УДК 343

Ихтияров У.

студент

Высшая школа юриспруденции и судебно-технической экспертизы

Санкт-Петербургский политехнический университет Петра Великого

(г. Санкт-Петербург, Россия)

ЦИФРОВЫЕ СЛЕДЫ КАК ДОКАЗАТЕЛЬСТВА В УГОЛОВНОМ ПРОЦЕССЕ: ПРОБЛЕМЫ ДОПУСТИМОСТИ И ПРОЦЕССУАЛЬНОГО ЗАКРЕПЛЕНИЯ

Аннотация: *в данной статье рассматриваются различные подходы к определению правовой природы цифровых следов, выявляются пробелы в законодательстве, регулирующем работу с электронными носителями информации, а также анализируются формирующиеся судебные практики. Целью настоящего исследования является выявление и систематический анализ теоретических и практических проблем, связанных с признанием цифровых следов в качестве судебных доказательств. Исследование основано на сочетании общенаучных методов, в том числе диалектического, системно-структурного и формально-логического анализа, а также специализированных методов, таких как формально-юридический анализ, сравнительно-правовой анализ и анализ судебной практики. Результаты исследования показывают, что основными препятствиями для эффективного использования цифровых доказательств являются отсутствие юридического определения понятия «электронные доказательства» в Уголовно-процессуальном кодексе Российской Федерации, формальный подход к оценке их допустимости в правоприменительной практике, технические трудности, связанные с обеспечением неизменности и подлинности данных, а также отсутствие процессуальных механизмов для извлечения информации, которая существует исключительно в виртуальной среде, например в облачных сервисах или на удаленных серверах. Результаты исследования представляют интерес для законодательной деятельности, направленной на совершенствование уголовно-процессуального законодательства, а также могут быть использованы на практике следователями, адвокатами и судьями при разработке единых стандартов работы с цифровыми следами.*

Ключевые слова: *уголовный процесс, цифровой след, электронное доказательство, допустимость доказательств, процессуальное закрепление, электронный носитель информации, доказывание, цифровизация правосудия.*

ВВЕДЕНИЕ.

Современный этап общественного развития характеризуется повсеместным внедрением цифровых технологий во все сферы человеческой деятельности, что оказывает значительное влияние на способы передачи и хранения информации. Актуальность данного исследования обусловлена тем, что информационно-телекоммуникационные сети, мобильные устройства и различные электронные носители стали не только средствами передачи данных, но и платформами для фиксации событий, имеющих юридическое значение. В сфере уголовного судопроизводства цифровизация проявляется в появлении новых видов доказательств и необходимости адаптировать традиционные правовые инструменты к современной технологической реальности. С одной стороны, цифровые следы, оставленные людьми, предоставляют правоохранительным органам беспрецедентные возможности для установления объективной истины и реконструкции хода событий. С другой стороны, уголовно-процессуальное право, отличающееся высокой степенью консервативности, сталкивается с необходимостью пересмотра и модернизации своих основополагающих институтов в связи с технической сложностью и изменчивостью цифровой среды [1].

В настоящее время использование цифровых доказательств является центральной темой научных дискуссий и юридической практики. Как справедливо отмечает профессор Е.П. Россинская «хотя феномен цифровых доказательств не является принципиально новым для правовой доктрины, формирование системного подхода к их применению на практике только начинается и сопряжено со значительными трудностями» [2]. Уголовно-процессуальный кодекс Российской Федерации предпринимает активные, но пока ограниченные шаги в направлении цифровизации процесса доказывания, что приводит к неоднозначности и противоречиям, связанным с признанием цифровых следов допустимыми доказательствами и обеспечением их надлежащей процессуальной формы [3].

Каждый год российские суды рассматривают множество уголовных дел, связанных с информацией, полученной с мобильных телефонов, компьютеров, из мессенджеров, социальных сетей и других цифровых платформ. Однако до сих пор не существует единых критериев или комплексной практики оценки таких доказательств.

