Оригинальная статья
https://doi.org/10.31429/20785836-17-2-28-33

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ЮРИДИЧЕСКОГО ДОКУМЕНТООБОРОТА: БЕЗОПАСНОСТЬ, ЮРИДИЧЕСКАЯ ЗНАЧИМОСТЬ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ И ИНТЕГРАЦИЯ С АНАЛИТИЧЕСКИМИ ПЛАТФОРМАМИ

Морозова О.Г.*[1], Стэллман И.Ю.
[1] ФГБОУ ВО «Кубанский государственный университет»
(Ставропольская ул., д. 149, г. Краснодар, Россия, 350040)

Ссылка для цитирования: Морозова О.Г., Стэллман И.Ю. Цифровая трансформация юридического документооборота: безопасность, юридическая значимость электронных доказательств и интеграция с аналитическими платформами. *Юридический вестник Кубанского государственного университета*. 2025;17(2):28–33. https://doi.org/10.31429/20785836-17-2-28-33

КОНТАКТНАЯ ИНФОРМАЦИЯ:
Морозова Оксана Геннадиевна, кандидат юридических наук, доцент, доцент кафедры теории и истории государства и права юридический факультет имени А.А. Хмырова ФГБОУ ВО «Кубанский государственный университет»
Адрес: ул. Ставропольская, д. 149, г. Краснодар, Россия, 350040
Тел.: +7 (918) 440-54-01
E-mail: Morozova.okcana@yandex.ru

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.
Финансирование. Исследование не имело спонсорской поддержки (собственные ресурсы).

Статья поступила в редакцию: 16.05.2025
Статья принята к печати: 13.06.2025
Дата публикации: 27.06.2025

Аннотация: Целью настоящей статьи является комплексный и многоаспектный анализ ключевых проблем, сопровождающих процесс цифровой трансформации юридического документооборота. Задачи исследования включают углубленное изучение вопросов обеспечения информационной безопасности электронных документов в правовой сфере, анализ доктринальных и правоприменительных подходов к установлению юридической значимости электронных документов как доказательств, а также исследование потенциала и рисков интеграции систем электронного документооборота с интеллектуальными аналитическими платформами. Методологическую основу составили системный анализ, формально-юридический метод, сравнительно-правовой анализ, а также анализ судебной практики и доктринальных источников. Основное внимание уделяется вопросам имплементации и соблюдения законодательства в сфере электронного документооборота, проблемам обеспечения целостности, аутентичности и конфиденциальности электронных доказательств, а также перспективам использования аналитических систем для повышения эффективности правоприменительного и правозащитного контроля в юридической сфере. Результаты исследования демонстрируют наличие ряда системных вызовов, среди которых выделяются проблемы стандартизации форматов юридически значимых документов, необходимость совершенствования криптографических средств защиты и потребность в формировании единообразной и предсказуемой судебной практики по вопросам признания электронных документов. Обосновывается тезис о необходимости глубокой адаптации существующих правовых механизмов к условиям цифровой среды, что включает не только техническое переоснащение, но и развитие цифровых компетенций юристов, судей и правоохранителей, а также активное внедрение верифицированных аналитических инструментов для обработки больших массивов юридически значимых данных. Делается вывод о наличии неразрывной диалектической взаимосвязи между глубиной и качеством цифровой трансформации юридической сферы и состоянием законности и правопорядка в современном информационном обществе.

Ключевые слова: цифровая трансформация, юридический документооборот, электронный документ, электронное доказательство, юридическая значимость, информационная безопасность, аналитические платформы, законность, большие данные, электронная подпись, правосудие.

