ЦИФРОВАЯ БЕЗОПАСНОСТЬ И ТЕХНОЛОГИЧЕСКИЙ СУВЕРЕНИТЕТ: НОВЫЕ ВЫЗОВЫ ДЛЯ МЕЖДУНАРОДНОГО БИЗНЕСА

В. И. Абрамов

доктор экономических наук, профессор кафедры управления бизнес-проектами Национального исследовательского ядерного университета «МИФИ», Москва, Россия
e-mail: viabramov@mephi.ru
ORCID: 0000-0002-9471-9408

А. В. Гаврилюк

аспирант факультета бизнес-информатики и управления комплексными системами Национального исследовательского ядерного университета «МИФИ», Москва, Россия
e-mail: xessov@yandex.ru
ORCID: 0009-0007-3194-4126

А. В. Путилов

доктор технических наук, профессор, декан факультета бизнес-информатики и управления комплексными системами Национального исследовательского ядерного университета «МИФИ», Москва, Россия
e-mail: avputilov@mephi.ru
ORCID: 0000-0002-5379-7506

Аннотация. В условиях ускоренной цифровой трансформации и нарастающей геоэкономической турбулентности проблемы обеспечения цифровой безопасности реального сектора экономики и достижения технологического суверенитета приобретают критическое значение для международного бизнеса. В данной статье проводится комплексный анализ ключевых рисков и стратегических вызовов, с которыми сталкиваются транснациональные компании в процессе цифровизации глобальных экономических отношений. Авторы рассматривают широкий спектр угроз – от учащающихся масштабных кибератак на критическую информационную инфраструктуру до прогрессирующей фрагментации цифрового пространства под воздействием протекционистских барьеров, технологических санкций и политики цифровой изоляции. Особое внимание в данной работе уделяется методологическим основам информационной безопасности и концептуальным подходам к построению технологического суверенитета, представляющим взаимосвязанные факторы обеспечения долгосрочной конкурентоспособности и устойчивого развития бизнеса в условиях глобальной нестабильности. На основе детального изучения практического опыта ведущих российских компаний, успешно адаптирующихся к новым реалиям, формулируются конкретные рекомендации по выстраиванию эффективных систем киберзащиты, локализации цифровых активов и построению стратегий технологической независимости. Результаты исследования представляют значительную ценность как для академического сообщества, изучающего трансформацию международных бизнес-моделей, так

и для практиков-руководителей компаний, специалистов по корпоративной безопасности и разработчиков цифровой политики, сталкивающихся с необходимостью пересмотра традиционных подходов в условиях кардинального изменения глобальной цифровой экосистемы.

Ключевые слова: цифровая безопасность, технологический суверенитет, международный бизнес, кибербезопасность, регулирование данных, цифровая экономика, санкционные риски, санкционное давление.

Поступила в редакцию: 06.05.2025
Принята к публикации: 29.05.2025

УДК 339.9
DOI: 10.24833/2949-639X-2025-2-12-28-42

Введение

Широкомасштабная цифровая трансформация, распространившись буквально на все области нашей действительности, успела стать неотъемлемой составной частью современного международного бизнеса. Глобальная взаимосвязанность, доступ к большим объемам данных, автоматизация производственных процессов – все это открывает новые возможности для роста и развития компаний. Однако вместе с тем цифровая эпоха порождает и новые вызовы, среди которых особое место занимают вопросы цифровой безопасности и обеспечения технологического суверенитета [8].

В процессе интенсивного продвижения информационных технологий и нарастания напряженности в геополитической сфере международный бизнес оказывается перед лицом непредвиденных проблем [12]. Кибератаки, утечки данных, промышленный шпионаж – эти и другие риски ставят под угрозу не только коммерческую тайну и финансовую стабильность компаний, но и их репутацию, а порой и само существование. Согласно исследованию McAfee[1], мировой ущерб от киберпреступности в 2020 г. превысил 1 трлн долл., что составляет более 1% мирового ВВП и подчеркивает масштаб угроз, с которыми сталкиваются компании, ведущие международное бизнес-взаимодействие.

В то же время технологический суверенитет, понимаемый как способность государств и компаний обеспечивать контроль над жизненно важными технологиями, инфраструктурой и информацией, приобретает все большую ценность и рассматривается как основной фактор достижения стратегической устойчивости. По мере роста уровня глобальной нестабильности и ужесточения санкционной конфронтации компании вынуждены пересматривать свои подходы к управлению цепочками поставок и сбыта, локализации данных и разработке собственных технологических решений. В России, например, вопросы обеспечения

[1] The Hidden Costs of Cybercrime. Cognizium. URL: https://cognizium.io/uploads/resources/McAfee%20-%20The%20Hidden%20Costs%20of%20Cybercrime%20-%202021%20-%20Jan.pdf (дата обращения: 20.04.2025).

технологического суверенитета активно обсуждаются в контексте импортозамещения и развития национальных IT-решений. Это подтверждается множеством научных статей в данном направлении, среди которых можно выделить работы заместителя президента Российской академии наук, руководителя Информационно-аналитического центра «Наука» РАН В. В. Иванова, который анализирует роль государственной политики в обеспечении технологической независимости и перехода национальной экономики к системе полного инновационного цикла [18].

