Дата поступления рукописи в редакцию: 01.02.2026 г.
Дата принятия рукописи в печать: 16.02.2026 г.
DOI: 10.24412/2782-3830-2026-1-22-29

ГОЛУБЦОВА Оксана Анатольевна,
кандидат экономических наук,
доцент кафедры прокурорско-следственной деятельности
Луганского государственного университета им. В. Даля
(Луганск, Российская Федерация) ORCID 0000-0003-2428-3642,
e-mail: gragov777@mail.ru

ПАМПУРА Александра Валериевна,
судья Ленинского районного суда города Луганска,
e-mail: seskenderova@mail.ru

БРОСЕВА Екатерина Сергеевна,
студентка 3 курса направления
подготовки «Юриспруденция»,
e-mail: mail@law-books.ru

ЦИФРОВОЙ СУВЕРЕНИТЕТ И ЗАЩИТА ДАННЫХ В РОССИЙСКОЙ ФЕДЕРАЦИИ: ЭКОНОМИКО-ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ТЕХНОЛОГИЧЕСКОЙ НЕЗАВИСИМОСТИ

Аннотация*. В статье рассматриваются актуальные экономико-правовые аспекты обеспечения цифрового суверенитета и защиты данных в Российской Федерации на фоне нарастающей геополитической напряженности и беспрецедентного санкционного давления. Авторы анализируют, как трансформация цифровой экономики и эскалация киберугроз (подтвержденные многочисленными инцидентами и крупными утечками данных в 2024 году) сделали технологическую независимость вопросом национальной безопасности.*

Исследование фокусируется на выявлении ключевых проблем в существующей нормативно-правовой базе, регулирующей импортозамещение ПО, защиту критической информационной инфраструктуры (КИИ) и обработку персональных данных. Отмечается, что действующие меры, такие как запреты на закупку иностранного ПО и требование локализации данных, недостаточны для формирования полного технологического суверенитета, поскольку не гарантируют доверенность и безопасность самого российского программного обеспечения. Отсутствие законодательно закрепленной методологии аудита исходного кода и обязательных программ поиска уязвимостей (Bug Bounty) создает внутренние риски.

В качестве направлений совершенствования предлагается комплекс мер: правовые — дифференциация требований к КИИ, гармонизация законодательства в рамках ЕАЭС, внедрение принципа «Security by Design» и создание независимых центров сертификации кода. Экономические инструменты должны сместиться от прямого субсидирования к стимулированию спроса через долгосрочные госзаказы с KPI, а также фокусироваться на поддержке прорывных технологий (RISC-V, ИИ) и развитии сервисной поддержки отечественных решений.

Цель статьи – выявить и систематизировать основные экономические и правовые проблемы, препятствующие сохранению и поддержанию цифрового суверенитета и защиты данных (в том числе персональных) в Российской Федерации на современном этапе, а также предложить сбалансированный комплекс рекомендаций для органов государственной власти и бизнеса, направленных на укрепление технологической независимости, повышение надежности защиты данных и обеспечение устойчивого развития российского цифрового пространства.

Ключевые слова*: цифровой суверенитет, защита данных, кибератака, технологическая независимость, безопасность, геополитическая нестабильность.*

GOLUBTSOVA Oksana Anatolyevna,
PhD in Economics, Associate Professor,
Department of Prosecutor's and Investigative Activities,
V. Dahl Luhansk State University (Luhansk, Russian Federation)

PAMPURA Alexandra Valerievna,
Judge of the Leninsky District Court of Luhansk

BROSEVA Ekaterina Sergeevna,
third-year student, Jurisprudence

DIGITAL SOVEREIGNTY AND DATA PROTECTION IN THE RUSSIAN FEDERATION: ECONOMIC AND LEGAL ASPECTS OF ENSURING TECHNOLOGICAL INDEPENDENCE

