

ВЕРИФИЦИРУЕМОСТЬ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

THE VERIFIABILITY OF DIGITAL EVIDENCE IN THE CRIMINAL PROCEEDINGS OF THE RUSSIAN FEDERATION

A. Namtsaraeva

Summary. The article reveals the concept of information verification, the problem of its application in law enforcement practice. The author has studied the issue of the transition of evidence assessment in the prism of digital technologies.

Keywords: verifiability, proof, digital information, messengers.

Намцараева Александра Куприяновна

Аспирант,

Байкальский государственный университет, Иркутск

namtsaraeva867@mail.ru

Аннотация. В статье раскрывается понятие верификации информации, проблема применения в правоприменительной практике. Автором изучен вопрос перехода оценки доказательств в призме цифровых технологий.

Ключевые слова: верифицируемость, доказательство, цифровая информация, мессенджеры.

Верифицируемость цифровой информации, используемой в судебной деятельности, представляет собой юридически значимое свойство, обеспечивающее возможность достоверного установления ее происхождения, неизменности и соответствия фактическому содержанию. При этом в рамках уголовного процесса верифицируемость выступает как предпосылка допустимости доказательства, его объективной оценки и законного использования при разрешении уголовно-правового спора¹.

Однако действующее уголовно-процессуальное законодательство не содержит определения или хотя бы описания данного свойства, что препятствует его нормативному закреплению в статусе уголовно-процессуальной гарантии.

Категория верифицируемости может быть соотнесена с тремя базовыми признаками доказательства, закрепленными в ч. 1 ст. 75 УПК РФ — законностью получения, допустимостью и достоверностью. В то же время она охватывает более узкий аспект — техническую и процедурную проверяемость информации, представленной в цифровой форме².

Верифицируемость предполагает наличие объективных критериев, позволяющих установить источник

информации, зафиксировать параметры ее создания, исключить вмешательство и обеспечить возможность повторной идентификации цифрового материала³.

На понятийном уровне верифицируемость может быть определена как свойство информации, обеспечивающее возможность ее последующего удостоверения независимым субъектом посредством закрепленных законом процедур и технических средств. Такая проверка может быть осуществлена путем сопоставления контрольных цифровых меток (хеш-сумм), анализа метаданных, воспроизведения логов событий, проверки цифровых подписей, а также иными способами, гарантирующими неизменность исходного содержимого⁴.

В уголовном процессе это качество особенно значимо, поскольку позволяет исключить представление сфальсифицированных или технически искаженных доказательств.

Правовая неопределенность понятия верифицируемости усугубляется отсутствием единых методических подходов к оценке цифровой информации. В силу отсутствия в УПК РФ нормы, регламентирующей порядок ее аутентификации, задача подтверждения подлинности данных возлагается либо на сторону, представляющую

¹ Изотов А.И. Филологическое знание: проблема степени верифицируемости // Филологические науки. Научные доклады высшей школы. 2016. № 1. С. 5.

² Пастухов П.С. Доктринальная модель совершенствования уголовно-процессуального доказывания в условиях информационного общества. М.: Юрлитинформ, 2015. С. 35.

³ Леонтьева Е.Ю., Леонтьев М.А. О возможности верифицируемости современного научного знания // Мировое сообщество: проблемы и пути решения. Уфимский государственный нефтяной технический университет. Уфа, 2011. С. 90.

⁴ Лаптев В.А., Соловяненко Н.И. Цифровое правосудие. Цифровой документ. М.: Проспект, 2022. С. 41.

доказательство, либо на суд, не наделенный необходимым техническим инструментарием. В результате цифровая информация, поданная в суд, может быть исследована без установления ее происхождения, целостности и неизменности, что противоречит требованиям допустимости и достоверности⁵.

Следует также учитывать, что верифицируемость имеет процедурную природу. Она не сводится к одноразовому акту установления фактов, а реализуется в динамике уголовного процесса — от момента представления цифрового объекта до его окончательной оценки в приговоре. Таким образом, обеспечение верифицируемости требует не только технических средств, но и нормативного механизма, регулирующего фиксацию, транспортировку, хранение и исследование цифровой информации⁶.

Без этого гарантии законного и справедливого судопроизводства утрачивают свою реализацию применительно к цифровым доказательствам.

