Дата поступления рукописи в редакцию: 25.10.2025 г. DOI: 10.24412/2782-3830-2025-10-149-155
Дата принятия рукописи в печать: 05.11.2025 г.

СИРАКАНЯН Аркадий Рашимович,
К.ю.н., заместитель директора института государства и права, старший преподаватель кафедры публичного и уголовного права Сургутского государственного университета,
e-mail: sirakanyan_ar@surgu.ru

КИБЕРКРИМИНАЛИСТИКА В СИСТЕМЕ СОВРЕМЕННОГО УГОЛОВНОГО СУДОПРОИЗВОДСТВА

Аннотация. *Данная статья посвящена комплексному исследованию места и роли киберкриминалистики в системе современного уголовного судопроизводства Российской Федерации. В условиях стремительной цифровизации общественных отношений и широкого распространения технологий искусственного интеллекта традиционные формы фиксации и анализа доказательственной информации подвергаются существенной трансформации. Автор рассматривает киберкриминалистику как междисциплинарную область знаний, находящуюся на стыке криминалистики, судебной информатики, кибербезопасности и уголовного процесса, обеспечивающую получение, верификацию, анализ и представление цифровых следов преступной деятельности.*

На основе анализа новейших отечественных и зарубежных исследований систематизируются подходы к определению понятия и предмета киберкриминалистики, раскрываются особенности жизненного цикла цифровых доказательств — от их обнаружения и фиксации до экспертного исследования и процессуального использования в суде. Отдельное внимание уделено проблемам допустимости, относимости и достоверности цифровых доказательств, а также вопросам обеспечения их подлинности и непрерывности «цепочки хранения».

Раскрываются организационно-методические трудности, сдерживающие интеграцию цифровых технологий в уголовное судопроизводство, включая отсутствие единой терминологической базы, недостаток процессуальной регламентации и нехватку подготовленных специалистов. Предложены направления дальнейшего развития киберкриминалистики: создание правовых основ функционирования электронного уголовного дела, стандартизация методик цифровой экспертизы, внедрение автоматизированных систем аналитической обработки доказательств и развитие научной школы цифрового доказывания.

Практическая значимость исследования заключается в обосновании модели взаимодействия следственных органов, экспертных учреждений и суда при обращении с цифровыми доказательствами в условиях киберугроз, что способствует формированию единого цифрового пространства осуществления правосудия.

Ключевые слова: *киберкриминалистика; криминалистика; цифровые доказательства; электронные доказательства; судебная компьютерно-техническая экспертиза; уголовный процесс; цифровые следы; цепочка хранения.*

SIRAKANYAN Arkadiy Rashimovich,
PhD in Law, Deputy Director of the Institute of State and Law, Senior Lecturer at the Department of Public and Criminal Law Surgut State University

CYBERCRIMINALISM IN THE MODERN CRIMINAL JUSTICE SYSTEM

Annotation. *This article is devoted to a comprehensive study of the place and role of cybercriminalism in the system of modern criminal justice in the Russian Federation. In the context of the rapid digitalization of public relations and the widespread use of artificial intelligence technologies, traditional forms of recording and analyzing evidentiary information are undergoing significant transformation. The author considers cybercriminalism as an interdisciplinary field of knowledge located at the intersection of criminology, forensic informatics, cybersecurity and criminal procedure, providing the acquisition, verification, analysis and presentation of digital traces of criminal activity.*

Based on the analysis of the latest domestic and foreign research, approaches to defining the concept and subject of cybercriminalism are systematized, and the features of the life cycle of digital evidence are revealed — from their detection and fixation to expert research and procedural use in court. Special attention is paid to the issues of the admissibility, relevance and reliability of digital evidence, as well as issues of ensuring their authenticity and continuity of the "storage chain".

The organizational and methodological difficulties hindering the integration of digital technologies into criminal proceedings are revealed, including the lack of a unified terminology base, lack of procedural regulation and lack of trained specialists. The directions of further development of cybercriminalism are proposed: the creation of legal foundations for the functioning of electronic criminal proceedings, the standardization of digital examination techniques, the introduction of automated systems for analytical processing of evidence and the development of a scientific school of digital evidence.

