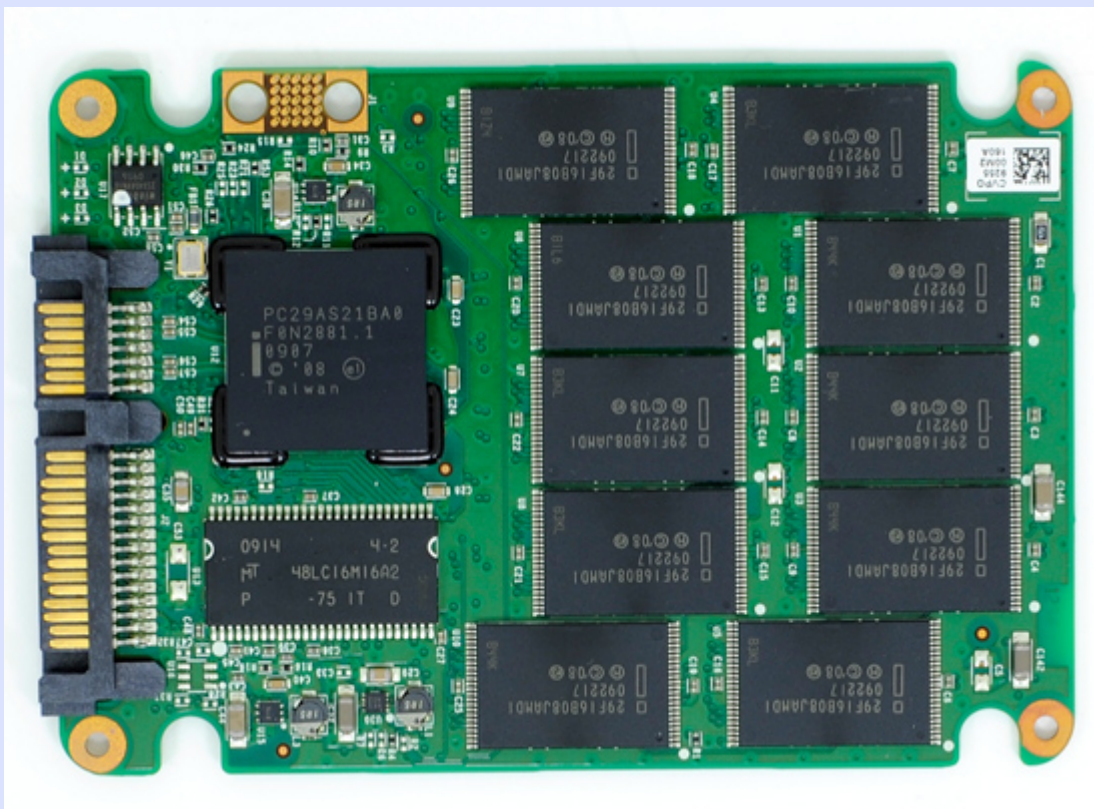


МЕЖДУНАРОДНЫЙ ФОРУМ ТЕХНОЛОГИИ БЕЗОПАСНОСТИ

Проблемы уничтожения информации на флэш-накопителях и пути их решения

Шахалов И.Ю. *Заместитель Генерального директора ЗАО «НПО «Эшелон»*

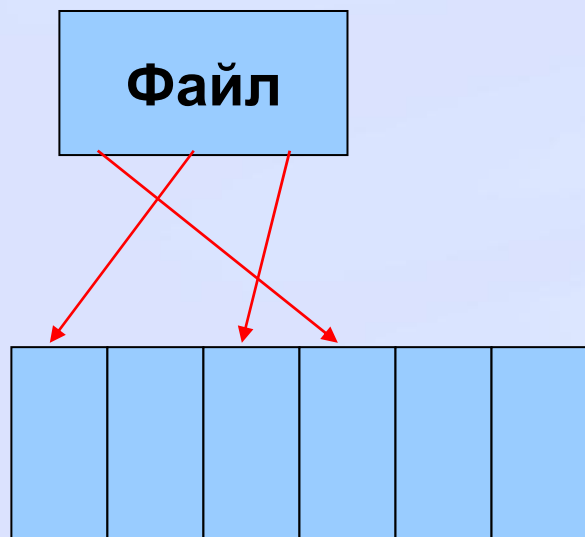
SSD и HDD



- Быстрее
- Легче
- Надежнее
- Экономичнее
- Сложнее

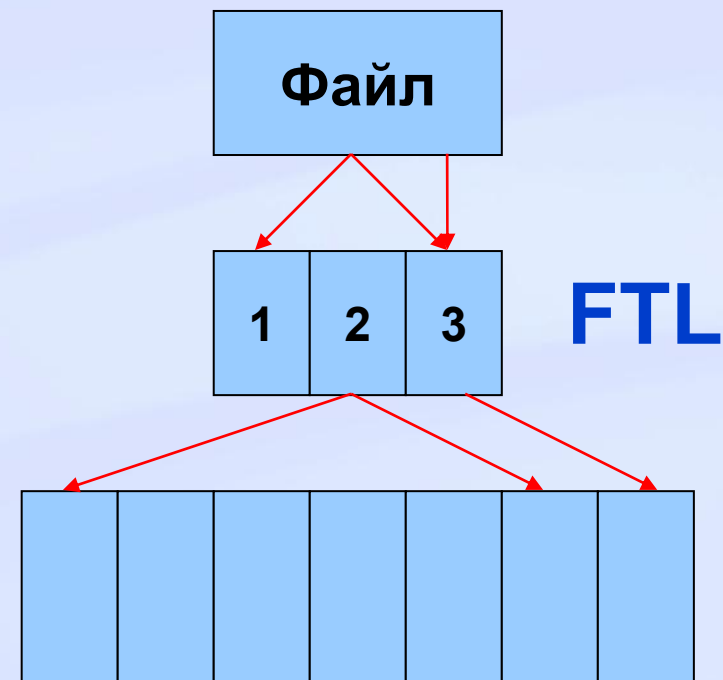
Адресация в SSD

HDD



Секторы диска

SSD



Блоки памяти

Алгоритм распределения нагрузки



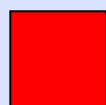
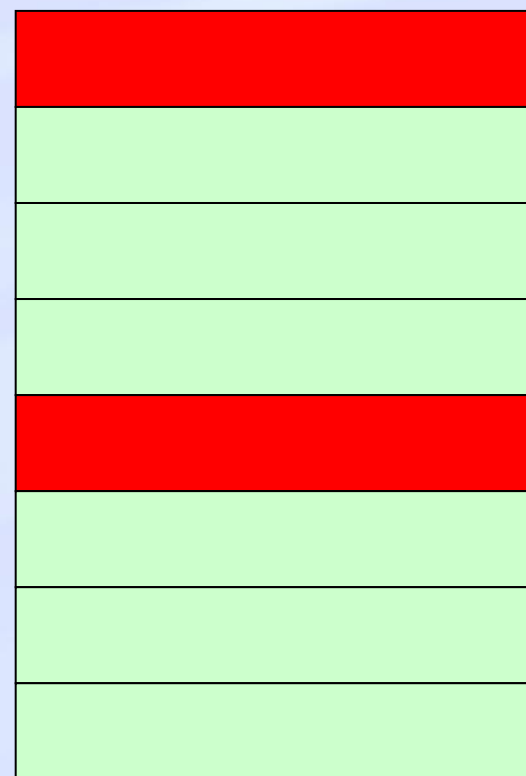
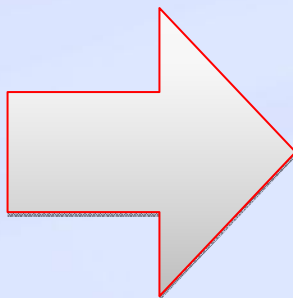
Износ

- Ячейки памяти SSD можно перезаписать всего около 10 000 – 100 000 раз
- Для минимизации этого эффекта в FTL используется алгоритм распределения нагрузки
- FTL всегда стремится записывать данные в наименее используемые ячейки

Проблема стирания

- Запись в ячейку флеш памяти требует предварительного электрического стирания
- Электрическое стирание ячейки до 3 000 раз медленнее чтения и записи
- Контроллер SSD накопителя стремится использовать время простоя накопителя для предварительного электрического стирания освободившихся блоков с помощью алгоритма самовосстановления

