Дата поступления рукописи в редакцию: 04.10.2026 г. DOI: 10.24412/2224-9133-2026-10-202-207
Дата принятия рукописи в печать: 10.11.2026 г.

ЭЛЬМУРЗАЕВ Асолтан Валерьевич,
Соавтор, кандидат юридических наук, доцент, 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: elmurzaev.78@mail.ru

ГУНЬКО Елизавета Владимировна,
Научный исследователь, Санкт-Петербургский университет Государственной противопожарной службы МЧС России им. Героя Российской Федерации генерала армии Е. Н. Зиничева,
e-mail: gunkoliza@list.ru

ЭЛЕКТРОННЫЕ ДОКАЗАТЕЛЬСТВА В РОССИЙСКОМ СУДОПРОИЗВОДСТВЕ: ПРАВОВАЯ ПРИРОДА, ДОПУСТИМОСТЬ И ОЦЕНКА

Аннотация. *В статье рассматривается, как электронные доказательства используются в российском судопроизводстве и какие вопросы возникают при их представлении и оценке. На материале норм гражданского, арбитражного и уголовного процесса анализируются электронные документы, переписка, аудио- и видеозаписи, интернет-публикации и данные цифровых носителей. Особое внимание уделяется установлению источника информации, проверке её целостности, идентификации автора и законности получения. Обосновывается позиция, согласно которой цифровая форма сама по себе не должна вести ни к автоматическому отказу в принятии материала, ни к признанию его достоверным. Сформулированы практические рекомендации по проверке электронных доказательств и возможным направлениям развития процессуального регулирования.*

Ключевые слова: *электронные доказательства, цифровые доказательства, электронный документ, допустимость доказательств, достоверность, электронная подпись, судебное доказывание, цифровая информация.*

Для цитирования: *Эльмурзаев А. В., Гунько Е. В. Электронные доказательства в российском судопроизводстве: правовая природа, допустимость и оценка // Право и управление. 2026. № 10. С. 202–207.*

ELMURZAEV Asoltan Valerievich,
Co-author, candidate of legal sciences, associate professor, associate professor of the department of administrative law and process of St. Petersburg University of the State Fire Service of the Ministry of Emergencies of Russia named after Hero of the Russian Federation, Army General E. N. Zinichev

GUNKO Elizaveta Vladimirovna,
Scientific researcher, St. Petersburg University of the State Fire Service EMERCOM of Russia named after Hero of the Russian Federation, Army General E. N. Zinichev

ELECTRONIC EVIDENCE IN RUSSIAN JUDICIAL PROCEEDINGS: LEGAL NATURE, ADMISSIBILITY AND ASSESSMENT

Annotation. *This article considers the use of electronic evidence in Russian judicial proceedings and the issues that arise when such evidence is submitted and assessed. It examines civil, commercial and criminal procedural rules concerning electronic documents, correspondence, audio and video recordings, online publications and data stored on digital media. Particular attention is paid to identifying the source of information, checking its integrity, determining authorship and establishing whether the data were obtained lawfully. The article argues that the digital format alone should neither justify automatic exclusion nor establish reliability. It offers practical recommendations for verifying electronic evidence and outlines possible ways to improve procedural regulation.*

Key words: *electronic evidence, digital evidence, electronic document, admissibility of evidence, reliability, electronic signature, judicial proof, digital information.*

For citation: *Elmurzaev A. V., Gunko E. V. Electronic evidence in russian judicial proceedings: legal nature, admissibility and assessment. Law and administration. 2026;(10):202–207. (In Russ.).*

Введение

Цифровые технологии изменили не только повседневное общение, но и способы фиксации юридически значимых событий. Сегодня договор можно заключить на онлайн-платформе, деловые вопросы обсудить по электронной почте или в мессенджере, а действия пользователя — отразить в журнале информационной системы. Обстоятельства дела также могут фиксироваться на фото, аудио- и видеозаписях, в метаданных и истории операций. Поэтому в суд всё чаще представляют сведения, которые изначально возникли и сохранились в цифровой среде. Работа с такими материалами требует особого внимания. В отличие от бумажного документа, цифровой файл легко скопировать, а некоторые его свойства — изменить. Метаданные зависят от устройства и программ, с помощью которых файл создан или обработан. Распечатка сообщения либо снимок экрана показывают часть содержания, но не всегда позволяют определить автора, точное время создания, полноту переписки или наличие изменений. Следовательно, важно не только решить, можно ли использовать электронные сведения в качестве доказательства, но и обеспечить возможность проверить их происхождение и надёжность.

