Вестник Восточно-Сибирского института МВД России. 2026. № 1 (116). С. 214-227.
Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2026, vol. 116, no. 1, pp. 214-227.

5.1.4. Уголовно-правовые науки (юридические науки)

Научная статья
УДК 343.985.7+343.1

ЭЛЕКТРОННО-ЦИФРОВЫЕ СЛЕДЫ КАК ДОКАЗАТЕЛЬСТВА ПРИ РАССЛЕДОВАНИИ ИНТЕРНЕТ-МОШЕННИЧЕСТВ: КРИМИНАЛИСТИЧЕСКИЕ И ПРОЦЕССУАЛЬНЫЕ АСПЕКТЫ

Родивилина Виктория Александровна[1], Коломинов Вячеслав Валентинович[2]
[1]Восточно-Сибирский институт МВД России, Иркутск, Российская Федерация, 377b@bk.ru, https://orcid.org/0000-0003-3231-1885
[2]Байкальский государственный университет, Иркутск, Российская Федерация, offroad88@mail.ru, https://orcid.org/0000-0001-9797-0908

Введение. Статья посвящена комплексному исследованию криминалистической природы и доказательственного значения электронно-цифровых следов в расследовании интернет-мошенничеств. В работе рассматривается необходимость различения пользовательских и автоматически формируемых следов, подробно раскрываются особенности их возникновения, классификации и процессуальной фиксации. Проведенный анализ действующего уголовно-процессуального законодательства показал, что в нем отсутствуют четкие нормы, регулирующие порядок извлечения, фиксации и использования цифровых следов в качестве доказательств, что приводит к разнородной судебной практике и неоднозначной оценке их допустимости. Для сопоставления подходов к работе с цифровыми данными проведен сравнительно-правовой анализ зарубежного опыта, включая законодательные инициативы США и Европейского союза, позволяющий выделить эффективные методы фиксации и оценки цифровой информации. На основании полученных данных обосновывается необходимость разработки национального регламента работы с электронно-цифровыми следами, который соответствовал бы современным международным стандартам цифровой криминалистики и обеспечивал бы единообразие процедур извлечения и проверки достоверности цифровых доказательств, а также внесение изменений в уголовно-процессуальное законодательство с целью повышения доказательственной ценности таких следов и снижения рисков их признания недопустимыми в суде.

Материалы и методы. В исследовании использованы методы сравнительно-правового анализа, изучение судебной практики, а также анализ международных стандартов цифровой криминалистики. Особое внимание уделено работам современных исследователей, рассматривающих вопросы обработки больших данных и использования алгоритмов искусственного интеллекта.

Результаты исследования. Выявлены ключевые проблемы процессуального характера: отсутствие в УПК РФ специальных норм для электронно-цифровых следов, неопределенность процедур извлечения автоматически генерируемых данных, разнородная судебная практика. Установлено, что существующие методы работы с цифровыми следами не учитывают их специфику, что снижает доказательственную ценность. Показана эффективность международных стандартов при обработке цифровой информации.

Выводы и заключения. Для решения выявленных проблем предлагаются: разработка федерального положения о цифровых следах, внедрение международных стандартов работы с ЭЦС, создание методических рекомендаций для следователей и экспертов. Подчеркивается необходимость модернизации уголовно-процессуального законодательства с учетом современных цифровых реалий.

Ключевые слова: криминалистика, цифровые доказательства, интернет-мошенничество, электронно-цифровые следы, допустимость доказательств, цифровая экспертиза, международные стандарты

Для цитирования: Родивилина, В. А., Коломинов, В. В. Электронно-цифровые следы как доказательства при расследовании интернет-мошенничеств: криминалистические и процессуальные аспекты // Вестник Восточно-Сибирского института МВД России. 2025. № 1 (116). С. 214-227.

5.1.4. Criminal Law Sciences
(Legal Sciences)

Original article

DIGITAL TRACES AS EVIDENCE IN INTERNET FRAUD INVESTIGATIONS: FORENSIC AND PROCEDURAL ASPECTS

Viktoriia A. Rodivilina[1], **Viacheslav V. Kolominov**[2]
[1]East Siberian Institute of the Ministry of Internal Affairs of Russia, Irkutsk, Russian Federation, 377b@bk.ru, https://orcid.org/0000-0003-3231-1885
[2]Baikal State University, Irkutsk, Russian Federation, offroad88@mail.ru, https://orcid.org/0000-0001-9797-0908

Introduction.

This article provides a comprehensive study of the forensic nature and evidentiary value of digital traces in internet fraud investigations, emphasizing the distinction between user-generated and automated traces [1]. The analysis reveals a lack of clear legal norms governing the extraction, preservation, and use of these traces, leading to inconsistent judicial

practice [1]. To improve upon this, a comparative legal analysis of international experiences—including initiatives in the US and the EU—highlights effective techniques for documenting and evaluating digital information [1]. For more details, read the full study.

