УДК 343.1

НАУЧНЫЙ ЖУРНАЛ
«БИЗНЕС И ОБЩЕСТВО»

Аршинов Иван Иванович

студент специалитета
Московский государственный юридический
университет имени О. Е. Кутафина
Москва, Россия

ГРАНИЦЫ ДОПУСТИМОСТИ ЦИФРОВЫХ СЛЕДОВ: ДОКАЗЫВАНИЕ ПРЕСТУПЛЕНИЙ В ЭПОХУ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И КРИПТОАКТИВОВ

Аннотация

Анализируются проблемы использования цифровых доказательств в российском уголовном процессе на фоне распространения искусственного интеллекта и криптоактивов. Отмечается отсутствие чётких дефиниций электронных доказательств в УПК РФ, что приводит к противоречиям в судебной практике. Рассматриваются особенности доказывания по делам, связанным с цифровыми активами и преступлениями, совершёнными с применением ИИ, а также вопросы допустимости и достоверности электронных улик. Обосновывается необходимость законодательного закрепления статуса и порядка обращения с цифровыми доказательствами. Предлагаются меры по совершенствованию законодательства и международного сотрудничества для эффективного расследования цифровых преступлений.

Ключевые слова: цифровые следы, искусственный интеллект, криптоактивы

Введение. В последние годы цифровые технологии, включая искусственный интеллект и криптоактивы, оказывают значительное влияние на трансформацию преступной деятельности и правоприменительной практики. Российское уголовное и уголовно-процессуальное законодательство сталкивается с необходимостью оперативной адаптации к новым угрозам, связанным с возникновением принципиально новых способов совершения преступлений. Законодательные инициативы, такие как проект № 8854948, отражают возрастающую обеспокоенность общества и государства опасностью цифровых преступлений и актуализируют вопросы доказывания и оценки цифровых следов. Однако действующая нормативная база пока не содержит четких и исчерпывающих положений относительно электронных доказательств, что приводит к неоднозначности судебной практики и затрудняет эффективное противодействие киберпреступлениям.

Цель исследования. Целью исследования является анализ актуальных проблем процессуального порядка сбора, изъятия, оценки и использования цифровых доказательств в российском уголовном процессе. Особое внимание уделяется вопросам допустимости, достоверности и достаточности электронных доказательств, а также необходимости их нормативного закрепления с учётом современных цифровых реалий. Материал и методы исследования В качестве основного материала использованы положения действующего уголовно-процессуального законодательства

Российской Федерации, включая статьи УПК РФ, а также проекты нормативных актов, в частности законопроект № 8854948. Анализируются практические теоретические разработки в области определения статуса электронных носителей и данных. Методологическую основу исследования составляют формально-юридический, сравнительно-правовой и аналитический методы, позволяющие выявить ключевые проблемы и тенденции в области уголовно-процессуального доказывания цифровых преступлений.

Результаты исследования. В российском уголовном процессе отсутствуют чёткие определения и процедуры обращения с цифровыми доказательствами, что усложняет их использование в делах, связанных с искусственным интеллектом и криптовалютами. Для цифровых следов важны критерии законности получения, достоверности, а также фиксация технических параметров (например, хеш-суммы, версия ПО, время создания файла). Особую сложность вызывает идентификация личности при анонимных криптовалютных транзакциях, а также получение данных с зарубежных платформ. Необходимы законодательное закрепление статуса электронных доказательств, разработка четких правил их сбора и обработки, создание специализированных экспертных центров и совершенствование международного взаимодействия. Это позволит повысить качество расследования цифровых преступлений и надежность использования электронных доказательств.

Внедрение цифровых технологий, включая искусственный интеллект и криптоактивы, стремительно трансформирует как преступную деятельность, так и саму правоприменительную практику. Российское уголовное и уголовно-процессуальное законодательство вынуждено адаптироваться к новым угрозам, связанным с возникновением совершенно новых способов совершения преступлений. Примером служит законопроект № 8854948, внесённый в Госдуму в апреле 2025 года, который предлагал признать использование искусственного интеллекта в преступных целях отягчающим обстоятельством [7]. Несмотря на возврат на доработку, сама инициатива иллюстрирует растущую обеспокоенность законодателя общественной опасностью цифровых преступлений. Однако реагирование на эти вызовы невозможно без фундаментального пересмотра принципов доказывания и оценки цифровых следов, охватывающих как электронные данные, связанные с ИИ, так и криптовалютные транзакции.

