. By W. van d Donk, B. Loader, P. Nixon, D. Rucht. – London: Routlege, 2004. - 336 p.

137. Evolution of the Cyber Domain: The Implications for National and Global Security. / Ed. by E. Tikk-Ringas. - London: Routlege, International Institute for Strategic Studies, 2015. - 212 p.

138. Fang B., Fang, Zhang. Cyberspace sovereignty. – Springer Singapore, 2018.

139. Goldsmith J. Who Controls the Internet? / J. Goldsmith, T. Wu. - Oxford: Oxford University Press, 2006. - 226 p.

140. International Relations and Security in the Digital Age / Ed. by J. Eriksson, G.Giacomello. - London: Routlege, 2007. - 256 p.

141. Jamieson K. H. Cyberwar: How Russian Hackers and Trolls Helped Elect a President What We Don't, Can't, and Do Know. – Oxford University Press, 2018. – 305 p.

142. iang 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.

143. Krasner S. D. Power, the state, and sovereignty: Essays on international relations. – Routledge, 2009.

144. Mathiason J. Internet Governance: The New Frontier of Global Institutions. - London: Taylor & Francis, 2008. - 178 p.

145. Mazanek B. Deterring Cyber Warfare / B. Mazanek, B. Thayer. – London: Palgrave McMiollan, 2014. – 95 p.

146. Mearsheimer J. The tragedy of great power politics. - WW Norton & Company, 2001. - 592 p.

147. Morozov E. The Net Delusion: The Dark Side of Internet Freedom. NY: PublicAffairs, 2011. – 429 p.

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

149. Nye J. The Future of Power in the 21st Century. - N.Y.: Public Affairs Press, 2011. - 300 p.

150. Price M. E. Media and sovereignty: The global information revolution and its challenge to state power. - MIT Press, 2004. - 326 p.

151. Schmitt M. Proxy Wars in Cyberspace: the Evolving International Law of Attribution / M. Schmitt, L. Vihul. - Fletcher Security, 2014. – 19 p.

152. Security in Cyberspace: Targeting Nations, Infrastructures, Individuals. / Ed by G. Giacomello. – NY: Bloomsbury Publishing USA, 2014. - 256 p.

153. Segal A. The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age. - Hachette UK, 2016. - 320 p.

154. Shitkov S.V. Sovereignty as practice in digital age / Zinovieva E.S., Shitkov S.V. // Digital International Relations. Singapore, 2023. C. 75-90.

155. Skolnikoff E. B. The elusive transformation: science, technology, and the evolution of international politics. - Princeton University Press, 1994. - 336 p.

156. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. / Ed. by M. Schmitt. - N.Y.: Cambridge University Press, 2017. - 638 p.

157. Tallinn Manual on the International Law Applicable to Cyber Warfare / Ed. by M. Schmitt. - N.Y.: Cambridge University Press, 2013. - 282 p.

158. Valeriano B. International Relations Theory and Cyber Security: Threats, Conflicts and Ethics in an Emergent Domain / B. Valeriano, R. Maness // The Oxford Handbook of Political Theory / Ed. by C. Brown, R. Eckersley. - Oxford: Oxford University Press, 2018. - P. 259 – 275.

159. Walker N. (ed.). Relocating sovereignty. – Routledge, 2018.

160. Wendt A. Quantum Mind and Social Science. Unifying Physical and Social Ontology. - Cambridge: Cambridge University Press, 2015. - 366 p.

161. Wendt A. Social Theory of International Politics. – N.Y.: Cambridge University Press, 1999. – 420 p.

Статьи и главы в научных изданиях, научные доклады, диссертации

На русском языке

162. Алиева З. М., Магомадова М. М., Разина И. С. Цифровая трансформация и цифровая экономика: исследование основных технологий и их характеристик //Региональные проблемы преобразования экономики. – 2024. – №. 5. – С. 151-158.

