Дата поступления рукописи в редакцию: 17.08.2026 г.
Дата принятия рукописи в печать: 01.10.2026 г.
DOI: 10.24412/2224-9133-2026-9-361-369

ОСТАШЕВ Алексей Анатольевич,
аспирант, АНО ВО «Российский новый университет», Москва, Россия,
e-mail: ostashev.lesha@yandex.ru

Научный руководитель:
КУЧИН Олег Стасьевич,
д.ю.н, профессор,
e-mail: mail@law-books.ru

ДОКТРИНА ПРОТИВОДЕЙСТВИЯ ИКТ-ПРАВОНАРУШЕНИЯМ 2026 ГОДА: ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ И ПУТИ ИХ РЕШЕНИЯ

Аннотация. *21 июля 2026 года на портале Министерства цифрового развития, связи и массовых коммуникаций РФ был опубликован проект Доктрины развития системы противодействия правонарушениям, совершаемым с использованием информационно-коммуникационных технологий (ИКТ) (далее – Доктрина). Доктрина декларирует приоритет совершенствования уголовно-процессуального законодательства в части цифровых доказательств и экспертного обеспечения, однако конкретные правовые механизмы реализации остаются нераскрытыми. В статье анализируются следующие правовые проблемы: отсутствие в Уголовно-процессуальном кодексе РФ (УПК РФ) самостоятельного института цифровых доказательств; системные нарушения требований допустимости при изъятии и исследовании цифровых следов; процессуальная неурегулированность легализации сведений из открытых источников. На основе анализа судебной практики делается вывод о «доктринальном разрыве» между стратегическими декларациями и процессуальными возможностями их реализации, а также предлагаются конкретные направления совершенствования УПК РФ.*

Ключевые слова: *цифровые доказательства, доктринальный разрыв, хеширование, доказательства, допустимость доказательств, ИКТ-преступления, уголовный процесс, метаданные.*

OSTASHEV Aleksei Anatolyevich,
postgraduate Student Russian New University (RosNOU); Moscow, Russia

Academic Supervisor:
KUCHIN Oleg Stasievich,
Doctor of Law, Professor

THE 2026 DOCTRINE ON COUNTERING ICT-RELATED OFFENSES: ISSUES REGARDING THE LEGAL REGULATION OF DIGITAL EVIDENCE AND SOLUTIONS

Annotation. *On July 21, 2026, the Ministry of Digital Development, Communications and Mass Media of the Russian Federation published a draft Doctrine for the development of a system to counter offenses committed using information and communication technologies (ICT) (hereinafter referred to as the Doctrine). The Doctrine declares that improving criminal procedural legislation regarding digital evidence and expert support is a priority; however, specific legal mechanisms for implementation remain unelaborated. This article analyzes the following legal issues: the absence of a distinct legal category for digital evidence in the Criminal Procedure Code of the Russian Federation (CPC RF); systemic violations of admissibility requirements during the seizure and examination of digital traces; and the lack of procedural regulation regarding the formal*

admission of information from open sources. Based on an analysis of judicial practice, the article identifies a "doctrinal gap" between strategic declarations and the procedural capabilities for their implementation, and proposes specific avenues for improving the CPC RF.

Key words: *digital evidence, doctrinal gap, hashing, evidence, admissibility of evidence, ICT crimes, criminal procedure, metadata.*

Введение

Стремительная цифровизация всех сфер общественной жизни, наблюдаемая в Российской Федерации на протяжении последнего десятилетия, имеет очевидную обратную сторону – высокий уровень преступности, сопряжённой с использованием информационно-коммуникационных технологий (далее – ИКТ). Предлагаемая для общественного обсуждения Доктрина определяет приоритеты, цели, задачи и основные направления развития системы противодействия ИКТ-правонарушениям на период до 2035 года.

Необходимо подчеркнуть, что на момент написания настоящей статьи Доктрина имеет статус проекта, вынесенного на общественное обсуждение; её текст может быть изменён до подписания Указа Президента РФ. Однако даже после утверждения Доктрина, по сложившейся в российской правовой системе традиции, останется стратегическим (доктринальным) документом, а не нормативным правовым актом прямого действия. Тем самым её положения не устанавливают прав и обязанностей участников правоотношений, а подлежат дальнейшему регулированию, уточнению и закреплению через последующие федеральные законы и подзаконные акты. Это порождает феномен так называемого «доктринального разрыва» – хронологического и содержательного отрыва деклараций от механизмов их реализации.

