

ПРАВОВЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЦИФРОВУЮ ЭПОХУ

Манжетов Артур Андреевич

аспирант,

ОЧУВО «Московский инновационный университет»

pro100arthurm@gmail.com

LEGAL METHODS OF ENSURING INFORMATION SECURITY IN THE DIGITAL AGE

A. Manzhetov

Summary. The article examines the main directions of legal methods for ensuring information security in the digital age, including the protection of confidential information, regulation of cybersecurity and countering disinformation. The author examines the theoretical and legal problems of the content and realization of human rights in the context of digitalization of society and interprets such definitions as «digital law», «digital sovereignty». The article provides a brief descriptive description of the problems existing in the field of legal methods of information protection in the digital age, and attempts to compare various legal methods in terms of their description, application and effectiveness in the context of information protection. The author draws attention to the fact that the legal essence of the problem of legal aspects of ensuring information security in the digital age lies in the absence of a single, universal model for regulating information relations in the context of digitalization and globalization and demonstrates how modern legislation seeks to adapt to the challenges associated with information protection, although, at the same time, it faces a number of problems.

Keywords: information security, digital rights, digital sovereignty, cybercrime, digital code, digitalization of society.

Аннотация. В статье рассматриваются основные направления правовых методов обеспечения информационной безопасности в цифровую эпоху, включая защиту конфиденциальной информации, регулирование кибербезопасности и противодействие дезинформации. Автор рассматривает теоретико-правовые проблемы содержания и реализации прав человека в условиях цифровизации общества и дает трактовку таких дефиниций как «цифровое право», «цифровой суверенитет». В статье дана краткая описательная характеристика проблем, существующие в сфере правовых методов защиты информации в цифровую эпоху, и предпринята попытка сравнить различные правовые методы с точки зрения их описания, применения и эффективности в контексте защиты информации. Автор обращает внимание на то, что юридическая суть проблемы правовых аспектов обеспечения информационной безопасности в цифровую эпоху заключается в отсутствии единой, универсальной модели регулирования информационных отношений в условиях цифровизации и глобализации и демонстрирует как современное законодательство стремится адаптироваться к вызовам, связанным с защитой информации, хотя, при этом оно сталкивается с рядом проблем.

Ключевые слова: информационная безопасность, цифровые права, цифровой суверенитет, киберпреступность, цифровой кодекс, цифровизация общества.

В условиях стремительной цифровизации и глобализации правовое регулирование информационной безопасности становится основополагающим инструментом для защиты данных на всех уровнях — от индивидуальных пользователей до государственных и корпоративных структур. Современные информационные ресурсы, такие как персональные данные, корпоративные секреты и государственные информационные системы, приобретают неопределимую ценность, что требует создания и внедрения комплексных правовых механизмов, способных эффективно обеспечивать их защиту в условиях цифровой эпохи.

Правовые методы обеспечения информационной безопасности охватывают широкий спектр направлений. Первое направление — защита конфиденциальной информации, которая включает регулирование процессов сбора, хранения, обработки и распространения данных. Здесь особое значение имеет соблюдение международных стандартов и локальных законодательных актов. Примером такого нормативного регулирования

является Общий регламент по защите данных (GDPR) в Европейском Союзе, который устанавливает строгие требования к защите персональных данных, определяет ответственность за их утечку и неправомерное использование, а также предусматривает значительные штрафные санкции за несоблюдение установленных норм. Кроме того, к правовым методам защиты информации относится управление доступом к данным, что подразумевает использование многоуровневых механизмов контроля, включая идентификацию, аутентификацию и авторизацию пользователей. Важным элементом является также нормативное регулирование информационных систем и сетевой инфраструктуры, направленное на предотвращение несанкционированного доступа, киберугроз и атак, которые могут поставить под угрозу целостность и конфиденциальность информации.

