Проблемы использования цифровых доказательств в уголовном процессе

Хавчаев Зураб Гаджибутаевич
магистрант, юридический институт, Дагестанский государственный университет, donhongil40@gmail.com

В настоящей статье рассматриваются теоретические и практические проблемы использования цифровых доказательств в уголовном судопроизводстве Российской Федерации. Актуальность темы обусловлена стремительной цифровой трансформацией общественных отношений и ростом числа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, что объективно требует модернизации подходов к доказыванию. Цель данного исследования состоит в выявлении проблемных аспектов правового регулирования процесса сбора, проверки и оценки цифровых доказательств. Кроме того, в рамках исследования планируется разработка предложений по совершенствованию уголовно-процессуального законодательства в этой области. Методологическую базу исследования составляют диалектический метод научного познания, формально-юридический метод, сравнительно-правовой метод, системно-структурный метод, а также методы анализа, синтеза и обобщения. В результате исследования обоснован вывод о необходимости легального закрепления понятия «цифровые доказательства», унификации процессуального порядка их изъятия и фиксации, а также внедрения специальных мер обеспечения достоверности и аутентичности цифровой информации в уголовном процессе.
Ключевые слова: цифровые доказательства, уголовный процесс, электронная информация, доказывание, цифровая трансформация.

Введение

Современный этап развития общества характеризуется глубокой цифровой трансформацией всех сфер жизнедеятельности. Информационные технологии проникают не только в экономику, социальную сферу и повседневное общение граждан, но и в сферу уголовного судопроизводства. Как справедливо отмечается в научной литературе, уголовное судопроизводство в настоящее время характеризуется усилением цифровизации. Все чаще в качестве средств доказывания выступают сведения, полученные из электронных источников: сообщения мессенджеров, данные с камер видеонаблюдения, информация с электронных носителей, скриншоты страниц сайтов и иные цифровые объекты.

Однако, несмотря на широкое распространение цифровой информации в правоприменительной практике, ее процессуальный статус остается неопределенным. Действующий Уголовно-процессуальный кодекс Российской Федерации не содержит легального определения цифровых или электронных доказательств, не устанавливает специальных правил их собирания, проверки и оценки. Это порождает множество проблем правоприменения, приводит к признанию судами доказательств недопустимыми и, как следствие, к невозможности установления объективной истины по уголовным делам.

Обсуждение

Вопрос о понятии и правовой природе цифровых доказательств представляет собой дискуссионную проблему в современной науке уголовного процесса. Отсутствие четкого легального определения данного феномена приводит к многообразию теоретических подходов и, как следствие, к противоречивой правоприменительной практике.

В научной литературе используются различные термины для обозначения доказательств, связанных с электронными информационными ресурсами, такие как "электронные доказательства", "цифровые доказательства", "доказательства в электронной форме" и "компьютерная информация". В науке уголовного процесса не достигнуто единого мнения относительно термина "электронные доказательства", а также относительно целесообразности их классификации как самостоятельного вида доказательств в уголовном судопроизводстве. Наиболее предпочтительным представляется использование термина "цифровые доказательства", который отражает сущностные характеристики информации, связанные с ее представлением в цифровой (двоичной) форме.

А.Ю. Черданцев предлагает следующее определение: «цифровые (электронные) доказательства — это информация, хранимая или передаваемая в двоичном виде, которая сохранила сведения о подлежащих установлению обстоятельствах уголовного дела в процессе собирания, проверки и оценки доказательства». Аналогичный подход встречается в более поздних работах.

Особенность цифровых доказательств заключается в их двойственной природе. По мнению В. Ф. Васюкова и Э. о. Дамирчиева «в отличие от материальных следов, образующихся под воздействием объективных физических, химических или биологических процессов, электронные данные формируются в результате взаимодействия двух факторов: аппаратной составляющей (физические носители) и программного обеспечения, созданного разработчиками на основе субъективно выбранных алгоритмов». Это означает, что цифровая информация всегда опосре-

дована техническими средствами и программным обеспечением, что создает дополнительные риски для ее достоверности.

