Оглавление

[ВВЕДЕНИЕ 3](#_Toc137933185)

[ГЛАВА 1 5](#_Toc137933186)

[ИССЛЕДОВАНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ 5](#_Toc137933187)

[1.1 Обзор литературы 5](#_Toc137933188)

[1.2 Способы безвозвратного физического уничтожения информации 5](#_Toc137933189)

[1.3 Способы безвозвратного программного уничтожения информации 7](#_Toc137933190)

[ГЛАВА 2 ПРОЕКТИРОВАНИЕ ПРОГРАММНОГО ПРИЛОЖЕНИЯ 9](#_Toc137933191)

[1.1 Теоретические сведения о хранении файлов 9](#_Toc137933192)

[1.2 Обзор алгоритмов безвозвратного программного уничтожения информации 10](#_Toc137933193)

[1.2 Выбор языка для разработки программного средства 12](#_Toc137933194)

[1.4 Разработка интерфейса программы 12](#_Toc137933195)

[1.5 Реализация стирания файлов 12](#_Toc137933196)

[ГЛАВА 3 ТЕСТИРОВАНИЕ ПРОГРАММНОГО ПРИЛОЖЕНИЯ 13](#_Toc137933197)

[ЗАКЛЮЧЕНИЕ 14](#_Toc137933198)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 15](#_Toc137933199)

# ВВЕДЕНИЕ

Благодаря научно-техническому прогрессу контролировать данные с каждым годом становится все сложнее. И дело отнюдь не только в развитии сетевых технологий. Если раньше, чтобы быть уверенным в собственной безопасности достаточно было сжечь несколько писем пикантного содержания, то сегодня удаляя компрометирующие вас документы с жесткого диска или SSD нельзя быть на 100% уверенным, что их не удастся восстановить.

Безвозвратное удаление данных – это уничтожению данных с жесткого диска или внешних носителях без возможности восстановления с помощью аппаратных средств или программного обеспечения. Процедура уничтожения данных необходима в случае утилизации поврежденного диска, его продажи или передачи другому пользователю для сохранения личной и секретной информации. При удалении файла операционная система стирает только указатель на этот файл в памяти, а пространство жесткого считается свободным. Пока не выполнится запись другой информации в этот отсек, прежние данные можно восстановить.

Навсегда удалить данные можно двумя способами: физическим и посредством специальной программы. Физическое уничтожение данных заключается в применении устройств на магнитных носителях. Жесткий диск после процедуры размагничивания становится непригодным для последующего использования. Если предполагается дальнейшая эксплуатация диска, то выбирается программа по удалению данных. Процесс очистки файлов и разделов осуществляется в ходе загрузки компьютера после того, как прогрузится операционная система. Защита от восстановления удаленных данных обеспечивается путем удаления всего файла (не только заголовка) и многократной перезаписи диска случайным набором байтов (шумом). В результате чего данные становится невозможно восстановить по оставшимся частям или по остаточной намагниченности. Необходимо помнить, что очищающей программой нельзя воспользоваться при поврежденном диске. Программы по удалению данных способны стирать информацию как с отдельных разделов, так и с целого диска. Программное обеспечение для уничтожения информации с компьютера простое в установке и использовании, есть много бесплатных решений, отлично справляющихся с возложенной задачей.

В данной программе сделана попытка объединить только самые нужные для пользователя функции по работе с файловой системой в наглядном и простом виде.

Целью курсового проекта является безвозвратное удаление файлов на языке Delphi.

Задачи:

1. Изучить материал, который необходим для выполнения работы
2. Разработать программу
3. Протестировать программу

Для выполнения поставленной задачи, необходимо современное оборудование, которое позволит комфортно работать. Программа разрабатывалась на операционной системе Windows 10, в среде разработки Embarcadero RAD Studio 11.

Объект исследования: использование среды Embarcadero RAD Studio 11, возможностей языка Delphi и его библиотек для решения поставленной задачи.

Предмет исследования: безвозвратное удаление файлов без возможности восстановления.

