УДК 004.454

Вестник УрФО № 3(45) / 2022, с. 17–23

Куц Д.В., Поршнев С.В., Куц М.П.

DOI: 10.14529/secur220302

АНАЛИЗ МЕХАНИЗМОВ УДАЛЕНИЯ ФАЙЛОВ НА SSD НАКОПИТЕЛЯХ

В статье обсуждаются особенности механизмов удаления выбранных файлов, хранящихся на SSD-накопителях, оказывающие влияние на хранение и удаление данных. Описаны отличия механизмов удаления файлов SSD- от HDD-накопителей, а также особенности данных механизмов, используемых SSD-накопителях с файловой системой NTFS, в которой включена поддержка команд TRIM и Deallocate, а также результаты исследования поведение SDD-накопителя с аномалиями при использовании команды TRIM. На основе данных результатов сделан обоснованный вывод о возможностях программного восстановления данных на SSD-накопителях.

Ключевые слова: *TRIM, deallocate, восстановление данных, solid-state drive, NTFS, твердотельный накопитель, выравнивание износа, сборка мусора.*

Kuts D.V., Porshnev S.V., Kuts M.P.

THE ANALYSIS OF FILE DELETION MECHANISMS ON SSD DRIVES

This article describes the specifics of SSD drives work that occurs when single files are deleted. The differences between SSD drives and traditional HDD-type drives in terms of behavior when deleting data are considered. The mechanisms of SSD operation that affect storage and deletion of data on drives are considered. Analysis of behavior of a number of SSD drives with the NTFS file system with support of TRIM and Deallocate commands is carried out. A study of behavior of drive with anomalies in TRIM operation is carried out. The conclusion about the possibilities of software data recovery on SSD is made.

Keywords: *TRIM, deallocate, data recovery, solid-state drive, NTFS, solid state drive, wear leveling, garbage collection.*

Анализ современного рынка накопителей информации на жестких дисках позволяет сделать вывод о том, что происходит активная замена HDD-накопителей более высокопроизводительными SSD-накопителями, надежность хранения данных на которых оказывается сравнимой с аналогичной характеристикой HDD-накопителей. В этой связи сегодня в большинстве серверных и десктопных решений в качестве основного носителя используются SSD-накопители, а HDD-накопители используются в качестве дополнительных накопителей для хранения больших объёмов данных, не требующих высокой скорости доступа.

Несмотря на то, что для операционной

системы (ОС) и для конечного пользователя SSD-накопитель по логике своей работы мало чем отличается от HDD-накопителя (за исключением быстродействия), на SSD-накопителях используются принципиально иные механизмы записи, хранения, удаления данных. Напомним, что на SSD-накопителе в качестве хранилища данных преимущественно используют NAND-память [1]. Данный тип памяти обладает высокой скоростью чтения, записи и значительной надёжностью, которому, однако, присущи некоторые недостатки. Из них основным оказывается конечный ресурс ячеек памяти на запись в них данных. Напомним, что в современных накопителях на жестких дисках ресурс памяти на запись определяется максимальным гарантированным объёмом записанной информации за весь срок пользования SSD-накопителя (англ. Total Bytes Written, TBW). При этом очевидно, что необходимым условием использование данного параметра является выполнение требования о том, количество операций записи в каждую ячейки памяти SSD-накопителя будет примерно одинаковым. Однако ОС, напротив, многие системные файлы (например, журнал транзакций, файл подкачки, log-файлы и др.), перезаписывает соответствующие данные в одни и те же ячейки памяти многократно, в то время как другие ячейки, в которые записаны не изменяемые регулярно данные, оказываются использованные, фактически, однократно. В результате возникает проблема неравномерного износа ячеек памяти SSD-накопителей, для решения которой используется технология выравнивания износа (англ. Wear Leveling), реализованная в контроллере SSD-накопителя [2], которая делает NAND-память надёжной и отказоустойчивой.

Технология Wear Leveling основана на совместном использовании абстрагированного логического адресного пространства SSD-накопителя и физических адресов ячеек памяти микросхем, обеспечиваемом технологией FTL (Flash Translation Layer), которая обеспечивает сопоставление логических и физических адресов SSD-накопителей. В данной технологии в случае записи новых данных логические адреса физических адресов ячеек памяти заменяются на адреса менее изношенных ячеек, что и обеспечивает равномерный износ каждой ячейки памяти носителя на твердом диске. К недостаткам технологии FTL следует отнести трудности, возникающие при перезаписи данных на SSD-накопитель, которые, в свою очередь, приводят к возникновению проблем гарантированного стирания файлов, связанных с тем, что данные, недоступные логически, микросхемах памяти остаются до тех пор, пока не доберётся «сборщик мусора».