Введение

Целью настоящей статьи является комплексный анализ проблем безопасности, юридической значимости электронных документов и интеграции систем юридического документооборота с аналитическими платформами. Актуальность исследования обусловлена стремительной и всеобъемлющей цифровизацией публичного управления, правосудия и делового оборота, влекущей за собой не просто эпизодический, а массовый и системный переход на электронный документооборот (далее – ЭДО). Данный процесс является составной частью более глобальной государственной задачи по построению в России информационного общества и цифровой экономики, что требует формирования адекватной, гибкой и прогностической системы правового обеспечения [9]. Реализация национального проекта «Цифровая экономика Российской Федерации» задает вектор на создание сквозных цифровых технологий, которые пронизывают все сферы общественной жизни, включая такую консервативную область, как юриспруденция[1]. Переход от бумажных носителей к цифровым форматам представляет собой не просто техническую замену, но качественную трансформацию, порождающую новые правовые феномены, требующие доктринального осмысления и нормативного закрепления. Как верно отмечает С.В. Бошно: «Цифровой документооборот перестал быть технологической экзотикой, превратившись в неотъемлемый элемент правовой системы» [1, с. 92]. Однако этот переход сопровождается комплексом системных рисков и правовых лакун, которые могут нивелировать ожидаемый положительный эффект.

Ключевыми проблемными зонами, требующими углубленного научного анализа, остаются: обеспечение многоуровневой защищенности электронных документов от несанкционированного доступа, модификации и уничтожения; формирование стабильной и единообразной судебной практики по вопросам исследования и оценки электронных доказательств [4]; а также крайне недостаточная степень использования потенциала современных аналитических систем для предиктивного анализа, мониторинга правоприменения и выявления правовых аномалий. Научная новизна исследования заключается в комплексном, междисциплинарном рассмотрении процесса цифровизации юридического документооборота с акцентом на взаимосвязь технологических, правовых и организационных аспектов, а также на системные риски и пути их минимизации через совершенствование законодательства и правоприменительной практики.

Методы исследования

Методологическую основу настоящего исследования составил комплекс общенаучных и специальных научных методов, применение которых обусловлено междисциплинарным характером и сложностью объекта изучения. Применение системного подхода позволило рассмотреть цифровой юридический документооборот не как изолированное явление, а как сложную, динамично развивающуюся систему, включающую в себя взаимосвязанные подсистемы: технологическую (программное обеспечение, каналы связи), правовую (нормативные акты, правовые режимы), организационную (регламенты, должностные инструкции) и процессуальную (порядок представления и исследования доказательств). В рамках данного подхода безопасность, юридическая значимость и аналитическая обработка данных рассматриваются как неотъемлемые свойства и функции этой единой системы. Формально-юридический метод был использован для детального анализа норм федерального законодательства, составляющих правовую основу ЭДО, в частности, положений Федерального закона от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи», Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также процессуальных кодексов (ГПК РФ, АПК РФ, КАС РФ, УПК РФ), регулирующих статус и порядок использования электронных доказательств. Анализ правоприменительной практики включал в себя изучение и обобщение судебных актов арбитражных судов и судов общей юрисдикции за последние 5–7 лет, связанных с оспариванием юридической силы электронной переписки, договоров, заключенных в электронной форме, а также иных электронных документов. Особое внимание

[1] Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7) [сайт]. Официальный сайт Правительства России; 2025 [обновлено 24 декабря 2018; процитировано 15 мая 2025]. Доступно: http://static.government.ru/media/files/urKHm0gTPPnzJlaKw3M5cNLo6gczMkPF.pdf.

уделялось делам, где предметом спора становилась аутентичность и целостность цифровых данных. Сравнительно-правовой метод применялся для сопоставления отечественного законодательства и правоприменительной практики с подходами, существующими в зарубежных правовых системах, в целях выявления перспективных моделей и лучших практик организации безопасного и юридически значимого ЭДО. Доктринальный анализ научных публикаций позволил выявить существующие в юридической науке дискуссионные вопросы и различные теоретические подходы к определению правовой природы электронного документа и электронного доказательства.

