УДК 004.324 Вестник УрФО № 1(51) / 2024, с. 39–44

Куц Д.В., Поршнев С.В., Соколов И.П., Куц М.П.

DOI: 10.14529/secur240105

АНАЛИЗ ПРОБЛЕМЫ НАДЁЖНОГО УДАЛЕНИЯ ФАЙЛОВ НА ТВЕРДОТЕЛЬНЫХ НАКОПИТЕЛЯХ И ПОДХОДОВ К ЕЕ РЕШЕНИЮ

В статье проводится анализ проблемы надёжного удаления отдельных файлов на твердотельных накопителях, обусловленные их структурно-функциональными особенностями, которые являются основной причиной, не позволяющей реализовать их эффективное удаление с данного типа накопителей, например, используя для этого штатные средства операционной системы, специализированное программное обеспечение от производителя накопителя или специализированные программные решения, доказавшие свою эффективность для накопителей на жёстких магнитных дисках.

Описаны известные методы решения данной проблемы. Предложена классификация данных методов. Приведены оценки возможности практического использования данных методов.

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

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

WAYS TO SOLUTION THE PROBLEM OF RELIABLE DELETION OF INDIVIDUAL FILES ON SOLID-STATE DRIVES

The article analyzes the problem of reliable deletion of individual files on solid-state drives, due to their structural and functional features, which are the main reason that does not allow their effective removal from this type of drive, for example, using standard operating system tools, specialized software from drive manufacturer or specialized software solutions that have proven their effectiveness for hard disk drives. Known methods for solving this problem are described. A classification of these methods is proposed. Assessments of the possibility of practical use of these methods are given.

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

Введение

Твердотельный накопитель (англ. Solid-State Drive, SSD), в отличие от более традиционных накопителей, например, таких как жёсткий диск, имеет более сложную структуру организации хранения информации в ячейках памяти. Данное обстоятельство обусловлено ограниченным ресурсом ячеек памяти после каждого стирания данных, находящихся в ячейке, происходит её постепенная деградация на физическом уровне. Для продления длительности жизни накопителя контроллер SSD реализует такой режим записи данных на диск, в котором количество стираний данных в ячейках, а, следовательно, и количество записей в каждую ячейку накопителя было одинаковым. Этим обеспечивается максимальная продолжительность жизни накопителя. Равномерный износ ячеек памяти обеспечивается реализацией в накопителе технологии «выравнивания износа» (англ. Wear Leveling, WL).

Технология WL [1] основана на совместном использовании абстрагированного логического адресного пространства SSD-накопителя и физических адресов ячеек памяти микросхем. Что, в свою очередь, обеспечивается технологией, реализующей алгоритм трансляции адресов флеш-памяти (англ. Flash Translation Layer, FTL), которая позволяет установить взаимно однозначное соответствие между логическими и физическими адресами ячеек флэш-памяти (англ. not and, NAND) SSD-накопителей. В данном алгоритме в случае записи новых данных на SSD-накопитель логические адреса физических адресов NAND-ячеек памяти заменяются на адреса менее изношенных NAND-ячеек, что и обеспечивает равномерный износ каждой ячейки памяти носителя на твердотельном накопителе [2].

Описанные выше особенности технологии FTL, приводят к тому, что при попытке стирания файла, путём перезаписи его содержимого, контроллер SSD с большой вероятностью подменит адреса ячеек и запись произойдёт в другие ячейки памяти. При этом ранее использованные ячейки, которых размещалось содержимое данного файла останутся не затёртыми. В этой связи в [2] был сделан обоснованный вывод о невозможности осуществления гарантированного затирания отдельных файлов на твердотельных накопителях в процессе его эксплуатации с помощью методов, рекомендованных действующей нормативно-правовой базой и зарубежными стандартами.

В настоящей статье авторами будет проведён анализ известных методов, обеспечивающих по мнению их авторов, гарантированное затирание отдельных файлов, удаляемых с SSD-носителя.

Анализ методов затирания отдельных файлов на твердотельных накопителях

Проблема стирания отдельных файлов на SSD-накопителях была впервые поднята исследовании «Reliably Erasing Data From Flash-Based Solid State Drives» [3], авторы которого описали результаты серии проведённых ими экспериментов, указывающих на невозможность осуществить полное затирание файлов традиционными инструментами, которые эффективно работали на жестких дисках. Таким образом, оказалось, что стирание определенных областей на SSD-накопителях, в связи с отсутствием соответствующих инструментов, является нетривиальной задачей.

