Международный научно-исследовательский журнал
«Прогрессивная экономика»
№ 8 / 2026 https://progressive-economy.ru/vypusk_1/formirovanie-rynka-otechestvennogo-programmnogo-obespecheniya-v-sfere-informaczionnoj-bezopasnosti-v-usloviyah-tehnologicheskogo-suvereniteta/
Научная статья / Original article
Шифр научной специальности ВАК: 5.2.3
УДК 338.242:004.056
DOI: 10.54861/27131211_2026_8_242

ФОРМИРОВАНИЕ РЫНКА ОТЕЧЕСТВЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ТЕХНОЛОГИЧЕСКОГО СУВЕРЕНИТЕТА: СРАВНИТЕЛЬНЫЙ АНАЛИЗ РОССИЙСКОЙ И КИТАЙСКОЙ МОДЕЛЕЙ СТИМУЛИРОВАНИЯ ИННОВАЦИОННОГО РАЗВИТИЯ ОТРАСЛИ

Щербинина А.В., *Московский государственный институт международных отношений МИД Российской Федерации (МГИМО МИД России),*
г. Москва, Россия
119454, Москва, проспект Вернадского, 76
e-mail: anv.shcherbinina@gmail.com

Аннотация. В статье проведён сравнительный анализ российской и китайской моделей государственного стимулирования отечественного программного обеспечения в сфере информационной безопасности (ИБ) в контексте курса на технологический суверенитет. Предмет исследования – инструменты и механизмы поддержки отрасли; объект – процесс формирования рынка отечественных средств защиты информации. На основе нормативных актов, отраслевой аналитики и корпоративной отчётности показано, что обе страны реализуют государственно-центричную модель, однако различаются по типу драйвера, глубине технологического стека и темпам внедрения. Российская модель носит преимущественно нормативный характер с высокими темпами реализации и опирается на реестр отечественного ПО, налоговый манёвр и грантовые механизмы индустриальных центров компетенций. Китайская модель (программа Xinchuang) характеризуется долгосрочным программным планированием, охватом полного технологического стека (процессоры и операционные системы) и постепенным горизонтом замещения в госсекторе к 2027 г. Сформулированы выводы в контексте российской промышленной политики: увязка программного суверенитета с аппаратным, поддержка конкуренции внутри реестра и стимулирование экспортной ориентации отрасли.

Ключевые слова: информационная безопасность, технологический суверенитет, импортозамещение, программное обеспечение, промышленная политика, Xinchuang, инновационное развитие.

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Для цитирования: Щербинина А.В. Формирование рынка отечественного программного обеспечения в сфере информационной безопасности в условиях технологического суверенитета: сравнительный анализ российской и китайской моделей стимулирования инновационного развития отрасли // Прогрессивная экономика. 2026. № 8. С. 242–255. https://doi.org/10.54861/27131211_2026_8_242.

Статья поступила в редакцию: 07.07.2026 г. Одобрена после рецензирования: 11.08.2026 г. Принята к публикации: 15.08.2026 г.

FORMATION OF THE DOMESTIC INFORMATION-SECURITY SOFTWARE MARKET UNDER TECHNOLOGICAL SOVEREIGNTY: A COMPARATIVE ANALYSIS OF THE RUSSIAN AND CHINESE MODELS OF STIMULATING INNOVATIVE INDUSTRY DEVELOPMENT

Shcherbinina A.V., *Moscow State Institute of International Relations of the Ministry of Foreign Affairs of the Russian Federation (MGIMO University), Moscow, Russia*
119571, Moscow, Vernadsky Avenue, 76
e-mail: anv.shcherbinina@gmail.com

Abstract. The article provides a comparative analysis of the Russian and Chinese models of state stimulation of domestic information-security (IS) software in the context of technological sovereignty. The subject of the study is the instruments and mechanisms of industry support; the object is the process of forming the market of domestic information-protection tools. Drawing on regulatory acts, industry analytics and corporate reporting, the study shows that both countries pursue a state-centred model, yet differ in the type of driver, the depth of the technology stack and the pace of adoption. The Russian model is predominantly regulatory, with a high pace of implementation, and relies on the register of domestic software, the IT tax manoeuvre and the grant mechanisms of industrial competence centres. The Chinese model (the Xinchuang programme) is characterised by long-term programme planning, coverage of the full technology stack (processors and operating systems) and a gradual horizon of substitution in the public sector by 2027. Lessons are formulated for Russian industrial policy: linking software sovereignty with hardware sovereignty, supporting competition within the register, and stimulating the export orientation of the industry.