Цель этого исследования — провести комплексный анализ основных проблем, связанных с использованием цифровых следов в системе уголовного правосудия, и предложить эффективные решения. Для достижения этой цели необходимо решить следующие задачи: проанализировать правовую природу цифровых следов и их статус в отечественном уголовно-процессуальном законодательстве, выявить пробелы и недостатки в процессуальном регулировании сбора и систематизации цифровых доказательств, провести детальный анализ существующей судебной практики оценки допустимости цифровых материалов, сформулировать обоснованные рекомендации и конкретные предложения по совершенствованию нормативно-правовой базы с учетом современных технологических условий. Это комплексное исследование необходимый шаг на пути к повышению качества уголовного судопроизводства и адаптации правовой системы к вызовам цифровой эпохи.

Материалы и методы.

Методологическая основа настоящего исследования формируется на базе принципов диалектического познания, что предполагает рассматривание изучаемых явлений во взаимосвязи и процессе их развития. В рамках работы применён формально-юридический метод, направленный на детальный анализ нормативных положений Уголовно-процессуального кодекса Российской Федерации, Федерального закона «Об оперативно-розыскной деятельности» (далее – ФЗ об ОРД), а также разъяснений, изложенных в постановлениях Пленума Верховного Суда РФ от 29 ноября 2016 года № 55 «О судебном приговоре» и от 31 декабря 2019 года № 62 «О применении судами норм уголовно-процессуального законодательства, регламентирующих доказывание» [4].

Использование системно-структурного анализа позволило уточнить позиционирование цифровых доказательств в рамках общей системы доказательств, которая регламентируется статьёй 74 УПК РФ. Такой подход способствует осознанию места электронных материалов в правовом поле доказывания.

Для более глубокого понимания практических аспектов исследования был использован метод анализа конкретных правовых ситуаций, а также обобщение судебной практики, в том числе прецедентов, размещенных в авторитетных справочных правовых системах «КонсультантПлюс» и «Гарант», а также решений, содержащихся в Банке судебных решений Верховного Суда Российской Федерации [5]. Всего в работе проанализировано около тридцати судебных решений за период с 2023 по 2025 год, касающихся вопросов недопустимости доказательств, полученных в электронном виде. Такой эмпирический анализ выявляет тенденции в правоприменительной практике и позволяет получить более полное представление о проблеме.

При обращении к опыту зарубежных государств использовался сравнительно-правовой метод, что позволило рассмотреть особенности регулирования электронных доказательств на международном уровне и внутри отдельных правовых систем. В частности, для этого были привлечены положения Конвенции Совета Европы о киберпреступности (Будапешт, 2001 г.), нормы Уголовно-процессуального кодекса Германии (StPO), а также Федеральных правил о доказательствах США (FRE) [6]. Такая интернациональная перспектива дает возможность выявить общие подходы и отличия в организации процедур доказывания с применением цифровых данных. Теоретическую базу исследования составили работы ведущих отечественных процессуалистов С.В. Корнаковой, Е.В. Чигриной, Н.Г. Яковлевой, А.И. Туршина, а также материалы научно-практических конференций и специализированных периодических изданий, охватывающих последние три года [7].

Данный комплекс источников позволяет обеспечить научную обоснованность и актуальность выводов исследования, сочетая теоретический анализ с эмпирическими данными.

Результаты.

Исследование выявило три основные группы системных проблем, которые существенно препятствуют эффективному использованию цифровых следов в уголовном процессе. К ним относятся: терминологическая неопределенность, недостаточная процессуальная регламентация процедуры изъятия и систематизации доказательств, а также сложность правовой оценки допустимости и достоверности таких доказательств судами [8]. Каждая из этих групп заслуживает отдельного подробного рассмотрения.