Для ее решения в [3] предложено модифицировать слой абстракции твердотельного накопителя (FTL) с целью проведения процедуры принудительной сборки мусора контроллером SSD, для стирания данных файла сразу после завершения процедуры его удаления. В качестве альтернативного способа решения проблемы авторы предложили одновременно проводить фоновую сборку мусора удалённых файлов и продемонстрировали, что применение данного способа позволяет увеличить скорость работы накопителя. Ещё один предложенный авторами метод - затирание со сканированием. В процессе его практического использования контроллер твердотельного накопителя сканирует свободные области накопителя и, в случае обнаружения блоков, занятых данными, осуществляет их стирание. Все три метода были опробованы на модели твердотельного накопителя и, в целом, показали достаточную эффективность. Однако, практическое применение данных методов вызывает серьёзные сомнения. Во всех случаях требуется модификация прошивки контроллера SSD, что трудноосуществимо, учитывая многообразие производителей и решений в этой области.

Во всех случаях снижалась производительность и долговечность устройства.

Еще два подхода решению проблемы затирания отдельных файлов предложен в [4]. В основу первого подхода положены идеи использовании криптографических методов, обеспечивающих безопасное удаление данных без их перемещения, которые, однако, используют существенные вычислительные ресурсы, что приводит к существенному уменьшению скорости записи/считывания данных с SSD-накопителя. В основу второго подхода – стирание информации на уровне блоков данных SSD-накопителей (изменение каждого из битов данного блока, используемых для хранения не удаленных данных с нуля на единицу), использование которого, однако, приводит к увеличению энергопотребления, снижению производительности и сокращению срока службы SSD, поскольку каждый блок может выдержать лишь ограниченное количество циклов записи/стирания. Результаты проведенных авторами [3] экспериментов показали достаточную эффективность второго подхода и незначительное снижение производительности SSD-накопителя. Однако, оказалось, что его практическое использование требует существенной доработки прошивки SSD-накопителя, что затрудняет его применение.

Еще один метод, призванный обеспечить гарантированное удаление информации на SSD-носителях, предложены в [5]. Он основан на использовании программного шифрования данных и, по своей сути оказывается близким к системе шифрования данных EFS (англ. Encrypting File System), реализующей шифрование на уровне файлов в операционных системах Microsoft Windows NT для файловой системы NTFS. В данном методе каждый файл шифруется индивидуальным ключом, который получается путём хеширования пароля пользователя, общего для всей системы, и добавляемой соли, в роли которой выступает имя файла. В криптографии соль – последовательность данных, добавляемая к хешируемому блоку данных, в нашем случае – паролю пользователя, с целью чтобы хэш – функция от одинаковых блоков данных имела разные значения. При этом для обеспечения надёжного удаления файла, стирается информация о ключе шифрования из главной файловой таблицы (Master File Table, MFT) NTFS, данные же файла, затираются с помощью команды TRIM интерфейса SATA (англ. Serial Advanced Technology Attachment), позволяющей операционной системе уведомить твердотельный накопитель о том, какие блоки данных (страницы) не несут полезной нагрузки и их можно не хранить физически.

Однако данный метод оказывается не вполне надёжным, так как стойкость шифрования будет во многом обеспечиваться стойкостью пароля пользователя. Хотя имя файла также хранится в зашифрованном виде, для многих файлов его легко установить с помощью методов компьютерной криминалистики и реализовать атаку перебора пароля по хешу с известной солью. На современных высокопроизводительных платформах скорость такого перебора может достигать 1 трлн паролей в секунду и выше, что позволяет перебирать даже весьма сложные пароли за обозримый интервал времени. Кроме того, затирание данных на твердотельном накопителе с помощью команды TRIM не всегда эффективно. Например, в [6] демонстрировано, что программное восстановление удалённых данных на некоторых SSD-накопителях даже с включёнными командами TRIM или Deallocate вполне может быть результативным, особенно, для файлов небольшого размера.

Кроме того, в [3] продемонстрировано, что даже при успешно отработавшей команде TRIM, удаляемые данные могут оставаться на накопителе ещё достаточно продолжительное время, пока до них не доберётся сборщик мусора. Отдельные области в MFT, где хранятся метаданные удаляемого файла, можно затирать только программно, т.к. в этом случае команда TRIM оказывается бесполезной, т.к. файловая система воспринимает MFT как отдельный файл, чем, по сути, она и является. В этом случае весьма высока вероятность восстановить метаданные файла. В текущей реализации обсуждаемый метод также не сможет работать с файловой системой, отличной от NTFS.

В этой связи в данном методе используется исключительно программное шифрование, что также негативно сказывается на производительности системы. Подводя итоги, можно сказать, метод, предложенный в [5], не является универсальным в части поддерживаемых файловых систем, не обладает достаточной надёжностью и не имеет достаточной производительности. В тоже время, метод не требует модификации прошивки контроллера твердотельного накопителя, существенно усложняет процесс восстановления удалён-

ных данных на SSD-накопителе и, при некоторой доработке, может быть использован для других файловых систем, например, семейства EXT в операционных системах Linux. Однако главную задачу – надёжного удаления отдельного файла на твердотельном накопителе данный метод решает не в полной мере.

