

НОРМЫ И ПРАВИЛА

ИССЛЕДОВАТЕЛЬСКАЯ СТАТЬЯ

СУВЕРЕННЫЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ ПОДХОДОВ В РОССИИ И ЗА РУБЕЖОМ

Дарья Александровна Королькова^аПетр Леонидович Отоцкий^бАлександр Сергеевич Юхно^б

EDN: XOYPDJ

^а Российская государственная академия интеллектуальной собственности^б Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации

Аннотация: Актуальность статьи обусловлена эволюцией технологий искусственного интеллекта (ИИ), которые становятся ключевым фактором экономической конкурентоспособности и стратегической устойчивости государств. Исследование направлено на выявление и систематизацию концептуальных подходов к пониманию суверенного ИИ, закрепленных в официальных документах отдельных государств. В работе выделены три взаимосвязанных элемента суверенного ИИ: технологический суверенитет, доверенные технологии ИИ, обучение ИИ-моделей на национальных наборах данных. Акцент сделан не на формальной юридической силе документов, а на содержательной логике закрепленных подходов. В целях системного сопоставления подходов к суверенному ИИ в различных юрисдикциях выделены три аналитических уровня.

Ключевые слова: суверенный искусственный интеллект, суверенные модели искусственного интеллекта, национальные модели искусственного интеллекта, технологический суверенитет, технологическая независимость, доверенные технологии искусственного интеллекта, зарубежный опыт

Благодарность: Работа подготовлена в рамках государственного задания Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации.

Дата поступления статьи в редакцию: 27 июля 2026 года.

SOVEREIGN ARTIFICIAL INTELLIGENCE: A COMPARATIVE LEGAL ANALYSIS OF APPROACHES IN RUSSIA AND ABROAD

RESEARCH ARTICLE

Daria A. Korolkova^аPetr L. Ototsky^бAlexander S. Yukhno^б^а Russian State Academy of Intellectual Property^б Russian Presidential Academy of National Economy and Public Administration

Abstract: The relevance of this article driven by the development of artificial intelligence (AI) technologies, which are becoming a vital element in a country's economic competitiveness and long-term strategic sustainability. The study's goal is to find and organize ways to understand AI in the context of sovereignty, as outlined in the official documents of individual states. The research identifies three interrelated elements of sovereign AI. These elements are technological sovereignty, trusted AI technologies, and the training of AI models using national datasets. Rather than focusing on the formal legal force of the documents, the authors emphasize the substantive logic of the approaches set forth therein. To systematically analyze approaches to sovereign AI across various jurisdictions, the article identifies three analytical levels: legal, economic, and strategic.

Keywords: sovereign artificial intelligence, sovereign artificial intelligence models, national artificial intelligence models, technological sovereignty, technological independence, trusted artificial intelligence technologies, international experience

Acknowledgment: The work was completed as part of the state assignment of the Russian Presidential Academy of National Economy and Public Administration.

Received: July 27, 2026.

Введение

В условиях глобальной конкуренции и геополитической нестабильности особую остроту приобретает задача обеспечения технологической независимости государств, что предполагает поиск оптимальных механизмов защиты суверенитета в сфере искусственного интеллекта (ИИ).

Суверенный ИИ подразумевает способность государства самостоятельно создавать, обслуживать и внедрять ИИ-системы с минимальной внешней зависимостью¹. Такой подход имеет ключевое значение для национальной безопасности, системы государственного управления и международных отношений [Dale, 2025. P. 1–10].

Под «суверенным искусственным интеллектом» понимается способность государства или организации разрабатывать, внедрять и управлять системами искусственного интеллекта с использованием собственной инфраструктуры, данных и вычислительных ресурсов. Суверенный ИИ гарантирует, что ИИ-технологии разрабатываются и эксплуатируются в соответствии с национальными приоритетами, ценностями и нормативными требованиями².

Для суверенного ИИ характерным признаком является то, что он формируется как результат взаимодействия четырех разных компонентов: территориального (где физически находятся данные и вычислительные мощности), операционного (кто осуществляет управление данными и вычислительными мощностями, обеспечивает их безопасность), технологического (кому принадлежат базовые технологии ИИ, инфраструктурная основа и интеллектуальная собственность) и юридического (какая юрисдикция регулирует доступ к данным и соответствие требованиям к качеству данных, на которых обучаются ИИ-модели, и безопасности самих ИИ-моделей³).

В разных государствах концепция «суверенного ИИ» может использоваться для решения принципиально разных задач и приоритетов в ИИ-сфере, в том числе для удержания или достижения технологического лидерства, обеспечения экономических эффектов от применения ИИ, защищенности критической инфраструктуры, сохранения национально-культурной идентичности.

В настоящее время концепция «суверенного ИИ» может раскрываться через три взаимосвязанных направления:

1. Технологический суверенитет, то есть способность самостоятельно разрабатывать, производить и внедрять критические ИИ-технологии. Он подразумевает наличие в государстве собственных вычислительных мощностей (чипов, центров обработки данных), контролируемых моделей генеративного ИИ, национальных платформ с наборами данных.

2. Доверенные технологии ИИ⁴, то есть технологии, которые отвечают стандартам безопасности и разработаны с учетом принципов эффективности, недискриминации и этичности. При использовании они исключают возможность причинения вреда человеку, нарушения его прав и свобод, а также нанесения ущерба интересам общества и государства.

3. Обучение ИИ-моделей на национальных наборах данных, которые отражают выбранный культурный код и социальный контекст, локальные традиции, языки, религиозные и семейные ценности, а также стратегические приоритеты национального развития.

Ниже, в рамках обзора зарубежных подходов к суверенному ИИ, показано, что в разных странах используется одно или сочетание нескольких из указанных направлений, тогда как в России рассматриваются одновременно все три направления.

В условиях формирования цифровой экономики подход к раскрытию содержания суверенитета изменяется [Зиновьева, Булва, 2021. С. 42]. В настоящий момент создается новая реальность, в которой эффективность государственного управления и уровень защищенности национальных интересов напрямую зависят от способности государства создавать, адаптировать и безопасно эксплуатировать ИИ-решения. Именно в поиске баланса между инновациями и контролем начинается формироваться технологический суверенитет государства [Юхно, 2026. С. 164].

Согласно Концепции технологического развития Российской Федерации, под «технологическим суверенитетом» понимается наличие в стране (под национальным контролем) критических и сквозных технологий собственных линий разработки и условий производства продукции на их основе, что обеспечивает устойчивую возможность государства и общества достигать собствен-

1 What is sovereign artificial intelligence. <https://montrealethics.ai/what-is-sovereign-artificial-intelligence/>; Сотрудники GZERO, Премьер-министр Великобритании хочет «суверенного ИИ». <https://www.gzeromedia.com/gzero-ai/british-pm-wants-sovereign-ai>

2 Considerations Regarding Sovereign AI and National AI Policy. https://sovereign-ai.org/white_paper/

3 What Is Sovereign AI? <https://www.oracle.com/asean/artificial-intelligence/what-is-sovereign-ai/>

4 См.: Указ Президента Российской Федерации «О развитии искусственного интеллекта в Российской Федерации» от 10 октября 2019 года № 490. *Собрание законодательства Российской Федерации*. 2019. № 41, ст. 5700.

Нормы и правила

ные национальные цели развития и реализовывать национальные интересы⁵.

В документе уточняется, что технологический суверенитет обеспечивается в двух формах: исследование, разработка и внедрение критических и сквозных технологий; производство высокотехнологичной продукции на основе указанных технологий⁶. Конечная цель обеспечения технологического суверенитета заключается в защите национальных интересов. Эффективность его достижения измеряется в том числе таким целевым показателем, как снижение коэффициента технологической зависимости⁷.

