



ҚЫЛМЫСТЫҚ ПРОЦЕСС, КРИМИНАЛИСТИКА, СОТ-САРАПТАМА ҚЫЗМЕТІ / УГОЛОВНЫЙ ПРОЦЕСС, КРИМИНАЛИСТИКА, СУДЕБНО-ЭКСПЕРТНАЯ ДЕЯТЕЛЬНОСТЬ / CRIMINAL PROCEDURE, CRIMINALISTICS, FORENSIC EXPERTISE

**УДК 343.14
МРНТИ 10.79.35**

А.С. Алишев, Б.Б. Сарсенбаева

*Алматынская академия Министерства внутренних дел Республики Казахстан имени М. Есбулатова,
г. Алматы, Республика Казахстан*

ЦИФРОВЫЕ ДОКАЗАТЕЛЬСТВА И ХЭШ-СУММЫ КАК ИНСТРУМЕНТ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННОМУ ЭКСТРЕМИЗМУ: СРАВНИТЕЛЬНО- ПРАВОВОЙ АНАЛИЗ

Аннотация. Статья посвящена анализу цифровых доказательств и хэш-сумм как эффективных инструментов противодействия информационному экстремизму. Рассматривается правовая неопределенность понятия цифровых доказательств в законодательстве Республики Казахстан и отсутствие единых процедур их фиксации, верификации и хранения. В статье подчеркивается необходимость нормативного закрепления хэш-функций как средства подтверждения неизменности цифровых следов, а также обязательного участия специалистов в области информационных технологий при работе с такими доказательствами. Сравнительно-правовой анализ зарубежной практики показывает наличие устойчивых механизмов цифровой криминалистики, обеспечивающих допустимость и достоверность цифровых улик в суде. В данной работе аргументируется важность изменения Уголовно-процессуального кодекса Республики Казахстан, а также внесения поправок в Закон «Об информатизации» с целью нормативного закрепления статуса цифровых доказательств и их гармонизации с международными стандартами. В статье подчеркивается, что реализация предложенных мер будет способствовать повышению эффективности борьбы с цифровыми проявлениями экстремизма, а также созданию устойчивой правовой базы в быстро трансформирующемся киберпространстве.

Ключевые слова: цифровые доказательства; хэш-функция; информационный экстремизм; кибербезопасность; уголовный процесс; цифровая криминалистика; допустимость доказательств; международный стандарт.

А.С. Алишев, Б.Б. Сарсенбаева

*Қазақстан Республикасы Ішкі істер министрлігінің М. Есболатов атындағы Алматы академиясы,
Алматы қ., Қазақстан Республикасы*

АҚПАРАТТЫҚ ЭКСТРЕМИЗМГЕ ҚАРСЫ ІС-ҚИМЫЛ ҚҰРАЛЫ РЕТІНДЕГІ ЦИФРЛЫҚ ДӘЛЕЛДЕМЕЛЕР МЕН ХЭШ-СОМАЛАР: САЛЫСТЫРМАЛЫ-ҚҰҚЫҚТЫҚ ТАЛДАУ

Аннотация. Мақалада цифрлық дәлелдемелер мен хэш-суммалар ақпараттық экстремизмге қарсы іс-қимылдың тиімді құралы ретінде қарастырылады. Қазақстан Республикасының заңнамасында цифрлық дәлелдемелер ұғымының құқықтық айқын еместігі мен оларды тіркеу, тексеру және сақтау рәсімдерінің біріздендірілмеуі мәселелері зерттеледі. Хэш-функцияларды цифрлық іздердің өзгермейтіндігін растау құралы ретінде және ақпараттық технологиялар саласындағы мамандардың қатысуын міндетті түрде нормативтік бекіту қажеттілігі атап өтіледі. Шет мемлекеттердің тәжірибесіне салыстырмалы-құқықтық талдау жүргізіліп, цифрлық криминалистиканың дәлелдемелердің жарамдылығы мен шынайылығын қамтамасыз ететін тұрақты тетіктері көрсетіледі. Мақалада ҚР Қылмыстық-процестік кодексіне өзгерістер енгізу, сондай-ақ «Ақпараттандыру туралы» Заңына цифрлық дәлелдемелердің құқықтық мәртебесін нормативтік тұрғыда бекіту және оларды халықаралық стандарттарға сәйкестендіру мақсатында түзетулер енгізудің маңыздылығы негізделеді. Мақалада ұсынылған шараларды іске асыру цифрлық экстремизм көріністеріне қарсы іс-қимылдың тиімділігін арттыруға, сондай-ақ жедел өзгеріп жатқан киберкеңістікте



тұрақты құқықтық негіз қалыптастыруға ықпал ететіні атап өтіледі.

