Дата поступления рукописи в редакцию: 25.12.2025 г.
Дата принятия рукописи в печать: 09.01.2026 г.
DOI: 10.24412/2782-3830-2025-12-70-78

ТЕРЕЩЕНКО Елена Анатольевна,
кандидат юридических наук, доцент,
заведующий кафедрой правовой
культуры и защиты прав человека
Федерального государственного автономного
образовательного учреждения высшего образования
«Северо-Кавказский федеральный университет,
e-mail: elena-tereshhenk@yandex.ru

ТРОФИМОВ Максим Сергеевич,
кандидат юридических наук, доцент,
доцент кафедры административного и финансового права
Федерального государственного автономного
образовательного учреждения высшего образования
«Северо-Кавказский федеральный университет»,
г. Ставрополь,
e-mail: sim-pai@mail.ru

ПИСКОВАТСКИЙ Данил Александрович,
ассистент кафедры уголовного права и процесса
Федерального государственного автономного
образовательного учреждения высшего образования
«Северо-Кавказский федеральный университет»,
e-mail: mr.piskovatskia@mail.ru

СООТНОШЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИНФОРМАЦИОННОГО СУВЕРЕНИТЕТА

Аннотация. *Актуальность исследования обусловлена критической зависимостью современного общества и государства от информационных технологий, порождающей новые угрозы и требующей выработки сбалансированных правовых механизмов. Целью статьи является анализ соотношения ключевых концептов — информационной безопасности и информационного суверенитета. Методологическую основу составляют формально-юридический и системный анализ, а также исторический подход, позволяющие исследовать эволюцию, нормативное закрепление и взаимосвязь данных категорий. В ходе рассуждений авторы выделяют общность понятий, заключающуюся в единой цели защиты национальных интересов, и ключевые различия, касающиеся уровня охвата и субъекта ответственности. Практическая значимость статьи заключается в выявлении системных проблем, таких как технологическая зависимость в условиях санкций и необходимость адаптации законодательства к вызовам киберпространства, а также в формулировании перспектив укрепления независимой информационной инфраструктуры. Основной вывод подтверждает тезис о взаимодополняющем характере информационной безопасности и информационного суверенитета: первая создает технико-правовые условия защищенности, а второй обеспечивает стратегическую самостоятельность государства в цифровой среде.*

Ключевые слова*: информационная безопасность, информационный суверенитет, государственная информационная политика, национальные интересы, кибербезопасность, киберугрозы, доктрина информационной безопасности, суверенный Рунет, информационное противоборство.*

Исследование выполнено за счет гранта Российского научного фонда № 25-28-01643 «Информационный суверенитет (суверенитет в информационной сфере): российский и зарубежный опыт правового регулирования и обеспечения», https://rscf.ru/project/25-28-01643/

TERESHCHENKO Elena Anatolyevna,
Candidate of Law, associate Professor,
Head of the Department of Legal Culture
and Human Rights Protection,
North Caucasus Federal University (Stavropol)

TROFIMOV Maksim Sergeevich,
Candidate of Law, associate Professor,
associate Professor Department of administrative and financial law
North Caucasus Federal University (Stavropol)

PISKOVATSKII Danil Alexandrovich,
assistant of the Department of Criminal Law and Procedure
North Caucasus Federal University (Stavropol)

THE RELATIONSHIP BETWEEN INFORMATION SECURITY AND INFORMATION SOVEREIGNTY

Annotation. *The relevance of the study is determined by the critical dependence of modern society and the state on information technologies, which gives rise to new threats and requires the development of balanced legal mechanisms. The aim of the article is to analyze the relationship between the key concepts of information security and information sovereignty. The methodological basis consists of formal-legal and systematic analysis, as well as a historical approach, which allow for the study of the evolution, normative consolidation, and interconnection of these categories. In their reasoning, the authors identify the commonality of the concepts, which lies in the shared goal of protecting national interests, and key differences concerning the level of scope and the subject of responsibility. The practical significance of the article lies in identifying systemic problems, such as technological dependence under sanctions and the need to adapt legislation to the challenges of cyberspace, as well as in formulating prospects for strengthening independent information infrastructure. The main conclusion confirms the thesis about the complementary nature of information security and information sovereignty: the former creates the technical and legal conditions for protection, while the latter ensures the strategic autonomy of the state in the digital environment.*