The article is devoted to a comprehensive study of the forensic nature and evidentiary value of digital traces in the investigation of internet fraud. The work examines the necessity of distinguishing between user-generated and automatically generated traces, detailing the specifics of their origin, classification, and procedural documentation. The analysis of the current criminal procedure legislation has shown a lack of clear norms regulating the procedures for the extraction, documentation, and use of digital traces as evidence, which leads to inconsistent judicial practice and ambiguous assessment of their admissibility. A comparative legal analysis of foreign approaches, including legislative initiatives from the United States and the European Union, was conducted to contrast methods of handling digital data, highlighting effective techniques for documenting and evaluating digital information. Highlighting effective techniques for documenting and evaluating digital information, the authors substantiate the need to develop a national protocol for handling digital traces. This protocol should align with modern international standards of digital forensics and ensure uniformity in procedures for extracting and verifying the authenticity of digital evidence. Furthermore, the authors propose amendments to criminal procedure legislation to enhance the evidentiary value of such traces and reduce the risk of them being deemed inadmissible in court.

Materials and Methods. The research employed methods of comparative legal analysis, study of judicial practice, and analysis of international digital forensics standards. Particular attention was paid to the works of contemporary researchers examining big data processing and the use of artificial intelligence algorithms.

The Results of the Study. The study identifies several key procedural issues: the lack of specific provisions for digital traces in the Criminal Procedure Code of the Russian Federation (CPC RF), procedural uncertainty regarding the extraction of automatically generated data, and inconsistent judicial practice. It was established that current methods of handling digital traces fail to account for their unique characteristics, thereby diminishing their evidentiary value. Furthermore, the utility of international standards in processing digital information was demonstrated.

Findings and Conclusions. To address the identified issues, the authors propose the development of a federal framework on digital traces, the implementation of international standards for handling digital evidence, and the creation of methodological guidelines for investigators and forensic experts. The study emphasizes the necessity of modernizing criminal procedure legislation to align it with contemporary digital realities.

Keywords: forensics, digital evidence, internet fraud, digital traces, admissibility of evidence, digital examination, international standards

For citation: Rodivilina, V. A., Kolominov, V. V. Elektronno-cifrovye sledy kak dokazatel'stva pri rassledovanii internet-moshennichestv: kriminalisticheskie i processual'nye aspekty [Digital Traces as Evidence in Internet Fraud Investigations: Forensic and Procedural Aspects]. Vestnik Vostochono-Sibirskogo institute MVD Rossii – Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2025, vol. 116, no. 1, pp. 214-227. (In Russ.)

В условиях стремительного развития цифровых технологий наблюдается значительное увеличение количества преступлений, совершаемых в информационно-телекоммуникационной среде, а особенно интернет-мошенничества, отличающиеся разнообразием форм, анонимностью преступников и сложностью их пресечения. Однако криминалистические методики зачастую отстают от уровня технической сложности и не соответствуют уровню технологического развития таких преступлений. В связи с этим необходима разработка научно обоснованного подхода к классификации и оценке электронно-цифровых следов (далее – ЭЦС) с учетом специфики интернет-мошенничеств как высокоадаптивной и трансграничной формы преступности. В современных условиях ЭЦС приобретают ключевое значение как важнейший источник сведений о механизме, способе и участниках преступления. Их анализ требует применения специализированных знаний и криминалистических методов, адаптированных к условиям виртуальной среды. В настоящем исследовании акцент сделан на уточнении юридической и криминалистической природы автоматических ЭЦС, особенностях их фиксации, допустимости и использования в доказательственном процессе при расследовании интернет-мошенничеств.

Следует различать электронные следы, оставленные в результате действий пользователя (например, метаданные файлов, куки, сетевой трафик), и следы, порождаемые автоматически в результате функционирования технической инфраструктуры. Последние требуют особых условий извлечения и чаще всего вызывают дискуссии в правоприменительной и научной среде, особенно в части их процессуальной допустимости и достоверности как доказательств.

Расследование мошенничеств, совершаемых с использованием цифровых технологий, связано с рядом затруднений: анонимностью злоумышленников, трансграничным характером преступлений, многообразием цифровых платформ и инструментов. При этом традиционные методики криминалистики не всегда позволяют эффективно работать с ЭЦС. Это обусловливает необходимость комплексного изучения природы, классификации и значимости ЭЦС при расследовании интернет-мошенничеств, а также совершенствования методического инструментария, применяемого к таким следам.