Annotation. *This article examines the current economic and legal aspects of ensuring digital sovereignty and data protection in the Russian Federation under conditions of growing geopolitical tensions and unprecedented sanctions pressure. The authors analyze how the transformation of the digital economy and the escalation of cyber threats (confirmed by numerous incidents and major data breaches in 2024) have made technological independence as a matter of national security.*

The study focuses on identifying key issues in the existing regulatory framework which regulate import substitution, the protection of critical information infrastructure (CII), and personal data processing. It is noted that current measures, such as bans on the purchase of foreign software and data localization requirements are insufficient to establish full technological sovereignty, as they do not guarantee the trustworthiness and safety of Russian software itself. The lack of a legislatively enshrined source code audit methodology and mandatory vulnerability detection programs (bug bounty) creates internal risks.

A range of measures is proposed for improvement: legal measures such as differentiating critical information infrastructure requirements, harmonizing legislation within the EAEU, implementing the "Security by Design" principle, and establishing independent code certification centers. Economic instruments have to be shifted from direct subsidies to stimulating demand through long-term government procurement with KPIs, and also focus on supporting breakthrough technologies (RISC-V, AI) and developing service support for domestic solutions. The purpose of this article is to identify and systematize the main economic and legal challenges that hinder the preservation and maintenance of digital sovereignty and data protection (including personal data) in the Russian Federation today, and to propose possible solutions.

Key words: *digital sovereignty, data protection, cyberattack, technological independence, security, geopolitical instability.*

Введение

Актуальность темы обусловлена нарастающей геополитической напряженностью и беспрецедентным давлением, оказываемым на Российскую Федерацию в цифровой сфере. В условиях беспрецедентных санкций и кибератак, обеспечение цифрового суверенитета и защиты данных приобретает характер не только экономической, но и национальной безопасности. Во-первых, глобальная цифровая экономика, характеризующаяся трансграничным потоком данных, создает как возможности для экономического развития, так и риски утраты контроля над критически важной информацией. Зависимость от иностранных технологий и платформ ставит под угрозу конкурентоспособность российских предприятий, уязвимость критической инфраструктуры и возможность эффективного осуществления государственного управления. Необходимость защиты данных российских граждан и организаций от несанкционированного доступа, использования и трансграничной передачи, особенно в условиях активной цифровой экспансии транснациональных корпораций и недружественных государств, требует разработки эффективных экономических и правовых механизмов. Во-вторых, обеспечение технологической независимости является ключевым фактором укрепления цифрового суверенитета. Разработка и внедрение отечественных цифровых технологий, включая программное обеспечение, оборудование и инфраструктуру, позволит снизить зависимость от иностранных поставщиков, стимулировать развитие инноваций и создать новые рабочие места в высокотехнологичных отраслях. Экономическое стимулирование отечественных разработчиков и создание благоприятной регуляторной среды для развития цифровой экономики требует детального анализа существующих экономических и правовых инструментов и разработки новых подходов. В-третьих, существующие правовые механизмы защиты данных в РФ, сформированные под влиянием международных стандартов и европейского опыта, требуют адаптации к новым реалиям и национальным интересам. Необходимо исследовать эффективность действующего

законодательства в сфере защиты персональных данных, кибербезопасности и регулирования цифровых технологий, а также разработать предложения по его совершенствованию с учетом экономических и технологических особенностей страны. При этом важно найти баланс между обеспечением защиты данных и свободы информации, стимулированием инноваций и сохранением конкурентоспособности российского бизнеса. В-четвертых, отсутствует комплексный экономико-правовой анализ взаимосвязи между цифровым суверенитетом, защитой данных и технологической независимостью в условиях геополитической нестабильности. Недостаточно изучены вопросы формирования эффективных моделей государственно-частного партнерства в сфере развития цифровых технологий, стимулирования инвестиций в отечественную цифровую инфраструктуру, а также защиты интеллектуальной собственности на российские разработки.

