

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ МЕЖДУНАРОДНОГО БИЗНЕСА, ЭКОНОМИКИ И УПРАВЛЕНИЯ
КАФЕДРА МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

ОТЧЕТ ПО ПРОИЗВОДСТВЕННОЙ НАУЧНО-
ИССЛЕДОВАТЕЛЬСКОЙ ПРАКТИКЕ (НИР)

Магистрант гр ММО-25-МО1



Н.А. Сыровец

Руководитель от профильной организации
Зав. кафедрой МОГУ
канд. экон. наук, доцент



Попова И.В.

Руководитель практики от кафедры

Канд. истор. наук, доцент



Ким А.А.

Владивосток 2026

Содержание

Путевка	3
Рабочий график (план)	5
Индивидуальное задание	6
Отзыв	8
Приложение А. Текст статьи по материалам проведенного исследования для публикации в научном издании	10

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ МЕЖДУНАРОДНОГО БИЗНЕСА, ЭКОНОМИКИ И УПРАВЛЕНИЯ
КАФЕДРА МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

ПУТЕВКА

Магистрант Сыровец Никита Андреевич

Фамилия Имя Отчество

учебная группа ММО-25-МО1

согласно приказу ректора № 1186-а от «20» мая 2026 г.

Направляется в ФГБОУ ВО «ВВГУ», Институт международного бизнеса, экономики и управления, кафедра международных отношений и государственного управления (МОГУ), г. Владивосток, ул. Гоголя, 41, ауд. 1527, тел. (243)240-41-60 для прохождения производственной научно-исследовательской практики (НИР) по направлению подготовки 41.04.05 Международные отношения. Международные отношения и приграничное сотрудничество на срок 6 недель с «25» мая 2026 г. по «18» июля 2026 г.

Руководитель практики от кафедры МОГУ

Канд. истор. наук, доцент

Ким А.А.

/  /

Подпись, печать

Тел. выпускающей кафедры 240-43-32

Отметки о выполнении и сроках практики принимающей организации

Полное наименование организации	Отметка о прибытии и убытии	Должность уполномоченного лица, подпись, печать
ФГБОУ ВО «ВВГУ», Институт международного бизнеса, экономики и управления Кафедра международных отношений и государственного управления г. Владивосток, ул. Гоголя. 41. ауд. 1527	Прибыл «25» мая 2026 г.	<i>печать</i>
ФГБОУ ВО «ВВГУ», Институт международного бизнеса, экономики и управления Кафедра международных отношений и государственного управления г. Владивосток, ул. Гоголя. 41. ауд. 1527	Убыл «18» июля 2026 г.	<i>печать</i>

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ МЕЖДУНАРОДНОГО БИЗНЕСА, ЭКОНОМИКИ И УПРАВЛЕНИЯ
КАФЕДРА МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

СОГЛАСОВАНО

УТВЕРЖДАЮ



Зав. кафедрой МОГУ, канд. экон. наук, доцент
И.В. Попова
«22» мая 2026 г

Канд. истор наук, доцент
А.А. Ким
«22» мая 2026 г

РАБОЧИЙ ГРАФИК (ПЛАН)

на выполнение отчета по производственной научно-исследовательской практики (НИР)

Магистранта Сыровец Никиты Андреевича
(Ф.И.О.)

Группы ММО-25-МО1 курса 1 направления обучения 41.04.05 Международные отношения. Международные отношения и приграничное сотрудничество

Место прохождения практики: ФГБОУ ВО «ВВГУ», Институт международного бизнеса, экономики и управления, кафедра международных отношений и государственного управления (МОГУ), г. Владивосток, ул. Гоголя, 41, ауд. 1527, тел. (243)240-41-60

Сроки прохождения практики: с «25» мая 2026 г. по «18» июля 2026 г.

№ п/п	Этапы (периоды) практики НИР	Вид работ	Срок прохождения этапа (периода) практики	Форма отчетности
1	Организационный этап	1.Организационное собрание (конференция) для разъяснения целей, задач, содержания и порядка прохождения практики 2. Разработка индивидуального задания.	22.05.2026	1.Решение выпускающей кафедры о назначении дня собрания. 2. Индивидуальное задание, утвержденное руководителем практики от ВВГУ
2	Основной этап (совместный руководителей практики рабочий график (план))	1.Прохождение инструктажа по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего распорядка. 2.Сбор информации. 3.Обработка, систематизация и анализ фактического и теоретического материала.	28.05.2026 - 18.07.2026	Выполнение индивидуального задания, утвержденного руководителем практики от ВВГУ
3	Заключительный	Составление отчета по практике Защита отчета по практике	18.07.2026	Отчет, экзаменационная ведомость

№ п/п	Этапы (периоды) практики НИР	Вид работ	Срок прохождения этапа (периода) практики	Форма отчетности
	этап			

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ МЕЖДУНАРОДНОГО БИЗНЕСА, ЭКОНОМИКИ И УПРАВЛЕНИЯ
КАФЕДРА МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

на выполнение отчета по производственной научно-исследовательской практики (НИР)

Студент: Сыровец Н.А.

Группы: ММО-25-МО1

Тема ВКР: ИИ и цифровая инфраструктура как инструменты геополитического влияния в российско-китайских отношениях

Срок сдачи отчета: 18.07.2026 г.

Содержание отчета по практике:

Введение Цель, задачи практики. Используемые подходы и методы исследования. Информационная база написания отчета.

Раздел 1. Систематизировать и обобщить информационные источники. Обобщить и критически оценить результаты исследований российских и зарубежных ученых в области выбранной темы ВКР

- 1.1 Осуществить подбор, систематизацию и обобщение информационных источников.
- 1.2 Обобщить и критически оценить результаты исследований российских ученых в области выбранной темы ВКР.
- 1.3 Обобщить и критически оценить результаты исследований зарубежных ученых в области выбранной темы ВКР.

