

Дата поступления рукописи в редакцию: 22.05.2026 г.

DOI: 10.24412/2076-1503-2026-7-806-809

Дата принятия рукописи в печать: 03.08.2026 г.

БЕЗЗАТЕЕВА Вероника Сергеевна,

*старший преподаватель кафедры гражданского права и кафедры информационной безопасности
Санкт-Петербургский государственный университет аэрокосмического приборостроения,*

e-mail: bezzateeva@inbox.ru

ПРОЦЕССУАЛЬНАЯ ДОСТОВЕРНОСТЬ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ В РИСК-ОРИЕНТИРОВАННОЙ МОДЕЛИ ЗАКРЕПЛЕНИЯ И ОЦЕНКИ

Аннотация. В статье рассматривается проблема процессуальной достоверности цифровых доказательств в российском судопроизводстве. Актуальность исследования обусловлена тем, что электронная переписка, скриншоты, сведения из государственных информационных систем, аудио- и видеозаписи, журналы событий и иные цифровые следы активно используются в доказывании, однако законодательство не содержит единой дефиниции цифрового доказательства и единых критериев проверки его происхождения, целостности и воспроизводимости. Предлагается применять «цифровой паспорт доказательства», позволяющий фиксировать источник, способ получения, метаданные, хеш-значение, условия хранения и проверочные действия. Делается вывод о необходимости сочетания законодательных стандартов, дополнительных разъяснений Верховного Суда Российской Федерации и локальных регламентов работы с цифровыми материалами.

Ключевые слова: цифровые доказательства; электронные доказательства; процессуальная достоверность; электронная подпись; скриншот; метаданные; искусственный интеллект.

BEZZATEEVA Veronika Sergeevna,

Senior Lecturer of the Department of Civil Law, Saint-Petersburg State University of Aeronautical Instrumentation

PROCESSUAL VALIDITY OF DIGITAL EVIDENCE IN A RISK-ORIENTED MODEL OF CONSOLIDATION AND EVALUATION

Annotation. The article discusses the problem of procedural reliability of digital evidence in Russian legal proceedings. The relevance of the study is due to the fact that electronic correspondence, screenshots, information from state information systems, audio and video recordings, event logs, and other digital traces are actively used in proof, but the legislation does not contain a unified definition of digital evidence and unified criteria for checking its origin, integrity, and reproducibility. It is proposed to use a "digital evidence passport" that allows to record the source, method of obtaining, metadata, hash value, storage conditions, and verification actions. The article concludes that it is necessary to combine legislative standards, additional clarifications by the Supreme Court of the Russian Federation, and local regulations for working with digital materials.

Key words: digital evidence; electronic evidence; procedural reliability; electronic signature; screenshot; metadata; artificial intelligence.

В современных условиях цифровизация правосудия перестала быть только техническим направлением судебной деятельности. Она изменила само содержание доказывания, поскольку значительная часть юридически значимых фактов фиксируется не в бумажном документе, а в электронной информационной среде. Доказательственное значение

приобретают сообщения электронной почты и мессенджеров, сведения из личных кабинетов, данные государственных информационных систем, журналы доступа, аудио- и видеозаписи. Действующее законодательство Российской Федерации допускает цифровую форму фиксации информации. Статьи 71 ГПК РФ и 70 КАС РФ называют документы и материалы в форме цифровой, графической записи, полученные

посредством электронной связи или сети Интернет. Статья 75 АПК РФ использует более лаконичную формулу об иных документах в форме цифровой, графической записи или иным способом, позволяющим установить достоверность документа. УПК РФ предусматривает электронные документы в судебном производстве, а электронные носители информации регулирует через правила о вещественных доказательствах, изъятии, копировании и хранении. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» устанавливает виды электронной подписи, но не охватывает массив неподписанных цифровых следов.

В результате сформировался нормативный разрыв: цифровые доказательства фактически применяются, однако единая процессуальная модель их проверки пока отсутствует. [1, 2] Это снижает предсказуемость судебной оценки, осложняет распределение бремени доказывания при возражениях о фальсификации и требует разработки единых критериев исследования цифровых объектов.

Методология исследования

Исследование основано на общенаучных и специальных юридических методах познания. Диалектический метод позволил рассмотреть цифровое доказательство как динамично развивающееся явление, находящееся на пересечении процессуального права, информационного права, технической фиксации данных и судебной экспертологии. Системный метод использовался для анализа цифровых доказательств во взаимосвязи с правилами допустимости, относимости, достоверности и достаточности доказательств, а также с институтами электронной подписи, нотариального обеспечения доказательств, судебной экспертизы и защиты от фальсификации. Сравнительно-правовой метод позволил сопоставить традиционные правила исследования письменных и вещественных доказательств с особенностями цифровых объектов, которые могут быть изменены, скопированы, удалены или воспроизведены в иной технической среде. Риск-ориентированный метод позволил дифференцировать объем проверочных действий в зависимости от вероятности искажения, монтажа, утраты контекста или синтетической генерации цифрового материала.