Таким образом, исследование экономико-правовых аспектов обеспечения технологической независимости в контексте цифрового суверенитета и защиты данных в РФ является своевременным, практически значимым и теоретически обоснованным. Результаты исследования позволят выработать эффективные рекомендации для органов государственной власти, бизнеса и научного сообщества по укреплению национальной безопасности, обеспечению устойчивого экономического развития и защите прав граждан в цифровом пространстве.

Материалы и методы

В эпоху, когда цифровые данные стали новой нефтью, а алгоритмы диктуют правила игры в геополитической шахматной доске, концепция технологической независимости приобретает совершенно новое измерение – цифровой суверенитет. Это не просто владение инфраструктурой, но и способность нации контролировать свои данные, определять правила их обработки и защищать их от внешних угроз. Правовые аспекты этого контроля становятся ключевым элементом в достижении устойчивой технологической независимости, но этот путь усеян сложными вызовами и неоднозначными решениями.

Цифровой суверенитет, в своей идеальной форме, предполагает создание автономной цифровой экосистемы, где сбор, обработка и хранение данных граждан и организаций осуществляется в соответствии с национальным законодательством и под контролем национальных институтов [1, с.8]. Это подразумевает не только наличие собственной цифровой инфраструктуры, но и правовую базу, обеспечивающую защиту данных, стимулирование развития отечественных технологических решений и ограничение зависимости от иностранных провайдеров.

Указ Президента РФ № 309 от 7 мая 2024 года [2] установил стратегические ориентиры и приоритеты развития России на период до 2030 года, с долгосрочным планированием до 2036 года, определив ключевые направления деятельности органов государственной власти на ближайшее и перспективное будущее. Его роль заключается в создании правовой основы для дальнейшего развития в области информационной безопасности и технологического суверенитета, стимулировании инноваций и обеспечении защиты национальных интересов в цифровом пространстве.

Также нормативно-правовым документом, регламентирующим в определенной степени поддержание цифрового суверенитета и защиту данных является Постановление Правительства РФ от 16 ноября 2015 г. № 1236 [3], которое устанавливает запрет на закуп иностранного ПО для государственных и муниципальных нужд, если существуют российские аналогичные продукты, включенные в Единый реестр российского ПО.

Государство активно поддерживает и регулирует процесс перехода на российские программные продукты, устанавливая нормативные акты и предписания.

Российское законодательство, в частности Указы Президента РФ № 166 [4] и № 250 [5], обязывает субъектов критической информационной инфраструктуры (КИИ) к переходу на отечественное программное обеспечение (ПО) и средства защиты информации (СЗИ) на объектах КИИ. Данные меры направлены на повышение информационной безопасности (ИБ) критически важных национальных IT-систем, включая структуры госорганов, оборонной промышленности, транспорта и здравоохранения.

С 1 января 2025 года вводится запрет на использование иностранного ПО на объектах КИИ для органов государственной власти и иных заказчиков. С 31 марта текущего года для госкомпаний установлен запрет на закупку иностранного ПО (включая ПАК) для объектов КИИ без согласования с уполномоченным федеральным органом.

Согласно Постановлению № 1478, приобретение ПО для значимых объектов КИИ возможно только из реестров российского или евразийского ПО. ПО, фактически разработанное в РФ или ЕАЭС, но отсутствующее в данных реестрах, приравнивается к иностранному и требует специального согласования.

Среди разрешенных к применению отечественных операционных систем (ОС) выделяются:

Astra Linux (сертифицированная, с встроенной защитой), «РЕД ОС» (универсальная для серверов и рабочих станций), а также семейство ОС «Альт» компании «Базальт СПО» (включающее «Альт СП», «Альт Рабочая станция», «Альт Сервер», «Альт Сервер Виртуализации», «Альт Образование» и Simply Linux).

Продолжается формирование нормативной правовой базы, регламентирующей импортозамещение программного обеспечения (ПО) и оборудования, а также повышение безопасности критической информационной инфраструктуры (КИИ). Для стимулирования руководителей субъектов КИИ к исполнению внедряемых регуляторных требований, предлагается ввести административную ответственность за несоблюдение перехода на отечественное ПО.

