5.1. ПРАВО
5.1. LAW

Научная статья
УДК 343.13
DOI: 10.25683/VOLBI.2025.71.1256

Maksim Sergeevich Pertsev
Postgraduate of the Department of Criminal Law,
field of training 40.06.01 — Jurisprudence,
Volzhsky branch of the Volgograd State University
Volzhsky, Russian Federation
pepper.ms@hotmail.com

Максим Сергеевич Перцев
аспирант кафедры уголовного права,
направление подготовки 40.06.01 — Юриспруденция,
Волжский филиал Волгоградского государственного университета
Волжский, Российская Федерация
pepper.ms@hotmail.com

БЕЗОПАСНОСТЬ ДАННЫХ И ЦИФРОВЫЕ СЛЕДЫ: ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ В УГОЛОВНОМ ПРОЦЕССЕ

5.1.4 — Уголовно-правовые науки

Аннотация. *В статье рассматривается актуальная проблема обеспечения безопасности и целостности цифровых следов, используемых в качестве электронных доказательств в уголовном процессе в условиях цифровой трансформации общества. Электронные доказательства играют ключевую роль в уголовном процессе, в связи с чем их защита от несанкционированного вмешательства имеет ключевое значение для обеспечения справедливости с момента их формирования до представления в суде. Уязвимость электронных данных может быть вызвана различными факторами, включая хищение данных, несанкционированный доступ, вирусы или хакерские атаки. Для обеспечения безопасности таких данных необходимы специальные знания и технологии. Эксперты в области цифровой безопасности должны постоянно совершенствовать свои навыки для предотвращения возможных атак. Важность сохранения целостности заключается в обеспечении их достоверности и неподдельности, т. к. любое изменение информации может привести к ошибочным выводам и серьезно повлиять на результат уголовного дела.*

Современные технологии, криптография и блокчейн, играют важную роль в защите электронных доказательств. Криптографические методы помогают обеспечить конфиденциальность и целостность данных, а блокчейн-технология обеспечивает децентрализованное хранение данных, что делает их более устойчивыми к вмешательству. Эффективная защита цифровых следов, их целостность и конфиденциальность важны для обеспечения справедливости и надежности уголовного процесса в эпоху цифровизации общества.

В статье рассмотрены сложности и особенности обеспечения целостности электронных доказательств, а также предлагаются стратегические направления, нацеленные на защиту электронных доказательств от искажения и фальсификации. Сформулированные выводы и предложения могут иметь значение для дальнейшего развития науки, а также правоохранительного и законодательного регулирования.

Ключевые слова: *электронные доказательства, цифровые следы, уголовный процесс, безопасность данных, цифровая трансформация, защита электронных доказательств, допустимость доказательств, электронные носители информации, правовой статус, технологии, конфиденциальность, целостность*

Для цитирования: Перцев М. С. Безопасность данных и цифровые следы: обеспечение целостности электронных доказательств в уголовном процессе // Бизнес. Образование. Право. 2025. № 2(71). С. 211—215. DOI: 10.25683/VOLBI.2025.71.1256.

Original article

DATA SECURITY AND DIGITAL FOOTPRINTS: ENSURING THE INTEGRITY OF ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS

5.1.4 — Criminal law sciences

Abstract. *The article discusses the current problem of ensuring the security and integrity of digital footprints used as electronic evidence in criminal proceedings in the context of digital transformation of society. Electronic evidence plays a key role in criminal proceedings, and therefore, protecting it from unauthorized interference is essential to ensuring justice from the moment it is generated to its presentation in court. The vulnerability of electronic data can be caused by various factors, including data theft, unauthorized access, viruses or hacker attacks. Ensuring the security of such data requires special knowledge and technology. Digital security experts must constantly improve their skills to prevent possible attacks. The importance of maintaining integrity lies in ensuring its reliability and authenticity, since any change in*

information can lead to erroneous conclusions and seriously affect the outcome of a criminal case.