163. Аничкина Т.Б. О некоторых приемах информационной войны США // США-Канада: экономика, политика, культура. - 2007. - № 7. - С. 123-127.

164. Бартош А.А. Саммит НАТО в Варшаве: предварительный анализ // Власть. - 2016. - № 9. - С. 25-30. URL: https://www.nato.int/nato_static_fl2014/assets/audio/audio_2017_11/20171108_171108c-ru.mp3

165. Барышников Д. Н., Туленков А. Ю. «Цифровая дипломатия» и государственный суверенитет в эпоху глобализации //Вестник Санкт-Петербургского университета. Международные отношения. – 2012. – №. 4. – С. 121-128.

166. Батуева Е.В. Американская концепция угроз информационной безопасности и ее международно-политическая составляющая // Дисс. … ученой степени кандидата политических наук. - М.: МГИМО, 2015. – 192 с.

167. Бедрицкий А.В. Международные договорённости по киберпространству: возможен ли консенсус? // Проблемы национальной стратегии. - 2012. - №4. URL:

http://www.riss.ru/images/pdf/journal/2012/4/10_.pdf (дата обращения 27.11.2025)

168. Безруков А. О. и др. Суверенитет и» цифра» //Россия в глобальной политике. – 2021. – Т. 19. – №. 2 (108). – С. 106-119.

169. Бойко С. М. Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: взгляд из прошлого в будущее //Международная жизнь. - 2016. - №. 8. - С. 53-71.

170. Бойко С.М. Проблематика международной информационной безопасности на площадках ШОС и БРИКС // Международная жизнь. – 2019. - №1. – С. 1 – 22.

171. Бойко С.М. Формирование системы международной информационной безопасности: российские подходы и инициативы // Международная жизнь. – 2018. - № 5.– С. 100 - 110.

172. Болгов Р.В. Информационные технологии в современных вооруженных конфликтах и военных стратегиях (политические аспекты). Дис... канд. полит.наук. - СПб.: СПбГУ, 2010. – 182 с.

173. Бурякова О.С. Информационная и знаниевая революции: сравнительный анализ концепций // Дисс ... кандидата филос. наук. - Ростов-на-Дону: Юж. Федер Университет, 2011. – 145 с.

174. Бухарин В. В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности //Вестник МГИМО университета. – 2016. – №. 6 (51). – С. 76-91.

175. Виноградова Е. В., Полякова Т. А. О месте информационного суверенитета в конституционно-правовом пространстве современной России //Правовое государство: теория и практика. – 2021. – №. 1 (63). – С. 32-49.

176. Воскресенский А.Д. Структурирование регионального пространства и его основные акторы. Регионализация и трансрегиональное

сотрудничество / А.Д. Воскресенский, Е.В. Колдунова, А.А. Киреева // Мировое комплексное регионоведение / Под ред. А.Д. Воскресенского. - М.: Магистр-Инфра-М, 2014. – с. 80-107.

177. Ватулина А. А. Трансформация нормативной силы Европейского союза и построение цифрового суверенитета под влиянием новых вызовов //Международные отношения. – 2025. – №. 2. – С. 178-189.

178. Гасумянов В. И. Международная информационная безопасность: практические меры и этический консенсус // Международная жизнь. - 2018. - Февраль. URL: https://interaffairs.ru/jauthor/material/1980

179. Демидов О.В. Киберстратегия США 2018. Значение для глобального диалога о поведении в сфере использования ИКТ и российско-американских отношений / О.В. Демидов, М. Ангмар. – М.: ПИР-Центр; «Триалог», 2019. – 30 с. – (Серия «Индекс Безопасности»).

180. Ефремов А. А. Государственный суверенитет в условиях цифровой трансформации //Правоведение. – 2019. – Т. 63. – №. 1. – С. 47-61.

181. Ефремов А. А. Формирование концепции информационного суверенитета государства //Право. Журнал Высшей школы экономики. – 2017. – №. 1. – С. 201-215.