Во-вторых, важнейшим аспектом правовой защиты информации является регулирование вопросов, связанных с кибербезопасностью. Это включает в себя защиту от кибератак, вирусных угроз, хакерских вмешательств

и несанкционированного доступа к информационным системам. Еще одним значимым аспектом является международное сотрудничество в области кибербезопасности, которое направлено на гармонизацию национальных законодательств и создание совместных стандартов безопасности. Это сотрудничество включает обмен информацией о киберугрозах, координацию действий в случае инцидентов и разработку совместных механизмов реагирования на угрозы. Правовые нормы, регулирующие киберпространство, должны учитывать трансграничный характер информационных потоков и предусматривать меры для защиты данных независимо от их географического расположения. Значимость этого элемента правовой защиты подтверждается данными аналитического отчета фонда Росконгресс, согласно которому в 2024 году объем мирового рынка кибербезопасности превысит 200 миллиардов долларов США¹. В отчете «Цифровой суверенитет: как государства защищают интересы в сети» подчеркивается, что государства все больше осознают необходимость разработки и внедрения правовых механизмов, направленных на создание устойчивой и защищенной критической информационной инфраструктуры. В рамках данного направления в России активно разрабатываются и принимаются правовые акты, обеспечивающие устойчивое функционирование критически важных информационных систем, от которых зависит национальная безопасность и общественная стабильность. Примером такого законодательства является Федеральный закон «О безопасности критической информационной инфраструктуры», который возлагает на операторов обязательства по защите таких объектов, определяет порядок их создания, эксплуатации и защиты. Этот закон регламентирует меры, необходимые для предотвращения угроз, и устанавливает ответственность за нарушение установленных норм, что является важным элементом правовой инфраструктуры безопасности.

Третье ключевое направление правового регулирования в сфере информационной безопасности — это противодействие распространению недостоверной или заведомо ложной информации, которая способна нанести ущерб общественным интересам и государственному суверенитету. В условиях глобальной политической напряженности и международных конфликтов борьба с фейковыми новостями и дезинформацией приобретает особую актуальность. Законодательство предусматривает уголовную ответственность за распространение ложной информации, особенно если она касается государственных органов или вооруженных сил. Это нашло отражение в недавних законодательных изменениях в России, направленных на усиление защиты информационного пространства от манипуляций и дезинформа-

ции, что, в свою очередь, способствует укреплению национальной безопасности и стабильности общества.

Кроме того, важной частью правовых методов является регулирование вопросов, связанных с цифровыми правами и цифровым суверенитетом. С развитием цифровых технологий возникает необходимость защиты прав пользователей в онлайн-пространстве, включая право на удаление информации, контроль над своими данными и правомерное использование результатов интеллектуальной деятельности. В России с 2019 года действует законодательство, регулирующее цифровые права, что подчеркивает значимость правовой защиты граждан в цифровом мире. Юридическая суть проблемы правовых аспектов обеспечения информационной безопасности в цифровую эпоху заключается в отсутствии единой, универсальной модели регулирования информационных отношений в условиях цифровизации и глобализации. Современное законодательство стремится адаптироваться к вызовам, связанным с защитой информации, но оно сталкивается с рядом проблем.

В XXI веке наблюдается стремительное развитие интернета и разнообразных информационных технологий, что влечет за собой трансформацию общественных отношений в информационной сфере. В своих трудах, Э.В. Талапина, исследуя влияние информационных технологий на развития прав человека в Интернете, выделяет следующие стадии:

1. Интернет как средство, как элемент известных прав человека (Интернет вплетен в права человека и является средством их реализации/нарушения);
2. Интернет как отражение известных прав человека (два режима прав человека — офлайн и онлайн);
3. Интернет как основа преобразования прав человека» (Талапина, 2019:54).

Другой исследователь этого направления, Е.Г. Стребкова рассматривает влияние новых технологий на реализацию конституционного права граждан на судебную защиту. Она считает, что «это право приобрело новые формы реализации с помощью современных информационных технологий, чат — ботов и искусственного интеллекта. Однако в процессуальном законодательстве есть противоречивые положения, которые вызывают сомнения в необходимости использования информационных технологий и интернета при обращении за судебной защитой (Стребкова, 2021:25). О проблемах распространения фейковых новостей и публикаций, которые направлены на дискредитацию Российской Федерации, пишет в своих публикациях В.В. Севостьянов. Он отмечает, что «искажение информации о Вооруженных силах РФ стало настолько распространенным явлением, что был принят Федеральный закон от 4 марта 2022 года № 32-ФЗ «О внесении изменений в Уголовный кодекс

¹ URL: <https://roscongress.org/materials/tsifrovoy-suverenitet-kak-zalog-globalnoy-bezopasnosti> (дата обращения 10.09.2024).