Цель исследования — определить особенности правового режима электронных доказательств в российском судопроизводстве и предложить меры, которые помогут повысить достоверность и проверяемость цифровых материалов. Для этого используются формально-юридический, системный и сравнительно-правовой методы, а также анализ действующих процессуальных норм. Исследование носит преимущественно нормативно-аналитический характер. Поэтому его выводы не следует рассматривать как замену самостоятельному анализу судебных решений по отдельным категориям дел.

1. Понятие и правовая природа электронных доказательств

Российское процессуальное законодательство не содержит единого определения «электронного доказательства», которое одинаково применялось бы во всех видах судопроизводства. При этом цифровые сведения могут использоваться в рамках уже известных процессуальных категорий: письменных и иных документов, вещественных доказательств, аудио- и видеозаписей. Так, статья 71 ГПК РФ допускает письменные доказательства в форме цифровой или графической записи, в том числе документы, полученные по электронной связи и через Интернет [1]. Сходный подход закреплён в статье 75 АПК РФ [2].

В уголовном процессе статья 74 УПК РФ называет среди видов доказательств вещественные доказательства, протоколы следственных и судебных действий и иные документы [3]. В зависимости от содержания и способа процессуального закрепления цифровые данные могут относиться к разным категориям. Например, файл может рассматриваться как документ, устройство хранения — как вещественное доказательство, а результаты осмотра телефона или компьютера — фиксироваться в протоколе следственного действия. Поэтому юридическая квалификация зависит не только от расширения файла или типа носителя, но и от того, каким образом сведения получены и представлены в дело.

В рамках настоящего исследования электронные доказательства понимаются как сведения о значимых для дела обстоятельствах, которые созданы, переданы, обработаны или сохранены с помощью цифровых технологий и представлены в установленной законом форме, позволяющей проверить содержание, происхождение и целостность этих сведений. В таком рабочем

определении важны три составляющие: сами данные, их существование в цифровой среде и возможность процессуальной проверки. Электронный документ и электронное доказательство — не одно и то же. Электронный документ представляет собой документированную информацию в цифровой форме, которую можно воспринимать с помощью технических средств. Электронное доказательство — более широкое понятие. Значение для дела могут иметь не только документы, но и записи камер наблюдения, переписка, журналы доступа, данные о местоположении, сведения о транзакциях и технические характеристики файлов. В зависимости от ситуации один объект может быть приобщён и исследован как письменное доказательство, иной документ, вещественное доказательство или приложение к протоколу. Отдельный вопрос связан с электронной подписью. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» устанавливает условия её использования и случаи, когда электронный документ признаётся равнозначным бумажному документу [4]. Подпись может помогать установить подписанта и проверить целостность документа в пределах конкретного вида подписи и применяемой системы. Однако она не подтверждает автоматически истинность всех изложенных в документе фактов. И наоборот, отсутствие квалифицированной электронной подписи не означает, что электронная переписка всегда лишена доказательственного значения: необходимо учитывать закон, характер отношений сторон и другие подтверждающие материалы.

2. Нормативное регулирование электронных доказательств

Правила работы с электронными доказательствами складываются из нескольких групп нормативных актов. Процессуальные кодексы определяют виды доказательств, порядок их представления и исследования. Законодательство об информации и электронной подписи регулирует отдельные вопросы создания, передачи, хранения и подтверждения электронных документов. При этом цифровые материалы не выделены в единую самостоятельную категорию с одинаковым правовым режимом для всех видов судопроизводства. В гражданском процессе статья 55 ГПК РФ определяет доказательства и предусматривает, что сведения, полученные с нарушением закона, не имеют юридической силы [1]. Статья 71 ГПК РФ допускает документы, полученные с помощью электронной связи и Интернета, а также материалы, выполненные способом, позволяющим установить их достоверность. В арбитражном процессе статья 75 АПК РФ прямо упоминает документы и цифровые записи, полученные посредством электронной или иной связи, включая Интернет [2]. Эти положения позволяют представлять электронные материалы, но сторона должна объяснить, какой факт они подтверждают и на чём основано доверие к ним.

Для электронного документооборота в судах важно постановление Пленума Верховного Суда РФ от 26 декабря 2017 г. № 57, посвящённое применению законодательства об электронных документах в судах общей юрисдикции и арбитражных судах [5]. Разъяснения касаются требований к электронным документам и порядка их подачи. Вместе с тем техническая возможность отправить файл через судебную информационную систему не решает вопрос о его доказательственном значении. Относимость, допустимость и достоверность материала оцениваются отдельно.

