МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ КАЗАХСТАН

АЛМАТИНСКАЯ АКАДЕМИЯ
имени МАКАНА ЕСБУЛАТОВА

КРИМИНАЛИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ ЦИФРОВОЙ ИНФОРМАЦИИ

Методические рекомендации

Алматы 2025

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ КАЗАХСТАН
АЛМАТИНСКАЯ АКАДЕМИЯ
имени МАКАНА ЕСБУЛАТОВА

КРИМИНАЛИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ ЦИФРОВОЙ ИНФОРМАЦИИ

Методические рекомендации

Алматы 2025

Обсуждено и одобрено на заседании научно-методическом совете Алматинской академии МВД Республики Казахстан им. М. Есбулатова (протокол №7 от «18» сентября 2025 года)

Рецензенты:

Коржумбаева Т.М. – начальник кафедры административно-правовых дисциплин Алматинской академии МВД Республики Казахстан им. М. Есбулатова, к. ю.н., ассоциированный профессор (доцент), полковник полиции.

Калиев А.А., – руководитель криминалистического отдела ДЭР по городу Алматы подполковник службы экономических расследований.

М.К. Сырлыбаев, Криминалистическое исследование цифровой информации: Методические рекомендации. – Алматы: ООНИиРИР Алматинской академии МВД Республики Казахстан им. М. Есбулатова, 2025. – 40 с.

Методические рекомендации подготовлены в соответствии с Планом НИД Алматинской академии позиция 8 Криминалистическое исследование цифровой информации (2025г.), и разработаны с учетом современных требований криминалистики и уголовно-процессуального законодательства. Отражают основные понятия, стандарты обнаружения, изъятия и исследования цифровой информации.

Методические рекомендации предназначены для сотрудников правоохранительных органов, а также научных и практических работников системы ОВД, преподавателей и обучающихся ведомственных и иных юридических учебных заведений.

Введение

В эпоху цифровой трансформации, когда информационные технологии пронизывают все сферы человеческой деятельности, криминалистическое исследование цифровой информации приобретает особую актуальность. Цифровая информация, как основа современных преступлений, требует специализированных подходов к ее выявлению, фиксации и анализу. Настоящие методические рекомендации разработаны в академическом стиле, опираясь на обширный массив научной литературы, нормативных актов Республики Казахстан и практических примеров. Они предназначены для специалистов в области криминалистики, сотрудников правоохранительных органов, судебных экспертов, а также студентов и аспирантов юридических вузов.

Структура включает четыре основных раздела, соответствующих запросу: понятие цифровых следов, способы создания, хранения и передачи цифровой информации, порядок обнаружения цифровых доказательств и процессуальный порядок их закрепления. Рекомендации основаны на Уголовно-процессуальном кодексе Республики Казахстан (УПК РК) от 4 июля 2014 года №231-V ЗРК, Законе Республики Казахстан «Об информатизации» от 24 ноября 2015 года №418-V ЗРК, а также на работах ведущих криминалистов, таких как Р.С. Белкин, Е.Р. Россинская, Д.В. Бахтеев и казахстанских специалистов в области цифровой криминалистики.

Цифровая криминалистика, как междисциплинарная область, сочетает элементы информатики, права и психологии. В 2025 году, по данным МВД РК, количество киберпреступлений выросло на 25% по сравнению с 2024 годом, что подчеркивает необходимость глубокого понимания цифровых следов. Рекомендации учитывают это, предлагая комплексные подходы к их исследованию.

Исторический обзор развития цифровой криминалистики в Казахстане (2010-2025)

Цифровая криминалистика в Республике Казахстан (РК) за последние полтора десятилетия прошла значительный путь, трансформируясь из зарождающейся дисциплины в ключевой инструмент противодействия киберпреступности. Этот процесс был обусловлен глобальной цифровизацией, ростом киберугроз и необходимостью адаптации правоохранительных органов к новым вызовам. Настоящий обзор охватывает развитие цифровой криминалистики в Казахстане с 2010 года по 2025 год, включая ключевые события, такие как введение электронного уголовного дела в Уголовно-процессуальный кодекс РК (УПК РК) в 2014 году и открытие первой специализированной криминалистической цифровой лаборатории в 2023 году. Также анализируются влияние Закона РК «Об информатизации», международные стандарты, включая Berkeley Protocol, и роль пандемии COVID-19 в ускорении цифровизации расследований. Документ включает анализ ключевых определений, примеры кейсов киберпреступлений и эволюцию понятий цифровых следов.

Ключевые положения Закона «Об информатизации»

Закон «Об информатизации» создает правовую основу для использования цифровых данных в уголовном процессе, обеспечивая их юридическую силу, защиту и интеграцию в расследования. Основные положения, относящиеся к цифровой криминалистике, включают:

Статья 1 определяет базовые термины, включая понятие «цифровые данные» как информацию в электронной форме, пригодную для обработки автоматизированными системами. Это определение обеспечивает правовую основу для признания цифровых следов, таких как логи, метаданные и контент с устройств, в качестве доказательств в уголовном процессе, что соответствует требованиям статьи 125 Уголовно-процессуального кодекса РК (УПК РК) о допустимости доказательств.

Статья 16 устанавливает требования к защите информации, включая обязательное использование шифрования, контроля доступа и других мер кибербезопасности. Эти положения имеют решающее значение для сохранения целостности и конфиденциальности цифровых доказательств, предотвращая их модификацию или утрату в ходе расследований. Например, использование сертифицированных программно-аппаратных комплексов в Digital Crime Lab (DCL), созданной в 2023 году, опирается на эти требования.

Статья 23 регулирует создание и функционирование информационно-коммуникационной инфраструктуры, включая государственные базы данных, такие как Система обмена информацией правоохранительных и специальных государственных органов (СИОПСО). Эта инфраструктура обеспечивает интеграцию данных из различных источников, включая криминалистические базы, что позволяет проводить анализ цифровых следов в реальном времени, например, при проверке судимости или идентификации подозреваемых.

Статья 67 устанавливает ответственность за нарушения в сфере информационной безопасности, включая киберпреступления, такие как несанкционированный доступ, распространение вредоносного ПО и фишинг. Это положение усиливает правовую базу для расследования киберпреступлений, предоставляя правоохранительным органам инструменты для привлечения виновных к ответственности.

Закон синхронизирован с положениями УПК РК, в частности со статьей 42-1, регулирующей электронное производство уголовных дел, и обеспечивает правовую основу для использования таких инструментов, как модуль «Электронное уголовное дело» (e-UD) и автоматизированные рабочие места «Криминалист» и «Эксперт». Эти механизмы, внедренные в 2017–2018 годах, позволяют собирать, хранить и анализировать цифровые доказательства в соответствии с международными стандартами юридической силы и достоверности.

Сравнение с международным опытом: Berkeley Protocol

Berkeley Protocol on Digital Open Source Investigations (2020), разработанный Калифорнийским университетом в Беркли, представляет собой международный стандарт для сбора, анализа и использования данных из открытых источников (OSINT) в расследованиях. Он акцентирует внимание на этических, методологических и технических аспектах работы с цифровыми данными, особенно из социальных сетей, видеохостингов и других публичных платформ. Сравнение Закона РК «Об информатизации» с Berkeley Protocol выявляет как сходства, так и различия в подходах к цифровой криминалистике.