Түйінді сөздер: цифрлық дәлелдемелер; хэш-функция; ақпараттық экстремизм; киберқауіпсіздік; қылмыстық процесс; цифрлық криминалистика; дәлелдемелердің жарамдылығы; халықаралық стандарт.

A.S. Alishev, B.B. Sarsenbayeva

The Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Esbulatov, Almaty, the Republic of Kazakhstan

DIGITAL EVIDENCE AND HASH SUMS AS A TOOL TO COUNTER INFORMATION EXTREMISM: A COMPARATIVE LEGAL ANALYSIS

Abstract. This article explores the role of digital evidence and hash functions as essential instruments in combating informational extremism. It discusses the existing gaps and ambiguities in the legal definition of digital evidence within Kazakhstan's legislative framework, as well as the absence of standardized protocols for their documentation, authentication, and preservation. The study emphasizes the urgent need to legally codify hash functions as a means to guarantee the integrity of digital traces and to mandate the involvement of IT professionals in the processing of such evidence. Through a comparative legal review of international practices, the article illustrates the presence of robust digital forensic systems that uphold the admissibility and credibility of electronic evidence in judicial proceedings abroad. The research substantiates the necessity for amendments to the Criminal Procedure Code and the Law "On Informatization" of the Republic of Kazakhstan, aiming to grant digital evidence formal legal status and ensure its harmonization with global norms. Ultimately, the article contends that implementing these reforms will significantly strengthen efforts to counter digital forms of extremism and help establish a resilient legal environment in the context of rapidly evolving cyberspace.

Keywords: digital evidence; hash function; information extremism; cybersecurity; criminal procedure; digital forensics; admissibility of evidence; international standard.

DOI: 10.52425/25187252_2025_37_155

Введение. Сегодня цифровизация оказывает все более сильное воздействие на жизнь общества. Это относится и к деятельности правоохранительных структур и судебной системы. Учитывая увеличение опасности распространения информационного экстремизма в онлайн-форме, актуальным является применение как цифровых данных, отражающих деяния, так и цифровых доказательств, позволяющих выявлять, документировать и преследовать подобные действия. Однако новые формы доказательств требуют не только технической составляющей, но и четкого законодательного регулирования, особенно в части их сбора, хранения и подлинности.

Одним из условий допустимости цифровых доказательств является обеспечение их целостности. Для этого международная практика использует криптографические методы, в частности хэш-функции, подтверждающие целостность с момента изъятия. В ряде стран, включая США и Канаду, уже разрабо-

тано законодательство, предусматривающее признание цифровых доказательств с соблюдением технологических стандартов. В Республике Казахстан (далее – РК) данная сфера остается нормативно неурегулированной, что препятствует эффективному использованию цифровых следов при расследовании преступлений, в т.ч. экстремистской направленности.

Материалы и методы. В исследовании использован комплекс общенаучных и специальных юридических методов. Использование диалектического метода дало возможность исследовать цифровые доказательства и хэш-функции в качестве формирующегося правового феномена в процессе цифровизации. Метод формально-правового анализа был применен для изучения нормативных документов РК и других стран. С помощью сравнительно-правового метода удалось определить общие и отличительные черты национальных систем регулирования цифровых доказательств



в аспекте борьбы с информационным экстремизмом. Применение системного подхода позволило всесторонне рассмотреть проблему на пересечении уголовного, информационного и международного права. В качестве эмпирической базы использованы законы, судебные решения, международные нормативные акты и научные публикации, посвященные рассматриваемой теме.

Результаты, обсуждение. Современный этап цифровизации общественных процессов превращает информационное пространство не только в площадку для коммуникации и обмена информацией, но и в сферу распространения различных деструктивных, включая экстремистские, идей. Противодействие информационному экстремизму предполагает не только применение идеологических и технических подходов, но и внедрение действенных правовых механизмов, в числе которых особое значение приобретают цифровые доказательства. Значимость таких доказательств существенно увеличивается в судебной практике, когда необходимо официально зафиксировать факты совершения противоправных действий с применением средств информационно-коммуникационных технологий [1]. Внедрение строгих цифровых процедур для фиксации, проверки целостности и анализа данных с обязательным документированием их сохранности является ключевым фактором совершенствования криминалистического обеспечения. Это способствует ускорению работы правоохранительных органов, повышению качества обработки цифровых следов, укреплению юридической значимости цифровых доказательств в судебных процессах и сокращению времени, необходимого для раскрытия уголовных правонарушений [2].

