JOURNAL OF MULTIDISCIPLINARY SCIENCES AND INNOVATIONS
VOLUME 5, ISSUE 04
MONTHLY JOURNALS
ISSN NUMBER: 2751-4390
IMPACT FACTOR: 9,08

PROBLEMS OF COLLECTING AND PRESERVING DIGITAL EVIDENCE

Saidkarimova Sadiyaxon Xurshidovna
Master's Degree Student
Tashkent State University of Law
Tashkent, Republic of Uzbekistan
saidkarimovasadiya@gmail.com

ПРОБЛЕМЫ СБОРА И ФИКСАЦИИ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ

Саидкаримова Садияхон Хуршидовна
Студентка магистратуры
Ташкентского государственного юридического университета
г.Ташкент, Республика Узбекистан
saidkarimovasadiya@gmail.com

АННОТАЦИЯ: Аннотация ўзбек тилида. Мазкур мақолада жиноий суд иш юритувида рақамли далилларни йиғиш ва қайд этиш муаммолари Ўзбекистон қонунчилигидаги сўнгги ислоҳотлар ҳамда халқаро стандартлар асосида таҳлил қилинган. Ишнинг мақсади — электрон маълумотларнинг мақбуллиги, ишончлилиги ва исбот кучиган салбий таъсир кўрсатувчи техник, процессуал ва ташкилий тўсиқларни аниқлашдан иборат. Тадқиқотда формал-юридик, қиёсий-ҳуқуқий, тизимли-таркибий усуллар ҳамда 2021–2026 йиллардаги халқаро илмий адабиёт ва расмий қўлланмалар контент-таҳлили қўлланилди. Аниқланишича, асосий хавф манбалари рақамли муҳитнинг ўзгарувчанлиги, далилларни олиб қўйиш жараёнида маълумотларнинг ўзгариб кетиши, етарли қайд этилмаганда метамаълумотларнинг йўқолиши, шифрланган ва синхронлашувчи қурилмалар билан ишлашдаги қийинчиликлар, булутли маълумотларнинг трансчегаравий жойлашуви, шунингдек хешлаш, воситаларни валидация қилиш ва сақлаш занжирини ҳужжатлаштиришнинг аниқ тартибга солинмаганлигидир. Муаллиф томонидан оригинал ва нусхаларни қайд этиш, процессуал ҳужжатлаштириш, мобил ва булутли манбалар билан ишлаш, криминалистик воситаларни синовдан ўтказиш ҳамда deepfake шароитида мультимедиа файлларни баҳолаш бўйича таклифлар ишлаб чиқилди.

АННОТАЦИЯ: Рассмотрены современные проблемы сбора и фиксации цифровых доказательств в уголовном судопроизводстве с учетом новейших реформ законодательства Узбекистан и международных стандартов. Цель работы — выявить ключевые технологические, процессуальные и организационные препятствия, снижающие допустимость, достоверность и доказательственную силу электронных данных. В качестве методов использованы формально-юридический, сравнительно-правовой, системно-структурный методы, а также контент-анализ международной научной литературы и официальных руководств 2021–2026 годов. Установлено, что основными источниками риска выступают изменчивость цифровой среды, возможность модификации данных уже на стадии изъятия, утрата метаданных при неполной фиксации, трудности работы с зашифрованными и синхронизируемыми устройствами, трансграничный характер облачной информации, пробелы в локальной регламентации хеширования, валидации

инструментов и документирования цепочки хранения. Сделан вывод о том, что надежность цифрового доказывания обеспечивается не самим фактом наличия электронных данных, а воспроизводимой процедурой их обнаружения, изъятия, копирования, хеширования, хранения, проверки и представления в суде.

ABSTRACT: The article examines contemporary problems of collecting and recording digital evidence in criminal proceedings, taking into account the latest legislative reform in Uzbekistan and current international standards. The aim is to identify the technological, procedural and organizational barriers that reduce the admissibility, reliability and probative value of electronic data. The study uses formal-legal, comparative-legal and system-structural methods, together with a content analysis of international scholarship and official guidance published in 2021–2026. It is established that the main risks are the volatility of digital environments, alteration of data at the moment of seizure, loss of metadata due to incomplete documentation, difficulties with encrypted and synchronized devices, the cross-border location of cloud data, and the insufficient local regulation of hashing, tool validation and chain-of-custody recording. It is concluded that the trustworthiness of digital proof depends not on the mere existence of electronic data, but on a repeatable and transparent procedure for discovering, seizing, imaging, hashing, storing, reviewing and presenting such data before a court.

