УДК 343.98:004.056

Бакытбеков Улукбек Бакытбекович, bakytbekov.ub@cert.gov.kg
Верзунов Сергей Николаевич, verzunov@hotmail.com
Институт машиноведения, автоматики и геомеханики НАН КР

ЦИФРОВАЯ КРИМИНАЛИСТИКА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ: ТЕОРИЯ, МИРОВАЯ ПРАКТИКА И ОПЫТ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

В статье анализируются научные подходы к понятию «цифровая криминалистика», раскрывается ее содержание и значение в системе криминалистического обеспечения расследований в развитых странах мира и в Кыргызской Республике. Обоснована позиция, согласно которой цифровая криминалистика не является самостоятельной наукой, а представляет собой направление развития традиционной криминалистики в условиях цифровизации.

Активная цифровизация государственных и общественных процессов в Кыргызской Республике оказывает существенное влияние на развитие криминалистической науки и практики расследования преступлений. В условиях широкого внедрения информационно-коммуникационных технологий трансформируются способы совершения преступлений, формы фиксации следов преступной деятельности и методы их криминалистического исследования.

Показано, что цифровые следы и цифровые доказательства приобретают особую значимость при расследовании преступлений, в том числе киберпреступлений, и требуют адаптации криминалистических методов с учетом норм уголовного и уголовно-процессуального законодательства Кыргызской Республики.

Ключевые слова: цифровая криминалистика, цифровизация, цифровые доказательства, кибербезопасность.

Введение

Цифровая криминалистика основывается на фундаментальных принципах криминалистической науки, в частности на принципе обмена, сформулированном Э. Локаром, согласно которому при любом взаимодействии объектов происходит взаимный перенос следов [1]. В условиях цифровой среды данный принцип проявляется в том, что использование информационно-коммуникационных технологий неизбежно сопровождается формированием цифровых следов, отражающих действия пользователя в информационном пространстве [2; 5].

В контексте цифровой криминалистики под цифровыми следами понимаются данные, формируемые в процессе использования цифровых устройств, информационных систем и сетевых сервисов [3; 5; 6]. Совокупность таких данных образует цифровой отпечаток пользователя и включает как сведения, возникающие в результате его действий в цифровой среде, так и информацию, автоматически фиксируемую программными и техническими средствами при функционировании цифровых технологий [5; 6].

Данные, составляющие активные и пассивные цифровые отпечатки, обладают высоким криминалистическим потенциалом и могут рассматриваться как источники сведений, которые при соблюдении требований уголовно-процессуального законодательства Кыргызской Республики и установленного порядка их получения, фиксации и приобщения могут быть использованы в качестве цифровых доказательств [2; 3; 11] при расследовании преступлений, в том числе киберпреступлений.

Цифровые данные могут храниться на различных носителях и в различных средах, включая персональные компьютеры, мобильные устройства, планшеты, периферийные и «умные» устройства, внешние накопители, сетевое оборудование, серверы и облачные хранилища [4; 7; 8]. Извлекаемая информация включает как данные, относящиеся к содержанию (тексты сообщений, изображения, аудио- и видеозаписи), так и метаданные, характеризующие параметры создания, передачи и использования информации, включая сведения о времени, месте и способе совершения цифровых операций.

Особую значимость для цифровой криминалистики приобретают данные, формируемые современными многофункциональными цифровыми устройствами,

совмещающими вычислительные, коммуникационные и сервисные функции. К таким устройствам относятся игровые консоли, интеллектуальные помощники и элементы экосистем «умного дома», которые накапливают значительный объем информации о действиях пользователей. Анализ возможностей использования данных, формируемых многофункциональными цифровыми устройствами, показывает их значительный криминалистический потенциал и возрастающую роль цифровых следов в системе криминалистического обеспечения расследований в условиях цифровизации.

Таким образом, цифровая криминалистика в условиях цифровизации выступает инструментом адаптации классических криминалистических принципов к новым технологическим реалиям, обеспечивая выявление, анализ и использование цифровых следов как значимого доказательственного ресурса.

Мировая практика становления цифровой криминалистики

Формирование цифровой криминалистики как направления криминалистической деятельности началось в конце XX века в условиях широкого распространения вычислительной техники и сетевых технологий. Первые системные разработки в данной сфере были осуществлены в Соединенных Штатах Америки, где в конце 1980-х – начале 1990-х годов правоохранительные органы столкнулись с необходимостью расследования преступлений [3; 7], связанных с несанкционированным доступом к компьютерным системам, распространением вредоносного программного обеспечения и злоупотреблением электронными данными.