Key words: *information security, information sovereignty, state information policy, national interests, cybersecurity, cyber threats, Information Security Doctrine, Sovereign Runet, information confrontation.*

Современный мир характеризуется стремительным ростом роли информационных технологий и глобальной зависимостью от них практически всех сфер жизнедеятельности общества и государства. Это обстоятельство порождает множество новых угроз и вызовов, требующих адекватных правовых механизмов реагирования. Современные технологии кардинально меняют способы коммуникации, производства, управления и потребления услуг. Интернет стал неотъемлемой частью повседневной жизни, позволяя мгновенно обмениваться информацией, совершать финансовые операции, получать образование и развлечения онлайн. Цифровые технологии трансформировали привычные формы социального взаимодействия. Люди стали чаще общаться через мессенджеры и социальные сети, что привело к новым формам общественных движений и способов выражения мнений. Появились новые профессии, связанные с управлением социальными сетями, маркетингом и созданием цифрового контента. Однако эта свобода имеет обратную сторону — увеличивается количество киберугроз, таких как хакерские атаки, кража персональных данных и распространение дезинформации. Одним из центральных понятий, отражающих специфику новой реальности, стало понятие «информационный суверенитет», которое неразрывно связано с категорией «информационная безопасность». В данной статье мы хотели бы поставит перед собой задачу рассмотреть соотношение этих двух фундаментальных понятий, выявить общие аспекты и различия, а также обозначить существующие проблемы, возникающие при попытке установить баланс между ними.

Как подчеркивает Ефремов А.А., современный этап развития законодательства представляет собой развитие так называемой «суверенизации», под которым он понимает уход от международно-правового регулирования отношений к национально-правовому.[3] Примером здесь

послужить могут изменения, одобренные в ходе общероссийского голосования 01.07.2020 г. о внесении изменений в Конституцию Российской Федерации, так согласно ч. 1 ст. 15 Конституция России имеет высшую юридическую силу, прямое действие и применяется на всей территории РФ. [8]

Исторически категория «информационная безопасность» возникла значительно раньше, чем концепция «информационного суверенитета». Изначально она была связана преимущественно с обеспечением сохранности конфиденциальной информации и противодействием несанкционированному доступу к ней. По мере распространения информационных технологий расширялось и понимание данного феномена.

Сегодня оно охватывает широкий спектр аспектов, включая защиту информационных систем, инфраструктуру, данные и даже личность пользователя.

В 2016 году Указом президента РФ № 646 была утверждена Доктрина информационной безопасности Российской Федерации (далее – Доктрина). Это основополагающий документ, определяющий государственную стратегию в области защиты информационных ресурсов и информационной среды страны. Доктрина устанавливает принципы, приоритеты и направления деятельности государства в области обеспечения информационной безопасности. Главная цель — защита жизненно важных интересов граждан, общества и государства от угроз, возникающих в информационной сфере.

Стоит отметить, что Доктрина служит основой для выработки и реализации государственной политики в области информационной безопасности. Она определяет направления действий исполнительных органов власти, бизнеса и гражданского общества, помогает координировать усилия различных структур и повышать общий уровень защищенности российского информационного пространства, также способствует формированию единого понимания природы и характера угроз, повышению культуры безопасности среди граждан и снижению вероятности нарушений закона и сбоев в системах управления государством и обществом.

