**Лабораторная работа № 11.2**

# **Скрытие данных на винчестере**

**Цель работы: формирование умений работы с программными средствами, позволяющими скрывать отдельные файлы разных типов на жестком диске.**

**Теоретические сведенья:**

В век высоких технологий информация представляется наибольшей ценностью. Поэтому неудивительно, что в последнее время создается множество средств для ее защиты. Среди соответствующих направлений наиболее развита криптография – алгоритмы постоянно совершенствуются, доказывается их стойкость, и у этого направления есть, по меньшей мере, два плюса. Во-первых, в отличие от теоретических принципов, в конкретные программные реализации могут закрадываться ошибки, приводящие к расшифровке за меньшее, чем расчетное, время. Во-вторых, очевидно, что в связи с развитием технологий через некоторое время перебор, занимающий на современном оборудовании не один год или даже десятилетие, будет выполняться за разумное время.

**Основные принципы**

Стеганография использует принципиально другой подход. Она скрывает не только информацию, но и сам факт ее наличия. В качестве примера из обычной жизни можно привести такой. Конечно, секретное письмо можно хранить в большом кованом сундуке с навесным замком, но можно и спрятать в потайном кармане. И если в первом случае информацию, возможно, кто-то попытается заполучить, то во втором случае у злоумышленника не будет практически никаких зацепок, чтобы догадаться, где она может находиться.

Такой принцип сохранения и передачи ценой информации известен уже давно. Еще Геродот описывал послания, написанные на деревянных дощечках. В отличие от обычного способа записи, когда сначала наносился слой воска, а потом писался текст, здесь секретная запись выцарапывалась прямо на дощечке, которую потом покрывали воском, где уже и писали, чаще всего, ложное сообщение. Также известны случаи передачи сообщений на голове раба. Сначала его брили, затем писали сообщение, а когда волосы снова отрастали, отправляли в путь.

**Компьютерная стеганография**

Основной целью компьютерной стеганографии является скрытие файла-сообщения внутри файла-контейнера. Кроме того, такая операция должна остаться незамеченной. Файл-контейнер обязан не терять функций, а наличие скрытого сообщения должно быть максимально сложно обнаружено.

Рассмотрим основные направления программных реализаций.

1. Алгоритмы, основывающиеся на свойствах текста. Это направление наиболее близко к некомпьютерной стеганографии. В качестве такого универсального примера можно указать, например, акростих. Но есть и чисто компьютерные методы, основывающиеся, например, на сходстве написания кириллических и латинских символов (можно считать одни единицами, а другие – нулями). Также можно выделять отдельные буквы или слова из текста по определенному алгоритму. Это одно из немногих направлений в информационной безопасности, где собственные алгоритмы могут довольно успешно конкурировать с известными, уже использующимися, ведь чем менее изучен алгоритм, тем труднее будет определить наличие скрытого сообщения.
2. Методы, использующие особенности компьютерных форматов. Этот метод прост в реализации и зачастую не требует специального ПО. Конкретные примеры – поле комментариев в формате .jpeg и поле «Company» в свойствах, исполняемых .exe. Простота реализации оборачивается и простотой обнаружения. Хотя и данные алгоритмы могут использоваться тогда, когда у злоумышленников нет даже подозрения на наличие тайной информации.
3. Алгоритмы, использующие избыточность аудиовизуальной информации. Второе название этого метода – метод младших битов. Основными контейнерами в данном способе скрытия являются форматы так называемого прямого кодирования, например, .bmp для графики или .wav для звука. В них каждый минимальный элемент, каковым, например, является пиксель в .bmp, описывается отдельной записью и никак не связан с остальными. Так, в обычном .bmp на каждый пиксель отводится 24 бита – по 8 битов на канал. При изменении младшего бита изображение практически не изменится. Во всяком случае, не каждый человек и не всегда сможет заметить разницу между пустым и заполненным контейнером.

Это направление – самое популярное среди разработчиков. Современные программы научились обращаться с форматами, поддерживающими сжатие, а для самых популярных разработок появились дешифровщики.

Программа Masker 7.0 (рис. 13.1) позволяет скрывать сообщения среди исполняемых видео- и аудиофайлов, а также в изображениях, причем поддерживается огромное число форматов, среди которых есть как форматы прямого кодирования, так и сжимающие (.jpeg, .mp3, .mpeg).

**Программа Masker 7.0**



Рис. 1

Чтобы начать работать, нужно на панели либо в меню выбрать пункт Open Carrier File и в появившемся окне указать файл-контейнер (рис. 13.2).



Рис. 2

После этого, в зависимости от ваших целей, нужно в следующем окне перейти на вкладку Open Hideout, где можно извлечь уже спрятанный файл, указав пароль, либо на Create New Hideout, где можно указать пароль и алгоритм шифрования для новых скрываемых данных. Шифрование – один из преимуществ программы: поддерживаются семь алгоритмов, среди которых есть BLOWFISH и TripleDES (рис. 13.3).



