БИЗНЕС-ИНФОРМАТИКА

BUSINESS INFORMATICS

Вестник НГУЭУ. 2025. № 4. С. 125–141
Vestnik NSUEM. 2025. No. 4. P. 125–141

Научная статья
УДК 004.056
DOI: 10.34020/2073-6495-2025-4-125-141

УСТОЙЧИВОСТЬ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В УСЛОВИЯХ ИМПОРТОЗАМЕЩЕНИЯ

Кузнецова Виктория Александровна[1], Сплюхин Денис Валерьевич[2], Нехорошков Евгений Владимирович[3], Ерофеев Михаил Владимирович[4], Василенко Ирина Андреевна[5], Бесчастнов Антон Алексеевич[6]

[1–6] *Научно-технологический университет «Сириус»*

[1] kuznetsova.via@talantiuspeh.ru
[2] splyuhin.dv@talantiuspeh.ru
[3] nehoroshkov.ev@talantiuspeh.ru
[4] erofeev.mv@talantiuspeh.ru
[5] vasilenko.ia@talantiuspeh.ru
[6] beschastnov.aa@talantiuspeh.ru

Аннотация. В работе исследованы проблемы устойчивости критической информационной инфраструктуры в условиях зависимости от иностранных поставщиков оборудования и программного обеспечения, влияния санкций на развитие цифровой трансформации отраслей промышленности России, а также показаны возможности импортозамещения. В части экономических аспектов проведен анализ влияния задач импортозамещения на расходы российских компаний и рассмотрены основные проблемы. По итогам работы обобщены концептуальные методологические подходы к формированию стратегий импортозамещения с учетом необходимости обеспечения устойчивости критической информационной инфраструктуры.

Ключевые слова: риски устойчивости, санкции, операционные системы, этапы импортозамещения

Финансирование. Результаты получены при финансовой поддержке проекта, реализуемого в рамках государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус» (Соглашение № 3-03 от 18.02.2025).

© Кузнецова В.А., Сплюхин Д.В., Нехорошков Е.В., Ерофеев М.В., Василенко И.А., Бесчастнов А.А., 2025

Контент доступен под лицензией Creative Commons Attribution 4.0 License

Для цитирования: Кузнецова В.А., Сплюхин Д.В., Нехорошков Е.В., Ерофеев М.В., Василенко И.А., Бесчастнов А.А. Устойчивость критической информационной инфраструктуры в условиях импортозамещения // Вестник НГУЭУ. 2025. № 4. С. 125–141. DOI: 10.34020/2073-6495-2025-4-125-141.

Original article

STABILITY OF CRITICAL INFORMATION INFRASTRUCTURE IN THE CONTEXT OF IMPORT SUBSTITUTION

Kuznetsova Viktoria A.[1], Splyukhin Denis V.[2], Nekhoroshkov Evgeny V.[3], Erofeev Mikhail V.[4], Vasilenko Irina A.[5], Beschastnov Anton A.[6]

[1–6] *Sirius University of Science and Technology*

[1] kuznetsova.via@talantiuspeh.ru
[2] splyuhin.dv@talantiuspeh.ru
[3] nehoroshkov.ev@talantiuspeh.ru
[4] erofeev.mv@talantiuspeh.ru
[5] vasilenko.ia@talantiuspeh.ru
[6] beschastnov.aa@talantiuspeh.ru

Abstract. This paper examines the sustainability of critical information infrastructure in the context of dependence on foreign hardware and software suppliers, the impact of sanctions on the development of digital transformation in Russian industries, and demonstrates opportunities for import substitution. Regarding economic aspects, it analyzes the impact of import substitution objectives on Russian companies' expenses and examines key challenges. The paper summarizes conceptual methodological approaches to developing import substitution strategies, taking into account the need to ensure the sustainability of critical information infrastructure.

Keywords: sustainability risks, sanctions, operating systems, stages of import substitution

Financing. The results were obtained with the financial support of the project implemented within the framework of the state program of the federal territory "Sirius" "Scientific and technological development of the federal territory "Sirius" (Agreement No. 3-03 dated 02/18/2025).

For citation: Kuznetsova V.A., Splyukhin D.V., Nekhoroshkov E.V., Erofeev M.V., Vasilenko I.A., Beschastnov A.A. Stability of critical information infrastructure in the context of import substitution. *Vestnik NSUEM*. 2025; (4): 125–141. (In Russ.). DOI: 10.34020/2073-6495-2025-4-125-141.

Введение

С каждым днем вопрос обеспечения безопасности значимых объектов критической информационной инфраструктуры (КИИ) приобретает все большее значение в контексте информационной безопасности всей страны. Нарушение или прекращение функционирования объектов КИИ может привести к серьезным негативным последствиям, не только к экономическому ущербу, но и к социальной дестабилизации, угрозе жизни и здоровью граждан. В связи с этим обеспечение безопасности КИИ является приори-

тетной государственной задачей и требует комплексного подхода, который включает в себя организационные, технические и правовые меры.

Особую актуальность проблема поиска решений для обеспечения технологического суверенитета, направленная на укрепление национальной безопасности и независимости в области КИИ, приобретает в условиях действия и введения новых санкций со стороны промышленно-развитых стран Запада. Общее количество санкций с 2014 г. в отношении российских юридических и физических лиц на I квартал 2025 г. составляет более 28,5 тыс.[1] Примерно 15 % санкций напрямую затрагивает ИТ-инфраструктуру. После 2022 г. санкционная динамика резко усилилась: США, ЕС и Япония запретили поставки микроэлектроники, телекоммуникационного оборудования и программного обеспечения двойного назначения.

На примере данных экспорта отдельных стран (табл. 1) можно проследить сокращение объемов поставок по статье ТН ВЭД ЕАЭС 8471 «Вычислительные машины и их блоки, магнитные или оптические считывающие устройства, машины для переноса данных на носители информации в кодированной форме и машины для обработки подобной информации», по которой в том числе осуществляются поставки высокотехнологичной ИТ-продукции и микроэлектроники.

