Дата поступления рукописи в редакцию: 04.10.2026 г.
Дата принятия рукописи в печать: 10.11.2026 г.
DOI: 10.24412/2224-9133-2026-10-590-596

КАЙТУКОВ Давид Александрович,
Россия, г. Владикавказ,
аспирант Северо-Осетинского государственного университета им. К.Л. Хетагурова, кафедра уголовного права и процесса, научная специальность 5.1.4. Уголовно-правовые науки,
e-mail: kaitukov.david@mail.ru

Научный руководитель:
КАРАЕВА Лора Хазбатровна,
заведующая кафедрой уголовно-правовых дисциплин, кандидат юридических наук, доцент,
e-mail: mail@law-books.ru

ЦИФРОВЫЕ СЛЕДЫ КАК ДОКАЗАТЕЛЬСТВА ПО УГОЛОВНЫМ ДЕЛАМ О КОРРУПЦИИ: ПРОБЛЕМЫ СОБИРАНИЯ И ОЦЕНКИ

Аннотация. *При расследовании коррупционных преступлений сведения о договорённостях, передаче вознаграждения и движении активов могут сохраняться в цифровой форме. Однако обнаружить такие сведения недостаточно: необходимо установить их происхождение и получить их с соблюдением процессуальных требований. В статье исследуются особенности собирания и оценки цифровых следов по делам о коррупции. Сопоставляются подходы к их правовой природе и отнесению к вещественным доказательствам либо иным документам. Рассматриваются применение ст. 164.1 УПК РФ, получение данных с удалённых ресурсов, участие специалиста и использование результатов оперативно-розыскной деятельности. Основной вывод касается разграничения технической целостности данных и их достоверности в уголовном процессе. Совпадение контрольных сумм позволяет проверить неизменность массива, но не устанавливает, кто создал информацию, кому принадлежит учётная запись или криптовалютный кошелёк и связана ли операция с коррупционным преступлением. Предлагается закрепить специальные правила обращения с цифровой информацией, дополнить требования к её фиксации и определять обязательность участия специалиста с учётом технической сложности получения данных и риска их утраты.*

Ключевые слова: *цифровой след, цифровые доказательства, коррупционные преступления, уголовно-процессуальное доказывание, электронный носитель информации, специалист, допустимость доказательств, достоверность доказательств.*

Для цитирования: *Кайтуков Д. А. Цифровые следы как доказательства по уголовным делам о коррупции: проблемы собирания и оценки // Право и управление. 2026. № 10. С. 590–596.*

KAITUKOV David Aleksandrovich,
Russia, Vladikavkaz, Postgraduate student North Ossetian State University named after K. L. Khetagurov Department of Criminal Law and Procedure, academic specialty 5.1.4. Criminal Law Sciences

Supervisor:
KARAEVA Laura Khazbatrovna,
Head of the Department of Criminal Law Disciplines, Candidate of Law, Associate Professor

DIGITAL TRACES AS EVIDENCE IN CRIMINAL CORRUPTION CASES: PROBLEMS OF COLLECTION AND EVALUATION

Annotation. *In corruption investigations, records of agreements, payments and asset transfers may be available in digital form. Finding these records is only the first step: their origin must be established and procedural requirements for obtaining them must be met. This article examines the collection and evaluation of digital traces in criminal corruption cases. It compares approaches to their legal nature and classification as physical evidence or other documents. The discussion covers Article 164.1 of the Russian Criminal Procedure Code, access to remotely stored data, specialist involvement and the use of information obtained through operational-search activities. The central argument is that technical integrity and evidentiary reliability require separate assessment. Matching hash values help verify that a data set remains unchanged, but do not establish who created the information, who controls an account or cryptocurrency wallet, or whether a transaction is connected to a corruption offense. The article proposes specific procedural rules for handling digital information, more detailed documentation requirements and a differentiated approach to mandatory specialist involvement based on the technical complexity of data acquisition and the risk of data loss.*

Key words: *digital trace, digital evidence, corruption crimes, criminal procedural proving, electronic data carrier, specialist, admissibility of evidence, reliability of evidence.*