Современные электронные доказательства формируются комплексом взаимосвязанных устройств – от систем умного дома и мобильных устройств до облачных платформ – и стремительно распространяются в цифровых экосистемах. Учитывая возрастающие объем, разнообразие и скорость данных, это требует проведения тщательного криминали-

стического анализа [3]. На этом фоне особое внимание заслуживает зарубежный опыт по фиксации и квалификации проявлений информационного экстремизма в киберпространстве.

Так, Б. Клиффорд фиксирует смещение экстремистского контента на «периферийные» хостинги и файлообменные сервисы, где традиционные механизмы модерации слабее. Автор рекомендует расширенные методики ОСИНТ-фиксации (захват HTML/JSON, серверного времени, заголовков HTTP, хэш-сверок) и раннее preservation-уведомление провайдеров для последующей процессуальной пригодности [4].

К. Клоники указывает, что частные платформы превратились в «новых регуляторов» речи: внутренние правила модерации и приоритеты удаления формируют саму судьбу цифровых следов (сохранение, блокировка, деиндексация). Это обстоятельство должно учитываться при квалификации проявлений информационного экстремизма и при оценке надежности фиксации [5].

В исследовании И. Авана подробно рассматриваются способы использования социальных медиа (Facebook, YouTube) террористическими группировками, в частности ИГИЛ, для вербовки, пропаганды и радикализации молодежи. Автор подчеркивает, что онлайн-платформы становятся не просто средой распространения экстремистских идей, но и инструментом киберджихада, направленного на психологическое влияние и вербовку уязвимых групп. При этом в работе описаны конкретные цифровые следы: видео, посты, ретвиты, комментарии, хэштеги, а также специализированные приложения, созданные террористическими структурами. Эти элементы могут быть интерпретированы как цифровые доказательства при наличии нормативной базы, позволяющей их идентификацию, фиксацию и последующую проверку достоверности [6].

Представляется, что описанные в исследовании цифровые следы могут приобретать статус доказательств в правовой плоскости, что требует отдельного



рассмотрения особенностей цифровых данных как объекта судебного анализа. В судебном процессе доказательства имеют решающее значение, поскольку они определяют, виновен ли подозреваемый в совершении преступления. Цифровые доказательства представляют собой любую накопленную, сохраненную или переданную в цифровом формате информацию, необходимую для подтверждения или опровержения факта, являющегося предметом судебных разбирательств. Цифровые данные не имеют материального аналога, их легче подделать или изменить, чем традиционные формы доказательств¹.

Судебная система сталкивается с различными проблемами из-за необходимости разработки правил обращения с цифровыми данными, которые обеспечивают надежность доказательств. Нарушение стандартных процедур может привести к тому, что целостность данных будет оспариваться в суде. Для признания цифровых доказательств допустимыми в судебном процессе необходимо, чтобы все процедуры их получения, фиксации и анализа проводились строго в соответствии с требованиями действующего законодательства и устоявшейся практикой правоохранительных и судебных органов². На сегодняшний день нормы Уголовно-процессуального кодекса РК (далее – УПК РК) недостаточно конкретизированы в части правового положения и специфики идентификации цифровых доказательств. Несмотря на то, что цифровые носители могут рассматриваться как разновидность вещественных доказательств, специфика их извлечения, обработки и последующего использования требует отдельного подхода со стороны органов уголовного преследования и суда. Для полноценного внедрения цифровых доказательств в уголовный процесс требуется не только разработка специализированных криминалистических методик, но и использование нормативных и технических средств, обеспечивающих их

достоверность.

Развитие цифровых технологий привело к созданию эффективных механизмов, обеспечивающих сохранность и неизменность цифровых данных. Среди таких мер – резервное копирование, дублирование данных, а также использование современных криптографических алгоритмов для вычисления контрольных сумм. Применение хэш-функций позволяет достоверно подтверждать подлинность и неизменность цифровых объектов, что существенно усиливает доверие к электронным доказательствам. Особое значение приобретает хранение цифровых доказательств как в месте изъятия, так и на защищенных ведомственных ресурсах правоохранительных органов.

Одним из самых надежных методов обеспечения неизменности цифровых данных является использование хэш-функций – криптографических алгоритмов, которые преобразуют любые данные в уникальную строку установленной длины, называемую хэш-суммой или дайджестом. К основным свойствам хэш-функций относят их детерминированность (идентичный результат при одном и том же входе), односторонность (невозможность восстановления исходных данных по хэшу), стойкость к коллизиям (маловероятность совпадения хэшей у разных данных) и высокую чувствительность к малейшим изменениям исходной информации. Совокупность этих характеристик позволяет рассматривать хэш-функции как основной инструмент верификации подлинности цифровых доказательств в уголовном процессе [7].