Калит сузлар: ҳақиқийлик; яхлитлик; метамаълумотлар; хешлаш; булутли криминалистика.

Ключевые слова: аутентичность; целостность; метаданные; хеширование; облачная криминалистика.

Keywords: authenticity; integrity; metadata; hashing; cloud forensics.

Обнаружено, что цифровые данные перестали быть периферийным приложением к уголовному делу и фактически стали его центральной доказательственной тканью. По данным проекта SIRIUS, поддерживаемого Европол и Евроюст, расследование и уголовное преследование в современной среде уже неотделимы от доступа к электронным данным, тогда как трансграничный доступ к ним по-прежнему осложняется медленными процедурами и риском утраты критически важных сведений[1].

В европейской литературе указывается, что необходимость трансграничного доступа к электронным доказательствам возникает примерно в 85% уголовных расследований, а около 65% запросов адресуются провайдерам, находящимся в иной юрисдикции. Тем самым вопрос о правильном сборе и надежной фиксации цифровых доказательств перестал быть узкоспециальным и превратился в один из базовых вызовов уголовного процесса[2].

---

[1] Sirius EU Electronic Evidence Situation Report. 2024. // URL: https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_E_Evidence_Situation_Report_2024.pdf

[2] Современные вызовы и угрозы национальной безопасности // URL: https://tver.ranepa.ru/upload/tver/dokumenty-pk-tver/%D0%A1%D0%B1%D0%BE%D1%80%D0%BD%D0%B8%D0%BA%20%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D0%B8%D0%B8_02.12.2025%20%D0%B3..pdf?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com

Установлено, что мировая научная литература последних пяти лет описывает проблему как междисциплинарную и все более сложную. Систематические обзоры 2024–2025 годов показывают, что наряду с классическими трудностями изъятия и копирования данных на первый план вышли облачная распределенность, многоарендность, постоянная синхронизация устройств, разнородность IoT-среды, закрытые мобильные экосистемы, антифорензика, а также кризис подлинности мультимедийных материалов на фоне deepfake-технологий. Отдельно подчеркивается, что оперативные, технические и управленческие ограничения влияют не только на качество анализа, но и на саму судебную пригодность цифрового следа[3].

Выяснено, что для правопорядка Республики Узбекистан тема приобрела особую актуальность в 2024–2025 годах. Законом от 21 ноября 2024 года № ЗРУ-1003 в УПК были введены положения о цифровых доказательствах, в том числе статья 204², подробно закрепившая их понятие и правила обращения с копиями, а также были скорректированы статьи о получении, хранении и пересылке доказательств. Одновременно Верховный суд в 2024 и 2025 годах уточнил подходы к исследованию цифровых доказательств в судебном заседании и к общему вопросу допустимости доказательств, а постановлением Президента от 21 июня 2024 года были поддержаны научно-исследовательская деятельность в сфере цифровой криминалистики и создание передвижной лаборатории. Это означает, что проблема теперь уже не теоретическая, а нормативно и институционально оформленная.

Однако сопоставление новой национальной регламентации с рекомендациями Национальный институт стандартов и технологий США, Scientific Working Group on Digital Evidence и Международная организация по стандартизации показывает, что между рамочным определением цифрового доказательства и детально воспроизводимой процедурой его собирания и фиксации существует заметный разрыв. Национальный закон уже признает значимость целостности и идентичности копии, но пока не детализирует обязательные правила хеширования, валидации инструментов, фиксации метаданных, работы с работающими системами, облачными сервисами и мультимедиа с подозрением на синтетическую генерацию[4].

Цель работы — выявить ключевые проблемы сбора и фиксации цифровых доказательств, охарактеризовать их технологические и процессуальные закономерности, выяснить пределы достаточности действующего регулирования Узбекистана и описать направления его дальнейшего совершенствования на основе международных стандартов и новейшей научной литературы.