Современные исследования, посвященные ЭЦС, охватывают широкий спектр проблем – от их классификации до вопросов правового регулирования и судебной оценки. Так, М. М. Льянов рассматривает ЭЦС как разновидность вещественных доказательств, обладающих криминалистической значимостью при расследовании преступлений в сети Интернет [1, с. 21]. В свою очередь, С. В. Тимофеев и Р. Х. Кочесоков отмечают, что их фиксация и последующее использование в доказывании напрямую влияют на качество собранной информации, которая в соответствии с уголовно-процессуальным законодательством может приобрести статус доказательств [2, с. 266]. Это актуализирует необходимость развития как новых, так и существующих инструментов противодействия цифровой преступности. Важность ЭЦС для раскрытия преступлений отмечает и ряд других ученых, указывая, что цифровой след состоит из двух элементов: материального носителя (электромагнитного поля) и информации – сведений об объективной реальности, сохраняющихся в компьютерных и иных цифровых устройствах [3, с. 39].

Зарубежная доктрина трактует цифровые доказательства преимущественно через призму их процессуальной целостности и аутентичности. E. H. Spafford подчеркивает их латентность и нестабильность, а также уязвимость к изменениям при некорректных действиях [4, p. 6]. В связи с этим международные стандарты, закрепленные, в частности, в ISO/IEC 27037:2012 [1], устанавливают требования к идентификации, извлечению и сохранению цифровых доказательств, делая акцент на обязательном документировании всех операций (создание хеш-сумм, использование write-blockers, ведение цепочки хранения) для последующего обоснования их допустимости в суде. E. Casey определяет цифровые доказательства как «любую информацию, пригодную для установления факта, которая либо создается, либо сохраняется в цифровой форме и извлекается с цифрового устройства» [5, p. 4]. При этом их уникальной особенностью он называет зависимость от контекста и обстоятельств дела, что предопределяет необходимость тщательного документирования процедур получения и хранения.

Таким образом, зарубежный опыт демонстрирует, что правовую значимость имеют не сами по себе извлеченные данные, а корректно задокументированный процесс их получения, гарантирующий достоверность и неизменность ЭЦС. В странах общего права (США, Великобритания) данные подходы закрепились в судебной практике, где критериями допустимости доказательств выступают корректность процедуры и возможность ее верификации.

Показательным примером применения данного подхода является знаковое дело «Lorraine v. Markel American Insurance Co.» (241 F.R.D. 534, D. Md. 2007)[2]. Судья Пол Гримм в своем решении детально проанализировал вопросы допустимости электронных доказательств, сформулировав теперь уже классический пятиэтапный тест для их оценки. Суд постановил, что для признания электронных данных допустимыми необходимо последовательно доказать их:

– релевантность (отношение к делу);

– подлинность (аутентичность) – то, что данные являются тем, чем их заявляет сторона;

– ненарушение правил о hearsay (недопустимости слухов) – если данные содержат утверждения, offered for the truth of the matter;

– соответствие правилу best evidence (наилучшего доказательства) – использование оригиналов или обоснование их отсутствия;

– надежность (reliability) процесса их создания и хранения.

В контексте автоматических ЭЦС ключевыми стали критерии подлинности (authenticity) и надежности (reliability). Суд указал, что подлинность электронных данных, включая автоматические логи и метаданные, может быть установлена не только прямыми свидетельскими показаниями, но и косвенными доказательствами, описывающими процесс и систему их генерации. Достаточным для этого может быть,

[1] ISO/IEC 27037:2012. Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence // iso.org : сайт. URL: https://www.iso.org/standard/44381.html (дата обращения: 21.07.2025).

[2] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534 (D. Md. 2007) // Federal Rules Decisions. 2007, vol. 241, pp. 534-553.

например, показание системного администратора о стандартных настройках программного обеспечения, генерирующего такие логи, или эксперта, объясняющего механизм их формирования и отсутствие признаков подделки. Таким образом, данный прецедент сместил фокус с невозможности допросить «очевидца» создания каждой записи на проверку исправности и стандартности работы системы, что открыло дорогу для широкого использования автоматических ЭЦС в судах стран общего права.

В Европейском союзе идет активная работа по созданию единого правового пространства для электронных доказательств. Регламент (ЕС) 2023/1543 (e-Evidence)[3], вступивший в силу в 2023 году, направлен на упрощение трансграничного доступа к электронным данным. Его ключевые принципы – взаимное признание электронных доказательств государствами-членами и соблюдение строгих стандартов их сбора провайдерами услуг связи. Это создает правовую основу для признания автоматически генерируемых ЭЦС, полученных из-за рубежа, при условии соблюдения унифицированных процедур.

Таким образом, международная тенденция заключается в смещении акцента с теоретических споров о природе цифровых следов на практическую стандартизацию процессов их обработки, что обеспечивает необходимый уровень доверия со стороны суда. Для российской системы заимствование подобных подходов имеет значение в контексте выработки единых стандартов обращения с ЭЦС, что позволит повысить их доказательственную ценность и снизить риск процессуальных ошибок.