Как можно увидеть из данных табл. 1, поставки из Чехии, Германии, США, Великобритании, Франции прекращены практически полностью. Частично проблема решается увеличением альтернативных поставок из Китая и Индии, но даже в этом случае опора на импортные технологии в ключевых секторах экономики, таких как КИИ, становится стратегически рискованной, поскольку потенциальное повторное введение санкций может подорвать национальную безопасность и устойчивость экономических систем.

Вопросы безопасности критической информационной инфраструктуры и создания условий для ее устойчивости поднимаются в работах многих российских и зарубежных исследователей. При этом отмечается актуальность не только устранения последствий атак или отказов инфраструктуры и программного обеспечения, но и создание таких систем, которые бы соответствовали определенным требованиям и целевым установкам, задаваемым на этапе проектирования [1]. В условиях нарастания внутренних и внешних угроз в сфере информационной безопасности необходима систематизация угроз информационной безопасности России, а также комплексный анализ наиболее существенных положений российского законодательства в сфере правовой регламентации обеспечения информационной безопасности государства [2, 3], как и совершенствование соответствующей ответственности за правонарушения в данной сфере [4]. При этом должны учитываться как общие требования, так и специфические свойственные отдельным отраслям, в том числе связанными с транспортно-логистической

[1] По материалам информационного сообщения «Путин назвал точное число введенных против России санкций. Эта цифра бьет рекорды: Госэкономика: Экономика: Lenta.ru». Интернет-источник: URL: https://lenta.ru/articles/2025/03/18/putin-nazval-chislo-vvedennyh-protiv-rossii-sanktsiy/ (дата обращения: 16.05.2025).

Таблица 1

Динамика экспорта отдельных стран в Россию по коду ТН ВЭД ЕАЭС 8471 «Вычислительные машины и их блоки, магнитные или оптические считывающие устройства, машины для переноса данных на носители информации в кодированной форме и машины для обработки подобной информации», млн долл. США[2]

Dynamics of exports of individual countries to Russia under the EAEU TN VED code 8471 "Computers and their units, magnetic or optical reading devices, machines for transferring data to storage media in coded form and machines for processing such information", in millions of US dollars

Страна	2013 г.	2015 г.	2017 г.	2019 г.	2021 г.	2022 г.	2023 г.	2024 г.
Китай	1915,4	1181,1	1675,6	2065,2	3301,5	2931,5	2916,8	3172,8
Чехия	492,1	359,1	327,7	310,9	305,5	71,7	0,001	0
Германия	390,3	109,4	141,2	144,9	171,7	25	0,4	0,4
Казахстан	186,2	4,3	1,5	2,8	0,8	296,8	125	70,5
Вьетнам	115,5	96	55,8	64	54,1	10,9	3	0
США	83,2	113,8	79,8	80,6	98,9	16,5	7,2	7,2
Польша	67,9	60,7	129,9	250,3	424,3	63,3	0,3	0,06
Великобритания	54,3	16,1	23,8	14	17,4	1,6	0	0
Франция	48,5	8,1	16,1	20,5	27,4	6,3	0,1	0,001
Индия	1,3	0,6	13,3	3,2	6,4	31,7	86	500

инфраструктурой [5]. В условиях активного развития и большого интереса со стороны многих стран к Арктике российская инфраструктура Северного морского пути и цифровые решения для ее сопровождения также требуют эффективных отказоустойчивых решений как в технологическом плане, так и учитывающих правовые и экономические аспекты.

В сложившейся ситуации отечественные исследователи уделяют большое внимание комплексному подходу обеспечения киберустойчивости критической информационной инфраструктуры и на уровне информационных систем, и на уровне отдельных сервисов и служб, а также автоматизированных систем управления [6]. Исследователями уделяется все больше внимания разработке новых методов оценки КИИ [7], систем классификации, устанавливающих классы защищенности для всей совокупности видов значимых объектов с позиции единой совокупности критериев [8] и их показателей [9], а также построению моделей управления рисками [10] и информационной безопасностью КИИ [11], внедрению комплексных решений защиты, интегрирующих в себе функционал SIEM-, DCAP- и DLP-систем [12].

В связи с этим актуальным становится развитие национальных решений, отражающих отказоустойчивость и безопасность инфраструктуры, а зарубежные решения должны находить именно полноценное импортозамещение. При этом импортозамещение должно осуществляться не как временная мера, а как элемент долгосрочной стратегии технологического суверенитета, направленной на укрепление национальной безопасности

[2] По данным запросов к базе данных TradeMap. Интернет-источник: URL: https://www.trademap.org/ (дата обращения: 20.05.2025).

и независимости в области КИИ. Даже после возможного снятия санкций и стабилизации международной политической обстановки необходимость в развитии отечественных технологий останется приоритетной задачей. Целью исследования является структуризация рисков и угроз устойчивости критической информационной инфраструктуры с учетом текущей зависимости от иностранного программного обеспечения и оборудования. В этом контексте далее обратимся к технологическим, правовым и экономическим аспектам импортозамещения.

Проанализируем более подробно ключевые технологические риски, связанные с зависимостью от иностранного программного обеспечения, использованием оборудования с закрытой архитектурой, а также прекращением технической поддержки и обновлений. Рассмотрены конкретные примеры последствий санкций для российских организаций, основанных на достоверных источниках и подтвержденных фактах.

Технологические аспекты

Зависимость от иностранного ПО (*ОС*, *СУБД*, *системы виртуализации*). Многие объекты КИИ в России исторически работают на зарубежном ПО, включая операционные системы (например, Windows, коммерческие дистрибутивы Linux), системы управления базами данных (Oracle Database, Microsoft SQL Server, IBM DB2) и платформы виртуализации (VMware vSphere, Citrix Hypervisor). Такая зависимость означает критическую уязвимость: в условиях санкций иностранные правообладатели могут приостановить предоставление своих продуктов и услуг. В результате организации рискуют остаться без лицензий, обновлений безопасности и технической поддержки, необходимых для стабильной и безопасной работы КИИ.