На практике, при рассмотрении уголовных дел, хэш-суммы используются для верификации цифровых документов – сравниваются значения оригинала и копии, и совпадение этих значений свидетельствует о сохранении целостности информации. Криминалистическое значение хэширования заключается в получении идентифицирующего признака цифрового объекта, фиксирующего его уни-

¹ Всестороннее исследование проблемы киберпреступности // Управление ООН по наркотикам и преступности. – 2013 [Электронный ресурс] – Режим доступа: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf (дата обращения: 17.02.2025).

² Цифровые доказательства // Управление ООН по наркотикам и преступности [Электронный ресурс] – Режим доступа: <https://synthetichdrugs.unodc.org/synthetichdrugs/ru/cybercrime/detectandrespond/investigation/digitalevidence.html> (дата обращения: 17.02.2025).



кальное состояние в момент изъятия [8]. В криминалистике хэш-функции выполняют роль своеобразного цифрового «отпечатка», позволяя отслеживать любые, даже незначительные изменения.

Наиболее распространенными алгоритмами хэширования, применяемыми в юридической и технической практике, являются:

- *MD5* – в прошлом широко применялся для проверки целостности файлов и хэширования паролей, однако в современных условиях его использование признано небезопасным из-за выявленных уязвимостей и вероятности возникновения коллизий. Применялся для верификации программного обеспечения и хранения паролей в устаревших системах [9];

- *SHA-256* – современный алгоритм семейства SHA-2, обладающий высоким уровнем криптографической стойкости. Применяется для создания цифровых подписей, проверки аутентичности документов, а также в блокчейн-системах, включая Bitcoin, где отвечает за хэширование транзакций и защиту целостности блоков;

- *SHA-512* – обеспечивает еще более высокий уровень безопасности и востребован в сферах, требующих усиленной защиты данных, таких как хранение паролей, электронная почта, а также специализированные блокчейн-платформы (например, BitShares) [10].

Проблемные аспекты и ограничения использования цифровых доказательств состоят в следующем.

Во-первых, криптографическое обеспечение целостности. Применение устаревших хэш-алгоритмов MD5 и SHA-1, уязвимых к коллизиям, не гарантирует требуемого уровня достоверности и неизменности данных. Для подтверждения целостности доказательственной копии следует использовать не ниже семейства SHA-2 (SHA-256/512) либо эквивалентные по стойкости алгоритмы с обязательной фиксацией хэш-значений в процессуальных документах и журналировании операций.

Во-вторых, валидность и воспроизво-

димость результатов. Допустимость и доказательственная сила цифровых данных обусловлены использованием валидированных программно-аппаратных средств. Необходимо документировать наименование, версии и настройки примененных инструментов, порядок их запуска, условия среды, а также обеспечивать возможность независимой проверки (повторяемости) результатов и их сверки сторонним экспертом/организацией. Все действия по извлечению, копированию и анализу должны протоколироваться с соблюдением «цепочки сохранности» носителей и образцов.

В-третьих, аутентификация медиаматериалов в условиях распространения синтетических медиа (deepfake). Для аудио-, видео- и фотодоказательств требуется комплексная проверка подлинности, включающая техническую (криминалистическую) экспертизу, установление происхождения и источника записи, анализ метаданных и истории правок/редактирования, а при необходимости – применение специализированных методов детекции признаков синтеза и монтажа. При невозможности исключить вмешательства или подмену доказательственная сила соответствующих материалов подлежит снижению вплоть до признания их недопустимыми.

Зарубежная практика, в частности опыт США, демонстрирует широкое применение хэш-функций для подтверждения целостности и аутентичности цифровых доказательств в рамках уголовных разбирательств. В соответствии с Правилom 901 Федеральных правил доказывания (Federal Rules of Evidence) хэш-значения применяются для идентификации электронных документов, представленных в суде. Так, использование алгоритма SHA-256 позволяет проверить неизменность файла с момента его получения, поскольку любое даже незначительное изменение данных немедленно отражается на хэш-сумме. Для подтверждения достоверности представляемой информации участник процесса обязан обосновать правильность расчета хэш-значения и его соответствие



оригинальному файлу³.

Таким образом, интеграция современных криптографических методов и хэш-функций в национальное уголовно-процессуальное законодательство является необходимым условием повышения эффективности противодействия преступлениям в цифровой среде, а также залогом укрепления доверия к цифровым доказательствам в судебной практике.