Российской Федерации и ст. 31 и 151 Уголовно-процессуального кодекса Российской Федерации. Вышеназванные правовые акты предусматривают уголовную ответственность за распространение заведомо ложной информации об использовании Вооруженных сил РФ» (Севостьянов, 2022:22).

Актуальные проблемы проектирования, разработки и внедрения в правоприменительную практику методов защиты информации поднимались в своих исследованиях Ю.А. Гатчина, В.В. Сухостат, А.С. Куракина, Г.Г. Камаловой, Е.Е. Фроловой и др.

В одном из своих выступлений на заседании международной школы-практикуме для молодых ученых-юристов А.А. Клишас председатель Комитета Совета Федерации по конституционному законодательству и государственному строительству, отметил, что реальная защита прав лиц в условиях развития цифровых технологий, обеспечение информационной безопасности, как государства в целом, так и отдельных индивидов в частности, лежит на национальных властных институтах, которые с учётом международных стандартов в области защиты прав человека, должны создавать реальные и действенные механизмы гарантии реализации прав на внутригосударственном уровне².

В условиях цифровой революции и роста объемов данных, передаваемых через глобальные сети, становится очевидной необходимость государственного регулирования, а также создания эффективной правовой политики в отношении информационной безопасности. Угрозы киберпространства, включая утечку данных, несанкционированный доступ к системам и дезинформацию, требуют внедрения новых правовых механизмов для защиты информационных ресурсов. Одним из нововведений правовой системы стало введение в правовое поле понятия «цифровые права». Эти права выступают как новая разновидность имущественных прав, адаптированных к условиям цифровой среды. Они включают в себя правомочия на цифровые активы, данные и информацию, которые приобретают ценность в условиях цифровой экономики. Понятие «цифровые права» отражает прогрессивное направление правовой мысли, адаптирующей традиционные категории имущественных прав к новым условиям киберпространства. Согласно российскому законодательству, цифровые права выступают ключевым элементом регулирования цифровых активов и транзакций, а также отношений, возникающих при использовании информационных технологий. Цифровыми правами признаются названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определяются

в соответствии с правилами информационной системы, отвечающей установленным законом признакам³.

Цифровизация жизнедеятельности граждан вызвала к жизни необходимость пересмотра и уточнения содержания, имущественных прав в контексте информационных технологий. Введение цифровых прав также отражает процессы институционализации правовых норм в условиях глобальной цифровизации. В современном правовом поле трактовка и объем цифровых прав могут изменяться, что обусловлено как изменениями в законодательстве, так и потребностью в адаптации к новым технологическим вызовам и угрозам. Важно отметить, что динамическая природа этих прав требует постоянного мониторинга правоприменительной практики, а также научных исследований, направленных на формирование эффективной правовой доктрины в данной сфере права.

Категории «цифровые права» и «цифровой суверенитет» возникли как ответ на вызовы, связанные с глобальной цифровизацией, которая требует новых подходов к правовому регулированию, новых механизмов защиты прав в цифровой среде: как на уровне индивидов, так и на уровне государств. Цифровой суверенитет представляет собой способность государства самостоятельно определять и контролировать свою цифровую инфраструктуру, данные и информационные потоки⁴. Если более подробно рассмотреть понятие «цифровой суверенитет», то нам необходимо будет обратиться не только к техническим характеристикам этой дефиниции, но и к тем процессам, которые смогли бы обеспечить право каждого гражданина на самоопределение в цифровой среде. Нам представляется интересным интерпретация понятия «цифровой суверенитет» в трудах С. Кутюр, С. Тоупина. Авторы анализируют различные концепции этой дефиниции: «суверенитет киберпространства», «цифровой суверенитет государства и правительства», «цифровой суверенитет коренных народов», «цифровой суверенитет и общественные движения», а также «личный цифровой суверенитет». (Кутюр С., Тоупин С, 2020: 48–69).

Нам также близка позиция тех ученых юристов, которые в своих исследованиях делают акцент на том, для реализации права на защиту, и соответственно на самозащиту, в эпоху цифровой трансформации общества необходимы новые механизмы обеспечения и охраны прав и свобод человека и гражданина⁵.

