МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

Институт кибербезопасности и цифровых технологий
(наименование института, филиала)

Кафедра КБ-2«Прикладные информационные технологии»
(наименование кафедры)

ПРАКТИЧЕСКАЯ РАБОТА

по дисциплине: «Основы информационной безопасности»

Уничтожение (очистка) остаточной информации в полупроводниковых и магнитных ЗУ
(задание)

Задание получил:

_1_ курс, группа _БИСО-02-23_ ___23Б0667___
Шифр

___Макаревич Сергей В.___
ФИО

Проверил:

«__»_____2023 г. _____
Дата *Подпись*

_____ _____
Отметка / результат *ФИО*

Москва 2023 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Цель работы:

1) Изучение способов и инструментов удаления остаточной информации из полупроводниковых и магнитных запоминающих устройств.

2) Приобретение опыта в использовании программных средств для уничтожения и восстановления данных в запоминающих устройствах.

1 План выполнения работы

Шаги выполнения работы:

1) Удалить файл и следить за процессом удаления при использовании стандартных средств операционной системы Windows.

2) Осуществить восстановление файла после его удаления стандартными средствами операционной системы Windows.

3) Изучить методы безвозвратного удаления данных с электронных носителей путем повторного перезаписывания.

4) Проконтролировать процесс удаления файла при помощи программы-ширедера, осуществляющей многократную перезапись.

2 Состав оборудования для работы

Перечень оборудования:

1) Персональный компьютер (ПК).

2) Отформатированный съемный носитель для проведения тестов (флешка).

3 Необходимое программное обеспечение

Перечень необходимых программ:

1) Eraser – программа-шреддер.

2) Back2Life - программа для восстановления удаленных файлов.

3) HxD - hex-редактор.

4 Проблема остаточной информации

Остаточная информация представляет собой данные, которые остаются на запоминающем устройстве после формального удаления данных. Эта информация может сохраняться из-за процесса формального удаления или в результате физических характеристик запоминающих устройств. В обоих случаях возможно появление непреднамеренной утечки конфиденциальной информации, если хранилище данных выходит из-под контроля, например, при выбрасывании с мусором или передаче третьей стороне. Проблема надежного удаления конфиденциальной информации представляет интерес как для крупных компаний, стремящихся предотвратить утечку коммерческих секретов, так и для обычных пользователей, которые беспокоятся о защите личной информации.

5 Возникновение остаточной информации

Многие операционные системы, файловые менеджеры и другие программы предоставляют пользователю возможность перемещать файлы в корзину вместо их окончательного удаления, что обеспечивает возможность последующего восстановления. В целях повышения производительности операционные системы могут применять следующие методы:

1. Удаление индексного узла файла (i-node):

Например, в операционных системах UNIX иногда происходит удаление индексного узла файла без удаления его содержимого, что может ускорить процесс.

2. Оставление освобождаемой оперативной памяти без очистки:

- Операционные системы могут не освобождать оперативную память после удаления файла, что также способствует повышению производительности.

В операционной системе Windows и связанных с ней офисных приложениях образование остаточной информации может быть обусловлено следующим:

1. Особенности файловой структуры и хранения данных:

- При обычном удалении файлов информация из области данных не стирается, что приводит к образованию остаточной информации.

2. Резервирование информации для защиты от сбоев:

- Резервные и временные файлы, а также файлы автосохранения создаются для предотвращения потери данных при сбоях.

3. Создание временных файлов для различных процессов:

- Временные файлы спулинга, файлы печати и факсмодемной связи формируются в процессе работы системы.

4. Использование буферов и "теневых" областей памяти:

- Создание буферов и "теневых" областей памяти помогает обеспечить эффективную производительность компьютерной системы.

Исходя из причин образования остаточной информации, объекты, подлежащие контролю, включают:

- Отдельные удаляемые файлы:

- Необходим контроль за процессом удаления файлов и очисткой связанных данных.

Временные файлы:

- Управление созданием и удалением временных файлов для оптимизации пространства и предотвращения ненужных остатков.

Свободная область диска:

- Оптимизация процесса очистки свободного места на диске.

Неиспользуемые элементы каталогов:

- Контроль за удалением неиспользуемых элементов каталогов для улучшения структуры файловой системы.