The practical significance of the study lies in substantiating the model of interaction between investigative authorities, expert institutions and the court when handling digital evidence in the face of cyber threats, which contributes to the formation of a unified digital space for the administration of justice.

Key words*: cybercriminalism; criminalistics; digital evidence; electronic evidence; forensic computer-technical expertise; criminal procedure; digital traces; storage chain.*

Введение

Цифровая трансформация уголовного процесса радикально изменила источники доказательств, тактику следственных действий и роль экспертного знания. На первый план выходит обработка цифровых следов — данных, генерируемых в результатах сетевой активности человека и устройств, которые требуют специализированных методов обнаружения, фиксации, извлечения и интерпретации. В отечественной науке парадигма электронных/цифровых доказательств разработана в ряде трудов, подчёркивающих самостоятельность предмета исследования и необходимость методической унификации: от дефиниций до процессуальных гарантий.

Традиционные методы борьбы с цифровыми преступлениями зачастую оказываются недостаточно эффективными из-за высокой динамики развития атакующих технологий [1, с. 506].

При этом сохраняются концептуальные противоречия: закон не использует термин «электронное доказательство» как отдельный вид, тогда как в практике следствия и суда цифровые данные становятся ключевыми (переписка, сетевые логи, метаданные, дампы устройств, блокчейн-записи и т. п.).

Киберкриминалистика: предмет, метод и место в системе криминалистики

Под киберкриминалистикой понимают часть криминалистической науки, изучающую закономерности формирования, обнаружения, фиксации, изъятия, исследования и оценки цифровых следов в целях раскрытия и расследования преступлений, а также представления полученных данных в суде. Исследования последних лет предлагают уточнённые модели цифровых следов и структур криминалистической характеристики преступлений в сфере компьютерной информации.

Существует несколько подходов к пониманию статуса киберкриминалистики:

1. Интеграционный подход — рассматривает её как часть криминалистической техники, обслуживающую расследование преступлений с использованием ИКТ. Этой позиции придерживаются Г. В. Бондарева [2, с. 153].
2. Системный подход — определяет киберкриминалистику как междисциплинарную подсистему, объединяющую элементы криминалистической техники, тактики и методики, адаптированные к цифровой среде. Такой взгляд развивают Т. А. Ильяшевич и Э. Г. Хомяков [3, с. 175; 4, с. 74].
3. Автономный подход — трактует её как самостоятельную отрасль знания, находящуюся на стыке криминалистики, информатики, кибербезопасности и процессуального права. Эту точку зрения поддерживает Ф. А. Абашева, указывая, что цифровое пространство создаёт «новую криминалистическую реальность», где традиционные понятия следа и вещественного доказательства приобретают иной смысл [5, с. 31].

На практике эти подходы взаимодополняемы: киберкриминалистика фактически выступает инфраструктурной платформой для всех разделов криминалистики, обеспечивая их технологическое измерение.

Методический аппарат киберкриминалистики формируется на стыке правовых, инженерно-технических и поведенческих дисциплин. Классическая триада методов включает:

1. Технические методы — направлены на извлечение и фиксацию данных без изменения их структуры (бит-копирование, write-blockers, контроль хэш-сумм).

2. Аналитические методы — восстановление удалённых данных, временных шкал событий, идентификация пользователей, корреляция сетевых логов.
3. Интерпретационные методы — криминалистическая оценка значимости цифровых следов, определение механизма их формирования и связи с субъектом преступления.

Эти методы опираются на принцип обеспечения целостности и воспроизводимости результата. Как отмечает Т. А. Ильяшевич, «основным требованием к цифровому доказательству является возможность независимой повторной проверки действий эксперта с получением идентичного результата» [3, с. 174].