После ужесточения санкций с марта 2022 г. ведущие вендоры ПО, такие как Microsoft, Oracle и VMware, объявили о сворачивании бизнеса в России, прекратив продажи, поддержку и обновления. Даже открытое ПО, поддерживаемое иностранными компаниями, оказалось под вопросом: к примеру, Red Hat прекратила поддержку своих Linux-дистрибутивов для российских клиентов. Это привело к невозможности получать обновления безопасности и исправления ошибок, что трансформировало зависимость от иностранного ПО в риск правовой и технологической незащищенности. Некоторые организации были вынуждены использовать «серые схемы» для закупки иностранного ПО, что повышает вероятность инцидентов, включая кибербезопасностные.

Использование оборудования с закрытой архитектурой. Проприетарные аппаратные решения – сетевое и телекоммуникационное оборудование Cisco, маршрутизаторы и серверы IBM, а также инфраструктурные системы от Nokia, Ericsson, HP Enterprise, Dell EMC создают эффект «vendor lock-in», делая организации критически зависимыми от одного поставщика. В условиях санкций поставщик может принять решение о прекращении поставок запасных частей и новых устройств, а также об отключении сервисов активации и обновления ПО, что становится критическим фактором риска.

Cisco Systems полностью прекратила бизнес в России, деактивировала облачные Smart-аккаунты для обновления прошивок на ее маршрутизаторах и коммутаторах и даже уничтожила нераспроданные запасы оборудования на сумму ~3 млрд руб., чтобы техника не досталась незапланированным получателям[3]. Это не просто уход с рынка, а активное действие по предотвращению использования их продукции, что подчеркивает риски долгосрочной зависимости от закрытых архитектур. Аналогично IBM свернула операции, заблокировала облачные сервисы, а HPE и Dell прекратили поставки серверов. В телекоммуникационной отрасли Tele2 Россия столкнулась со срывом поставок от Nokia и Ericsson[4]. Случай с «Байкал Электроникс», создающей российские процессоры, которая приостановила выпуск чипов Baikal-S из-за отказа тайваньской фабрики TSMC, демонстрирует, что даже наличие собственных разработок чипов недостаточно без контроля над всей производственной цепочкой. Таким образом, санкционное «эмбарго» на оборудование с закрытой архитектурой приводит к дефициту инфраструктурных компонентов, риску простоев и повышению издержек на срочное импортозамещение.

Риски прекращения техподдержки и обновлений. Прекращение технической поддержки и регулярных обновлений ПО, включая патчи безопасности, со стороны иностранных правообладателей программно-аппаратных комплексов является серьезной угрозой для стабильности и безопасности КИИ. Это приводит к постепенному моральному устареванию критических систем, накоплению уязвимостей и возникновению сбоев, которые невозможно оперативно устранить.

С уходом вендоров доступ к обновлениям был ограничен или полностью закрыт. Например, пользователи оборудования Cisco и ПО VMware утратили доступ к новым версиям и патчам. Массовое неисполнение иностранными компаниями договорных обязательств по технической поддержке привело к судебным разбирательствам (например, «Мегафон» добился возврата 70 млн руб. за предоплаченную техподдержку ПО за техподдержку Red Hat[5]). В то же время другим организациям вернуть деньги не удалось – компаниям приходилось принимать убытки и переходить на собственное обслуживание систем. Крупные клиенты Oracle и IBM остались без официальной помощи в случае сбоев.

Риски прекращения обновлений и поддержки носят отложенный, но кумулятивный характер, приводя к накоплению «технического долга» и снижению надежности КИИ в долгосрочной перспективе. Для обеспечения технологической устойчивости КИИ необходимы меры по ускоренному переходу на технологически независимые решения. Российские власти и

[3] Американская Cisco уничтожила запчасти для оборудования в России. URL: https://www.cnews.ru/news/top/2022-10-12_bezhavshij_iz_rossii_red_hat_ne; https://www.forbes.ru/tekhnologii/487184-amerikanskaa-cisco-unictozila-zapcasti-dla-oborudovania-v-rossii-na-1-9-mlrd-rublej, свободный (дата обращения: 26.05.2025).

[4] Суд частично удовлетворил иск Tele2 к Ericsson из-за недопоставок оборудования. URL: https://www.interfax.ru/business/919137, свободный (дата обращения: 26.05.2025).

[5] Бежавший из России Red Hat не оказал техподдержку компании. URL: https://www.cnews.ru/news/top/2022-10-12_bezhavshij_iz_rossii_red_hat_ne, свободный (дата обращения: 26.05.2025).

отраслевые регуляторы уже отметили данную проблему – например, отмечалось, что к началу марта 2022 г. десятки компаний прекратили работу в России, прервались поставки техники и ПО, что послужило импульсом для программ импортозамещения. Несмотря на принимаемые меры, описанные инфраструктурные риски остаются существенным вызовом до полной реализации стратегий технологической независимости.

Правовые аспекты

Импортозамещение КИИ в России представляет собой сложный и многоэтапный процесс, требующий комплексного подхода к замене иностранных технологий, в том числе с учетом правовых аспектов, требований регуляторов, сертификации и национальных стандартов. Создание нормативно-правовых условий для импортозамещения также относится к правовым аспектам, требующим учета.

Решением проблемы технологического суверенитета в ключевых отраслях, включая кибербезопасность, является переход на отечественные, проверенные и надежные решения. Для стимулирования импортозамещения в секторе кибербезопасности Президентом и Правительством Российской Федерацией приняты основные нормативные документы. Так, для значимых объектов КИИ Указ Президента № 166 от 30.03.2022 г. установил запрет на приобретение иностранного ПО без согласования с уполномоченным органом с 31.03.2022 г. и обязал осуществить переход на российскую продукцию к 1 января 2025 г. Позднее Федеральный закон № 58-ФЗ от 07.04.2025 г. продлил сроки перехода до 1 сентября 2025 г. Указ Президента № 250 от 01.05.2022 г. потребовал от государственных организаций приведения стратегий в области информационных технологий и цифровизации в соответствии с требованиями информационной безопасности, а также ввел дополнительные меры по ее обеспечению. Во исполнение данных Указов принято Постановление Правительства № 1478 от 22.08.2022 г., которое установило строгие требования к ПО, применяемому государственными структурами и субъектами КИИ. Все используемое ПО должно быть включено в «Единый реестр российских программ», что подтверждает его происхождение и функциональность. Иными словами, на объектах КИИ должны внедряться сертифицированные отечественные продукты.