Цель настоящей статьи – выявить правовые пробелы в уголовно-процессуальном обеспечении положений Доктрины, относящихся к цифровым доказательствам и судебной компьютерно-технической экспертизе, и предложить конкретные направления совершенствования законодательства. Для достижения указанной цели поставлены следующие задачи:

проследить эволюцию нормативной базы противодействия ИКТ-правонарушениям;

проанализировать правовой статус Доктрины и феномен «доктринального разрыва»;

исследовать проблему отсутствия института цифровых доказательств в систематике УПК РФ;

выявить системные процессуальные нарушения при работе с цифровыми следами с опорой на судебную практику.

Методологическую основу исследования составляет специфика экспертно-криминалистического подхода, что обусловлено профилем образования Автора по специальности 40.05.03 «Судебная экспертиза» по профилю СКТЭ. Это позволяет рассмотреть заявленные Доктриной направления не только в плоскости догматического толкования норм, но и с позиции практических требований к изъятию, исследованию и процессуальному закреплению цифровых следов.

Нормативно-правовые предпосылки появления Доктрины

Правовое регулирование противодействия ИКТ-правонарушениям в России представляется последовательным движением от конкретных банковских мер к межведомственной системе и далее – к долгосрочной стратегической Доктрине:

Федеральный закон от 24.07.2023 года № 369-ФЗ, получивший неофициальное название «Антифрод 1.0», установил базовые обязанности банков по проверке переводов на признаки мошенничества до списания средств.

Распоряжением Правительства РФ от 30.12.2024 года № 4154-р была утверждена Концепция государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий (Далее – Концепция). Концепция ввела классификацию таких противоправных деяний, а также заложила основы специализированной цифровой платформы для оперативного обмена данными между участниками и механизма быстрой приостановки операций с денежными средствами.

Федеральный закон от 01.04.2025 года № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий». Данный закон создал ГИС «Антифрод» и определил порядок обмена информацией между участниками (ГИС «Антифрод» – это межведомственный контур, объединяющий банки, операторов связи, цифровые платформы и силовые органы).

Федеральный закон от 26 июня 2026 года № 210-ФЗ, неофициально «Антифрод 2.0» развил положения 41-ФЗ и расширил круг обязанных участников.

Доктрина 2026 года. Если Концепция 2024 года заложила концептуальные основы, далее 41-ФЗ создал инфраструктуру, а 210-ФЗ расширил её, то Доктрина 2026 года представляется объединяющим документом, который определяет развитие всей системы до 2035 года.

Вместе с тем, как показывает обзор предшествующей базы, между стратегическими доку-

ментами и их нормативным воплощением существует хронологический и содержательный разрыв: Концепция 2024 года была утверждена в декабре, закон 41-ФЗ – через четыре месяца, а его ключевые положения вступили в силу лишь через год. Предполагается, что аналогичная динамика ожидает и Доктрину 2026 года, что делает особенно актуальным анализ тех её положений, которые потребуют скорейшего нормативного закрепления – в первую очередь в уголовно-процессуальном законодательстве и экспертной практике.

Правовой статус Доктрины и проблема «доктринального разрыва»

Для правильной оценки перспектив реализации перечисленных направлений необходимо определить правовую природу анализируемого документа. В российской правовой теории вопрос о статусе доктринальных (стратегических) актов является дискуссионным. Как отмечают А.В. Малько и Я.В. Гайворонская, доктринальные правовые акты «не предоставляют субъективных прав, не налагают юридических обязанностей и не определяют мер юридической ответственности...» [7, с. 5]. В то же время авторы подчёркивают, что такие документы являются «правообразующими: предшествуют принятию серии правовых актов различных видов, предназначенных для реализации перспективных преобразований» [7, с. 16].

Согласно ст. 11 Федерального закона от 28 июня 2014 г. № 172-ФЗ «О стратегическом планировании в Российской Федерации», доктрины относятся к документам стратегического планирования, разрабатываемым в рамках целеполагания в сфере обеспечения национальной безопасности. Применительно к анализируемой Доктрине это означает, что даже после подписания Указа Президента РФ (предположительно – в 2026 или 2027 году) её положения не станут нормами прямого действия. Для этого потребуются самостоятельные нормативные правовые акты – федеральные законы, вносящие изменения в УПК РФ, УК РФ, ФЗ «Об ОРД», ФЗ «О ГСЭД» и иные акты.

Среди ключевых новаций, имеющих прямое отношение к предмету настоящего исследования, следует выделить следующие.

Во-первых, концепция цифрового токена (ЦТ) – криптографического объекта, верифицируемого цифрового отпечатка совокупности данных о физическом лице, распределённых между участниками экосистемы цифровой экономики. Сценарий опережающего развития, построенный вокруг ЦТ, предполагает отказ от централизованного хранения персональных данных в пользу криптографических производных – производных, уникальных, неотчуждаемых, динамичных и регенерируемых.

