УДК 4414

КРИМИНАЛИСТИЧЕСКАЯ РЕКОНСТРУКЦИЯ СОБЫТИЙ ПО ЦИФРОВЫМ СЛЕДАМ: АНАЛИЗ ГЕОЛОКАЦИИ, ВРЕМЕННЫХ МЕТОК И ОБЛАЧНЫХ ДАННЫХ КАК ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ

Кочутов В.В.

студент,

Калужский государственный университет им. К.Э. Циолковского,

г. Калуга, Россия[1]

Краснов Е.Д.

студент,

Калужский государственный университет им. К.Э. Циолковского,

г. Калуга, Россия

Аннотация.

Настоящая статья посвящена комплексному анализу криминалистической реконструкции событий на основе цифровых следов, выступающих в качестве доказательственной информации. На основе анализа актуальной судебной практики, материалов уголовных дел и доктринальных исследований автор рассматривает доказательственный потенциал и структурные дефекты трех категорий цифровых следов: данных геолокации, временных меток и облачных данных. В статье обосновывается положение о цифровой информации как третьей специфической разновидности следовой информации, исследуется проблема точности координат и процедурных требований к их фиксации в контексте статей 74, 81 и 164.1 УПК РФ. Особое внимание уделяется разделению следов на пользовательские и автоматически генерируемые, а

[1] ***Научный руководитель**: Дроздов Д.Е.*
Доцент кафедры Юриспруденции; к.ю.н. Калужский государственный университет им. К.Э. Циолковского, г. Калуга, Россия

также проблеме допустимости данных, полученных с нарушением процессуального порядка. В заключении автором формулируются рекомендации по совершенствованию методики реконструкции, включая переход от изолированного анализа отдельных артефактов к многоисточниковой верификации.

Ключевые слова: цифровые следы, криминалистическая реконструкция, геолокация, временные метки, метаданные, облачные данные, электронные доказательства, УПК РФ, допустимость доказательств.

CRIMINALISTIC RECONSTRUCTION OF EVENTS BASED ON DIGITAL TRACES: ANALYSIS OF GEOLOCATION, TIMESTAMPS AND CLOUD DATA AS EVIDENTIARY INFORMATION

Kochutov V.V.
Student,
Kaluga State University named after K.E. Tsiolkovsky,
Kaluga, Russia[2]

Krasnov E.D.
Student,
Kaluga State University named after K.E. Tsiolkovsky,
Kaluga, Russia

Abstract.
This article is devoted to a comprehensive analysis of criminalistic reconstruction of events based on digital traces acting as evidentiary information. Drawing on current

[2] ***Scientific supervisor:*** *Drozdov D.E. Associate Professor of the Department of Jurisprudence; Candidate of Legal Sciences, Kaluga State University named after K.E. Tsiolkovsky, Kaluga, Russia*

judicial practice, criminal case materials and doctrinal research, the author examines the evidentiary potential and structural defects of three categories of digital traces: geolocation data, timestamps and cloud data. The article substantiates the proposition that digital information constitutes a third specific type of trace information, explores the problem of coordinate accuracy and procedural requirements for their fixation in the context of Articles 74, 81 and 164.1 of the Criminal Procedure Code of the Russian Federation. Particular attention is paid to the distinction between user-generated and automatically generated traces, as well as to the problem of admissibility of data obtained in violation of procedural order. In conclusion, the author formulates recommendations for improving reconstruction methodology, including a shift from isolated analysis of individual artifacts to multi-source verification.

Keywords: digital traces, criminalistic reconstruction, geolocation, timestamps, metadata, cloud data, electronic evidence, Criminal Procedure Code of the Russian Federation, admissibility of evidence.

Цифровизация общественных отношений изменила не только способы совершения преступлений, но и структуру следовой информации, доступной органам предварительного расследования. Традиционная криминалистическая реконструкция опиралась на материальные следы, локализованные в физическом пространстве, и идеальные следы, запечатленные в памяти участников события. Сегодня к ним добавился третий тип. Как обоснованно отмечают Д.В. Бахтеев и Е.В. Смахтин, цифровые следы не могут быть отнесены к идеальным, но и не в полной мере соответствуют характеристикам материальных следов: они представляют собой третью специфическую разновидность следовой информации, используемой в доказывании по уголовным делам [1, с. 12]. К числу их системных признаков авторы относят опосредованность, возможность копирования без утраты содержания,

одновременное существование нескольких копий на разных носителях, необходимость применения технических средств для восприятия и обезличенность [1, с. 10–11].