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

183. К великому океану – Создание Центральной Евразии // Аналитический доклад Международного Дискуссионного клуба «Валдай». - М., 2015. URL: http://iwep.kz/files/attachments/article/2015-04-21/doklad_sozdanie_evrazii_ekonomicheskiy_poyas_shelkovogo_puti.pdf (дата обращения 27.11.2025)

184. Калиновский О.Н. Информационная война – это война? // Военная мысль. – 2001. - №1. - С. 57-58.

185. Карасев П.А. Политика безопасности США в глобальном информационном пространстве. Автореферат дис. на соискание … к.полит.н. по специальности 23.00.04. - М.: ИМЭМО РАН, 2015. URL: https://www.imemo.ru/files/File/ru/dis/2015_004_Karasiov_AUTR.pdf (дата обращения 27.11.2025)

186. Кибербезопасность гражданских ядерных объектов: оценка угрозы и пути ее преодоления. Доклад ПИР-центра. // Индекс безопасности. - 2016. - № 3-4. - С. 63-79.

187. Коротков А.В. Безопасность критических информационных инфраструктур в международном гуманитарном праве / А.В. Коротков, Е.С. Зиновьева // Вестник МГИМО-Университета. - 2011. - № 4. - С. 154-162

188. Кочетков А. П., Маслов К. В. Цифровой суверенитет как основа национальной безопасности России в глобальном цифровом обществе //Вестник Московского университета. Серия 12. Политические науки. – 2022. – №. 2. – С. 31-45.

189. Кутюр С., Софи Т. Что означает понятие» суверенитет» в цифровом мире? //Вестник международных организаций: образование, наука, новая экономика. – 2020. – Т. 15. – №. 4. – С. 48-69.

190. Кучерявый М.М. Информационное измерение политики национальной безопасности России в условиях современного глобального мира // Дисс. … ученой степени доктора политических наук. - СПб: СПбГУ, 2014.

191. Макарычева А.В. Подходы к преодолению традиционных и новых вызовов безопасности в Латинской Америке (на примере территориальных споров и информационных угроз) // Дисс… ученой степени кандидата политических наук. – М.: МГИМО, 2018. – 239 с.

192. Манойло А.В. Роль культурно-цивилизационных моделей и технологий информационно-психологического воздействия в разрешении

международных конфликтов // Дисс. … ученой степени доктора политических наук. - М.: МГУ, 2010. – 440 с.

193. Минбалеев А. В. и др. Методы и подходы к регулированию формирующейся отрасли квантовых коммуникаций в условиях современного информационного общества //Информационное общество. – 2024. – №. 4. – С. 112-120.

194. Никонов В. А. и др. Цифровой суверенитет современного государства: содержание и структурные компоненты (по материалам экспертного исследования) //Вестник Томского государственного университета. Философия. Социология. Политология. – 2021. – №. 60. – С. 206-216.

195. Ребро О. и др. Категория «Цифрового суверенитета» в современной мировой политике вызовы и возможности для России //Международные процессы. – 2021. – Т. 19. – №. 4. – С. 47-67.

196. Роговский Е.А. Выборы в США: успех технологических инноваций // Международная жизнь. - 2017. - №3. - С. 107-122.

197. Северс А.В. Стратегия микротаргетирования и роль социальных сетей в политических коммуникациях // Вестник Московского университета. Серия 10. Журналистика. - 2013. - № 2. - С. 38-47.

198. Фененко А.В. Военно-техническая модернизация и «циклы» сближения между США и Россией // Международные процессы. - 2011. - № 2. URL: http://www.intertrends.ru/twenty-sixth/005.htm (дата обращения 27.11.2025)

199. Фененко А.В. Международное соперничество за освоение общих пространств // Международные процессы. - 2010. - № 1. URL: http://www.intertrends.ru/twenty-second/003.htm (дата обращения 27.11.2025)

200. Цветкова Н. А. Социальные сети в публичной дипломатии США // Вестник Санкт-Петербургского университета. Серия 6. Политология. Международные отношения. – 2011. – №. 2. – С. 84 – 89.