Во-вторых, приоритет «совершенствования уголовного, уголовно-процессуального и оперативно-разыскного законодательства в части развития института цифровых (электронных) доказательств, новых форм и средств доказывания, а также фиксации и легализации цифровых следов». Это положение – единственное в Доктрине, которое прямо адресует проблемы доказательственного права, и именно оно составляет предметный фокус настоящей статьи.

В-третьих, нормативное закрепление использования сведений из разведки по открытым источникам (OSINT) в качестве доказательственной базы, а также развитие системы криминалистического учёта на основе цифрового следа устройства.

В-четвертых, развитие специализированных аналитических программных продуктов для проведения исследований и судебных компьютерно-технических экспертиз, а также введение новой специальности «Антифрод-специалист».

В-пятых, механизм «обратного взыскания» – наделение кредитных организаций полномочиями по совместному принятию решений о возврате денежных средств отправителям при переводах без добровольного согласия клиента путём взыскания сумм со счетов получателей. Правового основания для этого механизма в действующем законодательстве нет.

Сказанное позволяет выделить феномен, который в настоящей статье обозначается как «доктринальный разрыв» – хронологический и содержательный отрыв стратегических деклараций от процессуальных механизмов их реализации.

Доктрина декларирует развитие института цифровых доказательств, но не предлагает процессуальной модели их закрепления в УПК РФ. Она провозглашает легализацию цифровых следов, но не определяет, какой режим применим к данным на изъятом устройстве – режим осмотра (ст. 176 УПК) или режим получения сведений о сообщениях (ст. 186.1 УПК). Она указывает на необходимость развития экспертного обеспечения, но не конкретизирует требований к квалификации экспертов или к обязательности назначения компьютерно-технической экспертизы.

Между каждой из этих деклараций и её нормативным воплощением лежит цепочка: Доктрина → проект федерального закона → принятие закона → вступление в силу → формирование правоприменительной практики. Каждый этап требует времени, а результат не гарантирован. Более того, это означает, что технологические новации (цифровой токен, OSINT-доказательства и т.д.) будут опережать процессуальную базу их использования в уголовном процессе.

С учетом изложенного, предложения, формулируемые в настоящей статье, адресуются не столько тексту Доктрины (который на момент

написания является проектом и может быть скорректирован), сколько будущим нормативным правовым актам, которые будут приниматься на её основе.

Институт цифровых доказательств: пробел в систематике УПК РФ

Центральное противоречие, создаваемое положениями Доктрины, заключается в следующем: документ провозглашает «развитие института цифровых (электронных) доказательств» как приоритетное направление совершенствования законодательства, однако в действующем УПК РФ этот институт отсутствует. Часть 1 ст. 74 УПК РФ определяет доказательства как «любые сведения, на основании которых суд, прокурор, следователь, дознаватель могут установить обстоятельства, подлежащие доказыванию», – формулировку предельно широкую, не ограничивающую форму представления сведений. Однако ч. 2 той же статьи содержит исчерпывающий перечень источников доказательств – «цифровые»/«электронные» доказательства в этом перечне не названы. При этом в дальнейшем будет использоваться термин именно «цифровые данные», поскольку именно такое определение, равно как и его производные (например, цифровой носитель информации) отражает современное понимание сущности и специфики данных [13, с. 120].

В научной литературе сложились две позиции. Одни авторы (В.Г. Голубцов [3, с. 385], Л.В. Головко [4, с. 22–24], П.С. Пастухов [8, с. 703–705]) считают, что введение самостоятельного вида не требуется: действующее определение доказательств как «любых сведений» достаточно широко, чтобы включать электронные данные, а отдельная категория лишь усложнит процесс. Другие (В.В. Платонов [9, с. 11–13], А.А. Поддубняк [10, с. 217–218]) настаивают на выделении цифровых доказательств в самостоятельный вид, указывая на качественные отличия: нематериальность, зависимость от среды воспроизведения, невозможность восприятия без аппаратно-программных средств. В результате цифровые данные классифицируются как традиционные. В одном случае носитель (телефон, ноутбук, сервер) признаётся вещественным доказательством по ч. 4 ст. 81 и п. 5 ч. 2 ст. 82 УПК РФ – со всеми вытекающими правилами хранения, опечатывания и возврата владельцу. Во втором – сама информация (текст переписки, скриншот, файл) приобщается как иной документ по ч. 2 ст. 84 УПК РФ, допускающей фиксацию сведений на электронных носителях. В противовес к традиционной точке зрения, рассматривающей цифровые доказательства как разновидность традиционных существует иная точка зрения, базирующаяся на том, что цифровые данные обладают собственными уникальными характеристиками, такими как способность к мгновенному изменению без следов и копированию без утраты качеств, зависимость от программной среды, возможность существования одновременно в нескольких локациях и т.д. [12, с. 73]. Как отмечается в публикации 2026 года, отнесение цифровых доказательств к «иным документам» «игнорирует их уникальную природу, которая принципиально отличается от традиционных доказательств» [11, с. 294].