Modern technologies, cryptography and blockchain, play an important role in protecting electronic evidence. Cryptographic methods help ensure the confidentiality and integrity of data, and blockchain technology provides decentralized storage of data, which makes it more resistant to interference. Effective protection of digital footprints, their integrity and confidentiality is important for ensuring the fairness and reliability of criminal proceedings in the era of digitalization of society.

The article examines the complexities and features of ensuring the integrity of electronic evidence, and proposes strategic directions aimed at protecting electronic evidence from distortion and falsification. The author believes that the formulated conclusions and proposals may be important for the further development of science, as well as law enforcement and legislative regulation.

Keywords: *electronic evidence, digital footprints, criminal proceedings, data security, digital transformation, protection of electronic evidence, admissibility of evidence, electronic storage media, legal status, technology, confidentiality, integrity*

For citation: Pertsev M. S. Data security and digital footprints: ensuring the integrity of electronic evidence in criminal proceedings. *Biznes. Obrazovanie. Pravo = Business. Education. Law*. 2025;2(71):211—215. DOI: 10.25683/VOLBI.2025.71.1256.

Введение

Актуальность. Сегодня социум активно движется в эпоху цифровой трансформации, где многообразие информационных технологий охватывают все области человеческой деятельности. С одной стороны, цифровизация способствует появлению новых возможностей для развития науки, образования, управления, а с другой стороны — формирует новые вызовы, которые связаны с защитой данных. В условиях, когда наибольший массив информации хранится и передается в электронном виде, вопросы обеспечения безопасности информации становятся крайне важными. Особую значимость данные вопросы приобретают в области уголовного процесса, где электронные данные активно применяются в качестве доказательств.

Цифровые следы, которые оставляют пользователи в процессе взаимодействия с информационными системами, имеют особую значимость в качестве ресурса информации для расследования преступлений. Однако их применение в судебной практике сталкивается с многообразием трудностей.

В цифровую эпоху информация в электронном формате подвержена риску неправомерного доступа, искажения или уничтожения, что неминуемо ставит под сомнение ее подлинность и надежность. Кроме того, сама процедура получения, сохранения и анализа цифровой информации требует не только специфических компетенций, но и специализированного инструментария, доступ к которому у правоохранительных органов зачастую ограничен.

В связи с этим ключевым приоритетом уголовного судопроизводства в современных реалиях становится обеспечение неприкосновенности электронных доказательств. Понятие целостности данных подразумевает их неизменное состояние с момента создания и до момента представления в судебном заседании. Для достижения этой цели необходима интеграция надежных защитных механизмов, таких как криптографические протоколы, технологии распределенного реестра (блокчейн) и системы контроля версий.

Изученность проблемы. Вопросы обеспечения информационной безопасности и сохранности цифровых следов в рамках уголовного судопроизводства активно исследуются в современной юридической науке. Они освещалась в диссертациях М. О. Медведевой [1], М. С. Сергеева [2] и А. А. Балашовой [3]. Работы В. В. Крылова [4], А. С. Агафонова [5], а также коллектива авторов под руководством С. В. Зуева [6] посвящены анализу электронных доказательств, как источникам доказательственной информации в процессе уголовного судопроизводства. Вопросы, касающиеся анализа методов защиты электронных доказательств от несанкционированного проникновения, освещаются в работах А. В. и Е. И. Шигуровых [7], А. И. Жмурова [8], М. Ш. Махтаева [9]. Изучение возможностей криптографической защиты информации и применения блокчейн-технологий для обеспечения сохранности цифровых улик освещаются в трудах Н. Г. Муратовой, М. С. Сергеева, К. Г. Попова, Р. Р. Шамсутдинова, Р. Р. Абсатарова, Д. А. Сенькина, Н. И. Назарова, М. В. Кузнецова, Н. В. Машинской, А. Б. Коновалова, А. В. Глухих, К. М. Бортникова, А. В. Шигурова, Н. А. Подольного и др.