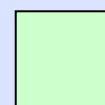
Алгоритм самовосстановления



Занятые области



Области, помеченные
как свободные



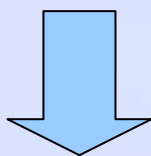
Очищенные области

Проблемы криминалистического анализа SSD-накопителей

- Самопроизвольное изменение состояния накопителя
- Невозможность фиксации состояния снятием контрольной суммы
- Возможность мгновенного удаления данных быстрым форматированием
- Игнорирование блокираторов записи
- Отсутствие внешних признаков работы

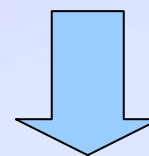
Самопроизвольное изменение состояния

Изъятие диска



417010bebaed0a00
32b96ac461dd9d67

После изучения
экспертом
криминалистом

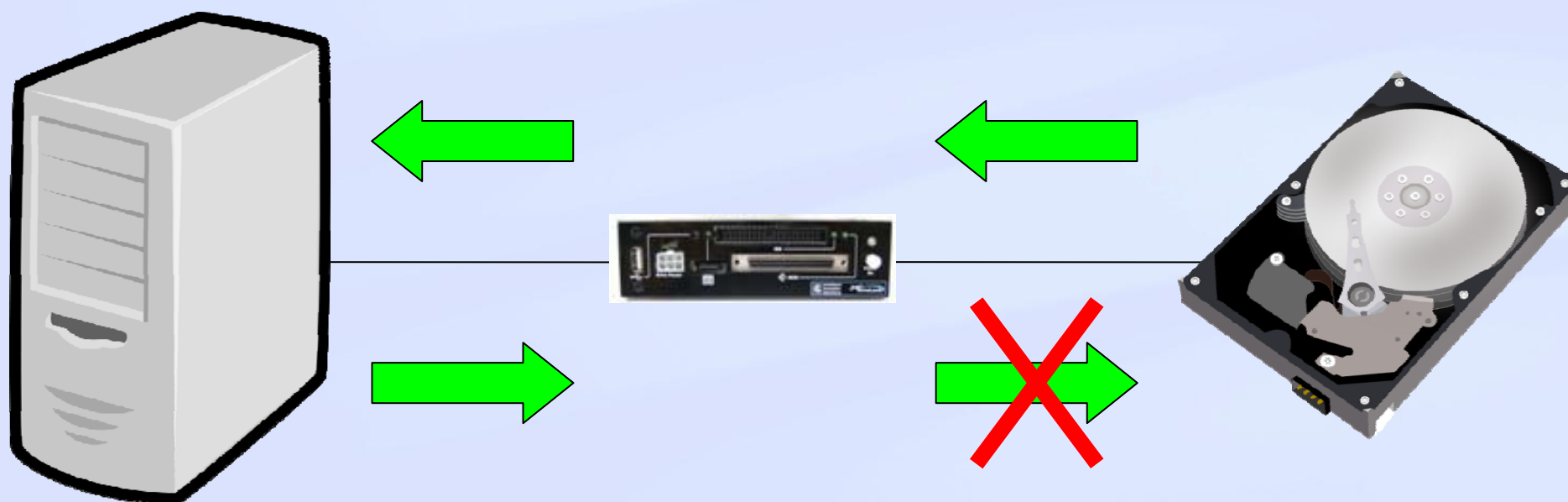


5718e5479fb415a1
00364676191a3471

Быстрое форматирование

- Не удаляет данные, но помечает диск как свободный и заново создает структуру файловой системы
- Выполняется очень быстро по сравнению с полной перезаписью
- Алгоритм самовосстановления после быстрого форматирования может самостоятельно полностью очистить диск