Первая группа проблем: терминологическая неопределенность. Уголовно-процессуальный кодекс Российской Федерации не содержит официального определения понятий «электронные доказательства» или «цифровые следы». В научном сообществе также нет единого мнения о точном значении этих терминов и их статусе в системе доказательств. Законодатель выделил электронные носители в отдельную категорию вещественных доказательств в пункте 5 части 2 статьи 82 Уголовно-процессуального кодекса Российской Федерации [3]. Однако такой подход вызывает опасения, поскольку для процесса доказывания важны не физические носители (например, флешка, жесткий диск или смартфон), а содержащаяся на них уникальная информация. Следует отметить, что в законодательстве нет четкого определения термина «электронные носители», что, по мнению экспертов, создает правовую неопределенность. В результате сотрудники правоохранительных органов часто сталкиваются с трудностями при классификации таких объектов, как флеш-карты или жесткие диски, не говоря уже о данных, хранящихся в «облачных» технологиях, которые не имеют физической формы [9].

Чтобы проиллюстрировать эту проблему, рассмотрим пример из судебного дела 2024 года. В одном из уголовных дел, рассмотренных судом в Свердловской области, следователь изъял у подозреваемого смартфон, который был приобщен к делу в качестве вещественного доказательства. Однако суд постановил, что скриншоты сообщений в Telegram, сделанные с этого устройства, не могут быть приобщены к делу. Основанием послужило отсутствие в протоколе обыска описания метода копирования данных и подтверждения сохранения их неизменности [10]. Данный случай отражает распространённую проблему в российской правоприменительной практике, указывающую на недостаток процедурных норм и методических подходов к работе с цифровыми доказательствами.

Вторая группа проблем: пробелы в процессуальной регламентации собирания и закрепления. Статья 164.1 Уголовно-процессуального кодекса Российской Федерации устанавливает правила изъятия электронных носителей, но опыт применения этого положения показывает, что оно недостаточно эффективно и не имеет четкого механизма, учитывающего современные технические реалии. В частности, значительные трудности возникают в ситуациях, когда информация хранится не на физическом устройстве, а удаленно, например на сервере или в мессенджерах, использующих сквозное шифрование. В таких обстоятельствах традиционные следственные действия, в том числе обыск и выемка, зачастую неприменимы из-за отсутствия физического объекта, который можно было бы изъять.

Процедуры получения данных от провайдеров или в рамках международного правового сотрудничества в соответствии с договорами о взаимной правовой помощи (Mutual Legal Assistance Treaty, MLAT) слишком бюрократизированы и занимают много времени — от нескольких месяцев до года. За это время информация может быть удалена или изменена, что значительно снижает ее ценность как доказательства.

Кроме того, существует острая проблема, связанная с правовым статусом специалистов, занимающихся сбором цифровых следов. Цифровые данные очень уязвимы для изменений и удаления, и зачастую достаточно одного действия, чтобы информация была утеряна. Для сбора и сохранения цифровых доказательств требуются специальные технические навыки. Однако роль такого эксперта в уголовном процессе четко не определена. В статье 58 Уголовно-процессуального кодекса Российской Федерации термин «специалист» используется в общем смысле, без учета особых требований к работе с электронными носителями, что не отражает необходимость в специальных знаниях и методах работы с цифровыми доказательствами. На практике это приводит к тому, что эксперт ограничивается простыми скриншотами.

Третья группа проблем: оценка допустимости и достоверности. Суды, которые традиционно рассматривают дела, связанные с материальными объектами и бумажными носителями информации, часто применяют формальный подход к оценке цифровых доказательств. В некоторых случаях скриншоты переписки или распечатки файлов принимаются в качестве доказательств без детального анализа исходных данных, что снижает достоверность представленных доказательств [13]. Обобщая практику Верховного суда Российской Федерации за первое полугодие 2025 года, следует подчеркнуть, что высший судебный орган подчеркивает, что «распечатки электронной переписки, не заверенные лицом, проводившим выемку, и не подкрепленные результатами экспертизы, не могут считаться безусловным доказательством» [14]. Однако, несмотря на такие разъяснения вышестоящих судов, практика нижестоящих судов часто демонстрирует тенденцию к игнорированию этих рекомендаций.