For citation: *Kaitukov D. A. Digital traces as evidence in criminal corruption cases: problems of collection and evaluation. Law and administration. 2026;(10):590–596. (In Russ.).*

Введение

Расследование преступления всё чаще требует обращения к сведениям, которые сохранились в памяти устройства или в информационной системе. Масштаб использования цифровой среды в преступных целях отражает статистика МВД России: за одиннадцать месяцев 2025 г. зарегистрировано 627 тыс. преступлений, совершённых с использованием информационно-телекоммуникационных технологий [9, с. 147]. Эта цифра не характеризует коррупционную преступность отдельно. Она показывает общий контекст, в котором следователю приходится работать с электронной информацией и решать вопрос о её доказательственном значении.

По делам о коррупции цифровые сведения могут оказаться необходимыми для установления самого предмета взятки и способа её передачи. А. А. Титов рассматривает использование криптовалют при хищениях, легализации доходов и коррупционных действиях [3, с. 3]. Автор приводит случай возбуждения в Москве в 2023 г. уголовного дела по ст. 290 УК РФ в отношении должностного лица правоохранительного органа, получившего взятку в биткоинах. При обыске изъяли ноутбук; его исследование позволило обнаружить сведения для доступа к криптовалютным кошелькам [3, с. 205]. Для доказывания в таком случае важны и само устройство, и доступные через него данные об активах и операциях. Изъятие компьютера лишь открывает возможность получить эти сведения.

Разные стороны этой проблемы рассмотрены в юридической литературе. Е. Р. Россинская исследует цифровые следы как объекты судебной экспертизы [1, с. 109–113], З. И. Харисова — способы их собирания, фиксации и сохранения [2, с. 119–123]. Работа А. А. Титова посвящена цифровому следообразованию в криптовалютной среде [3]. М. С. Спиридонов обсуждает пределы применения цифровых технологий и искусственного интеллекта в доказывании [6, с. 481–497], А. В. Шушеначев — риски цифровизации уголовного процесса [5]. При сопоставлении этих исследований обнаруживаются разногласия относительно процессуального статуса цифровой информации и того, какие признаки позволяют считать её достоверной.

В настоящей статье исследуется использование цифровых следов при доказывании по уголовным делам о коррупции. Объект исследования — отношения, возникающие при получении и использовании цифровой информации в производстве по таким делам; предмет — нормы уголовно-процессуального законодательства, научные подходы к собиранию, проверке и оценке цифровых следов и материалы правоприменительной практики. Цель работы состоит в том, чтобы определить особенности обращения с такими следами и предложить изменения в порядке их собирания и оценки. Для этого рассматриваются правовая природа цифрового следа и формы его процессуального закрепления, роль специальных знаний и условия использования результатов оперативно-розыскной деятельности. Отдельно исследуется вопрос о соотношении технической целостности данных и их достоверности. Использованы формально-юридический и сравнительно-правовой методы, анализ и обобщение правоприменительной практики.

Цифровой след в системе уголовно-процес-

суальных доказательств

Цифровой след и доказательство, сформированное на его основе, следует различать. Компьютерная информация может возникнуть в связи с преступлением, но одного этого обстоятельства недостаточно для её использования в доказывании. Сведения нужно обнаружить и зафиксировать, установить их источник, а затем получить и закрепить в предусмотренной законом процессуальной форме. Поэтому вопрос о статусе цифрового следа включает как свойства самой информации, так и порядок работы с ней.

И. И. Беккер связывает особенности цифровых следов с тем, что они отражают событие преступления в информационном поле и возникают при преобразовании компьютерной информации. При этом след может дублироваться на других электронных носителях, сохраняя основные характеристики [11, с. 36]. В определении Е. Р. Россинской цифровой след представляет собой криминалистически значимую компьютерную информацию о событиях или действиях, которая возникает, обрабатывается, хранится и передаётся посредством компьютерных средств и информационных систем. Для работы с ней имеют значение возможность удалённого доступа и изменения данных, их распределение между системами, метаданные и особенности форматов хранения [1, с. 109].

Эти свойства затрудняют отнесение цифровой информации к видам доказательств, перечисленным в ст. 74 Уголовно-процессуального кодекса Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (далее — УПК РФ). В научной литературе предложено несколько решений.