ФСТЭК является основным регулирующим органом, ответственным за разработку норм безопасности и аттестацию информационных систем, кроме секретных сведений согласно «Положению по аттестации объектов информатизации по требованиям безопасности информации», утвержденному Гостехкомиссией РФ 25.11.1994 г., а также приказами ФСТЭК № 235 от 21.12.2017 г. и № 239 от 25.12.2017 г. ФСБ отвечает за безопасность секретной информации и криптографических средств. Сертификация ФСБ необходима для ПО, применяющего алгоритмы шифрования, одобренные для использования в России. Требования к сертификации криптографических средств ФСБ обычно не являются общедоступными, должно быть специальное разрешение для доступа.

Процесс сертификации включает оценку функциональности ПО, стабильности и устойчивости к уязвимостям, что приводит к улучшению общего качества отечественных продуктов, предоставляя отечественным поставщикам ПО конкурентное преимущество перед зарубежными решениями, особенно в контексте государственных закупок и развертывания КИИ. Данные требования можно рассмотреть на примере оборудования и программного обеспечения.

Серверное оборудование. Сравнительный анализ отечественных и зарубежных серверных и сетевых решений (табл. 2) показывает наличие конкурентоспособных российских продуктов. Отечественные серверные решения, такие как YADRO VEGMAN R220 G2 и Гравитон С2122, обладают достаточной вычислительной мощностью для большинства прикладных задач на объектах КИИ и включены в Единый реестр российской радиоэлектронной продукции Минпромторга.

Однако серверы на базе отечественных процессоров «Эльбрус» существенно уступают по производительности. В области сетевого оборудования отечественные коммутаторы, например, Yadro KORNFELD D2132, обладают достаточной функциональностью для корпоративных сетей КИИ, но зарубежные аналоги (Juniper EX4650) обеспечивают более высокую

Таблица 2

Сравнительные характеристики зарубежных и российских серверов
Comparative characteristics of foreign and Russian servers

Критерий	Dell PowerEdge R740[6]	Cisco UCS C220 M5[7]	YADRO VEGMAN R220 G2[8]	Сервер «Эльбрус 804» (ТВГИ. 466535.217)[9]	Гравион С2122[10]
Поддержка ОС	Windows Server, Linux	Windows Server, Linux	Astra Linux SE, Альт, РЕД ОС, SpaceVM, РОСА, vStack и др.	Эльбрус ОС, Astra Linux, Альт	Astra Linux SE, Альт Сервер, ОС Лотос, ОПО Эльбрус
Включен в реестр	Нет	Нет	Да	Да	Да

[6] Dell. PowerEdge R740. Технический паспорт. [Электронный ресурс]. URL: https://i.dell.com/sites/csdocuments/shared-content_data-sheets_documents/en/poweredge-r740-spec-sheet.pdf, свободный (дата обращения: 27.04.2025).

[7] Cisco Systems. UCS C220 M5 Server. Technical Specifications. [Электронный ресурс]. URL: https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m5-sff-specsheet.pdf, свободный (дата обращения: 27.04.2025).

[8] YADRO. Сервер VEGMAN Rx20 G2. Технический паспорт. [Электронный ресурс]. URL: https://st.yadro.com/docs/VEGMAN/YADRO_VEGMAN_Rx20-G2_DS_RUS.pdf, свободный (дата обращения: 27.04.2025).

[9] АО «МЦСТ». Описание сервера «Эльбрус 804». [Электронный ресурс]. URL: https://www.mcst.ru/elbrus_804, свободный (дата обращения: 27.04.2025).

[10] Karma-Group. Сервер 2U Гравитон С2122Э. [Электронный ресурс]. URL: https://www.karma-group.ru/catalog/servery-graviton/s2000e/s2122e/, свободный (дата обращения: 27.04.2025).

плотность портов и расширенный функционал. Это указывает на частичную, но не полную конкурентоспособность отечественных решений, что может привести к «нишевому» суверенитету, где высоконагруженные и передовые системы останутся уязвимыми. Для обеспечения устойчивого технологического суверенитета требуется стратегическое наращивание компетенций и производственных мощностей в сфере ИТ-инфраструктуры.

Программное обеспечение. Переход на отечественные операционные системы в инфраструктуре КИИ – одна из ключевых задач в условиях импортозамещения. Для оценки возможностей и ограничений таких решений проведен сравнительный анализ ключевых характеристик современных операционных систем: архитектурная поддержка, открытость кода, наличие сертификаций ФСТЭК и ФСБ, а также регистрация в Едином реестре российского ПО. Результаты анализа сведены в табл. 3 для наглядного представления и последующей интерпретации.

Таблица 3

Сравнительная характеристика отечественных и зарубежных операционных систем для КИИ по сертифицированным исполнениям

Comparative characteristics of domestic and foreign operating systems for critical information infrastructure based on certified implementations

Параметр	Astra Linux[11]	РЕД ОС[12]	ОС «Альт»[13]	Windows[14]	Ubuntu[15]
Разработчик	«Группа Астра» (АО «НПО РусБИТех»)	ООО «РЕД СОФТ»	ООО «Базальт СПО»	Microsoft Corp.	Canonical Ltd.
В реестре российского ПО[16]	Да (№ 369)	Да (№ 3751)	Да (№ 1292)	Нет	Нет
Сертификация ФСТЭК[17]	Сертификат № 2557	Сертификат № 4060	Сертификат № 3866	Сертификат № 292/1/1 (истек 13.04.2021)	Нет
Сертификация ФСБ[18]	Есть (класс 1Б, разрешено для обработки гостайны)	Нет	Есть (только ограниченный доступ, класс АК3)	Есть (только ограниченный доступ, классы АК2/АК3)	Нет

[11] Astra Linux: сайт. URL: https://rusbitech.ru/products/os/astra-linux-se (дата обращения: 24.05.2025).