³ Гражданский кодекс Российской Федерации (часть первая)» от 30.11.1994 N 51-ФЗ (ред. от 08.08.2024) (Электронный ресурс). URL: https://www.consultant.ru/document/cons_doc_LAW_5142/8568bf88dfcdd96ec39cede2444c36c998fbde3/. Дата обращения. 10.09.2024)

⁴ URL [https://roscongress.org/materials/tsifrovoy-suverenitet-kak-zalog-globalnoy-bezopasnosti\(Lfnfj,hfotybz%2010%2F2024\)](https://roscongress.org/materials/tsifrovoy-suverenitet-kak-zalog-globalnoy-bezopasnosti(Lfnfj,hfotybz%2010%2F2024))

⁵ Галиев М.С. Право на защиту как общеправовой принцип права в эпоху цифровой трансформации // Право и государство: теория и практика. 2018. № 8. С. 62.

² URL: <https://alf.ru/news/xiii-mezhdunarodnaya-shkola-praktikum-molodykh-uchenykh-yuristov-pravo-v-usloviyakh-tsifrovoy-realnoy/> дата обращения 10.09.2024)

В Российской Федерации принят ряд законов и нормативных актов, которые формируют правовую основу для защиты информационных систем от кибератак, а также регулируют использование электронной подписи и деятельность в сфере электронной коммерции. Эти правовые инструменты играют ключевую роль в укреплении цифровой экономики. В то же время в современном правовом поле еще есть ряд проблем, связанных с применением правовых методов защиты информации в условиях цифровой эпохи. Как отмечает А.К. Дубень, в условиях глобальной цифровой трансформации и необходимости построения информационного общества проблемы, касающиеся определения основополагающих принципов правового обеспечения информационной безопасности приобретают особое значение⁶.

Одним из ключевых аспектов формирования выше-названных проблем является быстрое развитие технологий, которое зачастую опережает адаптацию правовых норм. Это затрудняет эффективное регулирование новых форм информационных технологий, нейросетей и искусственного интеллекта. Постоянное обновление законодательства и его адаптация к новым вызовам является необходимостью, однако этот процесс требует значительных ресурсов и времени. Кроме этого, мы не можем не обратить внимание на тот факт, что информационные технологии не знают географических ограничений, и это тоже усложняет применение национальных законов в сфере информационной безопасности. Решение этих проблем требует разработки международных соглашений и эффективного сотрудничества между государствами. Создание единых стандартов и принципов регулирования информационной безопасности на международном уровне, как это происходит в рамках международных организаций и форумов, становится необходимым для борьбы с глобальными киберугрозами. Третьей ключевой проблемой является киберпреступность, которая продолжает эволюционировать и становится все более изощренной. Современные кибератаки часто сложны и многоуровневы, что требует постоянного обновления правовой базы и оперативного реагирования правоохранительных органов. Важно также разрабатывать превентивные меры, направленные на предупреждение киберпреступлений и защиту критической информационной инфраструктуры.

Вопрос конфиденциальности и защиты персональных данных также требует пристального внимания. С развитием цифровой экономики все большее количество личных данных обрабатывается и хранится в электронном виде, что создает новые риски утечек и несанкциониро-

ванного доступа. Одной из основных задач правового регулирования в этом контексте является нахождение баланса между правом на частную жизнь и потребностью в сборе и обработке данных для государственных и коммерческих целей. Разработка эффективных механизмов защиты персональных данных и их адаптация к новым вызовам становится первоочередной задачей для законодателей. В контексте развития искусственного интеллекта, больших данных и блокчейн-технологий особое значение приобретают вопросы юрисдикции и правовой ответственности за операции с цифровыми активами. Эти изменения отражают необходимость создания гибких нормативных режимов, способных адаптироваться к быстрым изменениям в технологической среде. Наконец, важным фактором остается образование и осведомленность. Недостаток знаний среди населения и недостаточное внимание к вопросам информационной безопасности может привести к неправильному использованию технологий и увеличению уязвимостей. Стремительное развитие цифровых ресурсов может существенным образом трансформировать всю систему прав человека. Как считает Э.В. Талапина, возникнет система прав человека 3.0.⁷ На форумах и юридических дискуссионных площадках ведутся дебаты о создании мирового (всемирного, универсального) суда по правам человека⁸.