В зависимости от того, что имеет доказательственное значение — материальный носитель или содержащаяся на нем информация, — цифровые объекты могут относиться к различным видам. Когда ключевое значение для расследования имеют физические параметры конкретного носителя данных (например, неисправный винчестер или USB-накопитель с явными признаками несанкционированного доступа), то подобные предметы правомерно причислять к материальным уликам. Если же основную ценность представляет смысловое наполнение информации — будь, то текстовые документы, структурированные массивы сведений, аудио- или видеоматериалы, — то более аргументированным выглядит их отнесение к разряду документальных свидетельств.

Цифровые доказательства обладают рядом специфических характеристик, которые отличают их от традиционных видов доказательств и требуют особых подходов к их собиранию, проверке и оценке.

Во-первых, это высокая степень изменчивости и уязвимости. По мнению Л. И. Викторовны ««Уязвимость» компьютерной информации, вызванная возможностью ее быстрого изменения и удаления лицами, совершившими преступление, либо их соучастниками, и необходимость дальнейшего использования такой информации в доказывании требуют законодательного закрепления дополнительных — помимо следственных действий — «способов» ее фиксации сотрудниками правоохранительных органов». Несвоевременное изъятие цифрового носителя или неквалифицированные действия следователя могут привести к безвозвратной утрате доказательственной информации.

Во-вторых, это возможность существования в идентичных копиях без потери содержания. В отличие от вещественных доказательств, которые обладают уникальными характеристиками, цифровая информация может подвергаться неограниченному копированию без утраты идентичности. Это создает определенные сложности в определении процессуального статуса копий, однако также предоставляет возможность применения современных технологий для хранения и обеспечения сохранности данных.

В-третьих, это зависимость от технических средств и программного обеспечения. Идентичные данные могут быть подвергнуты различным интерпретациям в зависимости от применяемого программного обеспечения, что обуславливает необходимость стандартизации методик их анализа. Следователь и суд не могут непосредственно воспринять информацию, содержащуюся в цифровом виде, без применения специальных технических средств.

Процесс собирания цифровых доказательств в рамках расследования уголовных дел сталкивается с рядом проблем как процессуального, так и организационно-тактического характера. Основными процессуальными формами получения цифровой информации являются осмотр, обыск и выемка, в ходе которых могут быть обнаружены и изъяты персональные компьютеры, мобильные устройства, внешние накопители и другие технические средства хранения информации. Однако текущая процессуальная регламентация не вполне учитывает особенности цифровых объектов. Согласно мнению, изложенному в профильной литературе, технологическая природа объектов электронного следа диктует свои правила при осуществлении поисковых и фиксирующих действий. Ключевым моментом в ходе анализа компьютерных систем выступает предварительная фиксация всех установленных соединений с внешним оборудованием и перечня исполняемых в данный момент команд, поскольку экстренное прекращение подачи энергии влечет за собой безвозвратное стирание данных, размещенных в ОЗУ. Однако Уголовно-процессуальный кодекс Российской Федерации не содержит специальных правил, учитывающих эти особенности. Проблема заключается также в том, что далеко не всегда возможно изъятие самого носителя информации. В случаях, когда информация хранится в «облачных» сервисах или на серверах третьих лиц, физическое изъятие носителя невозможно либо экономически нецелесообразно. Возникает вопрос о процессуальном статусе информации, полученной из таких источников.

Особую сложность представляет собирание цифровых доказательств в ходе проверки сообщения о преступлении, до возбуждения уголовного дела. Как справедливо указывает А. М. Ибрагимовны «существующее правовое регулирование не отвечает информационным потребностям общества». В этот период следователь или оперативный сотрудник могут не обладает полным объемом процессуальных полномочий и квалификации, что может привести к утрате доказательственной информации.

Проверка и оценка цифровых доказательств — наиболее сложный этап доказывания, поскольку требует от следователя и суда не только юридических знаний, но и компетенции в области информационных технологий.