Доктрина, провозглашая приоритет развития института цифровых доказательств, фактически встаёт на сторону второй группы авторов – но не предлагает процессуальной модели. В этом проявляется рассмотренный выше «доктринальный разрыв»: декларация зафиксирована, а норма – нет.

Следует обратить внимание на одно из самых важных отличий цифровых доказательств от традиционных – одна и та же информация может одновременно существовать на физическом устройстве и в электронной форме. Для традиционного вещественного доказательства оригинальность – это физическая уникальность: физический предмет с отпечатками пальцев существует в единственном экземпляре. Для цифрового – оригинальность переходит из материального измерения в измерение происхождения и целостности: значим не носитель, а то, можно ли подтвердить, откуда получены данные и что они не изменены с момента фиксации. В понимании автора представляется очевидным, что сущностная природа цифровых данных существенно отличается от традиционной формы данных (информации).

Процессуальные последствия очевидны: если следователь изъял телефон (вещественное доказательство), скопировал с него данные (документ) и параллельно получил те же данные от оператора связи по запросу (иной документ) – три процессуально оформленных экземпляра одной и той же информации оказываются в деле под разными процессуальными названиями. Ни УПК РФ, ни разъяснения Пленума ВС РФ не предлагают правил разрешения этой коллизии.

Особого внимания заслуживает проблема метаданных – структурированной информации, описывающей характеристики цифрового объекта: дату и время создания, автора, модель устройства, геолокацию, историю правок, маршрут прохождения электронного письма через серверы. Доказательственное значение метаданных может превышать значимость самого содержания файла. Например, текст переписки в мессенджере может быть реконструирован и без оригинального устройства, но метаданные EXIF-фотографии (геокоординаты, модель камеры, временная метка) способны установить место и время совершения преступления, когда все иные следы утраче-

ны. Серверные логи фиксируют IP-адреса, время запросов, используемые браузеры – позволяя реконструировать поведение пользователя в сети.

Однако УПК РФ не содержит процедур работы с метаданными: ни порядка их фиксации при изъятии, ни требований к проверке их неизменности, ни норм об их процессуальной оценке. На практике следователь, приобщая к делу скриншот переписки или распечатку текстового файла, в большинстве случаев не фиксирует метаданные – они просто утрачиваются.

С позиции специалиста, обладающего образованием по специальности 40.05.03 «Судебная экспертиза», следует отметить следующее. В рамках компьютерно-технической экспертизы метаданные являются одним из первичных объектов исследования. Эксперт-криминалист извлекает их с использованием специализированных программных комплексов («Мобильный криминалист», FTK, Oxygen Forensic Detective, Cellebrite UFED и пр.) и анализирует для установления целостности, аутентичности и хронологии событий. Однако если на стадии предварительного расследования метаданные не были процессуально зафиксированы (не отражены в протоколе следственного действия, не сохранены в исходной структуре файла), эксперт работает с уже обезличенным материалом – восстановить утраченные метаданные технически невозможно, а сформулировать категорический вывод об аутентичности такого объекта он не вправе. Таким образом, процессуальная «невидимость» метаданных на стадии собирания доказательств напрямую снижает доказательственный потенциал экспертизы на стадии исследования – разрыв, который Доктрина не устраняет.

С учётом изложенного представляется обоснованным дополнить ч. 2 ст. 74 УПК РФ самостоятельным видом доказательств – «цифровые доказательства», – определив в ст. 5 УПК РФ их понятие с учётом двух составляющих: содержания (цифровой информации) и формы (электронного носителя или среды, в которой информация сохранена).

Необходимо также закрепить особенности оценки цифровых доказательств с точки зрения:

целостности и аутентичности как критериев достоверности (возможность подтвердить неизменность данных с момента фиксации);

возможности и обязательности фиксации метаданных при приобщении цифрового объекта к материалам дела;

многоресурсности (при наличии идентичных копий на нескольких носителях процессуально значимым установление происхождения и цепочки сохранения данных).

Доктрина создаёт основы для такого закрепления, но, как было показано ранее, между декларацией и принятием соответствующих поправок в УПК РФ лежит как минимум два-три года. На протяжении этого периода правоприменитель будет продолжать работать с цифровыми данными по правилам, для этих данных не предназначенным, – со всеми вытекающими рисками, анализ которых продолжен в следующем разделе.