[12] РЕД ОС: сайт. URL: https://redos.red-soft.ru/ (дата обращения: 24.05.2025).

[13] ОС «Альт»: сайт. URL: https://alt-linux.ru/ (дата обращения: 24.05.2025).

[14] Microsoft Support: сайт. URL: https://support.microsoft.com/ru-ru/windows. (дата обращения: 24.05.2025).

[15] Ubuntu: официальный сайт. URL: https://ubuntu.com/ (дата обращения: 24.05.2025).

[16] Единый реестр российских программ для электронных вычислительных машин и баз данных: сайт. URL: https://reestr.digital.gov.ru/ (дата обращения: 24.05.2025).

[17] Реестр сертифицированных продуктов ФСТЭК России: сайт. URL: https://reestr.fstec.ru/reg3 (дата обращения: 24.05.2025).

[18] Центр лицензирования, сертификации и защиты государственной тайны ФСБ России: сайт. URL: http://clsz.fsb.ru/clsz/certification.htm (дата обращения: 24.05.2025).

Проведенный анализ позволяет заключить, что переход на отечественные операционные системы в инфраструктуре КИИ возможен как с точки зрения обеспечения безопасности, так и выполнения требований регулятора. Отечественные решения, представленные в табл. 3, обладают необходимыми характеристиками для замещения зарубежных аналогов: они сертифицированы ФСТЭК и ФСБ, поддерживают широкий спектр архитектур, включены в Единый реестр российского ПО и ориентированы на работу в защищенных информационных системах.

Несмотря на соответствие формальным требованиям, при переходе на отечественные операционные системы возможны определенные сложности, такие как ограничение функционала вследствие удаления потенциально небезопасных компонентов при сертификации, недостаточная поддержка специализированного ПО и драйверов, необходимость развития компетенций для администрирования и эксплуатации отечественных систем.

Переход на использование отечественного инженерного и промышленного ПО еще десятилетие назад был заявлен в качестве одного из наиболее значимых мероприятий по обеспечению технологического суверенитета промышленных предприятий России. Однако импульс масштабной разработке и началу активного внедрения российских решений был дан в 2022 г., когда это стало частью государственной политики. Профильные органы власти начали осуществлять оперативный мониторинг и контроль ситуации, а также внедрили серьезные меры поддержки промышленности и разработчиков таких решений.

Существующие решения, хотя и приемлемы, но не всегда полностью удовлетворяют все потребности пользователей или неконкурентны по цене. Если функциональность и стоимость отечественных продуктов не будут улучшаться, предприятия могут использовать их не из-за преимуществ, а из-за отсутствия альтернатив, что может привести к снижению эффективности и конкурентоспособности в долгосрочной перспективе. Для преодоления ограниченной функциональности и оптимизации стоимости требуется не только государственная поддержка, но и создание конкурентной среды среди отечественных разработчиков, а также эффективных механизмов обратной связи от конечных пользователей для постоянного улучшения продуктов и более подробный учет экономических аспектов импортозамещения и обеспечения безопасности и отказоустойчивости КИИ.

Экономические аспекты

Одним из наиболее заметных последствий санкционной политики стал резкий сдвиг в структуре ИТ-рынка. Уход из России крупнейших международных вендоров освободил значительные рыночные ниши, что стимулировало рост спроса на отечественные программные и аппаратные решения и развитие альтернативных поставщиков и интеграторов. Согласно отчетам Ассоциации российских разработчиков ПО «Руссофт», в 2023 г. совокупная выручка российских ИТ-компаний увеличилась на 17 %. Однако этот рост происходил на фоне высокого уровня неопределенности, кадрового

дефицита и ограниченного доступа к современным технологиям производства (в том числе микроэлектронике и R&D-компетенциям). В долгосрочной перспективе такой рост требует значительных инвестиций в НИОКР и преодоления кадрового дефицита, иначе отечественные решения могут оказаться функционально или технологически неконкурентоспособными, что приведет к сохранению зависимости или отставанию от мировых лидеров.

Санкционные ограничения привели к увеличению совокупной стоимости владения (Total Cost of Ownership, TCO) ИТ-инфраструктурой, особенно в контуре КИИ. Уход поставщиков лицензионного ПО и оборудования вызвал необходимость его срочной замены или миграции, что потребовало привлечения внешних консультантов, проведения аудитов, доработки архитектурных решений и внедрения дополнительных защитных мер.

По данным Минцифры и ФСТЭК, доля иностранного ПО в российских компаниях, управляющих объектами КИИ, составляет 30–40 %, и лишь 15–20 % государственных компаний полностью перешли на отечественное ПО к концу 2024 г. В целом доля используемого российского ПО увеличивается и по итогам 2024 г. превысила 50 % (табл. 4).

Таблица 4

Динамика доли организаций, использующих российское ПО[19]

Dynamics of the share of organizations using Russian software

Профиль решаемых задач	2021 г.	2024 г.	Изменение, п.п.
По всем задачам	35,6	51,1	+15,5
Управление ресурсами и производством	57,9	68,7	+10,8
Проектирование и моделирование	32,1	49,7	+17,6
Управление технологическими процессами	32,7	47,3	+14,6

По оценкам Минцифры РФ, затраты на обслуживание корпоративных информационных систем в 2023 г. выросли в среднем на 30–40 % (рис. 1) по сравнению с докризисным уровнем и включали закупку оборудования по параллельному импорту по завышенным ценам, адаптацию под несовместимые отечественные решения, увеличение затрат на информационную безопасность и невозможность заключения SLA с международными вендорами. Кроме того, нестабильность поставок и технологическая неопределенность усилили потребность в резервировании ресурсов, что также увеличило эксплуатационные издержки субъектов КИИ.

