

В. А. Макарецва

студент 3 курса

Новосибирского национального исследовательского государственного университета

г. Новосибирска

Т. Ю. Сабельфельд

научный руководитель, канд. юрид. наук, доцент,

доцент кафедры правового обеспечения рыночной экономики экономического факультета

Новосибирского национального исследовательского государственного университета

г. Новосибирска

ЦИФРОВЫЕ ДОКАЗАТЕЛЬСТВА В УГОЛОВНОМ ПРОЦЕССЕ: ПРОБЛЕМЫ ДОПУСТИМОСТИ, ЦЕЛОСТНОСТИ И ОЦЕНКИ В УСЛОВИЯХ БЫСТРОГО РАЗВИТИЯ ТЕХНОЛОГИЙ

В статье проводится комплексный анализ проблем допустимости, целостности и судебной оценки доказательств в уголовном процессе Российской Федерации. Актуальность обусловлена отсутствием легального определения «цифрового доказательства» в Уголовно-процессуальном кодексе Российской Федерации, что приводит к фрагментарности правоприменительной практики. По итогам проведенного анализа предложены пути решения выявленных проблем посредством внесения изменений в законодательство.

Ключевые слова: уголовный процесс, цифровые доказательства, допустимость, целостность, искусственный интеллект.

V. A. Makartseva

3rd year student of Novosibirsk National Research State University, Novosibirsk

T. Y. Sabelfeld

Scientific supervisor, PhD in law, Associate Professor, Associate Professor

of the Department of Legal Support of Market Economics, Faculty of Economics,

Novosibirsk National Research State University, Novosibirsk

DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS: ISSUES OF ADMISSIBILITY, INTEGRITY, AND ASSESSMENT IN THE CONTEXT OF RAPID TECHNOLOGY DEVELOPMENT

The article provides a comprehensive analysis of the problems of admissibility, integrity, and judicial assessment of evidence in the criminal proceedings of the Russian Federation. The relevance of the article is due to the lack of a legal definition of “digital evidence” in the Criminal Procedure Code of the Russian Federation, which leads to a fragmented legal practice. Based on the analysis, the article proposes solutions to the identified problems through legislative amendments.

Keywords: criminal proceedings, digital evidence, admissibility, integrity, artificial intelligence.

Процессы цифровизации, охватившие
сегодня и сферу правоохранительной дея-

тельности, приводят к тому, что информация
с электронных носителей занимает одно из

ключевых мест в системе доказывания. Особенно ярко эту тенденцию можно проследить в уголовных делах о противоправных деяниях в сфере высоких технологий, коррупционных преступлениях, мошеннических действиях. По данным Генеральной прокуратуры РФ, в 2024 году зарегистрировано свыше 765 тыс. преступлений с использованием информационно-телекоммуникационных технологий, что подтверждает масштаб явления [1]. Однако развитие высоких технологий опережает темпы обновления процессуального законодательства. В результате чего возникает пробел в законодательстве.

Уголовно-процессуальный кодекс Российской Федерации (далее — УПК РФ) не содержит легального определения понятия «цифровое доказательство». В результате правоприменитель вынужден квалифицировать цифровые массивы через другие процессуальные формы, такие как вещественные доказательства (ст. 81 УПК РФ) или иные документы (ст. 84 УПК РФ) [2]. Подобный подход порождает неоднородность и уязвимость правоприменительной практики. Особенно остро это проявляется при решении вопросов о допустимости доказательств, обеспечении целостности цифровых данных, а также при судебной оценке материалов, полученных с участием алгоритмов искусственного интеллекта.

Целью статьи является выявление проблем допустимости, целостности и оценки цифровых доказательств в уголовном процессе Российской Федерации, а также разработка предложений по их преодолению. Для этого необходимы анализ законодательства, связанного с обращением с электронными носителями, обобщение российской судебной практики и сопоставление ее с зарубежной, определение направлений совершенствования законодательства и ведомственных стандартов.