В качестве эмпирической базы правового обзора использованы три группы источников. Первая группа — официальные акты и разъяснения, действующие в Республике Узбекистан: УПК в редакции после закона № ЗРУ-1003, акты о судебной практике, закон об электронном документообороте, закон об электронной цифровой подписи, а также постановление о развитии цифровой криминалистики. Вторая группа — международные стандарты и руководства: документы NIST, ISO/IEC 27037, материалы SWGDE, OSAC, Интерпола, Совета Европы, UNODC, Commonwealth и европейских институтов по электронным доказательствам. Третья группа — научные публикации 2021–2026 годов по облачной, мобильной, IoT- и мультимедийной криминалистике, а

[3] From digital trace to evidence: Challenges and insights from a trial case study // URL: https://www.sciencedirect.com/science/article/pii/S1355030625000905

[4] Сущенко С.А. / Электронные доказательства в уголовном процессе США // URL: электронные доказательства в уголовном процессе сшаКиберЛенинкаhttps://cyberleninka.ru › article › pdf

также по антифорензике, цепочке хранения, open-source инструментам и deepfake-детекции.

Рассмотрено применение формально-юридического метода для анализа терминологии, структуры и внутренней согласованности национальных норм; сравнительно-правового метода — для сопоставления узбекских процессуальных конструкций с международными руководствами по идентификации, сбору, копированию и сохранению данных; системно-структурного метода — для разложения проблемы на стадии обнаружения, изъятия, копирования, фиксации, хранения, проверки и представления в суде; контент-анализа — для выявления повторяющихся групп рисков в зарубежной литературе. Отбор международных публикаций производился по критерию тематической релевантности к проблеме допустимости, надежности и сохранности цифровых доказательств в уголовном процессе[5].

Раздел методологии сознательно ориентирован на воспроизводимость. Поэтому в анализ включались только те источники, которые позволяли проверить вывод по официальному тексту, аннотации либо авторитетному стандарту. Источниками возможной ошибки признаны: быстрое обновление программного обеспечения и изменение цифровых артефактов между версиями; неодинаковая поддержка разных моделей устройств; ограниченная публичность внутренних правил сервис-провайдеров; нехватка единых тестовых датасетов для deepfake-детекции; а также то обстоятельство, что разные эксперты могут обнаруживать разные подмножества релевантной информации в одном и том же массиве данных. Такие ограничения заранее учтены при оценке степени убедительности каждого вывода[6].

Материал исследования не включает самостоятельные эксперименты с вещественными носителями или живыми информационными системами; статья имеет доктринально-аналитический характер. Это означает, что основное внимание сосредоточено не на технической демонстрации конкретного инструмента, а на выработке юридически воспроизводимой модели обращения с цифровыми доказательствами, пригодной для следователей, прокуроров, судей и исследователей уголовного процесса.

Наиболее существенной технической проблемой признана изменчивость цифровой среды в момент изъятия. Руководства SWGDE прямо указывают, что live acquisition может оказаться единственной возможностью получения данных с зашифрованной работающей системы, однако такой способ сам по себе способен изменить системные и файловые даты, спровоцировать нестабильность процессов и повлечь так называемый smear-эффект. По этой причине порядок изъятия летучих данных не может быть интуитивным: он требует осознания порядка волатильности и обязательной фиксации каждого действия. Иначе следователь, пытаясь сохранить доказательство, может непреднамеренно создать новое доказательственное состояние, которое затем невозможно надежно отделить от первоначального.

Установлено, что международные рекомендации исходят из принципа минимизации изменений исходных данных. SWGDE связывает этот принцип с использованием аппаратных или программных write-blockers и с получением физического либо логического форензик-образа, тогда как NIST в своей научной оценке подчеркивает необходимость защиты исходных данных от непреднамеренной модификации и контроля

[5] https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27037:ed-1:v1:en

[6] Digital Investigation Techniques: A NIST Scientific Foundation Review // URL: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8354.pdf

целостности приобретенного массива. Отсюда вытекает важный практический вывод: цифровое доказательство должно изыматься не в том формате, который удобен для быстрого просмотра, а в том, который максимально сохраняет исходное состояние и допускает последующую проверку неизменности.