Сходства

1. Целостность доказательств: Как Закон (статья 16), так и Berkeley Protocol подчеркивают важность сохранения целостности цифровых данных. Protocol требует строгого документирования цепочки хранения (chain of custody), включая хеширование данных для подтверждения их неизменности, что соответствует казахстанской практике, применяемой в DCL с 2023 года, где используются программно-аппаратные комплексы для фиксации цифровых следов.

2. Юридическая сила: Оба документа признают необходимость соответствия цифровых доказательств правовым стандартам. В Казахстане это обеспечивается через УПК РК и Закон «Об информатизации», которые гарантируют допустимость электронных доказательств в суде. Berkeley Protocol, в свою очередь, предлагает методологии, обеспечивающие юридическую приемлемость данных из открытых источников, что частично интегрировано в казахстанскую практику с 2024 года в рамках Концепции обеспечения общественной безопасности.

Различия

1. Фокус регулирования: Закон РК «Об информатизации» сосредоточен на создании и защите внутренней информационно-коммуникационной инфраструктуры, включая государственные базы данных и системы, такие как СИОПСО. Berkeley Protocol, напротив, ориентирован на работу с

открытыми источниками, такими как социальные сети, и не регулирует государственные системы, а предоставляет рекомендации для универсального применения.

2. Этические аспекты: Berkeley Protocol уделяет значительное внимание этике, включая необходимость верификации источников, защиты конфиденциальности и минимизации вреда при сборе данных. Закон «Об информатизации» не содержит явных этических норм, хотя положения о защите персональных данных частично пересекаются с Законом РК «О персональных данных и их защите» № 94-V от 21 мая 2013 года. Этические аспекты в казахстанской практике пока развиваются, особенно в контексте анализа данных из социальных сетей.

3. Методология сбора данных: Berkeley Protocol предлагает структурированный процесс сбора данных, включая верификацию источников, геолокацию и временные метки. В Казахстане аналогичные методологии начали внедряться с 2024 года в рамках работы DCL, но они пока ограничены специализированными лабораториями и не имеют столь детализированного нормативного закрепления, как в Berkeley Protocol.

Интеграция международного опыта

С 2024 года Казахстан начал адаптировать элементы Berkeley Protocol в практику цифровой криминалистики, особенно в части верификации данных из открытых источников. Например, обучение сотрудников DCL включает изучение международных стандартов OSINT, что поддерживается сотрудничеством с ОБСЕ. Однако полная интеграция требует дальнейшего совершенствования нормативной базы, включая дополнение Закона «Об информатизации» положениями об этическом сборе данных и методологии верификации. Это позволит Казахстану соответствовать глобальным стандартам, таким как те, что применяются в юрисдикциях Совета Европы или Интерпола.

Роль Закона в развитии цифровой криминалистики

Закон «Об информатизации» сыграл ключевую роль в институционализации цифровой криминалистики в Казахстане, обеспечив правовую и техническую основу для работы с цифровыми доказательствами. Его положения способствовали созданию таких инфраструктурных решений, как СИОПСО и e-UD, а также специализированных лабораторий, таких как DCL. В сочетании с УПК РК Закон обеспечивает юридическую силу цифровых доказательств, что подтверждается статистикой: к 2023 году 43% досудебных расследований (115 811 дел) велось в электронном формате, из которых 13 417 были направлены в суд.

Вместе с тем, международный опыт, представленный Berkeley Protocol, указывает на необходимость дальнейшего развития. Включение этических стандартов, усиление методологической базы для OSINT и расширение подготовки специалистов в области цифровой криминалистики позволят Казахстану укрепить свои позиции в глобальной системе борьбы с киберпреступлениями. Закон «Об информатизации» остается основой для этих преобразований, но его потенциал будет реализован в полной мере при условии гармонизации с международными стандартами и внедрения инновационных технологий, таких как искусственный интеллект и блокчейн, для анализа и защиты цифровых доказательств.

1. Понятие цифровой информации и цифровых доказательств

Цифровая информация и цифровые доказательства представляют собой фундаментальные элементы современного правового регулирования, особенно в контексте цифровизации общества и государственных процессов. В законодательстве Республики Казахстан эти понятия интегрированы в систему норм, направленных на обеспечение информационной безопасности, юридической силы электронных данных и их использования в процессуальных действиях. Настоящий анализ опирается на ключевые нормативные акты, включая Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года №418-V (с изменениями и дополнениями по состоянию на 2025 год), Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года №231-V (с изменениями по состоянию на 2025 год), Закон Республики Казахстан «Об электронном документе и электронной цифровой подписи» от 7 января 2003 года №370-II (с изменениями по состоянию на 2025 год) и Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года №94-V (с изменениями по состоянию на 2025 год). Эти документы формируют правовую основу для определения, обработки и защиты цифровой информации, а также для ее трансформации в доказательства в рамках уголовного процесса.

Понятие цифровой информации

Цифровая информация в законодательстве Республики Казахстан трактуется как данные, представленные в электронно-цифровой форме, подлежащие хранению, обработке и передаче с использованием информационно-коммуникационных технологий. Согласно п.57 ст. 1 Закона «Об информатизации», электронные информационные ресурсы определяются как информация в электронно-цифровой форме, содержащаяся на электронном носителе и в объектах информатизации. Электронный носитель, в свою очередь, представляет собой

материальный объект, предназначенный для хранения информации в электронной форме, а также для ее записи или воспроизведения с помощью технических средств. Это определение подчеркивает материальную и техническую основу цифровой информации, отличая ее от традиционных форм и связывая с конкретными устройствами, такими как серверы, жесткие диски или облачные хранилища.

Закон «Об информатизации» классифицирует электронные информационные ресурсы по нескольким критериям: по принадлежности (государственные и негосударственные), по режиму доступа (общедоступные и с ограниченным доступом) и по содержанию (включая государственные секреты или конфиденциальную информацию). Государственные электронные информационные ресурсы формируются за счет бюджетных средств или в процессе деятельности государственных органов, в то время как негосударственные создаются на средства физических или юридических лиц. Общедоступные ресурсы предоставляются без условий, а ресурсы с ограниченным доступом регулируются законодательством или владельцами. Такие классификации обеспечивают правовую основу для регулирования доступа и использования цифровой информации, подчеркивая принципы открытости, объективности и надежности, изложенные в статье 3 указанного закона.

В контексте обработки цифровой информации статья 34 Закона «Об информатизации» устанавливает правила формирования и использования электронных информационных ресурсов. Они предназначены для удовлетворения информационных нужд государственных органов, физических и юридических лиц, а также для выполнения государственных функций и предоставления услуг в электронной форме. Управление данными в этих ресурсах должно соответствовать требованиям к управлению данными, что включает обеспечение их целостности, конфиденциальности и доступности. Кроме того, электронные документы формируются в сервисе цифровых документов на основе данных из информационных

систем, что усиливает интеграцию цифровой информации в государственные процессы.