В отечественной научной литературе раскрытию сущности технологического суверенитета уделяется значительное внимание. А.А. Афанасьев рассматривает вопросы реализации политики по достижению технологического суверенитета в России [Афанасьев, 2022. С. 2193–2212]. Т.Р. Гареевым проведен концептуальный и практический анализ технологического суверенитета, который рассматривается как кооперативная стратегия с элементами государственного контроля, неизбежно ведущая к технологическому протекционизму и фрагментации мировой торговли [Гареев, 2023. С. 38–54]. В исследовании Е.Б. Ленчук обосновывается объективная необходимость достижения технологического суверенитета для России вследствие высокой степени зависимости отечественной экономики от импорта в технологической сфере, что в условиях жестких внешних ограничений превращается в серьезное препятствие для дальнейшего развития государства [Ленчук, 2024. С. 232–237].

Е.С. Зиновьева и С.В. Шитьков анализируют подходы различных государств, включая Россию, Китай, США и государства БРИКС, к обеспечению независимости в цифровой сфере, а также обосновывают необходимость выработки международно-правовых норм в этой области [Зиновьева, Шитьков, 2023. С. 38–51]. Логика цифрового суверенитета соотносится с принципом необходимого доверия [Отоцкий, 2022. С. 2958–2975], в рамках которого существует некоторый оптимальный уровень доверия, обеспечивающий развитие цифрового общества. С этой позиции цифровая автаркия и полная зависимость от зарубежных поставщиков представляют собой два симметричных отклонения от необходимого уровня доверия.

Первая отсекает государство от глобальной сложности как ресурса развития, вторая – делает государство заложником внешних технологических субъектов.

18 марта 2026 года на федеральном портале проектов нормативных правовых актов был опубликован текст законопроекта «Об основах государственного регулирования сфер применения технологий искусственного интеллекта в Российской Федерации». В п. 4 ст. 4 этого законопроекта технологическая независимость определялась как «обеспечение самостоятельности Российской Федерации в области развития технологий искусственного интеллекта, в том числе путем разработки суверенных и национальных моделей искусственного интеллекта»⁸. Категория «модель искусственного интеллекта» трактовалась через дефиницию, закрепленную в Национальной стратегии развития ИИ до 2030 года, – как программа для ЭВМ, «предназначенная для выполнения интеллектуальных задач на уровне, сопоставимом с результатами интеллектуального труда человека или превосходящем их»⁹. По смыслу ч. 2 ст. 7 законопроекта, к суверенным и национальным моделям предлагалось предъявлять следующие требования: «все стадии разработки и обучения моделей искусственного интеллекта осуществляются на территории Российской Федерации»; «осуществляются гражданами Российской Федерации и российскими юридическими лицами»; «обучение моделей искусственного интеллекта с использованием наборов данных, формирование которых осуществляется на территории Российской Федерации гражданами Российской Федерации и российскими юридическими лицами»¹⁰.

26 июля 2026 года Президент Российской Федерации подписал Федеральный закон «О поддержке развития технологий искусственного интеллекта в Российской Федерации» № 243-ФЗ, направленный на создание правовых условий для ускоренного развития и внедрения ИИ и обеспечение технологического суверенитета. В п. 2 ст. 4 этого Закона технологическая независимость трактуется как «разработка больших фундаментальных моделей искусственного интеллекта и создание продукции с использованием таких моделей при сохранении национального контроля над критическими и сквозными технологиями на основе

8 <https://regulation.gov.ru/projects/166424>

9 П.п. «р» п. 1 Указа Президента РФ «О развитии искусственного интеллекта в Российской Федерации», которым утверждена Национальная стратегия развития искусственного интеллекта на период до 2030 года (от 10 октября 2019 года № 490). *Собрание законодательства Российской Федерации*. 2019. № 41. Ст. 5700.

10 <https://regulation.gov.ru/projects/166424/>

5 Распоряжение Правительства РФ «Об утверждении Концепции технологического развития на период до 2030 года» (вместе с «Концепцией технологического развития на период до 2030 года») от 20 мая 2023 года № 1315-р.

6 Там же.

7 Там же.

собственных линий разработки технологий в целях экспорта конкурентоспособной высокотехнологичной продукции и (или) замещения ею на внутреннем рынке продукции, создаваемой на базе устаревших и (или) иностранных технологий»¹¹. Акцент смещается с полной локализации в сторону контроля над критическими технологиями и создания конкурентоспособных продуктов, а также закрепления риск-ориентированного подхода к регулированию ИИ.

В ч. 2 ст. 6 данного Федерального закона закреплены критерии суверенной большой фундаментальной модели: разработчиком выступает российское юридическое лицо; российское юридическое лицо определяет и изменяет характеристики модели на всех стадиях ее жизненного цикла; обеспечивается полная техническая и технологическая воспроизводимость цикла разработки, включая обучение и матрицу исходных коэффициентов; подготовка ответов на запросы и хранение данных обеспечиваются в центрах обработки данных, расположенных на территории РФ и принадлежащих российским юридическим лицам; модель проходит подтверждение соответствия законодательству РФ и традиционным российским духовно-нравственным ценностям.

При этом следует подчеркнуть, что даже в рамках жесткого контура суверенной модели, предложенного в рассматриваемом Законе, доминирующими критериями выступают формальные признаки: гражданство разработчика и территориальная привязка процессов обработки данных. Содержательный аспект суверенитета (а именно – обучение модели на национальных наборах данных, транслирующих культурно-ценностный код и социальный контекст) не получает равнозначного нормативного закрепления. В результате конструкция суверенной модели тяготеет к юрисдикционно-географической, а не к культурно-содержательной парадигме, что снижает ее эффективность как инструмента сохранения и воспроизводства национальной идентичности в условиях технологической глобализации.

Согласно ч. 3 ст. 6 данного Закона, национальная большая фундаментальная модель допускает использование компонентов, разработанных за пределами РФ, но распространяемых на условиях открытой лицензии, при сохранении контроля над существенными характеристиками модели и соблюдении требований к локализации обработки данных и ценностному подтверждению.

В п. 6 ст. 4 Закон закрепляет принцип учета и уважения традиционных российских духовно-нравственных ценностей. Кроме того, в п. 9

ст. 4 закрепляется принцип безопасности, включающий «обеспечение информационной безопасности и устойчивости функционирования больших фундаментальных ИИ-моделей»¹². При этом критериев подтверждения соответствия законодательству и традиционным духовно-нравственным ценностям не предусматривается.

В п. 3 ч. 2 ст. 5 Федерального закона от 26 июля 2026 года № 243-ФЗ «О поддержке развития технологий искусственного интеллекта в Российской Федерации» обозначено, что Правительство РФ устанавливает случаи, в которых допускается применение исключительно суверенных и (или) национальных больших фундаментальных моделей (в банковской сфере и иных сферах финансового рынка – по согласованию с Центральным банком РФ), а также перечень исключений из них.

Таким образом, этот Закон интегрирует все три направления суверенного ИИ, выделенные в настоящем исследовании: технологический суверенитет (контроль над критическими и сквозными технологиями, собственные линии разработки – п. 2 ст. 4), доверенные технологии (риск-ориентированный подход, ценностное регулирование, безопасность – п. 5, 6, 9 ст. 4) и обучение на национальных наборах данных (требования к локализации обработки и хранения данных – ч. 2 и ч. 3 ст. 6).

Далее рассмотрим зарубежные подходы к пониманию концепции суверенного ИИ.