В сложившихся условиях компаниям необходимо переосмыслить свои стратегии и адаптироваться к новым реалиям. Вопросы цифровой безопасности и технологического суверенитета становятся важнейшими факторами повышения конкурентоспособности и устойчивого развития в современном мире.

Проблема цифровой безопасности также тесно связана с вопросами конфиденциальности данных и защиты прав пользователей. Так, например, подчеркивается, что концентрация данных в руках ограниченного числа технологических компаний-гигантов создает риски не только для отдельных пользователей, но и для бизнеса в целом, поскольку он становится «заложником» монополий на данные [19]. Это особенно актуально для компаний, работающих на международном уровне, так как им необходимо соблюдать различные нормативные требования, такие как Общий регламент Европейского союза по защите данных (GDPR) и Федеральный закон Российской Федерации № 152-ФЗ «О персональных данных».

Целью данной статьи является анализ новых вызовов, связанных с цифровой безопасностью и технологическим суверенитетом, и поиск путей адаптации международного бизнеса к этим вызовам.

Методологической основой статьи является обзор научной литературы, анализ нормативно-правовых актов, а также изучение практического опыта международных компаний. В ходе исследования использованы методы сравнительного анализа, систематизации и обобщения данных. Отметим, что в данной работе понятия «цифровая безопасность», «информационная безопасность» и «кибербезопасность» принимаются как тождественные и определяются как комплекс мер, направленных на защиту информационных систем, сетей и данных от несанкционированного доступа, кибератак и прочих угроз.

Исследование

Теоретические основы цифровой безопасности и технологического суверенитета

В условиях стремительной цифровой трансформации мировой экономики обеспечение цифровой безопасности и достижение технологического суверенитета становятся ключевыми приоритетами для устойчивого развития национальных экономик, включая Россию. В России цифровая трансформация является

национальной целью, и во многих регионах активно реализуются стратегии повышения цифровой зрелости [3]. Создание региональных цифровых экосистем является перспективной формой повышения эффективности регионального управления и качества жизни людей [10]. Необыкновенно привлекательные перспективы появляются в результате стремительного эволюционирования технологий искусственного интеллекта в современном мире, но вместе с тем возникают и серьезные угрозы, связанные с их освоением и распространением. Прежде всего это касается практики применения искусственного интеллекта в государственном управлении [2]. Благодаря цифровой макросреде с использованием IoT-устройств в городах и регионах появляются гибридные формы ведения хозяйства, при которых управление инфраструктурными процессами осуществляется дистанционно, максимально объективно, в автоматическом режиме и с высокой эффективностью [4]. Именно опираясь на эти методы, ведется интенсивная работа над технологиями цифрового двойника как одной из самых перспективных технологий современности, дающей возможность для принятия управленческих решений с учетом логики «из будущего» [9]. В условиях формирования многополярного мира и роста конкуренции между странами, когда необходим результат, выраженный в увеличении воспроизводства социальных и экономических благ за счет инструментов цифровой экономики, построение цифровых двойников на территории России представляет собой целесообразный процесс. Его эффективность позволит региону, где реализован цифровой двойник, при снижении бюджетных расходов заметно увеличить объемы пополнения бюджета, снизить выбросы и перераспределить высвобожденные средства на социальные блага [5]. Однако этот процесс сопровождается растущими вызовами, связанными с необходимостью защиты критически важной инфраструктуры, обеспечения информационной безопасности и снижения зависимости от зарубежных технологий. Актуальность данной проблемы обостряется текущей геополитической ситуацией, которая выявила уязвимости российской экономики, связанные с использованием импортных программных решений, оборудования и облачных сервисов.

В условиях продолжающейся глобальной цифровизации проблема цифровой безопасности приобретает особую значимость, особенно для международного бизнеса, который опирается на цифровые технологии для управления логистическими цепочками, взаимодействия с контрагентами и хранения критически важных информационных ресурсов.

В основе цифровой безопасности лежит система из трех столпов:

- конфиденциальность, которая подразумевает ограничение доступа к информации для предотвращения ее несанкционированного разглашения и защиты частной жизни;
- целостность, предполагающая гарантию неизменности и точности информации во время ее обработки, хранения и передачи – данный компонент защищает данные от случайной или преднамеренной порчи;

- доступность, которая заключается в обеспечении надежного, оперативного и беспрепятственного доступа к информационным ресурсам для пользователей, имеющих соответствующие права.

Впервые данная концепция появилась в 1975 г. у ученых из Массачусетского технологического института Дж. Зальцера и М. Шредера [20] и получила название «Триада CIA», (Confidentiality – конфиденциальность, Integrity – целостность, Availability – доступность).

Среди ключевых угроз цифровой безопасности на современном этапе можно выделить следующие:

- скоординированные кибератаки, направленные на дестабилизацию работы информационных сервисов и ресурсов, зачастую производимые с использованием вредоносного программного обеспечения, фишинга, а также программ-вымогателей;
- утечки данных, к которым относятся как целенаправленные, так и случайные нарушения «целостности» информации;
- высокая зависимость от иностранных поставщиков информационно-технологических решений и программного обеспечения.