Управление оставшимися данными после удаления файлов для обеспечения безопасности и конфиденциальности. Любой браузер содержит все ссылки, вводимые пользователем. Причем каждый браузер хранит историю в своем месте – если вы используете, например, Mozilla Firefox, то найдете ее в каталоге Documents and Setting\\Application Data\Mozilla\Firefox\Profiles\ . У каждого браузера существует кэш, в котором хранятся однажды загруженные страницы. Файлы Cookies часто содержат пароли доступа к веб-сайтам.

В каталоге Documents and Setting\\Local Settings\Temp можно обнаружить упоминания об установленных вами программах, содержимое когда-то распакованных архивов и прочие интересные вещи.

Swap-файл или файл подкачки – это место, в которое из оперативной памяти записывается временно неиспользуемая информация. Анализ этого файла (pagefile.sys), проведенный специалистом, тоже может многое рассказать.

Особый интерес для квалифицированного злоумышленника представляет компьютер, который погрузили в hibernate, то есть такое

состояние, когда на жесткий диск в файл hiberfil.sys записывается все содержимое оперативной памяти.

В папках, где когда-то были графические документы, могут остаться файлы Thumbs.db – кэш формируемых проводником эскизов, а в Documents and Settings\\Recent – ярлыки открывавшихся ранее файлов.

В системном реестре хранится огромное количество приватных данных – следы вашей работы оставляет в нем не только Windows, но и прикладные программы: проигрыватели, например, сохраняют список последних воспроизведенных файлов, а текстовые редакторы – открытых документов. При желании и наличии программы вроде PassView даже начинающий пользователь сможет вытащить из реестра пароли самого разного вида – от паролей Dial-Up-соединений до паролей интернет-пейджеров (ICQ).

Пиринговые клиенты, FTP-клиенты, интернет-пейджеры и “звонилки” складывают на диск не только свои временные файлы и всевозможные “хистори”, но и файлы своей конфигурации, часто содержащие пароли доступа. Пароль доступа к удаленному рабочему столу может хранится на диске. Наконец, непосредственно на жестком диске могут остаться следы удаленных конфиденциальных документов, поскольку при очистке Корзины файлы не затираются физически, а лишь помечаются как удаленные, и программы вроде EasyRecovery легко их восстанавливают.

Но даже если возможность обратимого удаления явно не реализована или пользователь не применяет её в большинстве случаев, удаляя файл, не удаляется содержимое файла непосредственно. Вместо этого удаляется запись о файле из директории файловой системы. Содержимое файла (т.е. реальные данные) - остаются на запоминающем устройстве (ЗУ). Данные существуют до тех пор, пока ОС не использует заново это пространство для новых данных. Во множестве систем остаётся достаточно системных метаданных для восстановления при помощи различных утилит.

Особая функция обеспечения безопасности - гарантированное уничтожение (очистка) данных.

Очистка, обычно, административная защита от непреднамеренного распространения данных внутри организации. Например, перед повторным использованием съемных носителей внутри организации, её содержимое может быть очищено для предотвращения непреднамеренного распространения информации следующему пользователю.

Уничтожение — удаление конфиденциальной информации с записывающего устройства так, чтобы данные не могли быть восстановлены никаким известным способом.

Гарантированное уничтожение информации возможно только при помощи специальных технических или программных средств.

Существует несколько методов уничтожения информации, хранимой на энергонезависимых носителях, которые делятся на:

1) программные, в основу которых положено уничтожение информации, записанной на магнитном носителе, посредством штатных средств записи информации на магнитных носителях. В случае уничтожения информации программным методом, носитель может быть повторно использован в других ПК, после инсталляции новой операционной системы (ОС) и приложений. Уничтожение производится наиболее простым и естественным способом – перезаписью информации. Перезапись – это процесс записи не конфиденциальных данных в область памяти, где ранее содержались конфиденциальные данные.

2) аппаратные методы, которые реализуются с помощью специального оборудования, воздействующего на различные носители. По способу воздействия аппаратные методы классифицируются на несколько подгрупп:

- методы без разрушения конструкции носителя; - методы, связанные с разрушением конструкции носителя. Программные методы уничтожения информации можно по степени надежности разделить на 3 уровня.

Уровень 0. Наиболее простая и часто применяемая форма уничтожения информации на носителях на жестких дисках (НЖМД). Вместо полной

перезаписи жесткого диска в загрузочный сектор, основную и резервную таблицы разделов записывается последовательность нулей.