В уголовном судопроизводстве особое значение имеют нормы УПК РФ о собирании, проверке и оценке доказательств, а также правила проведения следственных действий и оформления их результатов [3]. При работе с цифровыми устройствами важно зафиксировать, где и при каких обстоятельствах обнаружен объект, как его осматривали и копировали, а также какие меры приняли для сохранения исходных данных. Это позволяет впоследствии проверить действия уполномоченных лиц. Если получение информации затрагивает тайну переписки, частную жизнь или иные охраняемые законом интересы, необходимо установить наличие законного основания и соблюдение предусмотренной процедуры. Общие правила дополняет Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [6]. Он регулирует отношения, связанные с поиском, получением, передачей, производством и распространением информации, а также использованием информационных технологий. Эти акты образуют правовую основу для работы с цифровыми данными, но не дают готового ответа на каждый вопрос, возникающий при исследовании изменяемой или технически сложной информации.

3. Основные виды электронных доказательств и особенности их представления

На практике встречаются разные виды электронных доказательств. К ним относятся договоры и первичные документы в электронной форме, электронные письма и переписка в мессенджерах, публикации в социальных сетях, аудио- и видеозаписи, фотографии, сведения из баз данных и информационных систем, журналы событий и доступа, а также данные с телефонов, компьютеров и других цифровых носителей. Этот перечень открыт: способы создания и фиксации информации продолжают меняться вместе с технологиями. Переписка по электронной почте или в мессенджере может подтвердить ход переговоров, согласование условий сделки, направление

уведомления или признание определённых обстоятельств. Однако для её оценки важно выяснить, кому принадлежит адрес или аккаунт, когда отправлены сообщения, сохранён ли разговор целиком и нет ли существенных пропусков. Скриншот помогает показать, как переписка выглядела на экране, но при споре о подлинности лучше сохранить исходные сообщения, данные учётной записи и сведения об экспорте переписки. Если это возможно и необходимо, полезно получить подтверждение от оператора или соответствующего сервиса.

Информация на сайтах и в социальных сетях может быть изменена или удалена в короткий срок. При фиксации такой страницы желательно сохранять не только снимок экрана, но и адрес страницы, дату и время доступа, доступную электронную копию или исходный файл, а также описание способа фиксации. В зависимости от обстоятельств можно обратиться к нотариусу для обеспечения доказательств. Такая фиксация подтверждает, какое содержание было зафиксировано в определённый момент, но сама по себе не устанавливает истинность публикации и не всегда позволяет определить её фактического автора.

При исследовании аудио- и видеозаписей необходимо учитывать, сохранился ли файл целиком, при каких условиях велась запись, есть ли признаки монтажа, можно ли определить участников и соответствует ли запись обстоятельствам, на которые ссылается сторона. Значение могут иметь сведения об устройстве, времени создания и способе передачи файла. При обоснованных технических сомнениях допустимо поставить вопрос об экспертизе. Однако экспертное заключение не заменяет судебную оценку: специалист исследует вопросы в пределах своих знаний, а доказательственное значение материала определяет суд. В цифровых носителях и информационных системах могут храниться не только видимые пользователю документы, но и метаданные, история операций, системные журналы и другие технические сведения. Их смысл нельзя оценить без учёта условий формирования данных. Например, могут иметь значение часовой пояс, точность системного времени, правила ведения журналов, срок хранения информации и возможность её изменения администратором. Если файл извлечён из системы, но способ извлечения не описан, проверить происхождение и неизменность данных бывает сложнее.

4. Критерии допустимости и достоверности электронных доказательств

При оценке электронных доказательств важно не смешивать четыре критерия. Относимость показывает, связан ли материал с обстоятельствами, которые нужно установить по делу. Допустимость касается соблюдения установленных законом требований к доказательствам и способу их получения. Достоверность означает, насколько надёжны источник и содержащиеся в материале сведения. Достаточность оценивается по совокупности доказательств, позволяющей сделать обоснованный вывод. Сам по себе цифровой формат не отменяет ни одного из этих требований.

Одна из главных практических задач — аутентификация, то есть проверка того, что представленный объект действительно является тем материалом, за который его выдаёт сторона. Для этого могут иметь значение источник файла, история его хранения и передачи, наличие исходной версии, сведения об устройстве и программной среде, метаданные, электронная подпись, сопроводительные документы и согласованность с другими доказательствами. Чем проще изменить материал так, чтобы изменения не были заметны, тем важнее независимые способы проверки.