На текущем этапе понятие технологического суверенитета интерпретируется участниками академического сообщества различными способами, чаще всего с некоторыми уточнениями в зависимости от научной направленности и конечной цели проводимого исследования. Однако наиболее точное определение технологического суверенитета в контексте вопросов обеспечения цифровой безопасности можно представить как способность государства или предприятия контролировать критически важные технологии, инфраструктуру и данные, обеспечивая состояние их защищенности от внешних факторов.

Взаимосвязь цифровой безопасности и технологического суверенитета

Одной из стратегических целей технологического суверенитета Российской Федерации является обеспечение национальной безопасности и защиты данных через создание информационных систем высокой надежности, разработку собственных систем мониторинга и предупреждения киберугроз, а также поддержку законодательства, обеспечивающего защиту личной информации граждан [7].

Ключевую роль в глобальной цифровой экосистеме занимает международный бизнес, поскольку именно экономические институты различного уровня являются основными пользователями и разработчиками технологий. Вместе с тем в условиях геополитической турбулентности и усиления киберугроз международный бизнес первым попадает в зону риска и нуждается в защите.

Основные риски, с которыми сталкивается международный бизнес в условиях цифровой трансформации общества, и возможные способы их нейтрализации представлены в таблице 1.

Таблица 1

Риски цифровизации бизнеса и способы их нейтрализации

Риск	Характеристика	Способ смягчения последствий
Отсутствие подходов к управлению изменениями	Многие компании не имеют четкой стратегии для управления изменениями и интеграции инновационных решений, что потенциально затрудняет реализацию цифровых инициатив	Разработка и интеграция стратегий управления технологическими преобразованиями
Сложность использования новых технологий	Необходимость обладания специфическими компетенциями для использования нового программного обеспечения может препятствовать внедрению инноваций	Создание системы обучения и переквалификации кадров
Появление новых зон риска при обеспечении кибербезопасности	Развитие технологий искусственного интеллекта (ИИ) и больших данных дает злоумышленникам возможность создавать новые методы кибератак, что представляет собой серьезную угрозу	Фокусировка внимания на вопросах внутренней кибербезопасности компании, проведение регулярного аудита и обновление систем защиты
Использование программного обеспечения, разработанного за рубежом	Высокая степень зависимости бизнеса от иностранных разработок допускает возможность лоббирования политических интересов других стран путем ограничения доступа к технологиям	Сосредоточение внимания на использовании и развитии продуктов национального ИТ-сектора

Источник: составлено авторами на основе: [14–16].

Международный бизнес, как и любая иная экономическая деятельность, несомненно, обладает высоким уровнем риска в различных областях, однако в контексте цифровизации общества и нарастания геополитической напряженности на первый план выходят риски, связанные с использованием технологий как инструмента влияния на национальную экономику. В первую очередь, это представляет угрозу для логистических цепочек и ограничивает количество рынков сбыта для компаний с международными операциями.

Стоит отметить, что выработка стратегии минимизации и нейтрализации возможных рисков должна производиться в тесном взаимодействии государства и бизнеса, начиная с диверсификации существующих рисков и комплексной проработки каждой зоны риска.

Технологический суверенитет как стратегический императив

В условиях растущей зависимости международного бизнеса от цифровых технологий и усиления геополитических рисков технологический суверенитет становится не просто конкурентным преимуществом, но и стратегической необходимостью. Согласно исследованию BCG[2], компании, которые активно

[2] Annual Sustainability Report: From Bold Ideas to Exponential Impact. Boston Consulting Group (BCG). URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://media-publications.bcg.com/2023-Annual-Sustainability-Report-April-2024.pdf (дата обращения: 20.04.2025).

инвестируют в развитие собственных технологических решений, демонстрируют более высокую устойчивость к внешним неблагоприятным воздействиям на 30%, включая санкционные ограничения и киберугрозы. Данный феномен подчеркивает важность технологической независимости как ключевого условия долгосрочной конкурентоспособности.

Важным шагом на пути к технологическому суверенитету является локализация технологических решений, которая подразумевает создание и внедрение отечественных аналогов критически важных технологий, таких как операционные системы, системы управления базами данных, облачные платформы и решения для укрепления кибербезопасности. В России активно развиваются цифровые проекты, например, операционные системы семейства «Альт», Astra-Linux и РЭД ОС, а также продолжается работа над развитием отечественных процессоров «Байкал» и «Эльбрус». Следует учесть, что введение санкций в 2022 г. существенно повлияло на производство процессоров, которые выпускались тайваньской компанией “TSMC”, что вынудило разработчиков искать решения для бэкшоринга (переноса производственной деятельности на территорию России) и постепенно переходить от использования архитектуры ARM (которая также попала под санкции) к открытой архитектуре RISC-V [3].

Безусловно, решающим фактором в развитии национальных технологических решений и обеспечения цифровой безопасности является активная поддержка государством научных исследований в информационно-цифровой сфере, а также создание благоприятной среды для разработки и внедрения инноваций путем построения системы передачи знаний между научными учреждениями, бизнесом и государственными структурами.