Рис. 3

После указания всех параметров в основной части окна будут отображаться скрытые файлы. Чтобы добавить туда файлы, нужно щелкнуть правой кнопкой мышки и выбрать Hide/Add Files. Появится окно, в котором нужно будет выбрать эти файлы, а затем и указать параметры их сохранения (рис. 13.4). Например, можно добавить целую папку, сохранив ее структуру, или дать файлу-контейнеру статус «read-only», чтобы сохранить скрытые файлы более надежно.



Рис. 4

Извлечение файлов не вызовет затруднений: при открытии файла-контейнера нужно зайти на нужную вкладку, указать пароль, и перед вами появится список спрятанных файлов.

**Программа Safe Calculator**

Программа не требует инсталляции, работает в портативном режиме. Это значит, что программа не оставляет следов на компьютере.

В сущности, программа представляет собой сейф, который содержит важные данные и открывается только после ввода пароля (здесь он называется PIN-код).

Вот так выглядит файл программы в файловом менеджере (рис. 13.5):



Рис. 5

А вот так при запуске (рис. 13.6):



Рис. 6

В базовом режиме программа работает как стандартный Windows-калькулятор.

Для входа в секретный режим необходимо ввести PIN-код, заданный по умолчанию: 123. После этого нажимаем кнопку MS. Видим результат (рис. 13.7):



Рис. 7

Программа перешла в безопасный режим работы, в котором можно прятать данные.

Принцип работы прост: выберите файл, и программа сохранит его внутри своего тела, зашифрованным с помощью алгоритма RC4, который используется при WEP или WPA шифровании Wi-Fi сетей. Это не очень устойчивый алгоритм, но здесь идет расчет не на шифрование, а именно на стеганографию.

Для выбора файла необходимо нажать кнопку «+» в безопасном режиме работы программы. После этого необходимо нажать кнопку «=» для подтверждения того, что вам необходимо выбрать файл для сокрытия. Видим окно (рис. 13.8):



Рис. 8

Выбираем нужный файл (рис. 13.9):



Рис. 9

В данном случае это текстовый файл с именем очень важные пароли к кредиткам и банковским счетам.txt. Жмем кнопку Store. Во время процесса сокрытия файла в тело программы, программа начнет мигать и исчезать на пару секунд – это нормальный процесс, когда программа изменяет свое тело. После успешного завершения операции увидим окно с отчетом (рис. 13.10):



Рис. 10

Для выхода из секретного режима необходимо нажать кнопку MC. Программа автоматически перейдет в нормальный режим калькулятора (рис. 13.11):



Рис. 11

Если посмотреть на файл программы в файловом менеджере (рис. 13.12), то станет видно, что размер файла увеличился (было 225 280 Мбайт).



Рис. 12

Скрытие больших файлов тоже работает, но и размер программы тоже станет огромным, и это натолкнет на подозрения – ведь таких простых калькуляторов размером в десятки и сотни Мбайт явно не существует.

Для получения доступа к скрытым файлам вновь введите PIN-код и нажмите MS, программа входит в секретный режим (рис. 13.13):



Рис. 13

Для работы с программой в секретном режиме предусмотрены несколько команд:

* «+» – добавление файлов для сокрытия. При этом файлы из первоначального размещения удаляются;
* «-» – извлечение файлов из хранилища. При этом файлы извлекаются в папку с программой. Из самой программы файлы удаляются;
* «\*» – копия защищенного файла помещается в папку программы. В самой программе также остается защищенный файл;
* «/» – просмотр или запуск файлов, которые помещены в тело программы. Если вы просмотрели текстовый файл, то он после просмотра удаляется из тела программы;
* sqrt – просмотр/запуск сохраненного файла, с последующим выходом из программы;
* 1/х – замена сокрытого файла на новую версию файла с таким же именем и расширением;
* МС – возврат программы в режим классического калькулятора;
* MS – вывод на экран PIN-кода;
* New PIN – задание нового PIN-кода для доступа к программе. После нажатия необходимо ввести новый PIN, и нажать «=». PIN-код может быть от 1 до 32 цифр, в том числе отрицательным или дробным (в виде десятичной дроби). Для полного подтверждения нажмите клавишу MS;
* Status – вывод информации о сокрытых файлах;
* Help – вывод помощи. Работает в обоих режимах.

Если нажать кнопкой мышки на дисплей калькулятора, то можно включать/выключать режим скроллирования.

Кроме того, в режиме калькулятора есть одна важная команда: если нажать мышкой на дисплей калькулятора, то можно включать/выключать показ вводимого PIN-кода.

**Задание №1**

Скрыть текстовые документы, электронные таблицы, медиафайлы и архивы различных объемов с помощью программ Masker 7.0 и Safe Calculator. Определить, какой программой эффективнее скрывать какие файлы.

**Контрольные вопросы:**

1. Что такое компьютерная стеганография?

2. Основные особенности реализации компьютерной стенографии?

3. Особенности программы Masker 7.0.

4. Особенности программы Safe Calculator.

**Оформите отчет.**