

МАТВЕЕВА Екатерина Владимировна,
студентка, Санкт-Петербургского университета
Государственной противопожарной службы МЧС России
им. Героя Российской Федерации генерала
армии Е.Н. Зиничева,
e-mail: kattya_matveeva_2006@mail.ru

МОИСЕЕНКО Михаил Иванович,
Кандидат юридических наук,
доцент кафедры административного права и процесса,
Санкт-Петербургского университета Государственной
противопожарной службы МЧС России
им. Героя Российской Федерации генерала
армии Е.Н. Зиничева,
e-mail: mmimi1963@mail.ru

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ

Аннотация. Статья посвящена анализу современного состояния правового регулирования электронных доказательств в российском гражданском процессе. Исследуется соотношение цифровой среды и традиционной модели доказательственного права, закрепленной в ГПК РФ. Рассматриваются нормативные основания использования электронных данных в суде, выявляются пробелы в законодательной конструкции статьи 55 и статьи 71 ГПК РФ, а также проблемы судебной практики, связанные с допустимостью, достоверностью, идентификацией источника и обеспечением неизменности цифровой информации. Отдельное внимание уделяется переписке в мессенджерах, электронной почте, скриншотам, данным интернет-ресурсов, цифровым аудио- и видеозаписям, метаданным и иным данным, формируемым информационными системами. Обосновывается вывод о недостаточности существующего подхода, при котором электронные доказательства фактически распределяются между письменными доказательствами, вещественными доказательствами и аудио- и видеозаписями без признания их самостоятельной процессуальной природы. Предлагаются направления законодательной модернизации: закрепление дефиниции электронных доказательств в статье 55 ГПК РФ, установление требований к форме представления, правилам аутентификации, фиксации метаданных, проверке целостности цифрового файла, а также введение специальных процедур исследования электронных доказательств в судебном заседании.

Ключевые слова: электронные доказательства, гражданский процесс, ГПК РФ, допустимость доказательств, достоверность доказательств, цифровые данные, электронный документ.

MATVEEVA Ekaterina Vladimirovna,
student, St. Petersburg University of the State Fire Service
of the EMERCOM of Russia named after Hero
of the Russian Federation, General of the Army E.N. Zinichev

MOISEENKO Mikhail Ivanovich,
Candidate of Law, Associate Professor,
Department of Administrative Law and Process,
St. Petersburg University of the State Fire Service
of the EMERCOM of Russia named after Hero
of the Russian Federation, Army General E.N. Zinichev

PROBLEMS AND PROSPECTS OF LEGAL REGULATION OF ELECTRONIC EVIDENCE

Annotation. The article is devoted to the analysis of the current state of legal regulation of electronic evidence in the Russian civil process. The correlation between the digital environment and the traditional model of evidence law enshrined in the Code of Civil Procedure of the Russian Federation is examined. The article discusses the regulatory basis for the use of electronic data in court, identifies gaps in the legislative structure of Articles 55 and 71 of the Code of Civil Procedure of the Russian Federation, and addresses the challenges of judicial practice related to the admissibility, reliability, identification of the source, and ensuring the immutability of digital information. Special attention is paid to correspondence in instant messengers, e-mails, screenshots, data from Internet resources, digital audio and video recordings, metadata and other data generated by information systems. The conclusion is substantiated that the existing approach is insufficient, in which electronic evidence is actually distributed between written evidence, material evidence and audio and video recordings without recognizing their independent procedural nature. The paper proposes the following areas of legislative modernization: the consolidation of the definition of electronic evidence in Article 55 of the Civil Procedure Code of the Russian Federation, the establishment of requirements for the form of presentation, authentication rules, metadata recording, and digital file integrity verification, as well as the introduction of special procedures for examining electronic evidence in court.

Key words: electronic evidence, civil procedure, Civil Procedure Code of the Russian Federation, admissibility of evidence, reliability of evidence, digital data, electronic document.

Цифровизация общественных отношений изменила способ фиксации юридически значимых обстоятельств. Существенная часть коммуникации, хозяйственного взаимодействия, документооборота и заключения сделок переместилась в электронную среду. Обстоятельства, имеющие значение для разрешения гражданско-правовых споров, фиксируются в виде электронных писем, сообщений в мессенджерах, данных информационных систем, записей камер видеонаблюдения, файлов журналов регистрации событий, сведений, размещенных на сайтах, и иных цифровых объектов. Судебное доказывание оказалось вовлечено в пространство, где информация существует без устойчивого материального носителя, воспроизводится техническими средствами и поддается скрытой модификации.