Keywords: information security, technological sovereignty, import substitution, software, industrial policy, Xinchuang, innovative development.

JEL classification: O25, O38, L86, O57.

Conflict of interest. The author declares that there is no conflict of interest.

For citation: Shcherbinina A.V. (2026). Formirovanie rynka otechestvennogo programmnogo obespecheniya v sfere informatsionnoi bezopasnosti v usloviyakh tekhnologicheskogo suvereniteta: sravnitel'nyi analiz rossiiskoi i kitaiskoi modelei stimulirovaniya innovatsionnogo razvitiya otrasli [Formation of the domestic information-security software market under technological sovereignty: a comparative analysis of the Russian and Chinese models of stimulating innovative industry development]. Progressivnaya ekonomika [Progressive Economy], 8, 242–255. https://doi.org/10.54861/27131211_2026_8_242. (In Russ., abstract in Eng.)

The article was submitted to the editorial office: 07/07/2026. Approved after review: 11/08/2026. Accepted for publication: 15/08/2026.

Введение

Технологический суверенитет закрепился в качестве самостоятельной категории экономической политики России, а сфера информационной безопасности (ИБ) стала одним из наиболее чувствительных её сегментов. Секьюритизация промышленных стратегий и курс на технологическую самодостаточность стали глобальным трендом начала 2020-х гг., охватившим как развитые страны, так и ведущие экономики БРИКС [1]. Уход зарубежных вендоров и расширение внешних ограничений превратили задачу замещения иностранных средств защиты информации (СЗИ) в вопрос функциональной устойчивости критической инфраструктуры. Одновременно рынок отечественного ПО в сфере ИБ демонстрирует опережающие темпы роста, что делает его удобным объектом для изучения того, как меры государственного стимулирования трансформируют отраслевую структуру.

Курс на технологическую самодостаточность не является исключительно российским феноменом. Китайская Народная Республика реализует сопоставимую по масштабу стратегию, известную под названием Xinchuang («инновационное применение информационных технологий»), нацеленную на вытеснение иностранных аппаратных и программных решений из чувствительных информационных систем. Сходство целей при различии институциональных условий делает сопоставление двух моделей продуктивным. Цель исследования – провести сравнительный анализ российской и китайской моделей стимулирования инновационного развития отрасли отечественного ПО в сфере ИБ. Объектом исследования выступает процесс формирования рынка отечественных СЗИ, предметом – инструменты и механизмы государственной поддержки отрасли.

Обзор литературы

Проблематика технологического суверенитета активно разрабатывается в современной литературе. Курс на технологическую самодостаточность рассматривается как глобальный тренд, связанный с секьюритизацией промышленных стратегий и эволюцией моделей промышленной политики в странах Запада и БРИКС, включая Россию [1]. Исследователи подчёркивают принципиальное различие импортозамещения и технологического суверенитета: если первое ориентировано на поиск аналогов зарубежных решений, то второе предполагает создание собственных конкурентоспособных технологий [2]. Правовые и институциональные предпосылки формирования технологического суверенитета Российской Федерации, включая иерархию нормативных актов и нетипичные регуляторы (программы развития, стандарты), проанализированы в [3]; при этом санкционное давление трактуется как катализатор инновационного развития отраслей, в том числе оборонно-промышленного комплекса [4]. Ряд авторов рассматривает цифровой суверенитет как механизм обеспечения национальной безопасности [5].

Применительно к сфере ИБ импортозамещение анализируется как драйвер ускоренного вывода на рынок отечественного ПО и структурной перестройки отрасли [6; 7]. Отмечается, что национальный проект «Цифровая экономика» и реестр отечественного ПО задали целевые ориентиры локализации, однако сохраняются проблемы качества, зрелости решений и зависимости от аппаратной базы [7]. Китайский опыт представлен работами по эволюции политики КНР в области кибербезопасности [8], концепции киберсуверенитета [9] и правовому обеспечению безопасности данных [10]. Сравнительный анализ практики цифрового суверенитета в России и КНР показывает, что при общей приоритизации вопросов безопасности реализация соответствующей политики различается по институциональным механизмам [11]. Вместе с тем систематический экономический сравнительный анализ инструментов государственного стимулирования отрасли отечественного ПО именно в сфере ИБ в России и КНР, учитывающий глубину технологического стека и результаты рыночной динамики, в литературе представлен фрагментарно, что определяет вклад настоящего исследования.