Раздел 2. Представить содержание теоретической части (1й главы) магистерской диссертации в текстовом изложении

- 2.1 Сформировать текст 1-й главы магистерской диссертации, используя принципы планирования и проведения научного исследования и экспертно-аналитической работы на подготовительном этапе исследовательского процесса.
- 2.2 Подготовить текст для публикации по материалам научного исследования для публикации в научном издании.

Заключение: сформулировать основные выводы по итогам проведенного исследования, сделать заключение о достижении поставленной цели и решении обозначенных задач.

Список использованных источников (не менее 30-ти позиций не ранее 2022 года издания).

Приложение А. Текст статьи по материалам проведенного исследования для публикации в научном издании

Оригинальность текста работы не менее 70% с учётом цитирования. При возникновении подозрения на использование ИИ работа возвращается на доработку.

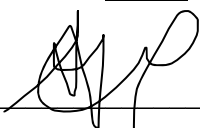
Руководитель практики от кафедры

Канд. истор. наук, доцент


_____ Ким А.А.

Задание получил:

Магистрант группы ММО-25


_____ Сыровец Н.А.

Дата 22.05.2026 г

ОТЗЫВ

руководителя практики от профильной организации
об обладании магистрантом компетенциями

В результате прохождения практики магистрант Сыровец Никита Андреевич показал обладание следующими компетенциями на следующем уровне:

Код компетенции, индикатора	Формулировка компетенции, индикатора	Сформированы полностью	В целом сформированы	Не в полной мере сформированы	Не сформированы
1	2	3	4	5	6
ОПК-3 Способен оценивать, моделировать и прогнозировать глобальные, макрорегиональные, национально-государственные, региональные и локальные политико-культурные, социально-экономические и общественно-политические процессы на основе применения методов теоретического и эмпирического исследования и прикладного анализа					
ОПК - 3.2К	Использует методы теоретического и эмпирического исследования и прикладного анализа по профилю деятельности в оценке и моделировании глобальных, макрорегиональных, национально-государственных, региональных и локальных политико-культурных, социально-экономических и общественно-политических процессов				
ОПК-4 Способен проводить научные исследования по профилю деятельности, в том числе в междисциплинарных областях, самостоятельно формулировать научные гипотезы и инновационные идеи, проверять их достоверность					
ОПК - 4.1К	Анализирует результаты исследований по профилю деятельности, устанавливает причинно-следственные связи между отдельными процессами и показателями, выявляет тенденции и закономерности, в том числе в междисциплинарных областях				
ОПК - 4.2К	Самостоятельно формулирует научные гипотезы и инновационные идеи, проверяет их достоверность				

Продолжение Таблицы

1	2	3	4	5	6
ОПК-5 Способен выстраивать стратегию по продвижению публикаций по профилю деятельности в средствах массовой информации на основе базовых принципов медиаменеджмента					
ОПК - 5.2К	Компилирует дайджесты и аналитические материалы по профилю деятельности для публикации в научных журналах и средствах массовой информации				
ОПК-7 Способен самостоятельно выстраивать стратегии представления результатов своей профессиональной деятельности, в том числе в публичном формате, на основе подбора соответствующих информационно-коммуникативных технологий и каналов распространения информации					
ОПК 7.2К	Обобщает результаты своей профессиональной деятельности и научно-исследовательской работы в публичном формате				
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий					
УК-1.4В	Вырабатывает стратегию действий в научно-исследовательской и экспертно-аналитической деятельности				
УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия					
УК-4.3К	Демонстрирует умение выполнять перевод академических текстов с иностранного на государственный язык				
УК-5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия					
УК-5.3К	Соблюдает требования уважительного отношения к культурным традициям различных национальных и социальных групп в процессе межкультурного взаимодействия				

Руководитель от профильной организации

Зав. кафедрой МОГУ

канд. экон. наук, доцент

Попова И.В.

Приложение А

Текст статьи по материалам проведенного исследования для публикации в научном издании

Цифровой суверенитет Российской Федерации в условиях усиления технологического влияния КНР

Сыровец Никита Андреевич

Магистрант направления международные отношения

Гр ММО-25-МО1

Научный руководитель: Николенко Анастасия Алексеевна

Доктор политических наук, доцент

ФБГОУ ВО «Владивостокский государственный университет»

Россия. Владивосток

E-mail: gogleva2002@gmail.com; Тел. +79242346612

ул. Гоголя, 41, г. Владивосток, Приморский край, Россия, 690014

Аннотация.

Цель исследования — выявить, каким образом усиление китайского технологического влияния отражается на цифровом суверенитете России и ее внешнеполитических возможностях.

В статье рассматривается проблема цифрового суверенитета России в контексте роста технологического влияния Китая. Особое внимание уделяется тому, как развитие российско-китайского сотрудничества в цифровой сфере влияет на возможности России сохранять самостоятельность в принятии политических и экономических решений. Анализируются основные направления технологической зависимости, а также преимущества, которые дает взаимодействие с КНР в условиях внешнего давления и санкций. В работе цифровой суверенитет понимается как способность государства контролировать цифровую инфраструктуру, данные и технологические стандарты. Делается вывод о том, что сотрудничество с Китаем одновременно выступает и ресурсом адаптации, и источником долгосрочных рисков асимметричной зависимости.