Актуальность темы обусловлена тем, что судебная практика уже активно использует данные геолокации, временные метки и облачные данные для установления обстоятельств преступлений, однако теоретическое осмысление пределов их доказательственной силы отстает от правоприменения. Как подчеркивают А.И. Кашапова и А.Г. Маркелов, цифровые следы обладают высокой информативностью и часто позволяют восстановить последовательность событий с точностью до секунды, однако для их эффективного применения требуется системная подготовка специалистов и унификация процессуальных процедур [2, с. 490]. При этом статистика неумолимо свидетельствует о росте преступности в цифровой среде: за январь–сентябрь 2023 года зарегистрировано 489,0 тыс. преступлений, совершённых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, тогда как за аналогичный период 2022 года — 378,5 тыс. [15, с. 273]. Как отмечает Х.Х. Рамалданов, преступность ушла в информационно-телекоммуникационную сеть Интернет, и собирать доказательственную базу по таким делам крайне затруднительно без применения цифровых технологий [15, с. 273]. Возникает фундаментальный вопрос: при каких условиях цифровой след действительно реконструирует событие, а при каких — лишь создает иллюзию точности?

Ключевая теоретическая проблема состоит в определении доказательственного статуса цифровых артефактов. Согласно ч. 1 ст. 74 УПК РФ, доказательствами по уголовному делу являются любые сведения, на основе которых суд, прокурор, следователь, дознаватель устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию [3]. При этом ч. 2 ст. 74 УПК РФ не предусматривает отдельного вида электронных (цифровых) доказательств, относя информацию на электронных носителях к вещественным

доказательствам (ст. 81 УПК РФ) либо к иным документам [1, с. 9; 3]. В этой связи в доктрине обоснованно ставится вопрос о необходимости законодательного закрепления понятия «цифровые доказательства»: как отмечает Н.И. Ревенко, анализируя монографию О.С. Кучина и Х.Х. Рамалданова, такое закрепление в УПК РФ будет способствовать упорядочению уголовно-процессуальных отношений [11, с. 120]. Авторы монографии также предлагают дополнить ст. 5 УПК РФ понятием «информационные технологии в уголовном судопроизводстве», поскольку закреплённое в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» определение (процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов) не учитывает специфику уголовно-процессуального доказывания [11, с. 121; 15, с. 274].

Между тем зарубежная доктрина акцентирует именно цифровую сущность рассматриваемых объектов: интерес вызывает в первую очередь сама цифровая информация, а не ее носитель [1, с. 9]. Как показывают В.А. Родивилина и В.В. Коломинов, международные стандарты, закрепленные, в частности, в ISO/IEC 27037:2012, устанавливают требования к идентификации, извлечению и сохранению цифровых доказательств, делая акцент на обязательном документировании всех операций — создании хеш-сумм, использовании write-blockers, ведении цепочки хранения [4, с. 218]. Показателен в этом смысле прецедент, рассмотренный федеральным окружным судом США (District of Maryland) по делу *Lorraine v. Markel American Insurance Co.* (2007), в котором суд сформулировал пятиэтапный тест допустимости электронных данных, сместив фокус с невозможности допросить «очевидца» создания каждой записи на проверку исправности и стандартности работы системы, генерирующей логи [4, с. 218]. При этом, как подчёркивает Н.И. Ревенко, одной из ключевых проблем внедрения цифровых технологий

остаётся аутентификация и идентификация полученной цифровой информации, а также её «недолговечность», в связи с чем предлагается законодательно закрепить порядок хранения цифровых доказательств и авторское определение «устойчивости цифровых доказательств в уголовном судопроизводстве» [11, с. 122]. Решение вопроса аутентификации возможно путём использования принципов, сформулированных Международной организацией по цифровым доказательствам (IOCE) [11, с. 122].