Материалы и методы

Методологической основой работы служит сравнительный институциональный анализ, дополненный описательным статистическим анализом рыночных показателей. Эмпирическая база включает три группы источников: нормативные правовые акты Российской Федерации и КНР; аналитические отчёты исследовательских центров (Центр стратегических разработок, TAdviser, Mordor Intelligence, Statista, а также оценки IDC и CAICT); данные корпоративной отчётности отраслевых компаний. При интерпретации количественных данных учитывались ограничения

сопоставимости: оценки объёма рынков различаются между агентствами вследствие различий в методологии, а прямое сопоставление в единой валюте затруднено, поэтому числовые показатели приводятся с указанием источника.

Результаты и обсуждение

Ядром российской модели выступает нормативно-ориентированный подход. Указ Президента РФ от 30.03.2022 № 166 ограничил с 1 января 2025 г. использование иностранного ПО на принадлежащих компаниям значимых объектах критической информационной инфраструктуры (КИИ), а закупку такого ПО ограничил ещё с 31 марта 2022 г. [12]. Указ Президента РФ от 01.05.2022 № 250 установил запрет с 1 января 2025 г. на использование СЗИ, произведённых в недружественных государствах или подконтрольными им организациями, и возложил на руководство организаций персональную ответственность за обеспечение ИБ [13]. Совокупно эти акты сформировали гарантированный внутренний спрос на отечественные решения.

Нормативные требования дополняются системой стимулов. Ключевым институтом является Единый реестр российских программ для ЭВМ и баз данных (ведётся в соответствии с постановлением Правительства РФ № 1236): по данным на июль 2026 г. он включал порядка 31,6 тыс. программных продуктов и 11,7 тыс. правообладателей, а включение в реестр открывает доступ к льготам и преференциям в государственных закупках [14]. Налоговый манёвр в ИТ-отрасли предусматривает для аккредитованных компаний пониженный тариф страховых взносов (7,6 % сверх единой предельной величины базы), а с 2025 г. – льготную ставку налога на прибыль 5 % вместо общей ставки 25 %; реализация прав на включённое в реестр ПО освобождается от НДС при условии, что доля профильной выручки составляет не менее 70 % [14; 15].

Инструментом прямого финансирования выступают индустриальные центры компетенций (ИЦК), координирующие особо значимые проекты импортозамещения отраслевого ПО. Гранты предоставляются через Российский фонд развития информационных технологий (РФРИТ) и Фонд «Сколково»; размер грантовой поддержки одного проекта варьируется в диапазоне от 100 млн до 2 млрд руб. [16; 17]. Результативность механизма подтверждается ростом покрытия отраслевых бизнес-процессов отечественными продуктами: в нефтегазовом секторе показатель вырос с 8 % до 81 %, в электроэнергетике – до 82 %, в металлургии – до 62 % [16].

Совокупный эффект мер отражается в динамике рынка. По оценке Центра стратегических разработок (ЦСР), объём российского рынка кибербезопасности вырос с 248,5 млрд руб. в 2023 г. до 314 млрд руб. в 2024 г. (прирост 26,3 %), при этом на отечественных вендоров приходится около 94 % рынка СЗИ, а к 2030 г. рынок прогнозируется на уровне около 968 млрд руб. [18]. По более раннему прогнозу ЦСР ожидался среднегодовой темп прироста 23,6 % и достижение к 2028 г. объёма 715 млрд руб. при росте доли

отечественных вендоров до 95 % [19]. Оценки TAdviser расходятся с оценками ЦСР: объём рынка за 2024 г. оценивается в 337 млрд руб. (прирост 27 %), а по итогам 2025 г. прогнозируется преодоление отметки 400 млрд руб. [20], что иллюстрирует проблему сопоставимости данных. На микроуровне рост отрасли подтверждается корпоративной отчётностью: выручка группы Positive Technologies по МСФО за 2024 г. составила 24,5 млрд руб. (прирост около 10 %) при объёме отгрузок 24,1 млрд руб.; итоговый результат оказался ниже первоначальных ожиданий менеджмента, что указывает на разрыв между регуляторным спросом и фактическими темпами внедрения [21].

Китайская модель опирается на институционально проработанную нормативную базу. Закон о кибербезопасности КНР вступил в силу 1 июня 2017 г. и закрепил обязательность многоуровневой системы защиты; Закон о безопасности данных действует с 1 сентября 2021 г., а Закон о защите персональной информации – с 1 ноября 2021 г. [22]. Технические требования конкретизирует система многоуровневой защиты MLPS 2.0, оформленная национальными стандартами (в том числе GB/T 22239-2019) и вступившая в силу 1 декабря 2019 г.; она предусматривает классификацию информационных систем по пяти уровням значимости [23].