Сборка мусора (Garbage collection) – это технология, осуществляющая зачистку неиспользуемого пространства SSD-накопителя. Ещё одна особенность памяти NAND состоит в том, что каждая ячейка памяти, перед повторной записью должна быть очищена. Процесс стирания в NAND-памяти, однако, значительно медленнее, чем запись или чтение. Соответственно, лучшей стратегией для SSD-накопителя является заблаговременная подготовка очищенных ячеек памяти для их быстрой записи в случае необходимости. Таким образом, на SSD-накопителях происходит регулярный процесс сборки мусора, что обеспечивает поддержку высокого быстродействия SSD-накопителя.

Одним из эффективных способов повысить эффективность сборки мусора на накопителе является информирование управляющего контроллера накопителя ОС о тех блоках данных, которые принадлежали уже удалённым файлам, а потому могут быть очищены. Данное информирование реализуется с помощью команды TRIM интерфейса SATA или Deallocate для интерфейса PCI-E. Отметим, что сборка мусора не заменяет функционал TRIM на SSD-накопителе, но, наоборот, TRIM помогает бы сборке мусора быть более эффективной и производительной [3]. Удаление данных может быть выполнено в фоновом режиме, в то время как пользователь использует ОС или может быть запрограммировано на очистку после перезагрузки [4], с которой, однако, на практике авторам сталкиваться не приходилось. При удалении файла, с включёнными командами TRIM или Deallocate, сектора с его данными, как показывает опыт, очищаются примерно за 5-15 секунд. Это порождает распространённое мнение о том, что восстановить удалённые файлы на SSD-накопителе с включённой командой TRIM без аппаратного вмешательства и чтения напрямую с микросхем памяти невозможно. Результаты нашего исследования, обсуждаемые далее, свидетельствуют о том, что данное утверждение оказывается не вполне справедливым.

Изначально отметим, что, во-первых, ко-

манды TRIM и Deallocate, даже будучи активными, не работают на внешних накопителях, подключенных через USB порт; во-вторых, команды TRIM и Deallocate не функционируют на виртуальных машинах и в RAID-массивах; в-третьих, особенности файловой системы NTFS не позволяют отрабатывать команд TRIM и Deallocate для файлов, хранящих содержимое в резидентных атрибутах [5] (размером менее 700 байт), что, потенциально, дает возможность восстановления любых удалённых файлов на SSD-накопителе. Кроме того, команды TRIM и Deallocate не работают при повреждении файловой системы тома или при его удалении. Также необходимо отметить, что в случаях, не имеющих отношения к вышеперечисленным, реализация сборки мусора на SSD-накопителе целиком и полностью лежит на производителе устройства. Для этой технологии нет единого стандарта, поэтому каждый производитель SSD реализует её по-своему. Следовательно, реализация работы команд TRIM и Deallocate и последующего затирания неактуальных данных сборщиком мусора, может существенно отличаться на накопителях разных производителей.

В рамках нашего исследования, мы использовали доступные нам SSD-накопители от 7 различных производителей, в том числе компаний Azerty, Samsung, Crucial, Kingston, Transcend, ADATA, Intel. Названия тестируемых моделей и их производителей представлены в табл. 1.

Таблица 1

Тестируемые модели SSD-накопителей

Модель SSD накопителя	Производитель	Ёмкость	Интерфейс
Bory R500 (029-1118)	Azerty	240 Gb	SATA III
870 EVO MZ-77E500BW	Samsung	500 Gb	SATA III
CT480BX500SSD1	Crucial	500 Gb	SATA III
SUV400S37/120G	Kingston	120 Gb	SATA III
TS256GSSD230S	Transcend	256 Gb	SATA III
AGAMMIXS11P-512GT-C	ADATA	512 Gb	NVMe M.2
SSDPEKKW256G8	Intel	256 Gb	NVMe M.2

В проведенных экспериментах была использована ОС Windows 10 Enterprise 21H2. Каждый из накопителей имел по одному системному разделу с файловой системой NTFS. В качестве ПО для проведения исследований, нами использовались 16-теричные редакторы WinHex и HxD. В ходе исследования проводились измерения времени, затрачиваемого соответствующим SSD-накопителем на затирание данных удаленных файлов разных размеров. Отметим, что у всех SSD-накопителей время затирания данных файлов, примерно, оказалось в пределах 5-15 секунд. В тоже время было обнаружено, что накопители производителей Samsung и Crucial не очищали стирали некоторую информацию из удаленных файлов, чем обеспечивалась возможность их программного восстановления в течении продолжительного периода времени. Также, нами были обнаружены фрагменты удалённых файлов, даже после отработки командой TRIM и сборщиком мусора. Для более детального исследования был проведён эксперимент, устанавливающий зависимость успешной отработки командой TRIM и последующей сборки мусора от размера удаляемого файла.