В качестве примера эффективных моделей взаимодействия государства и науки для укрепления технологической независимости можно рассмотреть Китай, где для поддержки инновационной деятельности реализуется несколько государственных программ: «Искра», «Факел» и «863». В рамках данных мер действуют налоговые льготы, обеспечивается поддержание благоприятной научной среды и финансирование перспективных направлений развития из бюджета. Разница между программами выражается в их отраслевой направленности, что дает возможность охватить большой круг сфер деятельности. Кроме того, Китай уделяет особое внимание подготовке квалифицированных кадров для высокотехнологичных секторов, стимулируя обучение студентов в ведущих университетах мира. Для привлечения выпускников зарубежных вузов в рамках программы «Факел» создаются льготные условия для открытия малого бизнеса, что способствует их вкладу в развитие национальной экономики [6].

В России создаются инновационные центры и научные кластеры (Сколково и Иннополис), позволяющие эффективно объединять усилия науки, бизнеса и государства для работы над созданием новых технологических решений. Кроме того, государство активно финансирует ведущие университеты и научные

центры, такие как Московский физико-технический институт (МФТИ), Высшая школа экономики (ВШЭ) и Национальный исследовательский ядерный университет (НИЯУ МИФИ), которые занимаются исследованиями в области цифровых технологий. В 2018–2024 гг. в рамках Национального проекта «Цифровая экономика» более 3,5 тыс. ИТ-компаний получили государственное финансирование на поддержку проектов, реализуемых на основе российских ИТ-решений. Были выданы льготные кредиты на сумму около 85 млрд руб., а свыше 70 тыс. человек завершили обучение по проекту «Цифровые профессии»[3]. В качестве логического продолжения проекта «Цифровая экономика» с 1 января 2025 г. в России стартовал Национальный проект «Экономика данных».

Не менее важным аспектом укрепления технологического суверенитета в цифровой сфере является создание международных альянсов и партнерства в области развития передовых технологий. Так, например, Российский фонд прямых инвестиций (РФПИ) в конце 2024 г. объявил о создании Альянса БРИКС по развитию ИИ, к которому на первом этапе присоединились более 20 компаний из Бразилии, Индии, Ирана, Китая, Объединенных Арабских Эмиратов (ОАЭ) и России[4].

Для многих российских компаний 2022 г. стал годом испытаний и вызовов. Рассмотрим некоторые примеры адаптации их деятельности к стремительно меняющимся условиям международного бизнеса. По словам Г. Грефа, председателя правления Сбербанка, уход иностранных вендоров стал испытанием на прочность для технологических возможностей экосистемы Сбера, поскольку пришлось отражать кибератаки не только на собственную информационную инфраструктуру, но и защищать от угроз государственные институты и сервисы. Однако, согласно годовому отчету, именно проведенная цифровая трансформация позволила Сберу хорошо подготовиться к решению проблем 2022 г.

В частности, ключевыми результатами Сбера стали следующие:

- облачная платформа “Platform V” для работы по созданию высоконадежных и защищенных приложений всех уровней сложности и ряд других решений на базе собственных технологий послужили ответным решением на ~85% случаев ухода зарубежных компаний, обеспечив тем самым снижение числа нежелательных инцидентов на 6% при почти полуторакратном увеличении количества внедренных ИТ-изменений;
- Центр киберзащиты Сбербанка, построенный на базе отечественных решений, 90% из которых – разработки Сбера, а также собственные продукты

[3] Минцифры и игроки рынка подвели предварительные итоги цифровизации в 2024 г. ComNews. URL: https://www.comnews.ru/content/232692/2024-04-17/2024-w16/1008/mincifry-i-igroki-rynka-podveli-predvaritelnye-itogi-cif (дата обращения: 20.04.2025).

[4] РФПИ и 20 компаний из стран БРИКС создают альянс по развитию ИИ. Интерфакс. URL: https://www.interfax.ru/russia/997144 (дата обращения: 20.04.2025).

во всех ключевых сферах кибербезопасности, которые позволили компании отразить больше DDoS-атак, чем совокупно за предшествующие семь лет[5].

Также стоит упомянуть, что Сбер активно развивает собственную цифровую экосистему, которая объединяет множество сервисов. В ее основе лежит технология искусственного интеллекта собственной разработки, на базе которого функционирует голосовой ассистент «Салют» и устройства для умного дома. Финансовый эффект от внедрения ИИ в 2023 г. превысил 350 млрд руб.[6].

Не обошел стороной 2022 г. и Яндекс – российскую транснациональную компанию в области информационных технологий, буквально «разделив» компанию на российский Яндекс и нидерландскую Yandex N.V., которая ранее выступала в качестве головной компании. В 2024 г. была заключена сделка на сумму 457 млрд руб., в результате которой основная часть бизнеса была локализирована в России, а новой головной компанией стала МКПАО «Яндекс» – консорциум частных инвесторов во главе с менеджерами Яндекса[7].