Целесообразность разработки темы обосновывается необходимостью выявлению основных уязвимостей электронных доказательств, проявляющихся в области уголовного судопроизводства. Исследования в области безопасности данных и цифровых следов способствуют разработке и внедрению новых технологий и методов киберзащиты, направленных на предотвращение несанкционированного доступа, изменения или утраты электронных данных.

Научная новизна исследования заключается в разработке стратегических направлений для комплексного решения проблем защиты электронных доказательств от искажения и фальсификации, что позволит повысить эффективность использования цифровых следов в уголовном судопроизводстве и гарантировать соблюдение прав участников процесса.

Цель работы заключается в выявлении основных угроз безопасности данных в рамках цифровых следов и их применении в уголовном процессе, а также в разработке стратегических направлений, нацеленных на защиту электронных доказательств от искажения и фальсификации.

Задачи исследования:

1) проанализировать существующие угрозы безопасности данных в контексте цифровых следов и их использования в уголовном процессе;

2) рассмотреть и оценить различные методы обеспечения целостности электронных доказательств;

3) изучить действующие правовые нормы, регламентирующие использование цифровых следов в качестве доказательств;

4) предложить стратегические направления для комплексного решения проблем защиты электронных доказательств от искажения и фальсификации.

Теоретическая значимость исследования состоит в расширении и углублении научных знаний в области защиты цифровых следов и электронных доказательств.

Практическая значимость работы заключается в возможности использования предложенных стратегических направлений для модернизации нормативной базы, регулирующей защиту электронных доказательств, а также в практической деятельности правоохранительных органов и судебной системы.

Методология исследования. В работе использованы методы системного анализа, анализа научной литературы, анализа законодательства, анализа применимости современных технологий в уголовном процессе, а также методы синтеза и обобщения полученных данных.

Основная часть

В настоящее время обеспечение безопасности данных, связанных с цифровыми следами и их применением в уголовном судопроизводстве, представляет собой серьезную проблему, требующую незамедлительного решения. Цифровые следы — это информация, генерируемая пользователями при использовании цифровых устройств и сетей. Эти данные могут быть использованы как для обеспечения безопасности и защиты прав граждан, так и для совершения преступлений, а также в качестве доказательств в уголовном процессе.

Основные угрозы безопасности данных в контексте цифровых следов включают в себя:

1) утечки данных и кибератаки;

2) несанкционированное собирание и использование данных;

3) подделка цифровых следов;

4) угрозы приватности;

5) использование данных в преступных целях.

Цифровые следы играют значимую роль в процессе расследования преступлений, однако их применение сталкивается с перечнем трудностей. Рассмотрим их подробнее.

1. Доказательная ценность: цифровые следы относятся к перечню допустимых доказательств в суде, однако их достоверность в обязательном порядке должна быть подтверждена.

2. Собирание и анализ данных: в процессе собирания цифровых следов необходимо соблюдать правовые нормы, поскольку неправомерное собирание данных может привести к их недопустимости в уголовном судопроизводстве.

3. Конфиденциальность и защита прав: применение цифровых следов должно соответствовать принципам защиты персональных данных. Следовательно, необходимо соблюдать баланс между интересами следствия и правами на конфиденциальность [10].

4. Технические сложности: анализ цифровых следов — это сложный процесс, который требует специфических знаний и специальных инструментов. Некорректная интерпретация данных может способствовать появлению ошибок в расследовании.

5. Этические вопросы: применение цифровых следов может вызывать этические вопросы, особенно если собирание данных осуществляется без разрешения пользователей.

Баланс между эффективностью расследования и защитой прав граждан — это ключевой аспект, который должен стать приоритетным для всех участников процесса: от следователей и юристов до технических специалистов, работающих над анализом данных. Профессионализм и ответственность на каждом этапе обработки цифровых следов являются гарантией того, что полученные данные не только допустимы в суде, но и справедливы по отношению к гражданам.