Центральной проблемой является обеспечение достоверности цифровых доказательств. По мнению В. Е. Пономарева «Обеспечение надежного хранения электронных доказательств требует комплексного подхода, включающего использование современных технологий, соблюдение законодательных норм и постоянный контроль за процессами хранения и доступа к данным. Только таким образом можно гарантировать, что электронные доказательства будут допустимыми и достоверными, что является ключевым фактором для успешного расследования и последующего использования доказательств в судебном разбирательстве», соглашаясь с вышесказанным можно сделать вывод что необходимо повышение гарантий обеспечения их достоверности путем внедрения и использования современных способов хранения и обеспечения ограниченного доступа. В отличие от традиционных доказательств, где подлинность может быть установлена путем прямого восприятия или экспертного исследования физических свойств объекта, достоверность цифровой информации требует проверки целостности файла, отсутствия несанкционированных изменений, подлинности электронной подписи и иных атрибутов. Цифровые доказательства характеризуются высокой степенью чувствительности и динамичности, что обуславливает необходимость специализированной подготовки и использования соответствующих средств для их сбора, верификации, хранения и оценки. В судебной практике имели место случаи, когда суды признавали цифровые доказательства недопустимыми вследствие нарушений процедуры их получения. Наиболее распространенными нарушениями являются: отсутствие понятых при изъятии электронных носителей (в случаях, когда их участие обязательно), неправильное оформление протоколов следственных действий, отсутствие сведений о технических средствах, использованных при фиксации доказательств, и другие.

Основная проблема правового регулирования цифровых доказательств заключается в отсутствии их легального закрепления в Уголовно-процессуальном кодексе Российской Федерации. Действующее законодательство не содержит ни определения цифровых доказательств, ни специальных правил их собирания, проверки и оценки. Многие учёные-правоведы и практикующие специалисты в области процессуального права, имеющие за плечами реальный опыт, приходят к выводу, что закреплять в за-

конодательстве отдельную статью, посвящённую цифровым (электронным) доказательствам, нецелесообразно. Аргументируют они это тем, что чётко очертить круг таких доказательств весьма проблематично хотя бы из-за отсутствия какого-либо единого подхода в науке — его не было и нет до сих пор. Как отмечают С. В. Корнакова и Е. В. Чигрина, «анализ положений ч. 2 ст. 74 УПК РФ позволяет сделать вывод, что законодатель электронные носители информации не выделяет в отдельную разновидность доказательств». Более того, с учётом стремительного развития технологий, включая персональные устройства, подобная правовая норма довольно быстро утратила бы свою актуальность и нуждалась бы в постоянных корректировках. Однако этот подход представляется спорным. Отсутствие специального регулирования приводит к правовой неопределенности. Проблемой является также разграничение вещественных доказательств и иных документов применительно к цифровым объектам. Поскольку цифровая информация может существовать как в материальной форме (на физическом носителе), так и в нематериальной (в сети Интернет, облачных хранилищах), ее отнесение к тому или иному виду доказательств требует четких критериев.

Особого внимания заслуживает вопрос о допустимости доказательств, полученных из открытых источников сети Интернет. Правоприменительная практика идет по пути признания таких доказательств допустимыми при условии соблюдения определенных требований (нотариальное удостоверение, указание даты и времени получения, точного адреса страницы). Однако единообразный подход отсутствует.

По итогам анализа проблематики применения цифровых доказательств в уголовном судопроизводстве представляется возможным сформулировать предложения по оптимизации отраслевого законодательства, первоочередным из которых видится легализация термина «цифровые доказательства» в статье 74 Уголовно-процессуального кодекса Российской Федерации.

На протяжении длительного периода времени отсутствие в Уголовно-процессуальном кодексе легального определения цифровых доказательств можно было рассматривать как преднамеренную стратегию обеспечения нормативной гибкости. Законодатель, по всей видимости, стремился избежать «ловушки конкретики», когда жесткое определение неизбежно устарело бы быстрее, чем закон вступает в силу. Действительно, если бы в 2010 году УПК зафиксировал определение через «файлы на жестком диске» или «данные на флеш-накопителе», это исключило бы из сферы доказательств облачные технологии, блокчейн-транзакции, показания носимых устройств (смарт-часов, медицинских имплантатов) и, в перспективе, нейроинтерфейсы или квантовые вычисления.

Придерживаясь принципа технологической нейтральности, законодатель сохранял понятие «открытым», позволяя правоприменителю каждый раз решать вопрос: может ли данный цифровой объект быть источником доказательств по тем же критериям, что и традиционный носитель. Такая «преднамеренная неопределенность» долгое время служила залогом долгосрочной эффективности уголовного процесса в эпоху смены технологических укладов. Как обоснованно указывает Р. В. Костенко «классические критерии допустимости доказательств, сформированные в эпоху «бумажного» делопроизводства, сталкиваются с новыми вызовами при оценке цифровых данных». Следственная и судебная практика постепенно вырабатывала критерии относимости, допустимости и достоверности цифровых объектов без жесткой привязки к их физической форме.