201. Цветкова Н.А. Программы Web 2.0 в публичной дипломатии США // США и Канада: Экономика, политика, культура. - 2011. - №3. - С. 109-122.

202. Цветкова Н.А. США - ИГИЛ: информационное противостояние кто побеждает в социальных сетях? // Азия и Африка сегодня. - 2017. - № 2 (715). - С. 2-7.

203. Черненко Е.В. Холодная война 2.0? Киберпространство как новая арена противостояния // Россия в глобальной политике. - 2013. - № 2. URL:http://www.globalaffairs.ru/number/Kholodnaya-voina-20-15874 (дата обращения 27.11.2025)

204. Чернобай А. Роль социальных сетей в мобилизации протестных настроений на Ближнем Востоке и в Северной Африке в январе-марте 2011 года // Идеологические аспекты военной безопасности. - 2011. - № 1. URL:http://mod.mil.by/iavb/2011n1/9.pdf (дата обращения 27.11.2025)

205. Шариков П.А. Политика США в области информационной безопасности // Дисс. … ученой степени кандидата политических наук. - М.: ИСКРАН, 2009. – 180 с.

206. Шитьков С.В. «Датский прецедент» в решении вопроса о праве Российской Федерации на недвижимость бывшего СССР // Право и управление. XXI век. – 2008. – № 1(6). – С. 30-37. – EDN MUNXAL.

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

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

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

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

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

212. Шитьков С.В. Правовой режим участия Российской Федерации в гражданских правоотношениях // Право и управление. XXI век. – 2007. – № 2(5). – С. 26-33. – EDN MUGDQR.

213. Шитьков С.В. Развитие цифрового суверенитета в рамках Евразийского экономического союза: стратегические приоритеты и институциональные механизмы // Евразийский Союз: вопросы международных отношений. – 2025. – Т. 14, № 5(70). – С. 1210-1218. – DOI 10.35775/PSI.2025.70.5.012.

214. Шитьков С.В. Становление права собственности в законодательстве дореволюционной России // Право и управление. XXI век. – 2009. – № 3(12). – С. 51-55. – EDN OPQQCB.

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

216. 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.

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

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

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

220. 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.

221. 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.

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

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

224. Юдин Н.О. Роль ТНК в современной мировой политике // Обозреватель. – 2020. – № 9(368). – С. 83-92. – EDN ZUTYFC.

225. Юдин Н.О. Транснациональная корпорация как актор гуманитарной дипломатии // Социально-гуманитарные знания. – 2024. – № 2. – С. 147-150. – EDN URFBKZ.

На иностранных языках

226. Bailard K. Ethnic conflict goes mobile: Mobile technology's effect on the opportunities and motivations for violent collective action // Journal of Peace Research. - 2015. - № 3 (52). - P. 323-337.

227. Bebber R. Treating Information as a Strategic Resource to Win the "Information War" // Orbis. – 2017. – №. 3. – С. 394-403.

228. Belli L. BRICS countries to build digital sovereignty //CyberBRICS: Cybersecurity regulations in the BRICS countries. – 2021. – С. 271-280.

229. Benhamou B. Souveraineté et Réseaux Numériques / B. Benhamou, L. Sorbier // Politique Étrangère. - 2006. - No 3. URL:http://www.google.com/url?sa=t&source=web&ct=res&cd=1&url=http%3A%2F%2Fwww.netgouvernance.org%2Fpolitiqueetrangere.pdf&ei=yqEZSqWtPJHGsgaA6Nm-Cg&rct=j&q=Souverainet%C3%A9+et+r%C3%A9seaux+num%C3%A9riques+&usg=AFQjCNGLwwRuGri8ijTGu_oScnl1GZabFQ (дата обращения 27.11.2025)

230. Biersteker T. J. State, sovereignty and territory //Handbook of international relations. – 2013. – С. 245-272.

231. Braud A. et al. The road to European digital sovereignty with Gaia-X and IDSA //IEEE network. – 2021. – Т. 35. – №. 2. – С. 4-5.