Уровень 1. Запись последовательности нулей или единиц в сектора, содержащие уничтожаемую информацию. Программный доступ к перезаписанным данным невозможен. Однако остается возможность восстановления информации.

Уровень 2. Использование нескольких циклов перезаписи информации. С увеличением числа циклов перезаписи усложняется задача восстановления удаленных данных. Полной гарантии необратимого разрушения информации нет и в этом случае, поскольку программно невозможно управлять траекторией движения блока головок НЖМД и процессом перемагничивания битовых интервалов.

Разработано большое количество рекомендаций, определяющих состав маскирующих последовательностей, записываемых в сектора данных при использовании методов 2-го уровня. В идеальном случае маскирующие последовательности должны подбираться таким образом, чтобы перемагнитить каждый битовый интервал в записи максимальное число раз. Выбор метода уничтожения зависит от метода кодирования информации, используемой на целевом носителе.

Надежное уничтожение (очистка) критичных файлов осуществляется путем несколько кратной записи случайных символов в область данных, где ранее они размещались.

Выбор конкретного метода также зависит от уровня секретности информации, подвергаемой уничтожению. Во многих странах существуют нормативные документы и государственные стандарты, строго регламентирующие состав и количество проходов при уничтожении информации.

В США большой популярностью пользуется метод, определенный Министерством обороны. Согласно этому методу, должна быть выполнена троекратная перезапись информации:

- запись в каждый байт перезаписываемой области случайно выбранного байта;

- запись в каждый байт перезаписываемой области дополнения к нему;

- запись в перезаписываемой области последовательности случайно выбранных байт.

Данный метод носит произвольный характер и не учитывает особенностей работы конкретных НЖМД. Министерство обороны США признает этот факт и при уничтожении информации высшей категории секретности запрещает использование программных методов.

В России рекомендации по выбору метода приводятся в следующих документах:

- В ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» определяется, что очистка внешней памяти при ее освобождении должна производиться путем записи в нее маскирующей информации. Количество и содержание проходов не уточняется.

- РД ФСТЭК России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации» в зависимости от класса защищенности СВТ система защиты должна затруднять (предотвращать) доступ пользователей к остаточной информации, а также осуществлять очистку оперативной (требования 2). Очистка производится путем записи маскирующей информации (последовательности случайных данных) в память при ее освобождении (перераспределении). Количество и содержание проходов не уточняется.

- РД ФСТЭК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» определяет, что в автоматизированных системах, аттестованных по классам защищенности

3А, 2А, 1А, 1Б, 1В и 1Г, должна производиться очистка внешней памяти путем двукратной произвольной записи. Содержание проходов не уточняется.

Помимо методов, определяемых государственными стандартами, существует целый ряд методов, предложенных независимыми экспертами в области информационной безопасности. Наиболее распространенными из них являются два метода – Б. Шнайера и П. Гутмана.

Б. Шнайер предложил метод уничтожения информации, состоящий из семи проходов: первые два – запись единиц и нулей соответственно, и последние пять – запись случайных данных. Однако ни количество проходов, ни выбор маскирующих последовательностей не обоснованы.

Обоснование выбора маскирующих последовательностей проводится для метода П. Гутмана. Метод состоит из 35 проходов, ориентированных на уничтожение записей, закодированных определенными методами.

Состав перезаписываемой сессии следующий: в первые 4 прохода записываются случайно выбранные символы в каждый байт каждого сектора, с 5 по 31 проход происходит запись определенной последовательности символов, в последние 4 прохода снова записываются случайно выбранные символы. Каждый проход с 5 по 31 был разработан с учетом конкретной схемы магнитного кодирования, то есть как целевой проход.

Перезапись данных усложняет процесс восстановления информации, но вероятность успешного восстановления остается выше нуля. Тем не менее для этого может потребоваться дорогостоящее и сложное оборудование и программное обеспечение. Преимущества программных методов включают:

- Возможность последующего использования носителей: После программной перезаписи информации носители данных могут быть повторно использованы.

- Низкая стоимость: Программные методы обычно более доступны с финансовой точки зрения.

- Простота использования: Программные методы легки в использовании и не требуют сложной конфигурации.

- Возможность использования в ходе работы вычислительной системы в качестве профилактической меры: Программные методы можно применять в процессе работы системы для предотвращения нежелательного доступа.