# ГЛАВА 1

# ИССЛЕДОВАНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ

## 1.1 Способы безвозвратного физического уничтожения информации

В сочетании с предварительным софтверным удалением файлов, физическое уничтожение накопителя полностью исключает вероятность восстановления данных с HDD даже с применением спецсредств. Способов расправиться с жестким диском существует немало, однако все их можно разделить на три обширные группы:

**Механическое уничтожение**

Нас интересует сугубо уничтожение магнитных пластин, так как DRAM-буфер, в котором кэшируются данные, очищается автоматически после обесточивания HDD, а единственное ПЗУ, имеющееся у винчестера, используется лишь для хранения на нем микропрограммы. Сразу оговоримся, что бить по жесткому диску кувалдой практически бесполезно: да, вы сможете уничтожить текстолитовые платы, разбить корпус (его пластиковую часть) и серьезно повредить блины, однако у профессионала все еще останутся шансы на восстановление информации. Чтобы достичь нужного результата, можно прибегнуть к услугам специализированного шредера.

Главная проблема таких устройств заключается в том, что они чрезвычайно дороги и занимают уйму места. Например, даже за самый простой агрегат уровня Ideal 0101 HDP придется выложить более 200 тысяч рублей, а ведь все, что умеет такой «малыш» с габаритными размерами 850 x 495 x 470 мм и весом 63 кг — проделывать в жестких дисках сквозные отверстия, что хотя и выводит винчестеры из строя, не может являться 100% гарантией уничтожения данных.

**Термическое уничтожение**

По сравнению с механической переработкой этот метод имеет одно весьма интересное преимущество: выбрав его, вы можете не беспокоиться о предварительном стирании данных с помощью специализированных утилит. Давайте вспомним определение ферромагнетика. Ферромагнитные материалы представляют собой кристаллические соединения, способные сохранять намагниченность в условиях отсутствия внешнего магнитного поля при температуре ниже точки Кюри. По достижении последней ферромагнетик утрачивает свои свойства, так что вся записанная информация оказывается гарантировано удалена.

Далее — простая математика:

* точка Кюри ферромагнитного покрытия на основе оксида хрома, которое используется в жестких дисках, составляет около 386 градусов Кельвина, то есть 113°С;
* температура плавления алюминия, из которого состоят сами пластины, составляет 660°С;
* температура пламени пропан-бутановой горелки, которую можно приобрести в любом строительном магазине, достигает 1300°С.

Плюсы такого подхода — ультрабюджетность и возможность «обработки» накопителя в домашних условиях, минусы — длительность процедуры и пожароопасность.

**Химическое уничтожение**

Смесь концентрированных азотной и соляной кислот, взятых в соотношении 1:3, более известная под названием «царская водка», способна без труда растворить жесткий диск даже целиком, не оставив и следа ни от сохраненных данных, ни от самого накопителя. Впрочем, HNO3 неплохо справляется с покрытием блинов даже соло.

Все перечисленные нами методики достаточно эффективны, хотя и не лишены ряда недостатков. Во-первых, подобные манипуляции потенциально травмоопасны, особенно в условиях нехватки времени: если в спешке можно серьезно повредить руку даже шлифовальной машинкой, то что уж говорить о кислоте или горелке? Во-вторых, вам потребуется закупить специальное оборудование, а для работы с кислотой так и вовсе иметь мини-лабораторию с хорошей вытяжкой. В-третьих, они мало подходят для ситуаций, когда «за вами уже выехали»: любой из приведенных методов занимает достаточно времени, часть которого придется потратить на разборку винчестера.

Но что, если проявить толику смекалки, заранее выкрутить все болты, удерживающие крышку HDD, и посадить ее на скотч, чтобы в случае чего быстро сорвать и извлечь блины? Хотя это действительно поможет сэкономить драгоценное время, здравой подобную идею не назовешь.

Если речь идет о «воздушном» накопителе (к таковым относятся модели емкостью до 6 ТБ включительно), вскрытие устройства негативно скажется на его надежности. Пускай такие винчестеры и не являются герметичными, даже они собираются в стерильных условиях, а барометрическое отверстие, присутствующее в корпусе каждого диска, и предназначенное для выравнивания давления, надежно защищено микрофильтром, задерживающим влагу и мелкодисперсные частицы. Кстати, для большей надежности внутрь HDD устанавливается еще и фильтр рециркуляции, обеспечивающий очистку воздуха в гермозоне во время работы устройства.

