УДК 004.056:33

А. С. Чередниченко

Донской государственный технический университет, г. Ростов-на-Дону

ЦИФРОВОЙ СУВЕРЕНИТЕТ КАК ФАКТОР ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИИ

Рассматриваются актуальные угрозы цифровому суверенитету Российской Федерации в условиях глобального технологического противостояния. Анализируются задачи, определенные в Доктрине информационной безопасности Российской Федерации, и предлагаются подходы к обеспечению устойчивости и независимости отечественной информационной инфраструктуры. Акцентируется внимание на экономических аспектах укрепления информационной безопасности государства.

***Ключевые слова**: цифровой суверенитет, информационная безопасность, государство, технологическое противостояние, защита информации, цифровая независимость, экономическая безопасность*

Постановка проблемы

В условиях глобального технологического противостояния цифровая инфраструктура Российской Федерации подвергается значительным рискам, связанным с зависимостью от зарубежных технологий, санкционным давлением и ограничением доступа к ключевым ИТ-ресурсам. Данные вызовы подрывают устойчивость национальной экономики и создают угрозы ее цифровому суверенитету. В связи с этим возникает необходимость комплексного анализа угроз и выработки управленческих решений, направленных на укрепление технологической независимости страны.

Анализ последних исследований и публикаций

В настоящее время актуальны вопросы обеспечения информационной безопасности и цифрового суверенитета России. В стране значительное внимание уделяется вопросам импортозамещения (Astra Linux, Байкал, Эльбрус), формированию независимой ИТ-инфраструктуры и обеспечению устойчивости национальной экономики в условиях санкционного давления.

Тему цифровой экономики, обеспечения цифрового суверенитета и его влияния на экономический рост исследовали различные ученые. Так, Т. К. Горемыкина, Н. А. Тришкина и Г. А. Лукошевичус рассматривали взаимосвязь новейших технологий с цифровым и экономическим суверенитетом, а также их роль в стимуляции экономического роста в России. Ученые М. Н. Дудин, В. С. Шкодинский и Д. И. Усманов проанализировали понятие цифрового суверенитета, выделили барьеры его достижения и предложили сценарии развития цифровой инфраструктуры РФ в условиях индустрии 4.0.

Цель статьи – провести анализ ключевых угроз цифровому суверенитету Российской Федерации в условиях глобального технологического противостояния, а также предложить управленческие и экономические подходы к обеспечению устойчивости и независимости отечественной цифровой инфраструктуры.

Основная часть

Цифровая трансформация современного общества делает информационные технологии ключевым фактором национальной безопасности. В условиях усиливающегося глобального технологического противостояния, вызванного геополитическими конфликтами и санкционной политикой, особенно актуальным становится вопрос обеспечения цифрового суверенитета Российской Федерации и ее информационной безопасности.

Одним из ключевых нормативных документов, определяющих политику государства в данной сфере, является Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ от 5 декабря 2016 года № 646). Целями государственной политики Российской Федерации в области информационной безопасности, согласно этого документа, являются:

- защита прав граждан в информационной сфере;
- устойчивое функционирование критической информационной инфраструктуры (КИИ);
- достижение технологической независимости;
- развитие отечественных научных и производственных компетенций;
- контроль информации от пропаганды и подрыва суверенитета;
- защита государственной тайны [1].

В настоящее время технологии становятся не только экономическим, но и политическим оружием, страны выстраивают свою внешнюю политику, апеллируя к двум факторам. Первым из них является цифровая зависимость – когда государство зависит от иностранных платформ, программного обеспечения, облаков, микропроцессоров, сетевого оборудования. Второй фактор – это технологический протекционизм – политика ограничения доступа к передовым технологиям другим странам с целью сохранения лидерства или нанесения ущерба. Такие крупные компании, как «Microsoft», «Google», «Amazon», «Intel», «Cisco», «Nvidia» стали опосредованными участниками геополитических конфликтов, выполняя решения своих правительств, либо добровольно ограничивая доступ к своим ресурсам пользователей из недружественных стран.