Д. А. Еркаев исходит из того, что компьютерную информацию нельзя полностью отождествлять с материальным объектом. Данные могут воспроизводиться техническими средствами и не связаны неразрывно с единственным носителем. Поэтому, по мнению автора, традиционное понимание вещественного доказательства не позволяет в полной мере учесть особенности компьютерной информации [10, с. 18–21].

И. И. Беккер, напротив, придаёт большее значение носителю. Электронная информация рассматривается им как сведения, хранящиеся на электронном носителе: для работы с ними в уголовном процессе требуется техническое устройство [11, с. 11]. При таком понимании порядок обращения с устройством во многом определяет и процессуальную судьбу содержащихся на нём данных.

Часть цифровых сведений может рассматриваться как иные документы. Н. Э. Бровкин обосновывает этот подход положениями п. 6 ч. 2 ст. 74 и ст. 84 УПК РФ: документальные сведения допускают не только письменную форму, но и фиксацию посредством фото- и видеозаписи и иных носителей информации [8, с. 57]. Здесь на первый план выходят содержание сведений, их происхождение и способность устанавливать обстоятельства, подлежащие доказыванию.

М. С. Спиридонов предлагает разграничивать новый вид доказательства и новый способ получения доказательственной информации. Само появление технологии, с его точки зрения, не требует расширять установленный законом перечень видов доказательств. Технические средства могут изменить порядок собирания сведений, которые затем используются в уже существующих процессуальных формах [6, с. 489–491].

На наш взгляд, выбор между вещественным доказательством, иным документом и самостоятельным видом доказательств не исчерпывает проблему. Существенна отмеченная Е. Р. Россинской двойственная природа цифрового объекта: информация существует во взаимосвязи с материальными средствами её хранения и воспроизведения [1, с. 109]. Вместе с тем перенос массива на другой носитель не обязательно меняет его содержание. Следовательно, при определении правового значения объекта нужно учитывать, как возникли данные, чем они связаны с расследуемым событием и в какой процессуальной форме получены. Физические свойства носителя дают ответ лишь на часть этих вопросов.

Это различие видно в приведённом А. А. Титовым примере взятки в цифровой валюте. Изъятый ноутбук, обнаруженные на нём сведения для доступа к кошелькам и информация об активах в соответствующей цифровой инфраструктуре связаны между собой, но требуют самостоятельного исследования [3, с. 205]. Признание ноутбука вещественным доказательством ещё не объясняет происхождение доступных через него данных и их значение для дела. Работа с носителем должна сопровождаться проверкой полученной информации.

Поэтому признавать каждый цифровой след самостоятельным видом доказательства оснований нет. Требуется специальный порядок обращения с цифровой информацией, применимый независимо от того, в какой из предусмотренных ст. 74 УПК РФ форм она используется. Его задача — позволить проследить происхождение данных, восстановить процедуру их получения и проверить, сохранились ли они без изменений. Именно эти гарантии имеют практическое значение при разрешении вопроса о возможности использовать сведения в доказывании.

Собирание цифровых следов и участие специалиста

При собирании цифровых следов следователь сталкивается с различием между местонахождением устройства и местом хранения инфор-

мации. Данные могут находиться в его памяти, распределяться между несколькими системами или храниться удалённо. В последнем случае обнаруженный телефон либо компьютер служит средством доступа к ресурсу. Модель, основанная на изъятии материального носителя, не охватывает всех этих ситуаций.

В научной литературе ст. 164.1 УПК РФ рассматривают как специальную норму об отдельных особенностях изъятия электронных носителей и копирования информации [10, с. 30; 11, с. 30]. Д. А. Еркаев указывает на ограниченность такого регулирования для данных на удалённых серверах. По его оценке, порядок фиксации и получения информации непосредственно с веб-сайтов, страниц социальных сетей и других удалённых ресурсов урегулирован недостаточно [10, с. 30–31].