Согласно Доктрине, под информационной безопасностью Российской Федерации понимается состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие, оборона и безопасность [9]. Такое определение соответствует определению безопасности, содержащемуся в современных толковых словарях политико-правового профиля: состояние, когда нет опасности, как определенное состояние, при котором ничто не угрожает кому-либо или чему-либо. [7, с.49]

Исходя из содержания Доктрины можно выделить основные задачи обеспечения информационной безопасности:

1) Защита критической информационной систем, под которой понимается совокупность информационных систем и ресурсов, повреждение или разрушение которых способно вызвать серьёзные последствия для государственной безопасности и всех сфер жизнедеятельности общества.
2) Борьба с киберпреступностью. Так за первую половину 2025 г., согласно исследованию компании «Код Безопасности», число кибератак на Россию увеличилось на 11 % по сравнению с предыдущем годом, количество критических инцидентов выросло на 13%, и, как подчеркивает Газета.ру, эта тенденция обусловлена тем, что злоумышленники все чащи прибегают в целевым атакам, используя продвинутые методы проникновения [10].
3) Повышение уровня осведомленности пользователей о рисках и мерах предосторожности.
4) Разработка нормативной базы, регламентирующей порядок взаимодействия субъектов информационной среды.

Возникающие в процессе цифровизации вызовы, угрозы и многочисленные риски актуализируют необходимость разработки и реализации комплексных мер, направленных на усиление организационной, технологической и правовой составляющих защиты. [6]

Сегодняшняя обстановка в области информационной безопасности России складывается в условиях активных преобразований и противостояния новым угрозам, так уже три с половиной года российский рынок информационной безопасности живет в условиях жестких международных санкций.

Россия стала самой санкционной страной в истории, количество введенных санкций с 2014 г. превысило 30 тысяч, по данным РИА-Новости от 18 июня 2025 г., больше всего ограничений ввели США – 24,5% от всех введённых странами мер, второе место в этом антирейтинге занимает Канада с долей в 13,1 % и замыкает тройку Швейцария с долей 11,8 % [11].

В сложившиеся обстановке Российская Федерация активно создает и развивает собственные технологии виртуализации, облачные сервисы, антивирусы, межсетевые экраны. Сегодня идёт процесс перехода от зарубежного к российскому программному обеспечению, кото-

рое имеет собственные средства защиты, это вызвано с массовыми атаками на государственные организации и учреждения отсюда и ужесточение регулирования.

Информационная безопасность в государственном секторе улучшилась благодаря введению ограничений на передачу зарубежных данных государственным сервисам и ведомствам. Теперь большинство государственных ресурсов заблокировано для HTTP/HTTPS запросов извне, кроме того, почта из иностранных доменов также не принимается. Однако, эти меры затруднили выявление злоумышленниками слабых мест в сетях госорганизаций, хотя полностью предотвратить подобные атаки не удалось, так как вредоносные скрипты продолжают использоваться даже на отечественных серверах [12].

Отсюда и вытекает необходимость в укреплении информационного суверенитета страны, как способности государства контролировать процесс формирования, распространения и потребления информации внутри своей территории, а также защищать собственные интересы в международном информационном пространстве. Этот термин отражает стремление государств сохранить независимость и самостоятельность в принятии решений относительно своего информационного пространства.

Первоначально идея суверенитета была связана преимущественно с территориальной целостностью и политическим господством государства. Она получила широкое признание благодаря развитию международных отношений и появлению первых международных договоров. Однако с началом научно-технического прогресса конца XIX в., особенно с появлением телеграфа и радио, стало ясно, что традиционные представления о суверенитете недостаточны для объяснения реальных условий существования государств.

Становление информационного суверенитета, как научной и политико-правовой категории, началось именно в XX в., когда резко возросла интенсивность потока информации, охватившего весь земной шар. Наиболее заметные события в истории этого процесса включают две мировые войны, Холодную войну и период глобализации второй половины столетия. Во времена холодной войны особое внимание уделялось информационным кампаниям, таким как пропаганда и контрпропаганда, влиянию телевидения и печати на общественное мнение. Советский Союз активно использовал собственный аппарат пропаганды, стремясь создать образ сильного и привлекательного социалистического государства, что значительно повлияло на понимание значения информации для государственной политики. США также активно использовали средства массовой информации для поддержки внешней политики, примером чему служат американские радиостанции Voice of America и Radio Free Europe, вещавшие на территорию СССР и Восточной Европы. Эти мероприятия подчеркнули важность контроля над информационными каналами и необходимость учитывать их влияние на государственную безопасность, как подчеркивают С.Н. Гавров и Д.А. Карташова, здесь не играет роли правда, главное выстроить лжепонимание среди жителей всего мира и в том числе России: «свободного мира Америки» и «плохой России». [1]

Поэтому сегодня государство стремится обеспечить соблюдение принципов информационного суверенитета путем принятия соответствующих нормативных актов, так как формирование самой концепции информационного суверенитета неразрывно связано с разработкой соответствующего правового механизма, призванного обеспечивать реализацию и защиту национальных интересов в информационном пространстве.