Объектом исследования стал накопитель Samsung 870 EVO MZ-77E500BW. В рамках первого этапа, на накопителе создавались по 10 файлов различного размера со случайными повторяющимися текстовыми сигнатурами, обеспечивающими быстрый поиск данных файлов на жестком диске (рис. 1). Цель данного эксперимента состояла: в проверке гипотезы о ли зависимость скорости отработки команды TRIM и сборщика мусора от размера файла; установлени зависимости числа случаев, в которых затирание не данных не произошло, от размера удаляемого файла; выявлении условий, при выполнении которых на накопителя остаются фрагменты удаленных файлов.

В ходе экспериментов каждый файл удалялся через проводник, минуя корзину. Далее, после удаления каждого файла с помощью 16-теричного редактора HxD проводился анализ содержимого секторов, в которых ранее размещался удаленный файл, с целью нахождения отметки времени соответствую-

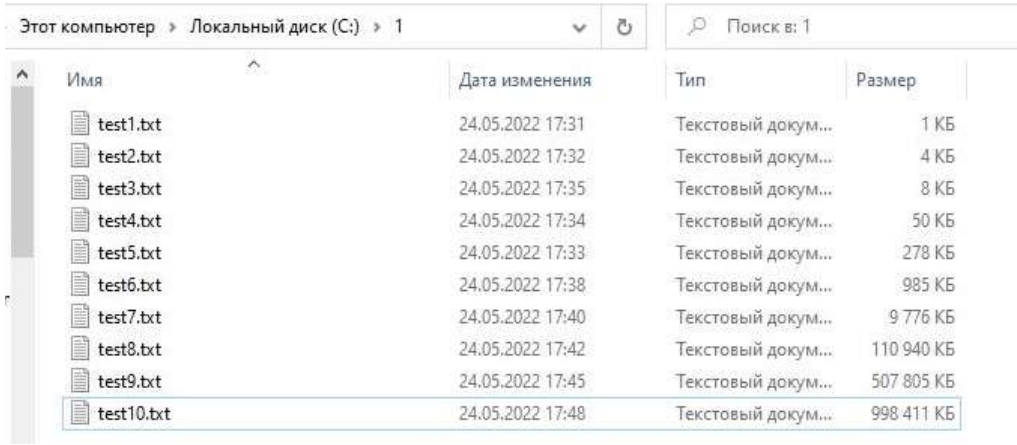

Рис. 1 Файлы различного размера, используемые в исследовании

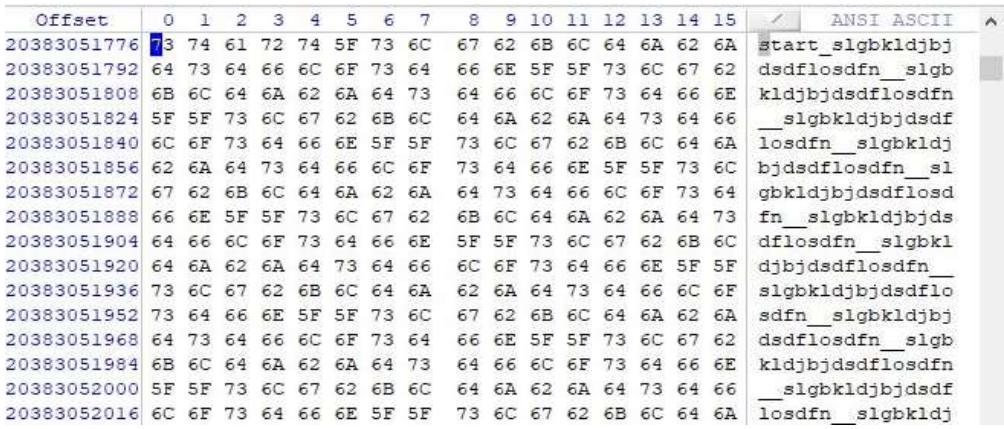

Рис. 2 Пример содержимого удаляемого файла

щей затиранию соответствующей информации. При этом, априори, мы ожидали, что данные сектора после удаления файлы могли быть отданы другому файлу и перезаписаны средствами файловой системы. Описанное действие можно обнаружить по факту принадлежности этих секторов новому файлу, так как, маловероятно, что данные сектора были бы перезаписаны нулями (что происходит при затирании информации с помощью сборщика мусора). Типичные экспериментальные результаты представлены в табл. 2.