Однако, разделяя логику законодателя в долгосрочной перспективе, полагаю, что на сегодняшний день пассивное ожидание «устоявшейся практики» уже исчерпало свой потенциал. Настал момент для легального закрепления понятия цифровых доказательств в законе. Аргументирую это несколькими факторами.

Во-первых, накоплен критический массив правоприменительной практики. С момента активного внедрения цифровых технологий в расследования прошло более десятилетия. Верховные суды (включая обзоры практики ВС РФ) неоднократно давали ориентиры по допустимости «электронных» доказательств. Однако отсутствие единой дефиниции привело к разночтениям: один и тот же объект (например, скриншот переписки, лог-файл сервера или дамп оперативной памяти) в разных регионах признается либо полноценным доказательством, либо «неформатным» файлом. Единая дефиниция устранит этот произвол.

Во-вторых, технический прогресс достиг уровня, когда «гибкость» оборачивается правовой неопределенностью. Мы больше не ждем принципиально новых носителей — все данные, включая будущие (нейроинтерфейсы, квантовая связь), по-прежнему обладают родовыми признаками: электронная природа, кодируемость, необходимость аппаратно-программной интерпретации. Законодатель способен дать определение через эти устойчивые признаки, не привязываясь к конкретным технологиям.

В-третьих, пробел в УПК уже восполняется подзаконными актами и ведомственными инструкциями, что ненормально для уголовного процесса. Вопросы изъятия, фиксации и оценки цифровых следов детально прописаны, например, в ведомственных порядках Следственного комитета России или Министерства внутренних дел Российской Федерации. Однако отсутствие базового понятия в самом кодексе порождает риск признания доказательств недопустимыми из-за формального нарушения «законности» происхождения — когда все процедуры соблюдены, но сам объект в законе не поименован.

В-четвертых, особую актуальность закрепление понятия и правил проверки цифровых доказательств приобретает в делах частного обвинения. Как показывает практика, именно по таким категориям дел (клевета, побои, оскорбления, умышленное причинение легкого вреда здоровью) цифровые доказательства предъявляются наиболее часто, причем преимущественно со стороны пострадавшего. Гражданин, обращаясь к мировому судье, прилагает к заявлению распечатки переписок из мессенджеров (WhatsApp, Telegram), скриншоты постов из социальных сетей, видеозаписи с камер мобильных телефонов или домофонов, аудиофайлы с диктофонов. Формально эти объекты не поименованы в кодексе, что ставит мировых судей перед сложным выбором: либо признавать их «иными документами» (ст. 84 УПК) с большой натяжкой, либо отказывать в приобщении. Легальное определение цифровых доказательств снимет этот вопрос, придав юридическую силу тем объектам, которые уже фактически стали основой частного обвинения.

Однако просто закрепить понятие недостаточно. Учитывая стремительное развитие технологий искусственного интеллекта, встает еще более острая проблема — подлинности цифровых доказательств. Уже сегодня существуют нейросети, способные с высокой достоверностью синтезировать голос любого человека (дипфейк аудио), генерировать реалистичное видео с любым сценарием (дипфейк видео) или создавать фальшивую переписку. В связи с этим полагаю, что цифровые доказательства, особенно по делам частного обвинения, где сторона обвинения часто не обладает специальными познаниями, должны до их предъявления суду проходить обязатель-

ную проверку на подлинность с помощью судебной экспертизы (или иного установленного законом механизма верификации).

Это может быть реализовано следующим образом:

Обязательное экспертное исследование для ключевых цифровых доказательств (аудио-, видеозаписей, скриншотов, файлов переписки), на которых сторона обвинения строит свои доводы. Частному обвинителю следует предоставить право ходатайствовать о назначении такой экспертизы, а в случае его имущественной несостоятельности — возможность освобождения от оплаты (по аналогии с назначением экспертизы по инициативе суда).