После вскрытия диска внутрь гермозоны неизбежно станет просачиваться пыль, что сперва приведет к появлению множественных ошибок чтения/записи, обусловленных нагревом сенсоров под действием силы трения, возникающей, когда движущаяся на огромной скорости пыль станет задевать их поверхность, а затем и к полному выходу винчестера из строя, поскольку мелкодисперсные частицы, подобно абразиву, будут повреждать слой ферромагнетика и стачивать сами головки чтения/записи. Ведь не стоит забывать, что размеры последних у современных жестких дисков не превышают 120 нанометров, а зазор между сенсорами и поверхностью блина составляет всего 12–15 нм, вследствие чего винчестеры чрезвычайно уязвимы.

## 1.2 Способы безвозвратного программного уничтожения информации

При удалении файлов через стандартный менеджер якобы стертая информация на самом деле никуда не девается. Все, что при этом происходит — присвоение соответствующим секторам статуса свободных, чтобы в будущем они были перезаписаны. Однако до тех пор, пока этого не произошло, файлы можно без особого труда восстановить при помощи специализированных программ.

Вывод напрашивается сам собой: для того, чтобы гарантированно удалить тот или иной файл, нам следует инициировать его принудительную перезапись. Для этих целей существует немало утилит, однако проще всего воспользоваться штатными средствами вашей операционной системы.

**Windows**

Начиная с Windows Vista операционные системы Microsoft по умолчанию однократно перезаписывают содержимое выбранного раздела нулями во время его полного форматирования. Количество циклов перезаписи можно задать и самостоятельно, однако для этого придется прибегнуть к услугам командной строки:

format d: /fs:NTFS /p:10

В данном примере мы форматируем том D в файловую систему NTFS, при этом даем операционной системе команду предварительно перезаписать весь раздел нулями 10 раз, используя параметр /p («passes»), задающий количество проходов. Перезаписать конкретный файл или каталог прицельно Windows, к сожалению, не позволяет. Впрочем, рассматривать это как серьезный недостаток нельзя: если уж и хранить конфиденциальную информацию, которую в какой-то момент может понадобится уничтожить, на ПК, то делать это следует, как минимум, на специально выделенном для этого разделе, а лучше всего — на отдельном накопителе, который можно будет быстро очистить непосредственно из вашей ОС.

**Linux**

Операционные системы семейства Linux традиционно предлагают своим пользователям куда больше простора. Так, например, если вам понадобилось быстро и надежно удалить один или несколько файлов, вы можете воспользоваться консольной утилитой shred:

shred -u -n 40 /private/file.txt

В этом примере мы перезаписали файл file.txt случайными данными 40 раз подряд (параметр -n, по умолчанию же shred совершает 25 проходов) и затем удалили его (параметр -u, поскольку по умолчанию shred не удаляет файлы, а сразу перезаписывает). Также утилита поддерживает удаление файлов по маске (например, \*txt) или обработку сразу нескольких файлов подряд в рамках одной команды — для этого необходимо указать ведущие к ним абсолютные пути, разделенные пробелами:

shred -u -n 40 /private/file.txt /private/file2.txt

Если же вы хотите дополнительно скрыть и сам факт «зачистки», то можете воспользоваться параметром -z:

shred -u -z -n 40 /private/file.txt

Единственный недостаток shred — данная утилита не умеет работать с директориями. Поэтому если вам требуется уничтожить содержимое целого каталога с вложенными папками, стоит воспользоваться wipe:

wipe -rf /private/\*

В данном примере мы отдали команду рекурсивно (-r) удалить все, что находится в папке private, а также отключили запрос подтверждения удаления папок и файлов (-f), которое wipe выводит по умолчанию. Среди интересных дополнительных опций, поддерживаемых утилитой, стоит выделить принудительное выполнение chmod для каталогов и файлов, защищенных от перезаписи (-c), работу в тихом режиме (-s) и возможность заставить wipe следовать символическим ссылкам (-D, конфликтует с -r).

