Дата поступления рукописи в редакцию: 05.12.2025 г. DOI: 10.24412/2782-3830-2025-11-130-136
Дата принятия рукописи в печать: 17.12.2025 г.

ТРУФАНОВА Александра Юрьевна,
магистр, Юго-Западный государственный университет,
e-mail:trufanovaalexandra@gmail.com

БРУСЕНЦЕВА Мария Игоревна,
магистр, Юго-Западный государственный университет,
e-mail: mari.kryukova.2002@mail.ru

ПЕНЬКОВА Ангелина Николаевна,
к.и.н., доцент кафедры теории и истории государства и права,
Юго-Западный государственный университет,
e-mail: angelina-pahomova01@rambler.ru

КОНСТИТУЦИОННО-ПРАВОВОЙ ИНСТИТУТ ЦИФРОВОГО СУВЕРЕНИТЕТА В РОССИЙСКОЙ ФЕДЕРАЦИИ: ПОНЯТИЕ И МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ

Аннотация. *В статье исследуется формирование и развитие конституционно-правового института цифрового суверенитета в Российской Федерации. Авторы анализируют доктринальные подходы к определению понятия «цифровой суверенитет», выявляют его сущностные характеристики и место в системе конституционного права. Особое внимание уделяется конституционным основам цифрового суверенитета, включая нормы о государственном суверенитете, правах и свободах человека в цифровую эпоху. Основной частью работы является комплексный анализ механизмов обеспечения цифрового суверенитета, охватывающий законодательные, организационно-управленческие, технические и правоприменительные аспекты.*

Ключевые слова: *цифровой суверенитет, конституционное право, национальная безопасность, информационная безопасность, цифровая среда, персональные данные.*

TRUFANOVA Alexandra Yurievna,
Master's degree student, Southwest State University

BRUSENTSEVA Maria Igorevna,
Master's degree student, Southwest State University

PENKOVA Angelina Nikolaevna,
Candidate of Historical Sciences,
Associate Professor of the Department of Constitutional Law,
Southwest State University

THE CONSTITUTIONAL AND LEGAL INSTITUTION OF DIGITAL SOVEREIGNTY IN THE RUSSIAN FEDERATION: THE CONCEPT AND MECHANISMS OF ENSURING

Annotation. *The article examines the formation and development of the constitutional and legal institution of digital sovereignty in the Russian Federation. The authors analyze the doctrinal approaches to the definition of the concept of "digital sovereignty", identify its essential characteristics and its place in the system of constitutional law. Special attention is paid to the constitutional foundations of digital sovereignty, including norms on state sovereignty, human rights and freedoms in the digital age. The main part of the work is a comprehensive analysis of the mechanisms for ensuring digital sovereignty, covering legislative, organizational, managerial, technical and law enforcement aspects.*

Key words: *digital sovereignty, constitutional law, national security, information security, digital environment, personal data.*

Стремительная цифровая трансформация всех сфер общественной жизни обусловила появление новых вызовов и угроз для национальной безопасности и государственного суверенитета. Виртуальное пространство, изначально воспринимавшееся как глобальная и децентрализованная среда, стало ареной геополитического соперничества, экономической конкуренции и идеологического противоборства. В этих условиях классическая концепция государственного суверенитета, закрепленная в статье 4 Конституции РФ, потребовала расширительного толкования и адаптации к реалиям цифровой эпохи.

Ответом на эти вызовы стало формирование в Российской Федерации конституционно-правового института цифрового суверенитета. Данный институт находится на стыке конституционного, информационного и международного права и представляет собой один из наиболее динамично развивающихся элементов правовой системы России. Его становление отражает осознание государством необходимости обеспечения независимости, устойчивости и конкурентоспособности национального цифрового пространства.

В современной российской правовой доктрине отсутствует единое легальное определение цифрового суверенитета. Однако его сущность раскрывается через совокупность научных подходов и нормативных положений.

Цифровой суверенитет — это способность государства независимо и эффективно осуществлять юрисдикцию над своим национальным сегментом информационно-телекоммуникационной сети «Интернет» (киберпространством), защищать права и законные интересы граждан и организаций в цифровой среде, обеспечивать безопасность и устойчивое функционирование критической информационной инфраструктуры, а также самостоятельно определять направления и приоритеты развития цифровой экономики и технологий.