Российское гражданское процессуальное законодательство не выработало завершенной модели регулирования таких доказательств. Статья 55 ГПК РФ содержит традиционный перечень средств доказывания и не выделяет электронные доказательства в самостоятельный вид. Статья 71 ГПК РФ допускает использование электронных документов в рамках письменных доказательств при условии возможности установить их достоверность. Подобная конструкция охватывает лишь часть цифровых данных [1]. Переписка в мессенджерах, скриншоты, сведения с веб-страниц, логи систем, данные мобильных приложений, облачные файлы, цифровые следы сетевой активности не укладываются в категорию письменного доказательства без существенных оговорок. В результате правоприменитель вынужден подводить различные по природе цифровые объекты под процессуальные формы, сформированные для бумажных документов и материальных носителей.

Проблема носит не терминологический, а структурный характер. Электронное доказательство отличается от бумажного документа способом существования, порядком восприятия и механизмами проверки. Для исследования цифровой информации требуются технические средства. Для оценки надежности необходим анализ происхождения файла, цепочки его передачи, метаданных, условий хранения и признаков вмешательства. Для установления принадлежности сообщения конкретному лицу недостаточно визуального содержания распечатки. Для подтверждения неизменности скриншота мало самого факта его нотариального удостоверения. Для проверки видеозаписи требуется определить источник создания файла, способ его извлечения, наличие следов монтажа и соответствие временных параметров.

Нормативная инерция в сфере доказательственного права приводит к ряду практических последствий. Участники процесса сталкиваются с неопределенностью при выборе формы представления электронных данных. Судебная практика вырабатывает собственные критерии приемлемости доказательств, однако эти критерии нередко имеют казуистический характер и различаются в зависимости от категории спора, уровня суда и конкретной процессуальной ситуации. Судья получает широкое усмотрение при оценке того, можно ли признать достоверной переписку в мессенджере, распечатку электронной почты, скриншот сайта, запись с телефона или сведения, выгруженные из корпоративной системы. Усмотрение в сфере технически сложных доказательств без закрепленных стандартов порождает неравномерность правоприменения.

Особую значимость вопрос приобретает в гражданском процессе, где принцип состязательности требует предсказуемых правил фор-

мирования доказательственной базы. Если участник спора не может заранее определить, какие цифровые данные будут приняты судом, в каком виде их надлежит представить и какие средства подтверждения подлинности потребуются, реализация права на судебную защиту осложняется. Возникает риск, при котором исход дела зависит не от содержания информации, а от удачности ее процессуального оформления и от субъективной готовности суда воспринимать конкретный цифровой источник как надежный [2].

Научная дискуссия об электронных доказательствах развивалась в русле двух основных подходов. Первый исходит из достаточности традиционной классификации доказательств и предлагает распределять электронные данные между уже известными категориями: электронные документы считать письменными доказательствами, цифровые носители относить к вещественным доказательствам, аудио- и видеозаписи оценивать в рамках прямо названных в статье 55 ГПК РФ средств доказывания. Второй подход исходит из наличия у цифровой информации самостоятельных признаков, исключающих ее полное растворение в классических видах доказательств. Для него характерно стремление выделить электронные доказательства как отдельную процессуальную категорию.

Первый подход удобен для сохранения формальной целостности кодекса, однако он не снимает практических противоречий. Электронный документ в цифровой системе не тождествен бумажному документу, поскольку его доказательственное значение определяется не только текстом, но и реквизитами файла, метаданными, электронной подписью, идентификаторами пользователя, журналом действий, серверным временем. Скриншот веб-страницы не является письменным доказательством в обычном смысле, потому что он отображает визуальное состояние интерфейса в конкретный момент, не раскрывая происхождения размещенной информации и условий ее фиксации. Переписка в мессенджере не совпадает с традиционным документом, так как ее значение зависит от принадлежности аккаунта, синхронизации устройств, истории редактирования и иных технологических обстоятельств. Видеофайл с камеры наблюдения отличается от аналоговой записи по способу формирования, степени сжатия, наличию встроенных временных меток, параметров кодирования и возможности машинного изменения.

Содержательное разграничение электронных доказательств можно строить по источнику происхождения и по способу фиксации информации. Одна группа включает цифровые коммуникации: электронную почту, SMS, MMS, сообще-

ния в мессенджерах, переписку в социальных сетях, уведомления из приложений, данные интернет-провайдеров и операторов связи. Другая группа охватывает электронные документы, созданные в информационных системах: договоры, акты, счета, заявки, реестры, выписки, подписанные электронной подписью либо существующие без нее. Третья группа объединяет мультимедийные данные: фотографии, аудиозаписи, видеозаписи, скриншоты, записи с камер видеонаблюдения, видеорегистраторов, мобильных устройств. Четвертая группа включает автоматически формируемые системой данные: логи, журналы авторизации, сведения о транзакциях, записи о геолокации, серверные отметки времени, идентификаторы устройств.

