Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Уфимский государственный нефтяной технический университет»

Кафедра вычислительной техники и инженерной кибернетики

Лабораторная работа № 8

по дисциплине Информационная безопасность

**Компьютерная стеганография**

Выполнил: студент гр. БПОи-16-01 К.И. Камалов

Проверил: кандидат технических наук, доцент Т.Х. Агишев

Уфа, 2019

**Цель работы**: познакомиться с компьютерной стеганографией.

**Задание на лабораторную работу:**

1. Зашифровать и спрятать текстовый файл в файлы формата .bmp, .gif или .wav с помощью программы **S-TOOLS.**

А. Взять файлы контейнеры из папки **foto** (black, flower, sky, write). С помощью программы **Watermark Hameleon** вставить водяной знак на изображения с вашей фамилией, прозрачность 50%.

Эти файлы *bmp* формата, спрятать в них файл *текст\_исх* из папки img. Изменился ли размер файлов? Сделать вывод.

Оцените изменение размеров файлов контейнеров после их наполнения в случае использования шифрования.

Б. Взять файлы контейнеры из папки img (black, flower, sky, write). Эти файлы переведите с помощью программы *Paint* в другой формат, например *GIF,* спрятать в них файл *текст\_исх* из папки img. Изменился ли размер файлов? Сделать вывод. Оцените изменение размеров файлов контейнеров после их наполнения в случае использования шифрования.

2. Спрятать текстовый файл в файлы формата bmp, с помощью программы **Magic.** Проделать аналогично пункт 1.

3. Зашифровать и спрятать текстовый файл с помощью программы **MASKER.**

4. Спрятать текстовый файл в файлы формата .bmp, с помощью программы **Safe Calculator.**

5. Спрятать текстовый файл в файлы формата, с помощью программы **SteganoImage.**

6.Подписать все файлы контейнеры с помощью программ **Watermark Hameleon** и **CryptoFoto.** Цифровой знак должен содержать вашу фамилию.

**Порядок выполнения работы**:

1. **Использование программы S-Tools**

С помощью программы Hameleon наносим водяные знаки на все исходные файлы.

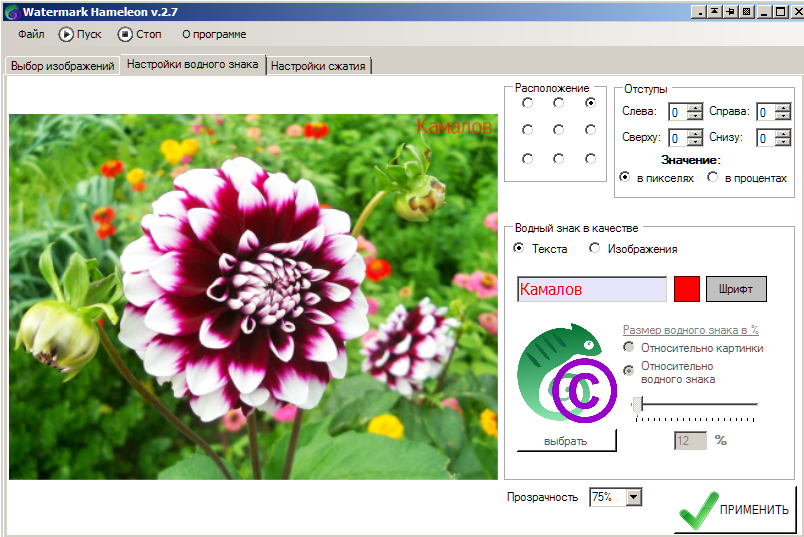
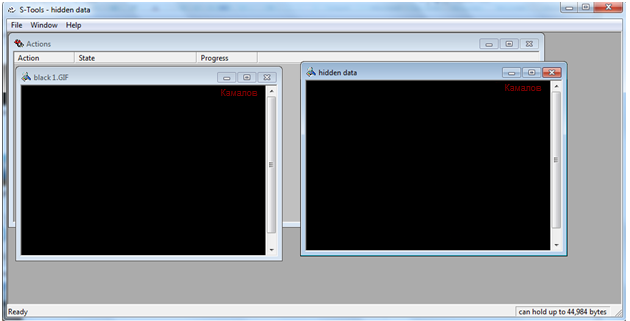
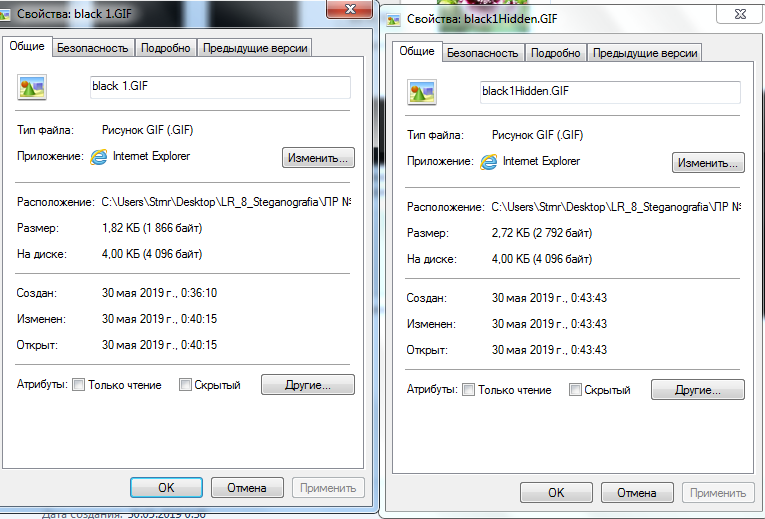
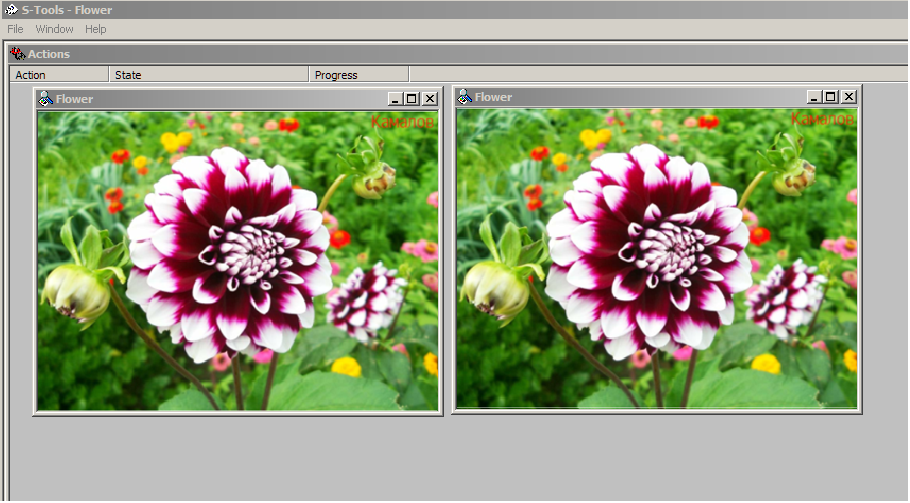