Подчеркивая ключевое значение верифицируемости, необходимо признать ее самостоятельной уголовно-процессуальной категорией, требующей закрепления в законе. Отнесение цифровых объектов к доказательствам должно сопровождаться формализацией процедуры проверки их подлинности, источника и целостности, а не оставаться предметом усмотрения участников или судебской оценки. Лишь при наличии соответствующих процессуальных фильтров верифицируемость может выполнять функцию гарантии — не декларативной, а реально действующей.

Развитие цифровых технологий обусловило появление новых видов информации, активно вовлекаемой в уголовное судопроизводство в качестве доказательственных средств. Особенность таких данных заключается в том, что они изначально создаются, передаются и хранятся в электронной форме, не имеющей материального носителя. Это обстоятельство требует особого правового подхода к их классификации и процессуальной оценке.

Цифровая информация, используемая в суде, может включать: электронные документы, сетевые сообщения (включая переписку в мессенджерах и социальных сетях), видеозаписи, аудиофайлы, файлы систем виде-

онаблюдения, данные GPS-навигации, сведения о действиях пользователей в информационных системах, метаданные (временные метки, IP-адреса, идентификаторы устройств), а также цифровые лог-файлы и записи экранов. Несмотря на многообразие форм, нормативное определение данных объектов в УПК РФ остается отсутствующим, что создает сложности при квалификации таких сведений в качестве доказательств.

В соответствии с ч. 2 ст. 74 УПК РФ, доказательствами признаются показания, вещественные доказательства, документы, заключения экспертов, протоколы следственных и судебных действий, а также иные сведения, полученные в установленном законом порядке. Однако цифровая информация может не соответствовать формальным признакам этих категорий. Например, переписка в мессенджере не является документом в классическом понимании, но может содержать сведения, имеющие доказательственное значение. Аналогичным образом, скриншот, содержащий изображение или текст, не является ни документом, ни вещью, но также способен подтверждать или опровергать факт, имеющий значение для дела⁷.

При этом действующее законодательство, включая положения ст. 81.1 УПК РФ, относящиеся к электронным носителям, не устанавливает критерии допустимости цифровой информации, представленной без материального носителя. Это обстоятельство особенно проблематично в условиях, когда доказательство представляется в виде цифровой копии без возможности установить его источник, механизм создания и цепочку хранения. Таким образом, доказательственная сила таких материалов оказывается под вопросом, что создает риск произвольной оценки суда.

Дополнительную сложность представляет отсутствие формализованных признаков подлинности цифровых объектов. Если для бумажного документа предусмотрено подпись, печать, исходящий номер, то в цифровой среде идентификационные признаки нередко отсутствуют либо легко подделываются. Без специальных процедур верификации невозможно определить, был ли конкретный файл изменен, кем и когда. В результате может возникнуть ситуация, при которой представленный суду материал будет формально отвечать внешним признакам доказательства, но фактически не обладать ни достоверностью, ни допустимостью.

Судебная практика подтверждает, что суды не всегда имеют единый подход к оценке цифровой информации. Отдельные дела демонстрируют признание скриншотов

⁵ Кувычков С.И. Использование в доказывании по уголовным делам информации, представленной в электронном виде: дисс. ... канд. юрид. наук. Москва, 2016. С. 64.

⁶ Социотехнический ландшафт цифровой реальности: философско-методологический концепт, онтологические матрицы, экспертно-эмпирическая верификация / В.И. Аршинов, М.В. Артеменко, И.А. Асеева [и др.]. Курск: Университетская книга, 2019. С. 56.

⁷ Дикарев И.С. Ознакомление с материалами уголовного дела в ходе предварительного расследования: cui bono? // Уголовное судопроизводство. 2019. № 4. С. 20.

допустимыми доказательствами без проведения технической экспертизы⁸, тогда как в других случаях суды отказываются приобщать цифровые файлы в отсутствие их подтвержденного источника⁹. Такая разнонаправленность порождает правовую неопределенность и противоречит требованию единообразного применения закона.