Обеспечение целостности электронных доказательств представляется гарантией неизменности, целостности и достоверности данных на всех этапах — собирания, хранения и передачи. Для обеспечения целостности применяются различные методы и технологии:

1. *Методы обеспечения целостности на этапе собирания данных*: применение криптографических хэш-функций [11], цифровая подпись, использование защищенных устройств и программного обеспечения, ведение журналов аудита (логов).

2. *Методы обеспечения целостности на этапе хранения*: шифрование данных, регулярное создание резервных копий, контроль доступа, проверка целостности с использованием хэш-сумм, использование блокчейн-технологий.

3. *Методы обеспечения целостности на этапе передачи*: использование защищенных протоколов передачи данных, цифровая подпись и шифрование при передаче, контроль целостности с использованием хэш-сумм, использование систем контроля ошибок.

Применение криптографических хэш-функций, цифровых подписей и защищенных программных и аппаратных средств на этапе собирания данных позволяет гарантировать их первоначальную неизменность и достоверность [12]. Важно четко фиксировать действия с помощью ведения журналов аудита, что добавляет дополнительный уровень защиты и позволяет отслеживать любые попытки манипуляции.

На этапе хранения данных жизненно необходимо применять технологию шифрования и регулярно создавать резервные копии. Контроль доступа позволяет ограничивать круг лиц, обладающих правом изменения или удаления данных, что минимизирует риски необоснованных изменений. Проверка целостности путем сравнения хэш-сумм и внедрение блокчейн-технологий обеспечивают высокую степень доверия к неизменности данных за все время их нахождения в сети.

Этап передачи данных в равной степени важен для поддержания целостности. Использование современных защищенных протоколов, таких как *TLS* и *IPsec*, в сочетании с цифровыми подписями и шифрованием, обеспечивает безопасность данных на пути их следования. Контроль целостности и применение систем контроля ошибок позволяют быстро обнаружить и исправить любые нарушения, произошедшие при передаче [13].

Применение цифровых следов в качестве доказательств в уголовном процессе имеет ряд правовых аспектов. Рассмотрим их подробнее:

1. *Законодательная база*: во многих странах применение цифровых следов регламентируется уголовно-процессуальным законодательством, законами о защите персональных данных, а также прочих нормативных правовых актов (далее — НПА), связанных с электронной подписью и электронным документооборотом. В России применение цифровых следов регулируется Уголовно-процессуальным кодексом РФ, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и прочими НПА.

2. *Допустимость доказательств*: цифровые следы могут быть получены только законным способом. Данные, которые были получены с нарушением процедуры, являются недопустимыми в качестве доказательств в уголовном судопроизводстве. В отдельных странах есть требования, согласно которым цифровые данные должны быть заверены электронной подписью или другим способом, подтверждающим их достоверность и подлинность.

3. *Достоверность и подлинность*: цифровые следы в обязательном порядке проверяются на предмет подлинности. Данный процесс включает в себя проверку целостности данных, отсутствия изменений и подтверждение источника информации. В отдельных случаях в суде необходимо заключение эксперта по цифровой криминалистике.

4. *Защита персональных данных*: в процессе применения цифровых следов необходимо соблюдать законодательство

о защите персональных данных. В Европе это регулируется Общим регламентом по защите данных, а в России — Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

5. *Международное сотрудничество*: в случаях, когда цифровые следы получены из-за границы, может потребоваться взаимодействие с правоохранительными органами других стран в рамках международных договоров (например, через Интерпол или соглашения о взаимной правовой помощи).

Современные технологии предоставляют уникальные возможности для получения и анализа доказательств, однако их использование должно быть строго регламентировано, чтобы обеспечить справедливость судебных разбирательств и защиту прав всех участников процесса [14]. Важным аспектом является необходимость соблюдения законности при собирании цифровых следов. Это подразумевает не только соблюдение процессуальных норм, но и обеспечение аутентичности и достоверности полученных данных, что критически важно для их признания в судебных инстанциях. Юридические и технические механизмы верификации здесь играют ключевую роль и требуют постоянного совершенствования и адаптации к новым вызовам.