С учетом этого возникает необходимость адаптировать данные подходы к условиям национального законодательства и правоохранительной практики. Данное правило может быть адаптировано и внедрено в правовую систему Казахстана следующим образом:

1. Законодательные изменения. Внести дополнения в статью 118 «Вещественные доказательства» УПК РК, согласно которым для подтверждения целостности цифровых доказательств необходимо использовать хэш-функции.

2. Изменения в следственно-экспертной практике. При изъятии цифрового носителя (жесткого диска, телефона и пр.) следователь должен:

- сделать дубликат (image) устройства с помощью специализированного ПО;
- вычислить хэш-сумму исходного носителя и зафиксировать ее в протоколе изъятия;
- использовать только копию (image) при анализе, сверяя хэш с оригиналом.

Совокупность указанных действий обеспечит соблюдение принципа подлинности цифровых доказательств и минимизирует риски их подделки или искажения. Судебные эксперты обязаны проверять неизменность доказательств по хэш-сумме и отражать это в заключении эксперта.

Зарубежный опыт также демонстрирует эффективность использования хэш-функций как инструмента подтверждения подлинности цифровых данных. Правило «902 Доказательства, подтверждающие сами себя» Федеральных правил доказывания (Federal Rules of Evidence) включает

цифровые данные, подтвержденные хэш-функциями, в список самоподтверждающих доказательств. Если квалифицированное лицо подтверждает, что хэш-функции копии совпадают с хэшем оригинала, данные считаются аутентичными, что исключает необходимость вызова свидетеля для подтверждения подлинности⁴.

В то время как законодательство США предусматривает упрощенные процедуры аутентификации цифровых доказательств, в правовой системе Казахстана подобные механизмы пока не получили нормативного закрепления. Соответственно на данный момент в РК отсутствует институт «самоподтверждающихся цифровых доказательств», подобных FRE 902. Даже при наличии хэш-суммы следователю или эксперту необходимо подтвердить:

- когда и как была получена копия;
- какие инструменты использовались для вычисления хэша.

К примеру, в Канаде допустимость цифровых доказательств регулируется законом о доказательствах (Canada Evidence Act), который включает разделы 31.1-31.8 допустимости цифровых документов. СЕА предусматривает, что цифровые документы должны быть аутентифицированы и проверены на целостность.

Для аутентификации цифровых документов требуются доказательства, это может включать в себя технические доказательства и показания свидетеля. Необходимо убедиться, что цифровой документ не был изменен или подделан, что гарантирует его надежность [9].

Цифровая информация играет важную роль в науке и технологиях, однако в законодательстве Казахстана нет ее четкого определения. Толкование определения имеет большую роль в юридической отрасли. К примеру цифровая информация в уголовном праве может рассматриваться в качестве предмета правонарушения, таким образом определение имеет ключевую роль для квалификации и установления степени общественной опасности [10].

³ Federal Rules of Evidence, Rule 901: Authenticating or Identifying Evidence. – 2022 [Электронный ресурс] – Режим доступа: https://www.law.cornell.edu/rules/fre/rule_901 (дата обращения: 17.02.2025).

⁴ Там же.



В Казахстане активно продвигается идея об использовании цифровых доказательств, однако в соответствующем законодательстве имеются пробелы в сравнении с зарубежным опытом. В частности, у нас есть порядок и правила, регламентирующие фиксацию и представление цифровых доказательств, однако они остаются фрагментарными и не всегда адаптированы к быстроменяющимся цифровым реалиям.

В Казахстане также пока отсутствует единая норма, обязывающая использовать хэш-функции в качестве обязательного элемента судебного цифрового доказательства.

К примеру, в соответствии со статьей 199 УПК РК протокол следственного действия при изъятии цифрового документа должен содержать сведения о применении хэш-функции. При снятии копии цифрового документа непосредственно на месте происшествия следователь обязан зафиксировать цифровой отпечаток (хэш-сумму), полученный в результате прохождения файла через криптографическую хэш-функцию. Данная процедура направлена на обеспечение доказательной целостности цифрового объекта⁵.

Фиксация хэш-суммы происходит следующим образом: после идентификации цифрового файла (например, видео, текстового документа или электронного письма), он копируется на защищенный носитель. С помощью специализированного программного обеспечения вычисляется хэш-сумма – уникальный строковый код, присваиваемый конкретному состоянию файла. Полученное значение хэша заносится в протокол с указанием:

- алгоритма хэширования;
- даты и времени вычисления;
- устройства или программного инструмента, с помощью которого производился расчет;
- лица, осуществившего процедуру.