Закон «Об электронном документе и электронной цифровой подписи» дополняет это понятие, определяя электронный документ как информацию в электронно-цифровой форме, удостоверенную электронной цифровой подписью. Электронная цифровая подпись (ЭЦП) представляет собой набор электронных символов, созданных средствами ЭЦП, подтверждающих аутентичность документа, его принадлежность и неизменяемость содержания. Согласно статье 7, электронный документ, соответствующий требованиям закона и подписанный уполномоченным лицом, приравнивается к документу на бумажном носителе. Это обеспечивает юридическую силу цифровой информации, делая ее эквивалентной традиционным формам при соблюдении условий, таких как верификация открытого ключа ЭЦП и использование аккредитованных центров сертификации.

Цифровая информация характеризуется свойствами, такими как машиночитаемость, воспроизводимость и подверженность модификациям, что требует строгих мер защиты. Статья 53 Закона «Об информатизации» определяет защиту объектов информатизации как комплекс правовых, организационных и технических мер, направленных на предотвращение несанкционированного доступа и воздействия. Защита включает обеспечение конфиденциальности ограниченных ресурсов, реализацию прав доступа и предотвращение незаконных действий, таких как блокирование, модификация или уничтожение данных. Владельцы и операторы обязаны принимать меры по выявлению нарушений, минимизации последствий и восстановлению данных, а также сообщать об инцидентах в Национальный координационный центр информационной безопасности.

Понятие цифровых доказательств

Цифровые доказательства в законодательстве Республики Казахстан интегрируются в общую систему

доказательств, регулируемую Уголовно-процессуальным кодексом. Хотя УПК не содержит прямого определения «цифровых доказательств», они подпадают под категорию доказательств как фактических данных, полученных в предусмотренном порядке, на основании которых устанавливается наличие или отсутствие правонарушения, виновность лица и иные обстоятельства (статья 111). Фактические данные включают показания, заключения экспертов, вещественные доказательства, протоколы и другие документы, среди которых электронные формы занимают значимое место.

Согласно статье 120 УПК, документы признаются доказательствами, если они содержат сведения, устанавливающие или опровергающие обстоятельства дела, и включают компьютерную информацию, фото-, видео- и аудиозаписи, полученные в соответствии с процедурой. Эти документы могут быть представлены в письменной или иной форме, включая электронную, и хранятся при деле или возвращаются владельцам с копированием. Статья 7 УПК определяет электронный документ как информацию в электронно-цифровой форме, удостоверенную ЭЦП, что связывает его с понятием из Закона «Об электронном документе и электронной цифровой подписи».

Допустимость цифровых доказательств регулируется статьей 112 УПК: данные недопустимы, если получены с нарушением закона, такими как насилие, обман или участие неуполномоченных лиц, что влияет на их надежность. Для цифровых доказательств это подразумевает соблюдение цепочки хранения, включая фиксацию в протоколах и использование технических средств для подтверждения неизменности. Сбор доказательств осуществляется через процессуальные действия, такие как осмотр, обыск и экспертиза (статьи 220-222), а также через запросы документов и предметов (статья 122), которые могут быть в электронной форме.

Статья 123 УПК устанавливает правила фиксации доказательств: они записываются в протоколы, с использованием технических средств, таких как аудио- или видеозапись,

детали которых фиксируются. Участники процесса имеют право на ознакомление, внесение изменений и возражения. Хранение вещественных доказательств, включая цифровые носители, регулируется статьей 118: они прикрепляются к делу и хранятся до вступления приговора в силу. В случае персональных данных хранение должно соответствовать Закону «О персональных данных и их защите», где статья 12 требует размещения баз данных на территории РК и обеспечения их целостности, конфиденциальности и доступности.

Оценка цифровых доказательств осуществляется по критериям релевантности, допустимости, надежности и достаточности (статья 125 УПК). Научно-технические средства, включая цифровые инструменты, могут использоваться для сбора и анализа доказательств с участием специалистов (статья 126). Электронный формат уголовного производства, предусмотренный статьей 42-1 УПК, позволяет вести дела в электронной форме по мотивированному постановлению, с учетом технических возможностей и мнений участников.

Защита и обработка цифровой информации как основа доказательств

Защита цифровой информации является ключевым аспектом, обеспечивающим ее трансформацию в доказательства. Статья 22 Закона «О персональных данных и их защите» обязывает владельцев, операторов и третьих лиц принимать меры по предотвращению несанкционированного доступа, выявлению нарушений и минимизации последствий. Обработка персональных данных, включая накопление, хранение и уничтожение, требует согласия субъекта (статья 8), за исключением случаев, предусмотренных законом. Согласие может быть дано в электронной форме через государственные сервисы, с детальной фиксацией условий.

В Законе «Об информатизации» статья 42 устанавливает требования к техническим средствам для хранения и передачи электронных ресурсов, включая обязательное создание

резервных копий. Защита персональных данных в электронных ресурсах регулируется статьей 56, требующей мер от сбора до уничтожения или обезличивания. Трансграничная передача данных разрешена только в страны, обеспечивающие адекватную защиту (статья 16 Закона «О персональных данных и их защите»).

Рекомендации по работе с цифровой информацией и доказательствами

Для эффективного применения понятий цифровой информации и доказательств рекомендуется:

1. Обеспечивать верификацию ЭЦП при работе с электронными документами, в соответствии со статьей 10 Закона «Об электронном документе и электронной цифровой подписи», используя открытые ключи и регистрационные сертификаты.

2. Соблюдать протоколы фиксации и хранения, включая резервное копирование и шифрование, как предусмотрено в статье 54 Закона «Об информатизации».

3. Получать согласие на обработку персональных данных в электронной форме через государственные сервисы (статья 8-1 Закона «О персональных данных и их защите»).

4. Использовать электронный формат производства для ускорения анализа доказательств (статья 42-1 УПК).

5. Мониторить инциденты безопасности и сообщать о них, чтобы сохранить целостность данных (статья 7-1 Закона «Об информатизации»).

В целом, законодательство Республики Казахстан обеспечивает комплексный подход к цифровой информации и доказательствам, балансируя между технологическими инновациями и правовой защитой.

2. Способ создания, хранения и передачи цифровой информации

2.1 Способы создания цифровой информации

Создание цифровой информации представляет собой процесс генерации, фиксации или преобразования данных в электронно-цифровой формат, пригодный для обработки, хранения и передачи с использованием информационно-коммуникационных технологий (ИКТ). Этот процесс является основой цифровой экономики, научных исследований и государственного управления. Основные методы создания цифровой информации включают следующие подходы:

1. **Дигитализация аналоговых данных**: Преобразование физических носителей информации, таких как бумажные документы, фотографии или аудиозаписи, в цифровой формат. Применяются технологии оптического распознавания символов (OCR) для текстов, аналого-цифровые преобразователи (АЦП) для аудио и видео, а также сканеры для изображений. Например, сканирование архивных документов в формат PDF или TIFF обеспечивает их доступность в цифровой среде. Этот метод требует высокой точности, так как ошибки при оцифровке могут привести к потере данных или их искажению.

2. **Генерация данных автоматизированными системами**: Создание информации посредством программного обеспечения, датчиков Интернета вещей (IoT) или алгоритмов машинного обучения. Например, системы мониторинга в реальном времени, такие как датчики температуры в промышленности или GPS-трекеры, генерируют цифровые данные о физических процессах. Базы данных (SQL или NoSQL) также создают структурированные данные, например, логи транзакций в банковских системах. Этот метод широко используется в автоматизированных системах, где данные генерируются без прямого участия человека.