Рис. 1,2 – Исходный файл







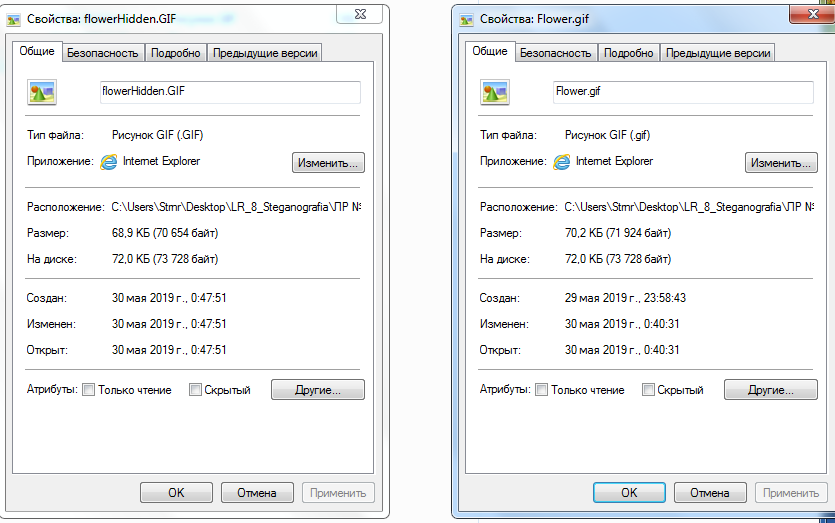
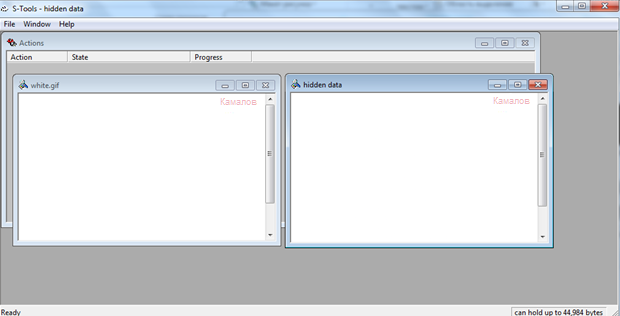
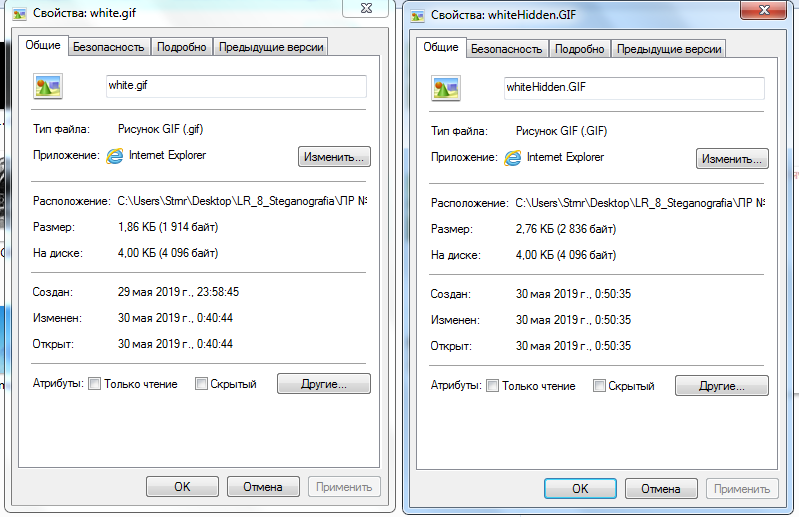