Методология исследования:

1. Сравнительный анализ - Сравнение технологического влияния Китая на Россию с влиянием США на Европу (GDPR vs российские законы о данных). Выявляются общие закономерности технологической зависимости;
2. Контент-анализ - Российские стратегические документы: «Цифровая экономика РФ» (2017-2030), закон «О суверенном интернете» (2019), доктрина кибербезопасности;
3. Кейс-стади - Российские ЦОД на китайском оборудовании — инфраструктурная зависимость;
4. Политический анализ экспертных материалов - Отчеты Роскомнадзора и Минцифры РФ.

Ключевые слова и словосочетания: цифровой суверенитет; цифровая инфраструктура; технологическая зависимость; импортозамещение; кибербезопасность; ИИ-сотрудничество; санкции и цифровизация; технологическая асимметрия.

Digital Sovereignty of the Russian Federation in the Context of Growing Technological Influence of the People's Republic of China

Syrovets Nikita Andreevich

Master's student in International Relations

Group MMO-25-MO1

Scientific supervisor: Nikolenko Anastasia Alekseevna

Doctor of Political Sciences, Associate Professor

Vladivostok State University

Russia. Vladivostok

E-mail: gogleva2002@gmail.com; Tel. +79242346612

41 Gogol Street, Vladivostok, Primorsky Krai, Russia, 690014

Abstract.

The purpose of this study is to identify how the growing Chinese technological influence affects Russia's digital sovereignty and its foreign policy capabilities.

The article examines the issue of Russia's digital sovereignty in the context of China's growing technological influence. It focuses on how the development of Russian-Chinese cooperation in the digital sphere affects Russia's ability to maintain its independence in making political and economic decisions. The article analyzes the main areas of technological dependence and the advantages that cooperation with China provides in the face of external pressure and sanctions. Digital sovereignty is defined as a state's ability to control its digital infrastructure, data, and technological standards. The article concludes that cooperation with China is both a resource for adaptation and a source of long-term risks of asymmetric dependence.

Research methodology:

1. Comparative analysis - Comparison of China's technological influence on Russia with the influence of the United States on Europe (GDPR vs Russian data laws). Common patterns of technological dependence are identified;

2. Content analysis - Russian strategic documents: "Digital Economy of the Russian Federation" (2017-2030), the law "On the Sovereign Internet" (2019), and the Cybersecurity Doctrine;

3. Case study - Russian data centers using Chinese equipment - infrastructure dependence;

4. Political analysis of expert materials - Reports by Roskomnadzor and the Ministry of Digital Development of the Russian Federation.

Keywords and phrases: *digital sovereignty; digital infrastructure; technological dependence; import substitution; cybersecurity; AI cooperation; sanctions and digitalization; technological asymmetry.*

Введение

Контроль над цифровой инфраструктурой, потоками данных и технологическими стандартами стал одним из ключевых компонентов национальной безопасности и внешнеполитической мощи в XXI веке. Понятие «цифровой суверенитет» выходит за рамки традиционного понимания суверенитета: оно включает способность государства осу-

пеществлять надзор и управление цифровыми сетями, хранением и передачей данных, а также формировать и внедрять технологические стандарты, обеспечивающие устойчивость критической цифровой инфраструктуры к внешнему давлению и санкциям [источник: ВШЭ, «Искусственный интеллект как инструмент цифрового суверенитета»].

Для Российской Федерации тема цифрового суверенитета актуальна вдвойне. С одной стороны, введённые против России экономические и технологические санкции усиливают необходимость поиска альтернативных каналов доступа к технологиям, оборудованию и инвестициям. С другой стороны, эти ограничения обнажают уязвимости национальной цифровой архитектуры и вынуждают принимать решения в условиях ограниченного выбора поставщиков и технологий. На этом фоне интенсивность и глубина технологического взаимодействия с КНР значительно возросли: телекоммуникационные проекты, поставки сетевого и дата-центрального оборудования, кооперация в области искусственного интеллекта и совместные стандартизационные инициативы стали важными элементами двусторонних отношений [источник: РИСИ/РСМД, «Практика цифрового суверенитета в России и КНР»].

Рост китайского технологического присутствия представляет для России двойственный феномен. В краткосрочной перспективе сотрудничество с Китаем открывает возможности для обхода санкционных ограничений, ускорения цифровой трансформации и укрепления некоторых элементов инфраструктуры. В долгосрочной перспективе активизация китайского влияния порождает риск асимметричной зависимости: критические компоненты цифровой экосистемы и ключевые цепочки поставок могут оказаться под контролем внешнего актора, что ограничит политическую и экономическую автономию России и поставит под сомнение реальные масштабы её цифрового суверенитета [источник: РСМД, «Геополитика центров обработки данных: опыт США и Китая, выводы для России»].

Цель данного исследования — выявить, каким образом усиление технологического влияния КНР отражается на цифровом суверенитете России и её внешнеполитических возможностях. В работе цифровой суверенитет трактуется как способность государства контролировать цифровую инфраструктуру, данные и технологические стандарты в интересах национальной безопасности и экономической независимости. В фокусе анализа находятся не только технические и инфраструктурные аспекты (поставки оборудования, совместные проекты, ЦОД), но и институционально-нормативные механизмы (регулирование данных, стандартизация, контроль доступа), а также геополитические последствия

этих трансформаций [источник: Дипакадемия, «Искусственный интеллект и геополитика»].

Предполагаемая исходная гипотеза исследования состоит в том, что сотрудничество с Китаем одновременно является важным ресурсом адаптации России к внешним технологическим ограничениям и источником системных рисков асимметричной технологической зависимости. Верификация этой гипотезы требует интеграции эмпирических данных о поставках и инвестициях, качественного анализа нормативной базы и экспертных оценок, а также рассмотрения сценариев развития технологического взаимодействия с учётом политических и экономических ограничений [источник: «Взаимодействие РФ и КНР в области искусственного интеллекта», 2025].