Вместе с тем после прекращения поддержки сервисов Microsoft Office 365 Яндекс предложил пользователям собственную разработку – бизнес-платформу «Яндекс 360», включающую в себя сервисы для организации работы компаний[8]. Кроме того, в компании реализуется разработка множества собственных технологических решений на основе машинного обучения и ИИ. Значительно диверсифицировав свою деятельность через предложение пользователям широкого спектра сервисов – от заказа такси и географических информационных систем с прогнозом погоды до онлайн-магазина товаров и собственной платежной системы «Яндекс Пэй», – компания «Яндекс» заняла ведущие позиции на многих рынках, демонстрируя устойчивую тенденцию к долгосрочному и устойчивому росту[9]. В 2023 г. инвестиции Яндекса в цифровую безопасность составили более 6 млрд руб. – вдвое больше, чем годом ранее. Инвестиции были направлены на повышение защищенности пользовательских данных и инфраструктуры, а также на развитие технологий для борьбы с мошенниками[10]. В 2024 г. количество активных пользователей Яндекс GO превысило 50 млн чел.[11]

---

[5] Годовой отчёт ПАО «Сбербанк» за 2022 г. Часть 2. Управление и корпоративная практика. Официальный сайт для акционеров Сбербанка. URL: https://shareholder.sberbank.com/AR22/management/part-2/ (дата обращения: 20.04.2025).

[6] Сбер в цифрах и фактах. Годовой отчет ПАО «Сбербанк» за 2023 г. Официальный сайт для акционеров ПАО «Сбербанк». URL: https://shareholder.sberbank.com/AR23/ar/ru/facts-and-figures.html (дата обращения: 20.04.2025).

[7] Yandex N.V. согласовал продажу активов в России. Коммерсантъ. URL: https://www.kommersant.ru/doc/6493340 (дата обращения: 20.04.2025).

[8] От Microsoft к Яндекс: импортозамещение в действии. Цифровой блок НИУ ВШЭ. URL: https://it.hse.ru/news/751503747.html (дата обращения: 20.04.2025).

[9] Информация для инвесторов: рынки деятельности. Официальный сайт для инвесторов Яндекс. URL: https://ir.yandex.ru/about/markets (дата обращения: 20.04.2025).

[10] ESG-отчет ПАО «Яндекс» за 2022 г. Яндекс. URL: https://esg-library.mgimo.ru/upload/iblock/a30/1970dfjpzlo66a3spu30tczo7rlg7ziw/Otchet-YAndeksa.pdf (дата обращения: 20.04.2025).

[11] Финансовые результаты ПАО «Яндекс» за IV квартал 2024 г. Официальный сайт для инвесторов Яндекс. URL: https://ir.yandex.ru/financial-releases?year=2024&report=q4 (дата обращения: 20.04.2025).

Не менее интересным примером адаптации к динамично меняющимся внешним условиям является российский онлайн-сервис для заказа такси «Максим», попавший под санкции США еще в 2018 г., когда приложение компании было удалено из AppStore за организацию деятельности в Иране. Компания вышла из ситуации, передав бизнес местной организации, и сосредоточилась на поиске новых рынков. Сегодня онлайн-сервис используется в 20 странах мира, крупнейшими из которых являются Бразилия, Вьетнам, Индонезия, Малайзия и Мексика. Широкая диверсификация рынков и использование программного обеспечения собственной разработки позволяют компании успешно развиваться, независимо от внешних факторов.

Санкционные ограничения затронули и отечественную авиапромышленность, которая ранее была в значительной степени ориентирована на использование импортных комплектующих для производства самолетов. Например, самолет Sukhoi Superjet 100 (SSJ-100) был оснащен двигателями совместного производства российского НПО «Сатурн» и французской компании “Safran Aircraft Engines” (бывш. Snecma). Однако уже в марте 2025 г. состоялся первый полет SSJ с полностью российским двигателем ПД-8. Также в рамках программы импортозамещения для самолета SSJ осуществляется замена порядка 40 систем и агрегатов[12].

Таким образом, проведенный анализ практики компаний и научных исследований демонстрирует, что современные вызовы международного бизнеса связаны с необходимостью поддержания баланса между глобальной конкуренцией и требованиями технологического суверенитета и безопасности. Результаты анализа представлены в таблице 2.

Таблица 2

Актуальные вызовы цифровой безопасности бизнеса в условиях технологического суверенитета: стратегии минимизации рисков

Категория рисков	Последствия для бизнеса	Стратегии смягчения последствий
Глобальная технологическая конкуренция	Возрастающее давление конкурентной среды: необходимость внедрения инновационных решений и поддержания конкурентоспособности	Участие в международном технологическом сотрудничестве
Экстерриториальные экономические ограничения	Ограничение доступа к глобальным рынкам и технологиям	Развитие национального технологического потенциала и диверсификация международного сотрудничества
Технологическая зависимость	Риски нарушения цепочек поставок и технологической зависимости от иностранных компаний	Инвестиции в национальные НИОКР и концентрация на критически важных технологиях для обеспечения национального суверенитета

[12] Самолет Superjet с двигателями ПД-8 совершил первый полет. Ростех. URL: https://rostec.ru/media/news/samolet-superdzhet-s-dvigatelyami-pd-8-sovershil-pervyy-polet/ (дата обращения: 20.04.2025).