Фундаментальная проблема правового регулирования цифровых доказательств в российском уголовном процессе заключается в отсутствии в ст. 74 УПК РФ [2] самостоятельного вида доказательств, специально предназначенного для фиксации электронной информации. Действующий перечень источников доказательств носит за-

крытый характер и сформирован в эпоху преобладания аналоговых носителей. В результате цифровые данные (бинарные коды, метаданные, журналы сетевой активности, хеш-суммы, результаты автоматизированной обработки) не получают прямого процессуального признания. Подобный пробел нарушает принцип определенности процессуальной формы, закрепленный в ч. 2 ст. 75 УПК РФ, согласно которому доказательства, полученные с нарушением требований закона, являются недопустимыми [2]. Неясность правового статуса порождает неоднородность в правоприменении. Следователи и суды вынуждены самостоятельно определять процессуальную природу каждого цифрового массива, что снижает единообразие практики и создает риски для прав участников процесса.

В правоприменительной деятельности цифровая информация приравнивается к классическим категориям, предусмотренным статьями 81 и 84 УПК РФ [2]. Снимки экранов интернет-страниц, переписки из мессенджеров, серверные журналы и файлы с данными нередко включаются в дело в виде распечатанных копий или на электронных носителях без учета их специфики. Подобный подход оставляет без внимания динамику цифровой среды. Цифровые массивы информации не всегда тождественны классическим документам, а для проверки лог-файлов данных требуется специализированное программное обеспечение. Отнесение таких объектов к вещественным доказательствам влечет обязанность к их физическому хранению, что технически не всегда оправданно и возможно. Кроме того, при квалификации по ст. 84 УПК РФ утрачивается возможность применения специальных криминалистических методик исследования, а защита лишается четких процедурных механизмов оспаривания подлинности, поскольку стандарты проверки «иных документов» не учитывают риски незаметного внесения изменений в двоичные данные.

Верховный Суд Российской Федерации последовательно уточняет критерии, при которых цифровая информация считается допустимой. Так, в определении от 7 февраля 2023 года № 5-КГ22-144-К2 говорится

о том, что электронная переписка приобретает доказательственную силу лишь при установлении трех обстоятельств: принадлежности учетных записей конкретным лицам, документирования используемого способа связи и наличия возможности проверить содержание сообщений [3]. Также Пленум Верховного Суда в постановлении от 15 декабря 2022 года № 37 предлагает расширительную трактовку категорий «компьютерная информация» и «компьютерные устройства», относя к ним любые электронные сигналы, смартфоны и сведения, передаваемые по каналам связи (пункты 2 и 21). Пункт 24 того же постановления прямо рекомендует Судам привлекать специалистов для разъяснения технических понятий и аспектов [4]. Однако данные разъяснения не содержат унифицированного процессуального механизма фиксации цифровых следов на стадии предварительного расследования. На практике специалисты редко участвуют при первичном изъятии устройств, а их заключения часто сводятся к констатации фактов без анализа метаданных и алгоритмов обработки, что в условиях внедрения новых инструментов повышает риски принятия решений на основе непрозрачных результатов машинного анализа.

Одной из наиболее острых проблем также является доступ к информации, размещенной на зарубежных серверах. Подавляющее большинство востребованных мессенджеров и облачных платформ используют инфраструктуры, находящиеся под иностранной юрисдикцией. Статьи 165 и 453 УПК РФ [2] предписывают получать такие данные только через процедуры международной правовой помощи. Однако следственная практика идет по пути упрощения, нередко применяются неформальные способы изъятия информации, которые при процессуальной оценке признаются нарушающими законность получения доказательств. К этому добавляется проблема длительных сроков исполнения официальных запросов. За это время многие провайдеры уничтожают информацию в соответствии с собственными политиками хранения данных, что делает невозможным ее последующее получение и ставит под сомнение сохранность уже имеющихся доказательств.

Хоть цифровые доказательства и обладают рядом преимуществ, такими как компактность и возможность быстрой передачи, они имеют ряд сложностей и ограничений, связанных с фальсификацией. Сохранение неизменности информации в электронном формате является основной предпосылкой для признания ее допустимой, достоверной и целостной. В отличие от традиционных физических объектов, цифровые данные могут быть изменены без каких-либо внешне заметных следов. Именно поэтому важно чрезвычайно зафиксировать ее в первоначальном состоянии. Хотя в статье 164.1 УПК РФ содержатся общие положения об осмотре и изъятии электронных устройств, закон не предлагает специальных процедурных инструментов, которые бы гарантировали неизменность двоичных данных [2]. В результате возникает правовая зона неопределенности: техническая целостность остается без процессуального подтверждения, а любые нарушения на этапе фиксации автоматически влекут признание доказательств недопустимыми на основании статьи 75 УПК РФ [2].