Как отмечают Д.А. Бадиков и А.В. Михайлова, современное уголовное судопроизводство переживает период фундаментальной трансформации, вызванной стремительным проникновением цифровых технологий во все сферы общественной жизни; традиционные методы расследования, основанные преимущественно на работе с материальными следами и свидетельскими показаниями, сегодня уже не могут в полной мере обеспечить эффективность раскрытия преступлений, значительная часть которых совершается в киберпространстве либо оставляет после себя характерный цифровой след [13, с. 1]. При этом цифровая трансформация в этой области представляет собой не просто техническое переоснащение правоохранительных органов, но глубокое изменение самой парадигмы доказывания, методов фиксации, изъятия и исследования информации [13, с. 2]. В этом контексте особое значение приобретают технологии лазерного сканирования и трёхмерного моделирования, позволяющие создать точную электронную копию места совершения преступления и подвергнуть её многократному исследованию, выполняя реконструкцию произошедшего без опасения утраты или трансформации исходной обстановки [13, с. 2]. Кроме того, большую роль играет внедрение беспилотных летательных аппаратов, которые позволяют производить аэрофотосъёмку и видеомониторинг больших территорий, предоставляя объективные данные, получить которые в ходе традиционного осмотра затруднительно [13, с. 2].

Данные геолокации обладают интуитивной убедительностью: координата, извлеченная из телефона или сообщения, кажется прямым указанием на факт присутствия в определенной точке пространства. Кашапова и Маркелов относят геолокацию к следам, охватывающим метаданные, IP-адреса, историю браузера и переписку, формирующим уникальный информационный профиль личности [2, с. 489]. Бадиков и Михайлова также выделяют использование данных геолокации, логов соединений и информации из облачных хранилищ в качестве одного из ключевых направлений перехода от традиционных методов фиксации доказательств к цифровым [13, с. 1].

Согласно п. 2 ст. 2 Федерального закона от 14.02.2009 № 22-ФЗ «О навигационной деятельности», под средствами навигации понимаются технические средства, устройства и системы, предназначенные для формирования навигационных сигналов, передачи, приёма, обработки, хранения и визуализации навигационной информации [14, с. 1]. Как отмечает В.Ю. Кузовлев, широчайшие возможности для установления пространственно-временных характеристик события преступления открываются благодаря использованию современных средств навигации [14, с. 2]. В диссертационном исследовании Н.Ю. Дусевой обозначен ряд тактических задач, решение которых основано на использовании пространственно-временной информации: установление фигурантов и возможных свидетелей преступления; розыск лиц; установление места и обстоятельств совершения преступления; установление средств совершения преступления; установление алиби лица; розыск похищенного [14, с. 2]. По мнению В.Ю. Кузовлева, данный перечень может быть расширен за счёт таких задач, как: установление факта и времени нахождения лица в определённом месте и маршрута его движения; проверка показаний о месте и времени определённого события; установление длительности нахождения лица в определённом месте; проверка факта совместного нахождения разных лиц [14, с. 2].

Решение указанных задач возможно посредством анализа данных контента картографических приложений, имеющихся в программном обеспечении большинства современных смартфонов, с помощью, в частности, аппаратно-программного комплекса UFED (производство компании Cellebrite, Израиль), используемого в практической деятельности экспертно-криминалистических подразделений органов внутренних дел, криминалистических подразделений Следственного комитета РФ и других правоохранительных органов [14, с. 2]. Повышению эффективности работы по выдвижению и проверке следственных версий способствуют такие аналитические возможности комплекса UFED, как: совместное отображение маршрутов передвижения разных лиц в определённый промежуток времени на единой картографической основе; восстановление хронологии событий по имеющимся данным геолокации; установление точного времени и даты посещения лицом определённого объекта (места); систематизация данных геолокации для их аналитической обработки за счёт группировки массивов данных по месту, времени, типам месторасположения, расстоянию и другим критериям [14, с. 3].