Агафонов А.С. говорит о цифровом суверенитете как правовом институте, т. е. системе норм права, регулирующих обособленные общественные отношения, связанные с обеспечением самостоятельности реализации публичных государственных функций в области создания и применения наукоемких информационных технологий, критически важных для обеспечения независимости и конкурентоспособности. В то же время важно отметить, что сегодня можно говорить только про его институциональное развитие, так как нормативная составляющая, которая регламентировала бы данные обособленные общественные отношения, еще не сформирована [1, С. 15].

Выделяются два ключевых аспекта цифрового суверенитета:

1. Внешний (международно-правовой) аспект. Невмешательство во внутренние цифровые дела государства, защита от внешних кибератак, информационно-психологических операций и цифрового давления.
2. Внутренний аспект. Обеспечение верховенства государственной власти в цифровом пространстве, создание правовых и технологических условий для реализации прав граждан, контроль за деятельностью IT-компаний, в том числе транснациональных.

С контекстуальной точки зрения, суверенитет и цифровой суверенитет имеют различные сферы применения и подходы. Кроме того, суверенитет – это общий принцип, обладающий равным объемом и значением повсюду и для всех государств, тогда как цифровой суверенитет может пониматься по-разному. В соответствии с доктриной и практикой, особенно при сравнении демократических и автократических стран, различные контексты применения цифрового суверенитета изменяют его функции и содержание данного понятия [2, С. 678].

Конституционной основой цифрового суверенитета являются следующие фундаментальные принципы и нормы.

Во-первых, государственный суверенитет (ч. 1, 2 ст. 4 Конституции РФ). Распространение суверенитета России на всю ее территорию, включая цифровое пространство.

Во-вторых, право на неприкосновенность частной жизни (ст. 23 Конституции РФ). Защита персональных данных, тайны переписки, телефонных переговоров и иных сообщений от несанкционированного доступа, в том числе со стороны иностранных государств и корпораций.

В-третьих, свобода информации (ч. 4, 5 ст. 29 Конституции РФ). Гарантии свободы массовой информации и права на поиск, получение и распространение информации любым законным способом, что предполагает создание защищенной и суверенной информационной среды для реализации этих прав.

В-четвертых, обеспечение национальной безопасности (ст. 82 Конституции РФ). Президент РФ как гарант суверенитета страны обязан принимать меры по защите государства от угроз, исходящих в том числе из киберпространства.

В-пятых, защита прав и свобод человека и гражданина (ст. 2, 17, 18 Конституции РФ). Обязанность государства защищать права человека в цифровой среде, которые являются непосредственно действующими и определяют смысл и содержание цифрового законодательства.

Таким образом, цифровой суверенитет не создает новую конституционную ценность, а

является логическим развитием и конкретизацией существующих базовых принципов в условиях цифровизации.

Провалинский Д.И. утверждает что, если известное нам физическое пространство трехмерно, то цифровое пространство выступает в качестве своеобразного «окна» в четвертое измерение, за которым ввиду отсутствия (с самого начала и на протяжении уже значительного отрезка времени) осознания всеми без исключения государствами и мировым сообществом в целом опасности не контролируемого правом и моралью поведения пользователей в сети «Интернет» уже прочно закрепился образ «зазеркалья», где традиционное понимание права и правопорядка размыто, искажено либо вовсе отсутствует. Такое состояние неопределенности, и прежде всего правовой, порождает множество проблем, а также вызывает большое количество вопросов, основные из которых можно сформулировать следующим образом. В чьей юрисдикции должно находиться цифровое пространство? Должны ли оно и его участники кому-то вообще подчиняться [3, С. 101-102]?

По нашему мнению, для того, чтобы цифровой суверенитет страны функционировал в полном объеме необходимы механизмы обеспечения. Механизм обеспечения цифрового суверенитета представляет собой сложную, многоуровневую систему взаимосвязанных мер.

Можно выделить несколько групп механизмов обеспечения.

Во-первых, нормативно-правовые механизмы.

Данная группа механизмов формирует правовое поле для реализации цифрового суверенитета.

