

Изучение функции уничтожения данных устройства Samurai Flash Drive

14.03.2012 был проведён ряд тестов для проверки эффективности уничтожения данных накопителем на флэш-памяти Samurai Flash Drive, далее «устройство».

Корпус предоставленного для тестирования экземпляра отсутствовал, для облегчения доступа к карте памяти формата microSD, на которой хранятся пользовательские данные.

Результаты проверки показали полное и необратимое уничтожение всей записанной информации при использовании каждого из предусмотренных инструкцией способов уничтожения. Ход тестирования описан ниже.

Тестирование

При проведении всех тестов использовалась одна и та же последовательность действий:

1. Прямая запись в сектора устройства специальной сигнатуры. В первом тесте адресное пространство накопителя было перезаписано полностью. В остальных только начало, от нулевого сектора до примерно двух-трёх миллионов секторов из 15 миллионов.
2. Изучение содержимого флэш-карты при подключении к компьютеру через устройство и через ридер.
3. Уничтожение данных.
4. Изучение содержимого флэш-карты при подключении к компьютеру через устройство и через ридер.

В качестве инструментов были выбраны бесплатные программные продукты, которые можно скачать из Интернета. Это было сделано для того, чтобы любой пользователь мог самостоятельно воспроизвести результаты теста, следуя описанной здесь последовательности.

Для изучения содержимого флэш-карты использовался hex-редактор CI Hex viewer.

Тестовая сигнатура записывалась с помощью программы для диагностики носителей информации HDDScan. В числе прочего, эта утилита даёт возможность осуществить ряд «тестов поверхности». При запуске теста Erase, сектора устройства, начиная с нулевого, заполняются специальной сигнатурой, состоящей из номера сектора, названия программы и символов #.

Далее следуют записи, сделанные в процессе тестирования.

1) Уничтожение вводом пароля «по принуждению».

Полностью перезаписываю содержимое флэшки, вставленной в устройство, с помощью HDDScan. Проверяю.

При подключении к компьютеру устройства с установленной флэшкой наблюдаю:

Нулевой сектор содержит нули и несколько ненулевых символов. Следующие три - абракадабру. Судя по всему, это нули, прошедшие через дешифровку. Далее до конца адресного пространства во всех секторах сигнатура HDDScan.

При подключении флэшки через ридер вижу:

Нулевой сектор содержит нули и несколько ненулевых символов. Сектора 1-3 заполнены нулями. Далее до конца адресного пространства абракадабра. Предполагаю, что это зашифрованная сигнатура HDDScan.

Следуя инструкции, задаю пароль для открытия и пароль «под принуждением». Затем подключаю устройство и ввожу пароль «под принуждением». Загорается и гаснет красный светодиод.

Не отключая от компьютера, изучаю содержимое устройства:

Первый сектор без изменений, дальше абракадабра.

Отключаю устройство от компьютера, переставляю флэшку в ридер, смотрю её содержимое:

Первый сектор без изменений, дальше до конца адресного пространства нули.

Вывод – данные уничтожены.

2) Уничтожение шестью неправильными вводами пароля.

Подключаю устройство с флэшкой к компьютеру, в проводнике появляется неотформатированный диск. Запускаю Erase тест HDDScan. Ожидаю некоторое время, завершаю тест.

Проверяю содержимое флэшки вставленной в устройство:

Нулевой сектор содержит нули и несколько ненулевых символов. Следующие три - абракадабру. Далее сектора заняты сигнатурой HDDScan. Затем до конца накопителя абракадабра.

Подключаю через ридер:

Нулевой сектор содержит нули и несколько ненулевых символов. Далее в 1-3 нули. Далее абракадабра. Потом опять нули.

Всё как надо. Теперь уничтожаю. Согласно инструкции, устанавливаю пароль 123. Затем шесть раз выполняю следующее: подключаю устройство к USB порту, нажимаю кнопку «ввод», наблюдаю загоревшиеся светодиоды и отключаю. На последней итерации светодиоды несколько раз моргают.

Подключаю, светодиоды несколько раз моргают. Накопитель компьютером не определяется. Нажимаю первую кнопку. Дважды мигает красный светодиод, и в проводнике Windows появляется неотформатированный диск.

Далее изучаю результат уничтожения.

Через устройство:

Первый сектор без изменений, дальше абракадабра.

Через ридер:

Первый сектор без изменений, дальше нули.

Данные уничтожены.

3) Уничтожение нажатием кнопок «1» и торцевой, в отключенном от компьютера состоянии.

Перезаписываю часть адресного пространства устройства, начиная с нулевого сектора, сигнатурой HDDScan.

Проверяю содержимое устройства:

Нулевой сектор содержит нули и несколько ненулевых символов. Следующие три - абракадабру. Далее сигнатура HDDScan. После неё абракадабра.

Вставляю microSD в ридер:

Нулевой сектор содержит нули и несколько ненулевых символов. Дальше 1-3 нули. Дальше абракадабра. Потом опять нули.

Теперь уничтожаю. Нажимаю одновременно торцевую кнопку и «1», и держу их пока светодиоды не перестанут моргать. Затем подключаю устройство к компьютеру и наблюдаю появившийся в проводнике неотформатированный диск.

Смотрю гексредактором:

В первом секторе без изменений, дальше абракадабра.

Вынимаю карточку из устройства, вставляю в ридер и смотрю что там. А там первый сектор без изменений и дальше нули.

Данные уничтожены.

4) Уничтожение удержанием кнопки 1 в момент подключения устройства к компьютеру.

Подключаю устройство с флэшкой к компьютеру, запускаю Erase test HDDScan, жду некоторое время.

Проверяю содержимое флэшки через устройство и ридер - всё нормально, запись сигнатуры прошла успешно.

Нажимаю и удерживаю кнопку 1 в момент подключения USB кабеля. Несколько раз мигают светодиоды, затем один раз мигает красный. Наблюаю в проводнике неотформатированный диск. Изучаю содержимое флэшки:

Через устройство:

В первом секторе без изменений, дальше абракадабра.

Через ридер:

Первый сектор без изменений, а дальше нули.

Данные уничтожены.

Дополнительная информация

Согласно утверждению производителя устройства, для уничтожения данных используется стандартная команда, выполняющая которую контроллер карты памяти обнуляет содержимое диапазона адресов, указанного в качестве параметра.

Из практики работы с накопителями на флэш-памяти известно, что далеко не все из них поддерживают полный набор команд, содержащийся в описании стандарта. При этом производители заявляют полную поддержку стандарта. Это касается не только поппате устройств, но и изделий наиболее именитых компаний.

Наблюдались даже такие явления, как выполнение или игнорирование команды устройствами одной и той же модели в зависимости от партии поставки. Поэтому очень важно использование в устройстве уничтожения данных именно той microSD карты, которая была установлена производителем, из предварительно протестированной партии.



Хозеичев
/ Хозеичев И. А.