В своем выступлении на XII Московском инновационном правовом форуме адвокат Игорь Бушманов обращает внимание на существующий дисбаланс в позициях участников судебного процесса, когда инициатива о назначении экспертиз в первую очередь исходит от следователя. Такая ситуация дает стороне обвинения возможность манипулировать исследованием цифровых доказательств, что существенно усложняет защиту обвиняемого [15]. Кроме того, традиционных критериев допустимости доказательств, основанных на характеристиках бумажных документов, зачастую недостаточно для оценки цифровых данных, поскольку они не учитывают особенности метаданных и системных артефактов, которые могут играть ключевую роль в установлении времени и географических параметров преступления [16].

В качестве наглядного примера рассмотрим уголовное дело о мошенничестве с использованием фишинговых сайтов. В рамках этого расследования следственные органы представили в суд протокол осмотра интернет-ресурса, составленный следователем без привлечения специалиста. Защита выразила сомнения в том, что обвиняемый действительно администрировал сайт в инкриминируемый ему период. Проанализировав представленные материалы, суд признал протокол осмотра недопустимым доказательством, поскольку процедура сбора цифровых следов была технически некорректной, а во время осмотра не были зафиксированы такие важные параметры, как DNS-записи и IP-адреса серверов [17]. Этот пример демонстрирует важность комплексного и технически обоснованного подхода к работе с цифровыми доказательствами, учитывающего специфику информационных технологий и их использования.

Четвертая группа проблем, выявленных в ходе исследования, связана с анализом криптовалютных транзакций как цифровых следов. Со временем растет число уголовных дел, связанных с незаконным оборотом криптовалюты, включая мошенничество, отмывание денег и финансирование терроризма. В то же время специфические технические характеристики блокчейна, такие как анонимность пользователей и децентрализованный характер сети, затрудняют расследование таких дел правоохранительными органами. Анализ правоприменительной практики за 2024–2025 годы показывает, что власти сталкиваются со значительными трудностями при установлении личности лиц, управляющих криптовалютными кошельками. Эта проблема особенно остро стоит в ситуациях, когда криптовалютные биржи, зарегистрированные в иностранных юрисдикциях, не предоставляют необходимую информацию по запросу следственных органов, что затрудняет проведение расследований [18].

Кроме того, даже при наличии данных о криптовалютных транзакциях возникают вопросы о правовом статусе таких данных в рамках уголовного судопроизводства. Обсуждается вопрос о том, можно ли считать данные из распределенного реестра (блокчейна) допустимым доказательством. Альтернативный подход организация судебно-компьютерной экспертизы, которая могла бы подтвердить подлинность транзакций и их связь с конкретным субъектом.

В качестве примера можно привести судебное дело о незаконном обороте наркотиков через даркнет-маркетплейс, в рамках которого суд отказался принять в качестве доказательства распечатки транзакций, полученные с помощью общедоступных блокчейн-браузеров. Отказ был мотивирован отсутствием подтверждения прямой связи между этими данными и обвиняемым [19]. Эта проблема требует как технических решений (обучение следователей работе с криптотрассирующими сервисами), так и процессуальных (закрепление порядка изъятия цифровых активов как электронных доказательств).

В свете вышесказанного становится очевидным, что необходимо разработать комплексные меры, охватывающие как технические, так и процедурные аспекты. С технической точки зрения, нужно внедрить программы обучения для следователей, чтобы повысить их квалификацию и навыки использования специализированных сервисов для отслеживания криптовалют. С другой стороны, крайне важно формализовать процесс изъятия цифровых активов в качестве электронных доказательств, что поможет устранить пробелы в доказательной базе и повысить эффективность расследований, связанных с блокчейном.

Обсуждение.

Полученные в ходе исследования результаты находятся в согласии с выводами, представленными в работах других специалистов, подчеркнувших необходимость пересмотра и реформирования существующих подходов к обращению с цифровыми доказательствами. В частности, анализ выявил, что нынешняя правовая конструкция, приравнивающая электронные носители к вещественным доказательствам, в значительной мере утратила актуальность и не соответствует современным реалиям. Более целесообразным является путь, который избрали многие страны с континентальной правовой традицией введение в процессуальное законодательство самостоятельного понятия «электронное доказательство», включая закрепление особых правил фиксации, хранения и проверки таких доказательств [20]. Например, Уголовно-процессуальный кодекс Германии содержит статью 110a StPO, которая регулирует порядок осмотра электронных носителей и данных, в США же Федеральные правила доказательств предусматривают признание информации в электронной форме в качестве «записи» или «документа» и устанавливают специфические требования к процессу ее аутентификации.