В этой связи необходимо вести речь о Федеральном законе «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ [13]. Данный закон является основой для всей системы регулирования информационных отношений в России. Он обеспечивает необходимую степень легитимации деятельности участников рынка информационных услуг, создаёт гарантии защиты интересов граждан и организаций и формирует пространство для развития информационных технологий в безопасной и прозрачной среде. Кроме того, указанный закон стал базисом для разработки множества последующих нормативных актов, направленных на детальное урегулирование конкретных направлений деятельности в информационной сфере, таких как обработка персональных данных, борьба с мошенничеством и защита авторских прав.

Однако, как отмечается, в литературе, стремительное развитие информационно-технологической отрасли и сопутствующий рост киберугроз опережают становление нормативно-правового регулирования в сфере киберпространства и информационной безопасности. Существующее регулирование не достигает требуемого уровня эффективности, отчасти вследствие отсутствия легальных дефиниций и единообразного понимания терминологического аппарата как в научной среде, так и в практике. Данная ситуация создает системную уязвимость и в целом существенно снижает уровень информационной безопасности государства. [5, с.42]

Сегодня актуальной задачей становится адаптация действующего законодательства к

изменениям, происходящим в сфере информационных технологий. Следует учесть рост числа кибератак, увеличение объема обрабатываемой персональной информации и переход к новым технологиям, таким как искусственный интеллект и большие данные. Следовательно, потребуется дальнейшее совершенствование законодательства, принятие поправок и дополнений, уточняющих ответственность и усиливающих меры защиты в свете новых технологических достижений.

Помимо внутреннего законодательства, важным элементом является участие государств в международных организациях и подписании соглашений, касающихся регулирования информационного пространства, согласно Договору о коллективной безопасности СНГ [14] - участники обязуются сотрудничать в целях борьбы с террористическими актами, экстремистскими движениями и иными угрозами, возникающими в результате злоупотреблений современными коммуникациями. Россия здесь выступает активным участником и лидером в процессе интеграции усилий по обеспечению коллективной безопасности в рамках СНГ. Российские военные специалисты регулярно участвуют в совместных учениях, проводятся совместные патрулирования границ, а также осуществляется передача вооружения и техники другим участникам договора. Перспективы дальнейшей деятельности в рамках Договора зависят от ряда факторов, включая геополитическую обстановку, экономическое положение государств-участников и общий климат в регионе. Вместе с тем, расширение практики многостороннего сотрудничества и внедрение инновационных подходов к решению существующих проблем позволит укрепить позиции стран-членов и повысить общую конкурентоспособность региона в целом.

Исторические предпосылки и законодательное регулирование дают свои плоды, а именно создание независимой инфраструктуры, позволяющей сохранять данные и осуществлять передачу информации внутри страны без привлечения иностранных серверов и каналов связи. Такая инфраструктура обеспечивает максимальную надежность и независимость от мировых провайдеров и предотвращает возможное вмешательство третьих стран в процесс обработки данных. Пример успешной реализации подобной схемы — проект «Суверенный Рунет» в России, направленный на создание автономного сегмента интернета, способного функционировать независимо от внешних воздействий. Использование отечественных разработок в области информационных технологий уменьшает зависимость от иностранных поставщиков и снижает вероятность использования уязвимостей, заложенных намеренно производителями другого государства. Государства стимулируют разработку и внедрение локальных операционных систем, приложений и оборудования.

Рассмотрев основные вопросы связанные и с информационной безопасностью и информационным суверенитетом, можно перейти к их соотношению сегодня, как мы поняли ранее информационная безопасность и информационный суверенитет являются ключевыми понятиями современной теории права и международного сотрудничества. Эти два термина часто используются одновременно, однако важно понимать различия и взаимосвязи между ними.