Стратегия национальной безопасности РФ определяет цифровой суверенитет как один из ключевых элементов национальной безопасности. Также, доктрина информационной безопасности РФ устанавливает национальные интересы в информационной сфере и угрозы им, задает основные направления государственной политики. В то же время важно отметить, что национальная стратегия развития искусственного интеллекта нацелена на обеспечение технологической независимости в сфере сквозных цифровых технологий.

На сегодняшний день в Российской Федерации действует законодательство, которое, в свою очередь, обеспечивает цифровой суверенитет. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ закрепляет требования по защите объектов критической информационной инфраструктуры (КИИ) от кибератак, создает систему государственного управления их безопасностью. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ вводит понятие «целостность» и «устойчивость» российского сегмента интернета, устанавливает основы его регулирования. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ требует локализации баз персональных данных российских граждан на территории РФ, что является краеугольным камнем цифрового суверенитета в сфере приватности.

Во-вторых, организационно-управленческие и технические механизмы, которые обеспечивают практическую реализацию правовых норм.

Создание специализированных органов власти позволяет контролировать соблюдение цифрового суверенитета РФ. Функции по обеспечению цифрового суверенитета возложены на Федеральную службу по техническому и экспортному контролю (ФСТЭК России), Федеральную службу безопасности (ФСБ России), Роскомнадзор, Министерство цифрового развития, связи и массовых коммуникаций. При этом необходимо чтобы параллельно работала система мониторинга и управления. Работа Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы (ГосСОПКА) позволяет отслеживает угрозы для КИИ.

Техническая инфраструктура «суверенного интернета» в соответствии с законом № 149-ФЗ обеспечивается национальной системой доменных имен (DNS), которая позволяет обеспечивать функционирование российского сегмента интернета в случае его отключения от глобальной инфраструктуры. Также организуются точки обмена трафиком, чтобы минимизировать его трансграничный поток и повысить управляемость.

Также важно отметить, что политика импортозамещения в государственном секторе и критически важной инфраструктуре (КИИ) России направлена на снижение зависимости от иностранных технологий и продуктов. Это стратегическое направление стало особенно актуальным в условиях экономических санкций и глобальной нестабильности, когда доступ к западным технологиям и программному обеспечению стал ограничен. Одним из ключевых элементов этой политики является развитие отечественных операционных систем (ОС). Примеры таких систем включают Astra Linux и «РЕД ОС». Эти операционные системы разрабатываются с учетом специфики

российского законодательства, требований к информационной безопасности и особенностей функционирования в государственных учреждениях.

В-третьих, правоприменительные и юрисдикционные механизмы.

Одним из ключевых правоприменительных механизмов является система сертификации и аккредитации программного обеспечения и оборудования, используемого в критически важной инфраструктуре (КИИ). Это позволяет гарантировать, что все используемые технологии соответствуют российским стандартам безопасности и не содержат уязвимостей, которые могут быть использованы для кибератак или утечки данных. Сертификация осуществляется Федеральной службой по техническому и экспортному контролю (ФСТЭК) и другими уполномоченными органами, что создает дополнительные барьеры для иностранных поставщиков, не прошедших соответствующие проверки.

Юрисдикционные механизмы обеспечения цифрового суверенитета предусматривают развитие судебной практики в области информационных технологий. Важным аспектом здесь является защита прав граждан и организаций в случае нарушения их цифровых прав, например, утечки персональных данных или неправомерного использования информации. Разработка специализированных судов или арбитражных органов, занимающихся исключительно делами в сфере цифровых технологий, может способствовать более эффективному разрешению споров и обеспечению соблюдения законодательства.

Федеральный закон «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации» от 01.07.2021 № 236-ФЗ предоставляет государственным органам инструменты для регулирования и контроля доступа к иностранным интернет-ресурсам. Основная цель этого закона заключается в защите прав граждан РФ и обеспечении безопасности информации. В рамках его применения могут быть введены следующие меры:

1. Замедление работы интернет-ресурсов. Одним из методов воздействия на иностранные сайты, которые нарушают права граждан, является замедление скорости их работы. Это достигается путем изменения маршрутизации интернет-трафика или внедрения технических решений, которые затрудняют доступ к ресурсам. Например, при попытке зайти на такой сайт пользователи могут сталкиваться с длительными загрузками или частыми сбоями.
2. Полная блокировка ресурсов. В случае серьезных нарушений, таких как распространение запрещенной информации или нарушение законодательства о защите персональных данных, может быть применена полная блокировка доступа к интернет-ресурсу. Это осуществляется через Роскомнадзор, который вносит сайты в реестр запрещенных ресурсов. Примеры таких мер включают блокировку ряда социальных сетей, которые не выполнили требования российских властей по локализации данных пользователей или по удалению запрещенного контента.