Особый интерес представляет зарубежный опыт в рамках правовой семьи общего права, где сформулированы четкие формализованные требования к «технической чистоте» получения цифровых данных, что выражается в соблюдении правил неприкосновенности цепочки хранения доказательств (chain of custody). В российской практике отсутствие последовательного документирования всех этапов движения цифрового файла от момента его изъятия и до представления в суд зачастую приводит к признанию такого материала недопустимым не на основании его содержания, а по формальным причинам [6]. В связи с этим некоторые исследователи, в частности Р.В. Костенко, предлагают законодательно закрепить обязанность следователя составлять «протокол работы с цифровыми данными», в котором все операции с файлом, включая копирование, хеширование, передачу на экспертизу были бы зафиксированы [19].

Остается актуальным и дискуссионным вопрос о приемлемости результатов оперативно-розыскной деятельности (ОРД), оформленных в цифровой форме. В соответствии со статьей 89 УПК РФ такие результаты могут быть использованы в доказательственном процессе при условии их соответствия установленным требованиям к доказательствам [3]. Вместе с тем, как отмечают авторы научных публикаций, оперативно-розыскные мероприятия проводятся вне рамок уголовного судопроизводства, и информации, полученной, например, посредством прослушивания телефонных разговоров, требуется процессуальное оформление через проведение следственных действий, таких как осмотр или выемка. На практике выполнение этих процедур часто сопровождается нарушениями: файлы могут копироваться на неподходящие носители, отсутствуют расшифровки применяемых технических средств, что существенно снижает надежность представленных доказательств [21].

Невозможно не затронуть и проблему аутентичности цифровых данных. В отличие от вещественных доказательств, цифровые файлы не обладают физической уникальностью, позволяющей однозначно определить их источник. Современные информационные технологии дают возможность создавать высококачественные подделки, включая так называемые «deepfake», а также изменять метаданные, например дату создания документа или модель устройства, с которого он был получен. Это порождает серьезные сомнения относительно достоверности таких доказательств, если не проводится соответствующая судебная экспертиза, подтверждающая их подлинность [22]. Ограничивающим фактором в этом отношении является значительное время, необходимое на проведение компьютерно-технических экспертиз из-за высокой загруженности профильных экспертных учреждений, что может привести к нарушению принципа разумного срока судопроизводства, фиксированного в статье 6.1 УПК РФ.

В научной среде обсуждаются различные варианты решения указанных проблем. Так, исследователи С.В. Корнакова и Е.В. Чигрина выдвигают предложение о внесении в УПК РФ отдельной главы, посвященной электронным доказательствам, где было бы регламентировано понятие и классификация таких доказательств, а также порядок их изъятия, фиксации, хранения и особенности процессуальной оценки [7]. Альтернативный путь предлагает А.И. Туршин, настаивая на первоочередном принятии постановления Пленума Верховного Суда РФ, которое обеспечило бы единообразие применения судьями правил работы с цифровыми следами, после чего можно было бы приступать к изменениям в законодательстве [8]. Оба подхода, учитывая их преимущества и необходимость комплексного регулирования, могут применяться параллельно и в совокупности способствовать повышению эффективности правового обращения с цифровыми доказательствами.

Выводы.