После 2014 года, особенно с 2022 года, на Российскую Федерацию были наложены беспрецедентные технологические санкции. Их цель – затормозить цифровое развитие, лишить доступа к инновационным ресурсам, ослабить оборонную и экономическую мощь страны. Основные меры давления были направленны на ограничения доступа к программному обеспечению (ПО) и запрет ввоза отдельных категорий товаров (таблица 1).

Таблица 1 – Направления технологического давления на Российскую Федерацию

Сфера	Направление технологического давления	Результат
Микроэлектроника	Прекращение поставок чипов от Intel, AMD, TSMC	Срыв контрактов, рост спроса на отечественные аналоги, зависимость от Китая
ПО	Блокировка Windows, AutoCAD, SAP, Oracle	Форсированное внедрение Astra Linux, Р7-Офис
Облачные сервисы	Удаление аккаунтов, блокировка доступа к GitHub, AWS	Потеря данных, утрата цифровых активов, миграция на российские облачные сервисы
Киберпространство	Блокировки сайтов, сервисов, отключение от API	Рост цифровой изоляции, развитие Рунета, национальных DNS и VPN

Цифровой суверенитет – это способность государства самостоятельно формировать и реализовывать политику в цифровой среде, обеспечивая контроль над критической информационной инфраструктурой, данными, технологиями и средствами коммуникации. Цифровой суверенитет обеспечивает не только информационную безопасность, но и устойчивость всей государственной системы в условиях кибервойн, санкционного давления и технологических блокад.

Основными показателями цифрового суверенитета Российской Федерации являются: технологическая независимость, устойчивость критической информационной инфраструктуры, уровень импортозамещения, защита данных и информационных ресурсов, суверенный интернет и нормативно-правовая защищенность.

С новой вехой – четвертой промышленной революцией, происходит направленность на внедрение в производственные процессы новых технологий, которыми являются цифровые технологии [2]. В настоящее время для предприятий стали развиваться возможности применения интеллектуальных систем, интернета вещей, сенсоров и т. д. К 2025 году уже практически повсеместно используется искусственный интеллект, который подходит под задачи контроля качества, автоматизации однотипных процессов. В таких компаниях, как, например, «АвтоВАЗ», применяется искусственный интеллект для обнаружения дефектов, в «Газпром» он используется для отслеживания изношенности деталей, что помогает заблаговременно получить информацию о выходе их из строя. Даже на атомных станциях применяются подобные технологии. Так, «Росатом» создал целую автоматизированную систему, которая управляет процессами на производстве. Эта концепция ведет к тому, что роль информационного сектора развивается и увеличиваются сферы применения интеллектуальных технологий, поэтому важность независимой цифровой среды приобретает все большую актуальность.

С развитием информационных технологий цифровой суверенитет все теснее становится связан с экономической политикой страны, поскольку процессы цифровизации оказывают на нее прямое влияние. Внедрение современных цифровых решений повышает эффективность работы предприятий и государственных структур, что способствует росту ВВП. В то же время, ущерб или невозможность использования новых технологий приводит к замедлению экономического развития, негативно сказывается на уровне жизни граждан и ценовой стабильности, требуя принятия мер для восстановления и стабилизации экономики [3].

Цифровой суверенитет непосредственно влияет на экономическую безопасность России, обеспечивая независимость от иностранных технологий и платформ. Развитие отечественного программного обеспечения, процессоров, облачных сервисов и критической инфраструктуры повышает эффективность промышленного и государственного сектора, снижает уязвимость к санкциям и международным технологическим ограничениям. Одновременно формируется национальная инновационная экосистема, стимулирующая создание собственных продуктов и сервисов, что укрепляет экономическую устойчивость и снижает финансовые и технологические риски.