Закрепление в законодательстве презумпции недостоверности цифрового доказательства, если сторона, его представившая, отказывается от добровольной экспертной проверки или препятствует изъятию исходного цифрового носителя (телефона, планшета и др.) для исследования.

Предлагаю следующее определение (как рабочий вариант для дискуссии) и дополнение к Уголовно-процессуальному кодексу Российской Федерации:

Цифровыми (электронными) доказательствами признаются фактические данные, имеющие доказательственное значение для разрешения уголовного дела, выраженные в электронной (цифровой) форме, которые либо материализованы на физическом носителе, либо циркулируют в среде информационно-телекоммуникационных сетей, будучи опосредованы применением соответствующих технических средств и специализированного программного обеспечения.

По делам частного обвинения цифровые доказательства, если они являются единственным или основным источником подтверждения вины, подлежат обязательной проверке на подлинность в порядке, установленном судом. Такая проверка осуществляется посредством судебной экспертизы либо с использованием иных предусмотренных законом методов верификации, обеспечивающих установление отсутствия монтажа, внесения изменений или синтеза с помощью технологий искусственного интеллекта и иных технических и аппаратно-программных средства.

Включение данной или аналогичной нормы в кодекс не будет препятствовать гибкости процесса, но придаст цифровым доказательствам юридическую обоснованность, единообразие и предсказуемость в применении. А введение механизма обязательной проверки подлинности, особенно в делах частного обвинения, станет ответом на вызовы, связанные с развитием генеративных нейросетей. Продолжение законодательного молчания сегодня — это уже не осторожность, а искусственное торможение развития уголовно-процессуальной формы и игнорирование реальной угрозы фальсификации цифровых доказательств с помощью технологий искусственного интеллекта.

Заключение

Проведенное исследование проблем использования цифровых доказательств в уголовном процессе позволяет сделать следующие выводы.

Современный этап развития уголовного судопроизводства характеризуется активным внедрением цифровых технологий и ростом значения цифровой информации в доказывании. Однако существующее правовое регулирование не в полной мере соответствует потребностям правоприменительной практики, что создает существенные проблемы при собирании, проверке и оценке цифровых доказательств.

Основные проблемы связаны с отсутствием легального определения цифровых доказательств, неопределенностью их процессуального статуса, недостаточной регламентацией порядка проведения следственных действий с цифровой информацией, а также сложностью обеспечения достоверности и аутентичности цифровых доказательств.

Решение указанных проблем видится в совершенствовании уголовно-процессуального законодательства путем легального закрепления понятия цифровых доказательств, установления специальных правил их собирания, проверки и оценки, а также внедрения современных технических средств обеспечения сохранности и неизменности цифровой информации.

Важным направлением является также повышение квалификации следователей, дознавателей и судей в области информационных технологий, формирование единых стандартов работы с цифровыми доказательствами, обобщение и распространение положительного опыта правоприменения.

Цифровая трансформация уголовного судопроизводства — объективный процесс, требующий адекватного правового реагирования. Своевременное и качественное правовое регулирование использования цифровых доказательств позволит повысить эффективность уголовного судопроизводства, обеспечить защиту прав и законных интересов участников процесса, а также способствовать достижению целей правосудия.

Литература

1. Васюков В. Ф., Дамирчиев Э. о. Понятие и виды цифровой информации, используемой в доказывании по уголовным делам // Криминалистика: вчера, сегодня, завтра. 2025. №. 2. С. 38–50.

2. Ибрагимова Алиса Мансуровна Модернизация доказывания в уголовном судопроизводстве в условиях цифровой трансформации // Вестник Казанского юридического института МВД России. 2025. №3 (61). С. 106–114.

3. Корнакова С. В., Чигрина Е. В. Электронные доказательства в российском уголовном процессе: проблемные вопросы // Юридический вестник Самарского университета Juridical Journal of Samara University. 2025. Т. 11, № 2. С. 44–50.

4. Коровников Александр Леонидович, Василий Васильевич Колениченко Электронные доказательства в системе процессуальных источников доказательств в уголовном производстве // Государственная служба и кадры. 2023. №4. С. 244–247.

5. Костенко Р. В. Допустимость доказательств в цифровую эпоху: трансформация процессуальных стандартов — Юридический вестник Кубанского государственного университета. 2025. № 1. С 30–35.