По результатам исследования можно сделать несколько ключевых выводов, которые обобщают основные направления работы и предлагают конкретные пути развития законодательной базы. Во-первых, существует объективная необходимость внести изменения в Уголовно-процессуальный кодекс Российской Федерации, чтобы четко определить и регламентировать понятие «электронные доказательства», а также установить их роль и место в общей системе доказательств, принимаемых судом. В частности, предлагается внести изменения в статью 74 Уголовно-процессуального кодекса Российской Федерации, добавив в часть 2 новый пункт 6, который следует сформулировать следующим образом: «Электронные доказательства - это информация в электронно-цифровой форме, хранящаяся на электронном носителе или в информационно-телекоммуникационной сети, на основе на основании которых следственные и судебные органы могут установить наличие или отсутствие обстоятельств, которые необходимо доказать по уголовному делу».

В то же время важно подчеркнуть, что электронные носители не должны рассматриваться как самостоятельные доказательства сами по себе, они служат исключительно материальной основой для записи электронных информации, то есть они выступают в качестве хранилища электронных доказательств.

Во-вторых, необходимо усовершенствовать процессуальные механизмы, отвечающие за сбор и фиксацию цифровых следов. В этом контексте крайне важно разработать правовые нормы для извлечения данных, не привязанных к физическим носителям, например информации, хранящейся в облачных сервисах или на удаленных серверах. Кроме того, необходимо четко определить правовой статус и функциональные полномочия специалистов по информационным технологиям, участвующих в следственной деятельности.

Представляется целесообразным ввести в Уголовно-процессуальный кодекс Российской Федерации понятие «специалист по компьютерно-техническим исследованиям», наделив их особыми правами и обязанностями, в том числе по использованию мер криптографической защиты при копировании и хранении данных. Такой подход повысит надежность и достоверность собираемых цифровых доказательств и усилит процессуальные гарантии.

В-третьих, крайне важно, чтобы судебные и следственные органы разработали и внедрили единые стандарты оценки допустимости цифровых доказательств. Вместо того чтобы полагаться исключительно на наличие упаковки или конверта с доказательствами, необходимо систематически проверять техническую целостность и безопасность данных с помощью таких инструментов контроля, как хеш-суммы и электронные подписи, с привлечением компетентных специалистов.

Кроме того, следует тщательно проверять законность и обоснованность методов получения электронных данных. Сочетание этих требований и мер, реализуемых комплексно и с учетом правовых, технических и организационных аспектов, позволит более эффективно использовать потенциал цифровых следов в правоохранительной деятельности, обеспечивая при этом соблюдение процессуальных гарантий, направленных на защиту прав и свобод человека. Такой сбалансированный подход создаст возможности для более справедливой и разумной судебной практики в условиях постоянного развития цифровых технологий и появления новых форм доказательств.

СПИСОК ЛИТЕРАТУРЫ:

1. Шаблинская В.Ю., Лукиных Л.В. Некоторые проблемы применения электронных доказательств в уголовном процессе // Молодой ученый. 2026. № 9 (612). С. 322-325

2. Россинская Е.П. Цифровые следы и вопросы на экспертизе: профессор о трендах уголовного процесса // РАПСИ. 2025. 26 марта. URL:

https://rapsinews.ru/digital_law_news/20250326/310736923.html (дата обращения: 05.04.2026)

3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 29.12.2025). Ст. 6.1, 58, 74, 82, 89, 164.1

4. Постановление Пленума Верховного Суда РФ от 31.12.2019 № 62 «О применении судами норм уголовно-процессуального законодательства, регламентирующих доказывание» // Бюллетень Верховного Суда РФ. 2020. № 3

5. Обзор судебной практики Верховного Суда РФ № 2 (2025) // СПС «КонсультантПлюс». URL: https://www.consultant.ru (дата обращения: 05.04.2026)

6. Костенко Р.В. Допустимость доказательств в цифровую эпоху: трансформация процессуальных стандартов // Юридический вестник Кубанского университета. 2024. № 3. С. 31-38

7. Корнакова С.В., Чигрина Е.В. Электронные доказательства в российском уголовном процессе: проблемные вопросы // Вестник Байкальского государственного университета. 2025. Т. 11, № 2. С. 44-50. DOI: 10.18287/2542-047X-2025-11-2-44-50

8. Туршин А.И. Исследование электронных доказательств в суде // Уголовный процесс. 2025. № 7. С. 45-52