Данный цифровой «отпечаток» позволяет в любой момент проверить подлинность

документа. Даже минимальное изменение в файле (вплоть до одного байта) приведет к полной смене хэш-суммы, что сигнализирует о возможном вмешательстве. Таким образом, внесение хэш-значения в протокол обеспечивает юридическую гарантированность неизменности цифрового доказательства в процессе его дальнейшего хранения, передачи и анализа.

Требования о предоставлении хэш-суммы имеются в Приказе Министра юстиции РК от 27 апреля 2017 года № 484 «Об утверждении Правил организации и производства судебных экспертиз и исследований в органах судебной экспертизы»⁶.

На основании изложенного предлагаем внести дополнения в УПК РК от 4 июля 2014 года № 231-V ЗРК.

1. Дополнить статью 118 «Вещественные доказательства» следующим абзацем:

«Цифровыми доказательствами признаются сведения, имеющие значение для уголовного дела и представленные в электронной форме, включая текстовые документы, электронную переписку, аудио- и видеозаписи, сетевые журналы, метаданные, а также любую информацию, созданную, сохраненную или переданную посредством электронных и телекоммуникационных средств».

2. Дополнить статью 199 «Протокол следственного действия» *предложениями следующего содержания:*

«При изъятии цифровых носителей или копировании информации следователь должен применять криптографические хэш-функции, а вычисленные хэш-суммы фиксируются в протоколе следственного действия».

Несоблюдение порядка документирования цифровых доказательств может привести к признанию их недопустимыми».

3. Дополнить статью 80 «Специалист» *предложениями следующего содержания:*

«При производстве следственных действий, связанных с обнаружением, изъятием, копированием, восстановлением

⁵ Уголовно-процессуальный кодекс Республики Казахстан: от 4 июля 2014 г. № 231-V ЗРК [Электронный ресурс] – Режим доступа: <https://adilet.zan.kz/rus/docs/K1400000231> (дата обращения: 18.02.2025).

⁶ Об утверждении Правил организации и производства судебных экспертиз и исследований в органах судебной экспертизы: приказ Министра юстиции Республики Казахстан от 27 апр. 2017 г. № 484 [Электронный ресурс] – Режим доступа: <https://adilet.zan.kz/rus/docs/V1700015180> (дата обращения: 18.02.2025).



или анализом цифровой информации, следователь обязан привлекать специалиста в области информационных технологий, цифровой криминалистики, кибербезопасности или иных смежных направлений.

Специалист оказывает содействие в:

- технически корректном извлечении и копировании цифровых данных;
- расчете и фиксации хэш-сумм;
- восстановлении удаленной, зашифрованной или поврежденной информации;
- обеспечении целостности и воспроизводимости цифровых доказательств;
- составлении протокола с указанием использованного оборудования и программного обеспечения».

Указать, что в заключении эксперта должна быть включена обязательная графа: «Хэш-сумма файла совпадает с оригиналом. Цифровое доказательство неизменно».

Обозначить, что привлечение специалиста является обязательным, если выполнение указанных действий требует специальных технических знаний или программно-аппаратных средств, нарушение порядка которых может повлечь утрату допустимости доказательств.

4. Ввести норму, аналогичную FRE 902:

«Цифровые копии доказательств, подлинность которых подтверждена хэш-суммой, совпадающей с оригиналом и заверенной экспертом, считаются допустимыми без необходимости вызова этого эксперта в суд».

Кроме того, необходимо:

- разработать и утвердить методические рекомендации МВД и Генеральной прокуратуры по фиксации, хранению и верификации цифровых доказательств с обязательным указанием хэш-суммы при изъятии;

- внести поправки в Закон РК «Об информатизации» 24 ноября 2015 года № 418-V ЗРК, дополнив статью 1 «Основные понятия»:

«Цифровые доказательства – это

информация в электронной форме, имеющая юридическое значение, полученная, сохраненная, переданная или зафиксированная с использованием цифровых технологий и предназначенная для использования в судопроизводстве, административных или иных официальных процедурах в соответствии с законодательством РК»;

- дополнить пункт 5 главы 2 «Порядок изъятия вещественных доказательств и документов по уголовным делам судом, органами прокуратуры, уголовного преследования и судебной экспертизы» Постановления Правительства РК «Об утверждении Правил изъятия, учета, хранения, передачи и уничтожения вещественных доказательств, изъятых документов, денег в национальной и иностранной валюте, наркотических средств, психотропных веществ по уголовным делам судом, органами прокуратуры, уголовного преследования и судебной экспертизы» от 9 декабря 2014 года № 1291 следующим предложением: «При изъятии цифровых документов в протоколе необходимо отразить хэш-сумму изымаемых файлов»⁷.