3. **Ручной ввод данных**: Пользовательский ввод через интерфейсы, такие как веб-формы, мобильные приложения

или API. Этот метод часто применяется в административных процессах, например, при заполнении электронных анкет или регистрации данных в CRM-системах. Несмотря на свою простоту, ручной ввод подвержен человеческим ошибкам, что требует дополнительных проверок.

4. **Алгоритмическое создание данных**: Использование искусственного интеллекта (ИИ) и больших языковых моделей для генерации текстов, изображений или синтетических данных. Например, модели ИИ, такие как нейронные сети, могут создавать синтетические датасеты для обучения других алгоритмов, минимизируя необходимость сбора реальных данных. Этот метод становится все более популярным в научных исследованиях и тестировании программного обеспечения.

Создание цифровой информации должно учитывать принципы конфиденциальности, целостности и доступности (CIA triad), описанные в международном стандарте ISO/IEC 27001:2013. Например, данные, содержащие персональную информацию, требуют согласия субъекта и ограничения по объему сбора в соответствии с принципом минимизации данных, закрепленным в Общем регламенте по защите данных (GDPR) ЕС (статья 5). Кроме того, для обеспечения аутентичности применяются цифровые подписи, основанные на криптографических алгоритмах, таких как RSA или ECDSA, которые гарантируют авторство и неизменность данных.

Технические аспекты создания включают использование стандартизированных форматов (JSON, XML, CSV) для структурирования данных, что упрощает их последующую обработку. Также применяются системы контроля версий (например, Git) для отслеживания изменений в программных данных, что особенно актуально в разработке ПО. Современные тенденции, такие как использование блокчейн-технологий для создания неизменяемых записей, дополнительно повышают надежность данных, особенно в финансовых и юридических приложениях.

2.2 Способы хранения цифровой информации

Хранение цифровой информации предполагает организацию данных на носителях или в системах, обеспечивающих их долгосрочное сохранение, доступность и безопасность. Основные методы хранения включают:

1. **Локальное хранение**: Использование физических носителей, таких как жесткие диски (HDD), твердотельные накопители (SSD), оптические диски (CD/DVD) или USB-накопители. Локальное хранение подходит для небольших объемов данных или в условиях ограниченного доступа к сети. Однако оно уязвимо к физическим повреждениям, краже или сбоям оборудования. Для повышения надежности применяются технологии RAID (Redundant Array of Independent Disks), обеспечивающие избыточность данных.

2. **Облачное хранение**: Хранение данных на удаленных серверах, управляемых провайдерами, такими как Amazon Web Services (AWS), Microsoft Azure или Google Cloud. Облачные системы обеспечивают масштабируемость, автоматическое резервное копирование и доступность через Интернет. Они используют распределенные архитектуры, такие как Hadoop Distributed File System (HDFS), для обработки больших объемов данных. Однако облачное хранение требует строгого соблюдения стандартов безопасности, таких как шифрование на уровне хранения (AES-256) и управления доступом (RBAC).

3. **Распределенное хранение**: Технологии, такие как InterPlanetary File System (IPFS) или блокчейн, позволяют фрагментировать данные и хранить их на множестве узлов, повышая устойчивость к сбоям и атакам. Например, блокчейн используется для хранения неизменяемых записей транзакций, где каждая запись защищена криптографическими методами. Этот подход особенно актуален для децентрализованных систем, таких как криптовалютные платформы.

Безопасность хранения регулируется международными стандартами, такими как NIST SP 800-209 «Security Guidelines

for Storage Infrastructure», который рекомендует многоуровневую защиту: шифрование данных в покое, регулярный аудит доступа и мониторинг угроз. GDPR (статья 32) требует технических и организационных мер для защиты данных, включая уведомление о нарушениях в течение 72 часов. Для обеспечения целостности применяются хэш-функции (например, SHA-256), а для доступности – системы резервного копирования и планы восстановления после сбоев (Disaster Recovery).

Современные тенденции в хранении включают использование квантовых технологий и оптических систем хранения, таких как 5D-оптические диски, способные хранить терабайты данных в течение тысяч лет. Также набирает популярность «холодное» хранение для редко используемых данных, минимизирующее энергопотребление. Однако эти технологии требуют значительных инвестиций и пока ограничены в коммерческом применении.

2.3 Способы передачи цифровой информации

Передача цифровой информации предполагает перемещение данных между системами, устройствами или пользователями через коммуникационные сети. Основные методы включают:

1. **Сетевые протоколы**: Использование стандартизированных протоколов, таких как HTTP/HTTPS для веб-данных, FTP/SFTP для передачи файлов, SMTP для электронной почты и MQTT для IoT-систем. HTTPS, основанный на TLS (Transport Layer Security), обеспечивает шифрование данных в процессе передачи, минимизируя риски перехвата. Для реального времени применяются протоколы WebSockets, обеспечивающие низкую задержку в двустороннем обмене.

2. **Защищенные каналы**: Виртуальные частные сети (VPN) и протоколы TLS/SSL используются для создания безопасных соединений, особенно при передаче конфиденциальных данных. VPN, такие как OpenVPN или WireGuard, шифруют весь сетевой трафик, обеспечивая конфиденциальность в публичных сетях. Для особо чувствительных данных

применяются квантовые криптографические протоколы, такие как BB84, хотя их внедрение пока ограничено.

3. **Децентрализованная передача**: Технологии peer-to-peer (P2P), такие как BitTorrent или блокчейн-сети, позволяют передавать данные без центрального сервера. Это повышает устойчивость к цензуре и сбоям, но требует дополнительных мер для обеспечения конфиденциальности. Например, в блокчейн-сетях данные передаются через консенсусные механизмы, такие как Proof-of-Work или Proof-of-Stake, с верификацией узлами сети.

Передача данных регулируется международными стандартами, такими как ISO/IEC 27001, требующими шифрования и аутентификации. GDPR (статья 44) устанавливает строгие правила трансграничной передачи данных, требуя адекватного уровня защиты в принимающей юрисдикции. Рекомендации Глобальной комиссии по стабильности киберпространства (GCSC) подчеркивают необходимость кибергигиены, включая защиту от вредоносных программ и атак типа «человек посередине» (MITM).

Технические аспекты передачи включают использование сетей пятого поколения (5G) для высокоскоростного обмена, а также разработку протоколов с низкой задержкой, таких как QUIC, заменяющий TCP в некоторых приложениях. Для обеспечения целостности применяются цифровые подписи и сертификаты, выданные доверенными центрами (например, Let's Encrypt). В IoT-системах передача оптимизируется для низкой пропускной способности с использованием протоколов, таких как CoAP.

2.4 Интеграция процессов и вызовы

Создание, хранение и передача цифровой информации тесно связаны и требуют комплексного подхода к управлению данными. Современные системы, такие как системы управления данными (DMS) или платформы больших данных (Big Data), интегрируют эти процессы, обеспечивая автоматизацию и мониторинг. Например, платформы, такие как Apache Kafka,

позволяют одновременно создавать, хранить и передавать данные в реальном времени, что критично для финансовых или медицинских приложений.