Важно отметить, что перед введением ограничительных мер может проводиться процедура уведомления владельцев сайтов о необходимости устранения нарушений. В случае игнорирования требований, меры становятся более строгими.

С целью усиления защиты информационной безопасности и предотвращения киберпреступлений в России установлены строгие меры ответственности за различные нарушения в области компьютерной информации и критической информационной инфраструктуры (КИИ).

Существуют меры как уголовной ответственности, так и административной.

Так, согласно ст.272 Уголовного кодекса РФ за неправомерный доступ к компьютерной информации устанавливается ответственность, наказание за которую может варьироваться от штрафов до лишения свободы на срок до 7 лет в зависимости от степени тяжести преступления.

Также, статья 273 УК РФ предусматривает уголовную ответственность за создание и распространение вредоносных программ, которые могут нанести ущерб компьютерам и сетям, например, вирусы, трояны и другие виды ПО, предназначенные для кражи данных или разрушения систем.

За нарушение правил эксплуатации КИИ статья 274 УК РФ устанавливает ответственность в виде штрафа, исправительных работ, принудительных работ, ограничения свободы или лишения свободы.

Кодекс об административных правонарушениях (КоАП) также содержит статьи, касающиеся нарушений в области защиты информации и правил обращения с персональными данными. Это может включать штрафы для физических и юридических лиц за несоблюдение требований законодательства.

Также согласно КоАП граждане, должностные лица, индивидуальные предприниматели и организации обязаны обеспечивать защиту

информации от несанкционированного доступа и утечек данных. За отсутствие таких мер могут быть предусмотрены административные штрафы.

Несмотря на наличие сформированной правовой базы, реализация цифрового суверенитета в Российской Федерации сталкивается с рядом серьезных вызовов, которые требуют внимания и комплексного подхода. Рассмотрим каждый из этих вызовов более подробно.

Одним из основных факторов, препятствующих достижению цифрового суверенитета, является сохраняющаяся зависимость России от иностранных технологий в ключевых областях, таких как производство микрочипов и высокоуровневое программное обеспечение. Например, большинство современных микросхем производится в таких странах, как Тайвань и Южная Корея, что создает уязвимости в критически важных инфраструктурах.

Кроме того, многие программные продукты, используемые в государственных и коммерческих структурах, разрабатываются западными компаниями. Это приводит к рискам утечки данных и зависимостям от внешних обновлений и поддержки. Для преодоления этого вызова необходимо инвестировать в развитие отечественных технологий, создание собственных производств и научных исследований, что требует значительных финансовых ресурсов и времени.

К тому же, Интернет по своей природе является глобальной сетью, и полная изоляция национального сегмента представляет собой не только технически сложную задачу, но и экономически невыгодную. Ограничение доступа к международным платформам и сервисам может замедлить инновации и развитие цифровой экономики. Например, многие российские компании зависят от облачных решений и программного обеспечения, предоставляемого зарубежными провайдерами. Если эти услуги будут ограничены или недоступны, это может привести к снижению конкурентоспособности российских компаний на международной арене. Кроме того, изоляция может затруднить сотрудничество с иностранными партнерами и ограничить возможности для обмена знаниями и технологиями.

Концепция цифрового суверенитета – ответная реакция государства (как модели организации социума) на те угрозы, которые оно ощущает благодаря отчасти неконтролируемому развитию ИКТ. Государство находится перед дилеммой. С одной стороны, прогресс несет в себе невиданные позитивные преобразования, позволяющие избавиться от многих исторических «болезней» человечества: бедности, ксенофобии, мракобесия, малограмотности и др. С другой стороны, побочным эффектом может стать если не уход государства с исторической сцены, то заметное снижение его роли как регулятора, охранителя, карателя. Попытками «нащупать» баланс в системе возникающих рисков и выступают отдельные законодательные акты, отстаивающие наличие верховенства власти (суверенитета) в киберпространстве [4, С. 181].