Для каждой из названных групп характерен собственный набор рисков. В цифровой переписке центральное значение имеет идентификация субъекта коммуникации. Для электронных документов — подтверждение авторства, целостности и юридической силы файла. Для мультимедийных объектов — выявление признаков монтажа, обрезки, перекодирования, искусственной генерации и нарушения непрерывности записи. Для системных журналов — установление надежности информационной системы, регламентов доступа и невозможности постфактумного изменения записей без следа [3].

Закон не закрепляет общие требования к представлению такого массива данных. В практике используются материальные носители, распечатки, выгрузки из приложений, ссылки на сайты, файлы, загруженные через государственные информационные системы, нотариальные протоколы осмотра интернет-страниц, акты специалистов, заключения экспертов. Набор форм зависит от инициативы стороны и от того, каким образом суд воспринимает допустимый способ приобщения к делу. Отсутствие единых технических стандартов означает отсутствие единых критериев полноты и надежности представления цифровой информации.

Проблема допустимости электронных доказательств связана с частью 2 статьи 55 ГПК РФ, согласно которой сведения о фактах должны быть получены в предусмотренном законом порядке. Для бумажного документа содержание этого требования относительно ясно. Для цифрового файла возникает цепочка вопросов: кем и когда он создан, каким устройством, где хранился, каким способом извлечен, кто имел доступ, проводилось ли копирование, изменялись ли системные атрибуты, фиксировалась ли контрольная сумма, сохранены ли метаданные, воспроизводится ли файл в исходном формате. При отсутствии специальных норм суд вынужден

решать эти вопросы через свободную оценку доказательств, что не обеспечивает необходимой устойчивости.

Допустимость тесно связана с формой представления. Действующее регулирование допускает подачу документов через системы электронного правосудия и портал государственных услуг, представление материалов на бумаге и на электронном носителе. Однако цифровое доказательство может утратить значимую часть своих свойств при переводе в бумажную форму. Распечатка электронной переписки не показывает сведения о сервере, маршруте сообщения, идентификаторах, времени доставки, возможном редактировании. Печатная копия скриншота скрывает свойства файла изображения. Распечатка веб-страницы не позволяет проверить адрес ресурса, HTML-код, дату обращения, заголовки ответа сервера и содержание активных элементов. Бумажная форма в ряде случаев превращает цифровое доказательство в производную фиксацию, обедненную по сравнению с исходным объектом [4].

Еще сложнее вопрос о достоверности. В части 3 статьи 67 ГПК РФ закреплено требование оценки достоверности доказательств. Для цифровой среды достоверность означает не совпадение с субъективным представлением суда о правдоподобии, а возможность установить подлинность источника, целостность содержания и отсутствие скрытого вмешательства. Наиболее уязвимым элементом выступает идентификация лица, от имени которого исходила информация. Адрес электронной почты, номер телефона, аккаунт в мессенджере, учетная запись в социальной сети не подтверждают автоматически, что сообщение создано именно стороной спора. Возможны использование третьими лицами, компрометация доступа, регистрация на чужие данные, передача устройства, взлом аккаунта, подмена имени пользователя.

По этой причине суды нередко требуют дополнительных подтверждений: ссылки в договоре на конкретные каналы связи, признание факта переписки другой стороной, последовательность коммуникации, наличие ответных сообщений, согласование существенных условий, сопоставление содержания переписки с последующими действиями сторон, сведения от оператора связи, данные о принадлежности номера телефона, материалы нотариального осмотра устройства. Такой подход в целом логичен, однако он не оформлен в виде нормы, а потому остается подвижным.

Переписка в мессенджерах стала одним из наиболее распространенных видов электронных доказательств. Гражданский оборот широко использует Telegram, WhatsApp и иные сервисы

для согласования условий поставки, сроков исполнения, объема работ, передачи претензий, направления уведомлений, подтверждения приемки. При этом мессенджерная коммуникация не обеспечена единым режимом доказательственного признания. Если договор прямо предусматривает обмен сообщениями через конкретный номер телефона или аккаунт, вероятность принятия таких материалов возрастает. Если подобного условия нет, суд оценивает совокупность признаков. Значение приобретают данные о владельце номера, содержание самой переписки, корреляция с банковскими операциями, логика поведения сторон после отправки сообщения.

