Критерии классификации электронных (цифровых) доказательств: Современные подходы и проблемы систематизации

Гулимова Дилшода Аллоёр кизи
Базовый Докторант кафедры Международного права и прав человека
Ташкентский Государственный Юридический Университет
dilshodaallayarovna@gmail.com
+998996920008

Аннотация. В статье исследуются теоретические и практические проблемы систематизации цифровых доказательств в современном уголовном процессе. Анализируется влияние эволюции информационных технологий на подходы к классификации виртуальных следов преступлений. Обосновывается, что традиционная дихотомия вещественных доказательств и документов неприменима к цифровой среде, поскольку электронная информация обладает самостоятельной правовой природой (sui generis). Ввиду разрозненности доктринальных подходов и усложнения структуры транснациональной киберпреступности, в статье предложена комплексная авторская классификация электронных (цифровых) доказательств, учитывающая их генезис, локализацию, способ фиксации и процессуальную функцию.

Ключевые слова: цифровые доказательства, электронные доказательства, классификация доказательств, виртуальные следы, киберпреступность, облачные вычисления, международный уголовный процесс.

ВВЕДЕНИЕ

В условиях глобальной цифровизации и стремительного роста транснациональной киберпреступности международное правоохранительное сообщество сталкивается с серьезными вызовами в сфере расследования уголовных дел. Виртуализация преступной среды привела к тому, что подавляющее большинство следов преступлений сегодня формируется в цифровом пространстве. Электронные доказательства в настоящее время играют решающую роль не только в расследовании киберпреступлений, но и в делах о традиционных видах транснациональной преступности.

Однако правовая наука и правоприменительная практика сталкиваются с серьезной проблемой: доктрина международного уголовного процесса и национальные юрисдикции до сих пор не выработали терминологического единства в отношении цифровых следов.

Параллельно используются такие дефиниции, как «компьютерная информация», «электронное доказательство», «цифровое доказательство» и «цифровой след». Отсутствие единого терминологического аппарата и, как следствие, общепризнанной классификации таких доказательств порождает коллизии при исполнении международных запросов о правовой помощи, замедляет процесс трансграничной передачи данных и создает риски признания полученных доказательств недопустимыми.

1. ЭВОЛЮЦИЯ ДОКТРИНАЛЬНЫХ ПОДХОДОВ К ПРИРОДЕ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ

Проблема классификации неразрывно связана с генезисом самого понятия «цифровое доказательство», развитие которого можно разделить на три ключевых этапа. На начальном

.

(«машинном») этапе информация не мыслилась в отрыве от ее физического носителя. Соответственно, компьютерные носители информации рассматривались преимущественно как разновидность традиционных вещественных доказательств. Такой подход делал классификацию элементарной (по типу физического носителя: жесткие диски, магнитные ленты), но процессуальное значение придавалось не столько самой виртуальной информации, сколько материальному объекту, который ее хранит. Развитие Интернета ознаменовало переход к сетевому периоду, где информация стала легко передаваться на огромные расстояния без физического перемещения носителя. Именно Конвенция о киберпреступности 2001 года заложила основу для работы с «электронными доказательствами». На этом этапе стало очевидно, что электронное доказательство по своей гносеологической природе принципиально отличается от бумажного документа, так как оно создается, хранится и передается в форме, недоступной для непосредственного человеческого восприятия без использования специальных технических средств. Следообразование в компьютерной среде происходит на логическом, а не на физическом уровне. Ученые начали указывать на ограниченность классической дихотомии «вещественное доказательство - иной документ» применительно к цифровой среде.

Современный («облачный») период окончательно оторвал данные от конкретного устройства пользователя и конкретной территории. Один и тот же массив информации может быть фрагментирован и распределен по серверам, находящимся в десятках различных государств. Это приводит к состоянию «утраты локализации» (loss of location). Термин «цифровой» более точно отражает бинарную природу информации независимо от физического способа ее передачи. Сегодня все большую поддержку находит концепция признания цифрового доказательства самостоятельным видом доказательств (sui generis). Цифровая информация обладает специфическими свойствами: неограниченная тиражируемость без потери качества оригинала, подверженность скрытой модификации, способность к мгновенной трансграничной передаче. Эти свойства делают невозможным прямое применение к цифровым доказательствам правил собирания и оценки, разработанных для классических документов или вещественных доказательств.

Отсутствие унифицированной классификации цифровых доказательств обусловлено несколькими факторами:

• **Технологическая динамика:** Скорость появления новых форматов данных (криптовалютные транзакции, логи IoT-устройств, метавселенные) опережает процесс правотворчества. Применение старых правовых концепций к виртуальным данным без учета их специфики приводит к существенному нарушению баланса между интересами следствия и правами личности на приватность.

• **Трансграничный характер:** В международном процессе для трансграничного обмена цифровыми доказательствами требуются специальные механизмы, базирующиеся на признании цифрового доказательства уникальным правовым феноменом. Однако разные юрисдикции классифицируют одни и те же данные по-разному (например, как "иные документы" в одной стране и как "вещественные доказательства" в другой).

• **Многослойность цифровых данных:** Любой цифровой файл состоит из основного содержания (payload) и метаданных (данных о данных). Правовая оценка этих слоев часто требует различных процессуальных режимов доступа.

Авторская классификация цифровых доказательств

Опираясь на то, что эволюция доктринальных взглядов демонстрирует поступательное движение к признанию самостоятельной процессуальной и информационной ценности виртуального следа, мы предлагаем многоуровневую классификацию цифровых доказательств. Данная система критериев позволяет не только структурировать криминалистическое

.

