УДК 004.356

УНИЧТОЖЕНИЕ ИНФОРМАЦИИ НА ЭНЕРГОНЕЗАВИСИМЫХ ЗАПОМИНАЮЩИХ УСТРОЙСТВАХ С ПРОИЗВОЛЬНЫМ ДОСТУПОМ

Дедюрин А.Б., студент группы ИТб-121,
Научный руководитель: Алексеева Г.А., старший преподаватель.

Кузбасский государственный технический университет имени Т.Ф.Горбачева
г. Кемерово.

Уничтожение данных – последовательность операций, предназначенных для необратимого удаления данных (в т.ч. и остаточной информации), программным или аппаратным методом. Уничтожение данных важный элемент поддержания информационной безопасности предприятия, использующийся для сохранения государственной или коммерческой тайны.

Процессы уничтожения данных на накопителях на жестких магнитных дисках изучены довольно давно. С современным развитием технологий, стали доступны твердотельные накопители (англ. solid-state drive, SSD)- немеханические накопители на основе микросхем памяти. Наиболее распространенный вид твердотельных накопителей использует для хранения информации флеш-памяти типа NAND, однако существуют варианты, в которых накопитель создается на базе DRAM-памяти, снабженной дополнительным источником питания — аккумулятором. SSD быстрее, легче, потребляют меньше энергии, более устойчивы к воздействиям внешней среды, обеспечивают произвольный доступ к любой области данных без дополнительных издержек.

Для чтения блока данных в винчестере сначала нужно вычислить, где он находится, потом переместить блок магнитных головок на нужную дорожку, подождать пока нужный сектор окажется под головкой и произвести считывание. Причем хаотические запросы к разным областям жесткого диска еще больше сказываются на времени доступа. При таких запросах HDD вынуждены постоянно «гонять» головки по всей поверхности «блинов» и даже переупорядочивание очереди команд спасает не всегда. А в SSD все просто — вычисляем адрес нужного блока и сразу же получаем к нему доступ на чтение/запись. Никаких механических операций — всё время

уходит на трансляцию адреса и передачу блока. Чем быстрее флэш-память, контроллер и внешний интерфейс, тем быстрее доступ к данным.

Так же появилось множество различной цифровой аппаратуры, которая требует большого количества памяти с низким энергопотреблением, а также с возможностью хранения информации при выключении устройства. Для этих целей используется флэш-память (Flash memory).

Гарантированное уничтожение данных.

В случае удаления файлов на уровне файловой системы, как правило, реального уничтожения данных не происходит. Файловая система лишь помечает участок на диске как свободный, освобождая это место для записи. Поэтому большинство стандартов и программ безопасного удаления данных используют многократную перезапись в секторах жесткого диска или блоках SSD- диска ложными данными. В зависимости от алгоритма, это может быть сгенерированное генератором псевдослучайных чисел, либо фиксированное значение. Как правило, каждый алгоритм предусматривает запись восьми битовых единиц(#FF) и нуля (#00), количество циклов перезаписи так же разнится в зависимости от алгоритма.

Распространенные алгоритмы:

Основными алгоритмами используемыми в широко распространенном программном обеспечении являются:

- Американский национальный стандарт DoD 5220.22-M;

1-й проход - случайно выбранные символы в каждый байт каждого сектора, 2 -дополнительные к записанным на 1-м проходе; 3 - снова случайно выбранные символы; 4 - верификация записей.

- Американский национальный стандарт NAVSO P-5239-26 (RLL);

1-й проход - 0x01 во все сектора, 2 -0x27FFFFFF, 3 - случайные последовательности символов, 4 - верификация.

- Американский национальный стандарт NAVSO P-5239-26 (MFM);

1-й проход - 0x01 во все сектора, 2 -0x7FFFFFF, 3 - случайные последовательности символов, 4 - верификация.

- Германский национальный стандарт VSITR;

1-й - 6-й запись чередующихся последовательностей вида: 0x00 и 0xFF; 7-й -0xAA; то есть 0x00, 0xFF, 0x00, 0xFF, 0x00,

0xFF, 0xAA.

- Российский национальный стандарт GOST P50739-95;

Запись логических нулей (чисел вида0x00) в каждый байт каждого сектора для систем с 6-го по 4-й класс защиты. Запись случайно выбранных символов (чисел) в каждый байт каждого сектора для систем с 3-го по 1-й класс защиты.

SSD очень трудно очистить от чувствительных к компрометации данных, используя традиционные методы безопасного затирания файлов и дисков. Даже в тех случаях, когда устройства SSD показывают, что файлы уничтожены, до 75 процентов данных, в них содержавшихся, могут всё ещё находиться в памяти флэш-драйвов. В частности, в некоторых случаях, когда твердотельные диски свидетельствуют, будто файлы «безопасно стёрты», на самом деле их дубликаты остаются в значительной степени нетронутыми во вторичных местоположениях.