В наше время существует целое направление, которое появилось из-за слияния экономики и информационно-коммуникационных технологий – ИКТ-сектор. Данная отрасль занимается производством изделий для создания информационной инфраструктуры, обеспечивающих возможность увеличения общего объема ВВП [4]. Так, реализация товаров, работ и услуг за первую половину 2025 года уже превысила их количество за тот же период 2024 года на 13,4 % – это около 1,9 трлн рублей. Самая большая часть – программное обеспечение – возросла на 36,1 %, а самый незначительный рост у телекоммуникаций – всего 5,2 %. Самыми крупными российскими компаниями в ИКТ-сфере являются: «Т1»; «Инфосистемы Джет»; «IBS Group»; «Ventra»; «Лаборатория Касперского»; «ИКС Холдинг»; «Ростелеком»; «МТС».

Современное государство невозможно представить без цифровых технологий, поскольку они пронизывают все сферы – от экономики до обороны. Таким образом, цифровой суверенитет становится неотъемлемой частью общегосударственной автономии, обеспечивая:

– политическую сферу – контроль над информационным пространством предотвращает вмешательство извне;

– социально-гуманитарную сферу – защита цифровых прав граждан, персональных данных, ограничение иностранного влияния на культуру и образование;

– экономическую сферу – независимое проведение экономических операций.

К числу наиболее значимых угроз цифровому суверенитету Российской Федерации относятся:

– зависимость от зарубежных программных и аппаратных решений;

– ограничение доступа к международным ИТ-платформам и сервисам;

– атаки на критическую информационную инфраструктуру;

– информационно-психологическое воздействие с использованием сетевых технологий.

В России имеются экономические проблемы, связанные с зависимостью от западных технологий. До санкций со стороны США и большинства стран, поддерживающих их, поставки требуемого оборудования шли непрерывно. А в настоящее время приходится искать ему замену. Из-за слабо развитого уровня развития его производства в нашей стране сделать это бывает достаточно сложно, а порой и невозможно. Из-за действия санкций появляется риск снижения экономической безопасности в стране, ведь требуются ресурсы, которые ранее применялись в интеграции с собственными разработками. Это приводит к замедлению разработки новых технологий на базе современного оборудования, так как его производство приходится начинать практически с нуля, создавая собственные аналоги, заменяющие иностранные разработки применявшегося длительное время оборудования [5].

В России уже развиваются технологии, которые могут стать полноценной заменой зарубежных аналогов. Так, например, отечественный вариант реализации спутникового интернета с течением времени может прийти на замену Starlink. Его разработкой занимается АО «Газпром космические системы» (ГКС) – компания, которая реализует телекоммуникационные услуги через спутниковые системы, а также применяет геоинформационные системы. Главная ее деятельность – это продажа услуг спутникового интернета. Так как в настоящий момент на территории России не работает Starlink, система спутниковой связи и вещания «Ямал» от ГКС может рассматриваться как альтернатива технологии компании «SpaceX» [6]. Основные отличия «Ямал» от Starlink приведены в таблице 2.