В США цифровая криминалистика получила развитие в деятельности ФБР, Секретной службы США и специализированных лабораторий компьютерной криминалистики. Существенный вклад был внесен в разработку методик изъятия и исследования цифровых доказательств, а также в формирование стандартов допустимости таких доказательств в суде.

В дальнейшем цифровая криминалистика получила развитие в Великобритании, Германии, Нидерландах, Франции, Канаде, Австралии и Японии, где она была интегрирована в систему судебной экспертизы и криминалистического обеспечения расследований. В указанных странах цифровая криминалистика рассматривается не как отдельная наука, а как междисциплинарное направление, объединяющее криминалистику, информационные технологии и право.

В научной и методической литературе внедрение цифровой криминалистики в деятельность правоохранительных органов развитых государств рассматривается как фактор, способствующий расширению круга доказательственных источников за счет цифровых следов, повышению эффективности расследования киберпреступлений и экономических преступлений, формированию единых стандартов работы с цифровыми доказательствами и развитию специализированной подготовки экспертов и следователей.

В ряде государств цифровая криминалистика стала составной частью национальных стратегий обеспечения информационной и кибербезопасности, а также защиты критической информационной инфраструктуры [8; 11].

Цифровая криминалистика в странах Центральной Азии

Развитие цифровой криминалистики в странах Центральной Азии носит неравномерный характер и во многом зависит от уровня цифровизации государственных процессов и состояния национальных систем кибербезопасности.

Наиболее системный подход наблюдается в **Республике Казахстан** [9; 10], где: созданы специализированные подразделения по расследованию киберпреступлений; развивается судебная цифровая экспертиза; цифровая криминалистика интегрирована в национальные программы кибербезопасности; ведется подготовка специалистов и научные исследования.

В других странах региона цифровая криминалистика находится на стадии формирования и преимущественно реализуется в прикладной деятельности правоохранительных органов без достаточной теоретической проработки.

Состояние цифровой криминалистики в Кыргызской Республике

В Кыргызской Республике цифровая криминалистика находится на этапе становления. Практическое использование цифровых методов осуществляется в рамках расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий, однако системный характер данная деятельность пока не приобрела. Это проявляется в недостаточной унификации ведомственных регламентов (стандартных операционных процедур) по обнаружению, изъятию, копированию и верификации цифровых носителей и данных, а также в ограниченной унификации подходов к назначению и проведению судебных компьютерно-технических исследований.

Развитие цифровой криминалистики в Кыргызской Республике обусловлено: активной цифровизацией государственного управления; ростом числа киберпреступлений; внедрением информационных систем в деятельность правоохранительных органов; формированием национальной системы кибербезопасности, что позволяет характеризовать ее текущее состояние как преимущественно прикладное направление криминалистической деятельности.

В научном аспекте цифровая криминалистика в Кыргызской Республике не сформировалась как самостоятельная отрасль криминалистической науки. Вместе с тем отдельные вопросы цифровых доказательств, электронных следов и применения информационных технологий в расследовании преступлений рассматриваются в трудах кыргызских ученых в рамках общей криминалистики, уголовного процесса и информационного права.

Таким образом, можно сделать вывод, что цифровая криминалистика в Кыргызской Республике развивается как направление адаптации классических криминалистических положений к условиям цифровизации, а не как обособленная научная дисциплина.

Понятие и содержание цифровой криминалистики

Цифровая криминалистика представляет собой направление криминалистической деятельности, ориентированное на выявление, фиксацию, сохранение, исследование и интерпретацию цифровых следов преступной деятельности. В рамках цифровой криминалистики осуществляется работа с цифровыми устройствами, информационными системами и сетевой инфраструктурой с целью установления фактических обстоятельств совершенного деяния.

Основными задачами цифровой криминалистики являются: установление характера и механизма произошедшего события; определение временных параметров цифровой активности; выявление возможных субъектов противоправных действий; получение и анализ цифровых доказательств, подтверждающих или опровергающих обстоятельства уголовного дела.

Одним из базовых методических требований, применяемых в рамках цифровой криминалистики, является обеспечение неизменности исходных данных, что предполагает применение специальных технических и процессуальных методов, направленных на сохранение целостности цифровой информации при ее изъятии и исследовании.

Выделение в рамках цифровой криминалистики отдельных направлений, таких как компьютерная, мобильная, сетевая и облачная криминалистика, а также криминалистика Интернета вещей и иных цифровых сред, следует рассматривать как условное разграничение по преобладающему объекту исследования и технической среде формирования цифровых следов, имеющее прикладное и методическое значение. Подобная дифференциация обусловлена спецификой исследуемых объектов и особенностями технологической среды, однако сама по себе она не свидетельствует о формировании цифровой криминалистики в качестве самостоятельной отрасли криминалистической науки. Все указанные направления опираются на единые теоретические основы, принципы и методологические подходы, выработанные в рамках традиционной криминалистики, и развиваются в логике их адаптации к новым условиям.

