К постановке проблемы затирания отдельных файлов на твердотельных накопителях

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

Уральский федеральный университет, Екатеринбург

Аннотация: В работе рассматриваются проблемы, связанные с гарантированным уничтожением информации, находящейся на твердотельных накопителях (*Solid-State Drive (SSD)*, диск). Проведен анализ требований к используемым методам гарантированного уничтожения информации, определенных в действующей отечественной нормативно-правовой базе и зарубежных стандартах. Рассмотрены особенности архитектуры твердотельных накопителей с точки зрения возможности применения рекомендаций отечественных и зарубежных стандартов затирания данных и поставлена проблема гарантированного затирания отдельных файлов на накопителях без возможности их восстановления, без их вывода из эксплуатации и физического уничтожения. Сделаны обоснованные выводы о невозможности эффективного осуществления гарантированного затирания отдельных файлов на твердотельных накопителях в процессе эксплуатации с помощью методов, рекомендованных действующей нормативно-правовой базой и зарубежными стандартами.
Ключевые слова: TRIM, deallocate, data recovery, восстановление данных, solid-state drive, твердотельный накопитель, wear-leveling, выравнивание износа, сборка мусора, гарантированное уничтожение данных, data sanitazing.

Введение

Одним из неотъемлемых этапов жизненного цикла накопителя информации в компьютерных системах является этап его вывода из эксплуатации с последующим гарантированным затиранием данных на этом накопителе. Необходимость данной процедуры может возникать вследствие замены накопителя по причине его критических сбоев, также по причине морального устаревания или плановой замены. Процедура затирания направлена на полное и необратимое удаление информации с носителя с целью предотвращения возможности восстановления этих данных злоумышленниками или неавторизованными лицами.

Она оказывается особенно важной при утилизации или перераспределении старого оборудования, так как в случае продажи, передачи или утилизации накопителей информации без должного удаления данных, существует риск утечки конфиденциальной информации. Например,

авторы [1, 2] на основе анализа статистики утверждаются, что практически половина накопителей, проданных на вторичном рынке, содержала сведения конфиденциального характера.

Одновременно существует проблема гарантированного затирания отдельных файлов, содержащих сведения конфиденциального характера, в процессе работы с накопителем без вывода его из эксплуатации. При этом процесс затирания отдельных файлов не должен затрагивать остальные файлы, находящиеся на данном накопителе.

Актуальность проблемы затирания данных без возможности их восстановления на накопителях подтверждается результатами анализа действующих отечественных и зарубежных нормативно-правовых актов, стандартах, требованиях и приказах уполномоченных органов, обсуждаемых далее.

В соответствие со «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации ФСТЭК РФ» (СТР-К) по окончании обработки защищаемой информации или при передаче управления другому лицу пользователь обязан произвести стирание временных файлов на несъёмных носителях информации. При этом, в соответствии с ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования», комплекс средств защиты (КСЗ) должен осуществлять очистку оперативной и внешней памяти. Очистка должна производиться путем записи маскирующей информации в память при ее освобождении (перераспределении).

В Федеральном законе № 152 «О персональных данных» от 27.07.2006 г. (152-ФЗ) также указывается, что уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе

персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных. Кроме этого, в приказе ФСТЭК № 235 от 21 декабря 2017 г. «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования», указывается на необходимость обеспечить уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации при выводе значимого объекта КИИ из эксплуатации. В нормативно-правовых актах также заявляется необходимость обеспечивания контроля за работой систем защиты, что подразумевает и контроль над эффективностью реализации гарантированного затирания данных.

Для гарантированного затирания информации с накопителя в Российской Федерации используется метод затирания данных по ГОСТ Р 50739-95, который реализуется в двух вариантах. Первый – это запись случайной последовательности байт на место затираемых данных. Второй – запись сначала нулей, затем случайной последовательности байт. При этом необходимо отметить, что в ГОСТ Р 50739-95 не учитывается тип накопителя и используемой в нём памяти.