Стержнем стратегии замещения выступает программа Xinchuang, охватывающая четыре взаимосвязанных сегмента: базовое аппаратное обеспечение, базовое программное обеспечение, прикладное ПО и информационную безопасность [24; 26]. Принципиальное отличие от российского подхода состоит в том, что замещению подлежит не только уровень ПО, но и весь технологический стек: продукты ИБ должны функционировать на отечественных процессорах (Kunpeng, Loongson и др.) и отечественных операционных системах (Kylin, UOS), что превращает задачу из переноса приложений в системную инженерную работу [25]. Реализация носит поэтапный и долгосрочный характер: программа развёртывается начиная с 2020 г. по стадиям – от закрытых рынков партийно-государственного управления к государственным корпорациям и далее к коммерческому сектору [24]. По сообщениям СМИ, государственным корпорациям было предписано заместить офисное ПО отечественными продуктами к 2027 г. (данные, которые информационные агентства не смогли независимо подтвердить) [27]. По отраслевым оценкам, к концу 2024 г. в рамках Xinchuang было выполнено около 30 % замещения, а период 2025–2026 гг. рассматривается как фаза ускорения [25].

Оценки объёма китайского рынка кибербезопасности существенно различаются в зависимости от методологии. По отраслевым данным со ссылкой на IDC и CAICT, в 2025 г. рынок оценивается в диапазоне примерно 120–150 млрд юаней (порядка 18,8 млрд долл. США по оценке IDC) [25]. Коммерческие аналитические агентства дают несовпадающие значения: Mordor Intelligence оценивает рынок 2025 г. примерно в 16,75 млрд долл. при

среднегодовом темпе прироста около 19 % до 2030 г. [28], тогда как Statista прогнозирует более умеренный темп около 8,6 % и объём порядка 23,75 млрд долл. к 2030 г. [29]. Существенный разброс оценок сам по себе является методологически значимым результатом.

Таблица 1

Сравнительная характеристика российской и китайской моделей стимулирования отрасли ИБ

Table 1

Comparative characteristics of the Russian and Chinese models of stimulating the IS industry

Критерий сравнения	Российская модель	Китайская модель (КНР)
Начало активной фазы	2021–2022 гг.	2019–2020 гг. (Xinchuang); нормативная база – с 2017 г.
Основной драйвер	Нормативно-ориентированный подход, новые требования регулятора к защите инфраструктуры	Программа (Xinchuang) в сочетании с нормативными требованиями (MLPS)
Ключевые нормативные акты	Указы № 166 и № 250; Федеральный закон № 187-ФЗ о КИИ	Закон о кибербезопасности (2017), MLPS 2.0 (2019), законы о безопасности данных и защите ПДн (2021)
Реестровый механизм	Единый реестр российского ПО (ПП № 1236)	Каталоги доверенных поставщиков и продуктов Xinchuang
Фискальные инструменты	Налоговый манёвр: налог на прибыль 5 %, взносы 7,6 %, освобождение от НДС	Налоговые льготы, преференции в госзакупках, отраслевые фонды
Прямое финансирование	Гранты РФРИТ и Фонда «Сколково» (ИЦК, особо значимые проекты)	Государственный заказ, госинвестиции, региональные субсидии
Глубина технологического стека	Преимущественно уровень ПО	Полный стек: отечественные процессоры (Kunpeng, Loongson) и ОС (Kylin, UOS)
Целевой горизонт	Запрет иностранных СЗИ и ПО на значимых объектах КИИ – с 2025 г.	Завершение замещения в госсекторе и госкорпорациях – к 2027 г.
Достигнутый уровень локализации	≈ 94 % рынка СЗИ занимают отечественные вендоры (2024 г.)	≈ 30 % замещения в рамках Xinchuang к концу 2024 г.

Источник: составлено автором по данным [12–29]
Source: compiled by the author based on data [12–29]

Проведённое сопоставление позволяет выделить как общие черты, так и качественные различия двух моделей. Общими являются государственно-центричный характер, связь отраслевой политики с задачами национальной безопасности, использование реестрово-каталожных механизмов допуска продукции и установление этапных сроков замещения. Ключевые различия сводятся к трём аспектам. Во-первых, глубина технологического стека: Xinchuang охватывает аппаратный уровень (процессоры и операционные системы), формируя аппаратный суверенитет, тогда как российские меры сконцентрированы преимущественно на уровне ПО, что сохраняет зависимость от иностранной элементной базы. Во-вторых, институциональная конфигурация: российский подход строится на открытых нормативных актах и грантовых механизмах, тогда как китайский в значительной степени опирается на закрытые директивы и отраслевые каталоги. В-третьих, скорость реализации: несмотря на то что Китай приступил к системному импортозамещению ПО раньше, высокие темпы внедрения позволили России достичь значимых результатов за более короткий период.