В условиях отсутствия четкого нормативного механизма оценки цифровых сведений особое значение приобретает их верифицируемость — то есть способность быть проверенными по признакам подлинности, происхождения, целостности и достоверности. Вся цифровая информация, вовлеченная в судопроизводство, нуждается в дополнительной правовой фильтрации, обеспечивающей возможность ее воспроизведения, контроля и анализа независимо от субъекта, ее представившего.

Цифровая информация, используемая в судебной деятельности, представляет собой особую категорию доказательственных данных, не охваченную в полной мере действующим правовым регулированием. Это требует не только расширения процессуальной классификации доказательств, но и внедрения механизмов, способных обеспечить нормативную верификацию их происхождения и содержания.

Верифицируемость цифровой информации, вовлеченной в уголовное судопроизводство, не может быть обеспечена исключительно правовыми средствами. Она требует взаимодействия двух взаимодополняющих компонентов: нормативной регламентации и технической инфраструктуры, способной гарантировать устойчивость, подлинность и воспроизводимость цифровых объектов. Эти условия составляют основу механизма, посредством которого верифицируемость трансформируется из абстрактной категории в правоприменимую гарантию.

С технической точки зрения верифицируемость базируется на ряде инструментов, позволяющих обеспечить контроль над цифровыми объектами: хеш-функции, временные метки (таймштампы), криптографические подписи, лог-файлы, цифровые идентификаторы, средства электронной подписи и блокчейн-технологии¹⁰.

⁸ Приговор Ленинского районного суда города Смоленска № 1-1/2024 от 10 января 2024 г. по делу № 1-1/2024. URL: <https://sudact.ru/regular/doc/JmNPdIT9bPVv/> (дата обращения: 10.04.2025).

⁹ Приговор Кинельского районного суда Самарской области № 1-14/2023 от 18 августа 2023 г. по делу № 1-14/2023. URL: <https://sudact.ru/regular/doc/pclKKrIAMZx/> (дата обращения: 10.04.2025).

¹⁰ Черкасова Е.С., Черкасов К.А. Психологическая экспертиза по верификации информации: базовые понятия, возможности, решаемые задачи // Российский следователь. 2020. № 10. С. 21.

Эти инструменты позволяют зафиксировать исходное состояние данных, идентифицировать отправителя и подтвердить неизменность содержимого на определенный момент времени. При этом эффективность таких средств зависит от их встраивания в процессуальные процедуры, а не только от их наличия как программных решений.

Применительно к уголовному процессу верифицируемость цифровой информации должна начинаться с момента ее создания или получения и сопровождаться на всех этапах обращения. Это включает:

- фиксацию метаданных, указывающих на источник, время, местоположение и технические параметры;
- использование неизменяемых форматов хранения (например, WORM-носителей или зашифрованных архивов);
- обязательное документирование всей истории передачи и преобразования данных.

Однако на практике такие требования не получили нормативной конкретизации в УПК РФ. Например, ст. 186.1 УПК РФ, регулирующая порядок получения информации, представленной в электронном виде, не устанавливают конкретных требований к формату, способу верификации или документированию цепочки хранения данных. В результате цифровые доказательства нередко приобщаются к материалам дела без технической проверки их подлинности, что обесценивает их доказательственную силу.

На уровне правового регулирования необходимым условием обеспечения верифицируемости является введение обязательных процедур идентификации цифрового источника и зафиксированного цифрового следа. Это предполагает внедрение в уголовный процесс:

- требований к платформам и программному обеспечению, с помощью которых создается или передается информация;
- стандартов сертификации используемых цифровых средств фиксации;
- обязательной экспертной или технической проверки файлов, представленных в суд.

Дополнительным условием выступает создание нормативно признанной системы доверия к цифровым источникам. В частности, использование государственных информационных платформ (например, ГАС «Правосудие») при подаче цифровых документов может стать условием презумпции достоверности данных, если в системе реализованы механизмы аудита, неизменности и аутентификации информации. В ином случае каждое представленное доказательство должно

сопровождаться технической справкой или экспертным заключением¹¹.

Важно также учитывать различие между процессуальной и технической верификацией. Первая предполагает соблюдение процедуры получения и представления доказательства, вторая — проверку его содержательной неизменности. Только совмещение этих уровней способно обеспечить юридическую надежность цифровой информации. При этом отсутствие хотя бы одного из компонентов порождает основания для признания доказательства недопустимым в силу нарушения требований ст. 75 УПК РФ.

