13. *Shamir A.*, *Biryukov A.*, *Perrin L. P.* Summary of an Open Discussion on IoT and Lightweight Cryptography // Proceedings of Early Symmetric Crypto workshop, 2017. University of Luxembourg, 2017.

УДК 004

М. С. Уфимцев
Научный руководитель: канд. тех. наук, доц. А. Н. Соколов
Южно-Уральский государственный университет, Челябинск

ИЗВЛЕЧЕНИЕ ПОБИТОВЫХ ОБРАЗОВ ФИЗИЧЕСКИХ УСТРОЙСТВ ХРАНЕНИЯ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ РАССЛЕДОВАНИЙ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. В работе рассматриваются основные проблемы, возникающие при извлечении побитовых образов физических устройств хранения информации. Рассмотрены возможные методы их решений. Охарактеризована правовая сторона вопроса и произведен поиск возможных критериев оценки эффективности операций по снятию образов.

Ключевые слова: инциденты информационной безопасности; форензика; расследование инцидентов информационной безопасности.

Специфика проведения расследовании инцидентов информационной безопасности требует максимально возможного сохранения неизменности исследуемых данных. Любой цифровой объект, с которым предстоит работать исследователю конкретного инцидента, представлен в виде компьютерной информации. Такой объект достаточно просто уничтожить, причем деструктивное воздействие может носить как умышленный, так и случайный характер.

Обеспечить полную неизменность компьютерной информации на любом носителе информации не представляется возможным за счет программно-аппаратной прослойки механизмов-посредников (работающих по принципу черного ящика) между информацией и исследователем. Примером может служить содержащийся в контроллере SSD-накопителя алгоритм ремапинга ячеек флеш-памяти, который при возникновении критических ошибок чтения/записи в ячейке сохраняет логическую структуру содержащейся в микросхеме памяти информации путем переноса сбойных ячеек в резервную область, тем самым нарушая исходную физическую структуру. В ряд этих проблем можно включить и продвинутые механизмы TRIM и garbage collection [1]. Вместо по-

нятия «неизменность» предпочтительнее использовать термин «целостность». В данном случае подразумевается, что информация в процессе хранения и передачи может сменять носители, перекодироваться, проходить через любые интерфейсы, использующие самые различные механизмы коррекции ошибок: требуется лишь обеспечить совпадение первоначальной информации, находящейся на носителе до исследования, с конечной. Причем критерий точности — совпадение до одного бита [2].

Обратимся к Федеральному закону от 28.07.2012 № 143-ФЗ [3]. Если в зарубежной практике вопрос целостности данных при исследовании инцидентов информационной безопасности достаточно серьезно проработан, то в России первые упоминания в сколь-либо серьезных нормативных актах появляются лишь в 2012 году. Представленный выше ФЗ вносит изменение в Уголовно-процессуальный кодекс Российской Федерации (п. 9.1 в статью 182 и п. 3.1 в статью 183) [4], которое затрагивает вопрос изъятия электронных носителей информации при проведении обыска. Присутствующая формулировка: «При производстве обыска не допускается копирование информации, если это может воспрепятствовать расследованию преступления либо, по заявлению специалиста, повлечь за собой утрату или изменение информации», — ясно показывает, что теперь требуется участие эксперта, имеющего знания и навыки в области информационных технологий, для решения проблемы грамотного изъятия и исследования носителей информации. В то же время проблемы обеспечения целостности компьютерной информации стали освещаться в отраслевых стандартах. Примером может служить Стандарт Банка России СТО БР ИББС-1.3–2016 [5]. В нем уже достаточно ясно описано требование обеспечения целостности: «Для сбора технических данных могут выполняться: <…> „криминалистическое“ копирование (создание образов) энергонезависимых технических данных запоминающих устройств СВТ методом побитного копирования». Данный подход максимально точно описывает главный принцип (p. 1) великобританской Ассоциации высших офицеров полиции, который в вольном звучит следующим образом: «Никакие действия правоохранительных органов, лиц, работающих в этих учреждениях, или их агентов не должны изменять данные, которые впоследствии могут быть использованы в суде» [6]. Дальнейшее развитие принципа сыграло важную роль в становлении такой ветви научного знания, как форензика (forensic science).