Ограничение доступа к зарубежным программным и аппаратным продуктам в ряде случаев привело к прямым потерям данных и простоям в функционировании компонентов КИИ, особенно в секторах, где отсутствовали технологически зрелые аналоги на внутреннем рынке. В телекоммуникационном секторе зафиксированы нарушения в работе магистраль-

[19] Из доклада Председателя Правительства РФ М.В. Мишустина на конференции «Цифровая индустрия промышленной России» (ЦИПР 2024, май). https://cipr.ru/

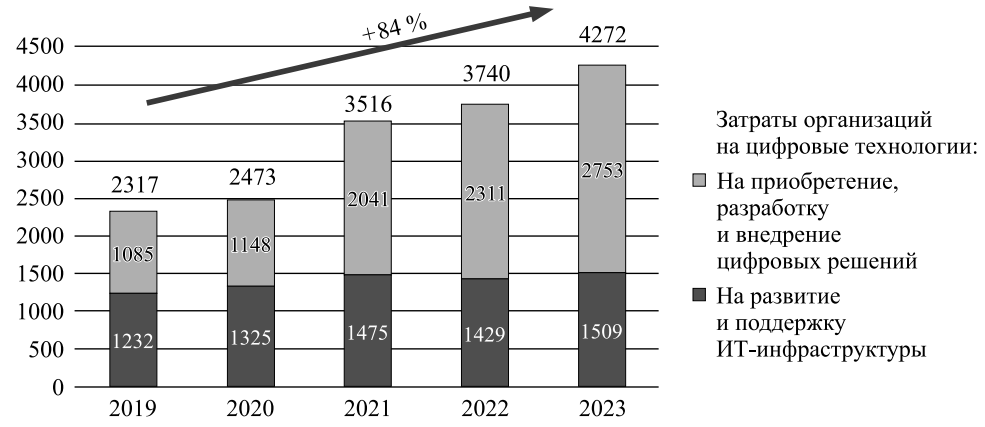


Рис. 1. Динамика корпоративных расходов на цифровые технологии, трлн руб.
Dynamics of corporate spending on digital technologies, trillion rubles

ной сетевой инфраструктуры из-за прекращения поставок компонентов от Ericsson, Nokia и Huawei, а также недоступности обновлений для оборудования Cisco и Juniper. В ряде регионов отмечались перебои в работе государственных информационных систем из-за недоступности облачных платформ (IBM Cloud, VMware Cloud). В банковском секторе и отрасли ТЭК прекращение обновлений для СУБД Oracle и SAP дестабилизировало работу информационно-аналитических платформ. При этом отсутствие полностью совместимых отечественных решений создало риски для целостности данных и увеличило вероятность бизнес-простоев.

В целом с аппаратным обеспечением ситуация напряженная: 75 % ИТ-инфраструктуры российских организаций по-прежнему базируется на зарубежных решениях. Многие компании предпочитают заменять западные ИТ-решения китайскими аналогами, что лишь частично решает проблему цифрового суверенитета.

Ключевыми проблемами остаются высокая стоимость перехода, недостаток функционала некоторых отечественных продуктов и несовместимость с существующими системами. Для их решения требуется активное развитие отечественных технологий, финансовая поддержка, совершенствование нормативной базы и особенно подготовка кадров.

Согласно отчету, опубликованному Ростелеком-Солар в 2023 г., потребность в специалистах по информационной безопасности в России оценивается в десятки тысяч человек. Поскольку кибербезопасность – молодая и динамично развивающаяся сфера, требующая постоянного обновления знаний и навыков специалистов, существующие образовательные программы в данной области зачастую не успевают за изменениями ландшафта угроз и технологическим прогрессом и требуют обновления учебных курсов [13, 14]. Кроме того, низкий уровень оплаты труда в государственных организациях и на предприятиях, обеспечивающих защиту КИИ, а также ограниченные возможности карьерного роста, способствуют оттоку кадров в коммерческий сектор и международные организации, которые зачастую предлагают более высокие зарплаты и привлекательные условия труда.

Указанные потери подчеркивают критическую значимость формирования автономной и отказоустойчивой цифровой среды в рамках стратегий импортонезависимости и требуют соответствующих методологических и методических подходов, отвечающих современным вызовам.

Методология импортозамещения

Импортозамещение КИИ в России представляет собой сложный и многоэтапный процесс, требующий комплексного подхода к замене иностранных технологий. Этот процесс включает несколько ключевых стратегий:

– поэтапная замена – предполагает постепенный переход от иностранных решений к отечественным аналогам, минимизируя риски несовместимости и сбоев. Приоритет отдается замене ПО (Astra Linux, РЕД ОС, МойОфис, RuStore);

– гибридные решения – комбинирование российских и нейтральных (не подсанкционных) технологий, таких как Open Source решения (Linux, Kubernetes, PostgreSQL), с отечественными разработками для создания высоконадежных систем;

– локализация производства – создание совместных предприятий с дружественными странами (Китай, Индия) для использования их производственных мощностей и опыта в создании отечественных решений, например, производство телекоммуникационного оборудования и серверов на базе процессоров Baikal и Elbrus.



Рис. 2. Блок-схема этапов импортозамещения в КИИ
Flowchart of import substitution stages in critical information infrastructure

Схема, представленная на рис. 2, позволяет визуально отразить комплексный и многоэтапный характер процесса импортозамещения, демонстрируя его системность и последовательность ключевых шагов, от замены ПО до локализации производства и оптимизации цепочек поставок.

Выводы

Успешное импортозамещение в КИИ является стратегической целью для обеспечения национальной безопасности и технологического суверенитета Российской Федерации. Комплексный анализ выявил глубокую зависимость от иностранных технологий, усугубленную санкционным давлением, что привело к значительным инфраструктурным и экономическим

рискам, включая потерю данных, простои систем и рост стоимости владения. Снятие санкций не устранит эти риски полностью из-за циклического характера геополитического давления и потенциальных скрытых угроз в иностранных технологиях.

Реализация стратегии импортозамещения требует системного подхода, включающего поэтапную замену ПО, внедрение гибридных решений и локализацию производства аппаратных средств, в том числе через совместные предприятия с дружественными странами. Однако существуют серьезные вызовы, такие как недостаточная функциональность некоторых отечественных продуктов и, что особенно критично, острая нехватка квалифицированных кадров для разработки, внедрения и поддержки российских решений. Недостаток специалистов напрямую угрожает качеству, надежности и устойчивости КИИ, увеличивает риски кибератак и затрудняет оперативное реагирование.