Для большинства типов накопителей осуществить контроль над перезаписью, удалением или затиранием данных несложно. Однако существуют определённые виды накопителей, на которых возможность произвести и тем более проконтролировать гарантированное затирание данных, будь то весь накопитель или же отдельные файлы, представляет значительную трудность.

Современными типами накопителей для хранения данных компьютерных систем являются твердотельные накопители или *SSD*-диски. Несмотря на более высокую стоимость памяти, твердотельные накопители

наиболее оптимальны с точки зрения сочетания факторов скорости и стоимости хранения данных [3], а также надёжности, долговечности и безотказности [4]. Для конечного пользователя *SSD*-диск выглядит достаточно похожим по своей логике работы, своим характеристикам на жесткий диск, за исключением скоростных показателей. Однако слой абстракции, обеспечиваемый контроллерами и жестких, и *SSD*-дисков, скрывает за собой совершенно разные виды технического исполнения. *SSD*-диски по своей внутренней структуре сильно отличаются от жестких дисков. На *SSD*-накопителях используются принципиально иные механизмы записи, хранения, удаления данных. Твердотельный накопитель регулярно меняет распределение ячеек памяти таким образом, что одному логическому адресу в разное время могут соответствовать разные адреса в микросхемах памяти устройства. Причина в применении на таких накопителях технологии выравнивания износа (*wear leveling*), которая позволяет увеличить срок службы накопителя за счёт обеспечения равномерного износа ячеек памяти. Происходит это путём подмены при записи адресов физических ячеек памяти на наименее изношенные. Вследствие этого, новые данные записываются в ячейки с иными физическими адресами. Обращаясь к ячейкам памяти для контроля перезаписи, мы получаем содержимое ячеек памяти, отличных от тех, в которых хранились изначальные затираемые данные.

Зарубежные руководства, стандарты и методы затирания данных

Одной из серьезных проблем, которые возникают вследствие особенностей внутреннего устройства *SSD*-диска, является гарантированное затирание информации на таких типах накопителей. Для разных видов накопителей и используемой в них памяти, существуют иностранные и отечественные стандарты обеспечения гарантированного затирания данных.

Суть этих стандартов сводится к затиранию всего накопителя или отдельных его областей путем записи в нужной области определенных

сигнатур данных, либо псевдослучайных, либо фиксированных, с несколькими циклами перезаписи, обычно от двух до нескольких десятков. Кроме того, ряд стандартов ориентируется на использование встроенных в накопитель процедур затирания данных или специально разработанных программ от производителя устройства. Для затирания критичных данных, в том числе данных, составляющих государственную тайну, многие стандарты требуют физического уничтожения накопителя. Ряд стандартов, например, Германский национальный стандарт VSITR и стандарт армии США Army Regulation 380–19 на данный момент утратили актуальность, однако процедуры стирания информации, предлагаемые в них, по-прежнему используются некоторыми инструментами для затирания данных.

Национальный стандарт Министерства обороны США *DoD* 5220.22-*M* для удаления информации с накопителей типа «жёсткий диск» с данными, содержащими совершенно секретную информацию, требует размагничивания диска с использованием специализированной аппаратуры. Для информации, категорией ниже, допускается затирание диска путём записи в каждый байт накопителя значений либо 0x00, либо 0xFF, с последующим контролем записи, затем записи значений, противоположных предыдущему циклу с контролем записи, затем записи случайных значений с контролем записи. Для флэш-памяти *FEPROM* обсуждаемый стандарт предусматривает однократную запись каждого байта накопителя любым повторяющимся значением и последующее стирание данных на накопителе с использованием инструмента, предоставляемого производителем устройства, либо полное физическое уничтожение накопителя, с использованием, например, шредера. При этом стандарт не регламентирует затирание отдельных файлов или областей памяти, но только целиком накопителя.

