МАЗМҰНЫ / СОДЕРЖАНИЕ / CONTENT

Мақала туралы мәлімет

Конференция атауы	«Жастар және ғылым: бүгіні мен болашағы» жас ғалымдардың халықаралық ғылыми-тәжірибелік конференция материалдар жинағы
Сборник	«Молодежь и наука: настоящее и будущее». Сборник материалов Международной научно-практической конференции молодых ученых
Conference	The collection of materials from the International Scientific and Practical Conference of Young Scientists «Youth and Science: Present and Future»
Өткізілген күні	7 сәуір 2025, Атырау
ISBN	978-601-262-587-5
Жинақтағы жариялану №	116
Жинақтағы беттері	542-547
ӘОЖ/УДК/UDC	УДК 343.13
Секция	Секция IV. II Адам құқығын қорғау – құқықтық және әділ мемлекет құрудың кепілі/ / Защита прав человека – залог создания правового и справедливого государства
Автор(лар)	Рахметова Айсара Еркінқызы
Мәртебесі	Магистрант
Ғылыми жетекші	Научный руководитель, к.ю.н., профессор Шаяхметова Ж.Б.
Мақала атауы	ЗАРУБЕЖНЫЙ ОПЫТ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

УДК 343.13

ЗАРУБЕЖНЫЙ ОПЫТ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Рахметова Айсара Еркінқызы
магистрант 1 курса ОП 7М04211-Юриспруденция
Атырауского университета им. Х. Досмухамедова, г.Атырау, Республика Казахстан
Научный руководитель, к.ю.н., профессор Шаяхметова Ж.Б.

В эпоху цифровых технологий новые технологии и достижения в области компьютерных разработок изменили осознание того, как потенциально значимые доказательства преступлений будут оцениваться в международном уголовном праве. Новые технологии делают возможным архивирование данных, связанных с вооруженным конфликтом, из широкого спектра источников, включая, помимо прочего, спутниковые и геопространственные изображения, системы глобального позиционирования (GPS), данные мобильных телефонов, видео, фотографии, социальные сети и другие данные.

На примере практики Международного уголовного суда (МУС или «Суд») рассмотрены ряд важных проблем, связанных с проверкой подлинности цифровых доказательств, и адаптацией к этим изменениям. Учитывая тот факт, что положения МУС ратифицированы 134 государствами мира, полагаем следует рассмотреть вопрос его практику относительно цифровых доказательств [1].

Именно судебная практика, как конечная стадия оценки соблюдения процессуальных требований «обращения» с вещественными доказательствами, а также с учетом специфики уголовно-процессуального законодательства, вызывает огромный интерес в части результативности позитивности и негативности опыта.

Созданный в 1998 году МУС является первым в мире постоянным международным уголовным судом, которому поручено расследование и уголовное преследование за самые тяжкие преступления, представляющие опасность для международного сообщества: геноцид, преступления против человечности, военные преступления и преступления против мира и безопасности.

На момент своего создания МУС, возможно, не мог предвидеть грядущую революцию в цифровых технологиях и ее влияние на Суд.

Однако, спустя два десятилетия, процедуры Суда по доказыванию и проверки подлинности доказательств не соответствуют развитию современной эпохи. Хотя новые технологии во многом способствуют «осовремениванию» уголовного процесса, связанного с совершением международных преступлений, вместе с тем Суд не готов в полном объёме взять на себя сложную задачу по аутентификации и исследованию (проверке) цифровых доказательств.

Международные суды, уже давно пытаются оценить сложные области вне своей компетенции, включая, среди прочего, судебно-медицинскую, баллистическую, геномную экспертизы и многое другое.

По настоящее время остается проблемным вопросом обеспечение судебного контроля за законностью и достоверностью экспертных исследований в данном случае.

Дебаты относительно оценки научных доказательств служат аналогичной полезной отправной точкой для разработки соответствующей системы судебного контроля для аутентификации цифровых доказательств, что позволяет разрешить следующие вопросы относительно и отечественного законодательства:

1. Определить проблемы и риски нынешнего подхода к аутентификации и проверке цифровых доказательств;

2. Изучить мнения ученых по поводу анализа научных данных как аналогичной проблемы;

3. Определить наиболее прагматичный подход к проверке подлинности цифровых доказательств в дальнейшем.