**Mac OS**

В версиях операционной системы с 10.4 по 10.10 вы могли инициировать перезапись файлов, переместив их в корзину, а затем выбрав в Finder опцию «Очистить корзину необратимо», однако впоследствии Apple от нее отказалась. Вплоть до версии 10.11 для безопасного удаления данных можно было воспользоваться консольной командой srm:

srm -rm /private/

В данном примере мы рекурсивно удаляем содержимое папки private (-r), перезаписывая каждый файл случайными данными 7 раз подряд (-m). Также можно выбрать однократную перезапись файлов (-s) или же не указывать этот параметр вовсе — в этом случае утилита выполнит 35 проходов.

В актуальных версиях Mac OS инициировать безопасное удаление файлов с жесткого диска можно с помощью Дисковой утилиты (для этого необходимо нажать на кнопку «Параметры безопасности» и задать количество циклов перезаписи), либо через терминал, используя конструкцию вида:

rm -P /private/file.txt

Параметр -P является специфичным для Mac OS и сообщает утилите, что удаляемые файлы необходимо трижды перезаписать.

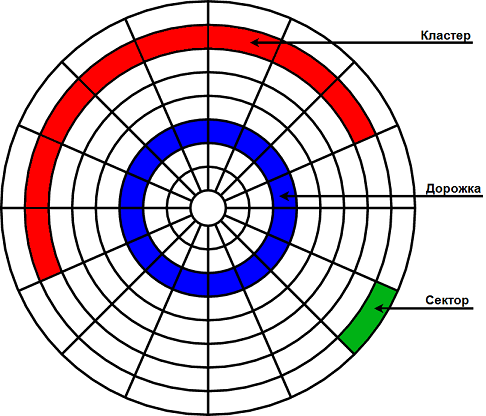
По умолчанию однократную перезапись файлов предлагает лишь встроенная в ОС Windows утилита format, тогда как все прочие средства безопасного удаления файлов совершают от 3 до нескольких десятков прогонов за раз. Аналогичным образом обстоят дела с бесплатным и коммерческим софтом от сторонних разработчиков.

## 1.3 Теоретические сведения о хранении файлов

В упрощенном виде жесткий диск можно представить как круг, который поделен радиальными дорожками. Каждая дорожка, свою очередь, делится на сектора. Сектора могут объединяться в кластеры. Минимальная адресуемая единица — сектор, его размер обычно составляет 512 байт. Схема расположения секторов представлена на рисунке 1.

Рисунок 1.

Схема расположения секторов

[](https://club.directum.ru/uploads/images/41-0.png_d9482d09-fedc-4590-a6f6-d5a635ac0cac.png)

Файл на жестком диске хранится «по частям». Т.е. если размер файла больше, чем размер сектора, то тело файла распределяется по свободным секторам диска. А информация о размещении файла на диске записывается в специальный раздел диска — таблицу размещения файлов.

При удалении файла тело файла остается на диске (в большинстве файловых систем). В таблице размещения файлов соответствующий файл помечается как удаленный, а занятые им сектора становятся «свободными» для записи. Но само тело файла в этих секторах остается. Если эти сектора ничем не занять, то удаленный файл вполне можно восстановить. Этот принцип лежит в основе работы множества утилит восстановления удаленных файлов.

Но даже если тело удаленного файла перезаписать, например, «нулями». То по-прежнему существует возможность восстановления информации из-за эффекта остаточной намагниченности.

Допустим, логические «1» и «0» характеризуются аналоговыми уровнями намагниченности +10 и -10 единиц, соответственно. То есть если головка диска считывает уровень +10, то это «1», если -10, то это «0» — происходит преобразование аналогового сигнала в цифровой.  
Аналоговый сигнал будет далек от «идеальных» +10 и -10. На самом деле у него будет какой-то разброс, к примеру от +8,5 до +11,5 – это будет «1». А от -11 до -9 – «0». Разброс будет обусловлен многими факторами, в том числе и эффектом остаточной намагниченности.

Рассмотрим пример. Какой-то бит информации закодирован как «1» и с него считывается +9,8 единиц. Затем этот бит перезаписали в «0». С него стало считываться не ровно -10, а допустим -9 единиц. Разница аналогового сигнала в +1 единицу от «идеального» значения может говорить о том, что ранее этот бит скорее всего имел противоположное значение. Таким образом, можно попытаться восстановить информацию, конечно, если для этого есть соответствующий инструмент. Но чем плотнее друг к другу находятся биты информации на диске, тем менее вероятно восстановление.