Разобравшись с терминологией и правовыми аспектами проблемы, приступим к освещению практической части вопроса. Стоит отметить, что принцип обеспечения целостности работает до первого получения цифрового побитового образа физического устройства хранения данных (далее — накопителя). Полученный в результате некоторых манипуляций образ может быть исследован любыми удобными средствами с любыми изменениями целостности, но

только при условии четкого документирования каждого шага с целью обеспечения повторяемости процесса исследования.

Стоит отметить, что в представленных формулировках нет объективного запрета на использование дистрибутива операционной системы с отключенным автоматическим и применяемым ручным монтированием файловых систем, например, используя команду mount с параметром «только чтение» (*mount -o ro /dev/sdXY /mnt*). Но стоит помнить, что, например, в данном случае при использовании поврежденных журналируемых файловых систем может произойти их восстановление с применением информации из журнала файловой системы. В итоге пользователь получит строчку в выводе буфера сообщений ядра (Dmesg): «recovery required on readonly filesystem <…> write access will be enabled during recovery», что свидетельствует о том, что система перезаписала часть данных на исследуемой файловой системе, обновив по крайней мере время последней записи данных файловой системы. Именно поэтому, из-за вероятности возникновения подобных ситуаций, данный метод признается несостоятельным.

Следующим шагом для увеличения степени надежности можно считать использование утилит класса disk definition, на вход которых подается одно из блочных устройств в системе (раздел накопителя с информацией, жесткий диск и т. п.). На выходе же при задании определенных параметров имеем полную побитовую копию блочного устройства. Полученный образ будет содержать служебные данные, структуру накопителя, свободные области файловых систем и неразмеченные области накопителя. При записи образа накопителя с блочного устройства не производится монтирование файловой системы, что минимизирует риски нарушения целостности исследуемого накопителя. Однако эксперты в области криминалистики и расследования инцидентов информационной безопасности сходятся во мнении, что обычной операционной системы с применением стандартных механизмов ограничения записи может быть недостаточно, что подтверждается рядом исследований и тестов [7]. В качестве решения проблемы предлагается использовать разного рода блокираторы записи, краткая классификация которых представлена ниже:

- программные блокираторы записи, например, отфильтровывающие запросы записи на пути к драйверу накопителей;
- аппаратные блокираторы, перехватывающие команды записи от операционной системы, предотвращая их передачу на накопитель. Операционной системе сообщается о подключении накопителя в режиме «только чтение», а любые команды записи эмулируются с использованием внутренних механизмов блокиратора либо отсекаются вовсе. Фактически на аппаратном уровне ограничиваются обращения с командами записи к подключенным накопителям [8].

Таким образом, рассмотрены правовые аспекты, регламентирующие процесс исследования накопителей информации. Приведены примеры деструктивных воздействий на устройства хранения информации. Представлены базовые механизмы предотвращения подобного рода воздействий.

Список литературы

1. *Bell G.*, *Boddington R.* Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? Murdoch University, 2010.

2. *Федотов Н. Н.* Форензика — компьютерная криминалистика. М. : Юр. мир, 2007.

3. Федеральный закон от 28 июля 2012 г. № 143-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации».

4. Уголовно-процессуальный кодекс Российской Федерации (ред. от 29.07.2017).

5. Стандарт Банка России СТО БР ИББС-1.3–2016. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств. Москва, 2016.

6. ACPO Good Practice Guide for Digital Evidence v5 (latest). ACPO, 2012.

7. Hardware Write Block [Электронный ресурс]. Режим доуступа: https://www.cftt.nist.gov/hardware_write_block.htm (дата обращения: 06.11.2017)

8. Write Blockers Block [Электронный ресурс], режим доуступа: http://www.forensicswiki.org/wiki/Write_Blockers (дата обращения: 06.11.2017).

УДК 004.056.53

И. Ф. Файсханов
Научный руководитель: д-р тех. наук, проф. Л. Г. Доросинский
Уральский федеральный университет, Екатеринбург

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ УСТОЙЧИВОГО КЛАВИАТУРНОГО ПОЧЕРКА

Аннотация. В данной работе основное внимание уделяется процессу аутентификации пользователей с помощью устойчивого клавиатурного почерка.

Данная тематика является перспективной и актуальной, поскольку вопросы безопасности информации всегда имеют высокий приоритет, особенно, если защищаемая информация представляет какую-либо ценность.

Проанализирован алгоритм работы системы аутентификации, приведенный в более ранней публикации. Приведены результаты текущих исследований клавиатурного почерка, а также о дальнейших планах по модернизации данной системы.