Ускоренный характер российской модели порождает специфические риски. Гарантированный регуляторный спрос при ограниченном числе поставщиков может ослаблять конкурентные стимулы к повышению качества продукции, а сжатые сроки – приводить к разрыву между формальным соответствием требованиям и фактической функциональной зрелостью решений. Незамкнутость технологического стека на аппаратном уровне сохраняет уязвимость отрасли перед внешними ограничениями поставок компонентов – проблему, которую китайская модель решает через параллельное развитие отечественных процессоров и ОС. Наконец, относительная узость внутреннего рынка усиливает значимость экспортной ориентации как условия устойчивого инновационного развития. Отсюда вытекает необходимость для российской промышленной политики: увязывать программный суверенитет с аппаратным, развивая доверенные программно-аппаратные комплексы (эта задача обозначена в Указе № 166 [12]); поддерживать конкуренцию внутри реестра; смещать акцент с формального комплаенса на практическую защищённость; стимулировать экспортную ориентацию отрасли на дружественные рынки.

Заключение

Проведённый сравнительный анализ показывает, что Россия и КНР реализуют принципиально схожие по целям, но различные по конструкции модели стимулирования отрасли отечественного ПО в сфере ИБ. Российская модель является нормативно-ориентированной и реализуется высокими темпами, с опорой на реестр, налоговый манёвр и грантовые механизмы ИЦК; китайская – программно-плановой и постепенной, с охватом полного технологического стека. Обе модели обеспечивают формирование гарантированного спроса и рост доли отечественных решений, однако

китайский подход системнее решает задачу аппаратной независимости. Таким образом, устойчивость технологического суверенитета в сфере ИБ определяется не только замещением на уровне приложений, но и глубиной охвата технологического стека, сохранением конкурентной среды и экспортным потенциалом отрасли.

Литература

1. Курс на технологический суверенитет: новый глобальный тренд и российская специфика // Балтийский регион. 2024. Т. 16. № 3. https://doi.org/10.5922/2079-8555-2024-3-6.

2. Калиненко Н. Л. Импортозамещение и технологический суверенитет // Образование и право. 2023. № 11. С. 90.

3. Аничкин Е.С. Правовое обеспечение технологического суверенитета Российской Федерации: предпосылки, состояние и перспективы // Lex Russica. 2026. № 79 (4 (233)). С. 18–29. https://doi.org/10.17803/1729-5920.2026.233.4.018-029.

4. Родина И.Б. Технологический суверенитет отраслей оборонно-промышленного комплекса: национальная идея и фактор технологического лидерства // Лидерство и менеджмент. 2025. Т. 12. № 4. С. 899–914. https://doi.org/10.18334/lim.12.4.123102.

5. Емелин Я. А., Руденко Е. А. Цифровой суверенитет как политический нарратив: государственные приоритеты и модели общественной адаптации // Общество: политика, экономика, право. 2026. № 1. С. 40–47. https://doi.org/10.24158/pep.2026.1.5.

6. Некрасов А.А. Импортозамещение и информационная безопасность России // Альманах Пермского военного института войск национальной гвардии. 2021. № 4 (4). С. 274–278.

7. Джангиров М. Ф. Импортозамещение на рынке информационной безопасности // Молодой ученый. 2023. № 1 (448). С. 4–7.

8. Разумов Е.А. Политика КНР по обеспечению кибербезопасности // Россия и АТР. 2017. № 4 (98). С. 156–170.

9. Михалевич Е.А. Концепция киберсуверенитета Китайской Народной Республики: история развития и сущность // Вестник Российского университета дружбы народов. Серия: Политология. 2021. Т. 23. № 2. С. 254–264. https://doi.org/10.22363/2313-1438-2021-23-2-254-264.

10. Романовский В. Г. Правовое обеспечение безопасности данных (опыт Китая) // Электронный научный журнал «Наука. Общество. Государство». 2024. Т. 12. № 1. С. 32–41. https://doi.org/10.21685/2307-9525-2024-12-1-4.