Для затирания данных отдельных файлов или каталогов в настоящее время на рынке представлено большое число программных инструментов для

каждой из используемых операционных систем, например, для Windows утилита *cipher*. Отметим полное затирание данных, находящихся на *SSD*-накопителе в *NAND*-памяти, являющейся разновидностью *FEPROM*-памяти, в ряде случаев оказывается невозможным даже с помощью утилит, поставляемых производителем данного устройства [5].

Дополнение стандарта *DoD* 5220.22-M *ECE* предусматривает затирание накопителя в 7 проходов. При этом, де-факто, реализуются два полных цикла стандарта *DoD* 5220.22-*M* и дополнительная запись в каждую ячейку накопителя псевдослучайных чисел.

В стандарте *NAVSO P*-5239-26 ВМС США, известный также, как «*Department of the Navy (DON) Standard for the Secure Erasure of Solid State Storage (SSS)*», даны рекомендации и установлены требования для безопасного удаления данных с накопителей на основе твердотельных носителей (*SSS*) в военных организациях ВМС США (*Department of the Navy*). Для *SSS*-накопителей стандарт *NAVSO P*-5239-26 предусматривает пятикратную перезапись на диск произвольных данных. При этом, перед началом процесса затирания, рекомендуется удалить с *SSS*-накопителя все зашифрованные ключи или данные, связанные с шифрованием. В случае, если *SSS*-накопитель не может быть безопасно затерт, например, из-за физического повреждения или неисправности, стандарт *NAVSO* P-5239-26 рекомендует физическое уничтожение накопителя, чтобы предотвратить возможность восстановления данных.

Стандарт США *Guidelines for Media Sanitization*» 800-88, разработанный Национальным институтом стандартов и технологий (*National Institute Standarts* NIST), содержит руководство по безопасному удалению информации с электронных носителей данных, в том числе, с жестких дисков (*HDD*), твердотельных дисков (*SSD*), магнитных лент, оптических дисков и других устройств хранения цифровой информации. В

случае поддержки устройством, данный стандарт рекомендует использовать команду *ATA Sanitize* с опцией стирания блоков (*Block Erase*) или криптографического стирания (*Cryptographic Erase*), так как подобные команды работают быстрее, чем перезапись стандартным способом. В случае применения опции стирания блоков, обсуждаемый стандарт рекомендует однократное выполнение процедуры стирания блоков, далее запись во все доступные области накопителя единицы и затем повторное использование процедуры стирания блоков. Если применяется опция криптографического стирания, стандарт рекомендует выполнить процедуру криптографического стирания блоков однократно, затем выполнить процедуру стирания с опцией *Block Erase*. Если опция *Block Erase* не поддерживается устройством, следует выполнить любую из процедур очистки данных, регламентированных стандартом. Также стандарт позволяет, в случае поддержки устройством, для затирания данных использовать спецификации *TCG Opal SSC* или *Enterprise SSC*, разработанные для накопителей с встроенным шифрованием данных.

С целью обеспечения гарантированного затирания накопителей стандарта *NVM PCI Express,* стандарт *NIST* 800-88 рекомендует использовать команды форматирования *NVM Express Format*, для устройств, поддерживающих данные команды. При этом команда *NVM Express Format* вызывается с опцией *User Data Erase* или с опцией *Cryptographic Erase*. После успешного применения процедуры *Cryptographic Erase* обсуждаемый стандарт рекомендует выполнить команду стирания с опцией *User Data Erase* или команду очистки накопителя.

В стандарте *NIST* 800-88 также определены такие методы затирания данных, как методы *Clear* (Очистка) и *Purge* (Очистка с принудительным удалением). Эти методы предполагают удаление данных с носителя без возможности их восстановления. Метод *Clear* обычно применяется для носителей, на которых не хранились критические данные, и может включать

в себя однократное перезаписывание данных с использованием нулей или случайных значений. Метод *Purge* включает многократное перезаписывание данных с использованием определенных шаблонов для обеспечения надежного удаления информации.