В статье 164.1 УПК РФ [2] и закреплены общие положения, касающиеся порядка осмотра и изъятия электронных носителей информации, но в законодательстве не предусмотрены специальные механизмы и инструменты, которые могли бы гарантировать сохранность двоичных данных. В результате чего могут возникать различные погрешности, которые могут повлечь за собой признание доказательств недопустимыми.

В криминалистической практике для обеспечения целостности применяются технические и программные средства: аппаратные блокираторы записи, создание бит-в-бит копий (образов) носителей, криптографическое хеширование (алгоритмы SHA-256), ведение журналов действий и анализ в изолированных лабораторных средах. Как отмечается в учебнике под редакцией С. В. Зуева, целостность электронного доказательства должна пониматься не только как отсутствие изменений в файле, но и как подтвержденная последовательность действий от момента изъятия до представления в суд [5, с. 84–85].

Судебная практика также свидетельствует о том, что процессуальные ошибки, допущенные при обращении с цифровыми носителями, влекут за собой негативные последствия.

Зарубежный опыт, в частности стандарты NIST (SP 800-86), OSAC 2024-N-0011, предлагает четкую модель обеспечения целостности, основанную на таких принципах, как изоляция источника, документирование каждого действия, обязательная верификация хеш-сумм [6, 7]. В России отсутствует единый федеральный стандарт, обязательный для всех правоохранительных ведомств. Как отмечается в учебном издании под редакцией С. В. Зуева, ведомственные инструкции Министерства внутренних дел и Следственного комитета России разрознены и не всегда учитывают специфику облачных хранилищ и IoT-устройств [5, с. 153–159].

Обобщение кассационных решений за 2024–2025 годы свидетельствует о том, что суды последовательно исключают из доказательственной базы материалы, полученные с отступлением от предписаний УПК РФ [2]. В частности, недопустимыми признаются случаи, когда копирование данных производилось в отсутствие собственника (владельца) устройства либо без участия понятых, а также без надлежащего документирования процедуры в протоколе. Из этого следует вывод: в современном правоприменении понятие «целостность» цифрового доказательства трактуется расширительно. Оно охватывает не только техническую неизменность файла как таковую, но и неукоснительное соблюдение установленного законом порядка его получения.

Процесс оценки цифровых доказательств в уголовном судопроизводстве сегодня сопряжен с новыми вызовами. Эти сложности вызваны правовой неопределенностью и высокой технологической сложностью самих исследуемых объектов. В практической деятельности правоприменители зачастую ориентируются на непосредственное визуальное или слуховое восприятие цифровых материалов, что в условиях быстрого развития искусственного интеллекта становится крайне трудоемким подходом. Единые процессуальные критерии, позволя-

ющие быстро и эффективно оценить информацию в цифровой среде, до сих пор не сформированы. Из-за чего суды и следственные органы вынуждены опираться на устаревшие методики, не учитывающие новые цифровые риски, такие как полная генерация контента искусственным интеллектом (в том числе дипфейки), контекстуальное искажение.

В такой ситуации технологии искусственного интеллекта выполняют две противоположные, но взаимосвязанные роли. С одной стороны, алгоритмы машинного обучения стали инструментами фабрикации доказательств, таких как синтез голоса, создание дипфейков, генерация документов. Павел Карсаев, основатель проекта по бесплатному повышению осведомленности сотрудников малого и среднего бизнеса по вопросам информационной безопасности «ИБ-грамотность.рф», полагает, что использование дипфейков уже подпадает под нормы уголовного и административного законодательства, в зависимости от целей и последствий их применения. По его мнению, уголовно-правовая оценка действий с применением дипфейков должна определяться их фактической направленностью: «Если дипфейк используется для распространения ложной информации, это может квалифицироваться как клевета (ст. 128.1 Уголовного кодекса Российской Федерации (далее — УК РФ)). Если же поддельное видео или аудиозапись применяется для мошенничества, то речь идет уже о ст. 159 УК РФ (“Мошенничество”))» [8].

С другой стороны, те же самые технологии выступают в качестве ключевого средства верификации. Нейросетевые детекторы способны обнаруживать незаметные для человека следы генерации, анализировать большие массивы информации, сопоставлять акустические и визуальные закономерности.