11. Практика цифрового суверенитета в России и КНР // Российский совет по международным делам (РСМД). 2023. URL:

https://russiancouncil.ru/analytics-and-comments/analytics/praktika-tsifrovogo-suvereniteta-v-rossii-i-knr/.

12. О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации : Указ Президента РФ от 30.03.2022 № 166. URL: http://www.kremlin.ru/acts/bank/47688.

13. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации : Указ Президента РФ от 01.05.2022 № 250. URL: http://www.kremlin.ru/acts/bank/47796.

14. Реестр российских программ для электронных вычислительных машин и баз данных : меры поддержки и статистика // Портал «Горький Тех». URL: https://gorky.tech/it-podderzhka/meryi-podderzhki/reestr-rossijskix-programm-dlya-evm-i-baz-dannyix/.

15. Льготы на российское ПО: налоговые преференции для бизнеса. URL: https://patent-family.ru/journal/uchet/lgoty-rossijskoe-po/.

16. Одно ПО на всех: как индустриальные центры компетенций работают над импортозамещением. URL: https://expert.ru/tekhnologii/odno-na-vsekh-po.

17. Заказ на ИТ: чем занимаются индустриальные центры компетенций. URL: https://www.rbc.ru/opinions/economics/17/11/2023/655721809a7947088ad0e688.

18. Прогноз развития рынка кибербезопасности РФ на 2025–2030 годы : обзор исследования ЦСР. 2025. URL: https://www.kpgn.ru/research/csr-rynok-ib-2025/.

19. ЦСР: к 2028 году объём российского рынка ИБ достигнет 715 млрд рублей // BIS Journal. URL: https://ib-bank.ru/bisjournal/news/21202.

20. Объём российского рынка информационной безопасности превысит 400 млрд рублей. 23.12.2025. URL: https://www.cnews.ru/news/line/2025-12-23_obem_rossijskogo_rynka.

21. Positive Technologies финализирует итоги 2024 года: объём отгрузок клиентам компании составил 24,1 млрд рублей. URL: https://group.ptsecurity.com/ru/news/positive-technologies-finaliziruet-itogi-2024-goda-obem-otgruzok-klientam-kompanii-sostavil-24-1-mlrd-rublej.

22. Data Protection Laws of the World: China. URL: https://www.dlapiperdataprotection.com/index.html?c=CN.

23. China Released Core National Standards, Updating Mandatory Cybersecurity Requirements under the Cybersecurity Multi-level Protection Scheme. URL: https://www.insideprivacy.com/data-security/cybersecurity/china-released-core-national-standards-updating-mandatory-cybersecurity-requirements-under-the-cybersecurity-multi-level-protection-scheme/.

24. Made in China 2025 is back, with a new name and a focus on database companies. URL: https://thechinaproject.com/2022/12/19/made-in-china-2025-is-back-with-a-new-name-and-a-focus-on-database-companies/.

25. 2026 China Cybersecurity Industry Deep Report: Xinchuang, AI Security, Critical Infrastructure & Data Security in the Era of Domestic Substitution. URL: https://faxiangongchang.com/en/reports/china-cybersecurity-2026.

26. China Builds Self-Reliant Domestic IT Infrastructure Ecosystem. URL: https://archive.opengovasia.com/2021/11/30/china-builds-self-reliant-domestic-it-infrastructure-ecosystem/.

27. China rushes to swap Western tech with domestic options as U.S. cracks down. URL: https://www.aol.com/news/china-rushes-swap-western-tech-010311675.html.

28. China Cybersecurity Market Size & Share Outlook to 2030. URL: https://www.mordorintelligence.com/industry-reports/china-cybersecurity-market.

29. Cybersecurity – China : Market Forecast. URL: https://www.statista.com/outlook/tmo/cybersecurity/china.

References

1. Kurs na tekhnologicheskii suverenitet: novyi global'nyi trend i rossiiskaya spetsifika [Course toward technological sovereignty: a new global trend and Russian specifics]. (2024). Baltiiskii region [Baltic Region], 16(3). https://doi.org/10.5922/2079-8555-2024-3-6. (In Russ., abstract in Eng.).

2. Kalinenko N.L. (2023). Importozameshchenie i tekhnologicheskii suverenitet [Import substitution and technological sovereignty]. Obrazovanie i pravo [Education and Law], 11, 90. (In Russ., abstract in Eng.).