В этом контексте цифровая криминалистика не образует обособленного предмета научного познания, а представляет собой совокупность криминалистических средств, методов и приемов, модифицированных с учетом особенностей цифровых следов и цифровой информации, возникающих в условиях цифровизации общественных и правовых отношений.

Компьютерная криминалистика направлена на исследование стационарных и портативных вычислительных систем, серверов, файловых систем, операционных сред и прикладного программного обеспечения. В рамках данного направления осуществляется восстановление удаленных данных, анализ системных журналов, исследование временных меток, выявление следов несанкционированного доступа и вредоносного программного обеспечения, а также реконструкция действий пользователя.

Мобильная криминалистика охватывает исследование смартфонов, планшетов, мобильных телефонов, SIM-карт, карт памяти и мобильных приложений. Особое значение в данном направлении имеет анализ пользовательской активности, извлечение данных коммуникаций, восстановление удаленной информации, а также исследование геолокационных данных и цифровых следов, формируемых мобильными экосистемами.

Сетевая криминалистика ориентирована на выявление и анализ цифровых следов, формируемых в процессе сетевого взаимодействия. Объектами исследования выступают сетевые журналы, трафик передачи данных, протоколы сетевого взаимодействия, маршрутизаторы, межсетевые экраны и иные элементы сетевой инфраструктуры. Данное направление играет ключевую роль при расследовании кибератак, несанкционированного доступа и инцидентов информационной безопасности.

Криминалистика облачных технологий связана с исследованием данных, размещенных в облачных сервисах и распределенных вычислительных средах. Специфика данного направления обусловлена трансграничным характером хранения информации, ограниченным физическим доступом к носителям и зависимостью от провайдеров услуг. В рамках облачной криминалистики анализируются журналы доступа, данные виртуальных машин, резервные копии и сервисные метаданные.

Криминалистика Интернета вещей ориентирована на исследование цифровых следов, формируемых «умными» устройствами, включая элементы систем «умного дома», носимые устройства, интеллектуальные датчики и бытовую электронику. Указанные устройства аккумулируют сведения о поведении пользователей, параметрах окружающей среды и временных характеристиках событий, что придает им значительную криминалистическую ценность.

Криминалистика мультимедийных данных - данное направление связано с исследованием цифровых изображений, аудио- и видеозаписей. Основными задачами являются установление подлинности мультимедийных файлов, выявление признаков монтажа или подделки, анализ технических параметров записи и условий ее создания. Мультимедийная криминалистика имеет важное значение при расследовании преступлений, сопровождающихся фиксацией событий средствами цифровой записи.

Криминалистика вредоносного программного обеспечения ориентирована на анализ программных средств, используемых для совершения киберпреступлений. В рамках данного направления исследуются механизмы функционирования вредоносных программ, способы их распространения, методы сокрытия активности и связи с инфраструктурой управления.

Криминалистика цифровых финансов и крипто активов - Данное направление связано с анализом цифровых финансовых операций, включая использование электронных платежных систем, криптовалют и распределенных реестров. Исследование транзакций, цифровых кошельков и блокчейн-структур позволяет устанавливать финансовые связи, источники средств и маршруты их перемещения, что приобретает особую актуальность в условиях роста экономических и киберпреступлений.

Понятие цифровой информации, цифровых устройств и цифровых доказательств

Цифровая информация представляет собой сведения, зафиксированные посредством двоичного кодирования и функционирующие в цифровом пространстве в результате как осознанных действий человека, так и автоматизированных процессов. К цифровой информации относятся текстовые данные, электронные сообщения, изображения, аудио- и видеоматериалы, иные файлы, а также метаданные, характеризующие условия их создания, передачи и использования.

Под цифровыми устройствами понимаются компьютеры, ноутбуки, планшеты, серверы, мобильные телефоны, смартфоны и иные технические средства, предназначенные для генерации, обработки, хранения, передачи и получения цифровой информации.

В рамках настоящего исследования под цифровыми доказательствами понимается доказательственная информация в цифровой форме, полученная, зафиксированная и исследованная с соблюдением требований уголовно-процессуального законодательства и используемая для установления обстоятельств, подлежащих доказыванию по уголовному делу. В уголовном судопроизводстве Кыргызской Республики цифровые доказательства подлежат получению и оценке в порядке, установленном УПК Кыргызской Республики [12].