Судебная практика осторожно относится к скриншотам переписки. Основание очевидно: изображение экрана легко модифицируется. Возможны редактирование текста, изменение имени контакта, удаление отдельных сообщений, монтаж фрагментов диалога, использование графических редакторов, генерация интерфейса сторонними программами. Даже при отсутствии злонамеренного искажения скриншот фиксирует лишь внешний вид приложения, а не исходные технические данные [5]. Для повышения доказательственной ценности обычно требуется нотариальный протокол осмотра устройства либо сайта, представление самого устройства, выгрузка чата, экспертное исследование файла или подтверждение переписки другой стороной.

Нотариальная фиксация электронных доказательств стала востребованным способом их предварительного обеспечения. Нотариус способен удостоверить факт нахождения определенной информации на экране устройства или на интернет-странице в конкретное время. Этот инструмент имеет высокую практическую ценность, особенно при угрозе быстрого удаления данных. Однако возможности нотариального осмотра ограничены предметом нотариального действия. Нотариус фиксирует доступное восприятию содержание, но не проводит криминалистическую проверку файла, не исследует механизмы его создания и не гарантирует отсутствия предшествующей подделки. Из этого следует, что нотариальный протокол повышает доказательственную устойчивость, но не заменяет собой анализ подлинности.

Электронная почта занимает промежуточное положение между формализованным и неформализованным способом коммуникации. Переписка с корпоративных адресов, прямо указанных в договоре или размещенных на официальном сайте организации, воспринимается судами как более надежная. Связь адреса с субъектом права в такой ситуации прослеживается через организационную структуру и деловые обычаи. Личные почтовые ящики требуют более

строгой проверки. Возникает вопрос, кому принадлежал доступ к учетной записи, из какого устройства и из какой точки осуществлялся вход, не было ли подмены отправителя через настройки клиента или через сторонний сервер.

Сама по себе распечатка электронной почты редко решает задачу подтверждения авторства. Значение имеют технические заголовки письма, маршрут передачи, доменное имя, SMTP-данные, серверные отметки времени, криптографические механизмы подписи, наличие цепочки предшествующих сообщений. Полноценная оценка таких сведений требует специальных знаний. Отсюда возникает потребность в процессуально оформленной компьютерно-технической экспертизе либо в участии специалиста при исследовании доказательства. Без этого электронная почта нередко оценивается по косвенным признакам, что снижает предсказуемость результата [6].

Сложности усиливаются в отношении данных, размещенных в сети Интернет. Информация на сайте может быть изменена или удалена в любой момент. Использование веб-страницы как доказательства требует ответа на несколько вопросов: кому принадлежит домен, кто контролирует размещение контента, существовала ли страница в указанном виде на определенную дату, каков был URL-адрес, отображалась ли страница публично, не использовались ли кэшированные копии или локальные версии. Скриншот сайта без указания адреса, даты и способа фиксации обычно обладает низкой доказательственной ценностью. Более убедительным способом считается нотариальный осмотр либо фиксация с применением программных средств, сохраняющих метаданные, код страницы и сетевые параметры доступа.

Отдельная категория — данные, автоматически создаваемые информационными системами. В спорах о банковских операциях, дистанционном обслуживании, доступе к личным кабинетам, использованию облачных сервисов и корпоративных платформ именно лог-файлы, журналы авторизации и системные записи могут отражать ключевые обстоятельства. Проблема состоит в том, что такие данные формируются и хранятся системой, контролируемой одной из сторон спора. Отсюда вытекает вопрос о доверии к архитектуре системы, регламентам безопасности, разграничению прав доступа и невозможности скрытой корректировки записей. Для судов оценка подобных данных особенно трудна, поскольку требуется понимание внутренних механизмов информационной системы.

Цифровые аудио- и видеозаписи включены в перечень средств доказывания, однако это не устраняет проблемы их проверки. Современные

инструменты монтажа позволяют изменять содержание записи без явных визуальных дефектов. Нейросетевые технологии делают возможной генерацию синтетических изображений и голоса, имитирующих реальных лиц. Судебная практика уже сталкивается с ситуациями, когда визуальная убедительность файла не означает его подлинности [7]. Для оценки видеозаписи необходимы сведения о модели устройства, исходном носителе, параметрах кодека, последовательности кадров, звуковой дорожке, встроенных временных метках, наличии следов перекодирования. Анализ фотографии требует проверки EXIF-данных, признаков редактирования и условий съемки. Без экспертных процедур суду трудно перейти от восприятия к верификации.