Зарубежные подходы к пониманию концепции «суверенного искусственного интеллекта»

В настоящее время концепция «суверенного ИИ» находится на стадии осмысления. Государства подходят к рассмотрению этого вопроса в зависимости от своих возможностей и положения в современной «гонке технологий ИИ». В данной части приведен обзор и сравнительный анализ подходов к правовой реализации суверенного ИИ в Европейском союзе, США, Китае, Корее, Сингапуре, Вьетнаме, Казахстане, а также ОАЭ и Саудовской Аравии. Выбор государств обусловлен важностью рассмотрения соответствующих политик стран, находящихся на разном уровне развития ИИ-технологий и использующих различные правовые инструменты. В конце раздела представлена сводная таблица по всем рассмотренным государствам на трех аналитических уровнях: правовом, экономическом и стратегическом. Список проанализированных государств не является избыточным, но показывает вариативность подходов к суверенному ИИ, позволяет оценить риски и возможности в этой области и выработать рекомендации для России.

¹¹ <http://publication.pravo.gov.ru/document/0001202607260003>

¹² Там же.

Нормы и правила

Опыт Европейского союза. Регламент ЕС об искусственном интеллекте (EU AI Act)¹³ не содержит ни термина «суверенный ИИ», ни «национальной платформы ИИ», ни «национальной инфраструктуры ИИ». Единственное косвенное упоминание относится к доверенным системам ИИ, которые призваны формировать высокий уровень доверия к ИИ-системам с высоким уровнем риска. Регламент требует обязательной проверки таких ИИ-систем перед введением в эксплуатацию, поскольку в ЕС акцент делается не на технологической независимости, а на безопасности, прозрачности и защите прав граждан.

Помимо рамочного регулирования, Европейский союз внедряет инициативы, прямо направленные на достижение технологической независимости, в частности, программу «Совместное предприятие в области высокопроизводительных вычислений» (EuroHPC JU), позволяющую координировать усилия государств-членов и объединять ресурсы для создания собственной инфраструктуры для суперкомпьютеров, обеспечивающей вычислительные мощности для обучения ИИ-моделей¹⁴. Одновременно с этим инициатива «Гайя-Икс» (Gaia-X) направлена на формирование безопасной, децентрализованной и федеративной европейской экосистемы данных, призванной предоставить бизнесу и государственным структурам альтернативу доминирующим американским и китайским облачным провайдерам¹⁵.

Вопросы технологического суверенитета ЕС также поднимаются в рамках инициативы «Суверенной облачной платформы» (Sovereign Cloud Stack (SCS))¹⁶, целью которой является создание открытой, прозрачной и независимой от поставщика облачной экосистемы, гарантирующей свободу выбора разработчиков и пользователей цифровых сервисов. Проект выделяет следующие четыре взаимосвязанных направления (SCS-1 – SCS-4):

- *суверенитет данных (SCS-1)* – возможность безопасно хранить и обрабатывать данные, контролировать их передачу третьим лицам;
- *возможность смены поставщика (SCS-2)*, предусматривающая предотвращение ситуации,

при которой использование проприетарного программного обеспечения привязывает заказчиков к одному поставщику;

- *технологический суверенитет (SCS-3)*, заключающийся в возможности свободно использовать, изучать, адаптировать и развивать облачные технологии;

- *оперативная компетентность (SCS-4)*, означающая документирование и прозрачность операционных процессов, позволяющая даже небольшим компаниям надежно управлять облачными платформами.

Перечисленные инициативы направлены на достижение технологической независимости ЕС в сфере ИИ, что компенсирует отсутствие в Регламенте ЕС об ИИ прямых требований к локализации разработок.

Опыт США. В отличие от рассмотренной выше модели, в США отсутствует единый кодифицированный документ об ИИ, который бы закреплял понятия «суверенный ИИ», «национальная платформа ИИ» или аналогичные им. Американский подход к обеспечению технологического лидерства и, по сути, суверенитета в этой сфере формируется преимущественно через подзаконные акты, в первую очередь через исполнительные указы Президента США. Ключевым документом в этой сфере является указ Президента США «Об устранении барьеров для американского лидерства в области искусственного интеллекта»¹⁷. Содержательно в этом указе делается ставка на национальную безопасность, предписывая федеральным ведомствам укреплять лидирующие позиции США в области развития ИИ.

В отличие от ЕС, который создает детальные требования к оценке соответствия систем высокого риска, или от Вьетнама и Казахстана с их жесткой привязкой к национальной инфраструктуре, США избирают дерегуляторную стратегию. Указ Президента США «Об устранении барьеров для американского лидерства в области искусственного интеллекта» прямо обязывает правительство США выявлять и отменять существующие правила, которые могут препятствовать безопасному развитию систем ИИ¹⁸.

2 июня 2026 года Президент США подписал исполнительный указ «Содействие передовым инновациям в области искусственного интеллекта и

13 The EU AI Act. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence of 13 June 2024. https://www.euaiaact.com/web_page_name

14 The European High Performance Computing Joint Undertaking (EuroHPC JU). https://www.eurohpc-ju.europa.eu/about/discover-eurohpc-ju_en

15 Gaia-X. <https://gaia-x.eu/>

16 The EU Commission's Cloud Sovereignty Framework. <https://sovereigncloudstack.org/en/the-european-commissions-cloud-sovereignty-framework/>

17 Removing Barriers to American Leadership in Artificial Intelligence. January 23, 2025. <https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence>

18 Там же.

Таблица 1. Уровни корпоративного суверенитета
Table 1. Levels of corporate sovereignty

Уровень суверенитета	Тип гарантии	Механизм обеспечения	Класс задач
Уровень 1. Собственное оборудование	Техническая (высокая)	Физически изолированная, самостоятельно размещенная инфраструктура на принадлежащих организации графических процессорах (GPU); отсутствие исходящей передачи данных	Секретные данные, ключевые корпоративные тайны
Уровень 2. Доверенные облачные вычисления	Техническая (средняя)	Арендуемые графические процессоры с аппаратным подтверждением исполнения и конфиденциальными вычислениями; работа в доверенной среде исполнения, подтверждаемая самим оборудованием и недоступная стороннему владельцу	Чувствительные рабочие процессы
Уровень 3. ИИ-сервисы без хранения пользовательских данных	Юридическая (средняя)	Закрытая модель, используемая под соглашением о нулевом хранении данных; гарантия основана на договоре, а не на физической изоляции вычислений	Повседневные нечувствительные задачи
Уровень 4. Прочие сторонние ИИ-сервисы	Юридическая (слабая)	Доступ через стандартный программный интерфейс (API) без соглашения о нулевом хранении данных; запросы и ответы могут сохраняться и использоваться оператором модели	Публичная и несущественная информация

Источник: Institutional Sovereignty in the Age of AI: 15 steps that every government and company can take to compound their alpha in the age of AI. Palantir Technologies. https://www.palantir.com/assets/xrfr7uokpv1b/7BF74dqqcPeVFMHRmy7F03/2a33ff9b4f9e11ba904445e637095960/Palantir_-_Institutional_Sovereignty_in_the_Age_of_AI.pdf?trk=article-ssr-frontend-pulse_little-text-block

Source: Institutional Sovereignty in the Age of AI: 15 steps that every government and company can take to compound their alpha in the age of AI. Palantir Technologies. https://www.palantir.com/assets/xrfr7uokpv1b/7BF74dqqcPeVFMHRmy7F03/2a33ff9b4f9e11ba904445e637095960/Palantir_-_Institutional_Sovereignty_in_the_Age_of_AI.pdf?trk=article-ssr-frontend-pulse_little-text-block

безопасности»¹⁹, который нацелен на поощрение инновационных разработок в области ИИ, ускорение ответственного внедрения его технологий в работу государственных органов и расширение использования ИИ-решений в промышленной сфере.