Результаты исследования

Безопасность юридического документооборота. Обеспечение защищенности систем электронного документооборота, используемых в деятельности государственных органов, органов местного самоуправления, судебной системы и коммерческих организаций, остается критически важным и наиболее уязвимым аспектом цифровой трансформации. Правовой режим информационной безопасности, установленный законодательством, предполагает комплексное и эшелонированное применение организационных и технических мер, направленных на нейтрализацию угроз конфиденциальности, целостности и доступности юридически значимой информации [1]. Анализ правоприменительной практики и отчетов регуляторов² выявил ряд типичных и системных нарушений: формальный подход к разработке и внедрению организационных мер защиты (Политики и Регламенты информационной безопасности зачастую носят декларативный характер и не отражают реальные бизнес-процессы), использование криптографических алгоритмов и протоколов, не соответствующих актуальным требованиям (например, применение устаревших стандартов ГОСТ), а также полное или частичное отсутствие формализованных регламентов реагирования на инциденты информационной безопасности. Это приводит к тому, что в случае компрометации системы установить ее причины и последствия юридически корректным способом становится крайне затруднительно. Эффективность государственного и ведомственного контроля в данной сфере существенно ограничена хроническим дефицитом профильных ИТ-компетенций у юристов и специалистов по делопроизводству, а также объективной сложностью проведения полноценного технического аудита и верификации реального уровня защищенности информационных систем контрагентов или нижестоящих организаций. Отдельной проблемой является человеческий фактор: методы социальной инженерии, направленные на сотрудников, имеющих доступ к системам ЭДО, остаются одним из наиболее эффективных векторов атак.

Юридическая значимость электронных доказательств. Несмотря на формальное провозглашение процессуальным законодательством равенства доказательственной силы электронных и бумажных документов (ст. 71 ГПК РФ, ст. 75 АПК РФ, ст. 84 УПК РФ), на практике суды и участники процесса продолжают сталкиваться с существенными проблемами при доказывании их подлинности, целостности и относимости. Как справедливо отмечает в своих работах А.В. Нестеров, теория и практика сталкиваются с отсутствием унифицированного доктринального подхода к самому понятию «электронный документ», что неизбежно порождает противоречия и несогласованность в правоприменении [7]. Особую сложность представляет оценка комплекса электронных доказательств в арбитражном процессе, где цена ошибки может быть чрезвычайно высока. Здесь требуется не только подтверждение формального факта отправки и получения электронного сообщения через оператора ЭДО, но и установление аутентичности его содержания в условиях потенциальных кибератак, таких как «man-in-the-middle» или компрометация учетных данных. Сомнения судов и оппонентов в процессе часто обусловлены ненадлежащим техническим и юридическим оформлением доказательств: отсутствие или использование ненадлежащего вида электронной подписи (например, простая электронная подпись там, где требуется усиленная квалифицированная), несоблюдение установленных законодательством или договором форматов документов, объективная сложность установления конкретного физического лица, сформировавшего и подписавшего документ от имени организации, а также наличие потенциальных уязвимостей в программно-аппаратной цепочке его создания, хранения и передачи [4]. Судебная практика выработала определенные подходы, например, необходимость предоставления протоколов осмотра доказательств, заверенных нотариусом, или проведения судебной компьютерно-технической экспертизы, однако это значительно усложняет и удорожает процесс [5].

Интеграция с аналитическими платформами. Повсеместная цифровизация юридической деятельности и накопление огромных массивов структурированных данных создают уникальные предпосылки для качественного преобразования правоприменительной и контрольно-надзорной

[1] Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации: учеб. пособие. М.: Юрист; 2001.

деятельности через интеграцию ведомственных и межведомственных систем ЭДО с интеллектуальными аналитическими платформами (далее – АП). Потенциальные возможности таких платформ чрезвычайно широки и выходят далеко за рамки простого статистического учета. Мониторинг правоприменения может осуществляться путем автоматизированного анализа больших массивов данных, извлекаемых из систем ЭДО судов (ГАС «Правосудие»), государственных органов (СМЭВ), Федеральной налоговой службы (данные из ЕГРЮЛ/ЕГРИП и систем контроля за НДС) для выявления системных нарушений законодательства. Например, такой анализ способен выявить аномально большое количество массовых отказов в предоставлении определенных электронных госуслуг в конкретном регионе или ведомстве, что может свидетельствовать о наличии коррупционных факторов или неверном толковании норм права. Предиктивная аналитика, в свою очередь, позволяет на основе анализа исторических данных и выявленных корреляций прогнозировать риски совершения правонарушений в сфере использования ЭДО, например, выявлять признаки мошеннических схем при проведении электронных торгов или при возмещении НДС. Однако следует признать, что правовое регулирование обработки больших данных (Big Data) и применения технологий искусственного интеллекта в юриспруденции катастрофически отстает от темпов технологического развития, что создает состояние правовой неопределенности и порождает риски нарушения прав граждан [6]. Внедрение отдельных элементов АП уже осуществляется в деятельности ряда ведомств, в частности, ФНС России и Прокуратуры РФ [10], но для его масштабирования требуется решение целого ряда задач: развитие нормативной базы, регламентирующей сбор, обработку и использование Big Data в государственных целях; обеспечение технической и семантической совместимости разнородных информационных систем; а также кардинальное повышение уровня ИТ-квалификации юристов и аналитиков[1].

