

ОБЕСПЕЧЕНИЕ ДОСТОВЕРНОСТИ ЦИФРОВЫХ ФОТОСНИМКОВ



Владислав ШАЛЬКЕВИЧ,
старший прокурор отдела
Генеральной прокуратуры
Республики Беларусь,
юрист 2 класса,
кандидат юридических наук

Одним из дополнительных средств фиксации доказательственной информации является фотосъемка. Она применяется при производстве практически всех следственных действий. Первоначально фотофиксация проводилась с использованием пленочных фотоаппаратов. Но быстрое развитие микропроцессорных технологий совершило революцию в этой области, вследствие чего широкое распространение получила цифровая фотоаппаратура.

К преимуществам цифровой фотографии по отношению к аналоговой относятся: простота осуществления съемки, возможности оперативно контролировать результаты съемки и производить печать фотоснимков, минуя стадию лабораторной обработки; большие емкости машинных носителей информации (далее — МНИ)*.

Цифровые фотографии, как и аналоговые, должны в неизменном виде сохранять первоначальное содержание доказательственной информации, фиксируемой в ходе следствен-

ного действия: то есть информация, содержащаяся на МНИ (цифровые фотоснимки), должна оставаться неизменной на любой стадии уголовного процесса. При этом в аналоговой фотографии существует эталон в виде негатива, с которым фотографию можно сравнить, в то время как технология цифровой фотосъемки создание негатива или иного объекта со схожими функциями не предусматривает. Поэтому, чтобы сделать возможным применение в уголовном процессе цифровой фотографии, должны быть найдены и внедрены в практику средства, во-первых, гарантирующие, что ни по каким причинам умышленного или случайного характера цифровые фотоснимки не изменились, и, во-вторых, позволяющие выявить факты внесения изменений, если такового производились.

В современной криминалистической литературе дано немало рекомендаций и методических указаний, направленных на решение этой задачи. Но они не устраняют проблемы. Это связано с тем, что в мире цифровых технологий безопасность — это процесс, а не продукт [12, с. 12]. И только путем применения научно обоснованной **системы правовых, технических, программных, организационных решений** могут быть обеспечены защита информации, передаваемой, обрабатываемой, хранящейся в цифровом виде, и, следовательно, ее достоверность.

По содержанию предлагаемых мер данные рекомендации можно разделить на несколько групп.

Первая группа рекомендаций, разработанных А.Е. Гучком и Г.А. Шумаком [6], Л. Исаевой [7], для обеспечения достоверности цифровых фотоснимков предусматривала изымать МНИ сразу после съемки следствен-

* В ст. 1 Закона Республики Беларусь “Об электронном документе” машинный носитель информации определяется как магнитный диск, магнитная лента, лазерный диск и иные материальные носители, используемые для записи и хранения информации с помощью электронно-вычислительной техники [10]. В нашем случае это флеш-карта, применяемая в цифровом фотоаппарате в качестве МНИ (примеч. авт.).

ного действия, упаковывать и печатывать, заверяя подписями следователя и понятых. Изготавливать фототаблицы рекомендовалось позднее, в ходе следственного осмотра МНИ. Решение проблемы обеспечения достоверности цифровых фотоснимков ограничивалось лишь организационными мерами, без учета цифровой природы этого объекта.