Заключение. В настоящее время в казахстанском законодательстве отсутствует комплексное регулирование вопросов, связанных с использованием цифровых эквивалентов документов. Это приводит к появлению правовой неопределенности и затрудняет эффективное применение цифровых доказательств в судебной практике. Недостаточная определенность нормативных актов, а также существующие процедурные правила оформления электронных данных способствуют возникновению трудностей в сфере доказывания и ставят под сомнение юридическую корректность соответствующих алгоритмов. Поэтому для устранения данных пробелов следует закрепить в законопроектах точное определение цифровых аналогов, обязательное применение хэш-функций при их изъятии и допущение к участию в процессах работы с электронным информационным

⁷ Об утверждении Правил изъятия, учета, хранения, передачи и уничтожения вещественных доказательств, изъятых документов, денег в национальной и иностранной валюте, наркотических средств, психотропных веществ по уголовным делам судом, органами прокуратуры, уголовного преследования и судебной экспертизы: постановление Правительства Республики Казахстан от 9 дек. 2014 г. № 1291 [Электронный ресурс] – Режим доступа: <https://adilet.zan.kz/rus/docs/P1400001291> (дата обращения: 18.02.2025).



ресурсом квалифицированных специалистов.

Анализ международного опыта показывает, что применение стандартизированных процедур цифровой криминалистики, таких как хэширование, верификация, аудит и логгирование действий, может существенно повысить надежность и допустимость цифровых доказательств. Внедрение

соответствующих норм в УПК РК, Закон «Об информатизации» и подзаконные акты позволят гармонизировать отечественную практику с международными стандартами, а также повысит справедливость, эффективность и технологическую устойчивость судебной системы в условиях цифровой трансформации.

Список использованной литературы:

1. Ильиных, Н.А. Киберэкстремизм: понятие и разграничение с иным информационным деструктивным воздействием в киберпространстве / Н.А. Ильиных // История и право. – 2023. – Т. 13. № 1. – С. 64-74.
2. Оракбаев, А.Б. Перспективы применения систем виртуализации по делам о массовых беспорядках / А.Б. Оракбаев // Құқық қорғау органдары академиясының Жаршысы. – 2024. – № 2 (32). – С. 192-205.
3. Quick, D. IoT Device Forensics and Data Reduction / D. Quick, K.-K.R. Choo // in IEEE Access. – 2018. – Vol. 6. – Pp. 47566-47574.
4. Clifford, B. Moderating Extremism: The State of Online Terrorist Content Removal Policy in the United States. – Washington, DC: Program on Extremism at The George Washington University, 2021. – 24 p.
5. Klonick, K. The New Governors: The People, Rules, and Processes Governing Online Speech / K. Klonick // Harvard Law Review. – 2018. – Т. 131. № 6. – Pp. 1598-1670.
6. Awan, I. Cyber-Extremism: ISIS and the Power of Social Media / I. Awan // Society. – 2017. – Vol. 54. No. 2. – Pp. 138-149.
7. Dmitrieva, A.A. Concept of Electronic Evidence in Criminal Legal Procedure / A.A. Dmitrieva, P.S. Pastukhov // Journal of Digital Technologies and Law. – 2023. – № 1 (1). – Pp. 270-295.
8. C. Rechberger, S. Krenn, R. Posch. Towards a Process Model for Hash Functions in Digital Forensics // Proceedings of the 11th International Conference on Availability, Reliability and Security (ARES 2016). – Salzburg, Austria: ACM, 2016. – Pp. 677-683.
9. Моисеев, В.А. Применение алгоритмов решения задачи выполнимости к криптоанализу хэш-функций семейства MD / В.А. Моисеев, В.В. Силаев // Математические структуры и моделирование. – 2014. – № 32. – С. 144-153.
10. Ким, А.С. Роль хэширования в работе «белого хакера» / А.С. Ким, Е.Е. Симаков, М.Н. Симакова // Юный ученый. – 2023. – № 8 (71). – С. 35-40.
11. Собиров, Ш. Сравнительно-правовой анализ регулирования электронных доказательств в уголовном судопроизводстве: опыт США, ЕС и стран СНГ / Ш. Собиров // Общество и инновации. – 2023. – № 4 (5). – Pp. 96-117.
12. Сарбасов, А.Е. Правовое понятие цифровой информации / А.Е. Сарбасов, Ж.Р. Дильбарханова // Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының ғылыми еңбектері. – 2024. – № 3 (80). – С. 10-15.