Таблица 2

Результаты проверки качества удаления файлов разных размеров с накопителя Samsung 870 EVO MZ-77E500BW

Имя файла	Размер (байт)	Отработка TRIM	Время затирания (сек)	Наличие фрагментов
test1	1002	нет	–	–
test2	4048	нет	–	–
test3	7 513	нет	–	–
test4	51 048	да	8.1	нет
test5	284 480	да	10.0	да (14 144 байт)
test6	1 008 008	да	6.4	да (8 584 байт)
test7	10 010 008	да	8.3	нет
test8	113 602 508	да	10.5	да (12 236 байт)
test9	519 991 928	да	9.0	нет
test10	1 022 372 072	да	5.7	нет

Из табл. 2 видно, что:

1) качество работы сборщика мусора явным образом зависит от размера файла и файлы, при этом удаленные файлы размером менее 7 КБ не затираются;

2) скорость затирания файла не зависит от его размера;

3) в ряде случае данные файла затирались не полностью и на накопителе оставалась информация, находившаяся ранее в конце удаленных файлов, объем который составлял 8-14 Кб.

Для более точного определения максимального размера удаляемого файла, который не затирается сборщиком мусора на SSD-накопителе, была проведена дополнительная серия испытаний, в ходе которой затиралась три файла, размеры которых были отличны друг от друга (см. табл. 3).

Из табл. 3 видно, что максимальный размер затираемого файла составляет ~ 10÷15 килобайт. Для уточнения размера удаляемого файла была проведена еще одна серию экспериментов, результаты которой представлены в табл. 4.

Таблица 3

Результаты поиска максимального размера файла, не затираемого накопителем при удалении

Имя файла	Размер (байт)	Отработка TRIM	Время затирания (сек)	Наличие фрагментов
test1	10 032	нет	–	–
test2	15 272	да	7.5	нет
test3	20 038	да	6.9	да (3142 байта)

Из табл. 4 видно, что минимальный размер затираемого файла на накопителе Samsung 870 EVO MZ-77E500BW составляет ~12.5Кб. Для всех файлов меньшего размера данный накопитель ведёт себя практически как жёсткий диск и не обеспечивает затирание удаленных файлов через сборщика мусора, что с достаточно высокой вероятностью позволяет восстанавливать эти файлы программными методами. Также было обнаружено, что в тех случаях, когда сборщик мусора не затирал некоторые ячейки памяти при первоначальном его использовании, то и далее при его повторном использовании данные ячейки оставались не затертыми. Эти данные хранятся в памяти до тех пор, пока не будут перезаписаны файловой системой. Кроме этого, данный накопитель в ряде случаев, даже после успешной отработки команды TRIM и сборщика мусора, не очищал окончание файлов. Оставшиеся фрагменты имели размер ~8÷14 Кб, что позволяет для некоторых типов файлов восстановить часть информации. Точную зависимость наличия фрагмента файла при затирании от его размера установить не удалось, однако примерно треть всех удаляемых файлов, размер которых превышал 20 Кб, в итоге оставляли после себя «хвосты». Одновременно с этим следует отметить, что некоторые, весьма распространённые типы файлов могут содержать достаточные объёмы информации и при этом иметь размер менее 12,5 Кб.

Таблица 4

Результаты поиска максимального размера файла, не затираемого накопителем при удалении

Имя файла	Размер (байт)	Отработка TRIM	Время затирания (сек)	Наличие фрагментов
test1	11 028	нет	–	–
test2	12 024	нет	–	–
test3	13 012	да	9.8	нет
test4	14 019	да	7.7	нет

В этой связи уместно отметить, что, например, файл текстового процессора MS Word формата DOCX с 760 символами текста имеет размер, примерно 12,5 Кб и, следовательно, не очищается командой TRIM на данном накопителе. Файл DOCX, созданный в редакторе Wordpad с одним символом текста имеет размер 1947 байт, следовательно, фай-

лы, созданные в этом редакторе, могут содержать достаточно большие объёмы текста в файлах размером менее 12,5 Кб. Файл электронных таблиц MS Exel с одним байтом информации имеет размер 8 458 байт, что также позволяет хранить в нем достаточно данных. При этом его объем не будет превосходить 12,5 Кб.