Постановление № 1478 ограничивает закупки ПО для значимых объектов КИИ только реестровым (российским/евразийским) ПО. Использование нереестрового ПО, даже отечественного производства, требует согласования с уполномоченным органом. Статья 10 ФЗ № 149 запрещает распространение информации, содержащей призывы к противоправным действиям, включая пропаганду войны и вражды [6].

В первом квартале 2024 года зафиксирован пятикратный рост объёма утекших данных, достигнув 38 миллионов электронных адресов и 121 миллиона телефонных номеров. Это тревожный сигнал, предвещающий увеличение киберугроз в российском цифровом пространстве. 2024 год ознаменовался серией заметных кибератак и утечек, демонстрирующих растущую изощренность и дерзость киберпреступников. Вот некоторые из наиболее резонансных инцидентов [7]:

Атака на ВГТРК. Кибератака нарушила вещание, внутренние IT-сервисы и связь в ВГТРК, вызвав проблемы с эфирным наполнением и перебои в работе внутренних систем. Инцидент подчеркнул уязвимость даже крупных медиахолдингов.

Взлом Dr.Web. Группировка DumpForums заявила об успешном взломе Dr.Web, похитив данные клиентов. Хотя Dr.Web признал попытку взлома, факт утечки опровергается. Этот случай указывает на увеличение атак на поставщиков антивирусного программного обеспечения.

Самая масштабная кибератака на Сбербанк. Заместитель председателя Сбербанка сообщил о беспрецедентной кибератаке, продолжавшейся 13 часов, с участием не только украинских IT-специалистов, но и нескольких бот-сетей, состоящих из более 62 тысяч устройств, что свидетельствует о растущей сложности и организованности кибератак.

DDoS-атаки на банки. Атаки, приведшие к недоступности мобильных приложений ВТБ, Росбанка, Альфа-банка и Газпромбанка, а также сбоям в работе веб-сервисов РСХБ и Райффайзенбанка, подчеркнули уязвимость финансовых институтов перед DDoS-атаками [8].

Кибератаки на Восточный экономический форум (ВЭФ). В течение четырех дней Восточный экономический форум подвергался сложным целевым атакам, свидетельствующим о стремлении киберпреступников использовать масштабные мероприятия для своих целей.

Кибератаки на инфраструктуру ЭП. Атака на федеральный центр выдачи электронных подписей (ЭП) привела к приостановке их выдачи более чем на сутки, подчеркивая уязвимость критически важных цифровых сервисов.

Рост DDoS-активности в телекоме. Инциденты, включая сбои в работе мессенджеров из-за DDoS-атак на операторов связи, и 74%-ный рост числа таких атак на телеком-компании, свидетельствуют об эскалации киберугроз в данном секторе.

Утечки персональных данных в e-commerce. Инцидент с интернет-аптекой apteka22.ru, в результате которого были скомпрометированы данные 152 тысяч клиентов (телефоны, ФИО, адреса, детали заказов), демонстрирует высокие риски при обработке и хранении персональной информации в сфере электронной коммерции.

Согласно статистике, 49% кибератак приводят к утечкам конфиденциальной информации. Эти данные указывают на необходимость усиления мер кибербезопасности, как на уровне компаний, так и на государственном уровне, для защиты конфиденциальности данных и обеспечения стабильности цифровой инфраструктуры.

Вскоре после предыдущего инцидента стало известно об утечке из еще одной онлайн-аптеки. Дамп базы данных клиентов, предположительно принадлежащий aptekiplus.ru, содержал имена, около 2 миллионов уникальных адресов электронной почты, 4,5 миллиона уникальных номеров телефонов, а также даты совершения заказов. Это подчеркивает системную проблему защиты персональных данных в сфере онлайн-торговли.