Не стоит автоматически считать электронный оригинал и его распечатку равнозначными во всех отношениях. Бумажная копия может точно передавать видимое содержание, но обычно не сохраняет все технические свойства исходного файла. Скриншот может показать, что определённое изображение отображалось на экране в момент фиксации, однако сам по себе не всегда доказывает, кто разместил информацию, как долго она была доступна и менялось ли её содержание. В то же время отвергать скриншот только из-за его формы тоже неправильно: его значение нужно определять с учётом остальных материалов дела. Проверить неизменность файла помогает криптографическая хеш-сумма. Её вычисляют при получении файла, а затем при необходимости сравнивают с контрольным значением. Совпадение хеш-сумм означает, что сравниваемые файлы побитово совпадают. Но это не доказывает истинность их содержания и не устанавливает автора. Чтобы результат можно было проверить, следует указать использованный алгоритм, дату вычисления, программное средство и лицо, проводившее процедуру.

Для проверки цифровых материалов полезно также документировать всю историю обращения с ними: кто обнаружил данные, на каком устройстве, каким способом была создана копия, кто имел доступ к исходному файлу и где хранились экземпляры. В уголовном процессе такая фиксация помогает проверить законность получения информации и сохранность объекта. В гражданском и арбитражном процессе она также полезна: сторона сможет объяснить происхождение представленного материала и при необходимости показать исходный файл.

Если другая сторона оспаривает подлинность цифрового материала, суду важно разо-

браться в сути возражений. Следует учитывать, насколько конкретно они сформулированы, можно ли представить исходный объект, нужно ли запросить данные у третьего лица, осмотреть устройство или назначить экспертизу. Выбранные меры должны соответствовать спорному вопросу. Не каждый файл требует экспертного исследования, но технически значимые сомнения нельзя оставлять без внимания только потому, что материал выглядит убедительно.

5. Проблемы правоприменения и возможные направления совершенствования регулирования

Первая сложность связана с терминологией и процессуальной квалификацией цифровых материалов. Сходные по своей технической природе сведения в зависимости от обстоятельств могут рассматриваться как электронный документ, иной документ, письменное или вещественное доказательство. Само по себе такое различие не обязательно означает недостаток закона: квалификация зависит от содержания объекта и способа его процессуального закрепления. Однако отсутствие общих ориентиров может затруднять единообразное применение правил и делать результат менее предсказуемым для участников процесса.

Вторая проблема — риск оценивать доказательство по внешнему виду, а не по его происхождению и проверяемости. Аккуратно оформленный скриншот может содержать недостоверные сведения, тогда как технически непривычный файл способен сохранять важную информацию. Поэтому при оценке следует выяснять, откуда получены данные, как они фиксировались, можно ли проверить их независимо и согласуются ли они с другими доказательствами.

Третья задача — найти баланс между эффективным доказыванием и защитой прав человека. Переписка, сведения об аккаунтах, геолокация и другие цифровые следы могут затрагивать частную жизнь, тайну сообщений, персональные данные или коммерческую тайну. Даже если информация полезна для дела, это не отменяет требований к законности её получения. Решая вопрос о приобщении материала, необходимо учитывать процессуальные нормы и специальные ограничения, относящиеся к конкретному способу сбора данных.

Четвёртая проблема возникает из-за неравного доступа к цифровой информации. Исходные данные могут находиться у владельца платформы, оператора информационной системы или другой стороны спора. Самостоятельно получить их участник процесса часто не может. В таких случаях важно своевременно использовать предусмотренные законом механизмы истребования доказательств. При дальнейшем развитии регулирования стоит учитывать и риск автоматического удаления данных, и необходимость ограничить раскрытие информации, не относящейся к делу.

Целесообразно подготовить общие методические рекомендации по представлению электронных материалов. В них можно предусмотреть перечень сведений, которые обычно помогают проверить файл: источник и способ получения; дата и время фиксации, а при необходимости — часовой пояс; имя и формат файла; сведения об устройстве или системе, если они известны; порядок копирования и хранения; контрольная сумма, если она вычислялась; информация о монтаже, преобразовании или конвертации; объяснение того, какой факт подтверждает материал. Эти рекомендации не должны превращаться в жёсткий набор формальностей для каждого случая: объём сведений следует соотносить с характером доказательства и обстоятельствами дела.

Дополнительно можно уточнить процессуальные подходы к электронным оригиналам, копиям и метаданным. При этом чрезмерно строгие технические требования способны создать препятствия для людей, которые не располагают специальными знаниями и ресурсами. Более сбалансированным решением представляется сочетание общих правовых гарантий, понятных методических рекомендаций и возможности привлекать специалиста тогда, когда без специальных знаний спорный вопрос не разрешить.