Оба понятия направлены на защиту интересов государства и общества. Информационная безопасность направлена на защиту информации от угроз, связанных с её обработкой, хранением и передачей. Информационный суверенитет касается вопроса самостоятельной политики государства в области информации и коммуникации. Национальные интересы — это приоритеты государства, направленные на обеспечение благополучия, безопасности и процветания нации. Их охрана и защита являются первостепенными задачами государства. Именно поэтому вопросы информационной безопасности и информационного суверенитета находятся в центре внимания руководства большинства стран мира, как трактует Е.В.Горбулева, национальные интересы имеют долгосрочный характер, они направлены на решение конечных задач и достижение целей как во внутренней политике, так и во внешней. [2] Поэтому оба аспекта — информационная безопасность и информационный суверенитет — формируют единую линию защиты национальных интересов. Без надежной защиты информации невозможно говорить о полноценном суверенитете, так как любое нарушение конфиденциальности или целостности ставит под угрозу стабильность и благополучие государства. Одновременно слабый контроль над процессом формирования и распространения информации лишает страну возможности полноценно защищать свои интересы и утверждать себя на международной арене. Таким образом, эффективное взаимодействие между информационной безопасностью и информационным суверенитетом обеспечивает высокий уровень защиты национальных интересов и создаёт базу для защиты от посягательств.

Защищенность информационных систем – это одно из ключевых проявлений общности понятий информационной безопасности и информационного суверенитет. Под защищенностью информационных систем понимается степень защищённости данных, обрабатываемых в информационных системах, от несанкционированного доступа, повреждения, утраты или раз-

рушения. Это достигается за счёт комплекса организационно-технических мер, направленных на профилактику, обнаружение и ликвидацию угроз информационной безопасности. Защищённость информационных систем играет важную роль и в поддержании информационного суверенитета государства. Как мы знаем, информационный суверенитет предполагает независимость и самоопределение государства в выборе и использовании информационных технологий, обеспечение безопасности национальных информационных ресурсов и снижение зависимости от иностранных технологий.

Когда речь идет о защищённости информационных систем, это напрямую влияет на достижение целей информационного суверенитета, поскольку надежно защищённая информационная среда предотвращает возможное вмешательство и контролирует использование национальных информационных ресурсов. Защищённость информационных систем является неотъемлемым компонентом и информационной безопасности.

Она включает в себя комплекс мер и процедур, направленных на предотвращение любых видов угроз, которые могут поставить под сомнение сохранность, целостность и доступность данных и информационных ресурсов. Защищённость информационных систем является обязательным условием существования государства в современном мире. Благодаря высокому уровню защищённости удаётся предотвратить негативные последствия, сохранить суверенитет и поддержать социально-экономическое развитие страны. Таким образом, защищённость информационных систем выступает фундаментом как информационной безопасности, так и информационного суверенитета.

Устойчивое развитие информационного пространства невозможно без уверенности граждан и организаций в их защищённости, что соответствует обоим понятиям. Информационная безопасность гарантирует доверие к конкретным системам, а информационный суверенитет обеспечивает общее ощущение безопасности и независимости в информационной среде. Четкость и прозрачность правил — это одна из ключевых предпосылок для укрепления доверия граждан и организаций к механизмам защиты информации и функционирования информационных систем. Ясность и доступность правил позволяют гражданам чувствовать себя уверенно, понимая, какие меры приняты для защиты их данных и интересов. Предположим, государство внедряет новую систему коммуникации мобильное приложение. Пользователям предоставляется полная информация о мерах защиты, проводится демонстрация работы системы, организуются встречи с представителями приложения для пояснений и консультаций. Подобные действия вызывают положительное восприятие нововведений и усиливают доверие граждан к продукту. Примером может послужить создание кроссплатформенного сервиса MAX, основанного в 2025 г. технологической компанией ВК. К 22 октября 2025 г. количество зарегистрированных пользователей составило 50 миллионов человек и с момента запуска приложения пользователи отправили 3,7 млрд сообщений, позвонили 842 раза и записали более 25 миллионов видеокружков [15].