В августе 2024 года произошел инцидент, потенциально имеющий серьезные последствия для национальной безопасности: в открытом доступе, оказалась база данных, содержащая информацию обо всех лицах, пересекавших границу России в период с 2014 по 2023 год. Эксперты IT-сообщества назвали это крупнейшей утечкой из баз данных ФСБ за всю историю ведомства. Несмотря на попытки опровергнуть подлинность данных, эксперты DLBI подтвердили её.

К 2025 году наблюдается устойчивый рост числа кибератак, приводящих к физическому

ущербу. По сравнению с 2023 годом, когда от таких атак пострадали 37,5% жертв, эта тенденция продолжает набирать обороты, что свидетельствует об углублении взаимосвязи между кибер- и физическими угрозами.

Все возрастающие масштабы и тяжесть последствий кибератак за последний год заставляют всерьез переосмыслить подходы к обеспечению защиты корпоративной информации и ИТ-инфраструктуры. Утечка конфиденциальных данных, финансовые потери и ущерб репутации – лишь немногие из потенциальных рисков [9, с.10].

На этом фоне, своевременная оценка и устранение уязвимостей, а также проактивный подход к кибербезопасности, становятся для организаций самым надежным способом защиты от киберугроз.

Однако, попытки полного обособления в цифровой сфере чреваты негативными последствиями. Во-первых, это может привести к технологической изоляции, замедлению инноваций и снижению конкурентоспособности. Во-вторых, создание полностью автономной инфраструктуры требует огромных финансовых и человеческих ресурсов, что не всегда под силу даже развитым странам. В-третьих, полный контроль над данными может нарушать права граждан на приватность и свободу выражения мнений [10, с.46].

Результаты и обсуждение

Правовые аспекты защиты данных в контексте цифрового суверенитета представляют собой сложный баланс между национальной безопасностью, экономическими интересами и правами человека. Рассмотрим некоторые из ключевых вызовов и возможных решений:

Первое, это локализация данных. Требование хранить данные граждан на территории страны является одним из наиболее распространенных, но и самых спорных инструментов. С одной стороны, это позволяет государству обеспечивать контроль за данными, доступ к ним и их защиту, а также эффективно применять законодательство о защите персональных данных, что способствует повышению доверия граждан и укреплению национальной безопасности. С другой стороны, это может быть признание эквивалентности стандартов защиты данных в различных юрисдикциях, что позволит обеспечить свободный поток данных между странами с высоким уровнем защиты.

Второе, это контроль за трансграничной передачей данных. Даже если данные хранятся на территории страны, они могут быть переданы за границу для обработки или хранения. Правовое регулирование трансграничной передачи данных должно обеспечивать адекватную защиту данных в юрисдикции получателя. Это может достигаться путем использования стандартных договорных условий, механизмов обязательных корпоративных правил (BCR) или получения согласия субъекта данных на передачу информации.

Третье, это обеспечение прозрачности и подотчетности. Государство должно обеспечивать прозрачность и подотчетность в вопросах цифрового суверенитета. Граждане должны иметь право знать, как их данные собираются, обрабатываются и используются, и иметь возможность контролировать эту деятельность. Важно, чтобы правовые нормы обеспечивали защиту прав граждан на приватность и свободу выражения мнений, а также устанавливали ответственность государства за нарушение этих прав.

Для эффективного построения цифрового суверенитета и надежной защиты данных необходимо скоординированное совершенствование как правовых, так и экономических инструментов (*рис.1*).