Второй подход, которого придерживались В. Антонов [1], М. Вандер [3], Г. Мухин [9], заключается в печати фотографий и записи файлов с фотоснимками, фиксирующими ход и результаты следственного действия, на диски CD-R (DVD-R) непосредственно в ходе следственного действия. Однако и такой подход небезупречен. Диски CD-R (DVD-R) являются одноразовыми МНИ, но существуют режимы записи, позволяющие в некоторых случаях дописывать на них информацию путем добавления следующей сессии (сессий), и так до исчерпания свободного пространства. Гипотетически представим ситуацию, когда на диск, априорно считающийся диском одноразовой записи, будет произведена запись дополнительной сессии (модифицированных фотоснимков). При этом файлы предыдущей сессии (то есть записанные в ходе следственного действия) могут стать недоступны стандартным средствам операционной системы (например, проводнику Windows). Кроме того, файлы с фотографиями, записанные во время дополнительной сессии (модифицированные фотоснимки), могут обладать теми же метаданными*, что и файлы основной сессии. Это определяется тем, что средства операционной системы, включающей в качестве подсистемы файловую систему, не обеспечивают контроля за изменением этой информации и, следовательно, она может быть модифицирована произвольным образом [8]. Задачу установления хронологической последовательности записи сессий возможно решить в ходе производства судебной компьютерно-технической экспертизы или следственного осмотра МНИ с участием специалиста.

Третий подход разработан Ю. Пономаренко и С. Молчановым [11]. Они предлагают обеспечивать защиту цифровых фотоснимков с помощью технологии **элек-**

тронной цифровой подписи (далее — ЭЦП). Верный по существу, такой подход, тем не менее, технологически избыточен. Это связано с тем, что в электронном документообороте средствами ЭЦП обеспечивается решение двух задач:

1. однозначного определения автора сообщения (аутентификация);
2. подтверждения целостности и неизменности содержания электронного документа [2, с. 72].

В случае, если источник сообщения совпадает с лицом, от имени которого оно распространяется (аутентичность), и содержание сообщения не изменилось в канале связи, можно сделать вывод, что информация, содержащаяся в электронном документе, является достоверной.

Задачи, решаемые путем применения ЭЦП в электронном документообороте, в уголовном процессе представлены лишь частично: здесь не требуется подтверждать авторство, необходимо лишь обеспечивать проверку целостности и неизменности информации.

Кроме того, для использования описанной технологии потребуются значительные финансовые затраты на разработку и сертификацию программных и аппаратных средств ЭЦП, создание и поддержание инфраструктуры открытых ключей проверки подписи.

Четвертую группу составляют рекомендации по применению ряда информационных технологий, использование которых ошибочно (стеганография [4]) или допустимо с существенными ограничениями и оговорками (программы для редактирования изображений, например, Photoshop [5]).

Стоящая перед нами частная задача — обеспечение достоверности цифровых фотоснимков, в общем виде может быть сформулирована так: обеспечение проверки достоверности информации, генерируемой, передаваемой, обрабатываемой и хранящейся в цифровом виде. Такая задача возникает и успешно решается в различных областях науки и техники путем использования **хеш-функции (hash function)**, под которой понимается некоторое математическое преобразование, обладающее следующими свойствами:

1. Хеш-функция может быть применена к **аргументу любого размера**. Аргументом в нашем случае является файл, содержащий цифровую фотографию. Его размер не имеет значения.

* К метаданным в зависимости от типа файловой системы и графического формата изображения относятся: имя и расширение файла; атрибуты файла; время создания, доступа, модификации файла (MAC-time); EXIF-информация (если формат файла jpeg) и др.

2. Результат этого преобразования, называемый **хеш-значение** (hash value)*, имеет **фиксированный размер**. То есть, независимо от размера обрабатываемого файла результатом хеширования будет последовательность двоичных цифр (бит) фиксированной длины. При этом следует иметь в виду, что хеш-значение **зависит только от содержания файла** со снимком и **не зависит от внешних данных** (метаданных).

3. Она должна быть **устойчива к коллизиям**. Это означает, что невозможно (или, с вычислительной точки зрения, очень сложно) подобрать другой файл, имеющий такое же хеш-значение. Поэтому в иностранной литературе хеш-значение иногда называют *fingerprint* (дактилоскопический отпечаток пальца), проводя аналогию с уникальностью папиллярных узоров пальцев рук человека.

4. Она должна быть **необратимой** — по известному хеш-значению невозможно (или, с вычислительной точки зрения, очень сложно) восстановить исходные данные.