Особую группу трудностей образуют мобильные устройства. SWGDE отмечает, что мобильная криминалистика сталкивается с быстрыми технологическими изменениями, множеством производителей и моделей, закрытыми операционными системами и проприетарными интерфейсами, затрудняющими извлечение данных. Более того, традиционный совет «включить режим полета» уже не универсален: в новых версиях мобильных ОС он может не отключать Bluetooth, BLE, Wi-Fi и иные протоколы либо отключать их лишь временно; экранирующие контейнеры тоже не всегда гарантируют абсолютную изоляцию. Тем самым проблема фиксации начинается до лаборатории — уже на месте обнаружения устройства, где необходимо документировать его состояние, вид соединений, заряд, блокировку, открытые приложения и способ изоляции.

Научные обзоры по мобильной форензике подтверждают, что неполнота извлечения связана не только с физическим доступом к телефону, но и с фрагментацией данных между локальным хранилищем, облачными сервисами и синхронизируемыми приложениями. Для Android-экосистемы 2024 года подчеркивается необходимость постоянного обновления методик под новые версии системы и приложения, а в обзоре по мобильной форензике 2024 года в качестве наиболее частых проблем названы гетерогенность устройств, фрагментация данных, сложность облачной синхронизации, а также приватностные и правовые ограничения. Это означает, что даже формально удачное физическое изъятие устройства

Содержательно важным признан и человеческий фактор. Руководство Интерпол для первых реагирующих специально подчеркивает, что правила обращения с цифровыми доказательствами должны обеспечивать сохранность данных таким образом, чтобы они могли поддерживать уголовное расследование и быть допустимыми в суде. Интерпол одновременно делает акцент на обучении, стандартных методологиях и полевой помощи лабораторий. Следовательно, на начальной стадии главная угроза цифровому доказательству часто заключается не в сложности самой технологии, а в том, что первым к устройству подходит неподготовленный субъект, не осознающий значения сетевой изоляции, питания, состояния экрана, автосинхронизации и журналов системного времени.

Обнаружено, что центральным узлом всей доказательственной конструкции остается цепочка хранения и передачи. Современный обзор chain of custody прямо определяет ее как критическую процедуру, документирующую полный и хронологический путь доказательства и поддерживающую его целостность и аутентичность на протяжении расследования. Руководство Совета Европы по электронным доказательствам формулирует ту же мысль практическим языком: сторона, представляющая электронное доказательство, должна показать, кто и как получил его, где и когда оно было получено, кто обеспечивал его сохранность и кто владел им на разных этапах; последовательность должна охватывать поиск, изъятие, защиту, анализ и представление в суде. Иными словами, цифровой след становится доказательством не в момент обнаружения, а в момент успешного документирования его биографии[7].

Практика Верховного суда Республики Узбекистан подтверждает этот вывод: цифровое доказательство должно быть исследовано в совокупности с документами,

[7] Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics // UR;: https://sefcom.asu.edu/publications/CoC-SoK-tps2024.pdf

фиксирующими обстоятельства его изъятия и результаты исследования. Это означает, что даже содержательно «правдивый» файл теряет значительную часть доказательственной силы, если неясно, при каких условиях он был получен, чем копировался, каким носителем был представлен, как сохранялся и как проверялась неизменность его состояния. В результате проблема фиксации оказывается двуслойной: нужно установить и содержание файла, и надежность процедуры обращения с ним.

В научной литературе 2025 года дополнительно подтверждено, что допустимость цифровых доказательств, полученных даже при помощи open-source инструментов, связывается не с коммерческим статусом программы, а с возможностью доказать подлинность, надежность, полноту и надлежащую цепочку хранения. Вместе с тем авторы отмечают, что отсутствие унифицированных рамок валидации open-source решений приводит к тому, что суды и практика нередко предпочтут более дорогой коммерческий инструмент. Это создает ненужный финансовый барьер для качественной криминалистики и одновременно усиливает значение прозрачных национальных стандартов проверки инструментов, а не их брендов[8].