Для достижения истинного технологического суверенитета необходимы не только государственно-частное партнерство, инвестиции в НИОКР и активное развитие отечественных технологических решений, но и системное решение кадровой проблемы, создание конкурентной среды для российских разработчиков и обеспечение постоянного улучшения продуктов на основе обратной связи от пользователей. Только такой всеобъемлющий подход позволит сформировать устойчивую и независимую цифровую среду для критически важных объектов, гарантируя долгосрочную стабильность и безопасность страны.

Список источников

1. *Остроумов О.А.* Проблема обеспечения функциональной устойчивости систем критически важных объектов // Электросвязь. 2022. № 1. С. 38–42. DOI: 10.34832/ELSV.2022.26.1.005.
2. *Горохова С.С.* О некоторых аспектах информационной безопасности в Российской Федерации // Современный юрист. 2018. № 2 (23). С. 128–138.
3. *Михнев И.П.*, *Михнева С.В.*, *Айвазян А.Г.*, *Серкина Е.П.* Правовое регулирование деятельности в сфере информационной безопасности в Российской Федерации: достижения, проблемы и перспективы развития // Вестник Алтайской академии экономики и права. 2018. № 6. С. 227–233.
4. *Дремлюга Р.И.*, *Зотов С.С.*, *Павлинская В.Ю.* Критическая информационная инфраструктура как предмет преступного посягательства // Азиатско-Тихоокеанский регион: экономика, политика, право. 2019. № 2. С. 130–139. DOI: 10.24866/1813-3274/2019-2/130-139.
5. *Семенов С.А.* Морская кибербезопасность в России // Транспорт Российской Федерации. 2019. № 3 (82). С. 11–14.
6. *Минаев В.А.*, *Королев И.Д.*, *Зеленцова Е.В.*, *Захарченко Р.И.* Критическая информационная инфраструктура: оценка устойчивости функционирования // Радиопромышленность. 2018. № 4. С. 59–67. DOI: 10.21778/2413-9599-2018-28-4-59-67.
7. *Калашников А.О.*, *Михалевич И.Ф.* Анализ систем классификации защищенности автоматизированных и информационных систем значимых объектов критической информационной инфраструктуры Российской Федерации // Информация и безопасность. 2018. № 1 (21). С. 28–37.
8. *Павлов Е.О.*, *Резниченко С.А.* Подходы к обеспечению безопасности объектов критической информационной инфраструктуры // Журнал высоких гуманитарных технологий. 2024. № 3 (6). С. 32–38.

9. *Бакулин М.А.* Управление рисками нарушения информационной безопасности значимых объектов критической информационной инфраструктуры // Системная инженерия и информационные технологии. 2023. № 5 (14). С. 78–87. DOI: 10.54708/2658-5014-SIIT-2023-no5-p78.
10. *Калашников А.О.*, *Аникина Е.В.* Модель управления информационной безопасностью критической информационной инфраструктуры на основе выявления аномальных состояний (Часть 1) // Информация и безопасность. 2018. № 2. С. 145–154.
11. *Морозов В.Е.*, *Милославская Н.Г.* Комплексные решения для минимизации внутренних угроз информационной безопасности // Вопросы кибербезопасности. 2024. № 5 (63). С. 67–78. DOI: 10.21681/2311-3456-2024-5-67-78.
12. *Лившиц И.И.*, *Перлак П.В.* Практика обучения по направлению функциональной безопасности в университете ИТМО // Вопросы кибербезопасности. 2023. № 3 (55). С. 50–61. DOI: 10.21681/2311-3456-2023-3-50-61.
13. *Гавдан Г.П.*, *Иваненко В.Г.*, *Салкуцан А.А.* Обеспечение безопасности значимых объектов критической информационной инфраструктуры // Безопасность информационных технологий. 2019. № 4. С. 69–82. DOI: 10.26583/bit.2019.4.05.
14. *Корнеев Н.В.* Импортозамещение и информационная безопасность объектов топливно-энергетического комплекса сегодня и комплексная безопасность в будущем // Информационные технологии. Проблемы и решения. 2022. № 3 (20). С. 95–100.

References

1. Ostroumov O.A. Problema obespechenija funkcional'noj ustojchivosti sistem kriticheski vazhnyh ob#ektov [The Problem of Ensuring the Functional Stability of Critical Facility Systems], *Jelektrosvjaz'* [*Elektrosvyaz*], 2022, no. 1, pp. 38–42. DOI: 10.34832/ELSV.2022.26.1.005.
2. Gorohova S.S. O nekotoryh aspektah informacionnoj bezopasnosti v Rossijskoj Federacii [On Some Aspects of Information Security in the Russian Federation], *Sovremennyj jurist* [*Sovremennyy Yurist*], 2018, no. 2 (23), pp. 128–138.
3. Mihnev I.P., Mihneva S.V., Ajvazjan A.G., Serkina E.P. Pravovoe regulirovanie dejatel'nosti v sfere informacionnoj bezopasnosti v Rossijskoj Federacii: dostizhenija, problemy i perspektivy razvitija [Legal Regulation of Activities in the Sphere of Information Security in the Russian Federation: Achievements, Problems, and Development Prospects], *Vestnik Altajskoj akademii jekonomiki i prava* [*Bulletin of the Altai Academy of Economics and Law*], 2018, no. 6, pp. 227–233.
4. Dremljuga R.I., Zotov S.S., Pavlinskaja V.Ju. Kriticheskaja informacionnaja infrastruktura kak predmet prestupnogo posjagatel'stva [Critical information infrastructure as an object of criminal encroachment], *Aziatsko-Tihookeanskij region: jekonomika*, *politika*, *pravo* [*Asia-Pacific region: economics*, *politics*, *law*], 2019, no. 2, pp. 130–139. DOI: 10.24866/1813-3274/2019-2/130-139.
5. Semenov S.A. Morskaja kiberbezopasnost' v Rossii [Maritime cybersecurity in Russia], *Transport Rossijskoj Federacii* [*Transport of the Russian Federation*], 2019, no. 3 (82), pp. 11–14.
6. Minaev V.A., Korolev I.D., Zelencova E.V., Zaharchenko R.I. Kriticheskaja informacionnaja infrastruktura: ocenka ustojchivosti funkcionirovanija [Critical information infrastructure: assessment of operational sustainability], *Radiopromyshlennost'* [*Radiopromyshlennost*], 2018, no. 4, pp. 59–67. DOI: 10.21778/2413-9599-2018-28-4-59-67.
7. Kalashnikov A.O., Mihalevich I.F. Analiz sistem klassifikacii zashhishhennosti avtomatizirovannyh i informacionnyh sistem znachimyh ob#ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii [Analysis of security classification systems