Верифицируемость цифровой информации требует институционального согласования технических решений с уголовно-процессуальными процедурами. Без этого цифровое доказательство рискует остаться непроверяемым, а значит — юридически ненадежным. Для преодоления этого разрыва необходимо не только правовое закрепление верификации как стадии доказывания, но и интеграция в уголовный процесс технологических стандартов контроля за подлинностью информации.

В рамках уголовного судопроизводства именно суд наделен функцией процессуального фильтра, обеспечивающего проверку допустимости, относимости и достоверности доказательств. Однако с переходом к использованию цифровых форм представления информации, возможности реализации этой функции оказываются существенно ограничены. Отсутствие универсальных критериев проверки цифрового объекта, незафиксированность специальных процедур его технической оценки и нормативная неопределенность понятия цифрового доказательства создают угрозу подмены правовой оценки формальной допустимостью¹².

Согласно положениям ч. 2 ст. 17 и ст. 88 УПК РФ, суд оценивает доказательства по своему внутреннему убеждению, основанному на совокупности имеющихся в деле данных. Однако при отсутствии объективных критериев верифицируемости цифровых сведений внутреннее убеждение оказывается изолированным от технической реальности. Так, оценка скриншота, файла, лог-записи или изображения, не сопровождающихся данными

о дате, источнике и целостности, не может быть признана достоверной без привлечения дополнительных процедур — как минимум, технической проверки происхождения и сохранности содержимого.

Отдельным аспектом является недопустимость перекладывания функции верификации на сторону, представившую доказательство. В условиях цифрового взаимодействия возможность фальсификации или искажения цифровой информации значительно выше, чем при работе с физическими объектами. Поэтому контроль над ее подлинностью должен осуществляться в пределах публичного механизма, а не зависеть от инициативы защиты или обвинения. Между тем, действующее законодательство не содержит положений, обязывающих суд проверять происхождение и неизменность цифровых данных, что нарушает баланс процессуальной ответственности.

Судебная практика подтверждает, что цифровая информация, полученная с нарушением принципов верификации, зачастую используется без должного критического анализа. В ряде случаев суды приобщают электронные письма, переписку из мессенджеров или видеозаписи с неизвестных устройств, руководствуясь лишь их визуальным соответствием обстоятельствам дела¹³. При этом не проводится анализ технических параметров, не исследуется лог-файл, не проводится сопоставление с иными источниками¹⁴.

Такая практика приводит к снижению доказательственного стандарта и противоречит назначению суда как гарантированно нейтрального и контролирующего органа.

Дополнительным фактором, снижающим эффективность судебных гарантий, является отсутствие в суде необходимой технической компетенции. В отличие от эксперта или специалиста, суд не располагает инструментарием для установления подлинности файла, подтверждения его неизменности или расшифровки метаданных. Это ставит под сомнение возможность полноценной оценки цифрового объекта без привлечения специальных знаний, что требует переосмысления роли судебной экспертизы и технической поддержки процесса исследования доказательств.

Судебные гарантии проверки цифровой информации в их существующем виде не обеспечивают полноту пра-

¹¹ Полстовалов О.В. Биотехнологические глобальные вызовы и возможности межотраслевой консолидации научных изысканий на уровне криминалистической профилактики // Юридическое образование и наука. 2023. № 6. С. 39.

¹² Яковлева К.Ю. Верификация как свойство электронной информации на примере видео-конференц-связи в уголовном процессе // Актуальные вопросы производства предварительного следствия в современных условиях совершенствования уголовно-процессуального законодательства. Сборник научных трудов Всероссийской научно-практической конференции. Москва, 2022. С. 470.

¹³ Приговор Юргинского городского суда Кемеровской области № 1-21/2023 от 7 июля 2023 г. по делу № 1-21/2023. URL: <https://sudact.ru/regular/doc/wBKO2zSne7rW/> (дата обращения: 10.04.2025).

¹⁴ Приговор Сыктывкарского городского суда Республики Коми № 1-651/2023 от 2 октября 2023 г. по делу № 1-651/2023. URL: <https://sudact.ru/regular/doc/HlhnR9kEiUHp/> (дата обращения: 10.04.2025).