Допустимость цифровых доказательств: системные процессуальные нарушения

В рамках действующих норм правоприменитель сталкивается с системными нарушениями требований допустимости (ст. 75 УПК РФ) при работе с цифровыми следами. Анализ судебной практики показывает, что эти нарушения носят не единичный, а массовый характер, и доктринальная декларация «легализации цифровых следов» не предлагает механизмов их устранения.

Ч. 3.1 ст. 164.1 УПК РФ устанавливает: при изъятии электронных носителей информации обязательно участие специалиста. Часть 3 ст. 177 УПК РФ требует упаковки, опечатывания и заверения подписью следователя. Цель этих требований очевидна: обеспечить неизменность данных и исключить возможность их модификации в интервале между изъятием и осмотром. Однако судебная практика демонстрирует принципиально разные подходы к оценке нарушений этих требований.

В Определении Конституционного Суда РФ от 31 мая 2022 г. № 1385-О по жалобе Н.Е. Щулепова осуждённый оспаривал конституционность ст. 164.1 и ч. 3 ст. 177 УПК РФ, указывая, что ноутбук и телефон были изъяты без участия специалиста и без надлежащей упаковки, а осмотр произведён спустя длительное время. КС РФ отказал в принятии жалобы, но – что принципиально важно – подтвердил обязательность требований, прямо указав: ст. 164.1 предписывает изымать электронные носители с участием специалиста, а ч. 3 ст. 177 – упаковывать и опечатывать. Вопрос о соблюдении этих требований в конкретном деле КС РФ отнёс к компетенции судов общей юрисдикции. Таким образом, КС РФ не санкционировал послабление – он подтвердил, что норма действует как обязывающая.

Однако суды общей юрисдикции на практике фактически нейтрализуют это требование. Показательно Определение Верховного Суда РФ от 21 мая 2025 г. по делу № 2-45/2024: телефоны по делу были изъяты в нарушение ст. 164.1 УПК РФ – без участия специалиста, а информация о соединениях зафиксирована при осмотре без судебного решения. Тем не менее ВС РФ не признал это основанием для недопустимости, указав, что телефоны изымались «как обычные предметы бытового назначения, при которых участия специалиста, применения специальных познаний и технологических процедур не требовалось».

С позиции специалиста, приведённая аргументация вызывает принципиальные возражения. Мобильный телефон – не «предмет бытового назначения», а сложный цифровой носитель, функционирование которого зависит от множества факторов: состояния операционной системы, активных сетевых подключений, процессов синхронизации с облачными сервисами, наличия шифрования и удалённого управления. Изъятие такого устройства без специалиста влечёт риски, которые невозможно компенсировать последующим осмотром:

при активной синхронизации с облачным хранилищем данные могут быть удалены дистанционно (функция «Найти устройство», технология «remote wipe»);

при отсутствии экранирующей упаковки устройство остаётся доступным для сетевых подключений, что позволяет изменить или уничтожить данные;

при некорректном выключении возможна утрата данных, хранящихся в оперативной памяти (volatile data) – журналов сессий, открытых вкладок, расшифрованных ключей.

Таким образом, позиция ВС РФ по факту нейтрализовала требование ст. 164.1: если телефон признаётся «бытовым предметом», участие специалиста никогда не потребуется. Доктрина же не определяет критериев, при которых участие специалиста является обязательным, – что оставляет правоприменителю возможность действовать по логике ВС РФ, а не КС РФ. Как отмечает А.А. Балашова со ссылкой на Апелляционное постановление Владимирского областной суда от 9 сентября 2021 г., «суд, рассматривая жалобы адвокатов о признании следственных действий выполненными в нарушение норм ст. 164.1 УПК РФ, чаще всего выносит постановление об отказе в удовлетворении ходатайств, аргументируя своё решение тем, что для изъятия электронных носителей информации специальных познаний не требуется» [1, с. 70].

Одной из наиболее острых процессуальных коллизий, оставленных Доктриной без внимания, является соотношение режима осмотра электронного устройства (ст. 176–177 УПК РФ) и режима получения сведений о соединениях и содержании сообщений (ст. 185, 186, 186.1 УПК РФ). Суть проблемы: доступ к переписке, передаваемой по каналам связи, требует судебного решения; доступ к той же переписке, сохранённой в памяти изъятого устройства, – не требует. Содержание охраняемой тайны от места хранения не зависит, но процессуальная логика этот факт игнорирует.

Согласно приговору Курганского городского суда Курганской области от 25 июня 2014 г. по делу № 1-230/2014 суд признал недопустимыми протоколы осмотра сотовых телефонов в части сведений о входящих и исходящих соединениях и текстах СМС-сообщений. Основание: следователь самостоятельно, без судебного решения, получил сведения, для которых ст. 186.1 УПК РФ требует санкции суда. Суд приравнял осмотр содержимого телефона к перехвату сообщений и применил режим тайны связи в соответствии со ст. 23 Конституции РФ.