Укрепление доверия — это не только задача информационной безопасности, но и необходимое условие для устойчивого формирования информационного суверенитета страны. Через прозрачность, интерактивность и вовлеченность удается создать атмосферу уважения и доверия, что ведет к прогрессу и процветанию нации в условиях современной цифровой реальности.

Таким образом, общность понятий информационной безопасности и информационного суверенитета проявляется в единстве целей, методов и ориентиров. данные понятия помогают обеспечить безопасное и свободное функционирование информационной среды, защищают интересы государства и граждан в условиях глобализации и цифровой революции.

Несмотря на сходства для полного рассмотрения соотношения информационного суверенитета и информационной безопасности следует выделить и различия, охватывающие многие вопросы как в политологии, так и в юриспруденции, хотя М.М. Кучерявый и В.В. Бухарин рассматривают как раз информационный суверенитет через призму угроз информационной безопасности. [4] Уровень охвата, это первое существенное различие между информационной безопасностью и информационным суверенитетом. Информационная безопасность охватывает локальные уровни и конкретные объекты. Это значит, что она направлена на защиту конкретных информационных систем, данных, документов и сетевых соединений, это могут быть отдельные организации - компании, учреждения, ведомства, частные лица; определенные системы: баз данных, корпоративных сетей, мобильных устройств. Тактический уровень, который сосредоточен на устранении конкретных угроз и обеспечении защиты конкретных объектов. Информационный суверенитет охватывает национальные и стратегические уровни. Он касается всей информационной среды государства, включая культурные, политические, экономические и технологические аспекты. Это вся информационная среда государства: Государственные структуры, гражданское общество, бизнес, культурные и образовательные учреждения. Широкий спектр интересов: Экономика,

политика, культура, идеология, наука. Создание условий для независимости: Развитие собственной технологической базы, подготовка кадров, разработка. Уровень охвата наглядно иллюстрирует основное различие между информационной безопасностью и информационным суверенитетом. Первый занимается локальными задачами и защитой конкретных объектов, второй — стратегическими вопросами и будущим развитием государства в информационной среде.

Ещё одним различием между информационной безопасностью и информационным суверенитетом касается субъекта ответственности — кого именно привлекают к исполнению задач и обеспечению защиты. Субъект ответственности информационной безопасности — это специалисты и профессионалы, назначенные заниматься защитой информации, здесь можно выделить службы безопасности компаний, сотрудники, ответственные за защиту данных и информационных систем, различные IT-подразделения, то есть специалисты, обслуживающие и настраивающие технику и программное обеспечение, если брать государственные органы, то специальные органы, следящие за выполнением законодательства и стандартов информационной безопасности. Субъект ответственности информационного суверенитета намного шире и охватывает многочисленные группы и слои общества. Основными представителями являются государственные органы исполнительные и законодательные ветви власти, определяющие политику и создающие законы, так же научное сообщество, ученые и исследователи, разрабатывающие технологии и инновации. Субъект ответственности является еще одним показателем различий между информационной безопасностью и информационным суверенитетом. Первая — узкопрофильная задача, осуществляемая профессионалами, вторая — широкая миссия, требующая коллективных усилий общества и государства.

Таким образом, информационная безопасность и информационный суверенитет представляют собой взаимодополняющие, но не тождественные категории. Информационная безопасность является тактико-операционной категорией, обеспечивающей защищенность данных, систем и инфраструктуры от угроз, в то время как информационный суверенитет выступает как стратегическая и политико-правовая концепция, направленная на обеспечение автономии и независимости государства в управлении своим информационным пространством и защите национальных интересов.

Фундаментальной связующей целью обоих концептов является защита национальных интересов. Информационная безопасность создает для этого технико-правовые условия (конфиденциальность, целостность, доступность информации), а информационный суверенитет определяет стратегические рамки и политическую волю для самостоятельного регулирования информационной среды, что в совокупности формирует единый контур национальной безопасности в цифровую эпоху.