Недостатки программных методов включают:

- Низкая скорость работы: Многократная перезапись современного носителя может занять несколько часов или даже дней.

- Низкая универсальность: Программы уничтожения информации могут не поддерживать устаревшие или нестандартные носители, а также могут быть неспособны к уничтожению информации с неисправных носителей.

- Отсутствие программного метода с обоснованной теоретической или практической эффективностью: Некоторых программных методов может не быть, и их эффективность может быть неоднозначной.

Для повышения надежности уничтожения информации используются аппаратные методы. Однако их недостатком является полное выведение очищаемого носителя из строя.

6 Полное стирание данных с переносного носителя

1. Установим программу для редактирования в шестнадцатеричном формате.

2. На внешнем носителе создадим обычный файл в формате текста, добавим в него текстовую информацию и сохраним (см. рисунок 1).

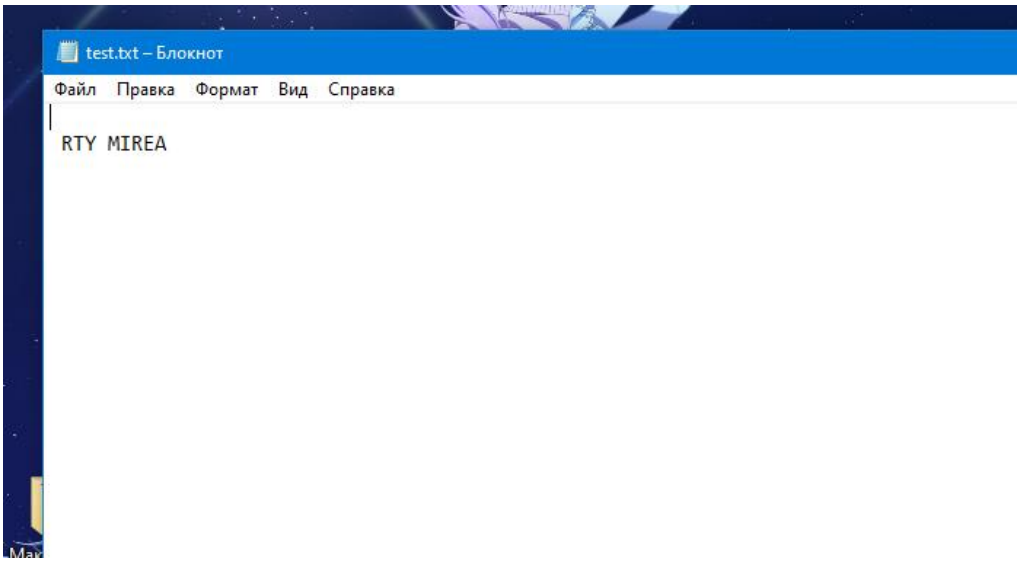

Рис 1 – Создание текстового файла “test”

3. Откроем диск в hex-редакторе и в диалоговом окне выберем съёмный носитель.

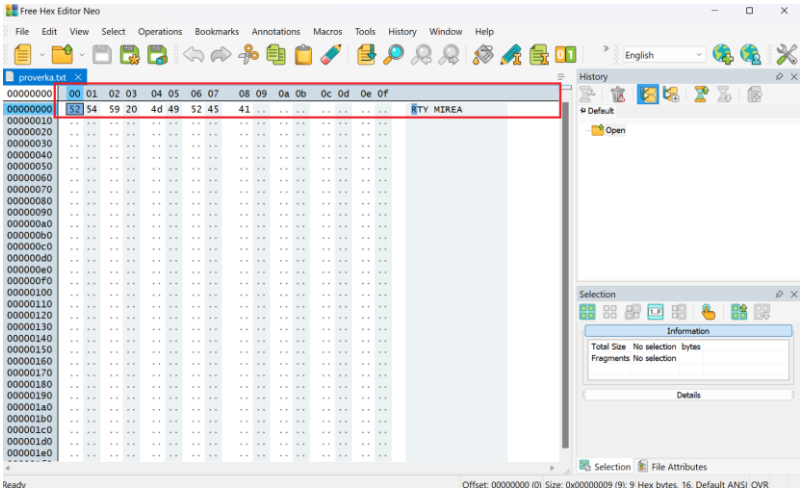

Рис. 2 – Содержание секторов диска

После выполнения этого действия вы увидите окно, отображающее содержимое всего диска, разделенного на секторы (см. рисунок 2), включая информацию о заголовке файловой системы.