Киберкриминалистика активно использует специализированные программно-аппаратные комплексы:

1. EnCase Forensic, FTK, X-Ways, Belkasoft Evidence Center, Autopsy — для анализа файловых систем, сетевого трафика и мобильных устройств;
2. Wireshark, Volatility, Magnet AXIOM — для анализа оперативной памяти, сетевых пакетов и временных меток;
3. отечественные решения — X-Forensics, FROST, СканЭКС-Цифра, рекомендованные Минюстом РФ.

Развитие методов связано с необходимостью адаптации к новым средам: облачным сервисам, блокчейн-платформам, зашифрованным мессенджерам. Это требует участия специалистов не только в области юриспруденции, но и кибербезопасности, криптографии и сетевых технологий.

Жизненный цикл цифровых доказательств и «цепочка хранения»

Цифровые доказательства характеризуются летучестью, воспроизводимостью и зависимостью от среды — операционных систем, сетевых протоколов, облачных платформ. Любое несанкционированное воздействие может изменить данные, поэтому первостепенной задачей становится фиксация всех действий с объектом и подтверждение его неизменности.

Термин chain of custody — «цепочка хранения» — введён в международную практику криминалистики и означает документально подтверждённую последовательность всех операций с цифровым носителем — от момента обнаружения до представления в суде. В российской научной традиции ему соответствуют термины «процессуальное сопровождение вещественных доказательств» и «контроль целостности электронного носителя».

Современные методики (ISO/IEC 27037:2012, ISO/IEC 27041:2015, ENFSI Best Practice Manuals) выделяют четыре основных этапа жизненного цикла цифровых доказательств [6, с. 117]:

1. Обнаружение (identification).

На этом этапе следователь или оперативный сотрудник определяет потенциальные источники цифровых следов — компьютеры, смартфоны, серверы, облачные учётные записи, мессенджеры, смарт-устройства.

Особенность в том, что носитель может быть удалённым (облачный сервер, VPN-канал, IoT-датчик), а физический доступ отсутствует. В таких случаях используются процессуальные инструменты — запросы операторам связи, международная правовая помощь (Mutual Legal Assistance Treaty), а также экспресс-фиксация скриншотов и сетевых логов.

2. Извлечение (acquisition).

Это критическая фаза, в которой формируется точная бит-копия устройства (бит-имидж) с использованием write-blockers и контролем целостности через хэш-функции (MD5, SHA-1, SHA-256).

Как отмечает А. О. Бессонова, допустимость доказательства в значительной мере зависит от того, была ли сохранена идентичность оригинала и копии, что обеспечивается только при форензически корректном извлечении [7, с. 893].

Извлечённые данные немедленно опечатываются и сопровождаются актом (протоколом копирования) с указанием времени, места, операторов и использованных устройств.

3. Сохранение (preservation).

Цель — исключить любые изменения в данных. В российской практике рекомендуется двухуровневое хранение: оригинал в опечатанном виде в доказательственном фонде следственного органа и рабочая копия в экспертном учреждении.

Применяются криптографические средства защиты (ГОСТ Р 34.11-2012), системы контроля доступа и автоматическое логирование всех операций с носителем.

4. Представление в суде (presentation).

На этом этапе следователь и эксперт обосновывают достоверность цифровых доказательств через предъявление протоколов изъятия, экспертных заключений и хэш-отчётов. Суд оценивает доказательство с точки зрения допустимости (ст. 75 УПК РФ) и относимости (ст. 74 УПК РФ).

В ряде дел суды отклоняют цифровые доказательства именно из-за нарушения цепочки хранения.

Несмотря на развитие нормативной базы, в российской практике до сих пор не утверждён единый национальный стандарт по работе с цифровыми доказательствами. Различные ведомства (МВД, СКР, Минюст, ФСТЭК) используют несогласованные методики.

Кроме того, недостаток оборудования (форензические станции, защищённые контейнеры) приводит к тому, что следователи вынуждены использовать обычные ПК, что создаёт риск изменения метаданных и повреждения информации.

Жизненный цикл цифровых доказательств является фундаментом достоверности и допустимости электронных доказательств.