В качестве правовых инструментов построения цифрового суверенитета и надежной защиты данных предлагаются следующие:

во-первых, дифференциация требований к КИИ, в частности ввести более гибкие и экономически обоснованные требования к субъектам КИИ. Для МСП и некритичных сегментов крупных компаний целесообразно разработать упрощенные, но верифицируемые стандарты перехода на отечественное ПО, чтобы избежать паралича бизнеса;

во-вторых, гармонизация регулирования данных с региональными нормами, а конкретнее усилить работу по гармонизации требований ФЗ-152 «О персональных данных» с региональными нормативными актами стран ЕАЭС, стремясь к созданию единого информационного пространства с доверенными партнерами, что упростит трансграничную передачу данных в рамках интеграционных проектов;

в-третьих, необходимо законодательное закрепление стандартов безопасности ПО, в частности внести поправки, обязывающие разработчиков российского ПО проходить обязательную сертификацию кода на отсутствие «закладок» и уязвимостей, используя независимые аккредитованные центры. Основная проблема заключается в том, что законы (ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» 187-ФЗ и ФЗ-152 «О персональных данных») часто устанавливают общие требования к безопасности (например, «использование сертифицированных средств защиты»), но не регламентируют конкретные методики и стандарты аудита самого кода.

Рис. 1 Предложения по совершенствованию правовых и экономических инструментов

Преодоление существующих технологических зависимостей и укрепление режима защиты данных невозможны без активного экономического стимулирования. В свете этого, для построения надежного цифрового суверенитета предлагается использовать следующий набор экономических мер:

– необходим переход от субсидирования к стимулированию спроса, то есть сместить фокус с прямого финансирования разработки на создание гарантированного и долгосрочного спроса на отечественные решения через механизмы государственного заказа с четкими метриками производительности (KPI), а не только наличия в Реестре.
– создание технологических «песочниц» для ИТ-прорывов, в частности финансирование должно быть сосредоточено на 5-7 критических направлениях (например, квантовые вычисления, глубокое машинное обучение, отечественные процессоры архитектуры RISC-V), где разрыв с мировыми лидерами критически велик;
– развитие механизмов сервисной поддержки, в этом случае государство должно стимулировать создание крупных федеральных центров технической поддержки и сопровождения отечественных ИТ-решений, чтобы устранить ключевой барьер для перехода – страх перед отсутствием квалифицированной помощи при внедрении и эксплуатации.

Цифровой суверенитет предполагает, что отечественное ПО должно быть «доверенным». Однако законодательство не всегда обязывает разработчика раскрывать критически важные части своего кода для независимой экспертизы. Если крупный российский разработчик использует в своем продукте компоненты, написанные третьими лицами (включая компании, имеющие связи с иностранными юрисдикциями), или использует проприетарные алгоритмы шифрования, государство не всегда имеет право требовать полного «вскрытия» этого кода для подтверждения его чистоты. Это создает внутренний риск суверенитета.

Отсутствие обязательного «Bug Bounty» (программы поиска уязвимостей), то есть для значимых объектов КИИ требования ФСТЭК включают аудит безопасности и предотвращение вторжений, что может включать привлечение внешних экспертов в рамках закрытых программ или пентестов, но не обязательный публичный Bug Bounty, как в США или ЕС, что также влияет на уровень надежности защиты данных. Законодательно не закреплена обязанность разработчиков критического ПО (особенно для КИИ) проводить публичные или закрытые программы по выявлению уязвимостей с привлечением широкого круга экспертов.

Заключение

Для устранения этих проблем предлагаются введение обязательного требования «Security by Design» (Безопасность по замыслу), в частности

внести в нормативные акты ФСТЭК и ФСБ требование обязательного документирования и прохождения аудита на этапе проектирования (архитектура безопасности), а не только перед выпуском продукта. Необходимо также создание аккредитованных центров аудита исходного кода. На уровне государства создать и аккредитовать независимые коммерческие/некоммерческие центры, специализирующиеся исключительно на глубоком анализе исходного кода критического ПО (для КИИ, государственных систем) с предоставлением «Сертификата доверия к коду», помимо стандартной сертификации продукта. Также целесообразно создать систему стимулирования программ Bug Bounty, предлагается законодательно поощрять (через налоговые льготы или субсидии) разработчиков, которые активно привлекают внешнее сообщество для поиска уязвимостей в своих продуктах, делая это частью их жизненного цикла.