Научная дискуссия

Глубокая и всепроникающая интеграция цифровых технологий в юридическую практику и документооборот порождает острые дискуссии в научном сообществе, затрагивающие фундаментальные основы права. По мнению С.В. Зыкова: «Правовая неопределенность в использовании больших данных остается главным барьером для внедрения аналитических платформ в юридическую практику» [2, с. 120]. Эта неопределенность касается не только технических, но и этических аспектов, например, допустимости использования предиктивной аналитики в правосудии, что может противоречить принципу презумпции невиновности. Ряд авторов, в частности представители правоохранительных органов, настаивают на необходимости расширения специальных полномочий контролирующих и надзорных органов для эффективного контроля за соблюдением законодательства в цифровой среде [13]. Это включает в себя предоставление им права на получение прямого доступа к данным операторов ЭДО и облачных хранилищ для проведения оперативных проверок и выемки цифровых улик. Другие исследователи, придерживающиеся либеральных позиций, указывают на серьезные риски такого подхода, связанные с возможностью избыточного вмешательства государства в частную жизнь и коммерческую тайну, и подчеркивают важность соблюдения строгого баланса между задачами контроля и необходимостью защиты прав и свобод, а также стимулирования развития цифровых технологий [3]. В более широком, философско-правовом контексте, Д.А. Пашенцев указывает на фундаментальные риски, связанные с трансформацией самой российской правовой традиции под влиянием глобальных цифровых платформ и англосаксонских правовых концепций, что в перспективе может привести к эрозии базовых принципов отечественного права, сформированных в рамках континентальной системы [8]. Обсуждается также вопрос о достаточности существующей законодательной базы, построенной по принципу «технологической нейтральности», или о необходимости принятия специальных, комплексных нормативных актов, таких как Цифровой или Информационный кодекс [11].

Практика показывает, что эффективность правового регулирования в новой цифровой реальности напрямую зависит от решения нескольких ключевых системных проблем. Во-первых, это проблема стандартизации. Отсутствие единых, юридически обязательных и технически строгих стандартов для форматов, метаданных и протоколов обмена для юридически значимого ЭДО создает «цифровой Вавилон», затрудняющий как взаимодействие систем, так и последующий надзор и анализ данных. Во-вторых, это проблема доверия. Необходимо дальнейшее развитие и повышение надежности национальной инфраструктуры доверия, включающей в себя не только удостоверяющие центры, но и доверенные третьи стороны, службы проставления штампов времени и архивы электронных документов. В-третьих, это проблема доказывания. Требуется дальнейшее

[1] Адыгезалова Г.Э. Правовая аналитика: учебник. М.: Директ-Медиа, 2023. 464 с.

совершенствование методик судебной экспертизы цифровых следов и повышение уровня цифровой грамотности судейского корпуса. Наконец, это кадровая проблема. Острый дефицит «цифровых юристов» – специалистов, обладающих глубокими познаниями одновременно в области юриспруденции, информационных технологий, криптографии и анализа данных, – является одним из главных препятствий для успешной цифровой трансформации [12].

Проведенное исследование позволяет сделать следующие выводы:

1. Цифровая трансформация юридического документооборота является объективным и необратимым процессом, который создает как уникальные возможности для повышения транспарентности, скорости и эффективности правоприменения, так и порождает значительные системные риски в области информационной безопасности, обеспечения достоверности информации и защиты прав субъектов данных.