Стандарт ВВС США *Air Force System Security Instruction* 5020 аналогичным образом требует для затирания *EEPROM*-памяти применения специальных программных продуктов, разработанных производителем устройства. После процедуры затирания стандарт рекомендует записать любую несекретную информацию во все блоки с данными. Как и в предыдущем стандарте, отсутствуют рекомендации по затиранию отдельных файлов на накопителе.

Стандарт *Air Force System Security Instruction* 8580, последний из разработанных стандартов данного типа для ВВС США на текущий момент, рекомендует реализацию двух проходов записи псевдослучайных данных, за которыми следует перезапись с заданным набором единиц и нулей и далее проверку, как минимум 1% окончательных перезаписанных данных, для того, чтобы гарантировать успешное затирание.

В ранее закрытом стандарте армии США *Army Regulatio*n 380–19 для затирания *FEPROM*-памяти рекомендуется проводить последовательно перезапись на диск случайных данных, далее постоянных значений и затем инвертированный байт. Также стандарт предусматривает дополнительную проверку записанных данных и применение дополнительных процедур затирания, если в ходе последующей проверки диска были обнаружены какие-либо сбои.

Стандарт министерства энергетики США *DOE M* 205.1-2 предусматривает затирание *FEPROM*-памяти в три этапа. Сначала затирание с использованием инструментов производителя памяти, затем дважды заполнение всего пространства накопителя случайными данными, после

этого однократное заполнение данными любого формата и проведение контроля над результатами выполнения описанной последовательности команд.

Стандарт Агентства Национальной Безопасности США *NSA* 130-1 рекомендует трехпроходную перезапись данных: сначала на носитель информации записываются псевдослучайные данные, далее другой набор случайных данных и затем данные, имеющие известную сигнатуру. Этот процесс завершается проверкой записанных данных.

В ФРГ требования к безопасности уничтожения данных на физических носителях информации установлены стандартом *DIN* 66399, в котором определены уровни защиты и соответствующие методы затирания данных. В соответствии с *DIN* 66399, методы затирания данных классифицируются по нижеследующим уровням и подуровням.

Уровень О (низкий уровень защиты):

– Подуровень О-1: уничтожение данных без специальных требований к безопасности (например, удаление данных с помощью стандартных функций операционной системы, форматирование носителя или обычное удаление файлов).

– Подуровень О-2: обычное уничтожение данных (например, перезапись данных с помощью программного обеспечения для стирания).

Уровень Т (средний уровень защиты):

– Подуровень Т-1: средняя степень уничтожения (например, многократное перезаписывание данных с использованием специализированного программного обеспечения для стирания).

– Подуровень Т-2: высокая степень уничтожения (например, физическое разрушение носителей данных с помощью измельчителей, дробилок или гильотин):

Уровень Н (высокий уровень защиты):

– Подуровень H-3: очень высокая степень уничтожения с использованием физического разрушения носителей данных, применяющего специальное оборудование для уничтожения (например, мультирежущие системы или пиролиз).

Также в ФРГ используется национальный стандарт *VSITR* (*Verschlusssachen-IT-Richtlinie*), который регулирует безопасность информации, в том числе, методы удаления данных. Для уничтожения информации на электронных носителях в данном стандарте рекомендуется использовать процедуры однократных, трех- или семиэтапных процедур. При использовании семиэтапной процедуры затирания данных, в блоки данных последовательно записываются единицы, затем нули, далее снова единицы, и так до конца 6-го этапа. Затем, на 7-м этапе, носитель заполняется случайными данными. Затирание данных в этом стандарте не зависит от типа памяти. Стандарт также не предусматривает особых действий при работе с *EEPROM*-памятью.

Семейство стандартов *BSI*, разработанных Федеральным управлением информационной безопасности ФРГ, в части затирания данных включает в себя оригинальный стандарт *BSI*-2011-*VS*, стандарт *BSI-GS* и дополнения к нему - *BSI-GSE*. В стандарте *BSI*-2011-*VS* рекомендуется следующая процедура затирания данных:

1. запись носитель информации случайных данных;
2. проверка записанных данных с целью оценки эффективности стирания данных;
3. однократное повторение пп. 1,2.