Основные вызовы включают:

– **Безопасность**: Уязвимости, такие как SQL-инъекции, DDoS-атаки или утечки данных, требуют постоянного обновления защитных мер. NIST SP 800-53 рекомендует многофакторную аутентификацию и регулярные тесты на проникновение.

– **Объем данных**: Экспоненциальный рост данных, особенно с развитием IoT и ИИ, требует масштабируемых решений хранения и передачи. По данным IDC, глобальный объем данных достиг 175 зеттабайт к 2025 году.

– **Совместимость**: Разнообразие форматов и протоколов затрудняет интеграцию систем. Стандарты, такие как OpenAPI или JSON-LD, помогают решать эту проблему.

– **Энергопотребление**: Облачные дата-центры и блокчейн-сети потребляют значительные ресурсы. Исследования MIT показывают, что блокчейн Биткойна может потреблять до 0,5% мирового электричества.

3. Порядок обнаружения цифровых доказательств

Обнаружение цифровых доказательств является ключевым процессом в цифровой криминалистике, направленным на идентификацию, сбор, приобретение и документирование данных, которые могут быть использованы в расследованиях и судебных разбирательствах. Этот процесс регулируется международными стандартами, такими как ISO/IEC 27037:2012 и ISO/IEC 27043:2015, а также лучшими практиками INTERPOL и NIST, обеспечивающими целостность, аутентичность и допустимость доказательств в суде. Порядок обнаружения включает несколько последовательных этапов: идентификацию, сбор, приобретение, документирование и предварительный анализ. Каждый этап требует строгого

соблюдения процедур для минимизации рисков модификации данных и обеспечения их юридической значимости.

3.1 Идентификация цифровых доказательств

Идентификация цифровых доказательств является первым шагом, целью которого выступает определение потенциальных источников данных, релевантных для расследования. Согласно ISO/IEC 27037:2012, идентификация включает поиск устройств, носителей и систем, содержащих цифровую информацию, такую как компьютеры, смартфоны, USB-накопители, серверы, облачные хранилища или устройства Интернета вещей (IoT). Ключевая задача – оценка волатильности данных, поскольку некоторые данные, например содержимое оперативной памяти (RAM), могут быть утрачены при выключении устройства. Руководства NIST SP 800-86 подчеркивают необходимость приоритизации источников на основе их релевантности и риска утраты данных.

Идентификация начинается с анализа контекста расследования. Например, в случае кибератаки криминалисты определяют, какие системы могли быть скомпрометированы, изучая сетевые журналы, метаданные или пользовательские действия. INTERPOL в Глобальных рекомендациях по цифровой криминалистике (2019) рекомендует первым респондентам фиксировать состояние устройств на месте происшествия, избегая ненужных взаимодействий, которые могут изменить данные. Это включает фотографирование устройств, запись серийных номеров и документирование сетевых подключений. Для облачных систем идентификация усложняется, так как данные могут быть распределены по нескольким юрисдикциям. UNODC в своих лучших практиках (2023) предлагает использовать API провайдеров для доступа к метаданным, сохраняя цепочку хранения (chain of custody).

Ключевым аспектом идентификации является определение типов данных, таких как файлы, логи, метаданные, сетевой трафик или удаленные записи. Например, в расследованиях финансовых преступлений идентифицируются

транзакционные логи, тогда как в делах о кибершпионаже – пакеты данных, захваченные с помощью инструментов, таких как Wireshark. ISO/IEC 27043:2015 подчеркивает необходимость планирования, включая предварительное определение релевантных источников на основе гипотез расследования.

3.2 Сбор цифровых доказательств

Сбор цифровых доказательств предполагает физическое или логическое извлечение данных из идентифицированных источников без их модификации. ISO/IEC 27037:2012 разделяет сбор на два подхода: статический и живой. Статический сбор проводится в контролируемых лабораторных условиях, где устройства изымаются и транспортируются для дальнейшего анализа. Живой сбор применяется, когда устройство активно, а данные волатильны, например, содержимое RAM или активные сетевые соединения. NIST SP 800-86 рекомендует использовать специализированные инструменты, такие как write-blockers, для предотвращения записи на носитель при статическом сборе, что минимизирует риск изменения данных.

Для статического сбора криминалисты создают бит-в-бит копии (forensic images) носителей с помощью инструментов, таких как FTK Imager или dd. Эти копии включают не только активные файлы, но и удаленные данные, которые могут быть восстановлены. Целостность копий верифицируется с помощью хэш-функций (SHA-256 или MD5), сравнивая хэш оригинала и образа. INTERPOL подчеркивает важность документирования процесса сбора, включая описание оборудования, программного обеспечения и условий окружающей среды, таких как температура или влажность, которые могут повлиять на носители.

Живой сбор используется в случаях, когда выключение устройства невозможно или нежелательно, например, в серверных системах или при расследовании атак в реальном времени. Инструменты, такие как Volatility или MemProcFS, позволяют извлечь содержимое памяти, включая запущенные процессы и сетевые соединения. Однако этот метод сопряжен

с риском, так как активная система может быть изменена во время сбора. UNODC рекомендует минимизировать вмешательство, фиксируя только необходимые данные и документируя каждое действие.

Сбор также включает работу с облачными данными, что требует взаимодействия с провайдерами. ISO/IEC 27050-1:2019 для электронного обнаружения (eDiscovery) подчеркивает необходимость юридических соглашений с провайдерами для получения доступа к данным, сохраняя их аутентичность. Например, запросы к AWS или Google Cloud должны сопровождаться судебными ордерами, чтобы обеспечить допустимость доказательств.

3.3 Приобретение и документирование цифровых доказательств

Приобретение цифровых доказательств заключается в создании точных копий данных для последующего анализа, сохраняя их в неизменном виде. Этот процесс тесно связан с цепочкой хранения, требующей строгого документирования всех действий. ISO/IEC 27037:2012 определяет приобретение как процесс копирования данных с использованием методов, исключающих их изменение. Например, использование write-blockers при копировании жестких дисков гарантирует, что оригинальные данные остаются нетронутыми. Для облачных данных применяются инструменты, такие как Magnet AXIOM Cloud, позволяющие извлекать данные из удаленных систем с сохранением метаданных.

Документирование является критическим аспектом, обеспечивающим юридическую допустимость доказательств. NIST SP 800-86 рекомендует фиксировать все детали: время, место, участников, используемые инструменты и методы. Документы включают фотографии устройств, протоколы сбора, хэш-суммы и журналы аудита. INTERPOL в Руководстве для первых респондентов (2023) подчеркивает, что отсутствие документации может привести к оспариванию доказательств в суде, особенно в международных делах. Например, в

расследованиях киберпреступлений, таких как фишинг, документируются IP-адреса, временные метки и цепочка передачи данных.

Для обеспечения целостности применяются криптографические методы. Хэш-функции, такие как SHA-256, используются для создания уникальных идентификаторов данных, которые проверяются на каждом этапе. Если хэш копии отличается от оригинала, доказательства считаются скомпрометированными. Кроме того, цифровые подписи, основанные на алгоритмах RSA или ECDSA, подтверждают аутентичность данных, особенно при передаче между юрисдикциями.