Несмотря на то, что существует множество серьезных проблем с представлением цифровых доказательств в Суд, особенно в сборе и сохранении цифровых доказательств, основное внимание уделено проверке подлинности цифровых доказательств.

В условиях развития технологий открываются возможности для модернизации уголовного судопроизводства, связанного с международными, трансграничными уголовными правонарушениями, где, однако, Суд не может в полной мере реализовать функции по аутентификации и проверке цифровых доказательств.

Прежде чем продолжить, важно уточнить термины, которые будут представлены в последующих разделах.

Аутентификация — это одновременно термин кибербезопасности и юридический термин, используемый для описания процесса доказательства того, что цифровой файл является подлинным или не поддельным. По сути, аутентификация гарантирует, что рассматриваемый элемент является тем, за что он выдает себя, и что он не подвергался манипуляциям или изменениям.

Верификация (проверка) — это процесс обеспечения того, чтобы утверждение или утверждение, сделанное в каком-либо средстве связи, было надежным и/или правдивым.

Верификация и аутентификация тесно взаимосвязаны, но различны. Например, возможно, что подлинный цифровой файл либо правдив, либо ложен; однако недостоверное доказательство следует считать предположительно не поддающимся проверке, поскольку было обнаружено, что этот цифровой файл был подделан, преобразован или изменен.

В МУС судьям предоставлена широкая свобода действий в принятии доказательств по своему усмотрению. Римский статут («Статут») является учредительным договором МУС и служит руководящим правовым инструментом Суда. Именно ратификация Римского статута 134 государствами мира, позволяет более широко рассмотреть международный и зарубежный опыт и характер его эффективности [2].

Правила процедуры и доказывания (RPE или «Правила», приложение к «Римскому статуту») предлагают дополнительную конкретику в отношении приема и обработки доказательств. Правило Регламента гласит: «Палата имеет право в соответствии с правом усмотрения, описанным в пункте 9 статьи 64, свободно оценивать все представленные доказательства, чтобы определить их относимость или допустимость в соответствии со статьей 69 Статута.

Другими словами, судьи обладают полномочиями принимать решения по любым вопросам, возникающим в отношении подлинности или проверяемости цифровых доказательств. Суд во многом полагается на усмотрение и опыт судей при надлежащей оценке принятых доказательств.

Этот гибкий подход к допуску доказательств также является результатом ограничений полномочий МУС. В отличие от внутренних уголовных расследований, где правоохранительные органы имеют право принуждать стороны посредством вызова в суд и ордеров на обыск, следственные группы МУС не обладают такими полномочиями.

Общий подход МУС к допустимости доказательств включает последовательный трехэтапный тест, в котором должен быть соблюден каждый из следующих критериев: относимость и доказательная ценность.

Относимость: «В соответствии со статьями 64(9)(a) и 69(4) Римского статута и далее сформулированными в прилагаемых Правилах процедуры и доказывания, доказательства будут считаться относящимися к делу, если «представленные доказательства подтверждают наличие факта и проблема более или менее вероятная». Другими словами, доказательства могут считаться относящимися к делу, если они *prima facie* имеют отношение к делу» [3]

Доказательная ценность: Доказательная ценность обычно понимается как то, является ли доказательство достаточно полезным для доказательства важной части судебного разбирательства. По сути, доказательная ценность измеряет степень, в которой

представленные доказательства могут повлиять на определение факта или проблемы. Согласно статье 69 Статута, доказательная ценность предмета должна быть оценена, прежде чем он может быть принят в качестве доказательства [1].

Другими словами, вес, придаваемый доказательствам, должен полностью обеспечивать (не нарушать) права всех сторон и не быть явно несправедливым по отношению ни к обвинению, ни к защите, а также не наносить ущерба принципу справедливости судебного разбирательства.

Основное внимание в этом исследовании уделяется механизмам и проблемам аутентификации цифровых доказательств, и соответствующим процессам судебного рассмотрения. Однако концепции проверки и аутентичности могут запутаться, поскольку судьи начинают принимать решения о приемлемости, релевантности, доказательной ценности и весе цифровых доказательств.