Сформировавшаяся практика распределения бремени оспаривания электронных доказательств вызывает отдельные возражения. Нередко суд исходит из презумпции достоверности представленного цифрового материала, если противоположная сторона не доказала его фальсификацию. Такая логика в цифровой среде проблематична. Технически сложный факт подделки трудно доказать без доступа к исходному носителю, серверной инфраструктуре и специальному программному анализу. Участник процесса, не располагающий соответствующими ресурсами, оказывается в заведомо уязвимом положении. Бремя опровержения переносится на лицо, которое не создавало доказательство и не контролировало его хранение.

Процессуальный баланс требует иной модели. Сторона, ссылающаяся на электронное доказательство, должна подтвердить условия его происхождения, сохранности и представления в объеме, достаточном для проверки. При наличии конкретных возражений оппонента суд обязан решать вопрос о необходимости экспертного исследования, истребования оригинального носителя, данных от провайдера, оператора связи, владельца платформы либо администратора информационной системы. Презумпция надежности цифрового файла без анализа его технологической истории не соответствует природе такого объекта.

Причина перечисленных трудностей заключается в том, что действующее законодательство регулирует электронные доказательства фрагментарно. Нормы о подаче документов в электронном виде и о применении электронной подписи обеспечивают документооборот между участниками и судом, но не формируют полноценного режима для доказывания. Электронное правосудие в процедурной части развивается быстрее, чем доказательственное право [8]. Иск можно направить через цифровую систему, но вопрос о том, как исследовать содержание мес-

сенджера, проверить лог-файл или установить подлинность скриншота, остается вне детальной регламентации.

Постановления Пленума Верховного Суда Российской Федерации частично восполняют пробелы, однако они не создают стройной конструкции. Разъяснения касаются отдельных аспектов электронного документооборота и использования цифровых каналов связи, но не охватывают целиком проблематику электронных доказательств как самостоятельного явления. Казуистическое развитие разъяснений не может заменить законодательную модель, поскольку судья и участники процесса нуждаются в нормах, которые заранее задают стандарт собирания, представления, исследования и оценки цифровых данных.

Потребность в законодательной модернизации связана с несколькими задачами. Первая — определить процессуальную природу электронных доказательств. Вторая — закрепить требования к форме их представления. Третья — установить правила аутентификации источника и проверки целостности. Четвертая — разработать процедуры исследования таких доказательств в судебном заседании. Пятая — обеспечить баланс между технологической сложностью проверки и реальной доступностью судебной защиты [9].

Закрепление дефиниции электронных доказательств в статье 55 ГПК РФ представляется обоснованным. Под электронными доказательствами целесообразно понимать сведения об обстоятельствах, имеющих значение для дела, существующие в цифровой форме, полученные из информационных систем, сетей связи, электронных устройств, программных сред и иных цифровых источников, для восприятия и исследования которых необходимы технические средства. Такая дефиниция позволяет охватить и электронные документы, и цифровую переписку, и мультимедийные файлы, и системные журналы. Она не разрушает традиционную структуру доказательственного права, но устраняет концептуальный пробел.

Следующий шаг — установление общих требований к представлению электронных доказательств. Закон должен предусмотреть обязанность указывать источник происхождения данных, дату и способ их получения, сведения об устройстве или системе, из которой они извлечены, а также форму, в которой обеспечивается возможность проверки их целостности. Для файлов, представляемых на носителе или через информационную систему суда, требуется фиксация контрольной суммы либо иного идентификатора целостности. Для переписки — сохранение метаданных, позволяющих установить аккаунты, номера, временные отметки и структуру

диалога. Для интернет-страниц — указание URL-адреса, даты и времени доступа, способа фиксации содержимого. Для видеозаписей — представление в исходном либо максимально приближенном к исходному формату с данными о носителе и устройстве записи.

Нуждается в урегулировании вопрос о подлиннике и копии электронного доказательства. В бумажной среде эти категории относительно очевидны. В цифровой среде копия файла может быть полностью идентична оригиналу по содержанию, а различие между ними определяется не визуальным образом, а контекстом хранения и реквизитами. Закон должен исходить не из материального носителя как единственного критерия оригинальности, а из понятия первичного цифрового экземпляра и проверяемой цепочки сохранности. Если сторона представляет копию, она должна раскрыть, каким образом она получена из первоисточника, какие свойства файла сохранены и какие утрачены. При наличии спора суд должен иметь возможность потребовать исходный носитель либо доступ к системе хранения [10].