Структура статьи следующая: раздел I раскрывает теоретико-методологические основы анализа цифрового суверенитета; раздел II анализирует масштаб и направления китайской цифровой экспансии; раздел III рассматривает форматы российско-китайского сотрудничества; раздел IV оценивает преимущества и риски углубления технологического сотрудничества; раздел V предлагает стратегические рекомендации и сценарии развития; заключение подводит итоги исследования.

I. Теоретико-методологические основы анализа цифрового суверенитета

1.1. Понятие цифрового суверенитета: контроль над данными, инфраструктурой и технологическими стандартами

Цифровой суверенитет в современной литературе по международным отношениям и политической науке трактуется как способность государства обеспечивать контроль над ключевыми элементами цифровой среды — инфраструктурой, потоками и хранением данных, а также технологическими стандартами, определяющими архитектуру и правила функционирования цифровых систем. В отличие от классического понимания суверенитета, сфокусированного на территориальной целостности и монополии на легитимное насилие, цифровой суверенитет смещает акцент на контроль над нематериальными, но критически важными активами: каналами передачи информации, серверными мощностями, алгоритмическими платформами и нормативными режимами, регулирующими их использование.

В условиях глобализации цифровые потоки пересекают национальные границы с беспрецедентной скоростью, а ключевые элементы инфраструктуры зачастую находятся

под контролем транснациональных корпораций или иностранных государств. Это создаёт фундаментальное напряжение между экономической эффективностью глобальной интеграции и политической потребностью в национальной автономии. Государства, стремящиеся сохранить цифровой суверенитет, вынуждены искать баланс между открытостью к международному сотрудничеству и защитой критически важных цифровых активов от внешнего влияния.

В контексте данного исследования цифровой суверенитет понимается через три взаимосвязанных измерения:

- **Инфраструктурное измерение:** контроль над физическими и логическими компонентами цифровой среды (центры обработки данных, телекоммуникационные сети, оборудование, программное обеспечение). Способность государства обеспечивать независимость критической инфраструктуры от внешних поставщиков и операторов является базовым условием цифрового суверенитета.
- **Данные и информационные потоки:** способность регулировать сбор, хранение, обработку и трансграничную передачу данных, включая персональные данные, государственную информацию и коммерческие массивы. Контроль над данными становится инструментом как внутренней политики (защита приватности граждан, национальная безопасность), так и внешней (переговорная позиция в международных соглашениях, защита от цифрового шпионажа).
- **Технологические стандарты и нормативные режимы:** участие в формировании международных и национальных стандартов, определяющих архитектуру цифровых систем (протоколы связи, форматы данных, алгоритмические принципы). Государства, способные продвигать собственные стандарты или влиять на международное стандартизационное пространство, усиливают свой цифровой суверенитет и геополитическое влияние.

Важно отметить, что цифровой суверенитет не предполагает полной цифровой автаркии или изоляции от глобальных технологических цепочек. Напротив, в условиях взаимозависимости абсолютная автономия невозможна и экономически нецелесообразна. Речь идёт о способности государства сохранять стратегический контроль над критическими элементами цифровой экосистемы, минимизировать уязвимости от внешней зависимости и обеспечивать возможность самостоятельного принятия решений в ключевых сферах цифровой политики.

В российском контексте цифровой суверенитет эволюционирует от преимущественно декларативных мер (нормативные акты, стратегические документы) к практическим шагам по укреплению национальной цифровой инфраструктуры и снижению зависимости от иностранных технологий. Однако этот процесс сталкивается с серьёзными вызовами: ограниченностью отечественных технологических решений, необходимостью импорта критических компонентов (чипы, серверное оборудование, специализированное ПО) и растущим влиянием внешних акторов, среди которых КНР занимает всё более значимое место.

1.2. Теоретические подходы: неореализм, либерализм и многомерность цифрового суверенитета

Анализ цифрового суверенитета требует интеграции различных теоретических перспектив, каждая из которых выделяет определённые аспекты проблемы и предлагает специфические инструменты для её осмысления. В данном исследовании выделяются два ключевых теоретических подхода — неореализм и либерализм, — которые позволяют раскрыть многомерность цифрового суверенитета в контексте российско-китайских отношений.

Неореалистическая перспектива: технологии как ресурс национальной мощи

В неореалистической парадигме международные отношения рассматриваются как сфера конкуренции государств за власть и безопасность в условиях анархии международной системы. Технологии, включая цифровые, трактуются как стратегический ресурс, способный усиливать или ослаблять позиции государства в геополитической борьбе. С этой точки зрения, цифровой суверенитет становится инструментом обеспечения национальной безопасности и усиления относительной мощи государства.

Ключевые тезисы неореалистического подхода к цифровому суверенитету:

- Технологическая автономия как условие безопасности: зависимость от иностранных технологий создаёт уязвимости, которые могут быть экспортированы в условиях конфликта или геополитического давления.
- Цифровая инфраструктура как объект геополитической конкуренции: контроль над телекоммуникационными сетями, центрами обработки данных и ключевыми платформами становится ареной соперничества между великими державами.

- Технологические санкции как инструмент coercive diplomacy: ограничения на экспорт технологий используются как средство давления на государства-мишени.

В контексте российско-китайских отношений неореалистический подход позволяет объяснить, почему Россия, столкнувшись с западными технологическими санкциями, активно ищет альтернативы в сотрудничестве с КНР. Одновременно этот подход выявляет риски: замещение одной зависимости (западной) на другую (китайскую) может не решить проблему уязвимости, а лишь перенести её в иную плоскость.

