**Лабораторная работа № 17**

Тема работы: Скрытие данных на винчестере.

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

Задание 1. Программа Masker.

Программа Masker 7.0 поставляется через установщик (рисунок 1). Данный ПП 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). На рисунке 2 представлена главная форма ПП.

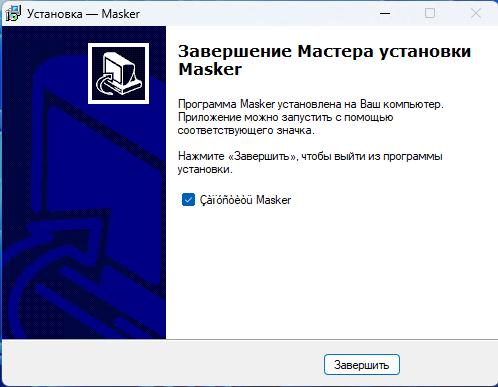


Рисунок 1 – Установка ПП.

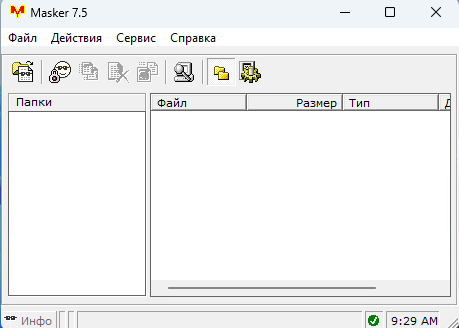


Рисунок 2 – Главная форма.

Чтобы начать работать, сначала необходимо создать файл-контейнер (рисунок 3).

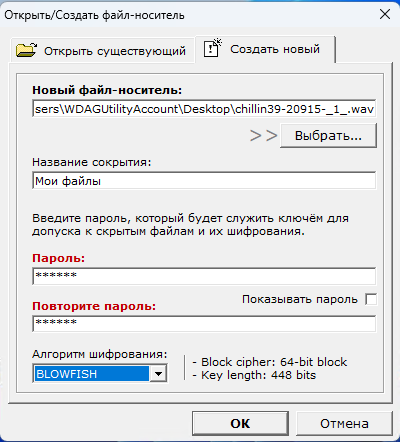


Рисунок 3 – Создание файла-носителя.

После создания файла-носителя, будет предложено добавить файлы и/или папки, которые необходимо спрятать (рисунок 4).

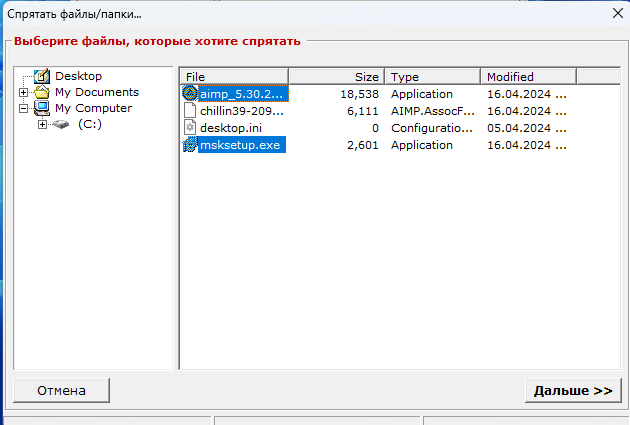


Рисунок 4 – Добавление файлов/папок в контейнер.

После 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.

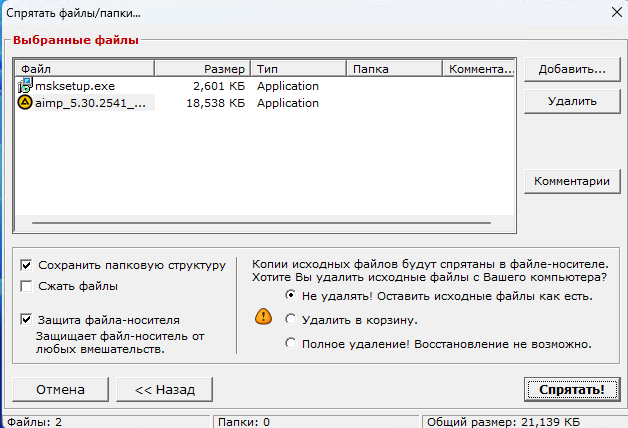


Рисунок 5 – Параметры сохранения файлов в контейнере.

Извлечение файлов не вызовет затруднений: при открытии файла-контейнера нужно зайти на нужную вкладку, указать пароль (рисунок 6), и перед вами появится список спрятанных файлов (рисунок 7).