Шаги выполнения:

1. Найдите, где располагается файл test.txt. Для этого в меню «Find» выберите «Find all» (рис. 3).

Введите в поле поиска нужные данные. Для более точного результата учитывайте регистр.

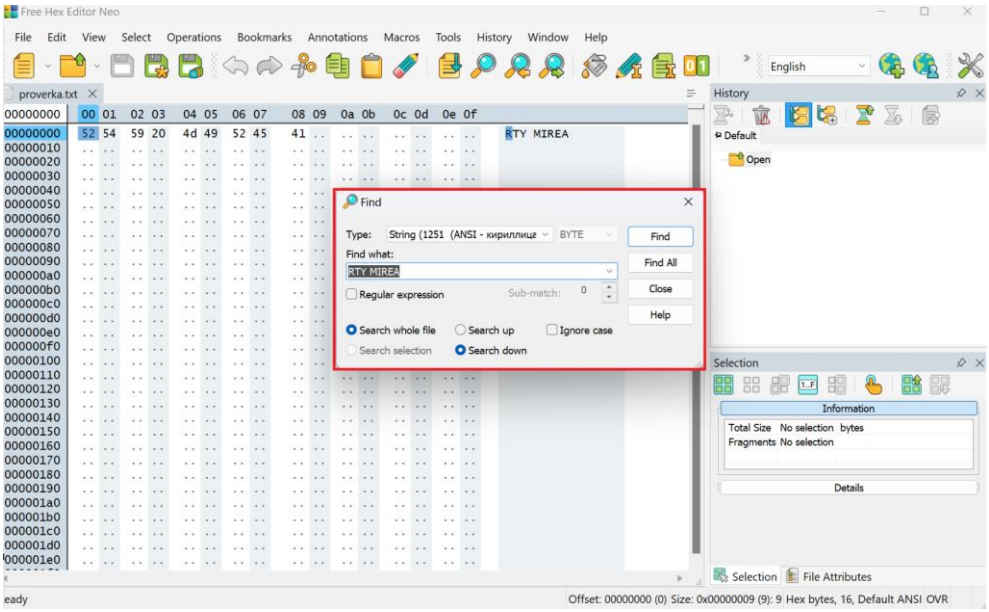

Рис 3 – Поиск сектора с текстовым файлом

2. Когда программа найдет искомое содержимое, то она автоматически перейдет на сектор с этим файлом (рис.4).

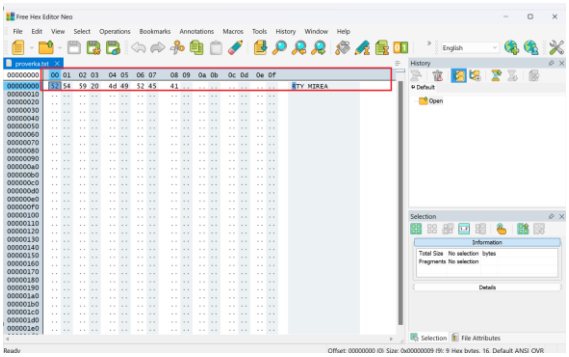

Рис. 4 – Найденный сектор с информацией тестового файла

3. Зафиксируем номер сектора (00000000).

4. Удалите файл с переносного носителя, используя стандартные инструменты операционной системы Windows.

5. Теперь удостоверьтесь, что информация из удаленного файла по-прежнему доступна. Для этого закройте вкладку с содержимым диска , так как программа не мгновенно обновляет изменения в реальном времени.

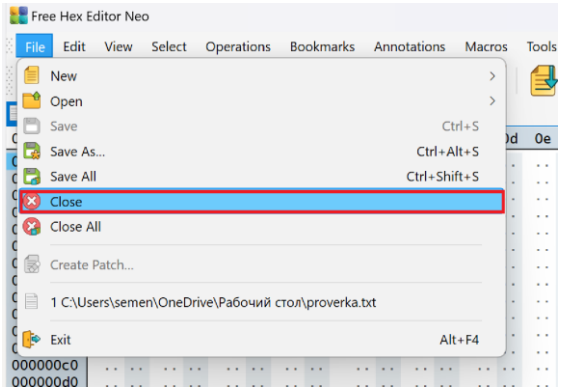

Рис. 5 – Закрытие содержания диска в hex-редакторе

Таким образом, в большинстве операционных систем после удаления файлов их содержимое остается доступным. Для полного и безвозвратного удаления файлов с персонального компьютера или ноутбука, необходимо провести процедуру уничтожения и стирания данных. После такого удаления восстановление данных становится невозможным. Хотя операционная система Windows не предлагает встроенного инструмента для сканирования и

уничтожения удаленных файлов, существует широкий выбор стороннего программного обеспечения, из которого можно выбрать подходящий вариант.