6. Литвинова Ирина Викторовна, Допустимость электронных доказательств, полученных в результате проведения оперативно-разыскных мероприятий // Уголовное судопроизводство № 03/2023. С. 36–39.

7. Пономарев Виталий Евгеньевич Технико-криминалистическое обеспечение хранения электронных доказательств // Юридическая наука. 2024. №6. С. 316–320.

8. Рамалданов Х. Х. Проблемы использования и хранения цифровых доказательств в доказывании в уголовном процессе // Вестник Казанского юридического института МВД России. 2023. Т. 14. № 2 (52). С. 105–111.

9. Сидорова, Е. З., Грибунов, О. П. Особенности квалификации и предупреждения преступлений, совершаемых с использованием информационных (цифровых) технологий: учеб. пособие. Иркутск: Восточно-Сибирский институт МВД России, 2024. 128 с.

10. Черданцев А.Ю. Понятие цифровых доказательств, современное состояние и их роль в доказательственном процессе // Юридическая наука и практика. 2019. Т. 15. № 4. С. 55–60.

Problems of using digital evidence in criminal proceedings

Khavchaev Z.G.
Dagestan State University

This article discusses the theoretical and practical issues of using digital evidence in the criminal proceedings of the Russian Federation. The relevance of this topic is due to the rapid digital transformation of social relations and the increasing number of crimes committed using information and telecommunication technologies, which requires modernization of approaches to proof. The purpose of this research is to identify the problematic aspects of the legal regulation of the process of collecting, verifying, and evaluating digital evidence. Additionally, the research aims to develop proposals for improving the criminal procedure legislation in this area. The methodological basis of the study includes the dialectical method of scientific cognition, the formal-legal method, the comparative-legal method, the system-structural method, as well as the methods of analysis, synthesis, and generalization. The study substantiates the need for the legal definition of the concept of "digital evidence," the unification of the procedural order for their seizure and fixation, and the implementation of special measures to ensure the reliability and authenticity of digital information in the criminal process.

Keywords: digital evidence, criminal process, electronic information, proof, digital transformation.

References

1. Vasyukov V. F., Damirchiev E. o. THE CONCEPT AND TYPES OF DIGITAL INFORMATION USED IN EVIDENCE IN CRIMINAL CASES // Criminalistics: Yesterday, Today, Tomorrow. 2025. No. 2. Pp. 38–50.
2. Ibragimova Alisa Mansurovna MODERNIZATION OF EVIDENCE IN CRIMINAL PROCEEDINGS IN THE CONDITIONS OF DIGITAL TRANSFORMATION // Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2025. No. 3 (61). Pp. 106–114.
3. Kornakova S. V., Chigrina E. V. Electronic Evidence in the Russian Criminal Procedure: Problematic Issues // Juridical Journal of Samara University. 2025. Vol. 11, No. 2. Pp. 44–50.
4. Korovnikov Alexander Leonidovich, Vasily Vasilievich Kolenichenko Electronic Evidence in the System of Procedural Sources of Evidence in Criminal Proceedings // State Service and Personnel. 2023. No. 4. Pp. 244–247.
5. Kostenko R. V. Admissibility of Evidence in the Digital Age: Transformation of Procedural Standards — Legal Bulletin of the Kuban State University. 2025. No. 1. Pp. 30–35.
6. Litvinova Irina Viktorovna, Admissibility of Electronic Evidence Obtained as a Result of Operational Investigative Activities // Criminal Proceedings No. 03/2023. Pp. 36–39.
7. Ponomarev Vitaly Evgenievich, Technical and Criminalistic Support for the Storage of Electronic Evidence // Legal Science. 2024. No. 6. Pp. 316–320.
8. Ramaldanov Kh. Kh. Problems of using and storing digital evidence in proving in criminal proceedings // Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2023. Vol. 14. No. 2 (52). Pp. 105–111.
9. Sidorova, E. Z., Gribunov, O. P. Features of qualification and prevention of crimes committed using information (digital) technologies: textbook. manual. Irkutsk: East Siberian Institute of the Ministry of Internal Affairs of Russia, 2024. 128 p.
10. Cherdantsev A.Yu. The concept of digital evidence, the current state and their role in the evidentiary process // Legal Science and Practice. 2019. Vol. 15. No. 4. Pp. 55–60.