Проблемы с надёжным затиранием данных на SSD, происходят из-за радикально иной внутренней конструкции носителя. Традиционные приводы типа ATA и SCSI используют намагничиваемые материалы для записи информации в конкретное физическое место, известное как LBA или адрес логического блока. В дисках SSD, с другой стороны, для цифрового хранения используются чипы, для управления контентом применяющие FTL или «слой флэш-трансляции». Когда данные в таком носителе модифицируются, то FTL часто записывает новые файлы в разные места, попутно обновляя карту распределения памяти для отражения сделанных перемен. Результатом таких манипуляций становится то, что остатки от прежних файлов, которые авторы именуют «цифровыми останками», в виде неконтролируемых дубликатов продолжают сохраняться на диске.

Перезапись данных на SSD приводит лишь к логическому удалению(т.е. данные становится невозможно извлечь с помощью SATA или SCSI-интерфейсов).

Подходы к гарантированному уничтожению:

1)Метод затирания данных предполагает использование обычных команд ввода-вывода для перезаписи каждого блока по его адресу. Многократная программная перезапись лежит в основе многих стандартов и инструментов гарантированного удаления.

2)Размагничивание, сильное переменное магнитное поле, излучаемое системой для размагничивания, индуцирует мощные токи в металлических слоях микросхемы. Эти токи могут повредить микросхемы, сделав чтение с них невозможными.

Пример: Электромагнитное поле, создаваемое в полеобразующей системе, разрушает составляющие флэш и обеспечивает нарушение связей в кристалле микросхемы. На рис. 1 приведен результат воздействия изделием УЭ-03 на флеш носитель.

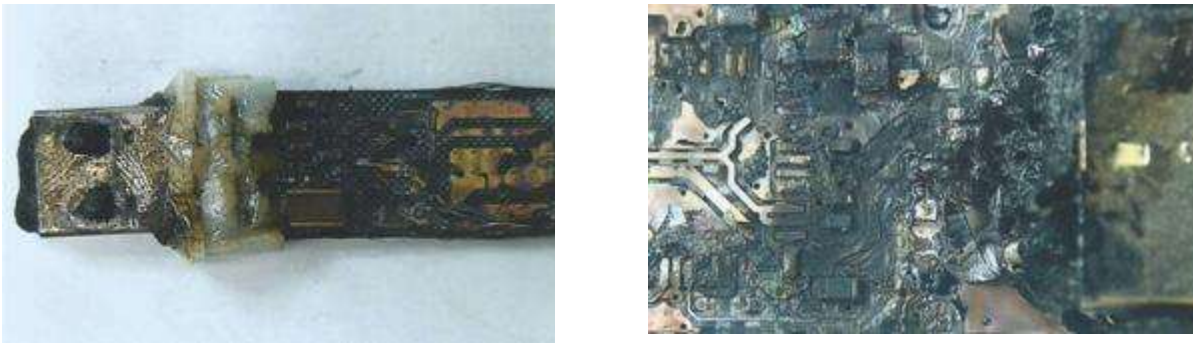

Рис1. Результат воздействия изделием УЭ-03 на флеш носитель.

3)Шифрование данных. Некоторые SSD шифруют данные по умолчанию, что обеспечивает повышенную безопасность. Удаление ключа шифрования из хранилища ключей делает чтение данных невозможным. Опасность метода в том, что он полагается на правильное затирание контроллером накопителя внутреннего хранилища информации, содержащего ключ и все производные значения, которые могут быть полезны при крипто-анализе.

4)Физическое уничтожение носителя. Название метода говорит само за себя. Количество вариантов ограничено только воображением и некоторыми законами РФ. Например: физическое повреждение(удар, прокол и т.д.),нагрев микросхемы выше некоторой температуры. Значение температуры, выше которой происходит повреждение информации, должно определяться специальными исследованиями. Нагрев можно осуществить, например, СВЧ излучением.

Вывод: гарантированно уничтожить данные может оказаться довольно таки сложным делом. Изобретено уже множество методов, проведены исследования, но технологии хранения информации изменяются, а значит должны изменяться и технологии уничтожения данных. Все методы что разрабатывались для стирания данных с HDD, оптических дисков и магнитных носителей уже не могут обеспечить высокую степень безопасности, касающейся уничтожения данных. Есть встроенные команды для уничтожения, но не всегда производитель реализует их корректно. При удалении данных важно помнить сложность SSD- устройств и по возможности комбинировать некоторые из методов уничтожения данных, чтобы, как говорится, наверняка.

Список литературы:

1.Питер Ю, Мануэль Кардона, “Основы физики полупроводников.” М.: ФИЗМАТЛИТ, 2002 г.–560с.

2.Хабрахабр[Электронный ресурс] URL:https://habrahabr.ru/

3.К.Касперски. “Восстановление данных. Практическое руководство”,– М.: БХВ-Петербург,2007г.–352с.

4.А.В.Кузьмин, “Flash-память и другие современные носители информации.”-М.:Москва, 2005 г.–80с.