В [7] предложено встраивать систему страничного шифрования в общий уровень трансляции флэш-памяти FTL твердотельного накопителя. Суть метода состоит в следующем. Шифрование осуществляется для каждой страницы перед сохранением ее во флэш-памяти NAND и перед извлечением данных осуществляется их расшифровка для каждой страницы. Хранение ключей организуется в определенном участке флэш-памяти, известном как Зона Хранения Ключей. При удалении определённого файла, удаляется блок, в котором расположены ключи шифрования файла. Ключи шифрования хранятся в заголовке страницы памяти NAND. Очистка производится на каждом блоке области хранения ключей. При очистке выбирается новый блок области хранения ключей для копирования использующихся ключей, находящиеся в тех же местах. Эксперименты, проведённые авторами, подтвердили высокую эффективность предложенного метода. Однако, как и в ряде предыдущих работ, данный метод требует модификации прошивки контроллера, что весьма затруднительно на практике.

В [8] предложен метод частичной очистки данных в многоуровневых ячейках Multi Level Cell (MLC) флэш-памяти с использованием однократной записи. В данном методе применяется однократная запись для затирания данных на страницах MSB (Most Significant Bit, хранящих два старших бита ячейки) и LSB (Least Significant Bit, хранящих два младших бита ячейки). Проведенные авторами [8] эксперименты показали, что затирание лишь половины данных в ячейке памяти, в первую очередь LSB, является достаточно надёжным методом, и не позволяет осуществить эффективное восстановление данных. Однако метод не применим на более современной памяти твердотельных накопителях типа TLC (Triple Level Cell, с трехуровневыми ячейками памяти) и QLC (Quad Level Cell, с четырёхуровневыми ячейками памяти), о чём пишут сами авторы в [8], в связи с иной, более сложной организацией хранения данных.

Результаты проведенного нами анализа известных методов затирания отдельных файлов, находящихся на SSD-накопителях, в обобщенном виде оказывается удобным представить в виде сводной таблицы (табл. 1).

Таблица 1

Результаты сравнительного анализа методов затирания файлов, находящихся на SSD-накопителях

Метод затирания файла	Программная универсальность	Аппаратная независимость	Производительность	Срок службы	Надёжность затирания
Принудительная сборка мусора	Не зависит от файловой системы и ОС	Требуется модификация прошивки контроллера	Существен-но снижена	Сущес-твен-но снижен	Высокая
Криптографическое стирание с принудительной сборкой мусора	Не зависит от файловой системы и ОС	Требуется модификация прошивки контроллера	Незначи-тель-но снижена	Незначи-тельно снижен	Высокая
Программное шифрование данных	Работает только на NTFS в среде Windows.	Не зависит от типа SSD и его производителя	Существен-но снижена	Не влияет	Низкая
Шифрование, встроенное в FTL	Не зависит от файловой системы и ОС	Требуется модификация прошивки контроллера	Незначи-тель-но снижена	Незначи-тельно снижен	Высокая
Метод частичной очистки данных	Не зависит от файловой системы и ОС	Требуется модификация прошивки контроллера	Незначи-тель-но снижена	Незначи-тельно снижен	Высокая

Из табл. 1 видно.

1. Сегодня не существует единого универсального метода стирания файлов на SSD-носителях.

2. Все известные методы могут быть классифицированы на следующие группы:

1) методы, требующие модификации прошивки контроллера, оказывающиеся неприменимыми на практике, так как на защищаемых компьютерах устанавливаются твердотельные накопители от разных производителей с различными микросхемами памяти и внутренними алгоритмами работы контроллера;

2) программные методы, которые, не смотря на свою аппаратную независимость, зачастую не обладают достаточной надёжностью затирания данных, что не исключает их последующего восстановления;

3) технологии криптографического стирания данных, реализованные во многих твердотельных накопителях, предназначены не для затирания отдельных файлов, но затирания сразу всего накопителя. Использование аппаратных возможностей SSD для криптографического стирания отдельных файлов требуют модификации прошивки контроллера.

Следовательно, разработка надежного универсального алгоритма гарантированного удаления файлов, размещенных на SSD-накопителях, имеющего приемлемую, с точки зрения практики, скорость работы, и наказывающего существенного влияния на его производительность и срок службы является актуальной. Результаты проводимых авторами исследований в данной области являются предметом последующих публикаций.