Соблюдение цепочки хранения обеспечивает три ключевых гарантии:

1. Неизменность данных, достигаемая техническими и криптографическими средствами.
2. Проверяемость действий, реализуемая через детальное документирование каждого этапа.
3. Воспроизводимость результатов, позволяющая эксперту или суду повторно убедиться в целостности доказательства.

Нарушение любой из этих гарантий ставит под сомнение всю систему доказывания в цифровую эпоху. Таким образом, формирование национального стандарта chain of custody и подготовка специалистов в области киберфорензики становятся стратегическими задачами уголовного судопроизводства России на ближайшее десятилетие.

Допустимость, относимость и достоверность электронных/цифровых доказательств

В уголовном процессе допустимость доказательств определяется через призму требований ст. 74, 75 и 89 УПК РФ, согласно которым доказательствами признаются любые фактические данные, на основе которых суд устанавливает обстоятельства дела, если они получены в соответствии с законом.

Однако УПК не содержит термина «электронное доказательство», что порождает проблему дефинитивного вакуума. На практике используется совокупность категорий — «электронный документ», «иные носители информации», «цифровые данные».

Как отмечает С. И. Грицаев, электронные доказательства нельзя отождествлять с вещественными доказательствами, так как они существуют не в материальной, а в информационной форме, что требует иного процессуального подхода к их фиксации и исследованию [8, с. 50].

Эта позиция поддерживается также И. А. Тайтаковым, который предлагает включить в ст. 74 УПК РФ самостоятельный пункт о «цифровых (электронных) доказательствах» с перечислением допустимых способов их получения [9, с. 98].

Таким образом, уже на уровне понятийного аппарата существует необходимость системного пересмотра законодательства с целью учёта особенностей цифровых данных — их нематериальности, воспроизводимости и зависимости от технической среды.

На теоретическом уровне дискуссия сосредоточена вокруг статуса «электронного документа» и «электронного носителя» как процессуальных форм источников доказательств, а также допустимости данных, извлечённых автоматизированными средствами. Обзор научных работ 2020–2025 гг. позволяет выделить три группы проблем:

1. дефинитивные — отсутствие единообразия терминов «цифровые», «электронные» доказательства;
2. процессуальные — требования к фиксации, заверению целостности и процедурам верификации;
3. оценочные — стандарты доказанности и распределение бремени доказывания при оспаривании достоверности цифровых данных.

Из этого представляется возможным сделать вывод о том, что цифровые данные нельзя редуцировать к «бумажному документу»: метод их получения, среды хранения, криптографические средства защиты становятся элементами критерия достоверности, что требует междисциплинарной экспертизы.

Судебная компьютерно-техническая экспертиза (далее – СКТЭ) и экспертные риски

Как отмечает профессор А.И. Усов, в настоящее время СКТЭ — «это динамично развивающееся судебно-экспертное направление, предмет которого находится в сфере компьютерной информации и напрямую зависит от постоянно обновляющейся номенклатуры и характеристик компьютерных средств и систем» [10, с. 214].

СКТЭ занимает центральное место в киберкриминалистике, являясь основным процессуальным инструментом легализации цифровых доказательств.

Именно эксперт превращает данные, полученные в ходе оперативно-розыскных или следственных действий, в процессуально значимую форму, обладающую свойствами достоверности и проверяемости.

Согласно ст. 195–207 УПК РФ, экспертиза назначается при необходимости специальных знаний. В отношении цифровых данных это означает необходимость знаний в области информационных технологий, компьютерных систем, сетевой безопасности, криптографии и анализа цифровых носителей.

На сегодняшний день, компьютерно-техническая экспертиза становится не просто техниче-

ским действием, а ядром доказательственного процесса при расследовании преступлений, связанных с информационными технологиями.

На практике без заключения эксперта невозможно подтвердить аутентичность цифрового следа, определить механизм его возникновения и установить источник данных, что делает эксперта ключевым субъектом цифрового доказывания.