В указе содержатся конкретные поручения различным ведомствам и агентствам, включая усиление киберзащиты федеральных информационных систем, создание межведомственного центра по кибербезопасности ИИ и разработку директив для защиты критической инфраструктуры. Кроме того, документ предусматривает разработку процесса оценки кибервозможностей ИИ-моделей и определение порога, при котором модель может быть признана «защищенной передовой моделью». Также уделяется внимание борьбе с преступным использованием ИИ и защите американской интеллектуальной собственности в сфере ИИ-технологий.

Ключевая особенность закрепленного в указе подхода – отказ от чрезмерно обременительного регулирования, которое могло бы тормозить прогресс развития ИИ-сферы. Этот документ призван установить оптимальный баланс между активным стимулированием технологического развития в сфере искусственного интеллекта и надежной защитой национальной безопасности.

19 Executive Orders «Promoting advanced artificial intelligence innovation and security». June 2, 2026. <https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/>

Одновременно проблематика суверенного ИИ прорабатывается технологическими корпорациями. Например, в докладе «Институциональный суверенитет в эпоху искусственного интеллекта» компания «Palantir Technologies» переносит концепцию суверенного ИИ с государственного на корпоративный уровень, рассматривая суверенитет как право собственности организации на используемые ею данные и возможность использования ИИ без передачи критических данных посторонним лицам (операторам ИИ-сервисов). Доклад выделяет четыре уровня суверенитета (см. таблицу 1) и предлагает 15 практических шагов для обеспечения корпоративного суверенитета на основе принципа нулевого доверия к внешним поставщикам моделей²⁰. Любая передовая модель, используемая без соглашения об отсутствии хранения пользовательских данных, рассматривается как «склонная к извлечению» данных из организации.

Представленный подход существенно сужает категорию суверенитета, сводя ее к техническим параметрам контроля над данными и вынося за скобки государственно-правовой контекст. Между тем именно политико-правовое измерение,

20 Institutional Sovereignty in the Age of AI: 15 steps that every government and company can take to compound their alpha in the age of AI. Palantir Technologies. 07.2026. https://www.palantir.com/assets/xrfr7uokpv1b/7BF74dqqcPeVFMHRmy7F03/2a33ff9b4f9e11ba904445e637095960/Palantir_-_Institutional_Sovereignty_in_the_Age_of_AI.pdf?trk=article-ssr-frontend-pulse_little-text-block

Нормы и правила

включая национальное регулирование и юрисдикционные ограничения, остается за рамками анализа, что делает концепцию методологически уязвимой. Как следствие, предлагаемые практические рекомендации оказываются применимы лишь в корпоративном сегменте и не могут претендовать на универсальность.

Опыт Китайской Народной Республики (КНР). Подход, реализуемый КНР, заключается в создании своей ИИ-экосистемы (от производства чипов и вычислительной инфраструктуры до разработки фундаментальных ИИ-моделей и прикладных сервисов). Ключевыми инструментами выступают достаточно строгие правила о локализации данных, а также развитие собственных технологических стандартов, не ориентированных на совместимость с зарубежными аналогами²¹.

В августе 2025 года был опубликован документ «Мнения Государственного совета по углубленной реализации инициативы “Искусственный интеллект+”»²², который конкретизирует стратегию развития искусственного интеллекта в КНР до 2027, 2030 и 2035 годов. На первом этапе (до 2027 года) планируется усилить роль ИИ в государственном управлении и цифровой экономике, повысить уровень проникновения ИИ-агентов нового поколения в различные сферы жизни до 70 %, а также достичь интеграции ИИ-технологий в шести ключевых секторах экономики. К 2030 году в качестве целевого ориентира заявлено обеспечение устойчивого развития ИИ, что предполагает не только наращивание технологического потенциала, но и формирование завершенной институциональной и инфраструктурной среды для применения ИИ-решений в масштабах всей страны.

На общегосударственном уровне в КНР отсутствует единый закон об ИИ, аналогичный вьетнамскому или казахстанскому. Вместо этого для целей регулирования сферы ИИ используется сочетание отраслевых нормативных актов, национальных стандартов и руководств, обладающих «мягкой силой». Показательным примером является принятие стандарта прозрачности больших языковых моделей «Рекомендации по доверенным базовым моделям искусственного интеллекта»²³. Документ предполагает обязательный аудит источников обучения ИИ, интегрированную систему отслеживания

изменений параметров после релиза генеративных моделей, отдельный реестр для разработчиков ИИ (в том числе иностранных компаний), желающих оперировать на китайском рынке.

В 2020 году было выпущено Руководство по построению Национальной системы стандартов ИИ нового поколения²⁴, направленное на содействие непрерывному развитию ИИ-технологий в экосистеме с открытым исходным кодом. Документ определяет базовые этические нормы, безопасность эксплуатации, защиту данных и интеллектуальной собственности, учитывая различие целей и зон ответственности разработчиков, поставщиков и пользователей ИИ-решений²⁵.

В 2023 году Управлением киберпространства Китая совместно с еще несколькими национальными ведомствами были изданы «Временные меры по управлению службами генеративного искусственного интеллекта» (от 10 июля 2023 года)²⁶, вступившие в силу 15 августа 2023 года. Как указано в ст. 1, документ разработан в целях содействия здоровому развитию и регулируемому использованию генеративного искусственного интеллекта, сохранения национальной безопасности и учета общественных интересов, а также для защиты прав граждан и юридических лиц.

Помимо стратегического планирования и нормативно-технического регулирования, Китай реализует масштабную инфраструктурную инициативу, направленную на достижение технологической независимости как одного из ключевых компонентов суверенного ИИ. Так, национальная программа «Восточные данные – западные вычисления» является стратегической инициативой по перераспределению вычислительных ресурсов между экономически развитым востоком и обеспеченным ресурсами западом Китая. Ее суть заключается в создании национальной сети центров обработки данных, которая переносит ресурсоемкие вычислительные задачи (хранение архивов, обучение ИИ и др.) в западные регионы с дешевой возобновляемой энергией и холодным климатом, а задачи, не требующие значительных вычислительных мощностей, оставляет на востоке²⁷.

24 https://cset.georgetown.edu/wp-content/uploads/t0401_AI_standards_guidelines_EN.pdf

25 См. подробнее: https://www.digitalpolicy.gov.hk/en/our-work/data_governance/policies_standards/ethical_ai_framework/doc/HK_Generative_AI_Technical_and_Application_Guideline_en.pdf

26 15 Interim Measures for the Management of Generative Artificial Intelligence Services (2023). <https://clck.ru/38Qr5D>

27 Национальный проект КНР «Вычисления Восток-Запад». https://scdr.sic.gov.cn/SmarterCity_new/yjcg/jlfx/0408/2c-97b8cb-95c74996-0196-146609b2-0b94.pdf

21 См. подробнее: План развития ИИ нового поколения (2017), Меры в области генеративного ИИ (2023), Закон о безопасности данных (DSL).

22 https://www.gov.cn/zhengce/content/202508/content_7037861.htm

23 Временные меры по управлению службами генеративного искусственного интеллекта № 15 от 15.08.2025. https://www.gov.cn/zhengce/zhengceku/202307/content_6891752.htm

Таким образом, КНР демонстрирует важный методологический принцип: жесткость в вопросах обеспечения суверенной инфраструктуры для ИИ и гибкость в вопросах регулирования развития и использования ИИ-решений.