Категория рисков	Последствия для бизнеса	Стратегии смягчения последствий
Проблемы цифровой безопасности	Необходимость использования надежных мер кибербезопасности и соблюдения регуляторных требований	Внедрение прогрессивных подходов к обеспечению цифровой безопасности и взаимодействие с национальными программами в области кибербезопасности
Баланс между международным сотрудничеством и национальными интересами	Учет геополитических факторов и обеспечение технологического суверенитета	Участие в стратегическом международном партнерстве с приоритетным вниманием к национальному технологическому развитию

Источник: составлено авторами на основе: [1], [11], [13], [17].

Таким образом, в условиях цифровой трансформации и геополитических вызовов бизнесу необходимо сочетать инновации, международное сотрудничество и развитие отечественных технологий, что позволит минимизировать риски и обеспечить устойчивое развитие.

Заключение

На основании проведенного анализа можно сделать вывод о том, что цифровая безопасность и технологический суверенитет являются основой и необходимым условием устойчивого развития страны. Разработка эффективных стратегий адаптации, интеграция в бизнес-процессы отечественных технологических решений, а также тесное взаимодействие бизнеса и государства позволяют экономике минимизировать риски и вырабатывать эффективные меры противодействия вызовам современного мира.

Важно отметить, что достижение технологической независимости требует комплексного подхода, который в равной мере учитывает интересы государства частного сектора экономики. Кроме того, вопросы обеспечения технологической независимости тесно сопряжены с развитием человеческого капитала, что заслуживает отдельного внимания и детального изучения исследователями в дальнейшем.

ЛИТЕРАТУРА:

1. *Абдулов Р.Э., Реснов Д.Г.* Перспективы достижения технологического суверенитета и цифровизации в России на фоне беспрецедентного санкционного давления // Креативная экономика. 2022. Т. 16. № 12. С. 4591–4604.
2. *Абрамов В.И., Абрамов А.В., Столяров А.Д.* Инновационные тренды и вызовы использования генеративного искусственного интеллекта в управлении // Муниципальная академия. 2024. № 4. С. 200–210.

3. *Абрамов В.И., Андреев В.Д.* Первый год реализации программ цифровой трансформации в регионах России: проблемы и результаты // Вопросы государственного и муниципального управления. 2024. № 2. С. 110–128.
4. *Абрамов В.И., Андреев В.Д.* Перспективы использования интернета вещей при цифровой трансформации государственного и муниципального управления (на примере Финляндии) // Муниципальная академия. 2022. № 2. С. 34–42.
5. *Абрамов В.И., Андреев В.Д.* Сравнительный анализ цифровых двойников регионов // Информационное общество. 2023. № 4. С. 106–117.
6. *Абрамов В.И., Гаврилюк А.В., Путилов А.В.* Сравнение подходов к обеспечению технологического суверенитета в разных странах // Тренды развития современного общества: управленческие, правовые, экономические и социальные аспекты: сборник научных статей XIV Всероссийской научно-практической конференции (5–6 июня 2024 г., г. Курск). 2024. С. 15–21.
7. *Абрамов В.И., Гаврилюк А.В., Путилов А.В.* Технологический суверенитет: базовые принципы и стратегические цели // Управление экономикой, системами, процессами: сборник статей VIII Международной научно-практической. конференции «Международный институт рынка» (28 ноября 2024 г., г. Пенза). 2024. С. 11–18.
8. *Абрамов В.И., Гаврилюк А.В., Путилов А.В.* Технологический суверенитет – инструментарий обеспечения устойчивого развития страны // Экономические стратегии. 2025. № 3. С. 27–39.
9. *Абрамов В.И., Гордеев В.В., Столяров А.Д.* Цифровые двойники: характеристики, типология, практики развития // Вопросы инновационной экономики. 2024. Т. 14. № 3. С. 691–716.
10. *Абрамов В.И., Ломакин В.А., Столяров А.Д.* Цифровая экосистема региона как перспективная модель территориального развития экономики // Информационное общество. 2024. № 6. С. 6–27.
11. *Белоусов Ф.А., Иванова А.К., Неволин И.В.* Технологический суверенитет и глобальная конкуренция // Цифровая экономика. 2024. № 4 (30). С. 24–33.
12. *Толорая Г.Д.* БРИКС в мировых финансах и экономике. М.: МГИМО. 2024. 541 с.
13. *Гареев Т.Р.* Технологический суверенитет: от концептуальных противоречий к практической реализации // Terra Economicus. 2023. Т.21 (4). С. 38–54.
14. *Герасимов Б.Н.* Развитие экономических систем: теория, методология, практика: монография. Пенза: ПГАУ. 2024. 275 с.
15. *Гераськина Е.И.* Вызовы и угрозы информационной безопасности в российском обществе в XXI веке // Актуальные исследования. 2023. № 21 (151). С. 69–73.
16. *Головков С.С., Калинина И.А.* Ключевые риски цифровой трансформации бизнеса // Инновации и инвестиции. 2023. №3. С. 139–143.
17. *Дудин М.Н., Шкодинский С.В., Продченко И.А.* Экономические и инфраструктурные инструменты обеспечения государственного экономического суверенитета в цифровой экономике: опыт Российской Федерации и мира // Вопросы инновационной экономики. 2022. Т. 12. № 1. С. 57–80.
18. *Иванов В.В.* Основные направления государственной политики обеспечения технологического суверенитета // Экономика науки. 2024. Т. 10. №1. С. 10–20.
19. *Zuboff S.* The Age of Surveillance Capitalism: The Fight for A Human Future at the New Frontier of Power. N. Y.: Public Affairs. 2018. 717 p.
20. *Saltzer J.H.* The Protection of Information in Computer Systems // Proceedings of the IEEE. 1975. Vol. 63. No. 9. Pp. 1278–1308.

