

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)**

Факультет Информатика и вычислительная техника

(наименование факультета)

Кафедра Кибербезопасность информационных систем

(наименование кафедры)

**Лабораторная работа № 4**

на тему «Скрытие данных на винчестере»

Выполнил обучающийся гр. ВКБ53

Донеров Юрий Андреевич

Проверил:

доцент каф. «КБИС» Сафарьян

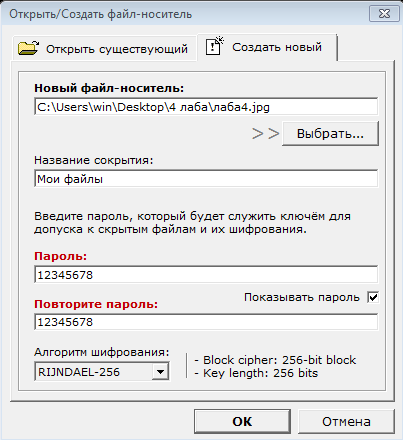
Ольга Александровна

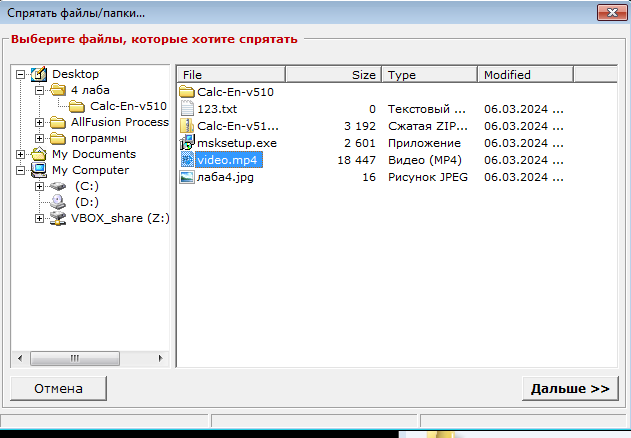
г. Ростов-на-Дону

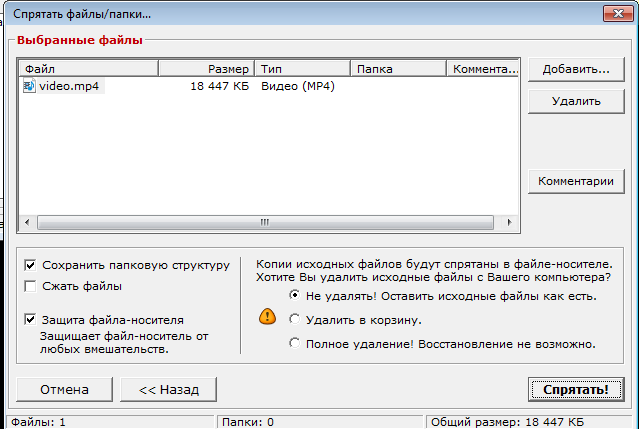
2024

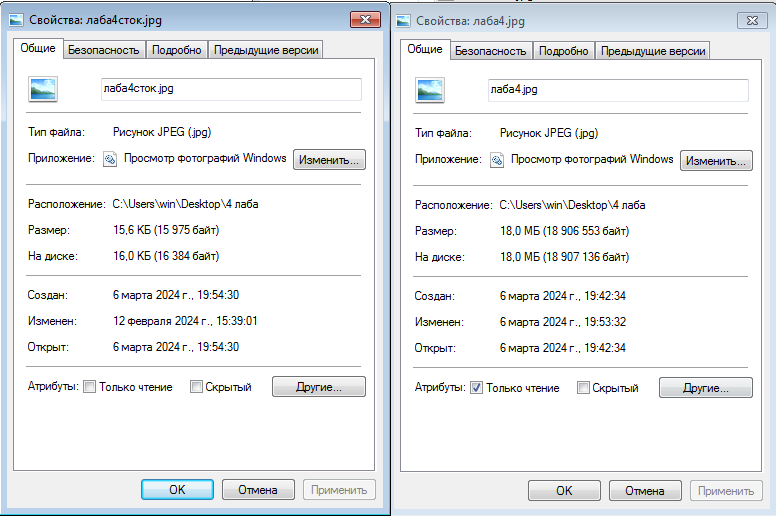
**Цель работы:** формирование умений работы с программными средствами, позволяющими скрывать отдельные файлы разных типов на жестком диске.

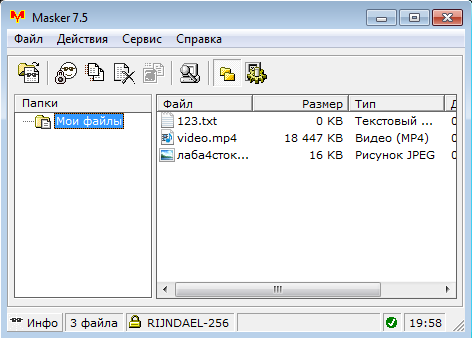
**Ход работы:**



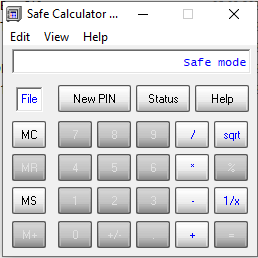


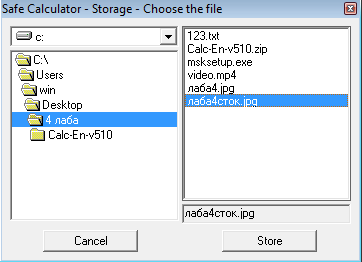
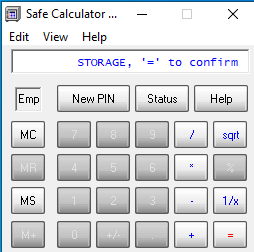






Ввели пароль 123 и нажали MS, последовал переход в безопасный режим, в котором можно прятать данные





**Вывод:** Данная лабораторная работа позволила сформировать навыки работы с программными средствами, позволяющими скрывать отдельные файлы разных типов на жестком диске.

Masker 7.0 имеет большую гибкость для работы с разными контейнерами, больше функционал и производительность, что способствует более эффективной работе с файлами большого объёма, однако сам факт наличия такого ПО должно оставаться в секрете

Calc-En 510 обладает большей скрытность, копируя все базовые характеристики калькулятора, однако не позволяет с такой лёгкостью скрывать файлы больших объёмов.

**Контрольные вопросы**

**1. Что такое компьютерная стеганография?**

Компьютерная стеганография — это направление классической стеганографии, основанная на особенностях компьютерной платформы

(Поля в word, сокрытие в кластер)

**2. Основные особенности реализации компьютерной стеганографии?**

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.

**3. Особенности программы Masker 7.0**

Программа Masker 7.0 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). Masker 7.0 позволяет использовать шифрование 7 алгоритмами.

**4. Особенности программы 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). В базовом режиме программа работает как стандартный Windows-калькулятор.

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