Либералистическая перспектива: регуляторное сотрудничество и многосторонние форматы

В отличие от неореализма, либеральный подход акцентирует внимание на возможности сотрудничества между государствами через институты, нормы и взаимозависимость. С этой точки зрения, цифровой суверенитет не обязательно достигается через автаркию или технологическую изоляцию, но может укрепляться через участие в многосторонних форматах, гармонизацию регуляторных режимов и создание общих стандартов.

Ключевые тезисы либералистического подхода:

- Институциональное сотрудничество как инструмент защиты интересов: многосторонние форматы (БРИКС, ШОС, ЕАЭС) предоставляют государствам возможности для координации цифровых политик.
- Регуляторная гармонизация и стандарты: согласование правил трансграничной передачи данных, стандартов кибербезопасности и норм цифрового регулирования позволяет государствам создавать альтернативные экосистемы.
- Взаимозависимость как источник стабильности: экономическая и технологическая взаимозависимость между государствами может снижать вероятность конфликтов.

В контексте данного исследования либералистический подход позволяет рассмотреть российско-китайское сотрудничество не только через призму конкуренции и зависимости, но и как потенциальную платформу для развития альтернативных регуляторных и инфраструктурных решений.

Синтез подходов: многомерность цифрового суверенитета

Ни один из подходов в отдельности не способен полностью объяснить динамику цифрового суверенитета в условиях российско-китайского взаимодействия. В данном ис-

следовании применяется интегративный подход, сочетающий insights обоих направлений: цифровой суверенитет понимается одновременно как стратегический ресурс национальной мощи (неореализм) и как объект потенциального многостороннего сотрудничества (либерализм).

II. Китайская цифровая экспансия: масштаб и направления проникновения в российскую инфраструктуру

2.1. Инструменты экспансии КНР: «Цифровой шелковый путь», 5G-сети Huawei и облачные платформы

Китайская стратегия цифровой экспансии реализуется через комплекс взаимосвязанных инструментов, которые можно условно разделить на три уровня: геостратегический, инфраструктурный и сервисный.

Геостратегический уровень: «Цифровой шелковый путь»

Инициатива «Цифровой шелковый путь» (Digital Silk Road), запущенная в 2015 году как цифровое дополнение к инфраструктурному проекту «Один пояс — один путь», направлена на создание глобальной цифровой инфраструктуры, включающей прокладку оптоволоконных кабелей, строительство центров обработки данных, развитие спутниковых систем навигации (BeiDou) и продвижение китайских технологических стандартов в странах-партнёрах.

В контексте российско-китайских отношений «Цифровой шелковый путь» предоставляет институциональную рамку для углубления сотрудничества в сфере цифровых технологий. Россия интегрируется в эту архитектуру через совместные проекты в области телекоммуникаций, логистики данных и цифровизации транспортных коридоров. Однако участие несёт и риски: инфраструктурные проекты зачастую предполагают долгосрочную зависимость от китайского оборудования, программного обеспечения и технической поддержки.

Инфраструктурный уровень: 5G-сети Huawei

На инфраструктурном уровне ключевым инструментом китайской экспансии выступают телекоммуникационные решения, прежде всего 5G-сети, развёртываемые компанией Huawei. Несмотря на отсутствие официальных заявлений о полномасштабном развёртывании 5G от китайских вендоров в России, оборудование Huawei уже широко пред-

ставлено в российской телекоммуникационной инфраструктуре: базовые станции, маршрутизаторы, системы передачи данных.

Проблема зависимости от Huawei имеет несколько измерений: техническое (оборудование требует специфической экспертизы), политическое (доминирование одного вендора создаёт риски внешнего давления), безопасностное (потенциальные уязвимости в оборудовании).

Сервисный уровень: облачные платформы

На сервисном уровне китайская экспансия реализуется через облачные платформы и цифровые экосистемы, среди которых выделяются Alibaba Cloud, Tencent Cloud и Huawei Cloud. Эти платформы предлагают российским компаниям и государственным структурам альтернативу западным облачным сервисам (AWS, Microsoft Azure, Google Cloud), доступ к которым ограничен санкциями.

Преимущества китайских облачных платформ очевидны: доступ к современным технологиям, конкурентоспособные цены, отсутствие санкционных ограничений. Однако существуют и скрытые риски: данные, размещённые на китайских платформах, могут подпадать под юрисдикцию КНР, что создаёт потенциальные уязвимости для конфиденциальности и суверенитета данных.

2.2. Масштабы присутствия китайских решений в России: статистика, сегменты и фактор санкций

По оценкам аналитических агентств и отраслевых отчётов, к 2026 году доля китайских решений в отдельных сегментах российской IT-инфраструктуры превышает 30%, а в некоторых нишах (телекоммуникационное оборудование, серверное оборудование для ЦОД) достигает 50–60%. Этот рост произошёл преимущественно в период 2022–2026 годов, когда западные санкции создали вакуум, который быстро заполнили китайские поставщики.

Структура китайского присутствия в России:

- **Телекоммуникационное оборудование:** Huawei, ZTE занимают доминирующее положение в поставках оборудования для мобильных сетей (4G/5G), маршрутизаторов и коммутаторов. По некоторым оценкам, доля китайского оборудования в сетях российских операторов «большой тройки» превышает 60%.

- **Серверное оборудование и ЦОД:** китайские производители (Huawei, Inspur, Lenovo) стали ключевыми поставщиками серверов и систем хранения данных для российских дата-центров.
- **Программное обеспечение и платформы:** китайские решения в области управления базами данных, аналитики больших данных и искусственного интеллекта постепенно проникают в корпоративный и государственный секторы.
- **Потребительская электроника и экосистемы:** смартфоны (Xiaomi, Huawei, Oppo, Vivo), умные устройства и платформы (WeChat, Alipay) занимают значительную долю российского рынка.