Таблица 2 – Основные различия систем спутниковой связи «Ямал» и Starlink

Критерий сравнения	Система спутниковой связи и вещания «Ямал»	Глобальная система спутниковой связи Starlink
Компания-разработчик	АО «Газпром космические системы» (Россия)	«SpaceX» (США)
Орбита	Спутники «Ямал» находятся на геостационарной орбите (GEO, ~36 000 км)	Starlink работает на низкой околоземной орбите (LEO, ~550 км)
Количество спутников	5 («Ямал-202», Ямал-300К», «Ямал-401», «Ямал-402», «Ямал-601»)	7 264
Подключение	VSAT-терминал, установка требует специальных знаний, оборудование массивнее	Компактная автоматическая антенна («тарелка») + сразу Wi-Fi
Скорость	до ~100 Мбит/с	Достигает почти 200 Мбит/с
Масштаб	Несколько геостационарных аппаратов, покрывающих Россию, Европу, часть Азии и Африки	Глобальная сеть из тысяч спутников
Цена оборудования	90 000 руб.	40 000 руб.
Доступность	Доступна по всей территории России, а также дает возможность бесшовного прохождения на 100 % Северного морского пути от Роттердама до Пусана	Доступна в 123 странах и регионах мира (по состоянию на 2025 год). Недоступна в России
Особенности и надежность работы	Система демонстрирует высокую устойчивость к неблагоприятным погодным условиям и космическим воздействиям за счет современных технологий, систем навигации и управления. Это обеспечивает бесперебойную связь даже во время сильных дождей и снегопадов	Динамическая маршрутизация: система постоянно анализирует загруженность каналов, погодные условия и другие факторы, выбирая оптимальный путь для передачи данных

Итоги сравнения показывают, что «Ямал» опирается на ограниченное число геостационарных аппаратов, что приводит к высокой задержке сигнала, необходимости установки дорогостоящего и громоздкого оборудования. Starlink же, напротив, использует низкоорбитальную группировку из тысяч спутников, что обеспечивает низкие задержки, более высокие скорости передачи данных. Таким образом, Starlink технологически более продвинут и массово ориентирован, тогда как «Ямал» выступает одним из локальных решений, ориентированным на нужды России.

Выполнение задачи по доступу к широкополосному интернету для всей территории России возможно благодаря технологическому прогрессу. Так, к 2026 году планируется запустить в космос на высокоэллиптическую орбиту спутник «Экспресс-РВ», целью которого будет наладить связь в зоне Северного морского пути. Как рассказывают производители данной системы, ее функционал ожидается большим, чем у Starlink. Эта разработка является ярким примером того, как из-за санкций происходит создание собственных технологий.

На основании вышеизложенного определим основные направления (пути) достижения цифрового суверенитета Российской Федерации. В обобщенном виде они представлены в таблице 3.

Таблица 3 – Пути достижения цифрового суверенитета Российской Федерации

Направления	Характеристика
Импортозамещение ПО и оборудования	Развитие отечественных операционных систем – Red OS, Astra Linux, Альт, процессоров – Байкал, Эльбрус, а также систем управления базами данных – Tantor, Proxims DB
Защита КИИ	Внедрение национальных стандартов безопасности, аудит инфомационной безопасности
Суверенный интернет	Развитие собственного DNS, магистральных сетей, центров обработки данных
Использование институциональных мер	Правовое регулирование (ФЗ-187), развитие системы «ГосСопка», контроль информации со стороны федеральных служб (ФСБ, ФСТЭК)
Научно-исследовательские и опытно-конструкторские работы	Поддержание научно-исследовательских институтов и вузов в части разработки отечественных продуктов в области информационной безопасности

Самая важная сфера развития отечественных информационно-коммуникационных технологий – разработка и продажа программного обеспечения, поэтому данная область нуждается в защите в первую очередь. К проблемам в данной среде можно отнести два типа нарушений – атаки злоумышленников, приводящие к несанкционированному воздействию, нарушение конфиденциальности, доступности, целостности информации. Второй тип – это нарушение авторских прав.

Защита программного обеспечения предполагает реализацию функций резервирования и возврата к состоянию, когда система была не подвергнута атаке или изменению, такой способ восстановления называют backup. Каждый раз, когда выходят обновления или новые версии приложения, а также дополнений к нему, нужно проверять их подпись и целостность. Например, такая проверка происходит при скачивании макросов – VBA-кода, который используется в Microsoft Office. Приложение может отказать в правах доступа, если обнаружит подозрительный документ, который пытается запуститься вместе с программой. Программное обеспечение должно иметь периодическое обновление с новыми методами защиты от уже выявленных ошибок и уязвимостей [7].

