УДК 343.98

О. А. Слащинин
следователь главного следственного управления
Следственного комитета Республики Беларусь

ИСПОЛЬЗОВАНИЕ ХЕШ-ФУНКЦИЙ В УГОЛОВНОМ ПРОЦЕССЕ

Функции хеширования (хеш-функции) получили широкое распространение при осуществлении криптографических методов обработки и защиты информации. Вычисление значений функций хеширования (далее — хеш-суммы) применяется для реализации процедур электронной цифровой подписи, проверки целостности передаваемых данных [1, с. 1–2], обеспечения работы технологии блокчейн, функционирования аутентификации в электронных системах защиты, построения уникальных идентификаторов для массива данных, а также для решения иных узкоспециализированных задач. В свою очередь, хеш-функции могут применяться для криминалистического обеспечения оценки доказательств и расследования любых видов преступлений, где фигурирует информация цифровой природы. Теоретическая возможность применения хеш-функций в уголовном процессе (в частности, при оценке достоверности цифровых фотографий и иной электронной информации) ранее обосновывалась учеными-криминалистами [2; 3]. В целях дополнительного обоснования вышеуказанной возможности предлагается рассмотреть сущность хеш-функций в их самом упрощенном виде, а также проблемы, которые могут возникнуть при их использовании.

Сущность рассматриваемой технологии. Функция хеширования заключается в преобразовании входных данных произвольного размера посредством определенного математического алгоритма в битовую строку фиксированного размера, т. е. вычислении их хеш-суммы.

1. Входные данные. В связи с тем, что электронные файлы (далее — файл) любого формата представляют собой массив данных той или иной системы счисления (например, двоичный код: BY значится как 01000010 01011001), они могут преобразовываться (кодироваться по разрядности) в различные битные форматы. Данному преобразованию подлежат любые данные, независимо от их размера (1 байт — 1 терабайт) или формата (текст, графика, звук, видео и иные).

2. Математический (криптографический) алгоритм. Вычисление хеш-суммы входных данных произвольного размера производится по специально разработанным алгоритмам, основанным на различных математических

операциях (деление/умножение и иные). Так, заданный алгоритм преобразует входные данные в необходимую для его работы разрядность, после чего уже высчитывает хеш-сумму из полученного массива. Существуют различные семейства алгоритмов (например, CRC*, MD*, SHA* и иные) со своими свойствами, преимуществами и недостатками.

3. Битовая строка. Результатом преобразования входных данных конкретным математическим алгоритмом является битовая (цифро-буквенная) строка (например, 128/160/256-битные и иные размеры вывода). Указанный размер заранее установлен соответствующим алгоритмом и почти не зависит от размера входных данных (даже в случае, если их двоичный код (блоки) во много раз превосходит количество бит, заданных алгоритмом). Это связано с тем, что в зависимости от битного формата — 128/160/256-бит — различные входные данные в двоичной системе могут иметь большое количество уникальных хеш-сумм: 2^{128}, 2^{160}, 2^{256} соответственно (рисунок 1).