9. Рамалданов Х.Х. Особенности изъятия электронных носителей информации в уголовном процессе // ЭКОНОМИКА. ПРАВО. ОБЩЕСТВО. 2025. № 4

10. Архив Ленинского районного суда г. Екатеринбурга. Уголовное дело № 1-456/2024. Приговор от 15.08.2024

11. Валиев Э.А., Шайхутдинова З.З. Электронные доказательства в уголовном процессе: проблемы допустимости // Актуальные вопросы права, экономики и управления. Чебоксары: ИД «Среда», 2025. С. 462-464

12. Тихонова К.В. Специалист в области информационных технологий в уголовном судопроизводстве // Российский следователь. 2025. № 2. С. 28-31

13. Овчинникова Е.А. Оценка цифровых доказательств в российском уголовном процессе // Молодой ученый. 2026. № 11 (614). С. 182-183

14. Обобщение практики рассмотрения уголовных дел с использованием электронных доказательств // Бюллетень Верховного Суда РФ. 2025. № 4. С. 12-18

15. Бушманов И. Выступление на XII Московском инновационном юридическом форуме // РАПСИ. 2025. 26 марта. URL: https://rapsinews.ru (дата обращения: 05.04.2026)

16. Кузнецов А.А. Критерии допустимости электронных доказательств: от формы к содержанию // Законность. 2026. № 1. С. 18-22

17. Апелляционное постановление Московского городского суда от 12.03.2025 по делу № 22-2456/2025. Архив Мосгорсуда

18. Баранов А.Н. Криптовалютные следы в уголовном процессе: проблемы выявления и закрепления // Информационная безопасность регионов. 2025. № 2. С. 56-61

19. Архив Калининского районного суда г. Санкт-Петербурга. Уголовное дело № 1-789/2025. Приговор от 10.11.2025

20. Зайцев О.А. Электронные доказательства в уголовном процессе Европы: сравнительно-правовой анализ // Журнал российского права. 2025. № 5. С. 92-103

21. Костенко Р.В. Цепочка хранения цифровых доказательств: зарубежный опыт и перспективы внедрения в России // Информационное право. 2025. № 3. С. 35-40

22. Смирнов А.В. Результаты ОРД в цифровой форме: проблемы введения в уголовный процесс // Оперативник (сыщик). 2025. № 3. С. 41-45

23. Федотов Н.Г. Судебная компьютерно-техническая экспертиза цифровых следов: современные возможности и перспективы // Эксперт-криминалист. 2026. № 1. С. 23-27

Ihtiyarov U.

student

Higher School of Jurisprudence and Forensic Technical Expertise

Peter the Great St. Petersburg Polytechnic University

(St. Petersburg, Russia)

DIGITAL TRACES AS EVIDENCE IN CRIMINAL PROCEEDINGS: ADMISSIBILITY AND PROCEDURAL FORMALIZATION ISSUES

Abstract: *this article examines various approaches to defining legal nature of digital traces, identifies gaps in legislation regulating work with electronic data carriers, and analyzes emerging judicial practice. The purpose of this study is to identify and systematically analyze theoretical and practical problems related to recognizing digital traces as judicial evidence. The study is based on a combination of general scientific methods, including dialectical, system-structural, and formal logical analysis, as well as specialized methods such as formal legal analysis, comparative legal analysis, and judicial practice analysis. The findings show that major obstacles to effective use of digital evidence include absence of a legal definition of «electronic evidence» in Criminal Procedure Code, formal approach to assessing admissibility in law enforcement practice, technical difficulties related to ensuring data integrity and authenticity, as well as lack of procedural mechanisms for extracting information that exists exclusively in virtual environment, for example in cloud services or on remote servers. The study results are relevant for legislative activity aimed at improving criminal procedure legislation and can also be used in practice by investigators, defense attorneys, and judges when developing unified standards for handling digital traces.*

Keywords: *criminal procedure, digital trace, electronic evidence, evidence admissibility, procedural formalization, electronic data carrier, evidentiary process, justice digitalization.*