Фактор санкций выступает ключевым драйвером роста китайского присутствия. После 2022 года российские компании столкнулись с ограничениями на импорт западных технологий. В этих условиях китайские поставщики стали практически единственной доступной альтернативой.

2.3. Технологический «мостик» для импортозамещения vs усиление асимметрии

Китайское технологическое присутствие в России выполняет функцию «мостика» для импортозамещения: оно позволяет временно компенсировать утрату доступа к западным технологиям. Однако эти выгоды сопровождаются структурными рисками:

- **Асимметрия технологической зависимости:** КНР выступает донором технологий, Россия — реципиентом.
- **Ограниченный трансфер технологий:** критические технологии остаются под контролем Китая.
- **Риски внешнего давления:** Китай может использовать технологическую зависимость как инструмент давления.
- **Стандарты и экосистемы:** интеграция в китайские технологические экосистемы ограничивает возможности для будущей диверсификации.

III. Форматы российско-китайского сотрудничества в цифровой сфере

3.1. Совместные проекты в области искусственного интеллекта

Сотрудничество между Россией и Китаем в сфере искусственного интеллекта (ИИ) представляет один из наиболее динамичных форматов цифрового взаимодействия. В

2024–2025 годах был запущен ряд совместных лабораторий ИИ на базе российских и китайских университетов и исследовательских центров. Примером служит сотрудничество между Сбером и Baidu в области машинного обучения, обработки естественного языка и компьютерного зрения.

Ключевые направления включают совместные исследовательские проекты, ограниченный обмен анонимизированными данными в приоритетных областях (медицина, транспорт, безопасность) и координацию позиций по вопросам регулирования ИИ в международных форматах (ООН, ШОС, БРИКС). В 2025 году на саммите ШОС была принята декларация о принципах этичного использования ИИ, разработанная совместно российскими и китайскими экспертами.

Однако сотрудничество сталкивается с ограничениями. Сохраняется асимметрия в технологических компетенциях: китайские компании обладают более развитыми платформами ИИ и большими массивами данных, тогда как российские партнёры часто выступают в роли локальных интеграторов. Реальный трансфер технологий остаётся минимальным: китайские компании не склонны делиться ключевыми алгоритмами и архитектурными решениями. Несмотря на прогресс в пилотных проектах, такие проекты позволяют России получать доступ к передовым технологиям и обучать кадры, даже если полный трансфер технологий не происходит.

3.2. Центры обработки данных и инфраструктурные проекты в рамках ШОС

Инфраструктурное сотрудничество в области центров обработки данных (ЦОД) реализуется преимущественно в рамках Шанхайской организации сотрудничества (ШОС). Идея создания трансграничной инфраструктуры ЦОД в пространстве ШОС направлена на снижение зависимости от западных облачных платформ и дата-центров, расположенных в потенциально недружественных юрисдикциях.

Проект предполагает строительство сети дата-центров на территории стран-участниц ШОС, объединённых высокоскоростными каналами связи и управляемых по единым стандартам безопасности. В 2025 году был запущен пилотный проект ЦОД в Казахстане с участием китайских (Huawei, Alibaba) и российских («Ростелеком», «Яндекс») компаний. Общий объём инвестиций в инфраструктуру ЦОД в пространстве ШОС к 2026 году оценивается в 15–20 млрд долларов.

Для России участие в таких проектах имеет двойственное значение. С одной стороны, это открывает доступ к современным инфраструктурным решениям и обеспечивает резервирование данных в «дружественных» юрисдикциях. С другой стороны, доминирование китайских компаний в строительстве и эксплуатации ЦОД создаёт риски зависимости: ключевые компоненты инфраструктуры поставляются китайскими вендорами, а техническая поддержка контролируется из КНР. Вопросы суверенитета данных остаются острыми: даже если данные физически хранятся на территории России, их логическое управление может осуществляться через китайские платформы.

3.3. Гармонизация стандартов кибербезопасности и цифрового регулирования

Третий формат сотрудничества — координация подходов к кибербезопасности и цифровому регулированию, включая стандарты защиты данных, требования к оборудованию и нормы трансграничной передачи информации. Это сотрудничество развивается как на двусторонней основе, так и в многосторонних форматах (ШОС, БРИКС, ООН).

Ключевые направления включают принципы «интернет-суверенитета» (право государств регулировать интернет-пространство на своей территории), стандарты кибербезопасности (защита критической информационной инфраструктуры, сертификация оборудования), регулирование трансграничной передачи данных (локализация персональных и государственных данных) и стандарты для ИИ. В 2025 году была принята «Дорожная карта по кибербезопасности ШОС», включающая общие стандарты для ЦОД.

Гармонизация стандартов упрощает вывод китайских решений на российский рынок и создаёт правовую определённость для инвесторов. Однако существуют риски: стандарты ШОС/БРИКС могут не быть совместимы с режимами других стран, китайские стандарты могут не оптимально подходить для российских условий, а гармонизация может закрепить технологическую зависимость. Тем не менее, для России участие в гармонизации стандартов представляет важный инструмент усиления переговорной позиции и продвижения альтернативных западным норм.

3.4. Расширение доступа к инфраструктуре при сохранении зависимости

Четвёртый формат — практическая интеграция российских пользователей в китайские технологические экосистемы через расширение доступа к инфраструктуре (облачные платформы, телекоммуникационные сети, оборудование ЦОД) при сохранении структурной зависимости от китайских поставщиков.