Емельянов А.А., Коршунов И.Л., Микадзе С.Ю отмечают, что цифровой суверенитет предполагает защиту от кибератак, т.е. наличие системы информационной безопасности. Созданием такой системы государство занимается уже давно, считая вопросы информационной безопасности приоритетными. Начиная с 2010 года, оно поддерживает отечественные разработки аппаратных и программных средств; более 30 млрд рублей вложено в создание российских технологий в области информационной безопасности. Проводятся организационные мероприятия, при ФСБ РФ в 2018 году создан Национальный координационный центр по компьютерным инцидентам. Его основным назначением является оперативное реагирование на компьютерные инциденты, связанные с кибератаками [5, С. 87].

Реализация концепции цифрового суверенитета может привести к рискам использования этой идеи для необоснованного ограничения свободы информации и усиления государственного контроля над цифровой жизнью граждан. Власти могут использовать предлоги безопасности для введения жестких мер по контролю за интернет-пространством, что может угрожать демократическим принципам и правам человека. Существуют опасения, что такие меры могут привести к цензуре информации и подавлению свободы слова. Поэтому важно находить баланс между обеспечением безопасности государства и защитой индивидуальных прав и свобод граждан. Это требует открытого диалога между государственными органами, бизнесом и гражданским обществом для разработки эффективных механизмов защиты прав человека в условиях цифровизации.

Таким образом, несмотря на важность цифрового суверенитета для обеспечения независимости страны в цифровом пространстве, его реализация требует комплексного подхода и учета множества факторов, включая технологические, экономические и правовые аспекты.

Перспективы развития цифрового суверенитета в России лежат в нескольких ключевых направлениях, которые требуют комплексного подхода и активных действий со стороны государства, бизнеса и общества. В условиях санкционного давления и технологической зависимости

от иностранных поставок Россия сталкивается с необходимостью ускоренного импортозамещения в критически важных отраслях. Это касается не только программного обеспечения, но и аппаратного обеспечения, включая микросхемы и другие компоненты.

Для решения этой задачи необходимо увеличить финансирование научных исследований и разработок в области высоких технологий. Это может включать создание научных центров, лабораторий и технопарков, где будут разрабатываться отечественные решения. Кроме того, поддержка стартапов и малых и средних предприятий (МСП) через предоставление грантов, налоговых льгот и субсидий на разработку новых технологий станет важным шагом к достижению цифрового суверенитета. Также следует разработать образовательные программы для подготовки специалистов в области IT и инженерии, что поможет создать квалифицированные кадры для отечественной индустрии.

В условиях глобальной цифровизации необходимо выстраивать новые международные отношения, которые позволят странам сотрудничать в области цифровых технологий, обеспечивая при этом безопасность и защиту данных. Создание совместных платформ для обмена данными и информацией между странами-участницами позволит упростить взаимодействие в сфере цифровых технологий. Совместная работа над созданием стандартов и правил управления интернетом, которые будут учитывать интересы всех участников, также имеет важное значение.

С учетом быстрого развития технологий необходимо адаптировать законодательство к новым реалиям, чтобы обеспечить защиту данных граждан и создать безопасную среду для использования искусственного интеллекта. Проведение ревизии действующего законодательства о персональных данных с целью устранения пробелов и недочетов, а также приведение его в соответствие с международными стандартами станет важным шагом. Разработка новых норм, регулирующих использование искусственного интеллекта, должна учитывать этические аспекты, ответственность за принятие решений и защиту прав граждан.

Важно не только защищать интересы государства, но и гарантировать права и свободы граждан в цифровом пространстве. Для этого необходимо проводить общественные обсуждения по вопросам цифрового суверенитета, чтобы учесть мнения гражданского общества и экспертов. Разработка механизмов защиты прав пользователей в интернете, включая право на доступ к информации, право на приватность и право на защиту данных, также имеет первостепенное значение. Учреждение независимых органов, которые будут следить за соблюдением прав граждан в цифровом пространстве и расследовать случаи их нарушения, поможет создать более справедливую цифровую среду.