В настоящее время в судебно-экспертной практике получили распространение следующие алгоритмы расчета хеш-значения: MD5, SHA-1. Применяемый алгоритм определяет длину хеш-значения, которая может быть 128, 256, 384, 512 и более бит. Для удобства использования хеш-значения представляют не в двоичной системе исчисления, а в шестнадцатиричной.

В электронном документообороте результат применения хеш-функции, называемый дайджест сообщения, выступает в качестве одного из элементов ЭЦП. Упрощенно схема его использования выглядит следующим образом. Для сообщения (электронного документа) средствами ЭЦП вычисляется по известному алгоритму дайджест сообщения, который затем передается вместе с сообщением. Получатель сообщения в свою очередь рассчитывает дайджест сообщения для полученного электронного документа и сравнивает его с имеющимся. Если они совпадают, то сообщение (электронный документ) при передаче не изменилось. В электронном документообороте дайджест сообщения служит **эталоном** для сравнения, в результате которого подтверждается неизменность сообщения.

* В различных областях науки и техники используют следующие термины, обозначающие результат применения хеш-функции: хеш-значение (hash value); свертка сообщения, дайджест сообщения (message digest); хеш (hash).

В судебной фотографии в качестве эталона (образца для сравнения) для аналоговых фотоснимков выступает негатив. Мы предлагаем **в качестве эквивалента негатива в цифровой фотографии использовать хеш-значение**.

На практике поставленная задача (удостоверение неизменности файла, содержащего фотоизображение) может решаться путем применения программного обеспечения, реализующего один из алгоритмов хеширования данных. Это может быть, например, программа **MD5 File Hash Utility****, реализующая алгоритм MD5.

Для вычисления хеш-значения необходимо выделить в проводнике Windows файл (файлы) с фотографией и “перетянуть” их в окно программы. Затраты времени на расчет хеш-значения для файла (файлов) минимальны. В этой версии программы существует ограничение — одновременно могут обрабатываться не более 500 файлов (рис. 1).

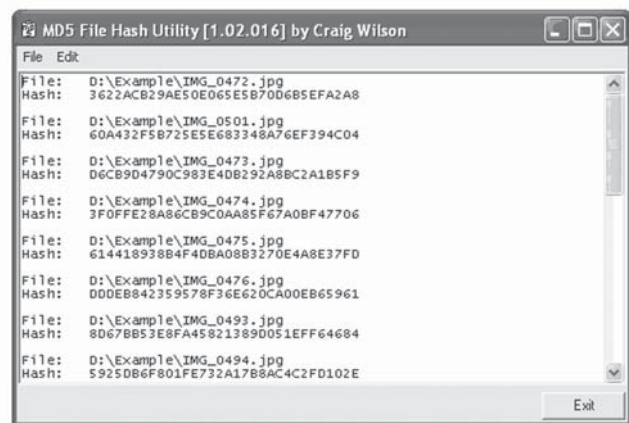


Рис. 1

Из окна программы все данные (имя файла, путь к нему, хеш-значение) должны быть скопированы и помещены в протокол следственного действия с указанием использованного программного средства и алгоритма, применявшегося для расчета. После этого файлы с фотографиями и файл с хеш-значениями могут быть записаны на любой МНИ для хранения.

Составляя фототаблицу, необходимо каждое изображение сопровождать сведениями о хеш-значении и применявшемся для его расчета алгоритме (рис. 2).

Впоследствии, в случае возникновения сомнения в достоверности фотоснимков, прило-

** Программа MD5 File Hash Utility может быть загружена с сайта <http://www.digital-detective.co.uk>. По условиям лицензионного соглашения она может бесплатно и свободно использоваться лицами, работающими в правоохранительной сфере.