Примером такого программного обеспечения является EaseUS Partition Master, выдающийся инструмент управления дисками для Windows 11/10. Он предоставляет функцию "Wipe data" («Уничтожение данных»), которая безвозвратно стирает все данные с диска в Windows 11/10/8/7. Программа позволяет полностью удалить все данные и разделы на жестком диске в соответствии со стандартами очистки DoD 5220.22-M. EaseUS Partition Master обладает множеством базовых и расширенных функций для управления жесткими дисками.

Откроем программу EaseUS Partition Master, кликнем правой кнопкой мыши на жестком диске или разделе, с которого нужно полностью удалить данные, и выберем опцию "Wipe Disk" (см. рисунок 6).

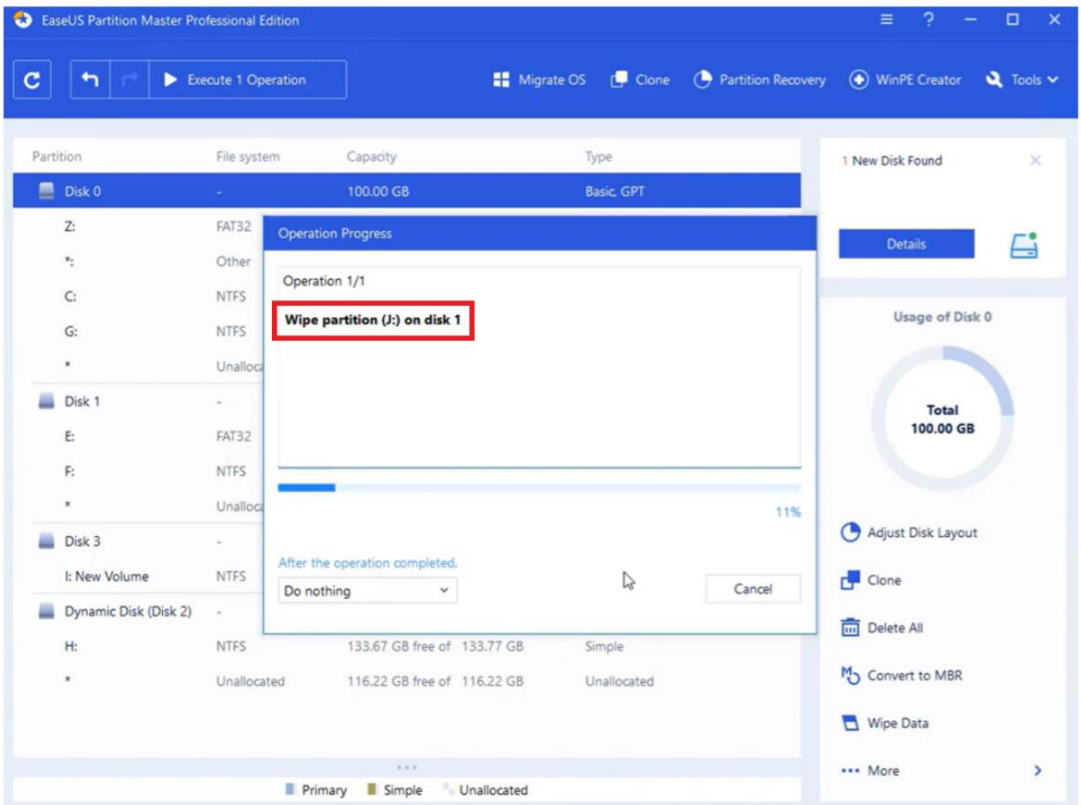

Рис 6 – Скриншот программы

3. В новом окне установим время очистки данных, затем нажмём "OK".