Для противодействия цифровому пиратству и незаконному распространению контента следует применять как технические, так и организационно-правовые меры. К основным мерам относятся: использование систем Digital Rights Management (DRM) для ограничения

несанкционированного копирования и распространения цифровой продукции, внедрение лицензионных ключей и онлайн-активации программного обеспечения, а также применение водяных знаков и других технологий отслеживания источников утечки данных. Важную роль играют и правовые механизмы защиты авторских прав, включая мониторинг торрент-сетей, блокировку пиратских ресурсов и судебное преследование нарушителей. Эффективная стратегия должна сочетать технологические средства защиты с развитием легальных цифровых платформ, обеспечивающих пользователям доступный и удобный способ получения контента.

В условиях текущего технологического давления со стороны зарубежных государств и компаний укрепление цифрового суверенитета становится стратегической необходимостью для России. Реализация положений Доктрины информационной безопасности Российской Федерации, развитие отечественных технологий и формирование безопасной цифровой среды – современная основа национальной экономической устойчивости. Дальнейших исследований требуют пути совершенствования правового и институционального регулирования в сфере информационной безопасности.

Выводы

Проанализированы основные угрозы цифровому суверенитету Российской Федерации, связанные с зависимостью от зарубежных технологий, ограничением доступа к международным ИТ-ресурсам, атаками на критическую информационную инфраструктуру, нехваткой высококвалифицированных специалистов по защите информации. Установлено, что важнейшим направлением обеспечения цифрового суверенитета выступает импортозамещение программного обеспечения и оборудования.

Предложены управленческие и экономические подходы к обеспечению устойчивой цифровой экономической безопасности России.

Государственная политика в области информационной безопасности должна быть направлена на технологическую независимость, поддержку отечественных разработчиков и формирование устойчивой цифровой национальной экономики.

Список литературы

1. Доктрина информационной безопасности Российской Федерации : утверждена Указом Президента Рос. Федерации от 5 декабря 2016 г. № 646. – Текст : электронный // Собрание законодательства Российской Федерации. – 2016. – № 50. – С. 17035–17043. – URL: https://clck.ru/3MqTST (дата обращения: 18.08.2025).

2. Дудин, М. Н. Цифровой суверенитет России: барьеры и новые траектории развития / М. Н. Дудин, В. С. Шкодинский, Д. И. Усманов. – Текст : электронный // Проблемы рыночной экономики. – 2021. – № 2. – С. 30–49. – URL: https://goo.su/GKOUdjY (дата обращения: 18.08.2025).

3. Горемыкина, Т. К. Цифровизация экономики России, цифровой суверенитет, их взаимосвязь и влияние на экономический рост / Т. К. Горемыкина, Н. А. Тришкина, Г. А. Лукошевичус. – Текст : электронный // Экономика. – 2023. – № 6. – С. 13–16. – URL: https://goo.su/0gN6H0J (дата обращения: 19.08.2025).

4. Логинов, В. Г. Доля продукции и услуг сферы информационных и коммуникационных технологий в ВВП / В. Г. Логинов. – Текст : электронный // Информационная среда сферы науки и инноваций. – С. 362–376. – URL: https://goo.su/b8Qo3 (дата обращения: 19.08.2025).

5. Водомеров, Н. К. Преодоление технологического отставания России и цифровая экономика / Н. К. Водомеров. – Текст : электронный // Теоретическая экономика. – 2019. – № 3. – С. 70–73. – URL: https://goo.su/MgPrK (дата обращения: 19.08.2025).

6. Вселенная возможностей ТЭК. Проект о космических технологиях на службе у отрасли. – Текст : электронный // Газпром космические системы : сайт. – URL: https://www.gazprom-spacesystems.ru/ru/ (дата обращения: 19.08.2025).

