ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ДАННЫХ, ХРАНЯЩИХСЯ В ОБЛАЧНЫХ ИСТОЧНИКАХ, В УГОЛОВНО-ПРОЦЕССУАЛЬНОМ ДОКАЗАТЕЛЬСТВЕ

Эсанова Жахонгира Мамадалиевича
Независимый исследователь

Аннотация: В статье анализируются криминалистические и правовые проблемы сбора доказательств облачной памяти. Опираясь на основания “Цифрового доказательства” в законодательстве Узбекистана показано, что только артефакты местных устройств и мобильная криминалистика помогут в расследовании. Блокчейн-технология предлагается как перспективное решение для обеспечения целостности доказательств.

Ключевые слова: Уголовный процесс, Облачное доказательство, Цифровое доказательство, Доказательство, Допустимость, Криминалистика, Трансграничность, Блокчейн.

Аннотация: Статья посвящена криминалистическим и правовым проблемам сбора доказательств из облачных хранилищ. На основе введения в законодательство Узбекистана понятия "Цифровое доказательство" обоснована необходимость анализа артефактов локальных устройств и мобильной криминалистики. В качестве перспективного решения для обеспечения целостности доказательств предлагается технология Blockchain.

Ключевые слова: Уголовный процесс, Облачные доказательства, Цифровые доказательства, Доказательство, Допустимость, Криминалистика, Трансграничность, Блокчейн.

Annotation: This article analyzes the forensic and legal challenges of collecting cloud storage evidence. Building upon the introduction of “Digital Evidence” in Uzbekistan's law, it argues that investigating local device artifacts and mobile forensics is crucial. Blockchain technology is proposed as a promising solution to guarantee the integrity of digital evidence.

Keywords: Criminal Procedure, Cloud Evidence, Digital Evidence, Proof, Admissibility, Criminalistics, Transborder, Blockchain.

ВВЕДЕНИЕ

Стремительное развитие информационно-коммуникационных технологий в мировом масштабе коренным образом изменило форму и сущность преступности. Сегодня электронные доказательства становятся неотъемлемой частью доказывания в уголовном процессе, резко возрастает количество и степень общественной опасности преступлений, совершаемых в

киберпространстве, особенно имущественных преступлений. С развитием цифровых технологий киберпреступность стала одним из самых быстрорастущих видов преступлений, представляющих наибольшую экономическую опасность. Согласно отчету международных исследовательских центров Cybersecurity Ventures, к 2025 году ежегодный глобальный ущерб от киберпреступности может достичь 10,5 триллиона долларов США. Основная часть доказательств в таких преступлениях, примерно более 80%, приходится на данные, хранящиеся в облачных сервисах (Google Drive, Telegram, корпоративные облака). Поэтому законное и эффективное использование этих доказательств, а также обеспечение защиты конституционных прав и свобод личности определяют актуальность темы.

Актуальность темы исследования напрямую связана с динамикой адаптации законодательства Республики Узбекистан к требованиям быстро развивающейся цифровой среды. В частности, принятие Закона Республики Узбекистан от 21 ноября 2024 года No ЗРУ-1003 отразило необходимость укрепления правовых основ института цифровых доказательств, возникшего пропорционально расширению преступности в условиях цифровой трансформации. Данным нормативно-правовым актом внесены фундаментальные изменения в Уголовно-процессуальный кодекс и другие процессуальные законы. В частности, введение таких новых понятий, как "цифровое доказательство" и "электронные данные," расширение перечня доказательств за счет вещественных, письменных и цифровых доказательств, а также установление процедур сбора, представления, проверки, хранения, связанных с цифровыми доказательствами, в том числе процессуальных гарантий, таких как обязательное участие специалиста, послужили устранению основных проблем на практике. Тем не менее, по-прежнему существуют серьезные криминалистические и правовые проблемы с использованием цифровых данных в облаке в качестве доказательств.

Процесс раскрытия преступлений, совершаемых в сфере цифровых технологий, характеризуется высокой степенью сложности, что объясняется применением преступниками различных методов сокрытия, направленных на сокрытие информации, имеющей значение для расследования. Однако актуальность криминалистических исследований в данном направлении определяется современными возможностями криминалистической техники. В частности, с помощью существующих на сегодняшний день специальных программно-аппаратных средств создается возможность в короткие сроки получать важную информацию, в том числе удаленную или зашифрованную, из облачных хранилищ и мобильных устройств участников ситуации. При раскрытии преступлений, совершенных с помощью мобильных устройств и

облачных сервисов, специалисты используют специальные криминалистические методы, применяемые в процессе экспертиз.