Обнаруженные особенности механизма стирания информации на накопителе Samsung 870 EVO MZ-77E500BW, в первую очередь, в зависимости отработки команды TRIM от размера файла и наличии «хвостов» файлов при их затирании, были также обнаружены на накопителях Samsung 860 EVO MZ-76E500BW и Crucial CT480BX500SSD1, поэтому целенаправленные исследования особенностей выполнения команды TRIM на этих накопителях являются целью дальнейших исследований.

Таким образом, программное восстановление удалённых данных на некоторых SSD-накопителях даже с включёнными командами TRIM или Deallocate вполне может быть результативным, особенно, для файлов небольшого размера. Для реализации надёжного программного затирания файлов, необходимо использовать специализированные инструменты, которые эффективно работают на HDD-носителях, и делают невозможным программное восстановление данных на SSD-носителях. В тоже время понятно, что они не смогут обеспечить гарантированное затирание данных файла на микросхемах памяти SSD, ввиду специфики работы технологии выравнивания износа (Wear Leveling). Следовательно, вопрос гарантированного затирания отдельных файлов на SSD-носителях остаётся актуальным.

Литература

1. Корнвелл М. «Анатомия твердотельного накопителя» Communications of the ACM, 2012, том 55, №12, С. 59–63.

2. Технология выравнивания износа в устройствах с флэш-памятью nand. [Электронный ресурс]. URL: https://www.micron.com/-/media/client/global/documents/products/technical-note/nand-flash/tn2942_nand_wear_leveling.pdf

3. Рент Т.М. «SSD контроллер». [Электронный ресурс] 9 Апр. 2010.

4. Мартин Н., Зиммерман Д., «Анализ вызовов устройствами с флеш-памятью для криминалистов». Университет Небраски, 15 окт. 2015.

5. Губанов Ю.А., Афонин О.А., "Восстановление данных на SSD накопителях: Понимание TRIM, сборки мусора и исключений" 2014. [Электронный ресурс]. URL: https://belkasoft.com/ssd-2014.

References

1. Kornvell M. «Anatomiya tverdotel'nogo nakopitelya» Communications of the ACM, 2012, tom 55, №12, P. 59–63.

2. Tekhnologiya vyravnivaniya iznosa v ustroystvakh s flesh-pamyat'yu nand. [Elektronnyy resurs]. URL: https://www.micron.com/-/media/client/ global/documents/products/technical-note/nand-flash/tn2942_ nand_wear_ leveling.pdf

3. Rent T.M. «SSD kontroller». [Elektronnyy resurs] 9 Apr. 2010.

4. Martin N., Zimmerman D., «Analiz vyzovov ustroystvami s flesh-pamyat'yu dlya kriminalistov». Universitet Nebraski, 15 okt. 2015.

5. Gubanov YU.A., Afonin O.A., "Vosstanovleniye dannykh na SSD nakopitelyakh: Ponimaniye TRIM, sborki musora i isklyucheniy" 2014. [Elektronnyy resurs]. URL: https://belkasoft.com/ssd-2014.

КУЦ Дмитрий Владимирович, старший преподаватель Учебно-научного центра «Информационная безопасность» Уральского федерального университета имени первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: d.v.kutc@urfu.ru

ПОРШНЕВ Сергей Владимирович, доктор технических наук, профессор, директор Учебно-научного центра «Информационная безопасность» Уральского федерального университета имени первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: s.v.porshnev@urfu.ru

КУЦ Мария Петровна, преподаватель кафедры Иностранных языков и образовательных технологий, Уральского федерального университета имени первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Куйбышева, 48а. E-mail: m.p.kutc@urfu.ru

KUTS Dmitry Vladimirovich, senior teacher of the Training and Scientific Center "Information Security", Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Sverdlovsk region, Ekaterinburg, Mira street, 19. E-mail:d.v.kutc@urfu.ru

PORSHNEV Sergey Vladimirovich, Doctor of Technical Sciences, Full Professor, Head of Unit, Training and Scientific Center "Information Security", Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Sverdlovsk region, Ekaterinburg, Mira street, 19. E-mail: s.v.porshnev@urfu.ru

KUTS Maria Petrovna, teacher of the Department of Foreign Languages and Educational Technologies, Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Sverdlovsk region, Ekaterinburg, Kuibysheva street, 48a. E-mail:m.p.kutc@urfu.ru