Анализ показал, что ЭЦС представляют собой продукт взаимодействия пользователя с цифровой средой, фиксируемый в виде логов, метаданных, сетевой активности, копий сообщений, электронных следов оплаты и других форм.

ЭЦС можно классифицировать по нескольким ключевым критериям:

1. По месту фиксации:

– на устройствах пользователя (компьютерах, смартфонах);

– на удаленных серверах (облачных хранилищах, корпоративных системах).

2. По способу образования:

– намеренные (созданные сознательными действиями пользователя);

– непреднамеренные (сформированные автоматически в процессе работы систем).

3. По содержательной направленности:

– сведения о личности (учетные данные, биометрия);

– данные о действиях (история посещений, транзакции);

– временные и пространственные метки (геолокация, таймстемпы).

Для фиксации ЭЦС применяются специализированные методы: форензик-извлечение, анализ лог-файлов, парсинг сетевого трафика, зеркалирование серверов.

Особую категорию составляют автоматически генерируемые следы, которые формируются без прямого участия пользователя. Как отмечает А. В. Кутузов,

[3] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings // Official Journal of the European Union. 2023. L 191. pp. 118-180. URL: https://eur-lex.europa.eu/eli/reg/2023/1543/oj/eng (дата обращения: 21.07.2025).

современные транспортные средства представляют собой уникальный источник таких доказательств, генерируя: точные параметры движения (скорость, координаты через системы типа ЭРА-ГЛОНАСС), детальную телеметрию бортовых систем и даже биометрические показатели водителя, фиксируемые датчиками усталости и контроля состояния [6, с. 81–83].

По результатам проведенных исследований можно утверждать, что данные этой категории характеризуются высокой доказательственной ценностью, поскольку позволяют детально реконструировать события; в то же время они отличаются технической сложностью извлечения, требующей применения специализированного программного обеспечения, и подвержены проблеме верификации, заключающейся в необходимости подтверждения их неизменности [6, с. 79–87.]

К автоматическим ЭЦС относят системные журналы, временные метки, записи активности серверов, данные маршрутизации и иные аналогичные источники. При корректном изъятии они могут обладать высокой доказательственной ценностью, однако их непроизвольный характер вызывает сомнения у следственных органов и судов относительно подлинности и соответствия объективной действительности. В связи с этим, как подчеркивают С. Е. Квасница и С. Ю. Бирюков, «деятельность субъекта расследования по поиску и изучению электронных доказательств в ходе производства по уголовному делу должна быть надлежащим образом обоснована имеющимися фактическими данными и осуществлена в строгом соответствии с законом» [7, с. 17].

В рамках цифровой криминалистики наблюдается определенная дихотомия в оценке доказательственной значимости автоматических ЭЦС. С одной стороны, как справедливо указывает E. Casey, машинные журналы, не подверженные субъективному влиянию человека, обладают потенциально большей объективностью [5, p. 152]. С другой стороны, их верификация представляет собой серьезную методологическую задачу, поскольку следователю и суду зачастую недоступна возможность проверить корректность работы алгоритмов, формирующих такие следы.

Разрешение этого противоречия не заключается в отказе от использования автоматических данных, а предполагает создание системы «технического доверия», базирующейся на следующих принципах:

– верификация алгоритмов: государственная аккредитация программных комплексов, применяемых для генерации и извлечения критически важных ЭЦС (например, логов банковских систем, интернет-провайдеров, государственных сервисов), с проведением экспертизы их кода на предмет корректности;

– сертификация источников данных: признание допустимыми автоматических ЭЦС, полученных из информационных систем, прошедших сертификацию ФСТЭК или ФСБ России, подтверждающую надежность и безопасность их функционирования;

– презумпция исправности технических средств: закрепление в законе презумпции корректной работы технического средства и достоверности сгенерированных им данных, если сторона защиты не докажет обратное через назначение соответствующей судебной экспертизы.

Применение такого подхода позволяет сместить акцент с теоретического обсуждения природы данных на практические механизмы их проверки и обеспечения достоверности.

В судебной практике встречаются случаи признания автоматических данных недопустимыми доказательствами в связи с отсутствием регламентированного протокола их извлечения. Например, в апелляционном определении Курганского областного суда от 24 августа 2021 г. по делу № 22-1169/2021 суд поддержал позицию защиты и признал распечатки электронной переписки недопустимым доказательством, указав, что «процесс изъятия… надлежащим образом не задокументирован, не указано, с помощью каких технических средств, какого программного обеспечения осуществлялось изъятие» [4] . Аналогичная проблема с фиксацией обстоятельств извлечения цифровых данных отмечена, в частности, постановлением Президиума Московского областного суда от 17 февраля 2021 г. № 44У-16/2021, который исключил скриншоты как доказательство, поскольку «не приведено данных о программном обеспечении, с помощью которого они были получены»[5]. Указанная проблема носит системный характер, что подтверждается аналогичными решениями других судов общей юрисдикции[6].