Основными целями исследования являются:

Целью настоящего исследования является разработка риск-ориентированной процессуальной модели закрепления и оценки цифровых доказательств, обеспечивающей проверку их происхождения, целостности,

принадлежности и воспроизводимости без необоснованного усложнения доступа к правосудию.

Актуальность разработки риск-ориентированной модели обусловлена рядом нерешенных теоретико-прикладных вопросов правового режима цифровых доказательств. Прежде всего, в действующем процессуальном законодательстве отсутствует единое понятие цифрового доказательства, что затрудняет формирование унифицированных критериев его допустимости, относимости и достоверности. Используемая законодателем формула о «документах и материалах, выполненных в форме цифровой записи» позволяет включать электронные сведения в доказательственный материал, однако не раскрывает их технологической и процессуальной специфики. Между тем цифровой объект отличается повышенной воспроизводимостью и изменчивостью: он может быть скопирован, преобразован, перемещен в иную информационную среду, представлен суду в виде файла, распечатки, скриншота либо иного производного отображения. В связи с этим цифровое доказательство целесообразно рассматривать не как изолированный информационный объект, а как совокупность взаимосвязанных элементов, включающих содержание сведений, источник их происхождения, техническую среду формирования, способ фиксации и доступные механизмы последующей проверки. Такой подход позволяет оценивать не только смысловое содержание представленного материала, но и условия его создания, сохранения, передачи и воспроизведения.

Особую сложность представляет судебная оценка скриншотов, электронной переписки и сообщений в мессенджерах, поскольку данные материалы нередко выступают производной формой фиксации первоначального цифрового следа. В судебной практике они могут признаваться доказательствами при наличии даты, времени, адреса интернет-страницы, сведений об отправителе, номере телефона, аккаунта или иных идентифицирующих признаках. Вместе с тем при невозможности установить принадлежность учетной записи, номера телефона или электронного адреса конкретному лицу такие доказательства нередко оцениваются критически либо исключаются из числа убедительных подтверждений юридически значимых обстоятельств. Подобный подход является процессуально оправданным, поскольку направлен на предотвращение фальсификаций, однако одновременно он свидетельствует об отсутствии единых стандартов аутентификации цифровых материалов и снижает предсказуемость

судебной защиты. В научной литературе справедливо подчеркивается, что идентификация источника, подтверждение достоверности и минимизация риска фальсификации относятся к числу ключевых проблем цифрового доказывания. [3]

Дополнительное значение указанная проблема приобретает в условиях развития технологий искусственного интеллекта. Генеративные модели позволяют создавать реалистичные изображения, тексты, аудио- и видеозаписи, которые внешне могут восприниматься как достоверное отражение действительности. В результате традиционная ориентация на формальное представление файла, распечатки или визуального отображения цифрового объекта уже не обеспечивает достаточного уровня процессуальной надежности. Проверка цифрового доказательства должна включать анализ его происхождения, целостности, условий хранения, признаков изменения, а при необходимости - возможность экспертной или специальной технической проверки. Следовательно, современное процессуальное право нуждается в переходе от формального признания цифровых материалов к воспроизводимой модели их закрепления и оценки, позволяющей проследить цепочку возникновения, фиксации, хранения и представления цифрового объекта в суде.

Исходная идея риск-ориентированной модели состоит в том, что разные цифровые доказательства имеют различный уровень уязвимости. Электронный документ с усиленной квалифицированной электронной подписью, скриншот из мессенджера без указания номера телефона и видеозапись, по которой заявлено возражение о возможном дипфейке, не должны проверяться одинаково. Суд оценивает не только вид доказательства, но и риск его искажения. Практическим инструментом может стать «цифровой паспорт доказательства», то есть приложение к ходатайству о приобщении материала или часть протокола осмотра. В него включаются: источник цифровых сведений; лицо, выполнившее фиксацию; дата, время и часовой пояс; устройство и программная среда; формат файла; метаданные; хеш-значение либо отметка о невозможности его получения; способ хранения; сведения об электронной подписи, отметке времени, нотариальном обеспечении или экспертной проверке.

Значение паспорта состоит не в усложнении доступа к правосудию, а в обеспечении проверяемости. Для скриншота сайта достаточно указать адрес страницы, дату и время фиксации, сведения о лице, выполнившем фиксацию, и

приложить распечатку либо электронный файл. Для переписки требуется раскрыть признаки принадлежности аккаунта стороне спора: договорное указание адреса, историю общения, сведения оператора связи, данные личного кабинета или иные подтверждения. Для аудио- и видеозаписи важны сведения о первичном устройстве записи, признаках монтажа и необходимости привлечения специалиста либо назначения экспертизы.