Нажмём кнопку " Perform the operation" в правом верхнем углу, проверим указанные настройки. Если все корректно - подтвердим их, нажав на "Apply".

4. Диск теперь полностью пуст. EaseUS Partition Master, инструмент управления разделами, предоставляет возможность многократного стирания жесткого диска. Обычно после двух процедур стирания ваши данные будут безвозвратно удалены и не смогут быть восстановлены.

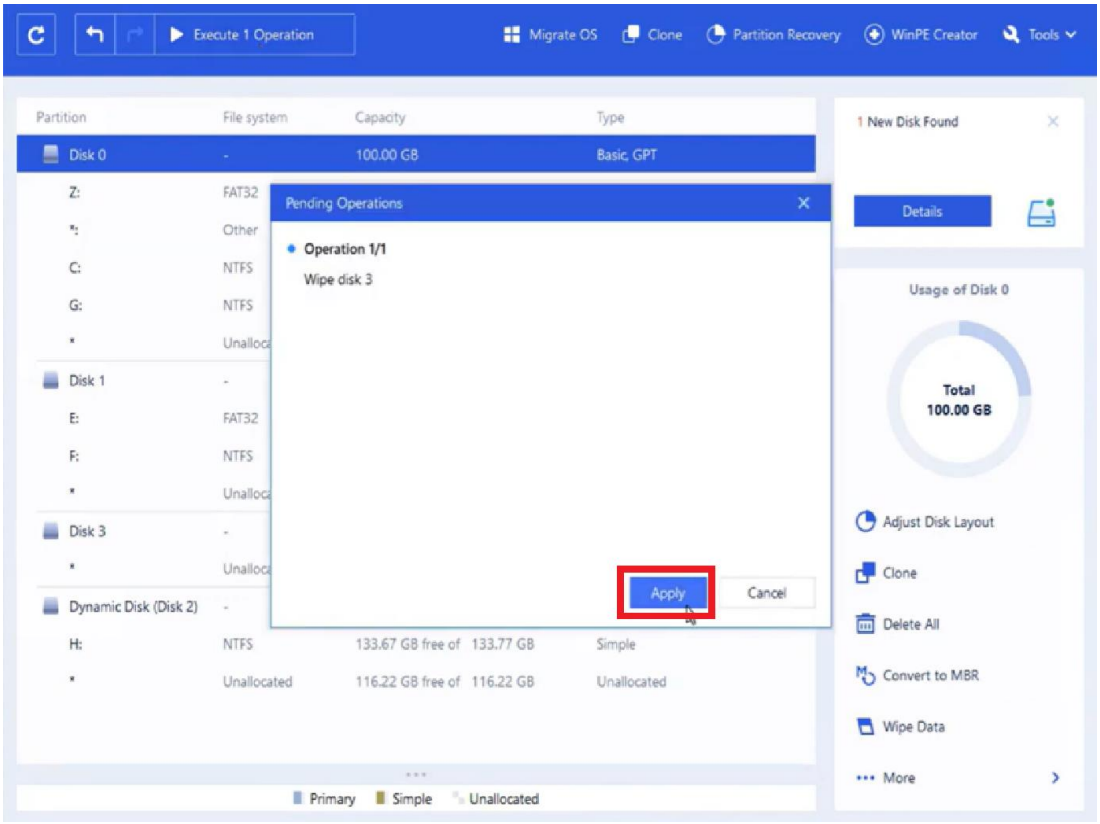

Рис 7 – Скриншот программы

ЗАКЛЮЧЕНИЕ

В процессе исследования методов удаления остаточной информации из полупроводниковых и магнитных устройств хранения данных, а также освоения программных средств для уничтожения и восстановления данных, были приобретены значительные навыки в обеспечении безопасности информации. Полученный опыт представляет собой значимый вклад в профессиональное развитие в области информационной безопасности.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

Литература:

1) Thornton, A. End-of-Life Data Security in the Enterprise / A. Thornton – Redemtech White Paper, 2002. – 9p

2) Коженевский С. Методы гарантированного уничтожения данных на жестких магнитных дисках /Сергей Коженевский// Публикация ЕПОС – 2003: http://www.epos.kiev.ua/pubs/nk/nzmd.htm

3) Гутман П. Безопасное удаление данных из магнитной и твердотельной памяти. Факультет компьютерных наук. Оклендского университета. / Питер Гутман/статья-1996:

https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html