3. Anichkin E.S. (2026). Pravovoe obespechenie tekhnologicheskogo suvereniteta Rossiiskoi Federatsii: predposylki, sostoyanie i perspektivy [Legal support for the technological sovereignty of the Russian Federation: prerequisites, current state and prospects]. Lex Russica, 79(4(233)), 18–29. https://doi.org/10.17803/1729-5920.2026.233.4.018-029. (In Russ., abstract in Eng.).

4. Rodina I.B. (2025). Tekhnologicheskii suverenitet otraslei oboronno-promyshlennogo kompleksa: natsional'naya ideya i faktor tekhnologicheskogo liderstva [Technological sovereignty of defense industry sectors: a national idea and a factor of technological leadership]. Liderstvo i menedzhment [Leadership and Management], 12(4), 899–914. https://doi.org/10.18334/lim.12.4.123102. (In Russ., abstract in Eng.).

5. Emelin Ya.A., Rudenko E.A. (2026). Tsifrovoi suverenitet kak politicheskii narrativ: gosudarstvennye prioritety i modeli obshchestvennoi adaptatsii [Digital sovereignty as a political narrative: state priorities and models of social adaptation]. Obshchestvo: politika, ekonomika, pravo [Society: Politics,

Economics, Law], 1, 40–47. https://doi.org/10.24158/pep.2026.1.5. (In Russ., abstract in Eng.).

6. Nekrasov A.A. (2021). Importozameshchenie i informatsionnaya bezopasnost' Rossii [Import substitution and information security in Russia]. Al'manakh Permskogo voennogo instituta voisk natsional'noi gvardii [Almanac of the Perm Military Institute of the National Guard Troops], 4(4), 274–278. (In Russ., abstract in Eng.).

7. Dzhangirov M.F. (2023). Importozameshchenie na rynke informatsionnoi bezopasnosti [Import substitution in the information security market]. Molodoi uchenyi [Young Scientist], 1(448), 4–7. (In Russ., abstract in Eng.).

8. Razumov E.A. (2017). Politika KNR po obespecheniyu kiberbezopasnosti [China's cybersecurity policy]. Rossiya i ATR [Russia and the Pacific], 4(98), 156–170. (In Russ., abstract in Eng.).

9. Mikhalevich E.A. (2021). Kontseptsiya kibersuvereniteta Kitaiskoi Narodnoi Respubliki: istoriya razvitiya i sushchnost' [The concept of cyber sovereignty of the People's Republic of China: history and essence]. Vestnik Rossiiskogo universiteta druzhby narodov. Seriya: Politologiya [RUDN Journal of Political Science], 23(2), 254–264. https://doi.org/10.22363/2313-1438-2021-23-2-254-264. (In Russ., abstract in Eng.).

10. Romanovskii V.G. (2024). Pravovoe obespechenie bezopasnosti dannykh (opyt Kitaya) [Legal framework for data security: China's experience]. Nauka. Obshchestvo. Gosudarstvo [Science. Society. State], 12(1), 32–41. https://doi.org/10.21685/2307-9525-2024-12-1-4. (In Russ., abstract in Eng.).

11. Praktika tsifrovogo suvereniteta v Rossii i KNR [Digital sovereignty practices in Russia and China]. (2023). Rossiiskii sovet po mezhdunarodnym delam [Russian International Affairs Council]. Retrieved from: https://russiancouncil.ru/analytics-and-comments/analytics/praktika-tsifrovogo-suvereniteta-v-rossii-i-knr/. (In Russ.).

12. O merakh po obespecheniyu tekhnologicheskoi nezavisimosti i bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii: Ukaz Prezidenta Rossiiskoi Federatsii ot 30.03.2022 № 166 [On measures to ensure the technological independence and security of the critical information infrastructure of the Russian Federation: Decree of the President of the Russian Federation dated March 30, 2022 No. 166]. Retrieved from: http://www.kremlin.ru/acts/bank/47688. (In Russ.).

13. O dopolnitel'nykh merakh po obespecheniyu informatsionnoi bezopasnosti Rossiiskoi Federatsii: Ukaz Prezidenta Rossiiskoi Federatsii ot 01.05.2022 № 250 [On additional measures to ensure the information security of the Russian Federation: Decree of the President of the Russian Federation dated May 1, 2022 No. 250]. Retrieved from: http://www.kremlin.ru/acts/bank/47796. (In Russ.).

14. Reestr rossiiskikh programm dlya elektronnykh vychislitel'nykh mashin i baz dannykh: mery podderzhki i statistika [Register of Russian computer programs and databases: support measures and statistics]. Portal «Gor'kii Tekh» [Gorky Tech Portal]. Retrieved from: https://gorky.tech/it-podderzhka/meryi-podderzhki/reestr-rossijskix-programm-dlya-evm-i-baz-dannyix/. (In Russ.).