В условиях увеличивающейся глобализации важно поддерживать международное сотрудничество для эффективного использования цифровых следов, полученных за рубежом. Такая кооперация требует гармонизации правовых норм и установления четких процедур взаимодействия, что позволит повысить эффективность расследований и укрепить международное правовое сообщество.

Результаты анализа обеспечения целостности электронных доказательств в уголовном процессе указывают на необходимость реализации инновационных подходов к их защите от искажения и фальсификации. Предлагаются следующие стратегические направления:

1. Формирование экосистемы цифровой доказательственной базы. Разработка единых национальных и международных стандартов собирания, хранения и обработки электронных доказательств, с акцентом на создание унифицированной терминологии и определение допустимых форматов данных. Это позволит создать единую, понятную и надежную цифровую среду для работы с доказательствами.

2. Внедрение принципов «доверенной цифровой среды». Регламентация обязательных процедур, обеспечивающих «прозрачность» и «контролируемость» процессов собирания, хранения и передачи электронных доказательств. Использование криптографических методов и цифровых подписей должно стать «золотым стандартом», а протоколирование всех действий (аудит) — неотъемлемой частью процесса.

3. Усиление «цифровой дипломатии». Активное участие в разработке международных стандартов для обеспечения совместимости и признания электронных доказательств в разных юрисдикциях. Упрощение процедур взаимной правовой помощи в случаях, связанных с электронными доказательствами [15], является ключевым элементом эффективного международного сотрудничества.

4. Установление «цифровой ответственности». Введение строгих санкций за несанкционированный доступ, изменение или уничтожение электронных доказательств, а также за нарушение установленных правил работы с ними. Это создаст необходимый превентивный эффект и укрепит дисциплину.

Установленные стандарты будут способствовать повышению уровня доверия к электронным доказательствам, в то время как регламентация процедур окажет положительное влияние на их устойчивость и надежность. Международное сотрудничество в рассматриваемой области даст возможность результативно применять электронные доказательства в трансграничных делах, в то время как строгая ответственность за нарушения будет способствовать образованию дополнительных гарантий их сохранности и достоверности.

Выводы

Сегодня в правовой области инновационные технологии являются обязательным условием усиления правовой системы государства. Однако недостаточно только интегрировать данные технологии — представляется необходимой перманентная адаптация данных инструментов к трансформирующимся условиям и появляющимся угрозам. Развитие профессиональных навыков, обмен передовым опытом и активная модернизация законодательной базы выступают основными факторами в данном вопросе.

Сегодня международное сотрудничество имеет особую значимость в связи с тем, что объединение усилий разных стран в рассматриваемой области оказывает положительное влияние на консолидацию мирового правого сообщества, а также способствует росту результативности расследований. Всё это формирует возможности применения цифровых доказательств, которые были получены в других юрисдикциях при условии соблюдения установленных стандартов и наличия устойчивых инструментов взаимодействия.

Перспективы судебного разбирательства находятся в тесной взаимосвязи с прогрессом в сфере собирания, анализа и применения цифровых следов. Однако для обеспечения законности судебного процесса представляется необходимым интеграция конкретных правовых рамок, которые регламентируют использование электронных доказательств.

Предложенные стратегические направления, включающие формирование экосистемы цифровой доказательственной базы, внедрение принципов «доверенной цифровой среды», усиление «цифровой дипломатии» и установление «цифровой ответственности», призваны комплексно решить проблему защиты электронных доказательств от искажения и фальсификации.