Особое значение имеет институт метаданных. В существующей практике они часто игнорируются, хотя именно метаданные нередко содержат ключ к проверке доказательства. Дата создания файла, дата изменения, автор учетной записи, геолокация, модель устройства, версия приложения, IP-адрес, идентификатор сообщения, параметры кодирования видео, серверные журналы, информация о загрузке и скачивании способны подтвердить или опровергнуть доводы стороны. Процессуальная регламентация должна прямо указывать, что метаданные являются частью электронного доказательства и подлежат исследованию вместе с основным содержанием.

Требует закрепления и механизм участия специалиста. Судья не обязан обладать специальными познаниями в области цифровой криминалистики, сетевых протоколов, мобильных приложений, программной архитектуры или методов выявления монтажа. В делах, где свойства электронного доказательства имеют решающее значение, участие специалиста при осмотре, воспроизведении и первичной оценке цифрового объекта должно стать обычной процессуальной практикой. Экспертиза необходима не во всех случаях, однако закон может предусмотреть более гибкий инструмент консультационного сопровождения исследования сложных цифровых материалов в заседании.

Перспективным направлением выступает разработка специальных протоколов судебного осмотра электронных доказательств. Общие правила осмотра не учитывают специфику цифровой среды. Между тем осмотр мобильного телефона,

облачного хранилища, мессенджера, веб-страницы или видеозаписи требует фиксирования последовательности действий, интерфейса, адресов, технических параметров, времени доступа, используемого программного обеспечения, устройства вывода, контрольной суммы извлекаемого файла. Процессуальный протокол должен сохранять не только результат восприятия, но и способ доступа к информации.

Еще одна перспектива связана с созданием унифицированных технических требований для информационных систем судов. Если электронные доказательства подаются через государственные цифровые платформы, такие платформы должны обеспечивать прием файлов в форматах, сохраняющих метаданные, автоматическое вычисление контрольных сумм, фиксацию времени загрузки и невозможность незаметной подмены. Судебная цифровая инфраструктура должна не просто принимать файл как вложение, а поддерживать минимальный стандарт доказательственной сохранности.

Не менее значима проблема персональных данных и коммерческой тайны. Электронные доказательства часто содержат массив сведений, выходящих за пределы предмета спора: историю переписки, контакты, файлы сторонних лиц, данные о местоположении, медицинскую либо финансовую информацию. Законодательная модернизация не может ограничиться вопросом допустимости; она должна установить правила процессуальной селекции и защиты таких данных. Возможны режимы представления обезличенных копий, частичного доступа, закрытого судебного исследования, использования специальных технических средств маскирования нерелевантной информации при сохранении проверяемости доказательства.

Реформа должна учитывать различие между гражданским и арбитражным процессом, но единые базовые принципы для электронных доказательств необходимы во всех процессуальных формах. Гражданский процесс особенно чувствителен к проблеме доступа к техническим ресурсам. Физические лица чаще располагают ограниченными возможностями по получению данных от операторов связи, провайдеров и владельцев цифровых платформ. Из этого следует обязанность суда активнее использовать инструменты содействия доказыванию при наличии обоснованного ходатайства стороны. Истребование цифровых следов у третьих лиц, обеспечение доказательств до их удаления, назначение экспертизы по вопросам целостности и авторства становятся средствами выравнивания процессуальных возможностей.

Вопрос о международном опыте также имеет практическое значение. Зарубежные пра-

вопорядки в различной степени закрепляют категории электронные доказательства, цифровые улики, информация, хранящаяся в электронном виде. Для них характерны три устойчивых элемента: признание цифровой информации самостоятельным объектом доказательственного регулирования, внимание к цепочке сохранности и наличие процедур раскрытия электронных данных. Российская модель не может быть механически скопирована с иностранной, однако заимствование структурных решений представляется продуктивным. Прежде всего речь идет о формализации требований к аутентичности и к документированию способов получения цифровой информации [11].

Реалистичный подход к перспективам правового регулирования требует отказа от идеи абсолютной технической достоверности. Любое доказательство оценивается в совокупности с другими материалами дела. Электронные данные не нуждаются в недостижимом стандарте безусловной истины. Требуется иной результат: создание процедур, при которых вероятность ошибочной оценки существенно снижается, а спор о надежности доказательства переводится из сферы интуитивного усмотрения в сферу проверяемых критериев. В цифровой среде это достигается через регламентацию источника, способа фиксации, метаданных, целостности, цепочки хранения и процессуального исследования.