К правовым методам защиты информации относятся различные законодательные и нормативные акты, а также процедуры и механизмы, которые регулируют обработку и защиту информации. Правовые методы защиты информации являются неотъемлемой частью системы обеспечения информационной безопасности. Они включают комплекс мер, направленных на регулирование отношений в этой сфере, контроль за соблюдением норм и привлечение к ответственности за их нарушение. Эффективная защита информации требует постоянного совершенствования законодательства, международного сотрудничества и гармонизации правовых норм. В России исследованиями, связанными с вопросами правовой защиты информации, занимаются такие учёные как, как Л.Л. Попов, А.А. Иванов и В.В. Голубцов, и др. которые известны своими работами в области информационного права и защиты информации. Необходимо отметить, что труды, посвящённые изучению методов защиты информации, часто бывают предметом междисциплинарных исследований, в которых участвуют не только юристы, но и специалисты в области информационных технологий, кибербезопасности и других смежных дисциплин.

⁶ Дубень А.К. — Принципы правового обеспечения информационной безопасности в системе принципов международного права // Международное право. — 2023. — № 2. DOI: 10.25136/2644-5514.2023.2.40089 EDN: KREABN URL: https://nbpublish.com/library_read_article.php?id=40089

⁷ Талапина, Э.В. Права человека в Интернете / Э.В. Талапина // Журнал российского права. — 2019. — № 2(266). — С. 41-54.

⁸ URL: https://izak.ru/institute/events/obzor-pervogo-dnya-xiii-mezhdunarodnoy-shkoly-praktikuma-molodykh-uchenykh-yuristov-pravo-v-usloviya/?sphrase_id=37962 (Дата обращения: 30.08.2024).

В июне 2024 года Институтом законодательства и сравнительного правоведения при Правительстве Российской Федерации был организован и проведен XII Петербургский международный юридический форум, в рамках которого ведущие ученые юристы рассуждали о принятии так называемого «Цифрового кодекса». Обсуждение на форуме подчеркнуло необходимость комплексного подхода к регулированию цифрового пространства, что позволит обеспечить правовую защиту граждан.

На сегодняшний день в нашей стране создан солидный пакет нормативно-правовых актов национально-го законодательства, регулирующий правоотношения в сфере информации, информационной и национальной безопасности. Нормы и институты правового обеспечения информационной безопасности закреплены в международных конвенциях и нормативных правовых актах национального законодательства Российской Федерации. К числу важных источников права в данной области следует отнести Конституцию Российской Федерации, Устав ООН, Федеральный закон «Об информации, информационных технологиях и защите информации», Закон Российской Федерации «О государственной тайне», Федеральный закон «О безопасности», «Стратегия национальной безопасности Российской Федерации», (утверждена Указом Президента РФ от 02.07.2021 № 400) и другие нормативно-правовые акты Президента РФ,

уполномоченных федеральных органов исполнительной власти⁹.

Кроме этого, геополитические вызовы, которые в настоящее время обозначились в общемировом пространстве, способствовали принятию новых нормативных документов в сфере информационной безопасности в РФ. Одним из таких актов стал Указ Президента РФ от 1 мая 2022 года № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». В соответствии с данным указом к 1 января 2025 года запрещается использовать иностранные ПО в органах государственной власти и в государственных корпорациях.

Таким образом, правовые методы защиты информации в цифровую эпоху сталкиваются с рядом вызовов, которые требуют комплексного подхода, включающего совершенствование законодательства, международное сотрудничество, борьбу с киберпреступностью, защиту конфиденциальности и активное повышение уровня осведомленности общества.

⁹ Манжетов, А.А. Особенности правового регулирования в сфере информационной безопасности: теоретический аспект / А.А. Манжетов, С.В. Баринев // Юриспруденция, государство и право: Актуальные вопросы и современные аспекты: сборник статей XIII Международной научно-практической конференции, Пенза, 05 июня 2023 года. — Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2023. — С. 103–107. — EDN EAI0YK.