На практике существует множество примеров, когда данные из облачных хранилищ способствовали раскрытию уголовных дел. Одним из самых ярких примеров является уголовное дело отца, избившего несовершеннолетнего сына. Отец удалил записанное им видео с своего мобильного устройства, но не учел, что его данные будут автоматически синхронизироваться с облаком. В результате, с помощью специальных программно-аппаратных средств, доказательства из облачного склада были восстановлены, и преступник был наказан.

Кроме того, данные в облачных хранилищах могут сыграть важную роль в расследовании других тяжких преступлений. Например, при расследовании заказанных убийств преступные связи могут быть выявлены путем обмена фотографиями между убийцей и заказчиком или восстановления геоданных.

Облачные данные являются основным объектом цифровой криминалистики и служат источником электронных доказательств для доказывания преступной деятельности. Хотя эти виртуальные базы данных обычно хранят метаданные и пользовательский контент, подтверждающие важные связи между субъектом преступления и его сообщниками, доступ к ним часто остается сложным и ограниченным из-за юридических и технологических барьеров и вопросов юрисдикции.

Поэтому, несмотря на высокую криминалистическую значимость облачных данных, важно уточнить его фундаментальное понятие и технологические основы.

Облачное хранилище (Cloud Storage) - это технологическая модель хранения цифровых данных на одном или нескольких виртуальных серверах или дата-центрах в глобальной сети (чаще всего в Интернете). В отличие от традиционных методов хранения данных (например, жесткий диск персонального компьютера), пользователи могут получить доступ к данным, хранящимся в облаке, в любое время, из любого места, через информационно-коммуникационные сети.

Облачная память отличается тремя основными характеристиками:

1. **Виртуализация:** Точное физическое местоположение данных остается неизвестным пользователю.
2. **Распространенность:** Информация часто хранится на нескольких серверах или в разных юрисдикциях.
3. **Эластичность:** Размер памяти может быстро меняться (расширяться или сужаться) в зависимости от спроса.

С точки зрения уголовно-процессуальной деятельности облачные воспоминания как источник доказательств имеют постоянно меняющийся и трансграничный характер, что порождает специфические проблемы при расследовании и доказывании преступлений.

Сервисы облачного хранилища можно разделить на три типа в зависимости от типа предоставляемых ресурсов: SaaS (Программное обеспечение как услуга), PaaS (Платформа как услуга) и IaaS (Инфраструктура как услуга). Облачные сервисы хранения типа IaaS предоставляют пользователям виртуальное пространство и позволяют хранить такие данные, как документы, изображения, музыкальные файлы. Кроме того, такие сервисы предлагают различные дополнительные услуги, такие как редактирование документов и изображений, музыкальные и видеоплееры, возможность отправки электронной почты.

Более того, большинство облачных сервисов хранения позволяют пользователям получать доступ к своему облачному хранилищу через компьютер или смартфон, что способствовало широкому распространению сервисов.

Процесс доказывания, направленный на правильное разрешение уголовного дела и установление истины, является центральной частью уголовного процесса. Как отмечает Ф.Ю. Бадалбоев, доказательная деятельность носит ретроспективный, формализованный и периодический характер. Основная сущность доказывания - подтверждение наличия обстоятельств, имеющих значение для дела, в отношении любых сведений, собранных субъектами уголовного процесса в установленном законом порядке.

Облачные данные являются основным объектом цифровой криминалистики и служат источником электронных доказательств для доказывания преступной деятельности. Хотя эти виртуальные базы данных обычно хранят метаданные и пользовательский контент, подтверждающие важные связи между субъектом преступления и его сообщниками, доступ к ним часто остается сложным и ограниченным из-за юридических и технологических барьеров и вопросов юрисдикции. Поэтому, несмотря на высокую криминалистическую значимость облачных данных, важно уточнить его фундаментальное понятие и технологические основы.

Процесс раскрытия преступлений, совершаемых в сфере цифровых технологий, характеризуется высокой степенью сложности, что объясняется применением преступниками различных методов сокрытия, направленных на сокрытие информации, имеющей значение для расследования. Однако актуальность криминалистических исследований в данном направлении определяется современными возможностями криминалистической техники.

В частности, с помощью имеющихся на сегодняшний день специальных программно-аппаратных средств создается возможность в короткие сроки получать важную информацию, в том числе удаленную или зашифрованную информацию, из облачных хранилищ и мобильных устройств участников ситуации. При раскрытии преступлений, совершенных с помощью мобильных устройств и облачных сервисов, специалисты используют специальные криминалистические методы, применяемые в процессе экспертиз.