Данные прецеденты демонстрируют, что допустимость автоматических данных определяется не их содержанием, а соблюдением формализованной процедуры извлечения, обеспечивающей аутентичность и целостность.

Проблема допустимости автоматически генерируемых ЭЦС в уголовном судопроизводстве по-прежнему остается предметом научной дискуссии. По наблюдению А. А. Бессонова, современные технологии искусственного интеллекта демонстрируют высокую точность анализа цифровых следов, достигающую 98 %, что находит применение, в частности, при географическом профилировании преступников [8, с. 97–98]. Однако отсутствие четко закрепленных законодательных и процессуальных стандартов извлечения и обработки таких данных значительно снижает их доказательственную ценность. Характерный пример, отраженный в практике Архангельского областного суда, подтверждает необходимость разработки унифицированных регламентов работы с автоматическими ЭЦС, которые обеспечили бы баланс между их объективностью и юридической надежностью.

При этом в научной литературе неоднократно подчеркиваются и объективные преимущества автоматических следов: они в меньшей степени подвержены фальсификации по сравнению с пользовательскими данными, исключают субъективное искажение информации и обеспечивают высокую детализацию временных меток [5, p. 201–207]. По мнению А. А. Бессонова, раскрытие этого потенциала возможно лишь при наличии комплексной нормативной базы, которая будет регламентировать методы извлечения автоматических ЭЦС, порядок их верификации и критерии достоверности [8, с. 98–99].

---

[4] Апелляционное определение Курганского областного суда от 24 августа 2021 г. по делу № 22-1169/2021 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru/regular/doc/4C3fPcFdP18W/ (дата обращения: 01.08.2025).

[5] Постановление Президиума Московского областного суда от 17 февраля 2021 г. № 44У-16/2021 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru/regular/doc/4C3fPcFdP18W/ (дата обращения: 01.08.2025).

[6] Обзор судебной практики Верховного Суда Российской Федерации № 1 (2021) : утв. Президиумом Верховного Суда Российской Федерации 22 января 2021 г. // Бюллетень Верховного Суда РФ. 2022. № 4.

Даже при условии разработки таких регламентов необходима их гармонизация с международными и национальными стандартами. В частности, в ISO/IEC 27037:2012 определены ключевые процедуры идентификации, сбора и сохранения цифровых доказательств, гарантирующие надежность и неизменность полученной информации.

В российской же практике неопределенность усугубляется сложной природой ЭЦС, что требует как правового, так и методического упорядочения порядка обращения с ними. Как справедливо отмечается в научной литературе, они представляют собой сложную информационную структуру, в которой, наряду с уголовно-релевантной информацией, содержится значительный объем вспомогательных данных, отвечающих за ее целостность и возможность восприятия [9, с. 105–107; 10, с. 95; 11, с. 79–80]. Особую сложность представляет работа с автоматически формируемыми ЭЦС, которые являются следствием воздействия технологических процессов без участия человека и вне его желания [12, с. 108]. К ним, в частности, относятся и цифровые отпечатки компьютерных устройств (Device Fingerprint) – уникальные идентификаторы, формируемые в виде производного значения параметров конфигурации программного и аппаратного обеспечения устройства. Важность их фиксации трудно переоценить, так как подделать такой отпечаток практически невозможно, а его идентификационный потенциал крайне высок [13, с. 390, 392]. Однако отсутствие законодательно закрепленного порядка их извлечения и процессуального закрепления (например, в соответствии с регламентом, подобным Стандарту Банка России СТО БР БФБО-1.7-2023 [7]) создает риски модификации или удаления данных и ставит под сомнение допустимость полученных с их помощью доказательств, несмотря на их объективную доказательственную ценность.

В целях обеспечения допустимости автоматических ЭЦС представляется целесообразным:

– разработать национальные методические рекомендации для экспертов и следователей;

– закрепить обязательность протоколирования программно-технических средств, используемых при извлечении следов;

– ввести экспертную оценку степени автоматичности и подверженности модификации каждого цифрового следа как отдельного элемента доказательственной базы.

Представляется, что для преодоления указанных трудностей необходима нормативная регламентация обращения с автоматическими ЭЦС, а также разработка специализированных методических рекомендаций, обеспечивающих их надлежащую процессуальную оценку. В частности, регламент должен включать:

– исчерпывающий перечень технических требований к средствам извлечения ЭЦС, включая обязательную верификацию результатов с помощью

[7] Стандарт Банка России СТО БР БФБО-1.7-2023. Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов с использованием технологии цифровых отпечатков устройств : принят и введен в действие приказом Банка России от 1 марта 2023 г. № ОД-335 «О введении в действие стандарта Банка России СТО БР БФБО-1.7-2023 // cbr.ru : сайт. URL: https://cbr.ru/Crosscut/LawActs/File/6177 (дата обращения: 05.08.2025).