Опыт Республики Корея. Государственная политика в сфере ИИ в этой стране сочетает амбициозные цели глобального лидерства с прагматичным инструментарием правового регулирования. Ключевым правовым документом, определяющим корейский подход к концепции «суверенного ИИ», является рамочный Закон «О развитии искусственного интеллекта и создании доверительной среды» (далее – Закон об ИИ Республики Корея). Как указано в ст. 1 Закона, его целью является «содействие здоровому развитию ИИ и созданию необходимой основы доверия путем определения основных вопросов, тем самым защищая права, интересы и достоинство граждан, улучшая качество их жизни и укрепляя национальную конкурентоспособность». Следовательно, законодатель рассматривает суверенитет в сфере ИИ не как самоцель, а как средство повышения национальной конкурентоспособности при одновременной защите прав граждан.

Закон об ИИ Республики Корея предусматривает:

1) Категоризацию ИИ по уровню воздействия. Закон закрепляет понятие «искусственный интеллект с высоким уровнем воздействия», под которым понимаются системы, которые потенциально могут оказать значительное влияние на жизнь, безопасность или основные права человека. Для таких систем устанавливаются дополнительные требования.

2) Предоставление государственных данных для обучения ИИ. Согласно ст. 6 Закона об ИИ Республики Корея, вопросы, касающиеся предоставления государственных данных в качестве данных для обучения ИИ, согласовываются с министром внутренних дел и безопасности. Такой подход обеспечивает, с одной стороны, доступ разработчиков к качественным данным, а с другой – сохранение государственного контроля над использованием чувствительной информации.

3) Разработку мер по созданию основы доверия к ИИ. Статья 29 Закона обязывает правительство разработать комплекс мер для минимизации потенциальных рисков влияния ИИ на жизнь граждан и создания основы доверия для безопасного использования ИИ.

4) Поддержку проверки и сертификации безопасности и надежности ИИ. Статья 30 Закона вводит механизм добровольной проверки и сертификации ИИ, который включает распростра-

нение руководств по разработке ИИ и поддержку создания и эксплуатации оборудования и систем, используемых для проверки и сертификации, поддержку подготовки профессиональных кадров, необходимых для проверки и сертификации.

Сертифицированные ИИ-решения имеют приоритет при государственных закупках, что создает рыночные стимулы прохождения добровольной сертификации, без жестких ограничений для всех поставщиков и разработчиков. Министерство науки и информационно-коммуникационных технологий предоставляет поддержку малым и средним предприятиям для прохождения сертификации ИИ-решений с высоким уровнем воздействия, что снижает барьеры входа на рынок и способствует развитию конкурентной среды.

Корейский подход к суверенному ИИ предлагает гибкую, многоуровневую систему, которая сочетает государственную поддержку инноваций, дифференцированное регулирование по уровню риска и стимулирование добросовестного поведения через рыночные механизмы, в частности, приоритет в государственных закупках.

Опыт Республики Сингапур. В 2024 году была выпущена Рамочная модель регулирования генеративного ИИ²⁸. Ключевыми элементами этой стратегии выступают развитие собственных научных и инженерных кадров, активное использование технологий с открытым исходным кодом, а также создание надежной цифровой инфраструктуры.

Прагматичный подход Сингапура выражается в стратегии «умной зависимости», сочетающейся с разработкой региональных ИИ-моделей, таких как SEA-LION²⁹.

Особого внимания заслуживает опубликованная 22 января 2026 года Управлением по развитию информационных и медиатехнологий Сингапура Рамочная программа по агентному ИИ³⁰. Этот документ призван регулировать ответственное использование передовых ИИ-агентов, обеспечивая безопасное внедрение при сохранении доверия, безопасности и подотчетности³¹.

Анализ сингапурского подхода к соотношению развития технологий ИИ и технологического суверенитета позволяет сделать следующие

28 Model AI Governance Framework for Generative AI. <https://aiverifyfoundation.sg/>

29 SEA-LION. <https://sea-lion.ai/>

30 Model AI Governance Framework for Agentic AI. <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2026/new-model-ai-governance-framework-for-agentic-ai>

31 См. подробнее: <https://www.imda.gov.sg/-/media/imda/files/about/emerging-tech-and-research/artificial-intelligence/mgf-for-agentic-ai.pdf>

Нормы и правила

Таблица 2. Комплексная карта: правовые, экономические и стратегические параметры
Table 2. Comprehensive chart: legal, economic, and strategic parameters

Раздел / фактор	США	КНР	ЕС	Республика Корея	Сингапур	ОАЭ / Саудов- ская Аравия	Вьетнам	Казахстан
А. ПРАВОВОЙ СЛОЙ – функциональный метод и правовые семьи ¹								
Правовая семья / стиль	Англо-американская (общее право)	Социалистическая	Романо-германская	Романо-германская	Англо-американская (общее право)	Религиозная (исламская) + смешанная	Социалисти- ческая (рома- но-герм. влия- ние)	Романо- германская (постсовет- ская)
Типinstrу- мента	Подзаконные акты (указы Президента)	Стратегии, техниче- ские стандарты, ру- ководства + инфра- структурные ини- циативы	Закон об ИИ + про- граммные инициа- тивы	Рамочный закон	Рамочная модель регу- лирования («мягкое право»)	Стратегии, мо- дели («мягкое право»)	Закон об ИИ	Закон об ИИ
Объект суве- ренности	Поддержка и разви- тие инновационной среды. Политика лидерства в ИИ-сфере. Безопасность разви- тия ИИ-систем. Отказ от чрезмерно обременительного ре- гулирования ИИ-сферы, которое могло бы тормозить прогресс	Создание отечественной ИИ-эко- системы (от производства чипов и вычислительной инфраструктуры до разработки фундаментальных ИИ-моделей и прикладных сервисов). Ключевыми инструментами выступа- ют правила о локализации данных, а также развитие собственных техно- логических стандартов, не ориенти- рованных на совместимость с зару- бежными аналогами	Требования к оцен- ке соответствия си- стем высокого ри- ска. Защита данных + открытая совмести- мая экосистема	Политика глобально- го лидерства в соче- тании с прагматич- ным инструментарием правового регу- лирования. Категоризация ИИ по уровню воздей- ствия. Предоставление го- сударственных дан- ных для обучения ИИ. Создание основы доверия к ИИ. Проверки и сертифици- кации безопасности ИИ	Модель «умной зависи- мости», признавая неиз- бежность использова- ния зарубежных ИИ-моделей, аппарат- ного и программного обеспечения для ИИ в областях, где это эконо- мически и технологиче- ски оправдано. Вместе с этим государство целе- направленно развивает и суверенные большие языковые модели (SEA- LION), собственный ка- дровый потенциал и цифровую инфра- структуру для ИИ	Создание от- крытой ис- ламской мо- дели генера- тивного ИИ, обученной на национальных наборах дан- ных, отражаю- щих культур- ный ислам- ский код «lais» и инве- стиции в ма- лые языковые модели (SLM)	Привязка к национальной. ИИ-инфра- структуре (вы- числения, дан- ные, LLM)	Привязка к националь- ной ИИ-инфра- структуре. Наш цифро- вая платфор- ма ИИ
Профильные акты	Исполнительный указ Президента США «Об устранении барьеров для американского лидерства в области искусственного интел- лекта» (2026); Исполнительный указ Президента США «Устранение препят- ствий на пути к ли- дерству США в обла- сти искусственного интеллекта» (2025)	Стратегия развития ИИ «Мнения Государственного совета по углублен- ной реализации инициативы "Искусственный интеллект+"» (2025). Стандарт прозрачности больших язы- ковых моделей: «Рекомендации по доверенным базовым моделям ис- кусственного интеллекта» (2025). «Временные меры по управлению службами генеративного искусствен- ного интеллекта» (2023). «Руководство по построению Национальной системы стандартов ИИ нового поколения» (2020)	Закон ЕС «Об искус- ственном интеллек- те» (2024)	Рамочный закон «О развитии искус- ственного интеллек- та и создании дове- рительной среды» (2026)	Рамочная модель регу- лирования генератив- ного ИИ (2024); Рамочная программа по агентному ИИ (2026)	Отсутствует правовой акт, регулирующий ИИ-сферу	Закон «Об ис- кусственном интеллекте» (2025)	Закон Республики Казахстан «Об искус- ственном ин- теллекте» (2025)