понимание цифровых следов, но и дифференцировать процессуальные механизмы их сбора и оценки.

Классификация по источнику (субъекту) формирования

Этот критерий имеет решающее значение для оценки достоверности доказательства и определения необходимости назначения компьютерно-технической экспертизы.

1. **Созданные человеком (Human-generated data):** Данные, содержание которых напрямую зависит от волеизъявления человека (электронные письма, текстовые сообщения в мессенджерах, документы Word/PDF, посты в социальных сетях). Оценка таких доказательств сфокусирована на идентификации автора и семантическом анализе содержания.
2. **Сгенерированные компьютером (Computer-generated data):** Данные, которые создаются автоматизированными системами без прямого участия человека (системные логи, записи в реестрах операционной системы, данные биллинга, координаты GPS, метаданные EXIF). Они обладают высокой степенью объективности, но требуют специальных знаний для их интерпретации.
3. **Смешанные (Composite data):** Результат взаимодействия человека и машины (например, финансовые транзакции в онлайн-банкинге или операции с криптовалютой, где человек инициирует перевод, а система генерирует криптографические хеши и логи маршрутизации).

Классификация по степени локализации и доступности

Данный критерий учитывает современные реалии "облачного периода" и фрагментацию данных, решая проблему юрисдикционных границ.

1. **Локальные (изолированные) доказательства:** Данные, физически находящиеся на изъятом устройстве (жесткий диск ПК, память смартфона), не требующие сетевого доступа для их извлечения.
2. **Сетевые (транзитные) доказательства:** Информация, перехваченная в момент ее передачи по каналам связи (сетевой трафик, перехват пакетов данных). Сбор таких доказательств требует проведения специальных оперативно-розыскных мероприятий в режиме реального времени.
3. **Облачные (распределенные) доказательства:** Данные, хранящиеся на удаленных серверах (часто за рубежом) или в децентрализованных сетях (блокчейн). Изъятие таких доказательств требует направления запросов о взаимной правовой помощи (MLAT) или использования механизмов, предусмотренных Вторым дополнительным протоколом к Будапештской конвенции.

Классификация по информационной структуре

Понимание структуры необходимо для правильного процессуального оформления (осмотра) виртуального следа.

1. **Контентные данные (Content data):** Непосредственное содержание коммуникации или файла (текст письма, изображение, видеозапись).
2. **Метаданные (Metadata):** Сведения о свойствах и характеристиках контентных данных (время создания файла, IP-адрес отправителя, геометки, информация об устройстве). В контексте доказывания метаданные часто имеют большую ценность, чем сам контент, так как позволяют установить время и место совершения деяния.
3. **Абонентские данные (Subscriber info):** Базовая информация, идентифицирующая пользователя в системе (ФИО, номер телефона, привязанная банковская карта, история платежей за услуги связи).

Классификация по криптографическому состоянию

Критерий, напрямую влияющий на техническую возможность использования доказательства в суде.

.

1. **Открытые (незашифрованные) данные:** Информация доступна для непосредственного чтения и анализа с помощью стандартного программного обеспечения.

2. **Зашифрованные (Encrypted) данные:** Информация подвергнута криптографическому преобразованию (сквозное шифрование в мессенджерах, зашифрованные контейнеры). Использование таких доказательств зависит от возможности получения ключей дешифрования.

3. **Скрытые (Стеганографические) данные:** Информация, факт существования которой умышленно скрыт (например, текстовое сообщение, программно встроенное в пиксели безобидного цифрового изображения).

ВЫВОДЫ

Традиционная доказательственная парадигма, ориентированная на физические объекты, исчерпала себя в контексте борьбы с современной киберпреступностью. Переход к пониманию цифровых доказательств как явления sui generis требует не только изменения терминологии, но и глубокой перестройки процессуальных институтов.

Предложенная авторская классификация по источникам формирования, локализации, структуре и криптографическому состоянию позволяет:

Во-первых, четко разграничить правовые режимы доступа к различным типам виртуальной информации (одно дело - осмотр локального жесткого диска, другое - трансграничный запрос биллинга из облачного хранилища).

Во-вторых, стандартизировать подходы следователей и судей к оценке допустимости и достоверности электронных улик. Унификация понятийного аппарата и системы классификации на международном уровне является критически важным условием для обеспечения эффективного трансграничного обмена доказательственной информацией в борьбе с транснациональной киберпреступностью.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. United Nations Office on Drugs and Crime (UNODC). Practical Guide for Requesting Electronic Evidence Across Borders. - Vienna: United Nations, 2019.

2. Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. - 3rd ed. - Academic Press, 2011.

3. Recommendation No. R (95) 13 of the Committee of Ministers to Member States concerning problems of criminal procedural law connected with information technology. - Council of Europe, 1995.

4. Конвенция о киберпреступности (ETS N 185) (Заключена в г. Будапеште 23.11.2001) // Бюллетень международных договоров. - 2005.

5. Mason, S. Electronic Evidence. – 4th ed. – London: Institute of Advanced Legal Studies for the SAS Humanities Digital Library, 2017.

6. Мещеряков, В. А. Следы преступлений в сфере высоких технологий // Библиотека криминалиста. Научный журнал. - 2013. - № 5.

7. Clough, J. Principles of Cybercrime. – 2nd ed. – Cambridge: Cambridge University Press, 2015.

8. Зуев, С. В. Электронные копии как самостоятельный вид доказательств // Законность. - 2018. - № 10.

9. Kerr, O. S. Searches and Seizures in a Digital World // Harvard Law Review. – 2005. - Vol. 119, No. 2.

10. (Дополнительная литература может быть добавлена автором при дальнейшей подготовке к публикации)

.