На практике существует множество примеров, когда данные, полученные из облачных хранилищ, помогли раскрыть уголовные дела. Одним из самых ярких примеров является уголовное дело отца, избившего несовершеннолетнего сына. Отец удалил записанное им видео с своего мобильного устройства, но не учел, что его данные будут автоматически синхронизироваться с облаком. В результате, с помощью специальных программно-аппаратных средств, доказательства из облачного склада были восстановлены, и преступник был наказан. Кроме того, данные из облачных хранилищ могут сыграть важную роль в расследовании других тяжких преступлений. Например, при расследовании заказанных убийств преступные связи могут быть выявлены путем обмена фотографиями между убийцей и заказчиком или восстановления геоданных.

Самый сложный аспект расследования преступлений, связанных с облачным хранилищем, заключается в том, что сложно определить, что пользователь делал с момента регистрации до завершения использования сервиса. Файл журнала (записи действий) облачного сервера может рассказать историю действий пользователя. Однако, чтобы защитить личную информацию клиентов, хостинговые компании не хотят раскрывать информацию о облачных серверах.

Тем не менее, расследование уголовных дел, связанных с облачным хранилищем, невозможно, поскольку следы использования сервиса остаются на устройстве пользователя. Хотя пользовательские файлы (документы, фотографии, электронные письма и история Интернета) являются лучшим цифровым доказательством, такие файлы не хранятся на локальном устройстве в облачной среде. Поэтому самый важный момент - где хранятся следы использования сервиса облачных вычислений и как их анализировать с точки зрения цифровой криминалистики. Традиционных методов цифровой криминалистики недостаточно для расследования облачных служб хранения данных. Поэтому для проведения расследования должна применяться не только традиционная компьютерная криминалистика, но и мобильная криминалистика.

При проведении цифровой криминалистики по облачной памяти необходимо проверить все устройства, которые могут получить доступ к

облачной памяти одного пользователя, так как следы, оставленные на компьютерах и смартфонах, дополняют друг друга.

Следователь собирает и анализирует данные со всех устройств (компьютеры, смартфоны, планшетные компьютеры и т. д.), которые пользователь использовал для доступа к облачному хранилищу:

- Система Windows и Mac: Следователь в первую очередь собирает переменные данные (содержание физической памяти, если это возможно). Затем он собирает неизменные данные (nonvolatile data) - историю Интернета, файлы журналов, файлы и каталоги.
- iOS (iPhone): Вы можете проверить резервные копии, хранящиеся на компьютере, или получить и проанализировать данные, используемые для iTunes, непосредственно с iPhone.
- Android: Данные можно получить после рутировки (rooting). Рутирование - это важный процесс для получения данных со смартфонов Android, поскольку доступ к системной папке и получение данных возможны только после рутирования.

Следователь анализирует собранные данные, проверяет наличие следов облачного хранилища и, если таковые имеются, определяет наличие данных учетной записи пользователя (ID и пароль).

Поскольку облачное хранилище в основном является веб-сервисом, сбор и анализ данных, связанных с историей Интернета, очень важны. С помощью файлов журналов веб-браузеров (Chrome, Safari, Internet Explorer и Firefox) можно узнать о действиях пользователя, таких как доступ к облачному хранилищу или вход в систему. Эти файлы журнала:

- Кэш-файлы: Содержат загруженные файлы, URL-адреса, время загрузки и объем данных.
- История: Сохраняет URL-адреса, заголовки веб-страниц и время посещения.
- Файлы cookie: Сохраняет информацию об изменениях и сроках действия файлов cookie, их названиях и значениях.
- Список загрузок: Содержит локальные маршруты и время загрузки загруженных файлов.

Кроме того, многие сервисы облачного хранения предоставляют клиентские приложения для удобства. При установке клиентского приложения в Windows его следы остаются в реестре, файлах журнала и файлах базы данных. Эти файлы очень важны, потому что они содержат следы использования облачного хранилища:

- Журнальные файлы на локальном компьютере содержат информацию о том, были ли логины успешными или неудачными, когда сервисы были

запущены и завершены, и когда файлы были синхронизированы. Это дает основание для создания временной шкалы (timeline).

- Файлы базы данных (Database files) создаются для управления файлами и папками в папках, предназначенных для синхронизации. Они хранят имена папок и файлов, время создания и последнего изменения, а также записи об удалении файлов.
- Среди оставшихся следов на смартфоне следует уделить приоритетное внимание проверке файлов базы данных, XML-файлов и плит-файлов, поскольку они содержат информацию об аккаунтах, синхронизированных и вошедших файлах.