Аппаратный блокиратор записи

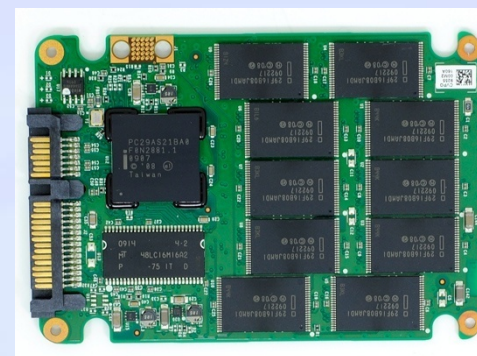
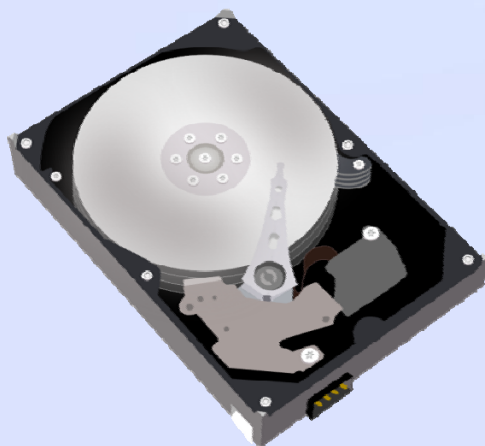


Игнорирование блокиратора записи

- Аппаратные блокираторы записи применяются в криминалистике для предотвращения изменений в анализируемых накопителях
- Блокиратор является внешним устройством и не влияет на работу контроллера SSD
- Блокиратор не способен воспрепятствовать работе алгоритма самовосстановления

Отсутствие внешних проявлений работы

Звук
Вибрация



???

Результаты экспериментов

- SSD носитель после быстрого форматирования полностью удалил данные в течение порядка 6 минут после включения
- При использовании стандартной криминалистической методики удалось восстановить лишь **0,003%** информации
- Аппаратные блокираторы записи не предотвращают самоочищение, хотя в конкретных случаях могут его замедлить

Методы стирания данных

- ATA Security set
- Многократная перезапись
- Размагничивание
- Шифрование

Методика испытаний методов стирания данных

- На накопитель записываются т.н. "отпечатки"
- Проводится процедура очистки
- Накопитель разбирается
- Остаточная информация считывается с ножек отдельных микросхем памяти

ATA Security set

- Команда SECURITY ERASE UNIT полностью затирает накопитель обнуляя все ячейки памяти

- Результаты экспериментов:

Всего проверено 12 накопителей

8 накопителей поддерживают команду SECURITY ERASE UNIT

Только 4 накопителя успешно выполнили команду

Один из накопителей сообщил что выполнил команду успешно, но данные остались нетронутыми

Размагничивание

- Применялась современная система размагничивания НЖМД, позволяющая полностью уничтожать данные на современных жестких дисках
- Все данные на микросхемах остались нетронутыми и доступными для считывания

Шифрование

- Многие SSD накопители по умолчанию шифруют данные
- Теоретически, для очистки такого накопителя достаточно надежно стереть ячейку памяти, содержащую ключ шифрования
- Метод не поддается надежной верификации

Многократная перезапись

- Перезапись данных по логическим адресам различными битовыми последовательностями
- Лежит в основе всех стандартов и инструментов гарантированной очистки данных с НЖМД
- В отличие от остальных методов возможно затирать как весь накопитель целиком, так и отдельные файлы
- Остаточную от удаления файлов информацию также возможно затереть путем перезаписи всего свободного пространства накопителя

Результаты экспериментов. Полное затирание носителя.

- В большинстве случаев двух проходов перезаписи оказалось достаточно для полного стирания исходных данных
- В то же время на одном из накопителей сохранилось около 1% данных после 20 проходов
- Хотя метод кажется эффективным, он все же не дает 100% надежности

Результаты экспериментов. Затирание отдельных файлов

- Испытано 13 протоколов перезаписи, представляющих собой различные государственные стандарты и коммерческие продукты
- Результат – от **0,57%** до **84%** данных сохранилось, ни один способ затирания не справился полностью
- Перезапись свободного пространства оставляет от **53%** до **87%** данных

Выводы

- Встроенные команды очистки эффективны, но не всегда реализованы корректно
- Двойная перезапись всего адресного пространства накопителя не гарантирует полное удаление данных
- Ни один из существующих методов удаления данных, пригодный для НЖМД, не эффективен для SSD
- Криминалистический анализ SSD накопителей сильно осложняется работой алгоритма самовосстановления, но не у всех производителей.



Спасибо за внимание!

Шахалов И.Ю.

Заместитель Генерального директора ЗАО «НПО «Эшелон»

Тел. (495) 645 38 10

E-mail: info@npo-echelon.ru

[www. npo-echelon.ru](http://www.npo-echelon.ru)

Информационная поддержка: www.ispdsn.ru