К 2026 году около 15% российских компаний среднего и крупного бизнеса используют китайские облачные сервисы (Alibaba Cloud, Tencent Cloud, Huawei Cloud) для хранения и обработки данных. Российские операторы, использующие оборудование Huawei и ZTE, де-факто интегрируются в китайские архитектурные решения и протоколы. Число российских пользователей WeChat оценивается в 3–5 млн человек, преимущественно среди предпринимателей, работающих с Китаем.

Этот формат отражает фундаментальную дилемму: необходимость интеграции в доступные технологические экосистемы против стремления к технологической автономии. Возможные стратегии балансирования включают диверсификацию поставщиков, локализацию критических компонентов (в 2025 году был запущен завод по сборке серверов Huawei в Калужской области), развитие национальных платформ и участие в многосторонних форматах. Россия вынуждена интегрироваться в доступные экосистемы для выживания в условиях санкций, но должна делать это стратегически, минимизируя долгосрочные риски.

IV. Преимущества и риски углубления технологического сотрудничества с КНР

4.1. Преимущества для России

Углубление технологического сотрудничества с Китаем предоставляет России ряд существенных преимуществ в условиях западных санкций.

Доступ к технологиям: после 2022 года Китай стал практически единственной доступной альтернативой западным технологиям. Китайские производители (SMIC, Huawei HiSilicon) предлагают чипы среднего и базового уровня. В 2025 году Китай поставил в Россию чипов на сумму около 2 млрд долларов. Alibaba Cloud, Tencent Cloud, Huawei Cloud предоставляют инфраструктуру для хранения и обработки данных. В 2025 году Alibaba Cloud открыла второй дата-центр в России.

Обход санкций: китайские вендоры не подвержены ограничениям на работу с российскими клиентами. Часть технологий поступает через реэкспорт из стран Центральной Азии и Кавказа. Расчёты в юанях и использование китайских платёжных систем (CIPS) позволяют оплачивать технологии. В 2025 году доля расчётов в юанях в российско-китайской торговле превысила 70%.

Укрепление инфраструктуры: оборудование Huawei и ZTE позволяет развивать сети 4G и готовиться к 5G. Китайские серверы замещают западные аналоги в российских дата-центрах. В 2024–2025 годах доля китайского оборудования в закупках российских операторов выросла с 45% до 65%. Более 50 российских компаний внедрили китайские системы компьютерного зрения.

В краткосрочной перспективе это критически важно для выживания и адаптации России.

4.2. Риски и уязвимости

Однако преимущества сопровождаются серьёзными рисками.

Утечка данных: согласно китайскому законодательству о национальной безопасности, китайские компании обязаны предоставлять доступ к данным по запросу государственных органов КНР. Российские пользователи часто не имеют полной информации о том, где хранятся их данные. Потенциальные уязвимости в оборудовании могут быть использованы для сбора информации. Рост доли WeChat и Alipay создаёт дополнительные каналы для сбора данных о пользователях.

Стандартизация под китайские нормы: использование оборудования Huawei и ZTE означает интеграцию в китайские архитектурные решения. Миграция данных на китайские платформы создаёт зависимость от специфических API. Гармонизация российских стандартов с китайскими нормами может закрепить зависимость и ограничить взаимодействие с другими юрисдикциями.

Долгосрочная зависимость: функционирование инфраструктуры зависит от обновлений ПО и технической поддержки, контролируемых китайскими вендорами. Критические технологии остаются под контролем Китая. В случае геополитических разногласий Китай может использовать технологическую зависимость как инструмент давления. Широкое использование оборудования Huawei создаёт ситуацию, при которой альтернативы практически отсутствуют.

Эти риски носят структурный характер и могут подрывать цифровой суверенитет в долгосрочной перспективе.

4.3. Сближение с Китаем как вынужденная адаптация

Сближение с Китаем представляет собой вынужденную адаптацию: Россия принимает Китай как единственную доступную альтернативу в условиях беспрецедентного западного давления.

В краткосрочной перспективе (3–5 лет) сотрудничество обеспечивает непрерывность функционирования инфраструктуры, экономическую стабильность и технологическое развитие. Китайские поставки позволяют поддерживать работу телекоммуникационных сетей, ЦОД и цифровых сервисов.

В долгосрочной перспективе (5–15 лет) накопление структурной зависимости создаёт серьёзные вызовы: потерю стратегической гибкости, ограничение национального технологического развития, риски внешнего давления и вопросы суверенитета данных.

Для балансирования необходима стратегия диверсификации партнёров (Индия, Турция, страны ASEAN, Персидский залив), участия в многосторонних форматах (ШОС, БРИКС), инвестиций в национальные решения и локализации критических компонентов. Сближение с Китаем усиливает краткосрочную устойчивость, но создаёт долгосрочные вызовы для цифрового суверенитета, требующие стратегического управления.

V. Стратегические рекомендации и сценарии развития

5.1. Развитие совместных стандартов в рамках ШОС

Первый приоритет — развитие совместных стандартов и инфраструктур в рамках многосторонних институтов (ШОС, БРИКС). Это позволяет снижать зависимость от любого единственного актора через создание коллективных альтернативных экосистем.

Ключевые направления: гармонизация стандартов кибербезопасности, создание трансграничных ЦОД, совместные стандарты для ИИ, единые правила трансграничной передачи данных. Преимущества: снижение зависимости от ^{одного} актора, усиление переговорной позиции, экономия ресурсов, политическая легитимность. Ограничения: разногласия между участниками, риск доминирования Китая, ограниченная совместимость с другими юрисдикциями.

5.2. Инвестиции в отечественные технологические аналоги

Второй приоритет — целевые инвестиции в развитие отечественных технологических решений в критических сегментах.

Ключевые направления: отечественные облачные платформы и ЦОД, операционные системы (на базе Linux), телекоммуникационное оборудование, решения в области кибербезопасности. Механизмы: государственные программы и гранты, налоговые льготы, преференции в госзакупках, венчурное финансирование, образовательные программы.