DIGITAL SECURITY AND TECHNOLOGICAL SOVEREIGNTY: EMERGING CHALLENGES FOR INTERNATIONAL BUSINESS

V. I. Abramov

Doctor of Economic Sciences, Professor at the Department of Business Project Management of the National Research Nuclear University MEPhI, Moscow, Russia
e-mail: viabramov@mephi.ru
ORCID: 0000-0002-9471-9408

A. V. Gavrilyuk

Postgraduate Student of the Faculty for Business Informatics and Complex Systems Management of the National Research Nuclear University MEPhI, Moscow, Russia
e-mail: xessov@yandex.ru
ORCID: 0009-0007-3194-4126

A.V. Putilov

Doctor of Engineering Sciences, Professor, Dean of the Faculty for Business Informatics and Integrated Systems Management of the National Research Nuclear University MEPhI, Moscow, Russia
e-mail: avputilov@mephi.ru
ORCID: 0000-0002-5379-7506

Abstract. Amid accelerated digital transformation and mounting geo-economic turbulence, the challenges of safeguarding digital security in the real economy and achieving technological sovereignty have become critically important for international business. This article provides a comprehensive analysis of the key risks and strategic challenges faced by multinational corporations in the digitisation of global economic relations. The authors examine a broad spectrum of threats – from the rising frequency of large-scale cyberattacks targeting critical information infrastructure to the progressive fragmentation of digital space driven by protectionist barriers, technological sanctions, and policies of digital isolation. Particular attention is devoted to the methodological foundations of information security and conceptual approaches to establishing technological sovereignty, which serve as interconnected factors in ensuring long-term competitiveness and sustainable business development in an era of global instability. Drawing on an in-depth study of leading Russian companies successfully adapting to these new realities, the paper formulates concrete recommendations for building effective cyber defence systems, localising digital assets, and developing strategies for technological independence. The findings hold significant value both for academia – particularly researchers examining the evolution of international business models – and for corporate practitioners, including senior executives, cybersecurity specialists, and digital policy developers, who face the pressing need to rethink conventional approaches in light of profound shifts within the global digital ecosystem.

Keywords: digital security, technological sovereignty, international business, cybersecurity, data regulation, digital economy, sanctions risks, sanctions pressure.

Submitted: May 06, 2025
Accepted: May 29, 2025

UDC 339.9
DOI: 10.24833/2949-639X-2025-2-12-28-42

REFERENCES:

1. Abdulov R.E., Resnov D.G. Perspektivy dostizheniya tekhnologicheskogo suvereniteta i tsifrovizatsii v Rossii na fone bespretsedentnogo sanktsionnogo davleniya [Prospects for Achieving Technological Sovereignty and Digitalization in Russia Under Unprecedented Sanctions Pressure]. *Kreativnaja jekonomika [Creative Economy],* 2022, no. 16 (12), pp. 4591–4604. (In Russ.).
2. Abramov V.I., Abramov A.V., Stolyarov A.D. Innovatsionnye trendy i vyzovy ispolzovaniya generativnogo iskusstvennogo intellekta v upravlenii [Innovative Trends and Challenges of Using Generative AI in Management]. *Municipal'naja akademija [Municipal Academy],* 2024, no. 4, pp. 200–210. (In Russ.).
3. Abramov V.I., Andreev V.D. Pervyy god realizatsii programm tsifrovoy transformatsii v regionakh Rossii: problemy i rezultaty [The First Year of Digital Transformation Programs in Russian Regions: Problems and Results]. *Voprosy gosudarstvennogo i municipal'nogo upravlenija [Public Administration Issues],* 2024, no. 2, pp. 110–128. (In Russ.).
4. Abramov V.I., Andreev V.D. Perspektivy ispolzovaniya interneta veshchey pri tsifrovoy transformatsii gosudarstvennogo i munitsipalnogo upravleniya (na primere Finlyandii) [Prospects of IoT in Digital Transformation of Public Administration (Case of Finland)]. *Municipal'naja akademija [Municipal Academy],* 2022, no. 2, pp. 34–42. (In Russ.).
5. Abramov V.I., Andreev V.D. Sravnitelnyy analiz tsifrovykh dvoynikov regionov [Comparative Analysis of Regional Digital Twins]. *Informacionnoe obshhestvo [Information Society],* 2023, no. 4, pp. 106–117. (In Russ.).
6. Abramov V.I., Gavrilyuk A.V., Putilov A.V. Sravnenie podkhodov k obespecheniyu tekhnologicheskogo suvereniteta v raznykh stranakh [Comparison of Approaches to Ensuring Technological Sovereignty in Different Countries]. *Trendy razvitija sovremennogo obshhestva: upravlencheskie, pravovye, jekonomicheskie i social'nye aspekty: Sbornik nauchnyh statej 14-j Vserossijskoj nauchno-prakticheskoj konferencii (05–06 ijunja 2024 g., g. Kursk) [Trends in the Development of Modern Society: Managerial, Legal, Economic and Social Aspects: Collection of Scientific Articles of the 14th Russian Scientific and Practical Conference (05–06 June 2024, Kursk)],* 2024, pp. 15–21. (In Russ.).
7. Abramov V. I., Gavrilyuk A. V., Putilov A. V. Tekhnologicheskiy suverenitet: bazovye printsipy i strategicheskie tseli [Technological Sovereignty: Core Principles and Strategic Goals]. *Upravlenie ekonomikoj, sistemami, processami: sbornik statej VIII Mezhdunarodnoj nauchno-prakticheskoj. konferencii «Mezhdunarodnyj institut rynka» (28 noyabrya 2024 g., g. Penza) [Management of Economics, Systems, Processes: Collection of Articles of the VIII International Scientific and Practical Conference "International Internet Market" (November 28, 2024, Penza)],* 2024, pp. 11–18. (In Russ.).
8. Abramov V.I., Gavrilyuk A.V., Putilov A.V. Tekhnologicheskiy suverenitet – instrumentariy obespecheniya ustoychivogo razvitiya strany [Technological Sovereignty as a Tool for Sustainable Development]. *Jekonomicheskie strategii [Economic Strategies],* 2025, no. 3, pp. 27–39. (In Russ.).