7. Чередниченко, А. С. Кибербезопасность информационно-управляющих систем в автотранспорте / А. С. Чередниченко. – Текст : электронный // Научно-технические аспекты развития автотранспортного комплекса: в рамках 11-го Международного научного форума Донецкой Народной Республики, Горловка, 28 мая 2025 г. : материалы XI Международной научно-практической конференции / редкол. : Д. Н. Самисько [и др.]. – Горловка : АДИ ДонНТУ, 2025. – С. 436–438. – URL: https://адидоннту.рф/news/p6dztr8a/ (дата обращения: 19.08.2025).

А. С. Чередниченко
Донской государственный технический университет, г. Ростов-на-Дону

Цифровой суверенитет как фактор экономической безопасности России

Высокий уровень цифрового суверенитета способствует технологической независимости государства, экономической устойчивости и национальной безопасности. Рассмотрены и исследованы основные угрозы и вызовы цифровой инфраструктуре Российской Федерации в условиях глобального технологического противостояния. Изучены ключевые направления обеспечения цифрового суверенитета, включая импортозамещение программного обеспечения и оборудования, развитие отечественных процессоров и операционных систем, а также создание суверенной информационно-технологической инфраструктуры. Разработаны системные подходы к укреплению устойчивости национальной экономики, обеспечивающие цифровую независимость и защиту критической информационной инфраструктуры, в том числе посредством совершенствования правового и институционального регулирования в сфере информационной безопасности.

Цифровой суверенитет государства отражает уровень технологической независимости и устойчивости к внешним воздействиям, что, в свою очередь, связано с возможностью обеспечения развития экономических и социальных процессов государства и его институтов. Его укреплению способствует научно-технический прогресс и эффективное управление информационной инфраструктурой.

Таким образом, цифровой суверенитет рассматривается не только как инструмент информационной безопасности, но и как фактор устойчивого экономического развития, политической автономии и социальной стабильности. Укрепление цифровой независимости государства становится ключевым элементом национальной стратегии в условиях глобального технологического противостояния.

ЦИФРОВОЙ СУВЕРЕНИТЕТ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ГОСУДАРСТВО, ТЕХНОЛОГИЧЕСКОЕ ПРОТИВОСТОЯНИЕ, ЗАЩИТА ИНФОРМАЦИИ, ЦИФРОВАЯ НЕЗАВИСИМОСТЬ, ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

A. S. Cherednichenko
Don State Technical University, Rostov-on-Don

Digital Sovereignty as a Factor of Russia's Economic Security

A high level of digital sovereignty contributes to the technological independence of the state, its economic sustainability and national security. The main threats and challenges to the digital infrastructure of the Russian Federation in the context of global technological confrontation are considered and investigated. The key areas of ensuring digital sovereignty including software and equipment import substitution, the development of domestic processors and operating systems, as well as the creation of the sovereign information technology infrastructure are studied. Systematic approaches are developed to strengthen the sustainability of the national economy, ensuring digital independence and protection of critical information infrastructure through improving legal and institutional regulation in the field of the information security.

The digital sovereignty of the state shows the level of technological independence and resilience to external impacts, which, in turn, are associated with the possibility of developing economic and social factors in the structure of the state and its institutions. The importance of the digital sovereignty increases the efficiency of information infrastructure management and contributes to the scientific and technological progress of the country.

Thus, digital sovereignty is considered not only as an instrument of information security, but also as a factor of sustainable economic development, political autonomy and social stability. Strengthening the digital independence of the state is becoming a key element of the national strategy in the context of global technological competition.

DIGITAL SOVEREIGNTY, INFORMATION SECURITY, STATE, TECHNOLOGICAL CONFRONTATION, INFORMATION PROTECTION, DIGITAL INDEPENDENCE, ECONOMIC SECURITY

Сведение об авторе:
А. С. Чередниченко
Телефон: +7 905 476-66-79
Эл. почта: lore7979@mail.ru

Статья поступила 27.08.2025

Рецензент: М. М. Гуменюк, канд. экон. наук, доц.,
Автомобильно-дорожный институт
(филиал) ДонНТУ в г. Горловка