Существует системный разрыв между скоростью технологического развития и адаптацией правового регулирования. Динамичный рост IT-сферы и киберугроз опережает нормотворческий процесс. Проблемы усугубляются отсутствием легальных дефиниций ключевых понятий (включая «информационный суверенитет»), что создает терминологическую неопределенность, затрудняет правоприменение и формирует системные правовые риски.

Внешнеполитический контекст (санкции) выступает катализатором импортозамещения и формирования суверенной инфраструктуры. Ответом на ограничительные меры и технологическое давление становится активная разработка национальных IT-решений (ОС, сервисы, средства защиты) и реализация проектов, подобных «Суверенному Рунету». Это свидетельствует о практической реализации концепции информационного суверенитета как инструмента противодействия внешним вызовам.

Субъектный состав обеспечения двух категорий принципиально различен. Информационная безопасность реализуется преимущественно узким кругом профессионалов (специалисты по ИБ, IT-подразделения), тогда как реализация информационного суверенитета требует консолидированных усилий всего государства (органы власти, законодатели, наука, бизнес, гражданское общество), что подчеркивает его общесистемный и политический характер.

Укрепление доверия граждан к цифровой среде является критически важным фактором, объединяющим обе концепции. Доверие формируется как за счет эффективных мер информационной безопасности (защита персональных данных, противодействие киберугрозам), так и благодаря открытой и предсказуемой политике государства в информационной сфере (прозрачность правил, суверенное регулирование). Это доверие выступает основой устойчивого развития информационного общества и легитимности государственной политики в данной области.

Для достижения обеспечения безопасности и независимости в условиях информационных войн, необходимо совершенствовать технологии построить независимую и устойчивую информационную среду. Отсюда соотношение обеих концепций позволяет создать эффективную систему защиты и развития государства в условиях цифровой реальности. Грамотное использование

каждого инструмента даст возможность укрепить безопасность и независимость страны в контексте глобализации и нарастающих информационных угроз.

Список литературы:

[1] Гавров С.Н., Карташова Д.А. Национальный информационный суверенитет сохраняет Россию в истории // Социально-гуманитарные знания. 2022. №6. С.169-172.

[2] Горбулева Е.В. Понятие национальных интересов Российской Федерации // Теория и практика современной науки. 2025. №4 (118). С.73-76

[3] Ефремов А.А. Формирование концепции информационного суверенитета государства // Право. Журнал Высшей школы экономики. 2017. № 1. С. 201–215.

[4] Зиновьева Е.А., Шитьков С.С. Цифровой суверенитет в практике международных отношений // Международная жизнь 2023. №3. С.38-51

[5] Ильясов С.М. Некоторые проблемы совершенствования нормативно-правовой регламентации вопросов информационной безопасности в Российской Федерации // Юридический вестник ДГУ. 2024. Т. 49, № 1 (69). С. 41–49. DOI: 10.21779/2224-0241-2024-49-1-41-49

[6] Наумов В.Б. Современное правовое регулирование идентификации в России. Трансформация информационного права: монография / отв. ред. Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов. М.: Институт государства и права РАН, 2023. 256 с.

[7] Рудницкий С.А. Государственный суверенитет как основа обеспечения национальной безопасности Российской Федерации // Ученые записки Крымского федерального университета имени В.И. Вернадского, Юридические науки. 2023. Т. 9 (75). № 4. С. 47–55.

[8] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) / [Электронный ресурс] / Режим доступа: URL: https://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения 10.10.2025).

[9] Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ №646 от 5 декабря 2016 года / [Электронный ресурс] / Режим доступа: URL: http://www.scrf.gov.ru/security/information/document5/ (дата обращения 11.10.2025).

[10] В России выросло число критических хакерских атак. // Газета.ру. от 22.09.2025 г. / [Электронный ресурс] / Режим доступа: URL: https://www.gazeta.ru/tech/news/2025/09/22/26784434.shtml (дата обращения 11.10.2025).

[11] Количество санкций против России превысило 30 тысяч // РИА-НОВОСТИ от 20.07.2025 / [Электронный ресурс] / Режим доступа: URL: https://ria.ru/20250720/strany-2030232496.html (дата обращения 13.10.2025).