Внедрение единых национальных и международных стандартов для собирания, хранения и обработки электронных доказательств, наряду с регламентацией обязательных процедур, обеспечивающих «прозрачность» и «контролируемость» процессов, создаст надежную основу для работы с цифровыми доказательствами. Активное участие в разработке международных стандартов и упрощение процедур взаимной правовой помощи позволит эффективно применять электронные доказательства в трансграничных делах.

Введение строгих санкций за несанкционированный доступ, изменение или уничтожение электронных доказательств создаст необходимый превентивный эффект и укрепит дисциплину. Реализация предложенных мер будет способствовать повышению уровня доверия к электронным доказательствам, их устойчивости и надежности, а также обеспечит дополнительные гарантии их сохранности и достоверности, что, в конечном счете, повысит эффективность уголовного судопроизводства в цифровую эпоху.

СПИСОК ИСТОЧНИКОВ

1. Медведева М. О. Уголовно-процессуальная форма информационных технологий: современное состояние и основные направления развития : дис. ... канд. юрид. наук. М., 2018. 250 с.

2. Сергеев М. С. Правовое регулирование применения электронной информации и электронных носителей информации в уголовном судопроизводстве : дис. ... канд. юрид. наук. Екатеринбург 2018. 322 с.
3. Балашова А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании : дис. ... канд. юрид. наук. М., 2020. 216 с.
4. Крылов В. В. Современная криминалистика. Правовая информатика и кибернетика. М. : ЛексЭст, 2007. 270 с.
5. Агафонов А. С., Количенко А. А. Электронный носитель информации как источник получения электронных доказательств по уголовным делам, связанным с нарушением правил дорожного движения // Безопасность дорожного движения. 2023. № 2. С. 45—49.
6. Основы теории электронных доказательств / под ред. С. В. Зуева. М. : Юрлитинформ, 2019. 400 с.
7. Шигуров А. В., Шигурова Е. И. Проблемы правовой регламентации использования электронных следов и электронных носителей информации при производстве по уголовному делу // Гуманитарные и политико-правовые исследования. 2020. № 1(8). С. 53—63.
8. Жмурова А. И., Вытовтов А. Е. К вопросу об использовании электронных (цифровых) доказательств в уголовном судопроизводстве // Научный дайджест Восточно-Сибирского института МВД России. 2022. № 2(16). С. 44—50.
9. Махтаев М. Ш. Основы расследования преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных технологий. М. : Юрлитинформ, 2023. 152 с.
10. Зуев С. В., Каменев А. С. Собирание и проверка электронной доказательственной информации стороной защиты в уголовном судопроизводстве : моногр. М. : Юрлитинформ, 2024. 158 с.
11. Митрофанова М. А. Электронные доказательства и принцип непосредственности в арбитражном процессе : дис. ... канд. юрид. наук. Саратов, 2013. 213 с.
12. Коновалова А. Б., Глухих А. В. Изъятие электронных носителей информации и копирование с них информации: к вопросу о новеллах правового регулирования // Общество. Наука. Инновации (НПК-2019) : сб. ст. XIX Всерос. науч.-практ. конф. : в 4 т. Киров : Вят. гос. ун-т, 2019. Т. 3. С. 417—423.
13. Zhang Y., Dong H. Criminal law regulation of cyber fraud crimes—from the perspective of citizens' personal information protection in the era of edge computing // Journal of Cloud Computing. 2023. Vol. 12. Art. 64. DOI: 10.1186/s13677-023-00437-3.
14. Шапошников К. М. К вопросу о понятии и сущности электронных носителей информации в уголовном судопроизводстве // Проблемы применения уголовного закона и уголовно-процессуального законодательства в деятельности следственно-судебных органов : сб. науч. ст. по итогам науч.-практ. конф. магистрантов. Симферополь : Ариал, 2023. С. 128—131.
15. Количенко А. А. Проблемы проверки и оценки электронных доказательств в современном уголовном процессе : дис. ... канд. юрид. наук. Н. Новгород, 2023. 224 с.