Существование суверенитета во всем его многообразии является важной идеей в научном и практическом ключе, поскольку помогает странам оставаться независимыми в эпоху всеобщей глобализации ключевых процессов. Данное учение развивается и эволюционирует вместе с человеческим обществом. Изначально людей волновала возможность обоснования самобытности народов и далее государств. На момент написания данной статьи социум все больше и больше связывает свое существование и функционирование с цифровыми технологиями и исходя из этого, все чаще и чаще перед государствами встает вопрос об обеспечении цифрового суверенитета. Его отличительная особенность заключается в дуализме между материальными технологиями и наличие специального программного обеспечения. Цифровой суверенитет, его защита и обеспечение является в XXI веке жизненно важным фактором для государства, которое стремится сохранить лидирующее позиции в мире [6, С. 82].

Таким образом, перспективы развития цифрового суверенитета в России зависят от комплексного подхода к решению перечисленных задач. Это требует активного участия всех заинтересованных сторон — государства, бизнеса и общества — для создания безопасной, инновационной и справедливой цифровой среды.

Подводя итог, отметим, что конституционно-правовой институт цифрового суверенитета в Российской Федерации прошел этап активного становления и представляет собой сегодня сложный, многоаспектный элемент системы национальной безопасности. Его основу составляют конституционные принципы государственного суверенитета, защиты прав человека и обеспечения обороны страны.

Сформированный механизм обеспечения цифрового суверенитета, включающий комплекс нормативных, организационных, технических и правоприменительных мер, демонстрирует целостный и системный подход государства к защите своих национальных интересов в киберпространстве. Однако эффективность этого механизма будет зависеть от успешного решения проблем технологической независимости, преодоления международной изоляции и нахождения сбалансированной модели, которая обеспечит не только безопасность, но и динамичное развитие

цифрового общества в России. Дальнейшее развитие данного института будет определяться эволюцией технологий, изменением геополитической обстановки и поиском адекватных правовых отв етов на новые цифровые вызовы.

Список литературы:

[1] Агафонов, А. С. Место цифрового суверенитета в системе информационного права / А. С. Агафонов // Электронное приложение к Российскому юридическому журналу. – 2024. – № 2. – С. 14-18.

[2] Роблес-Каррильо, М. Суверенитет и цифровой суверенитет / М. Роблес-Каррильо // Journal of Digital Technologies and Law. – 2023. – Т. 1, № 3. – С. 673-690.

[3] Провалинский, Д. И. Правовое обеспечение суверенитета в цифровом пространстве / Д. И. Провалинский // Правосудие. – 2024. – Т. 6, № 2. – С. 98-108.

[4] Романовская, О. В. Право, информационное общество, цифровой суверенитет / О. В. Романовская // Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. – 2024. – Т. 24, № 2. – С. 174-183.

[5] Емельянов, А. А. К вопросу о цифровом суверенитете России / А. А. Емельянов, И. Л. Коршунов, С. Ю. Микадзе // Известия Санкт-Петербургского государственного экономического университета. – 2022. – № 6(138). – С. 84-90.

[6] Карев, Д. А. Цифровой суверенитет / Д. А. Карев, Ю. В. Чертыковцев // Право и государство: теория и практика. – 2025. – № 4. – С. 80-83.

References:

[1] Agafonov, A. S. The place of digital sovereignty in the system of information law/A. S. Agafonov//Electronic Appendix to the Russian Legal Journal. – 2024. – № 2. - S. 14-18.

[2] Robles-Carrillo, M. Sovereignty and Digital Sovereignty/M. Robles-Carrillo//Journal of Digital Technologies and Law. – 2023. - T. 1, NO. 3. - S. 673-690.

[3] Provalinsky, D. I. Legal support of sovereignty in the digital space/D. I. Provalinsky//Justice. – 2024. - T. 6, NO. 2. - S. 98-108.

[4] Romanovskaya, O. V. Law, information society, digital sovereignty/O. V. Romanovskaya//Izvestia Saratov University. New series. Series: Economics. Management. Right. – 2024. - T. 24, NO. 2. - S. 174-183.

[5] Emelyanov, A. A. On the issue of digital sovereignty of Russia/A. A. Emelyanov, I. L. Korshunov, S. Yu. Mikadze//Izvestia of St. Petersburg State University of Economics. – 2022. – № 6(138). - S. 84-90.

[6] Karev, D. A. Digital Sovereignty/D. A. Karev, Yu. V. Chertykovtsev//Law and State: Theory and Practice. – 2025. – № 4. - S. 80-83.