for automated and information systems of significant objects of the critical information infrastructure of the Russian Federation], *Informacija i bezopasnost'* [*Information and Security*], 2018, no. 1 (21), pp. 28–37.
8. Pavlov E.O., Reznichenko S.A. Podhody k obespecheniju bezopasnosti ob#ektov kriticheskoj informacionnoj infrastruktury [Approaches to ensuring the security of critical information infrastructure objects], *Zhurnal vysokih gumanitarnyh tehnologij* [*Journal of high humanitarian technologies*], 2024, no. 3 (6), pp. 32–38.
9. Bakulin M.A. Upravlenie riskami narushenija informacionnoj bezopasnosti znachimyh ob#ektov kriticheskoj informacionnoj infrastruktury [Managing the Risks of Information Security Violations of Significant Objects of Critical Information Infrastructure], *Sistemnaja inzhenerija i informacionnye tehnologii* [*Systems Engineering and Information Technology*], 2023, no. 5 (14), pp. 78–87. DOI: 10.54708/2658-5014-SIIT-2023-no5-p78.
10. Kalashnikov A.O., Anikina E.V. Model' upravlenija informacionnoj bezopasnost'ju kriticheskoj informacionnoj infrastruktury na osnove vyjavlenija anomal'nyh sostojanij (Chast' 1) [Information Security Management Model for Critical Information Infrastructure Based on Anomalous State Detection (Part 1)], *Informacija i bezopasnost'* [*Information and Security*], 2018, no. 2, pp. 145–154.
11. Morozov V.E., Miloslavskaja N.G. Kompleksnye reshenija dlja minimizacii vnutrennih ugroz informacionnoj bezopasnosti [Comprehensive Solutions for Minimizing Internal Information Security Threats], *Voprosy kiberbezopasnosti* [*Cybersecurity Issues*], 2024, no. 5 (63), pp. 67–78. DOI: 10.21681/2311-3456-2024-5-67-78.
12. Livshic I.I., Perlak P.V. Praktika obuchenija po napravleniju funkcional'noj bezopasnosti v universitete ITMO [Training Practice in Functional Security at ITMO University], *Voprosy kiberbezopasnosti* [*Cybersecurity Issues*], 2023, no. 3 (55), pp. 50–61. DOI: 10.21681/2311-3456-2023-3-50-61.
13. Gavdan G.P., Ivanenko V.G., Salkucan A.A. Obespechenie bezopasnosti znachimyh ob#ektov kriticheskoj informacionnoj infrastruktury [Ensuring the Security of Significant Objects of Critical Information Infrastructure], *Bezopasnost' informacionnyh tehnologij* [*Information Technology Security*], 2019, no. 4, pp. 69–82. DOI: 10.26583/bit.2019.4.05.
14. Korneev N.V. Importozameshhenie i informacionnaja bezopasnost' ob#ektov toplivno-jenergeticheskogo kompleksa segodnja i kompleksnaja bezopasnost' v budushhem [Import Substitution and Information Security of Fuel and Energy Complex Facilities Today and Comprehensive Security in the Future], *Informacionnye tehnologii. Problemy i reshenija* [*Information Technology. Problems and Solutions*], 2022, no. 3 (20), pp. 95–100.

Сведения об авторах:

В.А. Кузнецова – кандидат экономических наук, руководитель группы, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», Сочи, Российская Федерация.

Д.В. Сплюхин – кандидат технических наук, ведущий инженер-исследователь, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», Сочи, Российская Федерация.

Е.В. Нехорошков – кандидат экономических наук, руководитель проекта, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», Сочи, Российская Федерация.

М.В. Ерофеев – кандидат физико-математических наук, ведущий научный сотрудник, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», Сочи, Российская Федерация.

И.А. Василенко – лаборант-исследователь, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», Сочи, Российская Федерация.

А.А. Бесчастнов – лаборант-исследователь, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», Сочи, Российская Федерация.

Information about the authors:

V.A. Kuznetsova – Candidate of Economic Sciences, Group Leader, Scientific Center for Information Technology and Artificial Intelligence, Sirius University of Science and Technology, Sochi, Russian Federation.

D.V. Splyukhin – Candidate of Technical Sciences, Leading Research Engineer, Scientific Center for Information Technology and Artificial Intelligence, Sirius University of Science and Technology, Sochi, Russian Federation.

E.V. Nekhoroshkov – Candidate of Economic Sciences, Project Manager, Scientific Center for Information Technology and Artificial Intelligence, Sirius University of Science and Technology, Sochi, Russian Federation.

M.V. Erofeev – Candidate of Physical and Mathematical Sciences, Leading Researcher, Scientific Center for Information Technology and Artificial Intelligence, Sirius University of Science and Technology, Sochi, Russian Federation.

I.A. Vasilenko – Research Assistant, Scientific Center for Information Technology and Artificial Intelligence, Sirius University of Science and Technology, Sochi, Russian Federation.

A.A. Beschatnov – Research Assistant, Scientific Center for Information Technology and Artificial Intelligence, Sirius University of Science and Technology, Sochi, Russian Federation.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

Статья поступила в редакцию	*10.07.2025*	*The article was submitted*	*10.07.2025*
Одобрена после рецензирования	*25.09.2025*	*Approved after reviewing*	*25.09.2025*
Принята к публикации	*09.10.2025*	*Accepted for publication*	*09.10.2025*