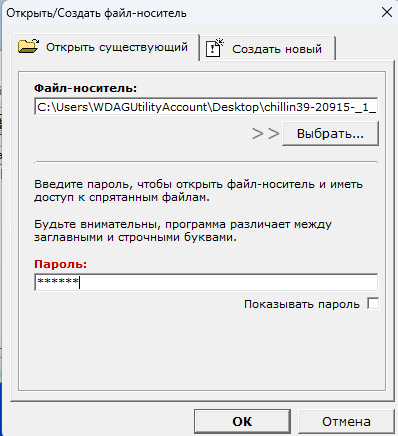
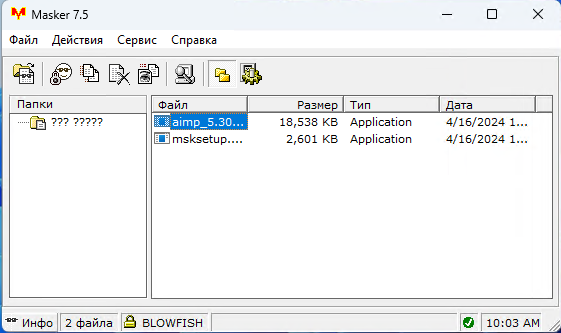


Рисунок 6 – Открытие файла-контейнера.

Рисунок 7 – Просмотр содержимого файла-контейнера.

Задание 2. Программа Save Calculator.

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

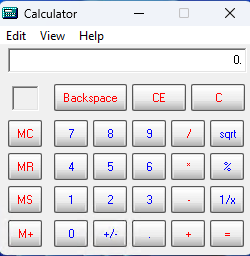
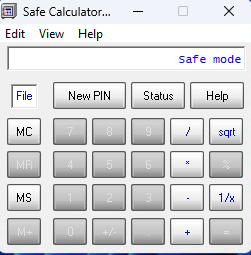


Рисунок 8 – Главная форма.

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 (рисунок 9).

Рисунок 9 – Save mode.

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 и выбираем файл (рисунок 10).

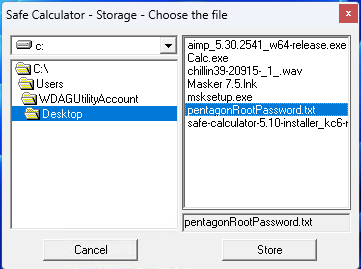
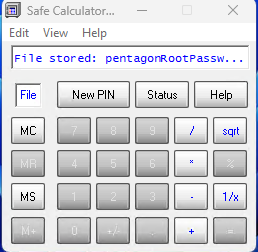


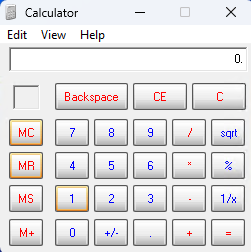
Рисунок 10 – Добавление файла.

В данном случае это текстовый файл с именем «pentagonRootPassword.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 (рисунок 11).

Рисунок 11 – Сообщение о сохранении файла.

Для выхода из секретного режима необходимо нажать кнопку MC. Программа автоматически перейдет в нормальный режим калькулятора (рисунок 12).

Рисунок 12 – Выход в нормальный режим.

Если посмотреть на файл программы в файловом менеджере (рисунок 13), то на рисунке 14 станет видно, что размер файла увеличился (было 220 КБ, стало 5.32 МБ).

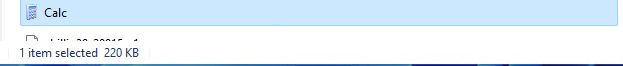


Рисунок 13 – Файл программы до добавления файла.



Рисунок 14 – Файл программы после добавления файла.

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.

Контрольные вопросы.

1. Компьютерная стеганография — это способ скрытой передачи информации, при котором данные встраиваются в некоторый носитель (например, изображение, аудиофайл или видео), таким образом, чтобы их наличие оставалось незамеченным для посторонних наблюдателей.

2. Основные особенности реализации компьютерной стеганографии включают:

* Скрытость: Основная задача стеганографии — обеспечить незаметность внедрения информации. Это означает, что носитель (например, изображение) после встраивания информации должен выглядеть неизменным для обычного пользователя.
* Устойчивость: Встраиваемая информация должна быть устойчива к различным видам атак, таким как сжатие, изменение формата, фильтрация и т. д. При этом стеганографический алгоритм должен сохранять возможность извлечения информации даже после таких преобразований носителя.
* Емкость: Стеганографический метод должен обеспечивать достаточную емкость для встраивания нужного объема информации без существенного увеличения размера носителя.
* Скорость: Процесс встраивания и извлечения информации должен быть достаточно быстрым, чтобы обеспечить удобство использования стеганографии в реальных приложениях.
* Независимость от типа носителя: Стеганографический алгоритм должен быть применим к различным типам носителей (изображения, аудио, видео и т. д.), не требуя специфических адаптаций для каждого из них.