232. Castells M. Communication, Power and Counter-power in the Network Society // International Journal of Communication. - 2007. - № 1. - P. 238-266.

233. Castells M. The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance // The Annals of the American Academy of Political and Social Science. - 2008. - № 616. URL:http://prtheories.pbworks.com/w/file/fetch/45138545/Castells_2008_The_New_Public_Sphere.pdf (дата обращения 27.11.2025)

234. Cavelty M. Aligning Security Needs for Order in Cyberspace //The Rise and Decline of the Post-Cold War International Order / Ed. by H. Maul – Oxford University Press, 2018. - P. 104 – 120.

235. Cavelty M. From Cyber-bombs to Political Fallout: Threat Representations with an Impact in the Cyber-security Discourse // International Studies Review. - Special Issue: International Relationships in the Information Age. – 2013. - № 1. - P. 105–122.

236. Civil Movements: The Impact of Facebook and Twitter // Arab social media report. - 2011. - № 2(1). URL: http://www.dsg.ae/portals/0/ASMR2.pdf (дата обращения 27.11.2025)

237. Couture S., Toupin S. What does the notion of “sovereignty” mean when referring to the digital? //New media & society. – 2019. – Т. 21. – №. 10. – С. 2305-2322.

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

239. Creemers R. China’s emerging data protection framework //Journal of Cybersecurity. – 2022. – Т. 8. – №. 1.

240. Creemers R. Cybersecurity Law and regulation in China: Securing the smart state //China Law and Society Review. – 2023. – Т. 6. – №. 2. – С. 111-145.

241. Creemers R. Great Power Relationships or Common Destiny? Chinese Government and Private Actors' Long and Winding Road to find a Place in Global Cyberspace //Routledge Handbook on Global China. – Routledge, 2024. – С. 107-123.

242. Creemers R. The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy //Journal of Contemporary China. – 2024. – Т. 33. – №. 146. – С. 173-188.

243. Cukier K. Multilateral Control of Internet Infrastructure and its Impact on US Sovereignty // Telecommunications Policy and Research Conference. - Alexandria, VA. October 2004.

URL:http://www.cukier.com/writings/cukier-netgov-TPRC04.pdf.html (дата обращения 27.11.2025)

244. Deibert R. Risking Security: Policies and Paradoxes of Cyberspace Security / R. Deibert, R. Rohozinski // International Political Sociology. - 2010. - №1. - P. 15–32.

245. Deibert R. The geopolitics of cyberspace after Snowden // Current History. - 2015. - Vol. 114. - №. 768. - P. 9-15.

246. Deibert R. Trajectories for Future Cybersecurity Research //The Oxford Handbook of International Security / Ed. by A. Gheciu and W. C. Wohlforth. - Oxford: Oxford University Perss, 2015. - P. 531 – 556.

247. Der Derian J. From War 2.0 to quantum war: the superpositionality of global violence //Australian Journal of International Affairs. - 2013. - T. 67. - №. 5. -P. 570-585.

248. Dixon H. Regulate to Liberate: Can Europe Save the Internet //Foreign Aff. – 2018. – T. 97. – P. 28 - 34.

249. Dogrul M. Developing an international cooperation on cyber defense and deterrence against cyber terrorism / M. Dogrul, A. Aslan, E. Celik // 3rd international conference on Cyber conflict (ICCC), 2011. - P. 1-15.