Цифровой суверенитет – это не статичная цель, а динамичный процесс, требующий постоянной адаптации к новым технологиям и угрозам. Правовое обеспечение этого процесса должно быть гибким, сбалансированным и ориентированным на защиту интересов всех заинтересованных сторон.

Проведенный анализ экономико-правовых аспектов обеспечения технологической независимости в контексте цифрового суверенитета Российской Федерации позволяет сформулировать следующие ключевые выводы, интегрирующие результаты исследования нормативной базы, текущей ситуации в сфере кибербезопасности и предложенных мер совершенствования:

Установлено, что в условиях беспрецедентного геополитического давления и эскалации киберугроз (подтвержденных ростом числа и сложности атак, а также масштабными утечками данных в 2024 году), концепция цифрового суверенитета трансформировалась из стратегической цели в неотложный императив обеспечения национальной безопасности. Зависимость от иностранных технологий и платформ, несмотря на существующие меры по локализации данных и запрету закупок, сохраняет критические уязвимости в инфраструктуре, особенно в секторах КИИ.

Существующее законодательство демонстрирует недостаточную детализацию в области верификации безопасности самого программного кода. Формальное включение продукта в Реестр российского ПО (РПО) не гарантирует его фактической устойчивости и доверенности. Критически важно законодательно закрепить методологию «Security by Design» и обязательность аудита исходного кода независимыми аккредитованными центрами для ПО, используемого на объектах КИИ. Отсутствие такой практики создает внутренний риск суверенитета, когда доверенность продукта не может быть полностью подтверждена. Эффективность текущих экономических мер требует смещения фокуса. Прямое субсидирование разработки должно быть дополнено гарантированным долгосрочным спросом со стороны государства, основанным на жестких метриках производительности (KPI), а не только на факте наличия в реестре. Финансовая поддержка должна быть сконцентрирована на прорывных технологических нишах (микроэлектроника, архитектуры RISC-V, ИИ), где разрыв с мировыми лидерами критичен для долгосрочной независимости.

Существует риск создания неконкурентных, дорогих отечественных решений из-за отсутствия должной конкуренции. Предлагаемые меры должны быть направлены на стимулирование конкуренции между российскими разработчиками. Кроме того, для повышения доверия к отечественному ПО и устранения барьеров внедрения необходимо развитие федеральных систем сервисной поддержки и законодательное поощрение программ Bug Bounty для постоянного повышения надежности продуктов.

Достижение устойчивого цифрового суверенитета требует системной конвергенции правовых и экономических рычагов. Правовое поле должно стать более точным в требованиях к качеству безопасности кода, а экономическая политика – более агрессивной в стимулировании прорывных R&D и обеспечении рынка конкурентными, верифицированными доверенными решениями. Только такой скоординированный подход позволит минимизировать риски технологической изоляции и обеспечить надежную защиту национальных информационных активов в долгосрочной перспективе.

Список литературы:

[1] Авдийский, В. И. Особенности влияния деструктивных событий цифрового пространства на экономическую безопасность в условиях цифрового суверенитета государства / В. И. Авдийский, А. В. Иванов // Развитие и безопасность. – 2024. – № 3 (23). – С. 4–25.

[2] Указ Президента РФ от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // Президент России: [сайт]. – URL: http://www.kremlin.ru/acts/bank/50542 (дата обращения 10.05.2025).

[3] Постановление Правительства РФ от 16.11.2015 № 1236 (ред. от 23.12.2024) «Об утверждении Правил формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и

единого реестра программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации» // КонсультантПлюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_189116/ (дата обращения 9.05.2025).

[4] Указ Президента РФ от 30.03.2022 № 166 (ред. от 07.04.2025) «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» // КонсультантПлюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_413177/ (дата обращения 10.05.2025).

[5] Указ Президента РФ от 01.05.2022 № 250 (ред. от 13.06.2024) "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации" // КонсультантПлюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_416198/ (дата обращения 10.11.2025).

[6] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (последняя редакция) // КонсультантПлюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 9.12.2025).