Противоположная позиция – в Кассационном определении Верховного Суда РФ от 30 сентября 2014 года № 2-18/08 рассматривался довод осуждённого Колобова В. Г., который утверждал, что осмотр его мобильного телефона проведён незаконно – якобы без судебного решения, а значит, нарушает конституционные права. Суд с этим доводом не согласился. Он указал, что осмотр телефона был проведён следователем в соответствии со статьёй 176 УПК РФ. А эта норма регулирует осмотр предметов (в том числе изъятых вещей) в целом. Верховный Суд разъяснил: для осмотра содержимого телефона (фото, сообщения, контакты) не требуется выносить отдельное судебное решение.

Таким образом, на сегодняшний день сосуществуют две взаимоисключающие позиции: одни суды исключают данные, полученные при осмотре телефона без судебного решения (Курганский горсуд), другие – допускают (ВС РФ, КС РФ). Кравцова А.Н. выделила три типичные ошибки правоприменительной практики: «подмена судебного порядка получения охраняемых законом сведений направлением запроса..., формальная фиксация факта изъятия электронного носителя без описания его состояния и без обеспечения неизменности данных..., обоснование атрибуции единственным техническим признаком, чаще всего IP-адресом» [6, 413]. Сторона защиты использует этот разрыв: в зависимости от состава суда и конкретных обстоятельств, одно и то же доказательство может быть признано допустимым или недопустимым.

Доктрина, провозглашая «легализацию цифровых следов», не разрешает эту коллизию. Представляется обоснованным предложение, уже сформулированное в научной литературе: дополнить УПК РФ статьёй 185.1 «Осмотр информации, содержащейся в электронном устройстве или на электронном носителе», предусмотрев необходимость судебного решения для доступа к сведениям о сообщениях и соединениях, хранящимся в памяти устройства, – по аналогии с режимом ст. 186.1 УПК РФ.

Третьим системным нарушением является отсутствие в УПК РФ требования об обязательной фиксации хеш-значений (контрольных сумм) при изъятии и копировании цифровых данных. Хеш-функция – криптографический алгоритм, преобразующий массив данных произвольного

объёма в строку фиксированной длины; изменение хотя бы одного бита исходных данных приводит к радикальному изменению хеш-значения, что позволяет однозначно подтвердить неизменность информации с момента фиксации. С позиции экспертной методики компьютерно-технической экспертизы, вычисление хеш-сумм (MD5, SHA-256) является базовым требованием криминалистической работы с цифровыми следами – оно зафиксировано в международных стандартах (ISO/IEC 27037:2012, руководства IOCE) и применяется во всех сертифицированных программных комплексах (EnCase, FTK, Cellebrite). Однако в отсутствие процессуальной обязанности следователь не обязан, а эксперт не вправе требовать – и хеш-фиксация остаётся на усмотрение правоприменителя. Результат: заключение эксперта, проведённое на материале без зафиксированной хеш-суммы, уязвимо для оспаривания по критерию достоверности исходных данных – эксперт не может категорически утверждать, что исследуемый материал идентичен тому, который был изъят. Беппаев Р.Ж. еще в конце 2025 года аналогичным образом отмечал, что формирования «цифровой процессуальной формы» необходимо «законодательное закрепление... механизмов обеспечения неизменности цифровых доказательств – использование хеш-функций для верификации, технологии блокчейн для создания неизменяемых журналов учёта доказательств, квалифицированных электронных подписей для удостоверения подлинности...» [2, с. 53].

Поскольку Доктрина не закрепляет процессуального механизма фиксации. Представляется необходимым дополнить ст. 164.1 УПК РФ положением об обязательном вычислении и фиксации хеш-значений изымаемых электронных данных в протоколе следственного действия – с указанием алгоритма (SHA-256 или эквивалентного) и значения контрольной суммы. В таком случае ч. 2-3 данной статьи могли бы быть дополнены следующим абзацем:

«При изъятии электронных носителей информации специалист в присутствии следователя и понятых вычисляет контрольную сумму (хеш-значение) изымаемых электронных данных с использованием криптографического алгоритма. Вычисленное хеш-значение, наименование и версия применённого алгоритма указываются в протоколе следственного действия».