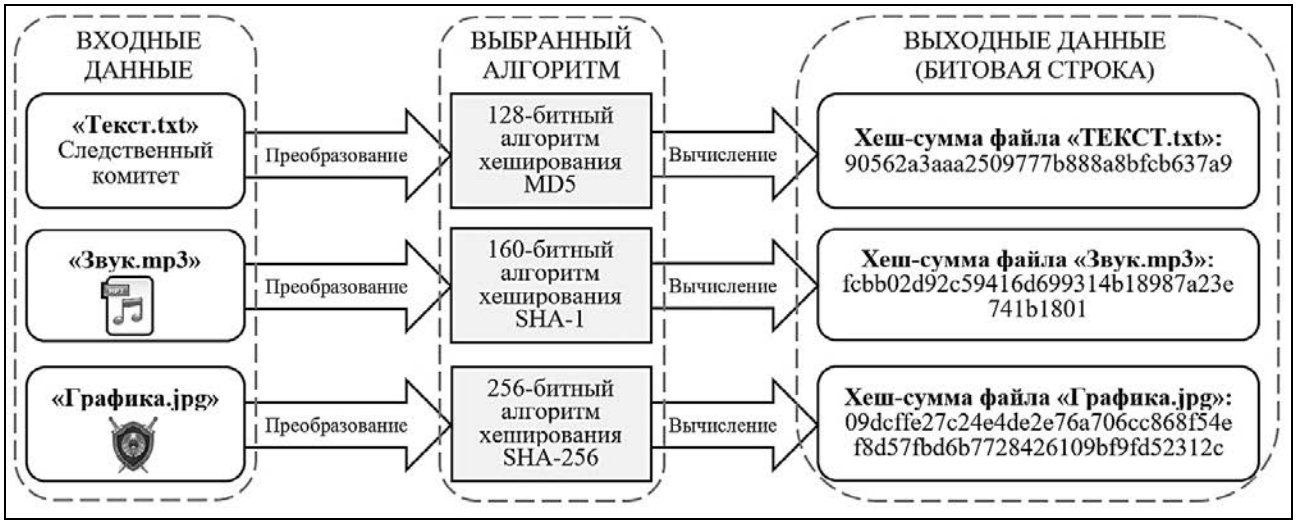

Рисунок 1 — **Пример реализации хеш-функции с файлами различных форматов (разделение функции на преобразование и вычисление является условным)**

Проблема использования хеш-функций. Существование в настоящее время множества алгоритмов связано с совершенствованием подходов к их разработке, постепенным устареванием и закономерным несоответствием отдельных хеш-функций текущим требованиям безопасности. Чтобы хеш-функция считалась криптографически стойкой, она должна быть детерминированной, необратимой и стойкой к коллизиям. Стоит отметить, что отдельными государственными и международными стандартами могут устанавливаться и иные требования (свойства), предъявляемые к хеш-функциям при выполнении конкретных практических задач (например, скорость вычисления хеш-суммы).

1. Детерминированность. Используемая хеш-функция при любых обстоятельствах, не касающихся изменения самого алгоритма, должна из имеющихся неизменных входных данных вычислять одну и ту же хеш-сумму.

2. Необратимость. Указанное свойство означает, что из битовой строки вычислить входные данные было бы невозможно или у этого имелась низкая вероятность, связанная с вычислительными сложностями данного процесса.

3. Устойчивость к коллизиям. В криптографии коллизией обозначается случай, при котором хеш-функция преобразует несколько массивов разных по содержанию входных данных в одинаковую битовую строку. Стоит отметить, что коллизии всегда будут присущи для любой хеш-функции в связи с тем, что разнообразность входных данных бесконечна, а количество уникальных хеш-сумм ограничено определенным размером битовой строкой. Хеш-функция может считаться относительно устойчивой к коллизиям, когда вероятность их обнаружения настолько мала, что для этого необходимы годы вычислений, т. е. при отсутствии более быстрого способа, чем полный перебор значений. Например, если хеш-функция используется для реализации процедур электронной цифровой подписи, то умение находить для нее коллизии равносильно возможности ее подделать. Так, устойчивая к коллизиям хеш-функция при изменении третьими лицами оригинального массива входных данных должна вычислять другую битовую строку, которая никак не должна коррелировать с ранее вычисленной битовой строкой первоначального массива. На основе вышеуказанных положений представляется возможным установить основную проблему использования хеш-функций: теоретическая возможность компрометации (взлома) используемого криптографического алгоритма.

Рассмотренные сущность и свойства хеш-функций позволяют определить возможности их использования при ведении уголовного процесса, а именно: 1) присвоение установленным в ходе предварительного расследования файлам соответствующих идентификаторов (хеш-сумм), на основании которых может производиться последующий поиск их дубликатов, исключение или сравнение (не-)интересующих массивов данных при осмотре (исследовании) электронных носителей информации участников уголовного процесса; 2) проверка целостности и неизменности (подлинности) ранее установленных файлов после их записи на другие носители информации, а также при движении материалов уголовного дела и находящихся при них носителей информации между органами, ведущими уголовный процесс; 3) установление факта модификации компьютерной информации в файлах, в том числе при расследовании обстоятельств внедрения в их содержимое вредоносных программ. Касательно использования

хеш-функций в уголовном процессе стоит отметить, что проблема их компрометации актуальна и для данной области их применения.

Решение данной проблемы заключается в выборе криптографически стойкого алгоритма, компрометация которого на момент его использования, согласно экспертным оценкам, теоретически (математически) сопоставима с вероятностью обнаружения двух людей с идентичными следами пальцев рук.

Список основных источников

1. Информационная технология. Защита информации. Функция хэширования : СТБ 1176.1-99. Минск : БелГИСС, 2001. 16 с. Вернуться к статье

2. Шалькевич В. Обеспечение достоверности цифровых фотоснимков // Законность и правопорядок. 2008. № 1 (5). С. 51–54. Вернуться к статье

3. Федотов Н. Н. Форензика — компьютерная криминалистика. М. : Юрид. Мир, 2007. 432 с. Вернуться к статье