Ожидаемые результаты: снижение зависимости от иностранных поставщиков, создание основы для долгосрочного технологического суверенитета, развитие национальных компетенций. Однако существуют вызовы: ограниченность ресурсов, конкуренция с иностранными решениями, риск неэффективного использования средств.

5.3. Переход от реактивной модели к стратегическому партнёрству

Третий приоритет — переход от реактивной модели (ответ на санкции) к проактивной стратегии, основанной на долгосрочном планировании.

Ключевые элементы: долгосрочное планирование (дорожные карты на 10–15 лет), сегментация и приоритизация (критические vs некритические сегменты), сбалансированное внешнее сотрудничество (диверсификация партнёров, переговоры о трансфере технологий), институциональная координация (межведомственный орган), мониторинг и оценка рисков.

Переход требует изменения менталитета: от восприятия сотрудничества как вынужденной адаптации к пониманию его как инструмента достижения стратегических целей при сохранении контроля над критическими элементами.

5.4. Сценарии развития

Сценарий 1: Углубление асимметричной зависимости. Россия продолжает полагаться на китайские технологии. Доля китайских решений растёт, трансфер технологий остаётся минимальным. Краткосрочная устойчивость, но долгосрочные риски усиливаются.

Сценарий 2: Сбалансированное партнёрство с диверсификацией. Россия сохраняет сотрудничество с Китаем, но диверсифицирует партнёров и развивает отечественные решения в критических сегментах. Доля китайских технологий стабилизируется. Сбалансированная устойчивость и сохранение гибкости.

Сценарий 3: Ускоренное развитие национальных решений. Россия делает ставку на масштабные инвестиции в отечественные технологии. Сотрудничество с Китаем носит вспомогательный характер. Долгосрочная устойчивость и максимальная гибкость, но высокие краткосрочные издержки.

Реалистичный подход предполагает комбинирование элементов разных сценариев: в критических сегментах — стремление к сценарию 3, в коммерческих — сценарий 2, в условиях острого санкционного давления — временный сценарий 1 с планом перехода к более сбалансированным моделям.

Заключение

Проведённое исследование подтвердило гипотезу о двойственном характере технологического влияния Китая на цифровой суверенитет Российской Федерации. Сотрудничество с КНР одновременно выступает важным ресурсом адаптации и источником долгосрочных рисков асимметричной зависимости.

Ключевые выводы:

- Цифровой суверенитет — многомерное понятие, включающее контроль над инфраструктурой, данными и технологическими стандартами.
- Масштаб китайской цифровой экспансии в Россию значителен: к 2026 году доля китайских решений в отдельных сегментах превышает 30%.
- Форматы сотрудничества разнообразны (ИИ, ЦОД, стандарты, экосистемы) и несут как выгоды, так и риски.
- Преимущества проявляются в краткосрочной перспективе, риски накапливаются в долгосрочной.
- Для балансирования необходима комплексная стратегия: многосторонние форматы, инвестиции в отечественные решения, диверсификация партнёров, мониторинг и адаптация.

Для сохранения цифрового суверенитета России нужно перейти от реактивной модели к стратегическому партнёрству с элементами технологической автономии. Это означает сохранение сотрудничества с Китаем там, где это необходимо, одновременные инвестиции в отечественные решения в критических сегментах, активную диверсификацию партнёров и постоянный мониторинг баланса выгод и рисков.

Цифровой суверенитет в XXI веке — это не автаркия и не изоляция, а способность государства контролировать свою цифровую судьбу в условиях глобальной взаимозависимости и технологической конкуренции.

Список использованных источников

1. Дипакадемия. Искусственный интеллект и геополитика. Доклад. 2024.
2. РИСИ/РСМД. Практика цифрового суверенитета в России и КНР. Аналитический доклад. 2025.
3. РСМД, АНО «Колаборатория». Геополитика центров обработки данных: опыт США и Китая, выводы для России. Доклад. 2024.
4. ВШЭ. Искусственный интеллект как инструмент цифрового суверенитета. Исследование. 2023–2024.
5. Вестник МГИМО-Университета. Статьи по цифровой геополитике и ИИ. 2024–2026.
6. Постсоветский материк. Профильные статьи по российско-китайским отношениям. 2024–2026.
7. Взаимодействие РФ и КНР в области искусственного интеллекта. NEA. 2025.
8. Совместные российско-китайские проекты в сфере ИИ и цифровых технологий. ВЭФ/МК. 2025.
9. Русский совет по международным делам (russiancouncil.ru). Аналитика по ИИ, ЦОД и РФ-КНР.
10. Валдайский клуб (ru.valdaiclub.com). Экспертная аналитика по цифровому суверенитету.

Ректору ФГБОУ ВО «ВВГУ»
профессору Т.В. Терентьевой
магистранта Н.А. Сыровец
группы ММО-25-МО1

ЗАЯВЛЕНИЕ

Прошу направить меня на учебную практику НИР (получение навыков научно-исследовательской работы)

(указать вид и тип практики)

В профильную организацию

ФГБОУ ВО «ВВГУ», Институт международного бизнеса, экономики и управления, кафедры международных отношений и государственного управления (МОГУ), находящуюся по адресу¹: Приморский край, г. Владивосток, ул. Гоголя, 41, ауд. 1527, тел. (243)240-41-60

Договор о комплексном сотрудничестве между ВВГУ и профильной организацией заключен.

«22» мая 2026г.

дата

 / Н.А. Сыровец /

подпись

Ф.И.О.

телефон магистранта и e-mail

89244051785

nikitasyrovec@gmail.com