Однако процессуальное использование результатов ИИ-анализа сталкивается с фундаментальной проблемой, которая заключается в том, что суды, стороны защиты и обвинения не имеют возможности проверить логику принятия решений нейросетью, что вступает в противоречие с принципом непосредственного исследования доказа-

тельств (ст. 240 УПК РФ) и требованием мотивированности судебных актов. Помимо этого, существующие экспертные методики в большинстве своем не приспособлены для работы с объектами, созданными или модифицированными нейросетями. Как отмечают Н. Ф. Бодров и А. К. Лебедева, в отсутствие специализированных разделов в методических рекомендациях вероятность выявления факта синтеза крайне низка. В ряде случаев эксперт приходит к выводу о невозможности предоставить ответ на поставленный вопрос. Для субъекта, назначившего экспертизу, подобное заключение фактически означает потерю возможности в дальнейшем использовать соответствующий факт в обоснование своей позиции [10, с. 19]. Дополнительную сложность представляет выявление признаков нейросетевой генерации: выполнение такой задачи доступно ограниченному числу высококвалифицированных специалистов, дефицит которых сохраняется.

Для преодоления выявленных недостатков представляется возможным реализовать комплекс мер нормативного и организационного характера. В частности, часть 2 статьи 74 УПК РФ целесообразно дополнить пунктом 4.1 «Цифровые доказательства». Кроме того, предлагается включить в УПК РФ статью 82.1 «Цифровые доказательства», закрепив в ней легальное определение соответствующего понятия и критерии допустимости цифрового доказательства, к которым относятся аутентичность, неизменность, законность получения и прослеживаемость происхождения. Представляется оправданным также утверждение межведомственного стандарта фиксации и хранения цифровых доказательств. Его положения могут охватывать порядок работы с облачными хранилищами, требования к обработке метаданных, правила хранения синтезированного контента и процедуры документирования цифровых следов. Дополнительным шагом должно стать принятие постановления Пленума Верховного Суда РФ, содержащего обобщение судебной практики оценки цифровых доказательств и разъяснения относительно процессуального статуса результатов, полученных с использованием технологий искусственного интеллекта.

Внедрение предложенных мер будет способствовать снижению правовой неопределенности, укреплению гарантий прав личности и повышению эффективности противодействия преступлениям, совершаемым с применением высоких технологий.

Список литературы

1. Генпрокуратура отметила спад темпов роста киберпреступности / Редакция сайта ТАСС // ТАСС: информационное агентство. 2025. 21 июля. URL: <https://tass.ru/obschestvo/24573429> (дата обращения: 23.05.2026).
2. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 09.04.2026) // Рос. газета. 2001. 22 декабря.
3. Определение Судебной коллегии по гражданским делам Верховного Суда Российской Федерации от 7 февраля 2023 г. № 5-КГ22-144-К2. URL: <https://legalacts.ru/sud/opredelenie-sudebnoy-kollegii-po-grazhdanskim-delam-verkhovnogo-suda-rossiiskoi-federatsii-ot-07022023-n-5-kg22-144-k2/> (дата обращения: 23.05.2026).
4. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 // Рос. газета. 2022. 28 декабря.
5. Электронные доказательства в уголовном судопроизводстве: учеб. для вузов / отв. ред. С. В. Зуев. М.: Юрайт, 2025. 193 с.
6. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response (NIST SP 800-86). Gaithersburg: NIST, 2006. 121 p.
7. Standard Guide for Forensic Digital Image: OSAC 2024-N-0011. 2 апреля. 2024. URL: https://www.nist.gov/system/files/documents/2024/03/29/OSAC%202024-N-0011%20Standard%20Guide%20for%20Forensic%20Digital%20Image%20Management_Version%201.0.pdf (дата обращения: 23.05.2026).
8. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 09.04.2026) // Рос. газета. 1996. 18 июня.
9. Никому не верю: как дипфейки повлияли на законодательство и судебную практику // Legal Academy: образовательная платформа. 1 апреля. 2025. URL: <https://legalacademy.ru/sphere/post/nikomu-ne-veryu-kak-dipeyki-povliyali-na-zakonodatelstvo-i-sudebnuyu-praktiku> (дата обращения: 23.05.2026).
10. Бодров Н. Ф., Лебедева А. К. Анализ судебной практики установления обстоятельств в случаях противоправного распространения генеративного контента, созданного с помощью технологий искусственного интеллекта // Юридические исследования. 2024. № 11. С. 1–25.