9. Abramov V.I., Gordeev V.V., Stolyarov A.D. Tsifrovye dvoyniki: kharakteristiki, tipologiya, praktiki razvitiya [Digital Twins: Characteristics, Typology, and Development Practices]. *Voprosy innovacionnoj jekonomiki [Innovation Economy],* 2024, no. 14 (3), pp. 691–716. (In Russ.).
10. Abramov V.I., Lomakin V.A., Stolyarov A.D. Tsifrovaya ekosistema regiona kak perspektivnaya model territorialnogo razvitiya ekonomiki [Regional Digital Ecosystem as a Promising Model of Territorial Economic Development]. *Informacionnoe obshhestvo [Information Society],* 2024, no. 6, pp. 16–27. (In Russ.).
11. Belousov F.A., Ivanova A.K., Nevolin I.V. Tekhnologicheskiy suverenitet i globalnaya konkurentsiya [Technological Sovereignty and Global Competition]. *Cifrovaja jekonomika [Digital Economy],* 2024, no. (30), pp. 24–33. (In Russ.).
12. Toloraya G.D *BRIKS v mirovykh finansakh i ekonomike [BRICS in Global Finance and Economy].* Moscow, MGIMO, 2024, 541 p. (In Russ.).
13. Gareev T.R. Tekhnologicheskiy suverenitet: ot kontseptualnykh protivorechiy k prakticheskoy realizatsii [Technological Sovereignty: From Conceptual Contradictions to Practical Implementation]. *Terra Economicus [Terra Economicus],* 2023, no. 21 (4), pp. 38–54. (In Russ.).
14. Gerasimov B.N. *Razvitie ekonomicheskikh sistem: teoriya, metodologiya, praktika [Development of Economic Systems: Theory, Methodology, Practice].* Penza, PGAU, 2024, 275 p. (In Russ.).
15. Geraskina E.I. Vyzovy i ugrozy informatsionnoy bezopasnosti v rossiyskom obshchestve v XXI veke [Challenges and Threats to Information Security in Russian Society in the 21st Century]. *Aktual'nye issledovanija [Current Research],* 2023, no. 21 (151), pp. 69–73. (In Russ.).
16. Golovkov S.S., Kalinina I.A. Klyuchevye riski tsifrovoy transformatsii biznesa [Key Risks of Business Digital Transformation]. *Innovacii i investicii [Innovations and Investments],* 2023, no. 3, pp. 139–143. (In Russ.).
17. Dudin M.N., Shkodinsky S.V., Prodchenko I.A. Ekonomicheskie i infrastrukturnye instrumenty obespecheniya gosudarstvennogo ekonomicheskogo suvereniteta v tsifrovoy ekonomike: opyt Rossiyskoy Federatsii i mira [Economic and Infrastructure Tools for Ensuring State Sovereignty in the Digital Economy: Experience of Russia and the World]. *Voprosy innovacionnoj jekonomiki [Innovation Economy],* 2022, no. 12 (1), pp. 57–80. (In Russ.).
18. Ivanov V.V. Osnovnye napravleniya gosudarstvennoy politiki obespecheniya tekhnologicheskogo suvereniteta [Key Directions of State Policy for Ensuring Technological Sovereignty]. *Jekonomika nauki [Economics of Science],* 2024, no. 10 (1), pp. 10–20. (In Russ.).
19. Zuboff S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* N. Y., Public Affairs, 2018, 717 p.
20. Saltzer J.H., Schroeder M.D. The Protection of Information in Computer Systems. *Proceedings of the IEEE,* 1975, no. 63 (9), pp. 1278–1308.