1 Zweigert K., Kötz H. Introduction to Comparative Law (translate Weir T.). 3 ed. New York: Clarendon Press, 1998. 714 p. https://books.google.ru/books?vid=ISBN0198268602&redir_esc=y

Раздел / фактор	США	КНР	ЕС	Республика Корея	Сингапур	ОАЭ / Саудовская Аравия	Вьетнам	Казахстан
Инициативы		Инфраструктурная инициатива. Национальная программа «Восточные данные – западные вычисления»	Суверенная облачная платформа (SCS). Программа «Совместное предприятие в области высокопроизводительных вычислений» (EuroHPC JU). Инициатива «Гайа-Икс» (Gaia-X)			Проект по созданию открытой исламской модели генеративного ИИ «Lais»		
В. ЭКОНОМИЧЕСКИЙ СЛОЙ – ресурсное обеспечение ²								
ВВП, млн \$, 2024	28,750,956	18,743,803	Например, Германия – 4,685,593, Франция – 3,160,443	1,875,388	547,387	Саудовская Аравия – 1,239,805, ОАЭ – 552,325	476,388	291,480
Частные инвест. в ИИ, 2024 ³	\$285,88	\$12,41	Франция – \$4.36, Германия – \$3.89	\$1,78	\$1,82	Саудовская Аравия – \$2,03	Нац. программа (огранич.)	Нац. программа (огранич.)
С. СТРАТЕГИЧЕСКИЙ СЛОЙ – модель «маркетинговых войн» ⁴								
Стратегия Траута	Оборона (лидер)	Наступление (№ 2)	Фланговая атака	Фланговая атака	Партизанские методы	Партизанские методы	Партизанские методы (автаркическая ниша)	Партизанские методы (платформенная ниша)
Логика стратегии	Не дать догнать; «атаковать себя» (дерегуляция), блокировать догоняющих	Удар в слабое место лидера: модели с открытыми весами, параллельный стек, свои стандарты	Новый фронт – права, открытые стандарты («брюссельский эффект»)	Фланг через риск-сертификацию и госзакупки	«Умная зависимость», региональная LLM	Ниша культурно-языковых моделей + капитал и чипы	Ниша национальной языковой инфраструктуры	Ниша национальной платформы
Главный риск / уязвимость	Утечка талантов; сужение отрыва (DeepSeek)	Доступ к передовым чипам (экспорт-контроль)	Мало передовых моделей; разрыв капитал – возможности	Зависимость от иностр. чипов / моделей; масштаб рынка	Небольшой масштаб; зависимость от внешних моделей	Кадров и устойчивость стека; зависимость от железа	Ресурсные ограничения; стоимость параллельной экосистемы	Незначительный по объемам рынок; ресурсные ограничения

2 Gross domestic product 2024. <https://datacatalogfiles.worldbank.org/ddh-published/0038130/DR0046441/GDP.pdf>

3 Stanford University «Artificial Intelligence Index Report 2025» (данные за 2024 год). <https://ict.moscow/analytics/ai-index-report-2025/>

4 Ries A. Trout J. Marketing Warfare. 20th Anniversary Edition. McGraw-Hill, 2006. 216 p. https://books.google.ru/books/about/Marketing_Warfare.html?id=G9KrQgAACAAJ&redir_esc=y

Нормы и правила

выводы. Сингапур реализует модель «умной зависимости», признавая неизбежность использования зарубежных ИИ-моделей, аппаратного и программного обеспечения для ИИ в областях, где это экономически и технологически оправдано. Вместе с этим государство целенаправленно развивает и суверенные большие языковые модели (SEA-LION), собственный кадровый потенциал и цифровую инфраструктуру для ИИ. Такой подход позволяет обеспечить достаточную независимость от зарубежных решений в стратегически важных областях, без сверхзатрат на создание параллельной экосистемы ИИ.

Опыт Социалистической Республики Вьетнам. В ст. 16 Закона «Об искусственном интеллекте»³² Социалистической Республики Вьетнам содержится подход к определению термина «национальная инфраструктура искусственного интеллекта», которая определяется как стратегическая, финансируемая государством, единая, открытая и безопасная экосистема. В состав вьетнамской национальной инфраструктуры ИИ входят следующие компоненты: вычислительные мощности и данные для обучения ИИ-моделей; платформы для обучения, тестирования ИИ-моделей; фундаментальные и мультимодальные ИИ-модели, а также большие языковые модели на вьетнамском языке и языках этнических меньшинств и др.

Вьетнамская национальная инфраструктура создается государством, бизнесом и общественными организациями как единая, общедоступная система, соответствующая стандартам безопасности и защиты данных. Использование значимых технологий ИИ в ключевых отраслях (определенных премьер-министром) должно опираться на эту инфраструктуру³³.

Таким образом, вьетнамский подход демонстрирует, что достижение суверенитета в сфере ИИ возможно не только через прямое провозглашение соответствующих терминов в законе, но и через создание институционально и технологически замкнутой национальной ИИ-инфраструктуры.

Опыт Республики Казахстан. В Законе «Об искусственном интеллекте»³⁴ Республики Казахстан термин «суверенный искусственный интеллект» не упоминается. Однако в п. 11 Общих положений Закона упоминается «национальная платформа искусственного интеллекта», под которой понимается технологическая платформа, предназначенная для сбора, обработки, хранения и распро-

странения библиотек данных и предоставления услуг в сфере искусственного интеллекта. Статья 25 Закона³⁵ устанавливает требования к национальной ИИ-платформе, предназначенной для обеспечения контролируемой среды для разработки, обучения и опытной эксплуатации ИИ-моделей и продуктов в течение ограниченного периода времени³⁶.

В отличие от Вьетнама с его акцентом на физическую инфраструктуру для ИИ, Казахстан делает ставку на цифровую платформу как институционально-технологический инструмент цифрового суверенитета, используемый для разработки ИИ.

Опыт ОАЭ и Саудовской Аравии. Подходы этих стран заключаются в создании генеративной ИИ-модели, обученной на национальных наборах данных, которые целенаправленно отражают арабский культурный код, исламские ценности, локальные традиции и социальный контекст. Двухязычная ИИ-модель «Jais», разработанная на основе открытого исходного кода и обученная на арабском и английском языках, учитывает культурные и религиозные особенности носителей арабского языка. Создание исламской модели генеративного ИИ, а также инвестиции в малые языковые модели (Small Language Models – SLM) стали ключевыми элементами стратегии ОАЭ и Саудовской Аравии по обеспечению технологического суверенитета. Такой подход позволяет странам региона не копировать западные модели, а создавать собственные ИИ-решения, в полной мере соответствующие стратегическим приоритетам национального и культурного развития³⁷. Суверенный ИИ в данном контексте ориентирован на данные, язык и культурные ценности, но не на вычислительную инфраструктуру и архитектуру ИИ-моделей.

В **таблице 2** представлены подходы к концепции «суверенного ИИ» в разных государствах.

Преимущества суверенного ИИ

Рассмотрим преимущества, которые появляются у государства, развивающего суверенный ИИ.