Изъять устройство и с его помощью получить сведения из другой информационной системы — технологически разные действия. При удалённом доступе объект может измениться независимо от следователя; доступ к нему может прекратиться до завершения копирования. З. И. Харисова обращает внимание на фрагментарность и изменчивость цифровых данных, в том числе в оперативной памяти и облачных сервисах [2, с. 120–121]. Выбор способа получения информации поэтому влияет на то, какие сведения удастся сохранить и насколько полно они будут отражать исходный объект.

Для выбора такого способа могут потребоваться специальные знания. Процессуальные полномочия следователя сами по себе не обеспечивают технически правильного обращения с устройством. Как отмечает З. И. Харисова, ошибочная последовательность действий при отсутствии необходимых знаний способна привести к утрате цифровых следов или к тому, что они останутся необнаруженными [2, с. 120].

Е. А. Бартенев и А. М. Сажаев рассматривают участие специалиста как самостоятельную форму применения специальных знаний. Он помогает обнаруживать и закреплять объекты, использовать технические средства, формулировать вопросы и разъяснять обстоятельства в пределах своей компетенции [7, с. 18–20]. Результаты его действий отражаются в протоколе следственного действия. При этом специалист оказывает помощь следователю, сохраняя вспомогательную процессуальную роль [7, с. 18].

Требование привлекать специалиста к любой операции с электронным носителем, однако, может неоправданно усложнять работу. Д. А. Еркаев допускает усмотрение следователя в технологически простых ситуациях [10, с. 32]. Для дистанционного получения информации тот же автор предлагает установить обязательное участие специалиста [10, с. 36–37]. Различие связано с характером действий и техническими рисками, которые они создают.

Полагаем, что при совершенствовании закона обязательность участия специалиста следует связывать с существенным риском утраты, изменения или неправильной интерпретации данных. Такой риск возникает при удалённом извлечении информации, создании криминалистической копии, работе с зашифрованными данными и техническом преодолении ограничений доступа. Помощь специалиста необходима и тогда, когда изменение состояния устройства может повлиять на содержимое следа. В остальных случаях вопрос об участии специалиста предлагается решать с учётом конкретного объекта и предстоящих действий. Получение данных дополнительно осложняется, если цифровая инфраструктура выходит за пределы одного государства. А. А. Титов связывает трудности расследования преступлений с использованием криптовалют с распределённостью этой инфраструктуры и необходимостью взаимодействовать с сервисами, обслуживающими оборот цифровых активов [3]. А. Г. Мовсисян также указывает на экстерриториальность расследования цифровых преступлений и потребность в межгосударственном взаимодействии [4, с. 185].

Отсюда возникает вопрос о порядке получения электронных данных, размещённых за пределами Российской Федерации или находящихся у иностранного сервис-провайдера. Общий механизм международного сотрудничества, предусмотренный гл. 53 УПК РФ, не рассчитан специально на работу с такими сведениями. Сроки исполнения запроса могут не соответствовать времени, в течение которого данные остаются доступными и неизменными. Специальная процедура трансграничного получения электронной информации требует отдельной разработки; подробно рассмотреть её в пределах настоящей статьи не представляется возможным.

Иной порядок первоначального получения цифровых сведений связан с оперативно-розыскной деятельностью. К. С. Малахов различает получение информации в ходе оперативно-розыскных мероприятий и её использование при доказывании. Поскольку материалы ОРД формируются вне процессуальной деятельности по уголовному делу, для их последующего использования требуется надлежащее введение в уголовный процесс [12, с. 43–44]. По мнению К. С. Малахова, результаты ОРД, полученные с соблюдением Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», могут использоваться в доказывании после закрепления и проверки следственным путем [12, с. 46]. При работе с цифровыми результатами ОРД нужно проверить и законность получения сведений, и

соблюдение порядка их процессуального закрепления. Эти проверки самостоятельны: правильно оформленный протокол не восполняет нарушения, допущенные при первоначальном получении информации.

Техническая целостность и достоверность цифровых данных

Цифровые сведения оцениваются по общим критериям, принятым в уголовном процессе. Каждое доказательство проверяется с точки зрения относимости, допустимости и достоверности, а их совокупность — достаточности для разрешения дела [8, с. 59]. Трудность заключается в установлении обстоятельств, на которых такая оценка должна основываться: цифровая форма может скрывать происхождение информации и условия её изменения.