Рассмотрено, что облачная среда радикально усложняет сбор и фиксацию доказательств. NIST в модели Cloud Computing Forensic Reference Architecture прямо указывает, что новые методологии необходимы для идентификации, получения, сохранения, исследования и интерпретации доказательств в многоарендных облачных средах с быстрым развертыванием, глобальной эластичностью и широким сетевым доступом. К числу вызовов отнесены распределенная архитектура, поиск артефактов в больших и динамичных системах, сбор летучих данных, невозможность снять образ со всех облачных артефактов, риск затронуть конфиденциальность иных арендаторов, восстановление удаленных данных, корреляция артефактов между провайдерами и синхронизация временных меток логов. Современный систематический обзор облачной форензики подтверждает те же проблемы, дополняя их вопросами территориальности, зависимости от облачного провайдера и сложностями законной передачи данных[9].

Выяснено, что трансграничность электронных доказательств становится не исключением, а правилом. SIRIUS Report 2024 фиксирует: существующие каналы судебного сотрудничества зачастую оказываются непригодно медленными, что может приводить к потере критичных данных; в ответ некоторые органы обращаются к прямому добровольному взаимодействию с иностранными провайдерами. Eurojust отдельно отмечает, что именно для ответа на эти вызовы в июле 2023 года в рамках Европейского союза был принят законодательный пакет по электронным доказательствам. Тем самым проблема сбора цифровых доказательств все чаще выходит за пределы вопроса «как изъять устройство» и превращается в вопрос «как быстро и законно зафиксировать данные, физически никогда не находившиеся у следователя».

Особого внимания заслуживают механизмы Будапештской конвенции и Второго дополнительного протокола. На странице Совета Европы, посвященной протоколу, указано, что по состоянию на 15 апреля 2026 года его ратифицировали лишь четыре государства, то есть он еще только приближался к вступлению в силу; вместе с тем сам протокол рассчитан именно на усиленное сотрудничество и раскрытие электронных

[8] The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance // URL: https://journals.plos.org/plosone/article?id=10.1371%2Fjournal.pone.0331683

[9] NIST Cloud Computing Forensic Reference Architecture // URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-201.pdf

доказательств, включая прямые запросы к регистраторам и сервис-провайдерам, экстренное взаимодействие, совместные расследования и видеоконференции. Одновременно на странице Parties/Observers к Конвенции о киберпреступности Узбекистан не указан ни среди сторон, ни среди observer countries. Это не отменяет возможности международного сотрудничества, но показывает, что быстрая трансграничная фиксация электронных данных для узбекской практики пока не опирается на полный инструментарий этой конвенционной системы[10].

Отсюда вытекает и практический вывод: даже при наличии общих норм УПК о работе с электронными данными и международном сотрудничестве необходимо развивать собственные ускоренные процессы раннего сохранения облачных и сетевых данных, национальные шаблоны preservation request и специализированные точки контакта с провайдерами. Совет Европы в своей платформе country wiki специально публикует шаблоны запросов о сохранении данных и о предоставлении subscriber information, а профиль Узбекистана уже связывает национальные нормы с expedited preservation и production order. Следовательно, следующий этап развития не в признании самой проблемы, а в ее операционализации до уровня ежедневной следственной процедуры.

Еще более остро сегодня стоит проблема мультимедийных файлов и deepfake. Исследование 2025 года по explainable deepfake detection подчеркивает: для юридических расследований недостаточно просто высокой точности; необходима также прозрачность и понятное объяснение, почему изображение признано синтетическим.

Правовая дискуссия подтверждает этот поворот. В докладе о deepfake-доказательствах для уголовного процесса отмечается, что у визуальных материалов размывается традиционная презумпция подлинности, а неравный доступ сторон к продвинутым инструментам выявления подделок ставит вопрос об equality of arms.

В этих условиях фиксация мультимедийного доказательства должна рассматриваться как многоуровневая процедура. Необходимо сохранять исходный файл в первичном виде, отдельно создавать рабочие копии, фиксировать сведения об источнике получения, вычислять хеш, документировать программное окружение и любые действия по обработке, а при наличии признаков синтетической генерации — раскрывать метод и пределы технической проверки. Иначе суд получает не доказательство, а набор плохо верифицируемых цифровых фрагментов, чья доказательственная ценность будет неизбежно снижаться.