Судебная практика подтверждает востребованность таких данных. Так, Псковским районным судом Псковской области (приговор от 11 июня 2025 г. по делу № 1-44/2025) были исследованы данные о геолокации, однако в данном конкретном деле они не стали основным доказательством [12]. В деле, рассмотренном Ленинским районным судом г. Омска (приговор от 20 февраля 2024 г. по делу № 1-24/2024), координаты, отправленные в мессенджере, послужили основанием для обнаружения тайника с наркотическим средством: подсудимые получили неверные координаты, после введения исправленных место было найдено [5]. В деле, рассмотренном Советским районным судом г. Омска (постановление от 29 апреля 2026 г. по делу № 1-3/2026), протокол осмотра телефона зафиксировал поисковый запрос с координатами, а

последующая проверка участка местности с использованием навигатора подтвердила их соответствие реальному расположению тайника [6].

Показательно, что в доктрине уже предлагается введение нового процессуального действия — получения информации о географических координатах места нахождения (геолокации) абонента, транспортного средства и (или) абонентского устройства [11, с. 121; 15, с. 275]. Как отмечает Н.И. Ревенко, авторы монографии О.С. Кучин и Х.Х. Рамалданов обосновывают необходимость дополнения УПК РФ таким процессуальным действием, а также видеопротоколированием следственного эксперимента, обыска и проверки показаний на месте [11, с. 121]. Эти предложения напрямую связаны с проблемой процедурной легитимации геолокационных данных, которые в настоящее время получаются в рамках иных следственных действий без специально предусмотренной процессуальной формы. Х.Х. Рамалданов также обосновывает необходимость дополнения ст. 177 УПК РФ частью, содержащей порядок применения технологий цифрового компьютерного моделирования при проведении осмотра, что позволит создавать объёмную модель места происшествия, транспортного средства, участка местности и использовать её при производстве судебной экспертизы [15, с. 275].

Однако за видимой простотой скрывается многослойная проблема точности. Координаты, полученные от мониторингового оборудования, могут носить приблизительный характер: на определение координат влияют недостаточный уровень сигнала GPS и характер местности [7]. Более того, координаты в свойствах фотоизображения могут отсутствовать вовсе: в деле, рассмотренном Псковским районным судом Псковской области (приговор от 29 января 2025 г. по делу № 1-44/2025), при осмотре телефона было установлено, что в свойствах фотографий участков лесного массива данные о геолокации не имеются, хотя скриншот карты с координатами сохранился отдельно [8].

Процедурный аспект не менее важен. Родивилина и Коломинов приводят показательные примеры из судебной практики: Курганский областной суд в

апелляционном определении от 24 августа 2021 г. по делу № 22-1169/2021 признал распечатки электронной переписки недопустимым доказательством, указав, что «процесс изъятия… надлежащим образом не задокументирован, не указано, с помощью каких технических средств, какого программного обеспечения осуществлялось изъятие» [4, с. 221]. Аналогично Президиум Московского областного суда постановлением от 17 февраля 2021 г. № 44У-16/2021 исключил скриншоты как доказательство, поскольку «не приведено данных о программном обеспечении, с помощью которого они были получены» [4, с. 221]. Эти прецеденты демонстрируют, что допустимость автоматических данных определяется не их содержанием, а соблюдением формализованной процедуры извлечения, обеспечивающей аутентичность и целостность. Согласно ч. 1 ст. 164.1 УПК РФ, изъятие электронных носителей информации не допускается, за исключением случаев, когда вынесено постановление о назначении судебной экспертизы, изъятие производится на основании судебного решения, либо на носителях содержится информация, полномочиями на хранение которой владелец не обладает [9]. Несоблюдение указанных требований является основанием для признания доказательств недопустимыми [9].