Результаты исследования и обсуждение

Анализ нормативных положений позволяет сделать несколько выводов. Во-первых, электронные доказательства не существуют отдельно от общей системы средств доказывания как полностью самостоятельная категория. Их процессуальный статус определяется применимым кодексом, содержанием информации и способом её закрепления. Во-вторых, действующее законодательство допускает использование цифровых материалов, однако сама возможность представить файл в суд ещё не подтверждает его происхождение, целостность или достоверность.

В-третьих, необходимо различать подлинность цифрового объекта и правдивость содержащихся в нём сведений. Подлинный файл может содержать ошибку; неизменность сообщения не доказывает, кто именно его отправил; электронная подпись не делает изложенные факты бесспорными. В-четвёртых, надёжность материала повышается, если сохранён исходный файл, описан способ его получения, зафиксированы значимые метаданные и проведено сопоставление с независимыми источниками.

Практические предложения направлены не на то, чтобы устанавливать сложные технические требования для каждого электронного материала. Их задача — обеспечить разумную возмож-

ность проверки. Конкретный объём необходимых действий должен зависеть от вида данных, значения спорного обстоятельства, характера возражений и вероятности того, что информация могла измениться.

Заключение

Электронные материалы стали обычной частью современного судопроизводства. Российское законодательство позволяет использовать цифровые документы и другие электронные сведения, однако единого определения электронного доказательства и полностью унифицированного порядка работы с ним пока нет. Поэтому при решении соответствующих вопросов необходимо совместно учитывать нормы процессуальных кодексов, законодательства об информации и правила об электронной подписи. Наиболее сложные вопросы связаны с установлением источника данных и их автора, проверкой целостности файла, сохранением контекста и законностью получения информации. Ни цифровой формат, ни распечатка, ни скриншот не должны заранее определять результат оценки. Важны соблюдение процессуальных требований, возможность проверить сведения, надёжность источника и связь материала с другими доказательствами.

Качество доказывания можно повысить, если фиксировать обстоятельства получения цифровых материалов, по возможности сохранять исходные файлы и метаданные, применять контрольные суммы и обращаться к специалистам при наличии существенных технических сомнений. Дальнейшее развитие регулирования должно обеспечивать гибкость по отношению к технологиям, соблюдать процессуальные гарантии и права личности и одновременно не создавать неоправданных формальных барьеров.

Список литературы:

[1] Гражданский процессуальный кодекс Российской Федерации от 14 ноября 2002 г. № 138-ФЗ (в действующей редакции). Ст. 55, 71.

[2] Арбитражный процессуальный кодекс Российской Федерации от 24 июля 2002 г. № 95-ФЗ (в действующей редакции). Ст. 64, 75.

[3] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (в действующей редакции). Ст. 74, 81, 84, 87–88.

[4] Об электронной подписи : Федеральный закон от 6 апреля 2011 г. № 63-ФЗ (в действующей редакции).

[5] О некоторых вопросах применения законодательства, регулирующего использование документов в электронном виде в деятельности судов общей юрисдикции и арбитражных судов : постановление Пленума Верховного Суда Российской Федерации от 26 декабря 2017 г. № 57.

[6] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ (в действующей редакции).

[7] Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ (в действующей редакции). Ст. 160, 434.

[8] Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 г. (с учётом действующих поправок). Ст. 23, 24, 45, 46.

References:

[1] Civil Procedure Code of the Russian Federation No. 138-FZ dated November 14, 2002 (as amended). Art. 55, 71.

[2] Arbitration Procedure Code of the Russian Federation No. 95-FZ dated July 24, 2002 (as amended). Art. 64, 75.

[3] Code of Criminal Procedure of the Russian Federation No. 174-FZ dated December 18, 2001 (as amended). Art. 74, 81, 84, 87–88.

[4] On electronic signature: Federal Law No. 63-FZ of April 6, 2011 (as amended).

[5] On some issues of application of legislation regulating the use of documents in electronic form in the activities of courts of general jurisdiction and arbitration courts: Resolution of the Plenum of the Supreme Court of the Russian Federation of December 26, 2017 No. 57.

[6] Information, Information Technology and Information Protection: Federal Law No. 149-FZ of 27 July 2006 (as amended).

[7] Civil Code of the Russian Federation (Part One) No. 51-FZ dated November 30, 1994 (as amended). Art. 160, 434.

[8] Constitution of the Russian Federation: adopted by popular vote on December 12, 1993 (taking into account the current amendments). Art. 23, 24, 45, 46.