криптографических хэш-функций (например, SHA-256) и ведение журнала аудита всех операций для обеспечения воспроизводимости процесса;

– четкий алгоритм действий следователя и специалиста при работе с автоматическими следами: от обеспечения целостности носителя на месте изъятия (с использованием аппаратных write-блокировщиков) до передачи материалов на экспертизу;

– процедуру сертификации программного обеспечения, используемого для извлечения и анализа ЭЦС, с созданием государственного реестра одобренных программных комплексов криминалистического извлечения данных, алгоритмы которых прошли верификацию;

– типовую форму протокола изъятия ЭЦС, обязывающую фиксировать не только обстоятельства обнаружения, но и метаданные процедуры извлечения: наименование и версию ПО, значение контрольных сумм (хешей), системное время и параметры настройки инструментов;

– критерии оценки допустимости автоматических ЭЦС судом, смещающие фокус с субъективного участия человека в их создании на проверку соблюдения регламента их извлечения и неизменности полученных данных.

Такой детализированный подход позволит устранить существующий правовой вакуум и создать унифицированную практику использования автоматических ЭЦС в уголовном судопроизводстве.

Актуальность проблем использования ЭЦС при расследовании интернет-мошенничеств определяется необходимостью комплексного подхода к их правовому и методическому обеспечению. С. А. Машков отмечает, что несмотря на возрастающую доказательственную ценность цифровых следов, сохраняется значительный правовой вакуум в части их процессуального закрепления и методического сопровождения [14, с. 84]. Действующее уголовно-процессуальное законодательство не содержит специальных норм, учитывающих специфику ЭЦС, вследствие чего они нередко квалифицируются как документы или вещественные доказательства (ст. 74 УПК РФ) без учета особенностей их нематериальной природы. Отсутствие регламентированных процедур извлечения и фиксации автоматически генерируемых данных приводит к неопределенности их оценки в судебной практике. Судебные решения по аналогичным делам демонстрируют неоднородность: ЭЦС то приравниваются к иным доказательствам, то отклоняются по формальным основаниям.

Методические аспекты также остаются недостаточно разработанными. Отсутствие унифицированных стандартов проверки и необходимость специальных технических знаний затрудняют корректное использование ЭЦС при расследовании. В то же время опыт анализа «больших данных», включая обработку информации из социальных сетей, открытых реестров, поисковых систем и иных источников, показывает возможности обеспечения неизменности цифровых доказательств и повышения их достоверности. В этой связи С. А. Машков обосновывает необходимость системного вовлечения ресурсов «больших данных» в криминалистическую практику, расширения судебно-экспертных исследований цифровой информации и привлечения специалистов в области информационно-аналитической деятельности [14, с. 84].

Таким образом, ЭЦС обладают высоким доказательственным потенциалом, однако их использование сопряжено с риском недооценки при отсутствии специализированных процессуальных и методических стандартов. Это обусловливает необходимость разработки нормативного регулирования и практических рекомендаций, адаптированных к особенностям автоматически формируемых цифровых данных.

Выделение ЭЦС в самостоятельный объект криминалистического исследования и их включение в систему доказывания отражают закономерный этап технологической эволюции криминалистики. Для реализации их потенциала требуется дальнейшее совершенствование методики извлечения, фиксации, интерпретации и оценки таких следов, а также закрепление их правового статуса в уголовно-процессуальном законодательстве.

Несмотря на объективные преимущества автоматических ЭЦС, их использование должно быть обусловлено разработкой законодательно закрепленных стандартов верификации, включая сертификацию программного обеспечения (далее – ПО) и презумпцию исправности технических средств при соблюдении установленных процедур извлечения. В связи с этим представляется необходимым разработать и закрепить на законодательном уровне Положение о порядке извлечения, фиксации и исследования электронно-цифровых следов. Его ключевыми разделами должны стать:

– Иерархия и классификация ЭЦС: закрепление предложенной в настоящей статье классификации (по способу образования, месту хранения и содержанию) для определения процессуального режима работы с каждым типом следов.

– Требования к программно-аппаратным комплексам: создание реестра аккредитованных Минюстом или Следственным комитетом Российской Федерации программных средств (например, на базе отечественного ПО) для криминалистического извлечения данных, чьи алгоритмы верифицированы и обеспечивают неизменность оригинального носителя.

– Унифицированный протокол извлечения: обязательная фиксация в протоколе следственного действия хэш-сумм извлеченных данных, точного наименования, версии и лицензии использованного ПО, параметров настройки оборудования, Ф. И. О. и квалификации специалиста, производившего извлечение.

– Статус специалиста: закрепление требований к образованию и компетенциям специалиста (криминалиста-программиста), привлекаемого для извлечения ЭЦС, с возможностью возложения на него функции понятого в случаях, требующих специальных знаний.