Реконструкция события невозможна без установления последовательности действий, и временные метки файлов представляются естественным инструментом для этой задачи. Родивилина и Коломинов относят временные и пространственные метки к содержательной группе электронно-цифровых следов и подчеркивают, что автоматические следы обладают высокой детализацией временных меток [4, с. 219, 221]. Однако судебная практика демонстрирует систематические проблемы, связанные с их интерпретацией. В деле, рассмотренном Псковским районным судом Псковской области (приговор от 29 января 2025 г. по делу № 1-44/2025), специалист, допрошенный по ходатайству защиты, перечислил технические причины, при которых дата последнего изменения файла может

предшествовать дате его создания: копирование или перенос файла, восстановление из резервной копии, ручное изменение временных меток, особенности файловой системы, влияние вредоносного программного обеспечения, проблемы с системными часами [8]. Тот же специалист указал, что внутренние текстовые даты документа «не являются независимым доказательством времени создания» и приобретают достоверность только при согласованности с другими данными — системными метаданными, внешними событиями, журналами [8].

Показательно, что в указанном деле протокол осмотра не зафиксировал сведений о настройках операционной системы, установленном офисном пакете и о том, проводилась ли валидация метаданных путем сопоставления с другими артефактами [8]. Это означает, что даже при наличии технической возможности проверки следователь может ею не воспользоваться, и тогда временная метка остается неверифицированной. Аналогичная осторожность прослеживается в экспертной практике: эксперт не может утверждать, что графический файл создан на конкретном устройстве в указанную дату, поскольку дата в свойствах файла отражает настройки устройства, а не объективное время. В деле, рассмотренном Псковским районным судом Псковской области (приговор от 17 августа 2025 г. по делу № 1-90/2025), суд исследовал заключение эксперта, согласно которому дата в свойствах файла отражает настройки устройства, а не объективное время; если на телефоне установлена неверная дата, файл будет содержать именно ее [10].

Отсюда следует методологический вывод: изолированная временная метка не обладает самостоятельной доказательственной силой. Реконструкция временной оси события должна опираться на корреляцию нескольких независимых источников — журналов событий операционной системы, логов приложений, данных оператора связи, записей видеонаблюдения. В этом контексте предложение о введении обязательного видеопротоколирования следственных действий (следственного эксперимента, обыска, проверки

показаний на месте) приобретает дополнительный смысл: видеозапись создаёт независимый временной маркер, который может быть сопоставлен с временными метками цифровых артефактов [11, с. 121]. Кроме того, технологии трёхмерного моделирования места происшествия позволяют зафиксировать пространственно-временные характеристики обстановки с точностью, недоступной традиционному протоколированию, и впоследствии неоднократно обращаться к электронной копии для проверки версий о последовательности событий [13, с. 2; 15, с. 275].

Облачные данные представляют наибольшую сложность для криминалистической реконструкции, поскольку разрывают связь между физическим носителем и содержащейся информацией. Бахтеев и Смахтин отмечают, что физическое нахождение следа на электронных носителях не исключает их виртуального нахождения в облачных сервисах; поскольку непосредственное изъятие таких следов практически невозможно, они не рассматриваются в классификации по месту нахождения, однако их копирование в ходе следственного действия не исключено [1, с. 12–13]. Родивилина и Коломинов классифицируют электронно-цифровые следы по месту фиксации на следы на устройствах пользователя и на удаленных серверах (облачных хранилищах, корпоративных системах) [4, с. 219]. Бадиков и Михайлова подчеркивают, что работа с цифровыми носителями информации и данными, изначально существующими в электронной форме, включает не только компьютерную технику и мобильные устройства, изъятые у подозреваемого, но и огромные массивы данных, генерируемых телекоммуникационными компаниями, провайдерами интернет-услуг и владельцами интернет-платформ [13, с. 2].

Проблема допустимости облачных данных имеет два измерения. Первое — правомерность доступа. Кашапова и Маркелов подчеркивают, что изъятие электронных носителей может быть произведено только на основании постановления следователя, а в случаях, когда требуется удаленный доступ, —

по судебному решению, что обеспечивает соблюдение ст. 23 Конституции РФ, гарантирующей тайну переписки и иных сообщений [2, с. 488]. Второе измерение — целостность данных. Как указывают Кашапова и Маркелов, в 2023–2025 годах МВД РФ и Роскомнадзор утвердили «Методические рекомендации по сбору и фиксации цифровых доказательств», где описаны требования к работе с такими материалами: обязательное составление протоколов, фиксация хэшей (SHA-256, MD5) и временных меток, сохранение цепочки хранения доказательств [2, с. 489]. Если облачная информация извлечена и сохранена без фиксации хеш-сумм, без протоколирования времени и способа извлечения, защита вправе ставить под сомнение ее тождественность исходной. Как отмечает Н.И. Ревенко, именно вопросы аутентификации и идентификации цифровой информации, а также её «недолговечности» относятся к числу ключевых проблем, требующих законодательного решения [11, с. 122].