Рис. 3 – Файл с зашифрованной информацией





1. **Использование программы Magic**

Открываем файл black 1.bmp



Рис. 6 –Добавление файла для скрытия

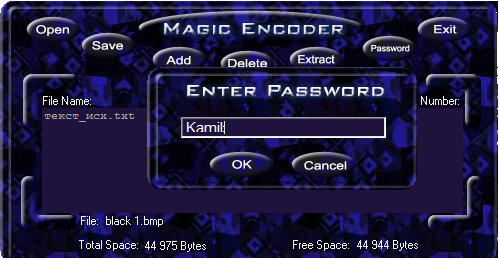
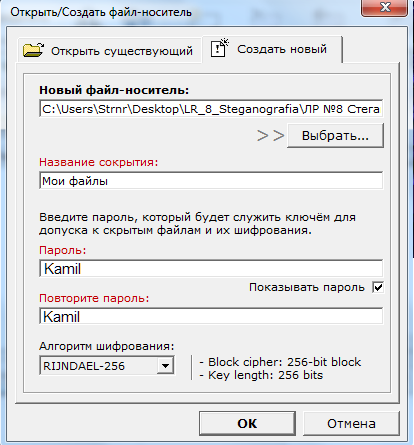


Рис. 7 – Добавление пароля

1. **Использование программы Masker**

Рис. 8 – Создание файла-носителя



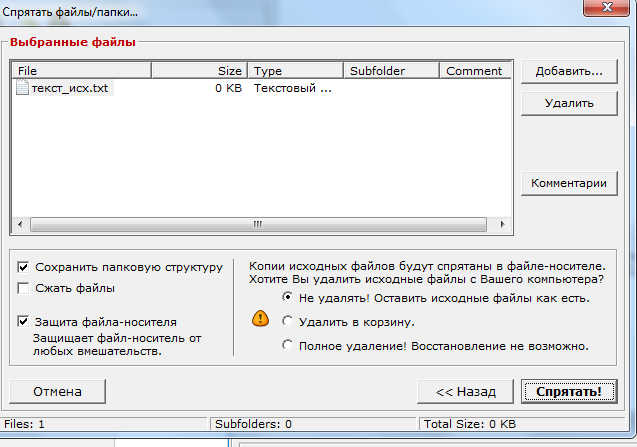


Рис. 9 – Скрытие файла

1. **Использование программы Safe Calculator**

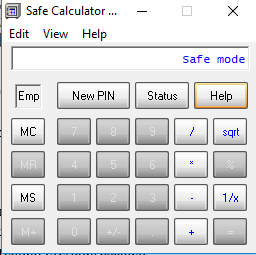


Рис. 11 – Безопасный режим для скрытия файлов

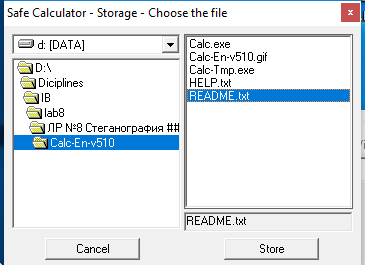