В уголовном процессе вопросы допустимости, относимости, достоверности и достаточности цифровых доказательств приобретают особую сложность. В действующем Уголовно-процессуальном кодексе Российской Федерации [8] до сих пор отсутствуют чёткие дефиниции понятий «электронные доказательства», «электронный документ», «электронный носитель», несмотря на упоминания в отдельных статьях (п. 4 ст. 81, ст. 164.1, ст. 474.1 УПК РФ). Это обстоятельство порождает неоднозначность в судебной практике, в особенности применительно к новым цифровым реалиям. В доктрине отмечается, что электронные доказательства — это сведения о юридически значимых обстоятельствах, зафиксированные на цифровых, звуковых, видео- или иных носителях и предназначенные для передачи с использованием технических средств [1]. Проблема заключается в том, что электронные носители зачастую рассматриваются как лишь технический посредник, в то время как материальные доказательства традиционно определяются физическим объектом, а не только содержащейся на нём информацией.

Необходимость законодательного закрепления категории электронных доказательств связана с принципиальным отличием цифровых следов от традиционных: они формируются не только посредством физических процессов, но и программным обеспечением, что приводит к появлению идеальных следов, существующих лишь в информационной плоскости. На практике возникает дилемма: считать ли такими доказательствами только информацию, зафиксированную в определённой форме (файл, запись, транзакция), или также материальный носитель (сервер, аппаратный кошелёк, карта с ключом). В современной российской правоприменительной практике применяется смешанный подход — цифровые данные могут быть признаны как «иными документами» (ст. 84 УПК РФ) [3], так и вещественными доказательствами (ст. 81 УПК РФ), если речь идёт, например, об аппаратных криптокошельках или носителях seed-фраз.

Законность получения доказательства – это краеугольный принцип, нашедший закрепление в ст. 7 УПК РФ. Любое цифровое доказательство, будь то выгрузка транзакций из блокчейна, копия файла нейросетевой модели или скриншот диалога, может быть признано недопустимым при нарушении процессуальной формы. Судебная практика уже сталкивалась со случаями исключения значимых цифровых файлов из материалов дела из-за нарушений при изъятии, копировании или хранении [4]. Поэтому сегодня особое значение приобретают процедуры фиксации неизменности

файлов, а именно хеш-суммы, указание версии программного обеспечения, времени создания образа, привлечение специалиста при копировании [6]. В случае нарушения любого из этапов возникает риск признания доказательства недопустимым, что особо актуально для преступлений совершенных с помощью криптовалюты, где цепочка транзакций и контроль над кошельком должны быть достоверно привязаны к личности подозреваемого.

Следующий ключёвой критерий – это достоверность, включающая аутентичность, неизменность и подлинность цифровых материалов. Для дел, связанных с искусственным интеллектом, особую сложность вызывает проверка фрагментов аудио-видеоконтента, способных быть созданными нейросетями. Судебная экспертиза подобных материалов часто опирается на вероятностные признаки, такие как особенности алгоритмов сжатия или регулярность шумов, однако технические возможности создания реалистичных фальсификаций зачастую опережают развитие средств их распознавания [6]. Поэтому при возникновении обоснованных сомнений в подлинности цифрового доказательства бремя доказывания его достоверности законом возлагается на сторону обвинения, а любое неустранимое сомнение толкуется в пользу обвиняемого, в полном соответствии с презумпцией невиновности (ст. 14 УПК РФ).

Специфика криптовалютных дел проявляется в необходимости не только доказать факт существования и движения активов, но и их связь с обвиняемым. Блокчейн предоставляет формально неизменяемую хронологию транзакций, однако для уголовно-процессуального доказывания требуются дополнительные подтверждения: установление владельца ключей или адреса-идентификатора, привязка к IP-адресу или устройству, сопоставление с перепиской или другим образом идентификации личности. Сами по себе анонимные транзакции не обеспечивают достаточности доказательств, так как не устанавливают умысел или контроль над активом. Бремя доказывания этих обстоятельств лежит полностью на стороне обвинения. Только в случае доказанности цепочки событий, а именно создание или получение ключа, выполнение транзакции, пользование криптовалютой возможно говорить о достаточности совокупности признаков доказательства (ст. 88 УПК РФ).