ЛИТЕРАТУРА

1. Галиев, М.С. Право на защиту как общеправовой принцип права в эпоху цифровой трансформации // Право и государство: теория и практика. — 2018. — № 8. — С. 62.
2. Дубень, А.К. Принципы правового обеспечения информационной безопасности в системе принципов международного права // Международное право. — 2023. — № 2. DOI: 10.25136/2644-5514.2023.2.40089 EDN: KREABN URL: https://nbpublish.com/library_read_article.php?id=40089 (дата обращения: 10.09.2024).
3. Кдлян, Е.Л., Магдесян, Г.А. Правовая регламентация защиты цифровых прав несовершеннолетних детей // Парадигмы управления, экономики и права. — 2024. — № 1(11). — С. 81–89. EDN FNIEQQ.
4. Камалова, Г.Г. Вопросы правового обеспечения информационной безопасности в контексте развития цифровых сервисов // Информационное право. — 2022. — № 4(74). — С. 38–40. DOI: 10.55291/1999-480X-2022-4-38-40. EDN KFTQQX.
5. Кутюр, С., Тоупин, С. Что означает понятие «суверенитет» в цифровом мире? // Вестник международных организаций. — 2020. — Т. 15, № 4. — С. 48–69 (на русском языке). DOI: 10.17323/1996-7845-2020-04-
6. Манжетов, А.А., Баринев, С.В. Особенности правового регулирования в сфере информационной безопасности: теоретический аспект // Юриспруденция, государство и право: Актуальные вопросы и современные аспекты: сборник статей XIII Международной научно-практической конференции, Пенза, 05 июня 2023 года. — Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2023. — С. 103–107. EDN EAI0YK.
7. Стребкова, Е.Г. Судебная защита прав и свобод в эпоху Индустрии 4.0 // Вестник Саратовской государственной юридической академии. — 2021. — № 4(141). — С. 25–33.
8. Сальникова, К.В. Роль информационных технологий как средства защиты ресурсов предприятия от несанкционированного доступа // Социально-экономическое управление: теория и практика. — 2020. — № 3(42). — С. 33–40. EDN MPZWTV.
9. Севостьянов, В.В., Минеев, О.А. О гражданско-правовых механизмах защиты Российской Федерации от диффамации // Правовая парадигма. — 2022. — Т. 21, № 3. — С. 20–28. DOI: 10.15688/1c.jvolu.2022.3.3. EDN TTWEVU.
10. Фролова, Е.Е., Купчина, Е.В. Цифровые инструменты защиты прав на интеллектуальную собственность: на примере блокчейн и искусственного интеллекта // Вестник Пермского университета. Юридические науки. — 2023. — № 61. — С. 479–498. DOI: 10.17072/1995-4190-2023-61-479-498. EDN FWYEIP.
11. Талапина, Э.В. Права человека в Интернете // Журнал российского права. — 2019. — № 2(266). — С. 41–54.
12. Федеральный закон от 27.07.2006 г. № 149-ФЗ (ред. от 03.04.2020) «Об информации, информационных технологиях и о защите информации». [Электронный ресурс]. Режим доступа: URL: <http://www.consultant.ru/> (дата обращения: 19.08.2024).

13. Федеральный закон «О безопасности критической информационной структуры» от 26 июля 2017 г. № 187-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 12 июля 2017 г. // Российская газета. — 2017. — 31 июля.
14. Федеральный закон «О безопасности» от 28 дек. 2010 г. № 390-ФЗ (в ред. от 6 февр. 2020 г.) // Собр. законодательство РФ. — 2011. — № 1. — Ст. 2. Электронный ресурс // СПС «Консультант». URL: <http://www.consultant.ru/document/cons> (дата обращения: 2.09.2024).
15. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации» (ред. 02.07.2021) // Официальный интернет-портал финансовой информации. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 12.08.2024).
16. Указ Президента РФ от 24 июля 2013 г. № Пр-1753 «Основы государственной политики в области обеспечения международной информационной безопасности до 2020 года» // СПС Консультант Плюс. [Электронный ресурс]. Режим доступа: URL: http://www.consultant.ru/document/cons_doc_LAW_178634/ (дата обращения: 17.08.2024).
17. Федеральный закон «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» от 18.03.2019 N 34-ФЗ (последняя редакция). [Электронный ресурс]. Режим доступа: URL: https://www.consultant.ru/document/cons_doc_LAW_320398/ (дата обращения: 07.09.2024).
18. Сайт Ассоциации юристов России. URL: <https://alrf.ru/news/xiii-mezhdunarodnaya-shkola-praktikum-molodykh-uchenykh-yuristov-pravo-v-usloviyakh-tsifrovoy-realno> (дата обращения: 10.09.2024).
19. Сайт фонда Росконгресс. URL: <https://roscongress.org/materials/tsifrovoy-suverenitet-kak-zalog-globalnoy-bezopasnosti> (дата обращения: 10.09.2024).

© Манжетов Артур Андреевич (pro100arthurm@gmail.com)

Журнал «Современная наука: актуальные проблемы теории и практики»