Выводы

Проведенный анализ позволяет сделать вывод о том, что цифровая криминалистика в современных условиях представляет собой объективно сформировавшееся направление развития традиционной криминалистики, обусловленное процессами цифровизации общественных отношений и внедрением информационно-коммуникационных технологий во все сферы жизнедеятельности. Использование цифровых устройств и сетевых сервисов при совершении преступлений приводит к формированию специфических цифровых следов, обладающих высоким доказательственным потенциалом и требующих особых методов выявления, фиксации, сохранения и исследования.

Мировая практика свидетельствует о том, что наиболее эффективные модели цифровой криминалистики реализованы в государствах с развитой системой кибербезопасности и судебной экспертизы, где цифровые доказательства интегрированы в уголовный процесс на основе единых стандартов и методик. В этих странах цифровая криминалистика рассматривается как междисциплинарное направление, объединяющее криминалистику, информационные технологии и право, что обеспечивает высокий уровень раскрываемости киберпреступлений и экономических преступлений.

Анализ состояния цифровой криминалистики в странах Центральной Азии показывает ее неравномерное развитие. Наиболее системный и институционально оформленный подход реализуется в Республике Казахстан, в то время как в других государствах региона цифровая криминалистика преимущественно носит прикладной характер и не получила достаточной теоретической проработки.

В Кыргызской Республике цифровая криминалистика находится на этапе становления и развивается преимущественно как направление практической деятельности правоохранительных органов. При этом отсутствует ее оформленность в качестве самостоятельного научного направления, а соответствующие исследования ведутся фрагментарно в рамках общей криминалистики, уголовного процесса и информационного права. В условиях реализации государственных программ цифровизации и формирования национальной системы кибербезопасности возрастает потребность в научном осмыслении цифровой криминалистики, разработке методических рекомендаций и подготовке профильных специалистов.

Таким образом, цифровая криминалистика в Кыргызской Республике должна рассматриваться как перспективное направление развития криминалистической науки, направленное на адаптацию классических криминалистических положений к цифровой среде и повышение эффективности расследования преступлений в условиях цифровизации.

Список литературы

1. Локар Э. Руководство по криминалистике : пер. с фр. М. : Юридическая литература, 2001. 512 с.
2. Белкин Р. С. Курс криминалистики : в 3 т. М. : Норма, 2001. Т. 1. 720 с.
3. Casey E. Digital Evidence and Computer Crime. 3rd ed. London : Academic Press, 2011. 840 p. URL: https://www.sciencedirect.com/book/9780123742681/digital-evidence-and-computer-crime (дата обращения: 13.01.2026).
4. Carrier B. File System Forensic Analysis. — Boston : Addison-Wesley, 2005. 768 p. URL: https://www.sciencedirect.com/book/9780321268174/file-system-forensic-analysis (дата обращения: 13.01.2026).
5. Kerr O. S. Digital Evidence and the New Criminal Procedure // Columbia Law Review. 2005. Vol. 105, no. 1. P. 279–318. URL: https://columbialawreview.org/content/digital-evidence-and-the-new-criminal-procedure/ (дата обращения: 13.01.2026).
6. Albert J., Venter H. Digital Forensics: An Introduction // Computer Fraud & Security.2017.No. 3.P. 19–26.URL: https://www.sciencedirect.com/science/article/pii/S1361372317300210 (дата обращения: 13.01.2026).
7. Digital Evidence in the Courtroom : report / National Institute of Justice (NIJ). Washington, DC, 2019. URL: https://nij.ojp.gov/topics/articles/digital-evidence-courtroom (дата обращения: 13.01.2026).
8. Digital Forensics in Cybercrime Investigations : report / European Union Agency for Cybersecurity (ENISA). Athens, 2020. URL: https://www.enisa.europa.eu/topics/cybercrime-and-digital-forensics (дата обращения: 13.01.2026).
9. Концепция «Киберщит Казахстана». Астана, 2017. URL: https://www.gov.kz/memleket/entities/ksis/documents/details/2864 (дата обращения: 13.01.2026).
10. Мадалиев А. К. Цифровая криминалистика в странах Центральной Азии // Вестник КазНУ. Серия юридическая. — 2021. № 4. С. 58–65. URL: https://bulletin-law.kaznu.kz/index.php/journal/article/view/1021 (дата обращения: 13.01.2026).
11. Global Cybercrime Strategy : report / Interpol. — Lyon, 2022. — URL: https://www.interpol.int/en/Crimes/Cybercrime/Global-cybercrime-strategy (дата обращения: 13.01.2026).
12. Уголовно-процессуальный кодекс Кыргызской Республики : принят Жогорку Кенешем Кыргызской Республики 30 июня 2017 г. — URL: http://cbd.minjust.gov.kg/act/view/ru-ru/111530 (дата обращения: 13.01.2026).