Само обнаружение файла на устройстве не устанавливает его относимость. Нужно выяснить, как его содержание связано с обстоятельствами дела. И. И. Беккер предлагает учитывать и характеристики файла, включая время создания, изменения и открытия. Для установления этой связи иногда требуются специальные знания или экспертное исследование [11, с. 42]. Метаданные в таком случае помогают определить значение сведений, которое не всегда понятно из одного лишь содержания файла. Сходная проблема возникает при анализе цифровых активов. Наличие кошелька или записи о транзакции ещё не свидетельствует о коррупционном характере операции. Необходимо установить, кто связан с этой операцией и какое отношение она имеет к расследуемому событию. Техническая запись фиксирует перемещение актива, но вопрос о его значении для уголовного дела требует дальнейшей проверки.

При оценке допустимости проверяют, кем и на каком основании получены сведения, как выполнено копирование и что зафиксировано в процессуальных документах. История последующего обращения с объектом должна позволять восстановить произведённые с ним действия. З. И. Харисова указывает на отсутствие единообразных подходов к фиксации цифровой информации, ее процессуальному оформлению и сохранению без изменений [2, с. 120–123]. Без этих сведений проверка соблюдения порядка получения данных затрудняется. Проверка достоверности предполагает, в частности, установление того, изменялись ли данные после их получения. Для этого применяют хеширование. З. И. Харисова описывает вычисление контрольной суммы как способ сопоставления файлов: совпадение хеш-значений позволяет судить об их идентичности и проверить сохранность массива при копировании или исследовании [2, с. 122].

Е. Р. Россинская рассматривает хеширование наряду с другими средствами сохранения цифровых следов. К ним относятся аппаратные блокираторы записи, защищённые криминалистические образы и специализированные хранилища [1, с. 109–110]. Эти средства предназначены для защиты объекта от случайного или намеренного изменения в ходе работы с ним. Предел такой проверки состоит в том, что неизменность данных не подтверждает истинность их содержания. Сопоставление хеш-значений позволяет проверить соответствие представленного суду файла ранее зафиксированному массиву. Однако оно не устанавливает, достоверны ли исходные сведения и кому они принадлежат. Поэтому И. И. Беккер связывает проверку достоверности электронной информации с выяснением её источника, автора и пользователя [11, с. 42]. Эти обстоятельства требуют самостоятельного исследования.

В деле о коррупции даже неизменная запись о криптовалютной транзакции оставляет открытыми вопросы о лице, контролировавшем кошелёк, исполнителе операции и её связи с преступлением. Ответить на них одним хешированием невозможно. Техническая целостность позволяет опираться на сохранённый объект при дальнейшей проверке, но не заменяет установления обстоятельств, о которых этот объект предположительно свидетельствует. Часть возникающих вопросов разрешается с помощью судебной экспертизы. Е. Р. Россинская отмечает, что появление новых цифровых объектов потребовало изменения экспертных методик и компетенций. Специалист может помочь определить вид исследования, подготовить материалы и сформулировать вопросы, требующие специальных знаний. При изучении заключения его помощь позволяет разобраться в научной обоснованности методики и в том, соответствуют ли выводы результатам исследования [1, с. 113].

Правовая оценка при этом остаётся за субъектом уголовного процесса. А. В. Шушеначев возражает против полной передачи технической системе решения вопросов относимости, допустимости и достоверности. Цифровые инструменты облегчают поиск и анализ информации, но не освобождают уполномоченное лицо от обязанности оценить доказательство [5, с. 224–226].

М. С. Спиридонов рассматривает этот предел применительно к искусственному интеллекту. Если математическая модель заранее присваивает доказательствам определённый вес, её использование вступает в противоречие с принципом свободной оценки доказательств. Алгоритм допустим как средство обработки информации; его результат не должен заранее определять доказательственную силу источника [6, с. 490–491].