Рис. 12 – Выбор файла для скрытия

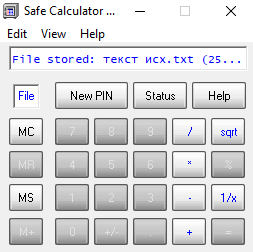


Рис. 13 – Результат скрытия

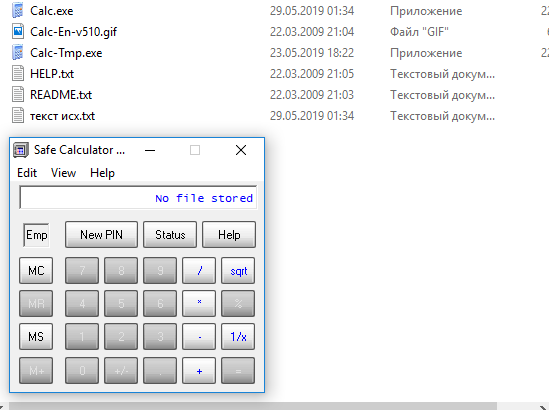


Рис. 14 – Извлечение скрытого файла

1. **Использование программы SteganoImage**

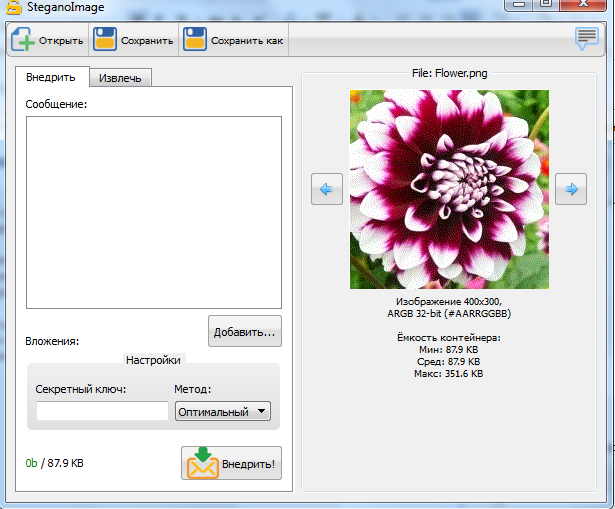


Рис. 15 – Открытие контейнера

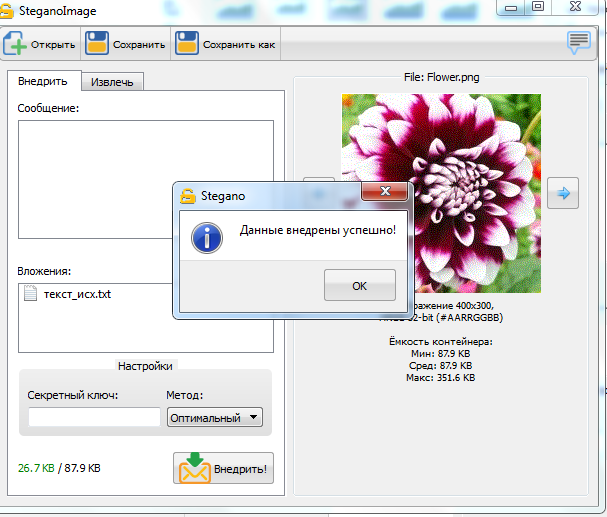


Рис. 16 – Внедрение скрытого файла

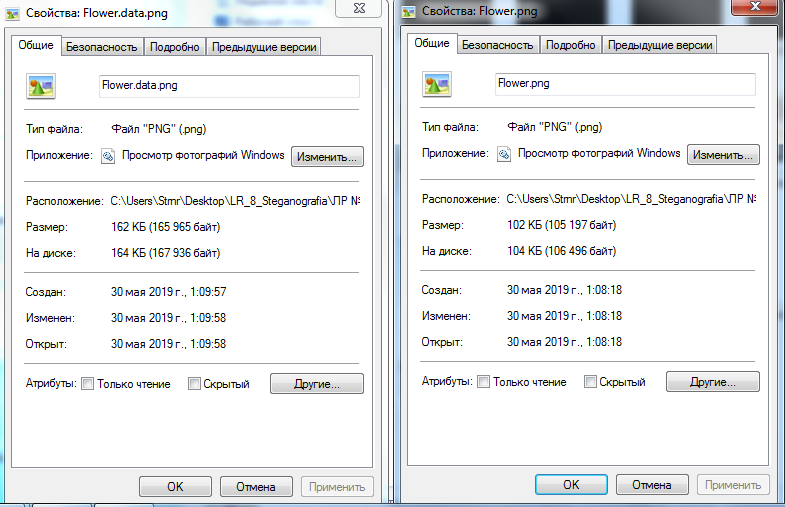


Рис.17 — Сохранение файла и сравнение размеров.

**Выводы по работе:**

В ходе выполнения данной лабораторной работы мы познакомились с компьютерной стеганографией.