Развитие технологий делает проблему срочной. Объем коммуникации в мессенджерах растет, электронная подпись применяется шире, камеры наблюдения и мобильные устройства непрерывно создают цифровой след, информационные системы фиксируют действия пользователей автоматически. Параллельно увеличиваются и риски: подмена идентификаторов, доступ к чужим аккаунтам, автоматическое редактирование файлов, использование облачных сервисов с неопределенной юрисдикцией хранения. Если доказательственное право не адаптируется к этим условиям, судебная практика будет все чаще сталкиваться с ситуацией, когда технически значимая информация существует, но не может быть убедительно легализована в процессе.

Поэтому модернизация не должна ограничиваться точечными поправками. Необходима связанная модель, включающая дефиницию электронных доказательств, общие требования к их представлению, правила исследования и оценки, положения о метаданных, критерии аутентификации, регламентацию участия специалиста и особенности судебного осмотра цифровых объектов. Такая модель обеспечит предсказуемость для участников процесса и сократит зависимость судебной оценки от ситуативных подходов.

В итоге проблемы правового регулирования электронных доказательств в российском гражданском процессе сводятся к трем ключевым узлам. Первый состоит в отсутствии прямого законодательного признания электронных доказательств как самостоятельной категории. Второй выражается в недостаточной регламентации допустимости и достоверности цифровых данных, включая идентификацию источника, проверку неизменности и определение формы представления. Третий проявляется в неравномерности судебной практики, которая восполняет законодательные пробелы фрагментарными критериями. Перспективы развития связаны с системным обновлением ГПК РФ, переходом к технологически нейтральным, но процессуально точным правилам и формированием стандартов судебной работы с цифровой информацией. Только при таких условиях электронные доказательства смогут выполнять свою доказательственную функцию без снижения гарантий справедливого судебного разбирательства.

Список литературы:

- [1] Мироедова О.В. Использование электронных документов в уголовном, гражданском и административном судопроизводстве // Холодная наука. 2025. №23, С. 57-65
- [2] Заиграева, В. И. Электронный документ как электронное доказательство в гражданском судопроизводстве / В. И. Заиграева // Современные проблемы теории и практики права глазами молодых исследователей: материалы XIV Всероссийской молодежной научно-практической конференции, Улан-Удэ, 26–27 марта 2020 года. – Улан-Удэ: Восточно-Сибирский государственный университет технологий и управления, 2020. – С. 18-22.
- [3] Боннер, А. Т. Административное судопроизводство в Российской Федерации: миф или реальность, или Спор процессуалиста с административистом / А. Т. Боннер // Закон. – 2016. – № 7. – С. 24-51.
- [4] Морозов, А. А. Теория и практика толкования понятия и содержания юридической ответственности за экологические правонарушения / А. А. Морозов // Образование и право. – 2025. – № 3. – С. 197-201.
- [5] Морозов, А. А. Правовая культура и экологическое право: формирование ответственного поведения граждан в условиях экологических кризисов / А. А. Морозов // Актуальные проблемы науки и практики: Гатчинские чтения – 2025: материалы XII международной научно-практической конференции, Гатчина, 29–30 мая 2025 года. – Гатчина: Гатчинский государственный университет, 2025. – С. 73-76.

[6] Морозов, А. А. Медиация при урегулировании споров в сфере строительства / А. А. Морозов // Примирительные процедуры в гражданском праве и судопроизводстве: Сборник материалов Международной научно-практической конференции, Санкт-Петербург, 26–27 апреля 2019 года / Под общей редакцией В.П. Очередыко, А.Н. Кузбагарова, С.Ю. Катуковой. Том Часть 2. – Санкт-Петербург: Центр научно-информационных технологий «Астерион», 2019. – С. 135-138.

[7] Морозов, А. А. Правовая характеристика товарищества собственников жилья как формы управления многоквартирным домом / А. А. Морозов // Актуальные проблемы юридической науки и практики: Гатчинские чтения-2018: Сборник научных трудов по материалам Международной научно-практической конференции, Гатчина, 25 мая 2018 года. Том 1. – Гатчина: Государственный институт экономики, финансов, права и технологий, 2018. – С. 176-178.

[8] Морозов, А. А. Гражданско-правовое регулирование механизма защиты прав предпринимателей в саморегулируемых организациях в сфере строительства / А. А. Морозов // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. – 2013. – № 11-2(37). – С. 120-122.