Достаточный уровень стратегической автономии. Развивая отечественные разработки в сфере ИИ, государства могут сохранить контроль над своей технологической инфраструктурой, защищать конфиденциальность данных и снижать уязвимость к внешнему давлению или принуждению.

32 <https://thuvienphapluat.vn/van-ban/EN/Cong-nghe-thong-tin/Law-134-2025-QH15-Artificial-Intelligence/689735/tieng-anh.aspx>

33 Там же.

34 <https://adilet.zan.kz/rus/docs/Z2500000230>

35 Там же.

36 Там же.

37 Эмираты запускают большую языковую модель на арабском языке. <https://vc.ru/id991602/830898-emiraty-zapuskayut-bolshuyu-yazykovuyu-model-na-arabskom-yazyke>

Культурная и ценностная релевантность. Разработанные за рубежом технологии ИИ могут не отражать культурные и ценностные особенности другого государства. Это может привести к развертыванию систем ИИ, которые будут неэффективными или даже вредоносными в национальном контексте. Развитие возможностей суверенного ИИ позволяет государствам создавать технологии, адаптированные к их культурному и ценностному контексту.

Защита конфиденциальности. Развивая суверенные ИИ-возможности, государства могут обеспечить соответствие обработки, хранения и передачи персональных данных национальным правовым нормам, более эффективно защищая конфиденциальность граждан.

Защита от манипулирования поведением населения. Системы ИИ могут оказывать влияние на поведение человека и манипулировать им, определяя в том числе потребительский выбор, электоральное поведение, социальную динамику, создавая угрозу национальной безопасности. Развитие суверенных ИИ-компетенций предоставляет государствам возможность вводить соответствующие этические нормы и надзорные механизмы [Юхно, Агеев, 2025. С. 314].

Эффективное государственно-частное партнерство. Сегодня крупные технологические компании являются локомотивами развития технологий ИИ [Khanal, Zhang, Taeihagh, 2025. P. 52–69], стратегия кооперации государств и технологических гигантов выглядит привлекательной и позволяет одновременно объединять финансовые, административные и интеллектуальные ресурсы бизнеса, государственных органов и научного сообщества [Prasad, Karanam, Ganesh, Liyakat, Talasila, Purushotham, 2024; Юхно, 2025. С. 139–149], обеспечивая доступ к передовым программно-аппаратным комплексам для развертывания ИИ-ориентированных государственных сервисов и решений [Zhang, Khanal, Taeihagh, 2025. P. 1–11].

Риски реализации концепции суверенного ИИ

Достижение технологического суверенитета предполагает выход за рамки существующего, внешне заданного экономического порядка, при этом экономическая нецелесообразность разработки и внедрения суверенных технологических решений вызывает вопросы [Юхно, 2026. С. 161]. Разработка и внедрение критически важных технологических решений в области ИИ, таких как фундаментальные модели, вычислительная инфраструктура, специализированные чипы, требуют значительных инвестиций, которые окупают-

ся лишь при масштабировании на многомиллионную (а в ряде случаев – и глобальную) аудиторию. Стратегическая автономия в сфере ИИ остается предметом активной научной полемики.

Во-первых, дискуссионным остается сам тезис о ее необходимости для государств, не входящих в число технологических лидеров, поскольку избыточная локализация способна замедлить инновационные процессы и привести к удорожанию разработок. Во-вторых, принципиальный вопрос вызывает сама достижимость стратегической автономии в условиях текущего темпа развития ИИ, когда фаза проектирования новой архитектуры модели может исчисляться месяцами, тогда как создание сопоставимой технологической инфраструктуры характеризуется длительным периодом реализации.

Проведенный сравнительно-правовой анализ подходов к суверенному искусственному интеллекту в Российской Федерации, государствах Азии (Вьетнам, Казахстан, Китай, Сингапур, Южная Корея), Европейском союзе и США позволяет не только выявить преимущества каждой модели, но и обозначить следующие риски, сопутствующие реализации политики укрепления суверенитета в сфере ИИ.

1. *Риск замедления технологического развития.* Жесткие требования к локализации всех стадий разработки, обучения и эксплуатации ИИ-моделей могут привести к технологической изоляции и, как следствие, к технологическому отставанию от мировых технологических лидеров.

Во-вторых, даже при значительных инвестициях создание полностью отечественной экосистемы требует времени, измеряемого годами. За этот период разрыв в качестве и функциональности ИИ-решений может стать непреодолимым. Как показывает опыт импортозамещения в других высокотехнологичных отраслях, таких как авиастроение, микроэлектроника, к моменту создания отечественного аналога зарубежный уходит на два-три поколения вперед.

В-третьих, искусственное ограничение круга поставщиков (отечественные разработчики, национальная платформа) сокращает конкуренцию на рынке, что может привести к технологической стагнации и консервации неоптимальных решений.

2. *Финансово-экономические риски.* Экономический эффект от создания суверенного ИИ сопряжен с временным лагом и высокой степенью неопределенности.

3. *Риски технической и организационной невыполнимости законодательных требований.* Отдельные требования, закладываемые в законода-

Нормы и правила

тельство о суверенном ИИ, могут оказаться неисполнимыми в силу современных технологических реалий.

Заключение

Анализ показывает, что концепция суверенного ИИ несет серьезные риски, несмотря на ее привлекательность для защиты национальных интересов. Полная технологическая независимость требует колоссальных ресурсов и ведет к изоляции и отставанию. Требование полной локализации часто невыполнимо из-за нехватки вычислительной инфраструктуры и кадров.

Предложенная в настоящей работе трехуровневая конструкция суверенного ИИ, включающая технологический суверенитет, доверенные технологии искусственного интеллекта и искусственный интеллект, обученный на национальных наборах данных, не является нормативным требованием и, следовательно, не задает жесткого стандарта, которому должны соответствовать суверенные модели ИИ, а служит инструментом для выявления того, какие из трех элементов в

большей или меньшей степени реализованы в подходе конкретного государства.

Оптимальным решением выступает селективный подход. Необходимо сохранять суверенитет в таких критических сферах, как оборона, критическая информационная инфраструктура, обработка биометрических и персональных данных. В остальных областях допустимо использование зарубежных решений и открытых стандартов.

Перспективным направлением дальнейших научных изысканий представляется исследование правоприменительной практики в государствах с действующими законами в сфере ИИ, а также мониторинг реализации подзаконных актов, принимаемых в развитие указанных законов. Такой анализ позволит оценить не только декларируемые, но и реально достижимые результаты правового регулирования в сфере суверенного искусственного интеллекта, а также выявить расхождения между нормативной моделью и практикой ее применения. Такой подход позволит усовершенствовать отечественное законодательство и выработать научно обоснованные рекомендации.