Литература

1. Куц Д.В., Поршнев С.В., Соколов И.П., Куц М.П: К постановке проблемы затирания отдельных файлов на твердотельных накопителях. Сетевой научный журнал «Инженерный вестник Дона», №2, 2024. URL: http://www.ivdon.ru/uploads/article/pdf/IVD_16__2y24_kuts_porshnev_sokolov_kuts.pdf_82cac7b31d.pdf (дата обращения: 25 марта 2023 г.).

2. Куц Д.В., Поршнев С.В., Куц М.П: Анализ механизмов удаления файлов на твердотельных накопителях//Вестник УРФО. Безопасность в информационной сфере. 2022, № 3(45) 2022, с. 17–23.

3. Michael Wei, Laura Grupp, Steven Swanson: Reliably Erasing Data From Flash-Based Solid State Drives. Proceedings of the FAST, Volume 11,2011.

4. Chen Liu, Hoda Aghaei Khouzani, and Chengmo Yang: ErasuCrypto: A Light-weight Secure Data Deletion Scheme for Solid State Drives. Proceedings of the Privacy Enhancing Technologies; 2017 (1):132–148.

5. Younsung Choi, Donghoon Lee, Woongryul Jeon, Dongho Won: Password-Based Single-File Encryption and Secure Data Deletion for Solid-State Drive. ICUIMC '14: Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication. January 2014. No.: 5. Pages 1–7.

6. Куц Д.В., Куц М.П: Deleted Data Recovery on Solid-State Drives by Software Based Methods. Proceedings of the 2022 Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT).

7. Singh, Bhupendra, Ravi Saharan, Gaurav Somani, Gaurav Gupta: Secure File Deletion for Solid State Drives. Proceedings of the IFIP International Conference on Digital Forensics, pp. 345-362. Springer, Cham, 2016.

8. Instant Data Sanitization on Multi-Level-Cell NAND Flash Memory. Proceedings of the 15th ACM International Conference on Systems and Storage. June 2022, p. 85–95.

References

1. Kuts D.V., Porshnev S.V., Kuts M.P: Analiz mekhanizmov udaleniya fajlov na tverdotel'nyh nakopitelyah. "Vestnik URFO. Bezopasnost' v informacionnoj sfere" ISSN 2225-5435, № 3(45) / 2022, str. 17-23. URL: http://www.ivdon.ru/uploads/article/pdf/IVD_16__2y24_kuts_porshnev_sokolov_kuts.pdf_82cac7b31d.pdf (date of the application: 25 march 2023 г.).

2. Kuts D.V., Porshnev S.V., Sokolov I.P., Kuts M.P: K postanovke problemy zatiraniya otdel'nyh fajlov na tverdotel'nyh nakopitelyah. Setevoj nauchnyj zhurnal «Inzhenernyj vestnik Dona» №2 2024. ISSN 2073-8633

3. Michael Wei, Laura Grupp, Steven Swanson: Reliably Erasing Data From Flash-Based Solid State Drives. Proceedings of the FAST, Volume 11,2011.

4. Chen Liu, Hoda Aghaei Khouzani, and Chengmo Yang: ErasuCrypto: A Light-weight Secure Data Deletion Scheme for Solid State Drives. Proceedings of the Privacy Enhancing Technologies, 2017 (1), p 132–148.

5. Younsung Choi, Donghoon Lee, Woongryul Jeon, Dongho Won: Password-Based Single-File Encryption and Secure Data Deletion for Solid-State Drive. ICUIMC '14: Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication. January 2014. No.: 5. Pages 1–7.

6. Kuts D.V., Kuts M.P: Deleted Data Recovery on Solid-State Drives by Software Based Methods. Proceedings of the 2022 Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT).

7. Singh, Bhupendra, Ravi Saharan, Gaurav Somani, Gaurav Gupta: Secure File Deletion for Solid State Drives. Proceedings of the IFIP International Conference on Digital Forensics, pp. 345-362. Springer, Cham, 2016.

8. Instant Data Sanitization on Multi-Level-Cell NAND Flash Memory. Proceedings of the 15th ACM International Conference on Systems and Storage. June 2022, p. 85–95.

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

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

СОКОЛОВ Илья Петрович, старший преподаватель Учебно-научного центра «Информационная безопасность», Уральский федеральный университет имени первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Мира, 19. E-mail: ipsokolov@urfu.ru

SOKOLOV Ilya Petrovich, senior teacher of the Training and Scientific Center "Information Security", Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Ekaterinburg, Mira street, 19. E-mail: ipsokolov@urfu.ru

КУЦ Мария Петровна, преподаватель кафедры Иностранных языков и образовательных технологий, Уральский федеральный университет имени первого Президента России Б.Н. Ельцина. 620002, г. Екатеринбург, ул. Куйбышева, 48а. E-mail: m.p.kutc@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, Ekaterinburg, Kuibysheva street, 48a. E-mail: m.p.kutc@urfu.ru