Кроме того, для разъяснения данных положений может быть введена ч. 4 следующего содержания:

«Контрольная сумма (хеш-значение) электронных данных, указанная в частях второй и третьей настоящей статьи, вычисляется до и после любого копирования, перемещения или иного процессуального действия с электронными носителями информации. Несовпадение контрольных сумм, выявленное при последующем исследовании, является основанием для проверки сохранности и неизменности соответствующих электронных доказательств. Порядок вычисления и фиксации контрольных сумм (хеш-значений) устанавливается федеральным органом исполнительной власти, осуществляющим функции по выработке государственной политики и нормативно-правовому регулированию в сфере внутренних дел».

В то же время стоит оговориться – функция хеширования служит для подтверждения или опровержения самого факта, что после конкретного момента цифровой объект не изменялся; т.е. не устанавливает автора сообщения, не отвечает на вопрос о законности получения информации и не заменяет процессуальной оценки доказательств судом [5, с. 146].

Заключение

Проведённое исследование позволяет сформулировать ряд выводов, значимых для уголовно-процессуальной науки и практики расследования ИКТ-преступлений.

Во-первых, Доктрина развития системы противодействия правонарушениям в сфере ИКТ задаёт принципиально новый вектор развития нормативной базы: акцент смещается с точечных антифрод-мер на системное формирование института цифровых доказательств и экспертного обеспечения. При этом документ носит стратегический характер и не содержит норм прямого действия – его положения должны быть имплементированы через изменения в УПК РФ и иные нормативные акты.

Во-вторых, феномен «доктринального разрыва» – хронологического и содержательного отрыва стратегических деклараций от процессуальных механизмов их реализации – подтверждается как теоретическими аргументами, так и эмпирическими данными. История реализации предшествующей Концепции (2024–2026 гг.) показывает, что между принятием стратегического документа и вступлением в силу конкретных норм, обеспечивающих его положения, проходит не менее полутора-двух лет, а в случае сложных процессуальных изменений – значительно больше. Для положений Доктрины, затрагивающих институт цифровых доказательств, этот разрыв может составить два-три года и более, в течение которых правоприменитель вынужден работать по устаревшим правилам.

В-третьих, в действующем уголовно-процессуальном законодательстве выявлен структурный пробел: цифровые доказательства не выделены в самостоятельный вид доказательств (ч. 2 ст. 74 УПК РФ), а их уникальные свойства (многоресурсность, копируемость, зависимость от ме-

таданных) не учтены в процессуальных правилах собирания и оценки. Это приводит к тому, что цифровые данные искусственно «встраиваются» в традиционные категории («вещественные доказательства» либо «иные документы»), что порождает внутренние противоречия и снижает доказательственную ценность материалов дела.

В-четвертых, анализ судебной практики выявил системные нарушения требований допустимости доказательств (ст. 75 УПК РФ) при работе с цифровыми следами. Наиболее острыми проблемами являются: изъятие электронных носителей без участия специалиста вопреки ст. 164.1 УПК РФ; коллизия между осмотром устройства (ст. 176 УПК РФ) и режимом тайны сообщений (ст. 186.1 УПК РФ); отсутствие обязательного требования о хеш-фиксации данных, без которой невозможно подтвердить их неизменность. Эти нарушения носят массовый характер и подтверждаются противоречивой судебной практикой, где одни и те же действия в одних случаях признаются допустимыми, а в других – служат основанием для признания доказательств недопустимыми.

С учётом изложенного, в статье предложены конкретные направления совершенствования уголовно-процессуального законодательства:

закрепить в ч. 2 ст. 74 УПК РФ самостоятельный вид доказательств – «цифровые доказательства»;

ввести в ст. 5 УПК РФ дефиницию цифровых доказательств, включающую содержание информации и форму её фиксации;

дополнить ст. 164.1 УПК РФ требованием об обязательной хеш-фиксации изымаемых данных с указанием алгоритма и значения контрольной суммы;

ввести специальную норму (например, ст. 185.1 УПК РФ), устанавливающую необходимость судебного решения для доступа к сведениям о сообщениях и соединениях, хранящимся в памяти изъятого устройства.

Реализация этих предложений позволит устранить наиболее острые процессуальные пробелы и создать правовую основу для эффективного использования цифровых доказательств в уголовном судопроизводстве. При этом отдельные аспекты темы – в частности, вопросы квалификации экспертов, стандартизации методик КТЭ и процессуальных механизмов работы с распределёнными криптографическими данными (включая концепцию цифрового токена) – требуют дальнейшего исследования.

Список литературы:

[1] Балашова А.А. Особенности изъятия электронных носителей информации // Вестник Уральского Юридического Института МВД России. 2025. № 3 (47). С. 68–71.

[2] Беппаев Р.Ж. Цифровой след как доказательство в уголовном процессе: проблемы допустимости и достоверности // Вопросы права. 2025. № 4. С. 51–54.

[3] Голубцов В.Г. Цифровизация и электронные доказательства в гражданском судопроизводстве // Вестник Пермского университета. Юридические науки. 2019. С. 379–386.