2. Основными проблемными зонами, сдерживающими позитивный потенциал цифровизации, остаются обеспечение должного технического и организационного уровня безопасности систем ЭДО, формирование единообразной и предсказуемой судебной практики признания юридической значимости различных видов электронных доказательств, а также крайне недостаточная интеграция существующих систем ЭДО с современными аналитическими платформами.

3. Для повышения эффективности правовой системы в условиях цифровизации необходим комплексный подход, включающий: совершенствование нормативной базы, более четко регламентирующей требования к безопасности ЭДО, порядку использования электронных доказательств и правовому режиму больших данных; развитие цифровых компетенций юристов, судей, прокуроров и следователей; стимулирование активного внедрения и развития отечественных специализированных аналитических платформ, интегрированных с ключевыми государственными источниками юридически значимых данных; а также укрепление практического взаимодействия между юридическим сообществом, регуляторами в сфере цифровых технологий (Роскомнадзор, ФСТЭК России, ФСБ России) и операторами критической информационной инфраструктуры.

4. Перспективным направлением дальнейших научных исследований является разработка доктринальных основ и практических моделей предиктивного анализа на основе обработки больших данных из систем юридического документооборота в целях профилактики правонарушений, а также исследование правовых и этических границ применения технологий искусственного интеллекта в сфере правосудия и государственного контроля.

Список использованной литературы:

1. Бошно С.В. Электронный документ и электронное доказательство в юридическом процессе: проблемы теории и практики. *Журнал российского права*. 2020;(8):91–105. DOI: 10.12737/jrl.2020.096.

2. Зыков С.В. Прокурорский надзор в цифровую эпоху: границы допустимого. *Государство и право*. 2023;(4):118–127. DOI: 10.31857/S102694520024889-1.

3. Казаков В.В. Информационная безопасность в деятельности органов прокуратуры: современные вызовы и пути решения. *Законность*. 2022;(5):12–16.

4. Кудрявцев В.Н. Электронные доказательства в гражданском и арбитражном процессе: проблемы допустимости и оценки. *Арбитражный и гражданский процесс*. 2021;(10):29–34.

5. Лаптев В.А. Электронное правосудие и искусственный интеллект: зарубежный опыт и перспективы для России. Вестник Санкт-Петербургского университета. Право. 2021;(12(3)):576–591. DOI: 10.21638/spbu14.2021.305.

6. Минбалеев А.В. Проблемы правового регулирования больших данных (Big Data). *Проблемы права*. 2019;(70(2)):74–79.

7. Нестеров А.В. Цифровая трансформация юридической деятельности и законодательства. *Правовое государство: теория и практика*. 2020;2(60):26–37.

8. Пашенцев Д.А. Российская правовая традиция перед вызовом глобализации. *Юридическая наука*. 2016;(3):9–12.

9. Полякова Т.А. Правовое обеспечение информационной безопасности при построении информационного общества в России: монография. М.: ИГП РАН; 2008.

10. Скуратов Ю.И. Цифровая трансформация прокуратуры: вызовы и перспективы. Вестник прокуратуры. 2023;(55(1)):3–9.

11. Талапина Э.В. Право и цифровизация: новые вызовы и перспективы. *Журнал российского права*. 2018;(2):5–17. DOI: 10.12737/art_2018_2_1.

12. Хабриева Т.Я. Право перед вызовами цифровой реальности. *Журнал российского права*. 2018;(9):5–16. DOI: 10.12737/art_2018_9_1.

13. Чугунов Ю.В., Смирнов А.А. Использование больших данных и аналитических платформ в деятельности органов прокуратуры. Информационное право. 2022;(69(3)):17–22.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Морозова Оксана Геннадиевна
кандидат юридических наук, доцент, доцент кафедры теории и истории государства и права юридический факультет имени А.А. Хмырова ФГБОУ ВО «Кубанский государственный университет»
ORCID: https://orcid.org/0000-0002-4699-1976

Стэллман Ирина Юрьевна
кандидат экономических наук