15. L'goty na rossiiskoe PO: nalogovye preferentsii dlya biznesa [Benefits for Russian software: tax preferences for businesses]. Retrieved from: https://patent-family.ru/journal/uchet/lgoty-rossijskoe-po/. (In Russ.).

16. Odno PO na vsekh: kak industrial'nye tsentry kompetentsii rabotayut nad importozameshcheniem [One software solution for everyone: how industrial competence centers pursue import substitution]. Ekspert [Expert]. Retrieved from: https://expert.ru/tekhnologii/odno-na-vsekh-po. (In Russ.).

17. Zakaz na IT: chem zanimayutsya industrial'nye tsentry kompetentsii [IT procurement: what industrial competence centers do]. RBK [RBC]. Retrieved from: https://www.rbc.ru/opinions/economics/17/11/2023/655721809a7947088ad0e688. (In Russ.).

18. Prognoz razvitiya rynka kiberbezopasnosti RF na 2025–2030 gody: obzor issledovaniya TsSR [Forecast for the development of the Russian cybersecurity market in 2025–2030: review of the CSR study]. (2025). Retrieved from: https://www.kpgn.ru/research/csr-rynok-ib-2025/. (In Russ.).

19. TsSR: k 2028 godu ob"em rossiiskogo rynka IB dostignet 715 mlrd rublei [CSR: the Russian information security market will reach RUB 715 billion by 2028]. BIS Journal. Retrieved from: https://ib-bank.ru/bisjournal/news/21202. (In Russ.).

20. Ob"em rossiiskogo rynka informatsionnoi bezopasnosti prevysit 400 mlrd rublei [The Russian information security market will exceed RUB 400 billion]. (2025). CNews. Retrieved from: https://www.cnews.ru/news/line/2025-12-23_obem_rossijskogo_rynka. (In Russ.).

21. Positive Technologies finaliziruet itogi 2024 goda: ob"em otgruzok klientam kompanii sostavil 24,1 mlrd rublei [Positive Technologies finalizes its 2024 results: shipments to the company's customers amounted to RUB 24.1 billion]. Positive Technologies. Retrieved from: https://group.ptsecurity.com/ru/news/positive-technologies-finaliziruet-itogi-2024-goda-obem-otgruzok-klientam-kompanii-sostavil-24-1-mlrd-rublej. (In Russ.).

22. Data Protection Laws of the World: China. DLA Piper. Retrieved from: https://www.dlapiperdataprotection.com/index.html?c=CN. (In Eng.).

23. China Released Core National Standards, Updating Mandatory Cybersecurity Requirements under the Cybersecurity Multi-level Protection Scheme. Inside Privacy. Retrieved from: https://www.insideprivacy.com/data-security/cybersecurity/china-released-core-national-standards-updating-mandatory-

cybersecurity-requirements-under-the-cybersecurity-multi-level-protection-scheme/. (In Eng.).

24. Made in China 2025 is Back, with a New Name and a Focus on Database Companies. (2022). The China Project. Retrieved from: https://thechinaproject.com/2022/12/19/made-in-china-2025-is-back-with-a-new-name-and-a-focus-on-database-companies/. (In Eng.).

25. 2026 China Cybersecurity Industry Deep Report: Xinchuang, AI Security, Critical Infrastructure & Data Security in the Era of Domestic Substitution. Retrieved from: https://faxiangongchang.com/en/reports/china-cybersecurity-2026. (In Eng.).

26. China Builds Self-Reliant Domestic IT Infrastructure Ecosystem. (2021). OpenGov Asia. Retrieved from: https://archive.opengovasia.com/2021/11/30/china-builds-self-reliant-domestic-it-infrastructure-ecosystem/. (In Eng.).

27. China Rushes to Swap Western Tech with Domestic Options as U.S. Cracks Down. AOL. Retrieved from: https://www.aol.com/news/china-rushes-swap-western-tech-010311675.html. (In Eng.).

28. China Cybersecurity Market Size & Share Outlook to 2030. Mordor Intelligence. Retrieved from: https://www.mordorintelligence.com/industry-reports/china-cybersecurity-market. (In Eng.).

29. Cybersecurity – China: Market Forecast. Statista. Retrieved from: https://www.statista.com/outlook/tmo/cybersecurity/china. (In Eng.).