Стандарт *BSI-GS* предусматривает однократное заполнение носителя данных случайными данными, проверку записи, затем затирание накопителя, с помощью программных инструментов производителя. В дополнении *BSI-GSE* стандарта *BSI-GS*, перед использованием инструмента затирания, от

производителя накопителя предусмотрен еще один этап записи случайных данных на носитель информации.

Британский стандарт *HMG Infosec Standard No.* 5 аналогичен стандарту *DOD* 5220.22-*M*. В нем определены два: базовый и расширенный методы перезаписи данных. В базовом методе данные в один проход посекторно перезаписываются нулями. В расширенном методе используется перезапись данных в 3 прохода. В первом проходе данные перезаписываются сигнатурой 0xFF, во втором 0x00, в третьем – псевдослучайными данными. Помимо перезаписи данных, стандарт также предусматривает использование размагничивания и физического уничтожение накопителя. Отметим, что стандарт не рекомендует применение технологии *Secure Erase*.

Международный стандарт *IEEE* 2883-2022 *Standard for Sanitizing Storage*, во многом основанный на стандарте *NIST* 800-88, является одним из самых современных стандартов в области затирания данных. Данный стандарт определяет следующие подходы к затиранию информации:

1. Затирание данных, затирание хранилищ данных и затирание накопителей. Здесь особое внимание уделяется удалению всех экземпляров хранимых данных, независимо от их местоположения, которые могут существовать в приложениях, облачных сервисах, виртуальных средах, основных вычислительных ресурсах и ресурсах хранения, вторичных и автономных хранилищах, архивах и системах защиты данных.

При затирании хранилищ данных, основное внимание фокусируется на данных, хранящихся в информационной инфраструктуре, использующей энергонезависимые хранилища (например, массивы хранения с фиксированными блоками, сетевые хранилища данных (*Network-attached storage (NAS)*), объектные хранилища, облачные хранилища и системы резервного копирования). Основной подход к затиранию накопителей в обсуждаемом стандарте ориентирован на данные, хранящиеся на

запоминающих устройствах и/или носителях информации. В этой связи стандарт рекомендует использовать следующие методы очистки для очистки физического устройства:

1. *Clear* (очистка).
2. *Purge* (очистка с принудительным удалением)
3. *Destruct* (уничтожение).

Выбор конкретного метода очистки зависит от типа очищаемого носителя и важности затираемых данных.

Метод *Clear* использует программные методы для удаления данных из всех адресуемых участков памяти, для защиты от попыток программного восстановления данных. Обычно используется для некритичных данных.

Метод *Purge* использует программные и физические методы для удаления данных из всех адресуемых и неадресуемых участков носителя информации, что делает невозможным восстановление данных лабораторными методами и позволяет повторно использовать устройство хранения данных.

Метод *Destruct* использует физические методы для разрушения носителя, что делает невозможным восстановление данных лабораторными методами и делает устройство непригодным для повторного использования. Стандарт использует такие техники затирания, как перезапись, блочное стирание, криптографическое стирание и размагничивание.

Известны также авторские методы затирания данных, которые были разработаны отдельными экспертами или организациями, среди которых выделим:

1. Метод Брюса Шнайера (*Bruce Schneier's Method*) [6] (Брюс Шнайер известный криптограф и эксперт в области безопасности информации). В данном методе используются: комбинация случайной записи данных, шаблоны записи и многократное перезаписывание, что обеспечивает

безопасное удаление информации с помощью семикратной перезаписи данных. В первые два прохода данные перезаписываются сигнатурой 0xFF, затем 0x00. Затем, в оставшиеся пять проходов, осуществляется перезапись случайными данными.