Литература

- Афанасьев А.А. Технологический суверенитет: основные направления политики по его достижению в современной России. *Вопросы инновационной экономики*. 2022. Т. 12. № 4. С. 2193–2212. <https://doi.org/10.18334/vinec.12.4.116433>
- Гареев Т.Р. Технологический суверенитет: от концептуальных противоречий к практической реализации. *Terra Economicus*. 2023. Т. 21. № 4. С. 38–54. <https://doi.org/10.18522/2073-6606-2023-21-4-38-54>
- Зиновьева Е.С., Бульва В.И. Цифровой суверенитет Европейского Союза. *Современная Европа*. 2021. № 2. С. 40–49. <http://dx.doi.org/10.15211/soveurope220214049>
- Зиновьева Е.С., Шитков С.В. Цифровой суверенитет в практике международных отношений. *Международная жизнь*. 2023. № 3. С. 38–51. EDN: HBTQYT
- Ленчук Е.Б. Технологический суверенитет – новый вектор научно-технологической политики России. *Журнал Новой экономической ассоциации*. 2024. № 3 (64). С. 232–237. <https://doi.org/10.31737/22212264.2024.3.232-237>. EDN: KCUGER
- Юхно А.С. Отраслевые экосистемы цифровых платформ в государственном управлении. *Управленческие науки*. 2025. № 4. С. 139–149. <https://doi.org/10.26794/2304-022X-2025-15-4-139-149>. EDN: EKTNTQ
- Юхно А.С. Технологический суверенитет как фактор укрепления государственного управления. *Государственное управление. Электронный вестник*. 2026. № 114. С. 160–173. <https://doi.org/10.55959/MSU2070-1381-114-2026-160-173>
- Юхно А.С., Азеев А.И. Эволюция культуры и экспансия искусственного интеллекта как вызовы системе государственного управления. *Социология власти*. 2025. Т. 37. № 4. С. 295–319. EDN: XEZJFA
- Dale R. Sovereign AI in 2025. *Natural Language Processing*. 2025. No. 31 (5). P. 1312–1321. <https://doi.org/10.1017/nlp.2025.10007>. In English
- Khanal S., Zhang H., Taeihagh A. Why and how is the power of Big Tech increasing in the policy process? The case of generative AI. *Policy and Society*. 2025. Vol. 44. No. 1. P. 52–69. <https://doi.org/10.1093/polsoc/puae012>. In English
- Ototsky P., Manenkov S., Smoliak A. Requisite trust requirements for digital society development. *Kybernetes*. 2023. Vol. 52. No. 9. P. 2958–2975. <https://doi.org/10.1108/K-04-2022-0610>. In English
- Prasad K.R., Karanam S.R., Ganesh D., Liyakat K.K.S., Talasila V., Purushotham P. AI in public-private partnership for IT infrastructure development. *The Journal of High Technology Management Research*. 2024. Vol. 35. No. 1. P. 100496. <https://doi.org/10.1016/j.hitech.2024.100496>. In English
- Ries A., Trout J. Marketing Warfare. 20th Anniversary Edition. McGraw-Hill, 2006. In English
- Timmers P. Ethics of AI and Cybersecurity When Sovereignty is at Stake. *Minds & Machines*. 2019. Vol. 29. P. 635–645. <https://doi.org/10.1007/s11023-019-09508-4>. In English
- Zhang H., Khanal S., Taeihagh A. Public-Private Powerplays in Generative AI Era: Balancing Big Tech Regulation Amidst Global AI Race. *Digital Government: Research and Practice*. 2025. Vol. 6. No. 2. P. 1–11. <https://doi.org/10.1145/3664824>. In English
- Zweigert K., Kötz H. Introduction to Comparative Law (translate Weir T.). 3 ed. N.Y.: Clarendon Press, 1998. In English

References

- Afanasyev A.A. Technological sovereignty: the main policies to achieve it in modern Russia. *Russian Journal of Innovation Economics*. 2022. Vol. 12. No. 4. P. 2193–2212. <https://doi.org/10.18334/vinec.12.4.116433>. In Russian
- Gareev T.R. Technological sovereignty: from conceptual contradiction to practical implementation. *Terra Economicus*. 2023. Vol. 21. No. 4. P. 38–54. <https://doi.org/10.18522/2073-6606-2023-21-4-38-54>. In Russian
- Zinovieva E.S., Bulva V.I. EU digital sovereignty. *Contemporary Europe*. 2021. No. 2. P. 40–49. <http://dx.doi.org/10.15211/soveurope220214049>. In Russian
- Zinovieva E.S., Shitkov S.V. Digital sovereignty in the practice of inter-

Д.А. Королькова, П.Л. Отоцкий, А.С. Юхно. Суверенный искусственный интеллект: сравнительно-правовой анализ подходов в России и за рубежом

national relations. *The International Affairs*. 2023. No. 3. P. 38–51. EDN: HBTQYT. In Russian

Lenchuk E.B. Technological sovereignty – a new trend in Russian scientific and technological policy. *Journal of the New Economic Association*. 2024. No. 3 (64). P. 232–237. https://doi.org/10.31737/22212264_2024_3_232-237. EDN: KCUGER. In Russian

Yukhno A.S. Industry ecosystems of digital platforms in public governance. *Management Sciences*. 2025. No. 4. P. 139–149. <https://doi.org/10.26794/2304-022X-2025-15-4-139-149>. EDN: EKTNTQ. In

Russian

Yukhno A.S. Technological sovereignty as a factor in strengthening public administration. *Public Administration. E-journal (Russia)*. 2026. No. 114. P. 160–173. <https://doi.org/10.55959/MSU2070-1381-114-2026-160-173>. In Russian

Yukhno A.S., Ageyev A.I. Cultural evolution and the expansion of artificial intelligence as challenges to the public administration system. *Sociology of Power*. 2025. Vol. 37. No. 4. P. 295–319. EDN: XEZJFA. In Russian

ИНФОРМАЦИЯ ОБ АВТОРАХ:

Дарья Александровна Королькова, кандидат юридических наук, доцент кафедры авторского права, смежных прав и частноправовых дисциплин

Российская государственная академия интеллектуальной собственности (Российская Федерация, 117279, Москва, ул. Миклухо-Маклая, 55а). E-mail: daria.kirilchenko@mail.ru
<https://orcid.org/0000-0003-0128-7624>

Петр Леонидович Отоцкий, кандидат физико-математических наук, ведущий научный сотрудник Дирекции приоритетных образовательных инициатив

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Российская Федерация, 119571, Москва, проспект Вернадского, 82). E-mail: peter.ototsky@phystech.edu
<https://orcid.org/0000-0003-1938-3518>

Александр Сергеевич Юхно, кандидат юридических наук, доцент, заведующий кафедрой государственного управления Института государственной службы и управления

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Российская Федерация, 119571, Москва, проспект Вернадского, 82). E-mail: yukhno-as@ranepa.ru
<https://orcid.org/0000-0003-2999-2982>

Для цитирования: Королькова Д.А., Отоцкий П.Л., Юхно А.С. Суверенный искусственный интеллект: сравнительно-правовой анализ подходов в России и за рубежом. *Государственная служба*. 2026. № 4. С. 6–19.

INFORMATION ABOUT THE AUTHORS:

Daria A. Korolkova, Candidate of Sci. (Law), Associate Professor, Department of Copyright, Related Rights, and Private Law Disciplines

Russian State Academy of Intellectual Property (55a, Miklukho-Maklaya St., Moscow, 117279, Russian Federation). E-mail: daria.kirilchenko@mail.ru
<https://orcid.org/0000-0003-0128-7624>

Petr L. Ototsky, Candidate of Sci. (Physical and Mathematical Sciences), Leading Researcher, Directorate of Priority Educational Initiatives

Russian Presidential Academy of National Economy and Public Administration (82, Vernadsky Prospekt, Moscow, 119571, Russian Federation). E-mail: peter.ototsky@phystech.edu
<https://orcid.org/0000-0003-1938-3518>

Alexander S. Yukhno, Candidate of Sci. (Law), Associate Professor, Head of the Department of State Studies, Institute of Public Administration and Civil Service

Russian Presidential Academy of National Economy and Public Administration (82, Vernadsky Prospekt, Moscow, 119571, Russian Federation). Email: yukhno-as@ranepa.ru
<https://orcid.org/0000-0003-2999-2982>

For citation: Korolkova D.A., Ototsky P.L., Yukhno A.S. Sovereign Artificial Intelligence: a comparative legal analysis of approaches in Russia and abroad. *Public Administration*. 2026. No. 4. P. 6–19.