References:

1. Il'inyh, N.A. Kiberjekstremizm: ponjatie i razgranichenie s inym informacionnym destruktivnym vozdejstviem v kiberprostranstve / N.A. Il'inyh // Istorija i pravo. – 2023. – Т. 13. № 1. – С. 64-74.
2. Orakbaev, A.B. Perspektivy primenenija sistem virtualizacii po delam o massovyh besporjadkah / A.B. Orakbaev // Құқық қорғау органдары академиясының Жаршысы. – 2024. – № 2 (32). – С. 192-205.
3. Quick, D. IoT Device Forensics and Data Reduction / D. Quick, K.-K.R. Choo // in IEEE Access. – 2018. – Vol. 6. – Pp. 47566-47574.



4. Clifford, B. Moderating Extremism: The State of Online Terrorist Content Removal Policy in the United States. – Washington, DC: Program on Extremism at The George Washington University, 2021. – 24 p.
5. Klonick, K. The New Governors: The People, Rules, and Processes Governing Online Speech / K. Klonick // Harvard Law Review. – 2018. – T. 131. № 6. – Pp. 1598-1670.
6. Awan, I. Cyber-Extremism: ISIS and the Power of Social Media / I. Awan // Society. – 2017. – Vol. 54. No. 2. – Pp. 138-149.
7. Dmitrieva, A.A. Concept of Electronic Evidence in Criminal Legal Procedure / A.A. Dmitrieva, P.S. Pastukhov // Journal of Digital Technologies and Law. – 2023. – № 1 (1). – Pp. 270-295.
8. C. Rechberger, S. Krenn, R. Posch. Towards a Process Model for Hash Functions in Digital Forensics // Proceedings of the 11th International Conference on Availability, Reliability and Security (ARES 2016). – Salzburg, Austria: ACM, 2016. – Pp. 677-683.
9. Moiseev, V.A. Primenenie algoritmov resheniya zadachi vpolnimosti k kriptanalizu hresh-funkcij semeystva MD / V.A. Moiseev, V.V. Silaev // Matematicheskie struktury i modelirovanie. – 2014. – № 32. – S. 144-153.
10. Kim, A.S. Rol' hreshirovaniya v rabote «belogo hakera» / A.S. Kim, E.E. Simakov, M.N. Simakova // Junyj uchenyj. – 2023. – № 8 (71). – S. 35-40.
11. Sobirov, Sh. Sravnitel'no-pravovoj analiz regulirovaniya jelektronnyh dokazatel'stv v ugolovnom sudoproizvodstve: opyt SShA, ES i stran SNG / Sh. Sobirov // Obshhestvo i innovacii. – 2023. – № 4 (5). – Pp. 96-117.
12. Sarbasov, A.E. Pravovoe ponjatie cifrovoj informacii / A.E. Sarbasov, Zh.R. Dil'barhanova // Qazaqstan Respublikasy IIM M. Esbolatov atyndary Almaty akademijasynyn ғылыми еңбектері. – 2024. – № 3 (80). – S. 10-15.

АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

Айбек Серикович Алишев – Қазақстан Республикасы Ішкі істер министрлігінің М. Есболатов атындағы Алматы академиясының докторанты, ұлттық қауіпсіздік және әскери іс магистрі, ORCID: <https://orcid.org/0009-0008-6197-557X>, e-mail: aibek_alishev@mail.ru.

Алишев Айбек Серикович – докторант Алматинской академии Министерства внутренних дел Республики Казахстан имени М. Есбулатова, магистр национальной безопасности и военного дела, ORCID: <https://orcid.org/0009-0008-6197-557X>, e-mail: aibek_alishev@mail.ru.

Alishev Aibek Serikovich – Doctoral Student of the M. Yesbolatov Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan, Master of National Security and Military Case, ORCID: <https://orcid.org/0009-0008-6197-557X>, e-mail: aibek_alishev@mail.ru.

Ботагоз Булатовна Сарсенбаева – Қазақстан Республикасы Ішкі істер министрлігінің М. Есболатов атындағы Алматы академиясының қылмыстық процесс және криминалистика кафедрасының профессоры, заң ғылымдарының кандидаты, ORCID: <https://orcid.org/0009-0006-9238-5172>, e-mail: hamudok@mail.ru.

Сарсенбаева Ботагоз Булатовна – профессор кафедры уголовного процесса и криминалистики Алматинской академии Министерства внутренних дел Республики Казахстан имени М. Есбулатова, кандидат юридических наук, ORCID: <https://orcid.org/0009-0006-9238-5172>, e-mail: hamudok@mail.ru.

Sarsenbayeva Botagoz Bulatovna – Professor of the Department of Criminal Procedure and Criminalistics of the Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Esbolatov, Candidate of Law, ORCID: <https://orcid.org/0009-0006-9238-5172>, e-mail: hamudok@mail.ru.