[4] Головко Л.В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? // Вестник экономической безопасности. 2019. № 1. С. 15–25.

[5] Демидченко Ю. В. Обеспечение целостности электронных доказательств в уголовном процессе: возможности криптографического хеширования // Право и практика. 2026. № 2. С. 142–147.

[6] Кравцова А.Н. Цифровые следы криминальной деятельности в виртуальном пространстве как основа формирования доказательств: проблемы допустимости и достоверности // Право и управление. 2026. № 8. С. 407–415.

[7] Малько А.В., Гайворонская Я.В. Доктринальные акты как основной инструмент правовой политики // Право. Журнал Высшей школы экономики. 2018. № 1. С. 4–25.

[8] Пастухов П.С. Электронные доказательства в нормативной системе уголовно-процессуальных доказательств // Пермский юридический альманах. 2019. № 1. С. 695–707.

[9] Платонов В.В. Теоретико-правовая модель электронных доказательств в уголовном судопроизводстве : автореферат дис. ... кандидата юридических наук : 5.1.4. / Платонов Валентин Васильевич; [Место защиты: «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)» ; Диссовет 24.2.336.03 (Д 212.123.ХХ)]. – Москва, 2026. – 31 с.

[10] Поддубняк А.А., Алиева А.А. Специфика доказательственного значения отдельных видов электронных носителей информации // Учёные записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. 2020. Т. 6 (72), № 4. С. 213–219.

[11] Торбин Ю.Г. Трансформация оценки доказательств в условиях цифровизации уголовного судопроизводства // Право и управление. 2026. № 8. С. 293–298.

[12] Федорова М.Д. Электронные доказательства в уголовном судопроизводстве: правовое регулирование и перспективы развития // Социальное управление. 2026. Т. 8, № 1. С. 71–77.

[13] Яковлева Н.Г. Использование цифровых доказательств в уголовном судопроизводстве Российской Федерации // Вестник Тверского государственного университета. Серия: Право. 2024. № 4 (80). С. 117–126.

References:

[1] A.A. Balashova. Features of withdrawal of electronic media // Bulletin of the Ural Law Institute of the Ministry of Internal Affairs of Russia. 2025. № 3 (47). S. 68-71.

[2] Beppaev R.Zh. Digital footprint as evidence in criminal proceedings: problems of admissibility and reliability // Legal issues. 2025. № 4. S. 51-54.

[3] Golubtsov V.G. Digitalization and electronic evidence in civil proceedings // Bulletin of Perm University. Legal sciences. 2019. S. 379-386.

[4] Golovko L.V. Digitalization in criminal proceedings: local optimization or global revolution? // Bulletin of Economic Security. 2019. № 1. S. 15-25.

[5] Demidchenko Yu. V. Ensuring the integrity of electronic evidence in criminal proceedings: the possibilities of cryptographic hashing // Law and practice. 2026. № 2. S. 142-147.

[6] Kravtsova A.N. Digital traces of criminal activity in the virtual space as the basis for the formation of evidence: problems of admissibility and reliability // Law and management. 2026. № 8. S. 407-415.

[7] Malko A.V., Gayvoronskaya Y.V. Doctrinal acts as the main instrument of legal policy // Law. Journal of the Higher School of Economics. 2018. № 1. S. 4-25.

[8] Pastukhov P.S. Electronic evidence in the regulatory system of criminal procedural evidence // Perm legal almanac. 2019. № 1. S. 695-707.

[9] Platonov V.V. Theoretical and legal model of electronic evidence in criminal proceedings: abstract dis.... Candidate of Legal Sciences: 5.1.4 / Platonov Valentin Vasilievich; [Place of defense: "O.E. Kutafin Moscow State Law University (MSLA)"; Dissertation Council 24.2.336.03 (D 212.123.XX)]. - Moscow, 2026. - 31 s.

[10] Poddubnyak A.A., Aliyeva A.A. Specifics of the evidentiary significance of certain types of electronic media // Scientific notes of the Crimean Federal University named after V.I. Vernadsky. Legal sciences. 2020. T. 6 (72), NO. 4. S. 213-219.

[11] Torbin Yu. G. Transformation of evidence assessment in the context of digitalization of criminal proceedings // Law and management. 2026. № 8. S. 293-298.

[12] Fedorova M.D. Electronic evidence in criminal proceedings: legal regulation and development prospects // Social management. 2026. T. 8, NO. 1. S. 71-77.

[13] Yakovleva N.G. Use of digital evidence in criminal proceedings of the Russian Federation // Bulletin of Tver State University. Series: Right. 2024. № 4 (80). S. 117-126.