IMG_0765.jpg

Хеш-функция: MD5

Хеш-значение: ED870202082EA4FD8F5488533A561B35

Рис. 2



IMG_0765.jpg

Хеш-функция: MD5

Хеш-значение: 1CADF4168FAC3EEBFB3FA6747115762

Рис. 3

женных к протоколу следственного действия в виде фототаблиц, нет необходимости проводить какие-либо экспертные исследования. Для установления факта модификации фотоснимка достаточно повторить процедуру расчета хеш-значения для сохраненных файлов с фотоснимками. В этих целях может быть использовано **любое** коммерческое либо свободно распространяемое программное обеспечение (например, EnCase, FTK Imager, MD5 File Hash Utility, Hasher из пакета ILook 8), реализующее алгоритм расчета хеш-значения, который был применен первоначально (в рассматриваемом нами случае — алгоритм MD5). Результаты (хеш-значения) следует сравнить и на основании этого сделать вывод о достоверности (или недостоверности)

информации, зафиксированной на цифровом фотоснимке (рис. 3).

Цифровая природа информации делает применение хеш-функций независимым от содержания информации. В данной статье описано использование хеш-функций для установления неизменности файла, содержащего цифровой фотоснимок. Однако этот же метод может быть применен и к файлам с текстовым документом, звуко- или видеозаписью следственного действия, зафиксированного цифровым устройством.

Использование хеш-функции в ближайшее время должно получить широкое распространение в следственной практике для обеспечения проверки достоверности информации, имеющей цифровую природу.

Список цитированных источников

1. Антонов, В.П. Использование цифровой фотографии при производстве следственных действий / В.П. Антонов // Вестник криминалистики. — 2007. — Вып. 1 (21). — С. 67—72.
2. Брассар, Ж. Современная криптология / Ж. Брассар. — М.: Издательско-полиграфическая фирма "Полимед", 1999. — 176 с.
3. Вандер, М. Цифровая фиксация аудио- и видеoinформации / М. Вандер, А. Холопов // Законность. — 2003. — № 8. — С. 38—40.
4. Газизов, В.А. К вопросу об использовании цифровой фотографии в расследовании преступлений / В.А. Газизов // Вестник криминалистики. — 2003. — Вып. 2 (6). — С. 81—85.
5. Газизов, В.А. Об использовании цифровых технологий при фиксации хода и результатов следственных действий / В.А. Газизов // Вестник криминалистики. — 2007. — Вып. 2 (22). — С. 64—71.
6. Гучок, А.Е. Процессуальные вопросы применения цифровой фотографии и видеозаписи при расследовании преступлений / А.Е. Гучок, С.Г. Молчанов, Г.А. Шу-

мак // Бюллетень главного управления предварительного расследования МВД Республики Беларусь. — 2004. — № 21—22. — С. 366—372.

7. Исаева, Л. Новые виды фотосъемки при осмотре места происшествия / Л. Исаева // Законность. — 2003. — № 8. — С. 15.

8. Кэрриэ, Б. Криминалистический анализ файловых систем / Б. Кэрриэ. — СПб.: Питер, 2007. — 480 с.

9. Мухин, Г. Фиксация доказательственной информации с использованием цифровой фотосъемки / Г. Мухин, В. Логвин // Судовы веснік. — 2007. — № 3. — С. 63—65.

10. Об электронном документе: Закон Респ. Беларусь, 10 янв. 2000 г., № 357-З; в ред. Законов Респ. Беларусь от 29.06.2006 г. № 137-З, от 20.07.2006 г. № 162-З // Консультант Плюс: Беларусь. Технология 3000 [Электронный ресурс] / ООО "ЮрСпектр". — Минск, 2008.

11. Пономаренко, Ю. Цифровая фотография в криминалистике: проблема защиты информации / Ю. Пономаренко, С. Молчанов // Проблемы правовой информатизации. — 2003. — Выпуск 6. — С. 203—206.

12. Шнайер, Б. Секреты и ложь. Безопасность данных в цифровом мире / Б. Шнайер. — СПб.: Питер, 2003. — 368 с.