3.4 Предварительный анализ цифровых доказательств

Предварительный анализ проводится для оценки релевантности собранных данных и определения их ценности для расследования. ISO/IEC 27043:2015 выделяет предварительный анализ как часть процесса расследования, где данные классифицируются и приоритизируются. Например, в делах о кибератаках криминалисты анализируют сетевые журналы для выявления точек входа или вредоносного ПО. Инструменты, такие как Autopsy или X-Ways Forensics, позволяют проводить поиск, по ключевым словам, восстанавливать удаленные файлы и анализировать метаданные.

NIST SP 800-86 подчеркивает, что предварительный анализ должен быть минимально инвазивным, чтобы избежать изменения данных. Например, анализ копий, а не оригиналов, предотвращает случайные модификации. UNODC рекомендует использовать автоматизированные инструменты, такие как системы искусственного интеллекта, для обработки больших объемов данных, особенно в расследованиях, связанных с большими данными (Big Data). ИИ может выявлять шаблоны, такие как аномалии в сетевом трафике, ускоряя процесс.

Предварительный анализ также включает определение необходимости специализированных экспертиз, таких как анализ вредоносного ПО или восстановление зашифрованных

данных. ISO/IEC 27037:2012 требует, чтобы аналитики были сертифицированы и использовали аккредитованные лаборатории (ISO/IEC 17025), чтобы гарантировать воспроизводимость результатов. Это особенно важно в международных расследованиях, где стандарты должны быть единообразными.

3.5 Вызовы и лучшие практики

Обнаружение цифровых доказательств сопряжено с рядом вызовов:

– **Волатильность данных**: Данные в RAM или временные сетевые соединения могут быть утрачены, что требует быстрого реагирования. NIST рекомендует приоритизировать живой сбор в таких случаях.

– **Облачные данные**: Доступ к данным, хранящимся в облаке, осложнен юрисдикционными ограничениями. ISO/IEC 27050-1 предлагает использовать международные договоры для упрощения доступа.

– **Шифрование**: Зашифрованные данные требуют специализированных методов, таких как криптоанализ. UNODC подчеркивает необходимость сотрудничества с экспертами по криптографии.

– **Объем данных**: Рост объемов данных (по прогнозам IDC, 175 зеттабайт к 2025 году) требует масштабируемых решений, таких как системы управления большими данными.

Лучшие практики включают:

– Использование стандартизированных инструментов и процедур, таких как FTK, EnCase или Cellebrite для мобильных устройств.

– Регулярное обучение криминалистов для соответствия всем стандартам международного уровня.

– Интеграция ИИ и автоматизации для ускорения анализа больших объемов данных.

– Международное сотрудничество через INTERPOL или UNODC для обмена доказательствами в трансграничных делах.

4. Процессуальный порядок закрепления цифровых доказательств

Процессуальный порядок закрепления цифровых доказательств в Республике Казахстан

В Республике Казахстан (РК) процессуальный порядок закрепления цифровых доказательств регулируется Уголовно-процессуальным кодексом (УПК РК) от 4 июля 2014 года №231-V (с изменениями на 16.07.2025), Гражданским процессуальным кодексом (ГПК РК) от 31 октября 2015 года №377-V (с изменениями на 24.05.2025), а также Административным процедурно-процессуальным кодексом (АППК РК) от 29 июня 2020 года №350-VI. Эти акты, в совокупности с международными стандартами цифровой криминалистики, такими как ISO/IEC 27037:2012, формируют правовую основу для идентификации, сбора, фиксации и представления цифровых доказательств. Закрепление цифровых доказательств в РК направлено на обеспечение их целостности, аутентичности и допустимости в судебных процессах.

Идентификация и сбор цифровых доказательств

Первый этап закрепления цифровых доказательств в РК – идентификация и сбор. Согласно статье 111 УПК РК, доказательствами являются любые данные, устанавливающие обстоятельства дела, включая цифровые данные, такие как электронные документы, логи, аудио- и видеозаписи. Статья 199 УПК РК регулирует осмотр и изъятие электронных носителей информации, таких как жесткие диски, смартфоны или облачные данные. Процесс начинается с определения источников данных, их волатильности и релевантности для дела. Например, содержимое оперативной памяти (RAM) требует немедленного сбора из-за его волатильности, что соответствует рекомендациям ISO/IEC 27037:2012 о приоритизации данных.

Сбор цифровых доказательств проводится с использованием специализированных инструментов, предотвращающих

модификацию данных. Для статического сбора создаются бит-в-бит копии (forensic images) с помощью программ, таких как FTK Imager, с последующей верификацией целостности через хэш-функции (SHA-256 или MD5). Живой сбор, применяемый для активных систем, использует инструменты, такие как Volatility, для фиксации данных памяти. Статья 119 УПК РК требует, чтобы все процессуальные действия, включая осмотр носителей, протоколировались, фиксируя время, место и участников.

Закон РК «Об электронном документе и электронной цифровой подписи» от 7 января 2003 года №370-II (с изменениями на 07.01.2025) определяет, что электронные документы, заверенные ЭЦП, имеют юридическую силу, равную бумажным, что упрощает их закрепление как доказательств (статья 10). Закон «О персональных данных и их защите» от 21 мая 2013 года №94-V требует согласия субъекта на сбор данных, за исключением случаев, предусмотренных УПК РК (статья 7).

Фиксация и документирование

Фиксация цифровых доказательств в РК осуществляется через протоколы процессуальных действий, как указано в статье 119 УПК РК. Протоколы должны содержать описание носителя, программного обеспечения, методов сбора и хэш-суммы для подтверждения целостности. Статья 221 УПК РК регулирует хранение вещественных доказательств, включая цифровые носители, в условиях, исключающих их повреждение или утрату. Например, носители хранятся в защищенных сейфах, а доступ к ним ограничен уполномоченными лицами.

В гражданском процессе, согласно статье 99 ГПК РК, доказательства на материальных носителях информации (например, USB-накопители или жесткие диски) исследуются судом с учетом их аутентичности. Статья 212 ГПК РК предусматривает воспроизведение аудио- и видеозаписей в судебном заседании, с обязательным протоколированием процесса. АППК РК (статья 128) устанавливает аналогичные требования для

административных дел, подчеркивая необходимость документирования всех действий с цифровыми данными.

Для обеспечения допустимости доказательств в РК применяются принципы цепочки хранения (chain of custody), соответствующие ISO/IEC 27037:2012. Это включает фиксацию каждого этапа обращения с доказательствами, от сбора до представления в суд. Например, при изъятии смартфона протокол должен указывать его модель, серийный номер и состояние на момент изъятия. Закон «Об информатизации» от 24 ноября 2015 года № 418-V требует использования сертифицированных систем для обработки данных, что повышает надежность фиксации.

Представление и исследование в суде

Представление цифровых доказательств в суде регулируется статьей 25 УПК РК, требующей оценки доказательств по внутреннему убеждению судьи, основанному на их законности и достоверности. Статья 563 УПК РК определяет допустимость доказательств, полученных за рубежом, при условии соблюдения международных договоров, ратифицированных РК, таких как Минская конвенция СНГ 1993 года. В гражданском процессе статья 16 ГПК РК закрепляет аналогичный принцип оценки доказательств, а статья 420 уточняет, что суд определяет порядок исследования с учетом мнений сторон.