При обеспечении допустимости облачных доказательств необходимо решить три основные правовые проблемы:

1. Облачные данные постоянно меняются. Традиционная "цепочка доказательств" технически неспособна доказать, что доказательство, хранящееся на облачных серверах, не было изменено до или во время хранения. Это особенно важно для доказательств, представленных обвиняемым.
2. Доказательства должны быть получены от поставщика на основании решения суда или согласия клиента. Большинство провайдеров (Amazon, Google) отказывают или задерживают передачу данных в национальные органы из-за своих соглашений об оказании услуг или национального законодательства.
3. Является ли любая копия данных, полученных из облака (оперативная копия, виртуальное изображение), оригиналом или производным доказательством? Эта проблема играет важную роль в оценке доказательственной значимости информации в суде.

В облачной криминалистике существуют вышеуказанные сложные проблемы в сборе и исследовании доказательств, которые напрямую влияют на эффективность следственного процесса.

Традиционные криминалистические методы (например, полное физическое копирование) не используются из-за постоянной работы облачных серверов и риска приостановки работы. Поэтому требуются новые, гибкие методы.

В настоящее время технология блокчейн рассматривается как перспективный механизм гарантирования ненарушения облачных доказательств. Основные характеристики блокчейна - неизменность, разрозненность и криптографическая зависимость каждой операции - являются идеальным решением для создания процессуальной цепочки доказательств.

Механизм работает следующим образом:

- Как только доказательство получено, его хэш-стоимость и время получения (тайм-штамп) записываются в распределенный реестр блокчейна.
- Впоследствии никто (даже провайдер) не сможет изменить эту запись.

Таким образом, блокчейн криптографически гарантирует процессуальный ход доказательств (когда, кем, каким процессуальным действием было получено доказательство) независимо от третьей стороны. Это значительно облегчает бремя доказывания целостности доказательств в суде.

ВЫВОДЫ И ПРЕДЛОЖЕНИЯ

Облачная память играет центральную роль в качестве основного источника доказательств при расследовании и раскрытии киберпреступлений в эпоху информационных технологий. Анализ, рассмотренный в статье, показывает, что, поскольку большая часть цифровых доказательств (более 80%) хранится в облачных сервисах, легальный, быстрый и эффективный доступ к этим данным остается основной актуальной проблемой цифровой криминалистики.

Из-за препятствий в получении доказательств в облаке (юрисдикция, ограниченность сотрудничества провайдера) полагаться только на данные сервера недостаточно. Сочетая методы компьютерной криминалистики и мобильной криминалистики, только анализ следов, оставленных на всех локальных устройствах (ПК, смартфоны), позволяет создать полную временную линию преступной деятельности.

Введение в Уголовно-процессуальный кодекс Республики Узбекистан понятия "цифровое доказательство" создало для следователей важную правовую основу для процессуально правильного использования доказательств, полученных из облачной памяти. Однако постоянно меняющийся и трансграничный характер облачной среды все еще вызывает проблемы в доказательстве допустимости и целостности аргументов.

Обеспечение неизменности облачных доказательств является ключевым условием. Технология блокчейн предлагается в качестве решения именно этой проблемы, гарантируя ненарушение цепочки доказательств и облегчая бремя доказывания в суде путем криптографической фиксации хэш-стоимости и времени получения доказательств.

Список литературы

1. Закон Республики Узбекистан (No ЗРУ-1003). О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан, направленных на совершенствование системы работы с цифровыми доказательствами. - Ташкент, 21 ноября 2024 года.
2. Cybersecurity Ventures. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. — Sausalito, Calif.: Cybercrime Magazine, 2025.
3. Бадалбоев Ф.Ю. Роль “цифровых доказательств” в системе уголовно-процессуального доказывания // Science Box. ОНЛАЙН НАУЧНЫЙ

ЖУРНАЛ "СТАБИЛЬНОСТЬ И ВЕДУЩИЕ ИССЛЕДОВАНИЯ." Том: 04, Издание: 12. Декабрь 2024.

4. Кодирова М.Х. Учебное пособие по доказательствам и доказыванию в уголовном процессе. Т:-ТДЮУ. 2024 г.
5. Исабаев Ё.Ж. Проблемы развития средств доказывания в уголовном процессе. Proceedings of International Conference on Scientific Research in Natural and Social Sciences Hosted online from Toronto, Canada.