[9] Морозов, А. А. Теория и практика реализации прав собственников в многоквартирном доме на проведение перепланировки и переустройства жилого помещения / А. А. Морозов // Теория и практика применения и толкования в частном праве: Сборник научных статей по материалам Международной научно-практической конференции, Санкт-Петербург, 15–16 ноября 2024 года. – Санкт-Петербург: ООО Центр научно-информационных технологий «Астерион», 2025. – С. 15-18.

[10] Боннер А.Т. Традиционные и нетрадиционные средства доказывания в гражданском и арбитражном процессе. – М.: Проспект, 2017. – 304 с.

[11] Афанасьев С.Ф., Зайцев А.И. Электронный гражданский процесс: современное состояние и перспективы развития // Российский судья. – 2022. – № 3. – С. 22-26.

References:

- [1] O.V. Miroedova. Use of electronic documents in criminal, civil and administrative proceedings//Cold Science. 2025. NO. 23, P. 57-65
- [2] Zaigraeva, V.I. Electronic document as electronic evidence in civil proceedings/V.I. Zaigraeva// Modern problems of the theory and practice of law through the eyes of young researchers: materials of

the XIV All-Russian Youth Scientific and Practical Conference, Ulan-Ude, March 26-27, 2020. - Ulan-Ude: East Siberian State University of Technology and Management, 2020. - S. 18-22.

[3] Bonner, A. T. Administrative proceedings in the Russian Federation: myth or reality, or Dispute between a proceduralist and an administrator/A. T. Bonner//Law. – 2016. – № 7. - S. 24-51.

[4] Morozov, A. A. Theory and practice of interpretation of the concept and content of legal responsibility for environmental offenses/A. A. Morozov//Education and law. – 2025. – № 3. - S. 197-201.

[5] Morozov, A. A. Legal culture and environmental law: the formation of responsible behavior of citizens in environmental crises/A. A. Morozov//Actual problems of science and practice: Gatchina readings - 2025: materials of the XII International Scientific and Practical Conference, Gatchina, May 29-30, 2025. - Gatchina: Gatchina State University, 2025. - S. 73-76.

[6] Morozov, A. A. Mediation in the settlement of disputes in the field of construction/A. A. Morozov//Conciliation procedures in civil law and legal proceedings: Collection of materials of the International Scientific and Practical Conference, St. Petersburg, April 26-27, 2019/Edited by V. P. Zavetko, A. N. Kuzbagarova, S. Yu. Katukova. Volume Part 2. - St. Petersburg: Center for Scientific and Information Technologies "Asterion," 2019. - S. 135-138.

[7] Morozov, A. A. Legal characteristics of a homeowners' association as a form of management

of an apartment building/A. A. Morozov//Actual problems of legal science and practice: Gatchina readings-2018: Collection of scientific works based on materials from the International Scientific and Practical Conference, Gatchina, May 25, 2018. Volume 1. - Gatchina: State Institute of Economics, Finance, Law and Technology, 2018. - S. 176-178.

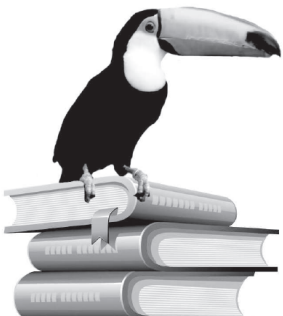
[8] Morozov, A. A. Civil regulation of the mechanism for protecting the rights of entrepreneurs in self-regulatory organizations in the field of construction/A. A. Morozov//Historical, philosophical, political and legal sciences, cultural studies and art history. Questions of theory and practice. – 2013. – № 11-2(37). - S. 120-122.

[9] Morozov, A. A. Theory and practice of exercising the rights of owners in an apartment building to carry out redevelopment and reconstruction of residential premises/A. A. Morozov//Theory and practice of application and interpretation in private law: Collection of scientific articles based on the materials of the International Scientific and Practical Conference, St. Petersburg, November 15-16, 2024. - St. Petersburg: Center for Scientific and Information Technologies Asterion LLC, 2025. - S. 15-18.

[10] Bonner A.T. Traditional and non-traditional means of proof in civil and arbitration proceedings. - M.: Prospect, 2017. - 304 s.

[11] Afanasyev S.F., Zaitsev A.I. Electronic civil process: current state and development prospects//Russian judge. – 2022. – № 3. - S. 22-26.





ЮРКОМПАНИ

www.law-books.ru

Юридическое издательство
«ЮРКОМПАНИ»

Издание учебников,
учебных и методических
пособий, монографий,
научных статей.

Профессионально.

В максимально
короткие сроки.

Размещаем
в РИНЦ, E-Library.