[12] Информационная безопасность в эпоху цифрового суверенитета / [Электронный ресурс] / Режим доступа: URL: https://www.it-world.ru/security/bb1zqodmglws08skc00k8s8408soswc.html (дата обращения 13.10.2025).

[13] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (ред. 01.09.2025) / [Электронный ресурс] / Режим доступа: URL: https: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 24.10.2025).

[14] Договор о коллективной безопасности от 15.05.1992 // Бюллетень международных договоров №12, декабрь 2000 г.

[15] Аудитория мессенджера Max достигла 50 млн пользователей // Радио-РБК от 27.10.2025 г. / [Электронный ресурс] / Режим доступа: URL: https://www.rbc.ru/rbcfreenews/68ff30439a7947691be20575 (дата обращения: 28.10.2025).

References:

[1] Gavrov S.N., Kartashova D.A. National information sovereignty preserves Russia in history// Social and humanitarian knowledge. 2022. №6. P.169-172.

[2] Gorbuleva E.V. The concept of national interests of the Russian Federation//Theory and practice of modern science. 2025. №4 (118). S.73-76

[3] Efremov A.A. Formation of the concept of information sovereignty of the state//Law. Journal of the Higher School of Economics. 2017. № 1. S. 201-215.

[4] Zinovieva E.A., Shitkov S.S. Digital sovereignty in the practice of international relations//International life 2023. №3. S.38-51

[5] S.M. Ilyasov. Some problems of improving the legal regulation of information security issues in the Russian Federation//Legal Bulletin of DSU. 2024. T. 49, NO. 1 (69). S. 41-49. DOI: 10.21779/2224-0241-2024-49-1-41-49

[6] V.B. Naumov. Modern legal regulation of identification in Russia. Transformation of information law: monograph/rev. ed. T.A. Polyakova, A.V. Minbaleev, V.B. Naumov. M.: Institute of State and Law of the Russian Academy of Sciences, 2023. 256 s.

[7] Rudnitsky S.A. State sovereignty as the basis for ensuring the national security of the Russian Federation//Scientific notes of the Crimean Federal University named after V.I. Vernadsky, Legal sciences. 2023. T. 9 (75). № 4. S. 47-55.

[8] Constitution of the Russian Federation (adopted by popular vote 12.12.1993 with amendments approved during the all-Russian vote 01.07.2020) /[Electronic resource]/Access mode: URL: https://www.consultant.ru/document/cons_doc_LAW_28399/ (date of appeal 10.10.2025).

[9] The information security doctrine of the Russian Federation, approved by Decree of the President of the Russian Federation No. 646 of December 5, 2016/[Electronic resource]/Access mode: URL: http://www.scrf.gov.ru/security/information/document5/ (date of reference 11.10.2025).

[10] The number of critical hacker attacks has increased in Russia .// Газета.ру. 22.09.2025/[Electronic Resource]/Access Mode: URL: https://www.gazeta.ru/tech/news/ 2025/09/22/26784434 .shtml (date of appeal 11.10.2025).

[11] The number of sanctions against Russia exceeded 30 thousand//RIA-NOVOSTI from 20.07.2025 /[Electronic resource]/Access mode: URL: https://ria.ru/20250720/strany-2030232496.html (date of appeal 13.10.2025).

[12] Information security in the era of digital sovereignty/[Electronic resource]/Access mode: URL: https://www.it-world.ru/security/bb1zqodmgl-ws08skc00k8s8408soswc.html (date of access 13.10.2025).

[13] Federal Law “On Information, Information Technology and Information Protection” of 27.07.2006 No. 149-FZ (ed. 01.09.2025) /[Electronic Resource]/Access Mode: URL: https: https://www.consultant.ru/document/cons_doc_LAW_61798/ (access date: 24.10.2025).

[14] Collective Security Treaty of 15.05.1992 // International Treaty Bulletin No. 12, December 2000.

[15] The audience of the Max messenger reached 50 million users//Radio-RBC dated 27.10.2025/[Electronic resource]/Access mode: URL: https://www.rbc.ru/rbcfreenews/68ff30439a7947691be20575 (access date: 28.10.2025).