Исследование цифровых доказательств включает их воспроизведение (например, демонстрацию видеозаписей) и экспертизу. Статья 116 УПК РК регулирует проведение компьютерно-технической экспертизы, которая может включать восстановление удаленных данных или анализ сетевых логов. Эксперты должны быть сертифицированы, а лаборатории – аккредитованы по ISO/IEC 17025. В случае облачных данных суд может запросить доступ через провайдера, что требует юридических соглашений, как указано в ISO/IEC 27050-1:2019.

Хранение и уничтожение

Хранение цифровых доказательств в РК осуществляется в защищенных условиях, исключающих несанкционированный доступ. Статья 221 УПК РК требует, чтобы носители хранились в сейфах или специализированных хранилищах, с регулярной проверкой целостности. Закон «О персональных данных и их защите» (статья 12) обязывает локализовать базы данных на территории РК, что влияет на хранение облачных доказательств. После завершения дела доказательства могут быть возвращены владельцу или уничтожены, если они не подлежат хранению (статья 98 ГПК РК).

Процессуальный порядок в странах СНГ

Страны Содружества Независимых Государств (СНГ), включая Россию, Беларусь, Узбекистан, Кыргызстан, Таджикистан, Армению и Молдову, имеют схожие, но различающиеся подходы к закреплению цифровых доказательств, обусловленные национальным законодательством и участием в международных договорах, таких как Минская конвенция СНГ 1993 года и Конвенция Совета Европы о киберпреступности 2001 года. Ниже рассматриваются ключевые аспекты в некоторых странах СНГ, основанные на их законодательстве и практике.

Россия

В Российской Федерации (РФ) процессуальный порядок закрепления цифровых доказательств регулируется Уголовно-процессуальным кодексом РФ (УПК РФ) от 18 декабря 2001 года №174-ФЗ (с изменениями на 01.07.2025). Статья 81 УПК РФ классифицирует цифровые данные как вещественные доказательства, если они хранятся на материальных носителях. Сбор проводится в рамках осмотра (статья 176) или выемки (статья 183), с обязательным протоколированием. Для живого сбора данных из активных систем применяются инструменты, такие как X-Ways Forensics, с фиксацией хэш-сумм.

Фиксация цифровых доказательств осуществляется через протоколы, включающие описание носителя, программного обеспечения и методов сбора. Статья 166 УПК РФ требует, чтобы протоколы содержали все детали, включая хэш-суммы для верификации. Хранение регулируется статьей 82, требующей защиты данных от утраты или модификации. Для облачных данных применяются запросы к провайдерам, что может быть осложнено юрисдикционными ограничениями.

Представление в суде включает воспроизведение данных (статья 271) и экспертизу (статья 195). Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года №149-ФЗ устанавливает требования к защите данных, включая шифрование и локализацию. Россия активно использует международное сотрудничество через INTERPOL и Минскую конвенцию для обмена цифровыми доказательствами.

Узбекистан

В Республике Узбекистан процессуальный порядок закрепления цифровых доказательств был институционализирован Законом №ЗРУ-1003 от 21 ноября 2024 года, внесшим изменения в Уголовно-процессуальный, Гражданский процессуальный и другие кодексы. Закон определяет цифровые доказательства как «электронные данные, содержащие сведения об обстоятельствах, имеющих значение для дела», включая электронные документы, аудио- и видеозаписи, а также данные из Интернета.

Сбор цифровых доказательств регулируется статьей 81 УПК РУз, требующей их представления вместе с носителями, если это возможно. При отсутствии носителя суд уведомляется с указанием причин. Фиксация осуществляется через процессуальные протоколы, включающие аудио- и видеозаписи, сформированные в электронном виде. Копии цифровых доказательств хранятся вместе с материалами дела. Закон

«О нотариате» предусматривает нотариальное заверение цифровых доказательств, что повышает их юридическую силу.

Исследование в суде включает осмотр и оценку данных, с возможностью привлечения экспертов. Закон «О судебной экспертизе» регулирует проведение компьютерно-технической экспертизы, соответствующей ISO/IEC 17025. Хранение и уничтожение цифровых доказательств осуществляются в соответствии с правилами, установленными кодексами, с учетом защиты персональных данных.

Беларусь

В Республике Беларусь порядок закрепления цифровых доказательств регулируется Уголовно-процессуальным кодексом РБ от 16 июля 1999 года №295-З (с изменениями на 01.01.2025). Статья 87 УПК РБ определяет доказательства, включая цифровые данные, как сведения, полученные законным путем. Сбор осуществляется через осмотр (статья 192) и изъятие (статья 198), с использованием инструментов цифровой криминалистики.

Фиксация проводится через протоколы, включающие описание носителей и методов сбора. Хранение регулируется статьей 89, требующей защиты данных от утраты. Закон РБ «Об информации, информатизации и защите информации» от 10 ноября 2008 года №455-З устанавливает требования к шифрованию и локализации данных. Представление в суде включает экспертизу (статья 201), с привлечением аккредитованных лабораторий.

Вызовы и международное сотрудничество в СНГ

Закрепление цифровых доказательств в странах СНГ сталкивается с вызовами, такими как:

– **Юрисдикционные барьеры**: Облачные данные, хранящиеся за рубежом, требуют международного сотрудничества через Минскую конвенцию СНГ или Конвенцию о киберпреступности.

– **Технические ограничения**: Недостаток сертифицированных лабораторий и квалифицированных специалистов в некоторых странах СНГ затрудняет обработку сложных данных.

– **Шифрование**: Зашифрованные данные требуют криптоанализа, что может быть ресурсоемким.

– **Гармонизация стандартов**: Различия в национальных законодательствах усложняют трансграничный обмен доказательствами.

Международное сотрудничество в СНГ осуществляется через Совет министров внутренних дел СНГ и INTERPOL, что упрощает обмен цифровыми доказательствами. Например, Минская конвенция (статья 53) позволяет запрашивать правовую помощь, включая передачу цифровых данных. ISO/IEC 27037:2012 и ISO/IEC 27043:2015 служат основой для унификации процедур в странах СНГ, обеспечивая совместимость.

Заключение

Цифровая криминалистика в Республике Казахстан и странах СНГ демонстрирует значительный прогресс в интеграции информационно-коммуникационных технологий в уголовный процесс, отражая глобальные тенденции цифровизации. Законодательная база, включая УПК РК, Закон «Об информатизации» и Закон «Об электронном документе и электронной цифровой подписи», обеспечивает правовую основу для работы с цифровыми доказательствами, гарантируя их целостность, аутентичность и допустимость. Процессы создания, хранения и передачи цифровой информации регулируются международными стандартами, такими как ISO/IEC 27037:2012 и NIST SP 800-86, с акцентом на использование криптографических методов (SHA-256, ЭЦП) и сертифицированных лабораторий (ISO/IEC 17025).