Сопоставление национальных и международных подходов позволяет сформулировать ряд практически ориентированных предложений.

Во-первых, целесообразно закрепить обязательный минимум реквизитов фиксации цифрового доказательства в самом УПК либо в подзаконной инструкции, обязательной для дознания, следствия и суда. В такой минимум должны входить: идентификаторы устройства и носителя, состояние питания и сети в момент обнаружения, сведения о блокировке, дата и время по устройству и по внешнему эталону, используемый инструмент и его версия, способ копирования, рассчитанные хеш-значения, основание live acquisition, данные о присутствовавших специалистах и непрерывный журнал передачи.

Во-вторых, необходима более четкая процессуальная дифференциация между полевым сбором, лабораторным приобретением и аналитической обработкой данных. Живое изъятие с работающей системы должно допускаться в качестве исключения, когда есть реальный риск утраты волатильной информации или когда иным способом нельзя

[10] Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence // URL: https://www.coe.int/en/web/cybercrime/second-additional-protocol

получить доступ к зашифрованным данным; при этом причина выбора именно live acquisition должна специально мотивироваться в протоколе.

В-третьих, следует ввести обязательную локальную валидацию критических инструментов: write-blockers, средств RF-изоляции, устройств снятия образов, программных модулей выгрузки и систем журналирования. Результаты испытаний, сведения об обновлениях и периодичности ретестирования должны быть доступны суду и сторонам процесса.

В-четвертых, для видео, аудио и иных мультимедийных материалов необходимо закрепить правило двойного сохранения: нативный оригинал плюс проверяемая рабочая копия в открытом или общедоступном формате, если закрытая система воспроизведения создает барьер для суда и защиты. При обработке изображений и видео любые шаги улучшения, реставрации либо применения нейросетевых средств должны фиксироваться с указанием версии программы и параметров обработки.

В-пятых, имеет смысл разработать национальный ускоренный механизм сохранения облачных данных и данных провайдеров до получения полного международного или межведомственного ответа. Речь идет о типовых preservation requests, централизованных контактных точках, протоколах взаимодействия со служебными аккаунтами провайдеров, а также инструкциях по фиксации интернет-данных и сетевых логов до их автоматического удаления.

В-шестых, для synthetic media необходимо выработать специальный стандарт судебной проверки подлинности. В него должны входить: приоритет представления исходного файла, проверка цепочки происхождения, фиксация устройства первоначального захвата, техническое исследование метаданных, раскрытие способа и ограничений использованного детектора, возможность для защиты получить разумный доступ к верификации и, при необходимости, участие IT-эксперта.

В-седьмых, необходимо институционализировать непрерывное обучение. Практический смысл имели бы отдельные модули для следователей, оперативных сотрудников, прокуроров, судей и адвокатов: от базовой цифровой сцены происшествия и сетевой изоляции телефона до оценки журналов хеширования, облачных ответов провайдера и deepfake-рисков.

В-восьмых, перспективным следует признать внедрение цифровых систем управления доказательствами с полноценным audit trail. Новые блокчейн-ориентированные модели действительно способны усиливать прозрачность, неизменяемость журналов и отслеживаемость операций, однако современная литература справедливо предупреждает: даже самая надежная запись о хеше и времени не доказывает истинность исходного содержания и не компенсирует дефекты первоначального получения.

Установлено, что проблема сбора и фиксации цифровых доказательств имеет двойственную природу. С одной стороны, она обусловлена свойствами самой цифровой среды: волатильностью, распределенностью, синхронизацией, шифрованием, антифорензикой, закрытыми форматами и ростом синтетического контента. С другой стороны, она порождается юридической и организационной незавершенностью процедуры: рамочной регламентацией, неполной валидацией инструментов, дефицитом навыков, несистемной документацией и отсутствием устойчивых моделей раннего сохранения данных.

Выяснено, что реформы Республики Узбекистан 2024–2025 годов принципиально изменили исходную точку дискуссии: цифровые доказательства получили прямое нормативное признание, а суду даны ориентиры по их исследованию и оценке. Тем не менее действующая конструкция все еще нуждается в развитии от уровня общей

допустимости к уровню детальной форензической процедуры. Именно на этом уровне решаются основные вопросы: что считать оригиналом, как фиксировать копию, когда допустимо живое копирование, как проверять неизменность, как документировать вмешательство в систему, как обращаться с облачными сервисами, и какие требования предъявлять к мультимедиа в эпоху deepfake.