Эффективное использование ЭЦС требует не только нормативного упорядочения, но и методического сопровождения на всех этапах их получения, интерпретации и представления в суде. Это делает необходимым формирование единой научно-методической базы цифровой криминалистики и подготовку централизованных рекомендаций для следователей и экспертов. Особое значение приобретает интеграция национальных подходов с международными стандартами в условиях роста трансграничной цифровой преступности, а также участие России в глобальных инициативах по развитию цифровой криминалистики.

Проведенное исследование демонстрирует, что систематизация знаний о природе, классификации и механизмах формирования ЭЦС, а также устранение

методических и процессуальных противоречий способствуют повышению эффективности борьбы с киберпреступностью и укреплению доверия граждан к правоохранительным органам. Развитие данного направления криминалистической науки и практики является важным условием обеспечения правовой безопасности и надежности системы правосудия в условиях цифровой реальности.

СПИСОК ИСТОЧНИКОВ

1. Льянов, М. М. Криминалистическое значение электронно-цифровых следов преступлений экстремистской и террористической направленности в сети «Интернет» : дис. ... канд. юрид. наук. Екатеринбург, 2025. 256 с.

2. Тимофеев, С. В., Кочесоков, Р. Х. Перспективы совершенствования российского законодательства в области использования цифровых следов преступления // Вестник Восточно-Сибирского института МВД России. 2024. № 4 (111). С. 262–277.

3. Цифровая валюта и цифровые финансовые права как предмет и средство совершения преступлений : монография / О. П. Грибунов, П. В. Никонов, С. В. Пархоменко и др. Иркутск : Иркутский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2023. 170 с.

4. Spafford, E. H. Some Musings on Digital Forensics // Journal of Digital Forensics, Security and Law. 2006, vol. 1, no. 1, pp. 3–9.

5. Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed. Academic Press, 2011, 807 p.

6. Кутузов, А. В. Отдельные направления использования компьютерных систем автомобиля для решения криминалистических задач // Сибирские уголовно-процессуальные и криминалистические чтения. 2025. № 1 (47). С. 79–87.

7. Квасница, С. Е., Бирюков, С. Ю. Электронные доказательства: проблемы допустимости в уголовном судопроизводстве // Вестник Волгоградской академии МВД России. 2024. № 2 (69). С. 104–111.

8. Бессонов, А. А. Современные информационные технологии на службе следствия // Сибирские уголовно-процессуальные и криминалистические чтения. 2022. № 1 (35). С. 94–100.

9. Мещеряков, В. А. Теоретические основы механизма следообразования в цифровой криминалистике : монография. М. : Проспект, 2022. 176 с.

10. Стельмах, В. Ю. Электронная информация в доказывании по уголовным делам: способы получения и место в системе доказательств // Библиотека криминалиста. Научный журнал. 2018. № 3 (38). С. 93–100.

11. Хомяков, Э. Г. О сущности цифровых следов в криминалистике и их фиксации // Общество, право, государственность: ретроспектива и перспектива. 2025. № 1 (21). С. 71–82.

12. Бычков, В. В., Вехов, В. Б. Электронное следообразование преступной деятельности в сети Интернет // Расследование преступлений: проблемы и пути их решения. 2020. № 1 (27). С. 106–111.

13. Вехов, В. Б., Смушкин, А. Б. Криминалистическое исследование цифровых отпечатков компьютерных устройств // Всероссийский криминологический журнал. 2024. Т. 18. № 4. С. 390–397.

14. Машков, С. А. «Большие данные» и криминалистика: возможности и перспективы // Сибирские уголовно-процессуальные и криминалистические чтения. 2024. № 2 (44). С. 78–86.

REFERENCES

1. Lyanov, M. M. Kriminalisticheskoe znachenie elektronno-cifrovyh sledov prestuplenij jekstremistskoj i terroristicheskoj napravlennosti v seti «Internet» [Forensic significance of electronic-digital traces of extremist and terrorist crimes on the Internet]. 2025, 256 p. (In Russ.).

2. Timofeev, S. V., Kochesokov R. H. Perspektivy sovershenstvovanija rossijskogo zakonodatel'stva v oblasti ispol'zovanija cifrovyh sledov prestuplenija [Prospects for improving Russian legislation in the field of using digital traces of crime]. Vestnik Vostochno-Sibirskogo instituta MVD Rossii – Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2024, vol. 111, no. 4, pp. 262-277. (In Russ.).

3. Gribunov, O. P., Nikonov, P. V., Parkhomenko, S. V. Cifrovaja valjuta i cifrovye finansovye prava kak predmet i sredstvo sovershenija prestuplenij [Digital currency and digital financial rights as a subject and means of committing crimes]. Irkutsk, 2023, 170 p. (In Russ.).

4. Spafford, E. H. Some Musings on Digital Forensics. Journal of Digital Forensics, Security and Law. 2006, vol. 1, no. 1, pp. 3-9.

5. Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed. Academic Press, 2011, 807 p.

6. Kutuzov, A. V. Otdel'nye napravlenija ispol'zovanija komp'juternyh sistem avtomobilja dlja reshenija kriminalisticheskih zadach [Certain directions of using car computer systems for solving forensic problems]. Sibirskie ugolovno-processual'nye i kriminalisticheskie chtenija – Siberian Criminal Procedure and Forensic Readings. 2025, vol. 47, no. 1, pp. 79-87. (In Russ.).

7. Kvasnica, S. E., Birjukov, S. Ju. Jelektronnye dokazatel'stva: problemy dopustimosti v ugolovnom sudoproizvodstve [Electronic evidence: problems of admissibility in criminal proceedings]. Vestnik Volgogradskoj akademii MVD Rossii – Vestnik of the Volgograd Academy of the Ministry of Internal Affairs of Russia. 2024, vol. 69, no. 2, pp. 104-111. (In Russ.).

8. Bessonov, A. A. Sovremennye informacionnye tehnologii na sluzhbe sledstvija [Modern information technologies in the service of investigation]. Sibirskie ugolovno-processual'nye i kriminalisticheskie chtenija – Siberian Criminal Procedure and Forensic Readings. 2022, vol. 35, no. 1, pp. 94-100. (In Russ.).

9. Meshherjakov, V. A. Teoreticheskie osnovy mehanizma sledobrazovanija v cifrovoj kriminalistike [Theoretical foundations of the trace formation mechanism in digital forensics]. Moscow, Prospekt, 2022, 176 p. (In Russ.).

10. Stel'mah, V. Ju. Jelektronnaja informacija v dokazyvanii po ugolovnym delam: sposoby poluchenija i mesto v sisteme dokazatel'stv [Electronic information in criminal proceedings: methods of obtaining and place in the system of evidence]. Biblioteka kriminalista – The Forensic Scientist's Library. 2018, vol. 38, no. 3, pp. 93-100. (In Russ.).

11. Homjakov, Je. G. O sushhnosti cifrovyh sledov v kriminalistike i ih fiksacii [On the essence of digital traces in forensics and their fixation]. Obshhestvo, pravo, gosudarstvennost': retrospektiva i perspektiva – Society, Law, Statehood: Retrospective and Perspective. 2025, vol. 21, no. 1, pp. 71-82. (In Russ.).

12. Bychkov, V. V., Vekhov, V. B. Jelektronnoe sledoobrazovanie prestupnoj dejatel'nosti v seti Internet [Electronic trace formation of criminal activity on the Internet]. Rassledovanie prestuplenij: problemy i puti ih reshenija – Crime Investigation: Problems and Solutions. 2020, vol. 27, no. 1, pp. 106-111. (In Russ.).

13. Vekhov, V. B., Smushkin, A. B. Kriminalisticheskoe issledovanie cifrovyh otpechatkov komp'juternyh ustrojstv [Forensic study of digital fingerprints of computer devices]. Vserossijskij kriminologicheskij zhurnal – Russian Journal of Criminology. 2024, vol. 18, no. 4, pp. 390-397. (In Russ.).

14. Mashkov, S. A. «Bol'shie dannye» i kriminalistika: vozmozhnosti i perspektivy ["Big Data" and forensics: opportunities and prospects]. Sibirskie ugolovno-processual'nye i kriminalisticheskie chtenija – Siberian Criminal Procedure and Forensic Readings. 2024, vol. 44, no. 2, pp. 78-86. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Родивилина Виктория Александровна, кандидат юридических наук, доцент, доцент кафедры криминалистики. Восточно-Сибирский институт МВД России. 664074, Россия, г. Иркутск, ул. Лермонтова, 110.

Коломинов Вячеслав Валентинович, кандидат юридических наук, доцент, доцент кафедры криминалистики, судебных экспертиз и юридической психологии. Байкальский государственный университет. 644025, г. Иркутск, ул. Ленина, 11.

INFORMATION ABOUT AUTHORS

Rodivilina Victoria Aleksandrovna, Candidate of Legal Sciences, Associate Professor, Associate Professor of the Department of Criminalistics. East Siberian Institute of the Ministry of Internal Affairs of Russia., Lermontov St., 110, Irkutsk, 664074.

Kolominov Vyacheslav Valentinovich, Candidate of Legal Sciences, Associate Professor, Associate Professor of the Department of Criminalistics, Forensic Expertise, and Legal Psychology. Baikal State University. Irkutsk, 11 Lenin St., 644025.

Статья поступила в редакцию 24.10.2025; одобрена после рецензирования 21.11.2025; принята к публикации 22.01.2026.
The article was submitted 24.10.2025; approved after reviewing 21.11.2025; accepted for publication 22.01.2026.