250. Ebert H. Contested cyberspace and rising powers // Third World Quarterly. – 2013. - №6. URL: https://www.tandfonline.com/doi/full/10.1080/01436597.2013.802502?scroll=top&needAccess=true (дата обращения 27.11.2025)

251. Falkner G. et al. Digital sovereignty-Rhetoric and reality //Journal of European Public Policy. – 2024. – C. 1-22.

252. Farrell H. Promoting Norms for Cyberspace. - NY: Council on Foreign Relations, 2015. URL: https://www.cfr.org/report/promoting-norms-cyberspace (дата обращения 27.11.2025)

253. Finnemore M. Cultivating International Cyber Norms. // America’s Cyber Future: Security and Prosperity in the Information Age. / Edited by K.

Lord, T. Sharp. - Washington, DC: Center for a New American Security, 2011. - P. 89-101

254. Finnemore M. International norm dynamics and political change / M. Finnemore, K. Sikkink // International organization. - 1998. - T. 52. - №. 4. - P. 887-917.

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

256. Giles K. Divided by a common language: cyber definitions in Chinese, Russian and English / K. Giles, W. Hagestad // 5th International Conference on Cyber Conflict (CyCon). - 2013. - P. 1-17.

257. Glasze G. et al. Contested spatialities of digital sovereignty //Geopolitics. – 2023. – T. 28. – №. 2. – C. 919-958.

258. Gorr D. Creating a secure cyberspace: Securitization in Internet governance discourses and dispositives in Germany and Russia / D. Gorr, W. J. Schünemann // International Review of Information Ethics. - 2013. - T. 20. - №. 12. - P. 37-51.

259. Herrera G. L. Cyberspace and sovereignty: thoughts on physical space and digital space //Power and security in the information age. – Routledge, 2016. – C. 67-93.

260. Inkster N. Chinese Intelligence in the Cyber Age // Survival: Global Politics and Strategy. – 2013. - №1. – P. 45–66.

261. Jervis R. Security regimes //International organization. - 1982. - T. 36. - №. 2. - P. 357-378.

262. Junio T. How Probable Is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate // Journal of Strategic Studies. - 2013. - №1. - P. 125–133.

263. Klimburg A. Mobilising Cyber Power. // Survival. – 2011. - №1. - P. 41–60.

264. Klimburg A. The Internet Yalta: Commentary // Center for New American Security. - 5.02.2013. URL:http://www.cnas.org/theinternetyalta (дата обращения 27.11.2025)

265. Krasner S. D. Abiding sovereignty //International political science review. – 2001. – Т. 22. – №. 3. – С. 229-251.

266. Krasner S. D. Sovereignty //Foreign Policy. – 2001. – С. 20-29.

267. Krasner S. D. Sovereignty: An institutional perspective //Comparative political studies. – 1988. – Т. 21. – №. 1. – С. 66-94.

268. Lambach D., Oppermann K. Narratives of digital sovereignty in German political discourse //Governance. – 2023. – Т. 36. – №. 3. – С. 693-709.

269. Lewis J. Confidence-building and international agreement in cybersecurity // Disarmament Forum. - 2011. - №4. - P. 51-60. URL: https://citizenlab.ca/cybernorms2012/Lewis2011.pdf (дата обращения 27.11.2025)

270. Lewis J. Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization. / J.Lewis, K.Timlin // UNIDIR. - 2011. URL: http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf (дата обращения 27.11.2025)

271. Libicki M. Expectations of cyber deterrence // Strategic Studies Quarterly. – 2018. - № 4. –P. 44 – 57.

272. Lindsay J. R. The impact of China on cybersecurity: Fiction and friction // International Security. - 2015. - №. 3. - P. 7-47.

273. Lindsay J. Stuxnet and the Limits of Cyber Warfare // Security Studies. – 2013. - № 3. – P. 365 – 404.

274. Lukasik S. J. A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains // Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy. - 2010. - T. 2. - P. 99-122.