Оценено влияние международных руководств и современной литературы как высокое и практически значимое. Они показывают, что надежное цифровое доказывание строится на шести взаимосвязанных элементах: минимизации вмешательства в источник, сохранении нативного состояния, хешировании и проверке целостности, непрерывной цепочке хранения, валидации инструментов и доступности проверки для суда и сторон процесса. В отсутствие хотя бы одного из этих элементов электронные данные не исчезают, но их доказательственная сила становится уязвимой.

Сделан общий вывод о том, что современная уголовно-процессуальная модель должна отказаться от наивного представления, будто цифровое доказательство «само говорит за себя». Напротив, обнаружено, что цифровое доказательство говорит убедительно только тогда, когда за ним стоит проверяемая, повторяемая и справедливая процедура его сбора и фиксации. Поэтому дальнейшее развитие узбекского законодательства и практики должно идти по пути стандартизации протоколов, технологической валидации, ускоренного сохранения данных, судебной проверки подлинности мультимедиа и полномасштабной подготовки правоприменителей.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Законодательство Республики Узбекистан

1. Уголовно-процессуальный кодекс Республики Узбекистан
2. Закон Республики Узбекистан “О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан, направленных на совершенствование системы работы с цифровыми доказательствами”
3. Закон Республики Узбекистан “Об электронном документообороте”
4. Закон Республики Узбекистан “Об информатизации”
5. Постановление Президента Республики Узбекистан “О мерах по организации научно-исследовательской деятельности в сфере цифровой криминалистики”

II. Учебники, научные статьи и доклады

1. Янковая В.Ф. Электронный документ как объект документоведения // Вестник Волгоградского государственного университета. 2013. №3.
2. Подволоцкий И.Н. Осмотр и предварительное исследование документов. М.: Юрлитинформ, 2004. 198с.
3. Новицкий В.А., Новицкая Л.Ю. Понятие и виды цифровых доказательств // Ленинградский юридический журнал. 2019. №1 (55)
4. Сущенко С.А. / Электронные доказательства в уголовном процессе США // URL: электронные доказательства в уголовном процессе сшаКиберЛенинкаhttps://cyberleninka.ru › article › pdf
5. Чернышов В.Н., Лоскутова Е.С. / Проблемы собирания и использования цифровых доказательств // URL: https://cyberleninka.ru/article/n/problemy-sobiraniya-i-ispolzovaniya-tsifrovyh-dokazatelstv/viewer
6. Безлепкина О.В., Федотова А.В. / Проблемные аспекты собирания электронных доказательств // URL: https://cyberleninka.ru/article/n/problemnye-aspekty-sobiraniya-elektronnyh-dokazatelstv/viewer

III. Электронные ресурсы

1. Современные вызовы и угрозы национальной безопасности // URL: https://tver.ranepa.ru/upload/tver/dokumenty-pk-tver/%D0%A1%D0%B1%D0%BE%D1%80%D0%BD%D0%B8%D0%BA%20%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D0%B8%D0%B8_02.12.2025%20%D0%B3..pdf?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com

7. Sirius EU Electronic Evidence Situation Report. 2024. // URL: https://www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_E_Evidence_Situation_Report_2024.pdf

8. From digital trace to evidence: Challenges and insights from a trial case study // URL: https://www.sciencedirect.com/science/article/pii/S1355030625000905

9. Digital Investigation Techniques: A NIST Scientific Foundation Review // URL: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8354.pdf

10. Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics // UR;: https://sefcom.asu.edu/publications/CoC-SoK-tps2024.pdf

11. The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance // URL: https://journals.plos.org/plosone/article?id=10.1371%2Fjournal.pone.0331683

12. NIST Cloud Computing Forensic Reference Architecture // URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-201.pdf

13. Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence // URL: https://www.coe.int/en/web/cybercrime/second-additional-protocol

14. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27037:ed-1:v1:en