Практика показывает, что нарушения методики проведения экспертизы часто приводят к исключению доказательства из материалов дела. Среди типичных ошибок:

1. Отсутствие write-blocker при копировании.

Любая запись на исследуемый носитель изменяет метаданные и делает невозможным подтверждение неизменности.

2. Отсутствие хэш-сумм или несоответствие контрольных значений.

Без этого невозможно доказать, что данные не подвергались модификации.

3. Использование несертифицированных программных средств.

Применение freeware-утилит, не обеспечивающих форензическую чистоту, ставит под сомнение достоверность результата.

4. Недокументированные действия.

Отсутствие детализированных протоколов, актов или журналов операций.

5. Выход эксперта за пределы компетенции.

Например, когда эксперт делает правовую оценку действий лица или квалифицирует деяние, что выходит за рамки его полномочий.

6. Нарушение chain of custody.

Отсутствие документального подтверждения передачи носителей между следствием и экспертом.

Эксперт не просто технический специалист, а гарант доказательственной чистоты цифровых данных. Он обеспечивает сохранность доказательства, документирует все действия и разъясняет суду технические аспекты. Эксперт становится медиатором между техническим фактом и правовой оценкой, а его заключение — инструментом перевода данных цифровой среды в язык права».

Таким образом, судебная компьютерно-техническая экспертиза является ключевым элементом цифрового доказывания. Её результаты определяют допустимость и доказательственную силу электронных следов, а качество проведения экспертизы напрямую влияет на исход уголовного дела.

Цифровые следы и криминалистическая характеристика преступлений в сфере компьютерной информации

Цифровой след — это информационное отражение действий человека или программного агента, оставленное в цифровой среде и обладающее свойствами индивидуализируемости, стабильности и воспроизводимости.

Как отмечает Э. Г. Хомяков, цифровой след не является физическим объектом, но обладает объективной природой, поскольку фиксируется на материальном носителе — накопителе данных, сервере, мобильном устройстве, облачном ресурсе [4, с. 79].

В отличие от традиционных следов (отпечатков, микрочастиц и т. д.), цифровой след имеет трёхуровневую структуру:

1. Физический уровень — данные, зафиксированные на материальном носителе (битовая структура, сектора памяти, файловые системы).
2. Логический уровень — информация, доступная пользователю или системе (файлы, базы данных, журналы событий).
3. Семантический уровень — смысловое содержание данных (переписка, транзакции, контент, действия пользователя).

Каждый из этих уровней требует отдельного подхода при фиксации, анализе и оценке.

В контексте киберпреступности содержание криминалистической характеристики преступлений обновилось: наряду с традиционными элементами (мотив, орудия, объект, личность) появилась цифровая среда преступления как новая системообразующая категория.

Современная структура характеристики включает:

1. Объект посягательства — компьютерная информация, персональные данные, цифровые активы, криптовалюты, информационные системы.
2. Способ совершения — фишинг, вредоносное ПО, DDoS-атаки, взлом, SQL-инъекции, атаки через социальную инженерию.
3. Средства и орудия — устройства (ноутбуки, смартфоны, серверы), программные средства (кейлоггеры, эксплойты, трояны, VPN-сервисы).
4. Следовая картина — логи, IP-адреса, хэш-записи, временные метки, cookie, сетевые трассировки.
5. Личность преступника — уровень технической подготовки, мотивация, социально-психологические особенности.

Цифровые следы — системообразующий элемент современной криминалистической характеристики преступлений в сфере компьютерной информации. Они обеспечивают объективную фиксацию действий преступника, механизмов атаки и каналов взаимодействия.

Развитие методов их поиска и анализа определяет эффективность расследования киберпреступлений.

Как справедливо подчёркивает З. И. Харисова, без изучения цифровых следов невозможно адекватно реконструировать механизм преступления, а значит, и обеспечить полноту доказательственного процесса [11, с. 201].