Особую сложность представляет работа с автоматически формируемыми следами, которые являются следствием воздействия технологических процессов без участия человека. Родивилина и Коломинов отмечают, что такие следы, при корректном изъятии, могут обладать высокой доказательственной ценностью, однако их непроизвольный характер вызывает сомнения у следственных органов и судов относительно подлинности [4, с. 220]. Совпадение копий координат и фотографий тайников на устройстве отправителя, получателя и в облачных резервных копиях мессенджеров, зафиксированное в протоколах осмотра по делу, рассмотренному Ленинским районным судом г. Омска (приговор от 20 февраля 2024 г. по делу № 1-24/2024), усиливает доказательственную силу каждой из них [5]. Напротив, расхождение или отсутствие одной из копий создает пространство для защиты.

Для обеспечения подлинности цифровых доказательств и неизменности данных с момента их изъятия в доктрине предлагается использовать технологии блокчейн (распределённого реестра), которые могут применяться

для фиксации цепи хранения цифрового доказательства, делая любую попытку внесения изменений очевидной для всех субъектов процесса [13, с. 3]. Как отмечают Бадиков и Михайлова, проблема сохранения подлинности доказательств, полученных цифровым способом, является одной из наиболее серьёзных, поскольку в электронный файл, в отличие от физического объекта, достаточно несложно внести изменения [13, с. 3]. Кроме того, одним из проблемных вопросов остаётся обеспечение информационной безопасности и соблюдение прав граждан при накоплении электронной информации в целях раскрытия и расследования преступной деятельности [13, с. 3]. В этом контексте заслуживает внимания предложение Х.Х. Рамалданова об использовании блокчейн-технологий в рамках электронного уголовного дела, что обеспечит прозрачность проводимых процессуальных действий, исключит фальсификацию доказательств, сократит издержки и сроки [15, с. 275]. Оценка цифровых доказательств, по мнению автора, возможна с помощью искусственного интеллекта под контролем лиц, осуществляющих предварительное расследование [15, с. 275].

Проведенный анализ позволяет сформулировать несколько выводов. Во-первых, криминалистическая реконструкция по цифровым следам не может строиться на презумпции точности технических данных: геолокация имеет погрешность, временные метки подвержены искажениям, облачные данные зависимы от процедуры доступа. Во-вторых, доказательственная сила цифрового следа определяется не его типом, а качеством его верификации. В-третьих, модель распределенного цифрового следа «устройство – сеть – приложение – аккаунт – облако – провайдер» должна стать методологической основой реконструкции. Как подчеркивают Бахтеев и Смахтин, необходимо комплексное исследование рассматриваемых следов как уголовно-процессуальными, так и криминалистическими методами [1, с. 13]. Как отмечают Бадиков и Михайлова, цифровая трансформация расследования является объективной необходимостью, требующей одновременного развития

технологий и совершенствования правового регулирования [13, с. 1]. Х.Х. Рамалданов, в свою очередь, указывает, что решение уголовно-процессуальных проблем применения цифровых технологий с учётом сегодняшних реалий слабо затронуто достижениями научно-технического прогресса, и подчёркивает необходимость законодательного закрепления определения информационных технологий в уголовном судопроизводстве [15, с. 273–274].