вовой защиты участников процесса. Без нормативного закрепления процедур верификации цифровых сведений, обязательного привлечения технических средств и стандартизации оценки подлинности, цифровое доказательство может утратить юридическую устойчивость. В этих условиях требуется не только расширение нормативной базы, но и институциональное усиление судебной роли в обеспечении достоверности цифровых материалов¹⁵.

¹⁵ Парыгина Н.Н. Тонкая грань и большая разница между утверждением о факте и выражением мнения // Евразийский юридический журнал. 2016. № 10 (101). С. 169.

В условиях цифровизации уголовного судопроизводства эффективное обеспечение верифицируемости информации невозможно без привлечения субъектов, обладающих специальными знаниями в области информационных технологий и цифровой безопасности.

Прежде всего, речь идет о специалистах и экспертах, чья деятельность прямо регламентирована уголовно-процессуальным законом и направлена на восполнение технической и предметной неполноты правоприменения.

ЛИТЕРАТУРА

1. Изотов А.И. Филологическое знание: проблема степени верифицируемости // Филологические науки. Научные доклады высшей школы. 2016. № 1. С. 5.
2. Пастухов П.С. Доктринальная модель совершенствования уголовно-процессуального доказывания в условиях информационного общества. М.: Юрлитинформ, 2015. С. 35.
3. Леонтьева Е.Ю., Леонтьев М.А. О возможности верифицируемости современного научного знания // Мировое сообщество: проблемы и пути решения. Уфимский государственный нефтяной технический университет. Уфа, 2011. С. 90.
4. Лаптев В.А., Соловяненко Н.И. Цифровое правосудие. Цифровой документ. М.: Проспект, 2022. С. 41.
5. Кувычков С.И. Использование в доказывании по уголовным делам информации, представленной в электронном виде: дисс. ... канд. юрид. наук. Москва, 2016. С. 64.
6. Социотехнический ландшафт цифровой реальности: философско-методологический концепт, онтологические матрицы, экспертно-эмпирическая верификация / В.И. Аршинов, М.В. Артеменко, И.А. Асеева [и др.]. Курск: Университетская книга, 2019. С. 56.
7. И.С. Ознакомление с материалами уголовного дела в ходе предварительного расследования: *cui bono?* // Уголовное судопроизводство. 2019. № 4. С. 20.
8. Приговор Ленинского районного суда города Смоленска № 1-1/2024 от 10 января 2024 г. по делу № 1-1/2024. URL: <https://sudact.ru/regular/doc/JmNPdIT9bPVv/> (дата обращения: 10.04.2025).
9. Приговор Кинельского районного суда Самарской области № 1-14/2023 от 18 августа 2023 г. по делу № 1-14/2023. URL: <https://sudact.ru/regular/doc/rcIKKrlAMZx/> (дата обращения: 10.04.2025).
10. Черкасова Е.С., Черкасов К.А. Психологическая экспертиза по верификации информации: базовые понятия, возможности, решаемые задачи // Российский следователь. 2020. № 10. С. 21.
11. Полстовалов О.В. Биотехнологические глобальные вызовы и возможности межотраслевой консолидации научных изысканий на уровне криминалистической профилактики // Юридическое образование и наука. 2023. № 6. С. 39.
12. Яковлева К.Ю. Верификация как свойство электронной информации на примере видео-конференц-связи в уголовном процессе // Актуальные вопросы производства предварительного следствия в современных условиях совершенствования уголовно-процессуального законодательства. Сборник научных трудов Всероссийской научно-практической конференции. Москва, 2022. С. 470.
13. Приговор Юргинского городского суда Кемеровской области № 1-21/2023 от 7 июля 2023 г. по делу № 1-21/2023. URL: <https://sudact.ru/regular/doc/wBKO2zSne7rW/> (дата обращения: 10.04.2025).
14. Приговор Сыктывкарского городского суда Республики Коми № 1-651/2023 от 2 октября 2023 г. по делу № 1-651/2023. URL: <https://sudact.ru/regular/doc/HlhnR9kEiUNr/> (дата обращения: 10.04.2025).
15. Парыгина Н.Н. Тонкая грань и большая разница между утверждением о факте и выражением мнения // Евразийский юридический журнал. 2016. № 10 (101). С. 169.