Оценка цифрового следа, следовательно, требует разграничивать техническую проверку объекта и проверку его доказательственного зна-

чения. В первом случае выясняют, правильно ли скопированы данные, каковы их характеристики и сохранились ли они без изменений. Во втором — устанавливают происхождение сведений, законность их получения, связь с делом и конкретным лицом. Если ограничиться технической проверкой, безупречно сохранённому файлу можно приписать значение, которого его содержание не подтверждает.

Заключение

Предлагается закрепить специальный процессуальный режим обращения с цифровой информацией, применимый ко всем этапам работы с ней: от обнаружения и получения до хранения и проверки. Его действие не следует ставить в зависимость от признания цифровых данных новым видом доказательств или от выбора одной из форм, предусмотренных ст. 74 УПК РФ. Общие требования к обращению с данными позволят учитывать их информационную и материальную стороны и сохранять процессуальные гарантии при переносе информации между носителями.

Статью 164.1 УПК РФ предлагается дополнить правилами получения сведений с удалённых ресурсов. При определении случаев обязательного участия специалиста следует учитывать сложность действий и риск изменения либо утраты информации. Его участие предлагается сделать обязательным при дистанционном извлечении данных, создании криминалистических копий и преодолении технической или криптографической защиты, а также при иных действиях, создающих существенный риск для сохранности сведений. В технологически простых случаях решение может зависеть от свойств объекта и содержания предстоящей работы.

В процессуальных документах необходимо фиксировать идентифицирующие характеристики цифрового массива и результаты контрольного хеширования. Документированию должны подлежать и последующие операции с данными, чтобы можно было проследить обращение с ними от обнаружения до экспертизы и судебного рассмотрения.

Техническая целостность цифрового следа и его уголовно-процессуальная достоверность требуют раздельной оценки. Совпадение контрольных сумм позволяет проверить неизменность данных. Происхождение сведений, их авторство, принадлежность учётной записи или цифрового актива и связь с коррупционным преступлением устанавливаются при проверке в совокупности с другими доказательствами. Экспертиза и программно-технические средства помогают провести эту работу; окончательная правовая оценка относится к компетенции уполномоченного субъекта уголовного процесса.

Список литературы:

[1] Россинская Е. Р. Современные проблемы судебной экспертизы в условиях цифровизации и пути их разрешения // Актуальные проблемы российского права. 2026. Т. 21. № 6. С. 107–119. DOI: 10.17803/1994-1471.2026.187.6.107-119..

[2] Харисова З. И. Проблемы и пути совершенствования деятельности по собиранию цифровых доказательств при расследовании преступлений в сфере компьютерной информации // Вестник Уфимского юридического института МВД России. 2025. № 2 (108). С. 116–126.

[3] Титов А. А. Раскрытие и расследование преступлений, совершаемых в отношении и с использованием криптовалюты (российский и зарубежный опыт): дис. … канд. юрид. наук : 5.1.4. Москва, 2025. 273 с.

[4] Мовсисян А. Г. Оптимизация уголовного судопроизводства в условиях цифровой трансформации // Юристъ-Правоведъ. 2024. № 1 (108). С. 182–187.

[5] Шушеначев А. В. Цифровые технологии в уголовном процессе: проблемы и риски // Вестник Российской правовой академии. 2024. № 1. С. 214–229. DOI: 10.33874/2072-9936-2024-0-1-214-229..

[6] Спиридонов М. С. Технологии искусственного интеллекта в уголовно-процессуальном доказывании // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 481–497. DOI: 10.21202/jdtl.2023.20.

[7] Бартенев Е. А., Сажаев А. М. Специалист и судебный эксперт в следственных действиях // Современное состояние, проблемы и перспективы развития специальных знаний : материалы Всероссийской научно-практической конференции, Новосибирск, 19 ноября 2024 г. Москва : Московская академия Следственного комитета Российской Федерации имени А. Я. Сухарева, 2025. С. 18–21.

[8] Бровкин Н. Э. Проблемы сбора, проверки и оценки доказательств в рамках уголовного дела в условиях цифровизации и глобализации // Наука и образование: отечественный и зарубежный опыт : материалы 82-й Международной научно-практической конференции, Белгород, 24 ноября 2025 г. Белгород : ООО «ГиК», 2025. С. 56–61.