Для совершенствования практики представляется необходимым: закрепление в методических рекомендациях требования фиксировать при осмотре устройства настройки геолокации, системное время и версии приложений; обязательная кросс-валидация временных меток с журналами событий; документирование способа доступа к облачным данным с указанием правового основания и хеш-сумм извлеченных файлов. Родивилина и Коломинов предлагают также разработать национальные методические рекомендации для экспертов и следователей, закрепить обязательность протоколирования программно-технических средств, используемых при извлечении следов, и ввести экспертную оценку степени автоматичности и подверженности модификации каждого цифрового следа [4, с. 222]. Кучин и Рамалданов, в свою очередь, обосновывают необходимость дополнения УПК РФ новыми процессуальными действиями — получением информации о геолокации и видеопротоколированием следственного эксперимента, обыска и проверки показаний на месте, а также дополнения ст. 177 УПК РФ положением о цифровом компьютерном моделировании при осмотре [11, с. 121; 15, с. 275]. Бадиков и Михайлова указывают на необходимость обновления профессиональной подготовки сотрудников правоохранительных органов и обеспечения информационной безопасности при сборе электронной информации [13, с. 1]. Только при соблюдении этих условий цифровой след превращается из технического артефакта в полноценное доказательство, способное выдержать состязательную проверку в суде.

Библиографический список:

1. Бадиков, Д. А. К вопросу об использовании цифровых технологий в расследовании преступлений / Д. А. Бадиков, А. В. Михайлова // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2026. – № 1. – С. 1–4.

2. Бахтеев, Д. В. Криминалистические особенности производства процессуальных действий с цифровыми следами / Д. В. Бахтеев, Е. В. Смахтин // Российский юридический журнал. – 2019. – № 6 (129). – С. 61–68.

3. Кашапова, А. И. Цифровой след как инструмент раскрытия преступлений в условиях киберреальности / А. И. Кашапова, А. Г. Маркелов // Вестник науки. – 2025. – № 12 (93). – Т. 2. – С. 487–492.

4. Кузовлев, В. Ю. Использование возможностей средств навигации в установлении обстоятельств совершения преступлений / В. Ю. Кузовлев // Известия Тульского государственного университета. Экономические и юридические науки. – 2017. – № 4-2. – С. 159–163.

5. Постановление Советского районного суда г. Омска от 29 апреля 2026 г. по делу № 1-3/2026 // SudAct : [сайт]. – URL: (дата обращения: 10.11.2026).

6. Приговор Ленинского районного суда г. Омска от 20 февраля 2024 г. по делу № 1-24/2024 // SudAct : [сайт]. – URL: (дата обращения: 10.11.2026).

7. Приговор Псковского районного суда Псковской области от 22 октября 2024 г. по делу № 1-145/2024 // SudAct : [сайт]. – URL: (дата обращения: 10.11.2026).

8. Приговор Псковского районного суда Псковской области от 29 января 2025 г. по делу № 1-44/2025 // SudAct : [сайт]. – URL: (дата обращения: 10.11.2026).

9. Приговор Псковского районного суда Псковской области от 11 июня 2025 г. по делу № 1-44/2025 // SudAct : [сайт]. – URL: (дата обращения: 10.11.2026).

10. Приговор Псковского районного суда Псковской области от 17 августа 2025 г. по делу № 1-90/2025 // SudAct : [сайт]. – URL: (дата обращения: 10.11.2026).

11. Рамалданов, Х. Х. Влияние информационных технологий на процесс доказывания в уголовном судопроизводстве / Х. Х. Рамалданов // Пробелы в российском законодательстве. – 2023. – Т. 16, № 7. – С. 273–279.

12. Ревенко, Н. И. Использование цифровых технологий в уголовно-процессуальном доказывании / Н. И. Ревенко // Вестник Омского университета. Серия «Право». – 2026. – Т. 23, № 2. – С. 120–122.

13. Родивилина, В. А. Электронно-цифровые следы как доказательства при расследовании интернет-мошенничеств: криминалистические и процессуальные аспекты / В. А. Родивилина, В. В. Коломинов // Вестник Восточно-Сибирского института МВД России. – 2026. – № 1 (116). – С. 214–227.

14. Уголовно-процессуальный кодекс Российской Федерации : федеральный закон от 18.12.2001 № 174-ФЗ (с последними изменениями и дополнениями) // Собрание законодательства РФ. – 2001. – № 52 (ч. I). – Ст. 4921.

15. Уголовно-процессуальный кодекс Российской Федерации. Статья 164.1. Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий // СПС «КонсультантПлюс». – URL: (дата обращения: 10.11.2026).