275. Lund S. Defending digital globalization: Let the data flow / S. Lund, J. Manyika // Foreign Affairs. – 2017. – T. 20. URL: https://www.foreignaffairs.com/articles/world/2017-04-20/defending-digital-globalization (дата обращения 27.11.2025)

276. Maas M. M. How viable is international arms control for military artificial intelligence? Three lessons from nuclear weapons //Contemporary Security Policy. – 2019. – P. 1-27.

277. Mačák K. From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers //Leiden Journal of International Law. – 2017. – T. 30. – №. 4. – P. 877-899.

278. Mainwaring S. Always in control? Sovereign states in cyberspace //European Journal of International Security. – 2020. – T. 5. – №. 2. – C. 215-232.

279. Manjikian M. From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik // International Studies Quarterly. – 2010. - № 2. - P. 381–401.

280. Mayer M. The global governance of large technical systems / M.Mayer, M.Acuto //Millennium. - 2015. - T. 43. - №. 2. - P. 660-683.

281. Moerel L., Timmers P. Reflections on digital sovereignty //EU cyber direct, research in focus series. – 2021.

282. Monsees L., Lambach D. Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity //European Security. – 2022. – T. 31. – №. 3. – C. 377-394.

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

284. Neuneck G. Civilian and military cyberthreats: shifting identities an attribution. // The Cyber Index. International Security Trends and Realities. - UNIDIR, 2013. URL:http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf (дата обращения 27.11.2025)

285. Nye J. Deterrence and Dissuasion in Cyberspace // International Security. - 2017. - T. 41. - №. 3. - P. 44-71.

286. Nye J. How sharp power threatens soft power. The Right and Wrong Ways to Respond to Authoritarian Influence // Foreign Affairs. - 2018. - Snapshot. January 24. URL: https://www.foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power (дата обращения 27.11.2025)

287. Nye J. Nuclear lessons for cyber security // Strategic Studies Quarterly. – 2011. – № 31. – Winter. – P. 20 -38.

288. Nye J. The regime complex for managing global cyber activities // Global Commission on Internet Governance Paper Series, 2014. – URL: https://dash.harvard.edu/bitstream/handle/1/12308565/Nye-GlobalCommission.pdf (дата обращения 27.11.2025)

289. Pohle J. et al. Digital sovereignty //Practicing sovereignty: Digital involvement in times of crises. – 2021. – T. 13. – №. 7. – С. 47-67.

290. Roberts H. Digital sovereignty and artificial intelligence: a normative approach //Ethics and Information Technology. – 2024. – T. 26. – №. 4. – С. 1-10.

291. Robles-Carrillo M. Sovereignty vs. digital sovereignty //Journal of Digital Technologies and Law. – 2023. – T. 1. – №. 3. – С. 673-690.

292. Rosato S. The Inscrutable Intentions of Great Powers //International Security. - 2015. - №. 3. - P. 48-88.

293. Segal A. When China Rules the Web: Technology in Service of the State //Foreign Aff. – 2018. – T. 97. – С. 10.

294. Shen Y. Cyber sovereignty and the governance of global cyberspace //Chinese Political Science Review. – 2016. – T. 1. – С. 81-93.

295. Stayner J. Web 2.0 and the transformation of news and journalism // Handbook of Internet Politics. / Ed. by A. Chadwick. - London: Routledge, 2008. - P. 201-213.

296. Stevens T. A cyberwar of ideas? Deterrence and norms in cyberspace //Contemporary Security Policy. - 2012. - №. 1. - P. 148-170.

297. Walker C. The meaning of sharp power. How authoritarian states project influence / C. Walker, J. Ludwig // Foreign Affairs. – 2017. - Snapshot. November 16. URL: https://www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power (дата обращения 27.11.2025)

298. Wendt A. Anarchy is what states make of it: the social construction of power politics // International Organization. – 1992. - No. 2. - P. 391-425.

299. Wendt A. Constructing International Politics // International Security. - 1995. - № 1(20). - P. 71-81.