2. Метод Питера Гутмана (*Gutmann Method*) [7], в котором используется 35 проходов для перезаписи данных с использованием различных шаблонов. В ходе реализации первых 4-х проходов на носитель информации записываются случайные данные, проходы с 5 по 31 используют сигнатуры, созданные с учетом конкретных схем магнитного кодирования. Отметим, что в современных дисках эти старые методы кодирования не используются, что делает многие проходы метода Гутмана лишними [7]. Кроме того, уже более 20 лет, в конструкцию жестких дисков *ATA IDE* и *SATA* включена поддержка стандарта «*Secure Erase*», что устраняет необходимость применения метода Гутмана при очистке всего диска. Метод, исходя из вышеизложенного, может быть эффективно применим только к накопителям на жёстких магнитных дисках. По мнению экспертов, к твердотельной памяти данный метод также не применим, что признаёт, в том числе, и сам автор в [7].

3. Метод *Blancco SSD Erasure* является проприетарным методом группы компаний «*Blancco Technology Group*», суть которого состоит в использовании множественных перезаписей случайных данных и использовании инструментов от производителя устройства. По утверждению разработчика данного метода, он оказывается наиболее эффективным для *SSD*-накопителей. Однако, данный метод опять же не регламентирует затирание отдельных файлов на *SSD*-накопителях.

4. Криптографический метод стирания. В соответствии со стандартом *IEEE* 2883-2022, методы криптографического стирания изменяют ключ шифрования, оставляя на носителе только зашифрованный текст, что

приводит к безвозвратной утере данных. У производителей накопителей подобные методы, традиционно называются *Instant Secure Erase*, например, разработанные компаниями *Seagate* и *Western Digital*.

Отметим, что методы очистки накопителей *Secure Erase* и *Sanitize* поддерживаются большинством производителей устройств *SSD*. При этом метод *Secure Erase* позволяет быстро сделать данные на диске недоступными для использования и программного восстановления путём стирания таблицы размещения данных (*mapping table*), метод *Sanitize* заставляет *SSD*-накопитель реализовать процедуру стирания блоков, после стирания таблицы размещения данных. Когда проделана данная процедура, считается, что данные восстановить невозможно, даже с применением физических методов.

Рассмотренные стандарты затирания данных вполне эффективны для жестких дисков и некоторых других типов накопителей и памяти, например, флеш-накопителей с *FEPROM*-памятью. Однако, результаты проведённых исследований [7], свидетельствуют о том, что процедуры затирания даже многократными проходами, из-за особенностей внутренней архитектуры *SSD*-дисков, могут быть неэффективны. Также ряд исследованных накопителей не имели штатных утилит для обеспечения затирания накопителя, или же, в некоторых случаях даже после работы таких программ данные всё равно удавалось считать с микросхем памяти [8]. Эти результаты позволяют сделать обоснованный вывод о том, что некоторые существующие инструменты от производителей *SSD* недостаточно эффективны и надёжны. Данный вывод был в дальнейшем подтвержден [9, 10].

Заключение

Результаты проведенного анализа российских нормативно-правовых актов и зарубежных стандартов, действующих в области гарантированного уничтожения цифровой информации на накопителях, позволяют сделать обоснованный вывод о том, что в них не затрагиваются вопросы, связанные с

гарантированным затиранием информации, находящейся в отдельном файле. В связи с этим, производители средств защиты от несанкционированного доступа для затирания отдельных файлов предлагают использовать комбинированные методы, основанные на применении перезаписи с возможностью выбора количества циклов и типа записываемых данных. При этом, однако, оказывается невозможным использование встроенных команд накопителя для реализации режимов *secure erase* или *sanitaze*, а также криптографического стирания. Кроме того, использование инструментов от производителя устройства также не представляется возможным для затирания данных отдельного файла.

Следовательно, можно констатировать, что проблема эффективного, и надёжного затирания отдельных файлов на накопителях типа *SSD*, по-прежнему остается нерешенной. В связи с этим, создание методов стирания отдельных файлов, которое будет описано авторами данного исследования в последующих публикациях, по-прежнему актуально.