Для уменьшения или исключения вероятности восстановления информации были разработаны алгоритмы безвозвратного удаления информации. Суть всех алгоритмов схожа — нужно перезаписать участки, на которых находился файл, некоторой информацией несколько раз.

# ГЛАВА 2 ПРОЕКТИРОВАНИЕ ПРОГРАММНОГО ПРИЛОЖЕНИЯ

## 1.1 Обзор алгоритмов безвозвратного программного уничтожения информации

**Американский стандарт DoD (Department of Defence) 5220.22-M**

Существуют несколько редакций алгоритма.

В одной из редакций используется три прохода по файлу. В первый раз файл перезаписывается нулевыми битами, второй – единичными битами, третий - случайной последовательностью из нулей и единиц. А, например, редакция "**Е"** предусматривает тоже три прохода по телу файла, но другой алгоритм:

* первый проход - сохраняются случайным образом выбранные символы в каждым байте каждого сектора;
* второй проход - записываются инвертированные данные (нулевой бит заменяется единицей, единичный - нулем);
* третий проход - записывается случайная последовательность.

В редакции "**ЕСЕ"** используется уже семь проходов, где чередуются проходы, использующиеся в редакции "**Е"**.

**Российский стандарт ГОСТ P50739-95**

ГОСТ Р 50739-95 определяет, что стирание производится путем записи в нее маскирующей информации, но количество циклов и содержание маскирующей информации не регламентируется. Однако многие считают, что ГОСТ использует два прохода: на первом файл затирается последовательностью из нулевых бит, а на втором — случайной последовательностью.

**Британский стандарт HMG IS5**

Есть две версии алгоритма. Первая просто перезаписывает файл последовательностью нулей. Вторая, трехпроходовая версия, аналогична одной из редакций американского стандарта DoD – сначала файл перезаписывается нулями, потом единицами и в завершение — случайной последовательностью.

**Немецкий стандарт VSItR**

Семипроходовый алгоритм. Сначала выполняются два прохода с перезаписыванием файла нулевыми и единичными последовательностями. Затем эти два прохода повторяются еще два раза. И седьмой проход из случайной последовательности.

**Метод Брюса Шнайера**

Снова семипроходовый алгоритм.

* Первый проход — перезапись файла последовательностью нулевых бит.
* Второй проход —перезапись файла последовательностью единичных бит.
* Проходы с 3 по 7 — перезапись случайной последовательностью.

Достаточно надежный алгоритм, хотя, сам Шнайдер как-то заявил:

«Последние исследования с помощью туннельных микроскопов показали, что даже этого может быть недостаточно».

**Метод Гутманна**

Алгоритм состоит из 35 проходов. Считается самым параноидальным и надежным. И одновременно самым медленным.

В первые четыре прохода записываются случайно выбранные символы в каждый байт каждого сектора, с 5 по 31 проход происходит запись определенной последовательности символов из [специальной таблицы](http://ru.wikipedia.org/wiki/Метод_Гутмана), в последние 4 прохода снова записываются случайно выбранные символы.

Таблица для перезаписи данных в проходах с 5 по 31 была рассчитана разработчиками алгоритма Питером Гутманом и Коллином Пламбом. Данные в таблице являются «универсальными» для дисков, в которых применяются методы аналого-цифрового преобразования последних лет. Сам Гутманн про использование своего метода говорит:

«На самом деле, нет смысла проводить полную 35-проходную перезапись для каждого диска, поскольку она нацелена на сочетание сценариев с участием всех трех типов кодирования технологии, которая охватывает все более чем 30-летние MFM методы. Если вы используете диск, который использует технологии кодирования Х, вам не нужно выполнять все 35 проходов, нужно выполнить только определенные».

Другими словами, если точно известно, какой метод кодирования используется в конкретном устройстве хранения, то нужно использовать лишь определенные проходы, подходящие для этого метода. Но часто используются все 35 проходов.

## 1.2 Выбор языка для разработки программного средства

## 1.3 Разработка интерфейса программы

## 1.4 Реализация стирания файлов

# ГЛАВА 3 ТЕСТИРОВАНИЕ ПРОГРАММНОГО ПРИЛОЖЕНИЯ

# ЗАКЛЮЧЕНИЕ

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

ПРИЛОЖЕНИЕ А