REFERENCES

1. Medvedeva M. O. Criminal-procedural form of information technologies: current state and main directions of development. Diss. of the Cand. of Law. Moscow, 2018. 250 p. (In Russ.)
2. Sergeev M. S. Legal regulation of the use of electronic data and electronic storage media in criminal proceedings. Diss. of the Cand. of Law. Ekaterinburg, 2018. 322 p. (In Russ.)
3. Balashova A. A. Electronic storage media and their use in criminal-procedural evidence. Diss. of the Cand. of Law. Moscow, 2020. 216 p. (In Russ.)
4. Krylov V. V. Modern forensic science. Legal informatics and cybernetics. Moscow, LexEst, 2007. 270 p. (In Russ.)
5. Agafonov A. S., Kolichenko A. A. Electronic information carrier as a source of obtaining electronic evidence in criminal cases related to violation of traffic rules. *Bezopasnost` dorozhnogo dvizheniya = Road safety*. 2023;2:45—49. (In Russ.)
6. Fundamentals of the theory of electronic evidence. S. V. Zuev (ed.). Moscow, Yurlitinform, 2019. 400 p. (In Russ.)
7. Shigurov A. V., Shigurova E. I. Problems of legal regulation of the use of electronic tracks and electronic media in the criminal proceedings. *Gumanitarnye i politiko-pravovye issledovaniya*. 2020;1(8):53—63. (In Russ.)
8. Zhmurova A. I., Vitovtov A. E. On the issue of the use of electronic (digital) evidence in criminal proceedings. *Nauchnyi daidzhest Vostochno-Sibirskogo instituta MVD Rossii = Scientific digest of the East Siberian Institute of the Ministry of Internal Affairs of Russia*. 2022;2(16):44—50. (In Russ.)
9. Makhtaev M. Sh. Fundamentals of investigating extremist crimes committed using information and telecommunication technologies. Moscow, Yurlitinform, 2023. 152 p. (In Russ.)
10. Zuev S. V., Kamenev A. S. Collection and verification of electronic evidentiary information by the defense in criminal proceedings. Monograph. Moscow, Yurlitinform, 2024. 158 p. (In Russ.)
11. Mitrofanov M. A. Electronic evidence and the principle of immediacy in arbitration proceedings. Diss. of the Cand. of Law. Saratov, 2013. 213 p. (In Russ.)
12. Konovalova A. B., Glukhikh A. V. Seizure of electronic storage media and copying of information from them: on the issue of innovations in legal regulation. *Obshchestvo. Nauka. Innovatsii (NPK-2019) = Society. Science. Innovations (NPK-2019). Collection of articles from the XIX All-Russian scientific and practical conference*. Kirov, Vyatka State University publ., 2019;3:417—423. (In Russ.)
13. Zhang Y., Dong H. Criminal law regulation of cyber fraud crimes—from the perspective of citizens' personal information protection in the era of edge computing. *Journal of Cloud Computing*. 2023;12:64. DOI: 10.1186/s13677-023-00437-3.
14. Shaposhnikov K. M. On the issue of the concept and essence of electronic storage media in criminal proceedings. *Problemy primeneniya ugolovnogo zakona i ugolovno-protsessual`nogo zakonodatel`stva v deyatel`nosti sledstvenno-sudebnykh organov = Problems of application of criminal law and criminal procedure legislation in the activities of investigative and judicial bodies. Collection of scientific articles following the results of the scientific and practical conference of master's students*. Simferopol, Arial, 2023:128—131. (In Russ.)
15. Kolichenko A. A. Problems of verification and evaluation of electronic evidence in modern criminal proceedings. Diss. of the Cand. of Law. Nizhny Novgorod, 2023. 224 p. (In Russ.)

Статья поступила в редакцию 15.02.2025; одобрена после рецензирования 15.03.2025; принята к публикации 17.03.2025.
The article was submitted 15.02.2025; approved after reviewing 15.03.2025; accepted for publication 17.03.2025.