[7] Преступность в России // TAdviser: [сайт]. – URL: https://www.tadviser.ru (дата обращения 7.12.2025).

[8] Михалева, А. Пять крупнейших хакерских атак 2024 года / А. Михалева // РБК: [сайт]. – URL: https://trends.rbc.ru/trends/industry/67613aff9a7947f4d1ea3f71?from=copy (дата обращения: 10.12.2025).

[9] Мухамадиева Э.Ф. Цифровой суверенитет и безопасность в эпоху информации: вызовы и стратегии развития России / Э.Ф. Мухамадиева, Н.И. Шабанов // Экономика и управление: научно-практический журнал. – 2024. – № 4. – С. 10–15. – DOI: 10.34773/EU.2024.4.2.

[10] Кубанцева, Е. В. Цифровая трансформация государственного управления как фактор достижения цифрового суверенитета в Российской Федерации / Е. В. Кубанцева // Общество: политика, экономика, право. – 2023. – № 9 (122). – С. 45–52. – DOI: 10.24158/pep.2023.9.5.

References:

[1] Avdisky, V.I. Features of the influence of destructive events of the digital space on economic security in the context of digital sovereignty of the state/V.I. Avdisky, A.V. Ivanov//Development and security. – 2024. – № 3 (23). - S. 4-25.

[2] Decree of the President of the Russian Federation of 07.05.2024 No. 309 "On the national development goals of the Russian Federation for the period up to 2030 and for the future until 2036 "// President of Russia: [website]. - URL: http://www.kremlin.ru/acts/bank/50542 (date of contact 10.05.2025).

[3] Decree of the Government of the Russian Federation of 16.11.2015 No. 1236 (ed. 23.12.2024) " On approval of the Rules for the formation and maintenance of a unified register of Russian programs for electronic computers and databases and a unified register of programs for electronic computers and databases from the member states of the Eurasian Economic Union, with the exception of the Russian Federation "//ConsultantPlus: [website]. - URL: https://www.consultant.ru/document/cons_doc_LAW_189116/ (accessed 9.05.2025).

[4] Decree of the President of the Russian Federation of 30.03.2022 No. 166 (ed. 07.04.2025) " On measures to ensure the technological independence and security of the critical information infrastructure of the Russian Federation "//ConsultantPlus: [website]. - URL: https://www.consultant.ru/document/cons_doc_LAW_413177/ (date of contact 10.05.2025).

[5] Decree of the President of the Russian Federation of 01.05.2022 No. 250 (as amended by 13.06.2024) " On Additional Measures to Ensure the Information Security of the Russian Federation "// ConsultantPlus: [website]. - URL: https://www.consultant.ru/document/cons_doc_LAW_416198/ (date of contact 10.11.2025).

[6] Federal Law of 27.07.2006 No. 149-FZ "On Information, Information Technology and Information Protection" (latest edition)//ConsultantPlus: [website]. - URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (accessed 9.12.2025).

[7] Crime in Russia//TAdviser: [site]. - URL: https://www.tadviser.ru (accessed 7.12.2025).

[8] Mikhaleva, A. Five largest hacker attacks in 2024/A. Mikhaleva//RBC: [website]. - URL: https://trends.rbc.ru/trends/industry/67613aff9a7947f4d1ea3f71?from=copy (access date: 10.12.2025).

[9] Mukhamadieva E.F. Digital sovereignty and security in the information age: challenges and development strategies of Russia/E.F. Mukhamadieva, N.I. Shabanov//Economics and management: scientific and practical journal. – 2024. – № 4. - S. 10-15. – DOI: 10.34773/EU.2024.4.2.

[10] Kubantseva, E.V. Digital transformation of public administration as a factor in achieving digital sovereignty in the Russian Federation/E.V. Kubantseva//Society: politics, economics, law. – 2023. – № 9 (122). - S. 45-52. – DOI: 10.24158/pep.2023.9.5.