Литература

1. Майкл Хилл. Report: 42% of Used Drives Sold on eBay Hold Sensitive Data. 2019. URL: infosecurity-magazine.com/news/used-drives-sold-sensitive-data-1-1/

2. Privacy for Sale. Data Security Risks in the Second- Hand IT Asset Marketplace. 2022. URL: blancco.com/resources/rs-privacy-for-sale-data-security-risks-in-the-second-hand-it-asset-marketplace/

3. Пономарев В.А. Математические модели производительности, надежности и стоимости функционирования системы хранения дедуплицированных данных на SSD-дисках // Инженерный вестник Дона, 2019, №6. URL: ivdon.ru/ru/magazine/archive/n6y2019/6012

4. Пономарев В.А., Питухин Е.А. Концептуальная модель функционирования системы хранения данных на основе твердотельных

накопителей с технологией дедупликации // Инженерный вестник Дона, 2019, №5. URL: ivdon.ru/ru/magazine/archive/N5y2019/5905.

5. Wei Michael, Grupp Laura M., Spada Frederick E., Swanson Steven. Reliably Erasing Data From Flash-Based Solid State Drives. Proceedings of the 9th USENIX conference on File and stroage technologies. 2011. с. 8.

6. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002. с. 816.

7. Гутман П. Secure deletion of data from magnetic and solid-state memory. 1996. URL: cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

8. Raquibuzzaman M, Buddhanoy M., Milenkovic A., Ray B. Instant Data Sanitization on Multi-Level-Cell NAND Flash Memory. Proceedings of the 15th ACM International Conference on Systems and Storage. 2022 doi.org/10.1145/3534056.3534941

9. Reardon J., Basin D. and Capkun S. 2013. SoK: Secure Data Deletion. IEEE Symposium on Security and Privacy. pp. 301–315. doi.org/10.1109/SP.2013.28

10. Reardon J., Basin D. and Capkun S. 2014. On Secure Data Deletion. IEEE Security Privacy 12, 3 (May 2014), pp. 37–44. doi.org/10.1109/MSP.2013.159

References

1. Hill Michael. Report: 42% of Used Drives Sold on eBay Hold Sensitive Data. 2019. URL: infosecurity-magazine.com/news/used-drives-sold-sensitive-data-1-1/

2. Privacy for Sale. Data Security Risks in the Second- Hand IT Asset Marketplace. 2022. URL: blancco.com/resources/rs-privacy-for-sale-data-security-risks-in-the-second-hand-it-asset-marketplace/

3. Ponomarev V.A. Inzhenernyj vestnik Dona, 2019, №6. URL: ivdon.ru/ru/magazine/archive/n6y2019/6012

4. Ponomarev V.A., Pituhin E.A. Inzhenernyj vestnik Dona, 2019, №5. URL: ivdon.ru/ru/magazine/archive/N5y2019/5905.

5. Wei Michael, Grupp Laura M., Spada Frederick E., Swanson Steven. Proceedings of the 9th USENIX conference on File and stroage technologies. 2011. p. 8.

6. Shnajer B. Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnye teksty na yazyke Si. M. Triumf, 2002. p. 816.

7. Guttman P. Secure deletion of data from magnetic and solid-state memory. 1996. URL: cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

8. Raquibuzzaman M., Buddhanoy M., Milenkovic A., Ray B. Proceedings of the 15th ACM International Conference on Systems and Storage. 2022 doi.org/10.1145/3534056.3534941

9. Reardon J., Basin D. and Capkun S. 2013. IEEE Symposium on Security and Privacy. pp. 301–315. doi.org/10.1109/SP.2013.28

10. Reardon J., Basin D. and Capkun S. 2014. IEEE Security Privacy 12, 3 (May 2014), pp. 37–44. doi.org/10.1109/MSP.2013.159

Дата поступления: 1.01.2024

Дата публикации: 11.02.2024