Киберкриминалистика, опираясь на понятие цифрового следа, формирует новую парадигму расследования — от пассивного реагирования к превентивному прогнозированию преступлений на основе анализа цифровых паттернов. Это направление становится ядром интеграции криминалистики, ИТ-технологий и уголовного судопроизводства XXI века.

Электронное уголовное дело: контуры модели

Переход к электронному уголовному делу (ЭУД) является естественным следствием цифровизации государственного управления и правосудия.

Если на первом этапе цифровая трансформация затронула документооборот и судебную переписку, то с 2020-х годов происходит формирование единого электронного контура уголовного судопроизводства, где все стадии — от регистрации заявления до вынесения приговора — существуют в цифровом виде.

Как отмечает Е. Попова, «электронное уголовное дело представляет собой совокупность цифровых документов, аудио- и видеозаписей, экспертных заключений, метаданных и протоколов, объединённых в защищённой информационной системе с обеспечением идентичности и целостности данных» [12, с. 54].

Киберкриминалистика в этой модели выполняет методологическую и технологическую функцию: обеспечивает сбор, верификацию и сохранность цифровых доказательств, формирует стандарты их легализации и интеграции в систему электронного правосудия.

Системная модель электронного уголовного дела включает три взаимосвязанных контура:

1. Контур сбора и фиксации данных — электронные протоколы, фото- и видеозаписи, аудиофайлы, заключения экспертов, отчёты о хэш-верификации, метаданные.

Важнейший элемент — автоматизированный журнал действий следователя и эксперта (digital audit trail), обеспечивающий непрерывный контроль за целостностью доказательств.

2. Контур процессуального документооборота — электронные постановления, ходатайства, обвинительные заключения, подписанные квалифицированной электронной подписью.

Этот контур уже реализован в МВД РФ через систему «Электронное уголовное дело» (ЭУД-СК), интегрированную с АИС «Дело-МИР».

3. Контур судебного рассмотрения и архивации — формирование электронного досье, передача материалов в суд через защищённые каналы связи (по протоколу СМЭВ 3.0), хранение в Федеральном архиве электронных дел.

Таким образом, ЭУД становится сквозной системой, обеспечивающей прослеживаемость каждого процессуального действия.

Ключевые дефициты и предложения

1. Терминологическая унификация. Необходимо единообразно использовать категории «электронные/цифровые доказательства», «электронный носитель», «цифровой след» (с перекрёстной отсылкой к киберкриминалистике).
2. Процедуры chain of custody. Закрепить обязательность форензически корректного извлечения и хранения, стандартизировать отчётность инструментов (hash-сопровождение, логирование, воспроизводимость).
3. Экспертные методики. Расширить перечень утверждённых методик СКТЭ, ввести требования к квалификации экспертов и оснащению лабораторий.
4. Электронное уголовное дело. Пилотировать защищённые контуры e-case с встраиванием форензических метрик (интеграция метаданных, неизменяемые журналы действий).
5. Подготовка кадров. Включить киберкриминалистику в программы следственных подразделений и судов, развивать межведомственные тренинги (следователь–оперативник–эксперт–прокурор).

Заключение

Киберкриминалистика сформировалась как самостоятельное направление, обеспечивающее процессуализацию цифровых следов и придающее доказыванию воспроизводимость, проверяемость и технологическую прозрачность. От междисциплинарной интеграции (право–ИТ–экспертиза) зависят допустимость, относимость и достоверность электронных/цифровых доказательств в суде. Научные результаты 2020–2025 гг. предлагают практические решения — от дефиниций и моделей цифровых следов до алгоритмов СКТЭ и контуров электронного уголовного дела; их внедрение требует стандартизации процедур, развития методик и кадрового обеспечения.

Список литературы:

[1] Сираканян А.Р. Использование цифровых технологий с искусственным интеллектом в борьбе с киберпреступностью в России и зарубежом // Вопросы российского и международного права. 2025. Том 15. № 2А. С. 506-515.