Уровень риска может быть низким, средним или высоким. Низкий риск характерен для данных государственных информационных систем и документов с проверяемой электронной подписью; средний - для скриншотов, переписки и личных кабинетов; высокий - при заявлении о фальсификации, признаках монтажа, неустановленной принадлежности аккаунта или вероятности синтетической генерации. При высоком риске требуются специальные знания: консультация специалиста, экспертное исследование или судебная экспертиза. [4]

Предлагаемая модель позволяет согласовать процессуальную экономию и необходимость достоверного судебного познания. В делах с низким уровнем риска суд может ограничиться проверкой электронных реквизитов, полномочий источника и формальной целостности документа. В делах со средним уровнем риска необходимо исследовать контекст получения цифрового объекта, принадлежность аккаунта или устройства, последовательность переписки, метаданные и возможные альтернативные источники подтверждения. В делах с высоким уровнем риска проверочные действия должны включать специальные знания, сопоставление оригинала и копий, анализ признаков монтажа, проверку хеш-значения и оценку возможности синтетической генерации.

Совершенствование регулирования может начинаться с закрепления в ГПК РФ, АПК РФ и КАС РФ общего определения цифрового доказательства как сведений об обстоятельствах дела, созданных, обработанных, переданных или сохраненных в электронной форме, достоверность которых проверяется через анализ источника, способа фиксации, целостности данных, метаданных, электронной подписи, журналов событий, заключения специалиста, экспертизы или иных средств. Такая дефиниция не отменяет действующие виды доказательств, но формирует единый стандарт исследования.

Во-вторых, необходимо установить минимальные реквизиты представления цифрового доказательства: источник, дату и способ фиксации, лицо, форму представления, а для файлов - формат, объем, хеш-значение и

сведения о носителе. Нотариальное обеспечение должно оставаться надежным способом фиксации, но не универсальным условием допустимости, иначе защита граждан, работников, потребителей и малых организаций будет осложнена.

В-третьих, следует развить разъяснения Верховного Суда Российской Федерации о правилах исследования цифровых доказательств: когда отсутствие нотариального удостоверения не препятствует оценке материала, какие признаки должен содержать скриншот, как проверять принадлежность аккаунта и как распределять бремя доказывания при заявлении о фальсификации цифрового объекта.

В-четвертых, организациям, регулярно представляющим цифровые материалы в суд, целесообразно утверждать локальные регламенты фиксации и хранения цифровых доказательств. Такие регламенты должны предусматривать порядок создания копий, сохранения метаданных, расчета хеш-значений, ограничения доступа к файлам, ведения журналов действий и оформления пояснений к цифровым объектам. Это особенно важно для банков, операторов электронных площадок, образовательных организаций, работодателей и иных субъектов, у которых значительная часть доказательственной информации возникает в электронных системах.

Цифровые доказательства стали обычным элементом судебного доказывания, однако их процессуальный режим остается недостаточно определенным. Законодательство допускает документы и материалы в цифровой форме, а также электронные документы в отдельных процессуальных режимах, но не устанавливает единой модели проверки происхождения, целостности, воспроизводимости и принадлежности цифровых данных. Поэтому судебная практика вырабатывает подходы по отдельным категориям споров, что приводит к различиям в оценке сходных материалов.

Предложенная риск-ориентированная модель позволяет избежать как общего недоверия к цифровым доказательствам, так и их некритического принятия. Центральным

элементом модели является цифровой паспорт доказательства, обеспечивающий прозрачность источника, способа фиксации, метаданных, хеш-значения, условий хранения и проверочных действий. Минимальные требования, развитие разъяснений Верховного Суда Российской Федерации и локальные регламенты позволят повысить предсказуемость оценки доказательств, снизить риск фальсификаций и сохранить баланс между доступностью правосудия и достоверностью судебного познания.

Список литературы:

- [1] Казиханова С. С. Электронные доказательства в теории судебных доказательств // Digital Law Journal. - 2024. - Т. 5. - № 4. - С. 79–95.
- [2] Костенко Р. В. Допустимость доказательств в цифровую эпоху: трансформация процессуальных стандартов // Юридический вестник Кубанского государственного университета. - 2025. - № 1. - С. 30–35.
- [3] Ковалева Н. В., Жук А. П. Допустимость электронных доказательств в гражданском процессе // Диалог. - 2025. - № 2. - С. 66–68.
- [4] Староверова О. В. Зарубежный опыт правового регулирования представления (цифровых) электронных доказательств в гражданском процессе // Вестник экономической безопасности. - 2025. - № 5. - С. 113–117.

References:

- [1] Kazikhanova S. S. Electronic evidence in the theory of forensic evidence//Digital Law Journal. - 2024. - VOL. 5. - № 4. - S. 79-95.
- [2] Kostenko R.V. Admissibility of evidence in the digital age: transformation of procedural standards//Legal Bulletin of Kuban State University. - 2025. - № 1. - S. 30-35.
- [3] Kovaleva N.V., Zhuk A.P. Admissibility of electronic evidence in civil proceedings//Dialogue. - 2025. - № 2. - S. 66-68.
- [4] Staroverova O. V. Foreign experience in legal regulation of the presentation of (digital) electronic evidence in civil proceedings//Bulletin of Economic Security. - 2025. - № 5. - S. 113-117.