Например, в деле «Прокурор против Жан-Пьера Бембы Гомбо» сторона обвинения предоставила десять аудиозаписей радиопередач, чтобы установить предысторию и контекст конфликта. Когда защита высказала возражения против допуска этих записей, Палата суда постановила, что «записи, подлинность которых не была подтверждена в суде, все же могут быть приняты к рассмотрению, поскольку аутентификация в суде является лишь одним из средств, которые Палата должна учитывать при определении подлинности предмета и доказательное значение» [4]

Однако определение допустимости каких-либо доказательств не имеет никакого влияния на доказательную силу, которую им придает сама Палата. Доказательственный вес означает относительную важность, придаваемую части признанных доказательств при принятии решения о том, доказан ли определенный вопрос или нет. Поэтому, в отличие от доказательной силы, вес доказательств оценивается судьями в конце судебного разбирательства, после заслушивания всей совокупности доказательств, принятых по делу.

В деле «Прокурор против Жан-Пьера Бембы Гомбо» МУС подтвердил, что у судей нет строгих требований выносить отдельное решение относительно подлинности представленных доказательств. Основная аргументация Палаты в этом деле заключалась в содействии справедливому и быстрому судебному разбирательству, как того требует статья 64 Статута.

Учитывая гибкий подход Суда к доказательствам, определение подлинности доказательств в конечном итоге остается на усмотрение судей. Это становится проблематичным при оценке цифровых доказательств, ввиду сложности технической стороны и необходимости соответствующих познаний.

При реализации полномочий суда создан Единый технический протокол или («Протокол электронного суда» или «Протокол»), который предназначен для обеспечения техническими протоколами и средством определения подлинности цифровых доказательств.

Большая часть Протокола электронного суда представляет собой относительно стандартное описание соглашений о наименованиях и характере процедур подготовки и подачи документов в электронную систему Суда. Однако методы аутентификации, предусмотренные Протоколом, требуют тщательного изучения [5]

Кратковременный характер цифровых доказательств поднимает вопрос о том, какие меры по сохранению необходимы или даже возможны в соответствии с действующим Статутом. Хотя полномочия прокурора ограничены до начала расследования, безграничный характер Интернета и распространение цифровых коммуникаций могут потребовать смягчения этих ограничений во время предварительного расследования.

Ценная цифровая информация, доступная во время развития или на ранних стадиях конфликта, может быть потеряна, если не обеспечить сохранность этой информации криминалистически обоснованным путем до начала расследования.

Например, прокурор должен иметь возможность использовать рамки сотрудничества, предусмотренные Римским статутом, которые призваны обеспечить помощь Суду на государственном уровне, чтобы обращаться к поставщикам услуг связи с просьбой сохранить пользовательские данные сверх обычных сроков их хранения.

Хотя сотрудничество государства на этапе предварительного расследования является добровольным, государства-участники должны рассматривать запросы информации к поставщикам услуг как часть своей обязанности по поддержке Суда.

То есть данный момент подразумевает обеспечение сохранности массива цифровой информации сверх установленного времени. Учитывая непродолжительный и нормативно не определенный характер хранения такой информации на серверах поставщиков услуг, а также сроки исковой давности в Республике полагаем Казахстан, полагаем необходимым определить конкретные обязательные сроки хранения цифровой информации (фото, видео фиксация и т.д.) в течении срока исковой давности.

Да, действительно, установлено обязательное хранение на электронном носителе материалов кредитного досье на заемщиков в течение 5 лет, вместе с тем имеется оговорка обязательности при условии наличия такой возможности формирования досье в электронном формате у банков [6].

Данные моменты конечно предполагают дополнительные финансовые затраты поставщиков услуг.

Статья 56 Римского статута допускает сбор доказательств, которые впоследствии могут быть недоступны для целей судебного разбирательства.

На этапе расследования статья 56 может быть применена для сохранения цифровой информации в странах, где прокурору физически ограничен вход на территорию предприятия, связанного с преступлением, но не являющегося участником уголовного процесса. Цифровые доказательства могут храниться в нескольких местах, и их сбор может не требовать физического доступа на территорию объекта или государства в целом. Это важнейшее подспорье для следователей МУС, которые полагаются на сотрудничество государственных органов, чтобы иметь возможность получить доступ и изъять доказательства.