[9] Панарина П. А. Особенности досудебного производства по уголовным делам, связанным с кибермошенничеством // Международные научные чтения : сборник статей VII Международной научно-практической конференции, 26 января 2026 г. Петрозаводск : МЦНП «Новая наука», 2026. С. 146–151.

[10] Еркаев Д. А. Проблемы выявления, фиксации и исследования вещественных доказательств по преступлениям, совершённым с ис-

пользованием сети Интернет (по материалам территориального органа внутренних дел) : выпускная квалификационная работа. Уфа : Уфимский юридический институт МВД России, 2025. 51 с.

[11] Беккер И. И. Тактика собирания и использования электронной информации при расследовании преступлений : выпускная квалификационная работа. Уфа: Уфимский юридический институт МВД России, 2022. 53 с.

[12] Малахов К. С. Современные технические средства и проблемы их применения в доказывании в ходе предварительного следствия (по материалам территориального органа внутренних дел) : выпускная квалификационная работа. Уфа: Уфимский юридический институт МВД России, 2022. 53 с.

References:

[1] Rossinskaya E.R. Modern problems of forensic examination in the context of digitalization and ways to resolve them // Actual problems of Russian law. 2026. VOL. 21. № 6. S. 107-119. DOI: 10.17803/1994-1471.2026.187.6.107-119..

[2] Harisova Z. I. Problems and ways to improve the collection of digital evidence in the investigation of crimes in the field of computer information // Bulletin of the Ufa Law Institute of the Ministry of Internal Affairs of Russia. 2025. № 2 (108). S. 116-126.

[3] Titov A. A. Disclosure and investigation of crimes committed against and using cryptocurrency (Russian and foreign experience): dis.... cand. jurid. Sciences: 5.1.4. Moscow, 2025. 273 pp.

[4] Movsisyan A. G. Optimization of criminal proceedings in the context of digital transformation // Lawyer-Lawyer. 2024. № 1 (108). S. 182-187.

[5] Shushenachev A. V. Digital technologies in criminal proceedings: problems and risks // Bulletin of the Russian Law Academy. 2024. № 1. S. 214-229. DOI: 10.33874/2072-9936-2024-0-1-214-229..

[6] Spiridonov M.S. Artificial intelligence technologies in criminal procedure evidence // Journal of Digital Technologies and Law. 2023. T. 1, NO. 2. PP. 481-497. DOI: 10.21202/jdtl.2023.20.

[7] Bartenev E.A., Sazhaev A.M. Specialist and forensic expert in investigative actions // Current state, problems and prospects for the development of special knowledge: materials of the All-Russian Scientific and Practical Conference, Novosibirsk, November 19, 2024 Moscow: Moscow Academy of the Investigative Committee of the Russian Federation named after A. Ya. Sukharev, 2025. S. 18-21.

[8] Brovkin N.E. Problems of collecting, checking and evaluating evidence in a criminal case in the context of digitalization and globalization // Science and education: domestic and foreign experience: materials of the 82nd International Scientific and Practical Conference, Belgorod, November 24, 2025 Belgorod: LLC "GiK," 2025. S. 56-61.

[9] Panarina P. A. Features of pre-trial proceedings in criminal cases related to cyber fraud // International scientific readings: collection of articles of the VII International Scientific and Practical Conference, January 26, 2026 Petrozavodsk: ICNP "New Science," 2026. S. 146-151.

[10] Erkaev D.A. Problems of identification, fixation and research of material evidence on crimes committed using the Internet (based on materials from the territorial body of internal affairs): final qualification work. Ufa: Ufa Law Institute of the Ministry of Internal Affairs of Russia, 2025. 51 pp.

[11] Becker I. I. Tactics of collecting and using electronic information in the investigation of crimes: graduation qualification work. Ufa: Ufa Law Institute of the Ministry of Internal Affairs of Russia, 2022. 53 pp.

[12] Malakhov K. S. Modern technical means and problems of their use in proving during the preliminary investigation (based on materials from the territorial body of internal affairs): final qualification work. Ufa: Ufa Law Institute of the Ministry of Internal Affairs of Russia, 2022. 53 pp.