[2] Бондарева Г. В. Электронные доказательства в раскрытии и расследовании преступлений // Юрист-правоведъ. 2020. № 3(94). С. 151-155;

[3] Ильяшевич Т. А., Лубяная Н.И. Практические аспекты производства судебной компьютерно-технической экспертизы в уголовном процессе // Юридическая наука. 2023. № 3. С. 174-178;

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

[5] Абашева Ф. А. Информационные технологии в уголовном процессе (обзор состояния и перспектив): Монография. – Ижевск: Удмуртский университет, 2024. – 120 с.

[6] Shcherba S.P., Litvishko P.A. Collecting Electronic Evidence in Criminal Cases in Russia and Foreign Countries: Experiences and Problems: Monograph. – Moscow: Publishing House “Gorodets”, 2024. – 224 c.;

[7] Бессонова А. О. Электронный носитель информации как вещественное доказательство: особенности формирования и использования // Вестник Удмуртского университета. 2024. №5. С. 892-896;

[8] Грицаев С. И., Деменков Д.А. Цифровые (электронные) доказательства в уголовном процессе // Вестник экономики и права. 2024. № 88. С. 48-54;

[9] Тайтаков И. А. К вопросу об электронных доказательствах в уголовном процессе // Вестник науки. 2025. № 8(89). С. 96-102;

[10] Усов А. И. Стандарты судебной экспертизы как инструмент цифровизации криминалистики // Современные технологии и подходы в юридической науке и образовании: Сборник материалов международного научно-практического форума, Калининград, 27–31 августа 2020 года. – 2021. – С. 213-221.

[11] Харисова З. И. О структурных элементах криминалистической характеристики преступлений в сфере компьютерной информации // Журнал прикладных исследования. 2025. № 4. С. 199-203;

[12] Popova E. I. Impact of Digital Technologies on Criminal Proceedings // International Journal of Law in Changing World. 2023. № 2(1). С. 52-56.

References:

[1] Sirakanyan A.R. Use of digital technologies with artificial intelligence in the fight against cybercrime in Russia and abroad//Issues of Russian and international law. 2025. Volume 15. No. 2A. S. 506-515.

[2] Bondareva G.V. Electronic evidence in the disclosure and investigation of crimes//Lawyer. 2020. № 3(94). S. 151-155;

[3] Ilyashevich T.A., Lubyanaya N.I. Practical aspects of the production of forensic computer-technical expertise in criminal proceedings//Legal science. 2023. № 3. S. 174-178;

[4] Khomyakov E. G. On the essence of digital traces in forensics and their fixation//Society, law, statehood: retrospective and perspective. 2025. № 1 (21). S. 71-82.

[5] Abasheva F. A. Information technologies in criminal proceedings (review of the state and prospects): Monograph. - Izhevsk: Udmurt University, 2024. - 120 s.

[6] Shcherba S.P., Litvishko P.A. Collecting Electronic Evidence in Criminal Cases in Russia and Foreign Countries: Experiences and Problems: Monograph. – Moscow: Publishing House “Gorodets”, 2024. – 224 c.;

[7] Bessonova A.O. Electronic information carrier as material evidence: features of formation and use//Bulletin of Udmurt University. 2024. №5. S. 892-896;

[8] Gritsaev S.I., Demenkov D.A. Digital (electronic) evidence in criminal proceedings//Bulletin of Economics and Law. 2024. № 88. S. 48-54;

[9] Taytakov I. A. On the issue of electronic evidence in criminal proceedings//Bulletin of Science. 2025. № 8(89). S. 96-102;

[10] Usov A.I. Forensic standards as a tool for digitalization of forensic science//Modern technologies and approaches in legal science and education: Collection of materials of the international scientific and practical forum, Kaliningrad, August 27-31, 2020. – 2021. - S. 213-221.

[11] Harisova Z. I. On the structural elements of the forensic characterization of crimes in the field of computer information//Journal of Applied Research. 2025. № 4. S. 199-203;

[12] Popova E. I. Impact of Digital Technologies on Criminal Proceedings // International Journal of Law in Changing World. 2023. № 2(1). S. 52-56.