Отсутствие международной помощи препятствовало расследованиям в прошлом, но, поскольку данные хранятся без учета физических границ и проходят через серверы, расположенные во многих странах, рассматриваются новые способы как государства-участники могут способствовать сохранению цифровых доказательств при транспортировке на сервера, доступ к которым возможен на территориях, находящихся под юрисдикцией Суда.

Вместе с тем, следует отметить, что возможности сети Интернет способствуют, а возможно даже компенсируют ограничения проверочных действий прокурором, в целях соблюдения требований законов о кибербезопасности и конфиденциальности, без официального запроса помощи государств вне юрисдикции Статута.

Протокол электронного суда требует, чтобы всем цифровым файлам, загружаемым в электронную систему, была присвоена цифровая подпись, которая «может использоваться для проверки подлинности доказательств, если подлинность оспаривается».

Цифровая подпись — это «математический алгоритм, обычно используемый для проверки подлинности и целостности сообщения» (CISA, без даты). Цифровые подписи уникальны для конкретного физического или юридического лица и используются для защиты и надежной аутентификации происхождения, целостности и неотречения подписи цифрового файла. Протокол электронного суда требует, чтобы участники торгов проверяли подлинность файлов с помощью алгоритма хеширования цифровых подписей, называемого MD5. Хотя в целом для Суда является хорошей практикой обеспечения безопасности требование цифровых подписей для целей аутентификации, использование MD5 следует рассматривать как проблему, вызывающую непосредственную и серьезную озабоченность МУС.

MD5 — это программа хэш-функции, первоначально созданная в 1992 году. Каждая цифровая подпись генерирует «хэш-функцию» или строку цифр и букв, созданную алгоритмом, уникальным для файла или документа. Хэш — это односторонняя функция. Это означает, что процесс, создавший хэш, не может быть отменен для поиска других файлов, генерирующих такое же значение хеш-функции. MD5 использует 128-битный «цифровой отпечаток» для создания одностороннего хеша, который по современным стандартам имеет относительно небольшое количество бит. MD5 не соответствует одному из основных

требований любой криптографической хэш-функции — вычислительно невозможно найти два разных файла с одинаковым значением хеш-функции. Это явление, когда несколько файлов имеют совпадающие хеш-функции, известно, как коллизия. Из-за известной уязвимости к коллизиям к 2008 году MD5 был признан во всем мире криптографически взломанным.

В 2011 году Инженерная группа Интернета (IETF), ведущая международная организация по протоколам Интернета, предупредила всех пользователей компьютеров, что «MD5 больше не приемлем там, где требуется устойчивость к коллизиям, например, цифровые подписи».

В 2012 году коллизионные уязвимости в MD5 были широко использованы с помощью сложного вредоносного ПО под названием Flame, которое в то время считалось «одной из самых сложных угроз, когда-либо обнаруженных». Flame заразил сети в Иране, Израиле, Судане, Сирии, Ливане, Саудовской Аравии и Египте, что позволило хакерам записывать аудио, делать снимки экрана, контролировать нажатия клавиш и открывать конфиденциальные файлы. Flame воспользовался слабой криптографией MD5 и обманом заставил зараженные компьютеры поверить в то, что вредоносное ПО имеет действительную цифровую подпись. Коллизионная атака Flame возобновила призывы исследователей прекратить использование MD5 для аутентификации цифровых подписей в любых целях [7].

Использование MD5 не только делает аутентификацию цифровых доказательств технически невозможной, но и подрывает легитимность Суда и объективность судебного процесса. Кроме того, любая сторона, желающая оспорить подлинность любых цифровых доказательств, представленных в Суд, может указать на широко разрекламированную и хорошо известную небезопасность MD5 и немедленно признать доказательства недостоверными, что фактически сводит на нет огромное количество времени и энергии, затраченных на сбор, защиту и представление доказательств в суд.

MD5 делает хранилище цифровых доказательств МУС небезопасным. Неспособность МУС обновить свою сломанную криптографию сродни тому, как сломать замок на воротах, где хранятся доказательства самых страшных преступлений в мире. Данные в электронных системах судебных органов могут быть подвергнуты соответствующим вредоносным атакам.

Замена MD5 более надежной криптографической программой устранит непосредственную уязвимость безопасности в системе. Однако удаление и замена MD5 более надежными криптографическими стандартами требует как криптографической гибкости, так и совместимости.