Обнаружение и закрепление цифровых доказательств в РК и СНГ включает идентификацию, сбор, фиксацию и представление данных, с учетом волатильности и юрисдикционных барьеров, особенно для облачных систем. Внедрение систем, таких как СИОПСО и e-UD, повысило эффективность расследований, сократив время обработки данных и обеспечив прозрачность. Интеграция ИИ и блокчейн-технологий, а также сотрудничество с INTERPOL и UNODC, укрепляют позиции региона в борьбе с киберпреступлениями, число которых в РК выросло на 25% к 2025 году.

Однако вызовы, включая шифрование, объем данных (175 зеттабайт к 2025 году по данным IDC) и недостаток кадров, требуют дальнейшего совершенствования. Гармонизация национальных законодательств СНГ через Минскую конвенцию и Конвенцию о киберпреступности, а также развитие этических стандартов в духе Berkeley Protocol, обеспечат соответствие глобальным требованиям. Будущее цифровой криминалистики в регионе связано с проактивным анализом данных и усилением кибербезопасности, что позволит эффективно противостоять новым вызовам.

Список используемой литературы

1. Белкин Р.С. Криминалистика: проблемы, тенденции, перспективы. Общая и частные теории / Р.С. Белкин. – Москва: Юридическая литература, 1987. – С. 272.

2. Россинская Е.Р. Криминалистика: учебник / Е.Р. Россинская. – 4-е изд., перераб. и доп. – Москва: Норма, 2020. – С. 784.

3. Бахтеев Д.В. Цифровая криминалистика: учебное пособие / Д.В. Бахтеев. – Москва: Юрайт, 2023. – С. 210.

4. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года №231-V ЗРК (с изменениями и дополнениями по состоянию на 16.07.2025). – Алматы: Юрист, 2025. – С. 320.

5. Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года №418-V ЗРК (с изменениями и дополнениями по состоянию на 07.01.2025). – Алматы: Юрист, 2025. – С. 48.

6. Закон Республики Казахстан «Об электронном документе и электронной цифровой подписи» от 7 января 2003 года №370-II ЗРК (с изменениями и дополнениями по состоянию на 07.01.2025). – Алматы: Юрист, 2025. – С. 32.

7. Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года №94-V ЗРК (с изменениями и дополнениями по состоянию на 07.01.2025). – Алматы: Юрист, 2025. – С. 28.

8. Гражданский процессуальный кодекс Республики Казахстан от 31 октября 2015 года №377-V ЗРК (с изменениями и дополнениями по состоянию на 24.05.2025). – Алматы: Юрист, 2025. – С. 256.

9. Административный процедурно-процессуальный кодекс Республики Казахстан от 29 июня 2020 года №350-VI ЗРК (с изменениями и дополнениями по состоянию на 16.07.2025). – Алматы: Юрист, 2025. – С. 200.

10. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 года №174-ФЗ (с изменениями и дополнениями по состоянию на 01.07.2025). – Москва: Проспект, 2025. – С. 304.

11. Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года №149-ФЗ (с изменениями и дополнениями по состоянию на 01.07.2025). – Москва: Проспект, 2025. – С. 40.

12. Закон Республики Узбекистан «О внесении изменений и дополнений в некоторые законодательные акты в связи с совершенствованием порядка работы с цифровыми данными» от 21 ноября 2024 года №ЗРУ-1003. – Ташкент: Адолат, 2024. – С. 24.

13. Закон Республики Беларусь «Об информации, информатизации и защите информации» от 10 ноября 2008 года №455-З (с изменениями и дополнениями по состоянию на 01.01.2025). – Минск: Национальный центр правовой информации, 2025. – С. 36.

14. Минская конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам от 22 января 1993 года // Собрание законодательства СНГ. – 1993. – №1. – С. 12-28.

15. Конвенция Совета Европы о киберпреступности (ETS № 185) от 23 ноября 2001 года // European Treaty Series. – 2001. – No. 185.

16. Berkeley Protocol on Digital Open-Source Investigations / University of California, Berkeley, Human Rights Center. – Berkeley: UC Berkeley, 2020. – 82 p.

17. ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. – Geneva: International Organization for Standardization, 2012. – 38 p.

18. ISO/IEC 27043:2015. Information technology – Security techniques – Incident investigation principles and processes. – Geneva: International Organization for Standardization, 2015. – 42 p.

19. ISO/IEC 27050-1:2019. Information technology – Electronic discovery – Part 1: Overview and concepts. – Geneva: International Organization for Standardization, 2019. – 30 p.

20. NIST Special Publication 800-86. Guide to Integrating Forensic Techniques into Incident Response / K. Kent, S. Chevalier, T. Grance, H. Dang. – Gaithersburg: National Institute of Standards and Technology, 2006. – 121 p.

21. INTERPOL Global Guidelines for Digital Forensics Laboratories. – Lyon: INTERPOL, 2019. – 56 p.

22. UNODC Comprehensive Study on Cybercrime. – Vienna: United Nations Office on Drugs and Crime, 2023. – 124 p.

23. Волеводз А.Г. Цифровые доказательства в уголовном процессе: международный опыт и российская практика / А.Г. Волеводз // Журнал российского права. – 2022. – №3. – С. 45-58.

24. Сырлыбаев М.К. Цифровая криминалистика в Казахстане: современные вызовы и перспективы / М.К. Сырлыбаев // Вестник Алматинской академии МВД РК. – 2024. – №2. – С. 12-20.

25. Коржумбаева Т.М. Правовые основы защиты цифровой информации в Республике Казахстан / Т.М. Коржумбаева // Юридическая наука и практика. – 2023. – №1. – С. 34-42.

26. Аубакирова А.А. Интеграция международных стандартов в криминалистическое исследование цифровых следов / А.А. Аубакирова // Журнал криминалистики и судебной экспертизы. – 2024. – №4. – С. 67-75.

27. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet / E. Casey. – 3rd ed. – London: Academic Press, 2011. – 840 p.

28. Carrier B. File System Forensic Analysis / B. Carrier. – Boston: Addison-Wesley, 2005. – 600 p.

29. Марков А.А. Технические аспекты фиксации цифровых доказательств / А.А. Марков // Криминалистика и судебная экспертиза. – 2023. – №2. – С. 23-31.

30. Журавлев С.Ю. Использование искусственного интеллекта в цифровой криминалистике / С.Ю. Журавлев // Информационная безопасность. – 2024. – №5. – С. 15-22.

31. IDC FutureScape: Worldwide DataSphere 2025 Predictions [Электронный ресурс] // International Data Corporation. – 2024. – URL: https://www.idc.com/getdoc.jsp?containerId=US50610524 (дата обращения: 12.09.2025).

32. Global Commission on the Stability of Cyberspace. Norm Package Singapore / GCSC. – 2018. – 24 p. – URL: https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Norm-Package-Singapore.pdf (дата обращения: 12.09.2025).

СОДЕРЖАНИЕ

Верстка:
Туренова Б.Ю.

Отдел организации научно-исследовательской и редакционно-издательской работы Алматинской академии МВД Республики Казахстан имени М. Есбулатова 050060 Алматы, ул. Утепова, 29

Подписано в печать 30 сентября 2025г.
Формат 60х84 1/16 Бум. тип. №1. Печать на ризографе. Уч.-изд. п.л. 2,3.
Тираж 50 экз.