Отдельной сложностью являются доказательства, размещённые на зарубежных облачных платформах и сервисах [5]. Без правовой помощи иностранного государства получить доступ к журналам действий или исходным моделям искусственного

интеллекта затруднительно, а неофициальное получение таких данных влечёт нарушение процессуальных требований и риск их признания недопустимыми. Для обеспечения полноты и допустимости цифровых доказательств требуется ускорение международного сотрудничества и унификация методик их оценки. Однако в условиях современной геополитической напряженности такие меры представляются малореализуемыми.

Ключевым понятием, характеризующим криптопреступления, становится «цифровая валюта» – совокупность электронных данных, которая одновременно служит и средством расчёта, и объектом преступного посягательства. Оборот криптоактивов в России регулируется Федеральным законом №259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [9]. Согласно ФЗ, российским юридическим лицам и резидентам запрещается принимать цифровую валюту в качестве оплаты за товары и услуги, а владение адресом-идентификатором цифровой валюты должно быть зафиксировано и при необходимости предоставлено государственным органам по запросу. Эти нормативные ограничения напрямую влияют на формирование доказательственной базы по делам о криптопреступлениях. При доказывании противоправности способа совершения преступления (например, при оплате преступного товара криптовалютой) обязательным становится установление факта нарушения установленного запрета - этот признак приобретает юридически значимое значение для квалификации события и способа совершения преступления.

Из изложенного следует, в российской системе требуется не только нормативное закрепление понятия и режима электронных доказательств, но и процессуальная детализация механизма их сбора, изъятия и копирования. Ключевые рекомендации, вытекающие из анализа практики и доктрины: введение в УПК РФ отдельной статьи об электронных доказательствах с определением их статуса и источников; расширение главы 25 УПК РФ положениями о копировании и изъятии электронных носителей с чёткой регламентацией участия специалистов и фиксации технических параметров; создание при Минюсте РФ специального центра по утверждению и ведению открытого реестра методик цифровой экспертизы; а также совершенствование механизмов международного сотрудничества в целях получения доказательств из зарубежных облачных сервисов. Очевидно, что к цифровым следам,

независимо от их природы, должны применяться общие критерии относимости, допустимости и достоверности, закреплённые в УПК РФ. Эффективность расследования и справедливость процесса возможны только при комплексном анализе как цифровых, так и традиционных доказательств, при строгом соблюдении процессуальных правил их сбора и оформления. Недостаточность, недопустимость или спорность ключевого цифрового доказательства могут помешать установлению не только специальных признаков, но и самого факта преступления.

Только при условии единых, чётко определённых критериев относимости, допустимости и достоверности, а также строгого соблюдения процессуальных стандартов, цифровые доказательства смогут выполнять свою функцию в уголовном процессе, обеспечивая достижение целей справедливого правосудия.

Список использованных источников

1. Александров А. С. Проблемы теории уголовно-процессуального доказывания, которые надо решать в связи с переходом в эпоху цифровых технологий // Судебная власть и уголовный процесс. 2018. № 2. С. 133-148. EDN: XWCHZB.

2. Батоев В. Б., Юможапов Р. С. Использование технологий искусственного интеллекта в выявлении видеодипфейков // Вестник Краснодарского университета МВД России. 2023. № 3 (61). С. 76-81. EDN: SYZWCV.

3. Вехов В. Б. Электронные доказательства: проблемы теории и практики // Правопорядок: история, теория, практика. 2016. № 4 (11). С. 46-50. EDN: XXXCNP.

4. Воронин М. И. Особенности оценки электронных (цифровых) доказательств // Актуальные проблемы российского права. 2021. № 8 (129). С. 118-128. DOI: 10.17803/1994-1471.2021.129.8.118-128. EDN: NCPIRV.

5. Лаптев В. А., Соловяненко Н. И. «Судебное облако»: правовые вопросы структурирования и защиты данных // Актуальные проблемы российского права. 2019. № 6. С. 195–204. DOI: 10.17803/1994-1471.2019.103.6.195-204. EDN: YQCYXJ.

6. Россинская Е. Р., Сааков Т. А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). С. 106-123. DOI: 10.24411/2587-9820-2020-10060. EDN: YKCUUH.

7. Законопроект № 885494–8 «О внесении изменения в статью 63 Уголовного кодекса Российской Федерации» // Система обеспечения законодательной

деятельности. URL: https://sozd.duma.gov.ru/bill/885494-8, (дата обращения: 20.04.2025).

8. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 05.12.2022) (с изм. и доп., вступ. в силу с 26.12.2022) // «Российская газета» от 22 декабря 2001 г. № 249.

9. Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. — 2020. — № 31 (ч. I). — Ст. 5018.