Криптографическая гибкость описывает способность машин добавлять новые криптографические алгоритмы или функции к существующему оборудованию или программному обеспечению, а также эффективно выводить из эксплуатации уязвимые или устаревшие криптографические системы. Функциональная совместимость описывает способность общаться и обмениваться информацией между различными системами.

Это непростая задача для всех сторон. Некоторые устаревшие машины и системы могут не поддерживать обновления безопасности, или пользователи могут не захотеть платить за обновления безопасности.

Суд также должен учитывать время и затраты на обновление протоколов безопасности для менее технологически продвинутых сторон. Например, сила более предпочтительной современной криптографии может замедлять работу старых машин, делая систему электронного суда менее доступной для менее технологически продвинутых пользователей. Таким образом, любые обновления протокола электронного суда должны тщательно сбалансировать соображения логики и безопасности всех участников процесса.

Разработка системы, сочетающей в себе криптографическую гибкость и функциональную совместимость, является необходимым шагом на пути к более безопасной электронной системе подачи заявок.

Однако это не решает проблему того, как Суду следует обращаться со всеми документами и файлами, заверенными с помощью MD5, по делам, находящимся на рассмотрении. В таких случаях могут быть только две возможные стратегии смягчения

последствий. Суд может потребовать от всех сторон повторно представить каждую часть цифровых доказательств с использованием новых, более безопасных алгоритмов хеширования. Это будет трудоемкий процесс для сторон и может нарушить статью 64 Статута, которая гласит: «Судебная палата должна обеспечить, чтобы судебное разбирательство было… оперативным».

Тот факт, что МУС по настоящее время требует использование цифровых подписей, предполагает, что Суд признает важность целостности и безопасности данных.

Поэтому крайне важно уделять приоритетное внимание надежным стандартам криптографии для защиты своей электронной системы при формировании, фиксации и хранении документов.

Подводя итог, можно сказать, что MD5 опасно устарел, и ему нельзя доверять в выполнении основной функции его предполагаемого использования — аутентификации цифровых файлов. Однако на территории Республики Казахстан, не смотря на известность данной проблемы с 2012 года, по настоящее время вопрос объективности прерогативы использования MD5, как способа идентификации и аутентификации, не рассматривается.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. The United Nations Diplomatic Conference of Plenipotentiaries on the Establishment of an International Criminal Court. [Электронный ресурс] – Режим доступа: https://www.ohchr.org/en/instruments-mechanisms/instruments/rome-statute-international-criminal-court/ (дата обращения: 15.12.2024).

2. Rome Statute. [Электронный ресурс] – Режим доступа: https://www.icc-cpi.int/sites/default/files/RS-Eng.pdf/ (дата обращения 15.12.2024).

3. Will Kenton Prima Facie: Legal Definition and Examples [Электронный ресурс] – Режим доступа: https://www.investopedia.com/terms/p/prima-facie.asp/ (дата обращения: 15.12.2024).

4. Бывший вице-президент ДРК получил 18 лет тюрьмы за военные преступления в ЦАР. [Электронный ресурс] – Режим доступа:https://ru.euronews.com/2016/06/21/icc-gives-former-rebel-warlord-18-years-for-war-crimes-and-crimes-against/ (дата обращения: 15.12.2024).

5. Unified technical protocol of the ICC [Электронный ресурс] – Режим доступа:https://www.icccpi.int/sites/default/files/RelatedRecords/CR2019_00267.PDF/ (дата обращения: 15.12.2024).

6. Об установлении Перечня основных документов, подлежащих хранению, и сроков их хранения в банках второго уровня, филиалах банков-нерезидентов Республики Казахстан Постановление Правления Национального Банка Республики Казахстан от 29 февраля 2016 года № 66. Зарегистрировано в Министерстве юстиции Республики Казахстан 17 мая 2016 года № 13710. [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/V1600013710/ (дата обращения: 15.12.2024).

7. How does the Flame malware take advantage of MD5 collision? [Электронный ресурс] – Режим доступа: https://crypto.stackexchange.com/questions/44151/how-does-the-flame-malware-take-advantage-of-md5-collision/ (дата обращения: 15.12.2024).