ЛАБОРАТОРНАЯ РАБОТА № 15

СТЕГОКОМПЛЕКСЫ, ДОПУСКАЮЩИЕ ИСПОЛЬЗОВАНИЕ АУДИОКОНТЕЙНЕРОВ, НА ПРИМЕРЕ ПРОГРАММЫ *INVISIBLE SECRETS*-4

Цель работы: изучение современных программных средств стеганографии на примере пакета *Invisible Secrets*-4.

Примечание. Для выполнения лабораторной работы на компьютере необходимо установить программу ***Invisible Secrets*-4**.

Описание лабораторной работы. Пакет *Invisible Secrets*-4 отличает проработанность пользовательского интерфейса, выполненного в виде «мастера», интегрированность в среду *Microsoft Windows* и удобство использования. Данный пакет программ может использовать в качестве контейнеров как аудио, так и графические файлы.

В качестве контейнеров данный программный продукт использует неупакованные аудиоданные, оцифрованные с разрядностью 8 или 16 бит на отсчет. Перед сокрытием сообщения оно шифруется. Доступны такие алгоритмы шифрования, как *Rijndael*, ГОСТ 28147—89, *Blowfish* и др.

При разработке стеганографических методов сокрытия информации основной целью является построение помехоустойчивого, необнаруживаемого метода. В связи с этим при рассмотрении программного продукта уделим особое внимание не интерфейсу, а реализованным методам.

Поскольку не для всех программных продуктов доступен исходный текст программы, то выводы часто приходится делать на основе анализа работы программы на тестовых контейнерах. В качестве тестовых контейнеров были выбраны: тональный сигнал с частотой 440 Гц и тишина (сигнал, у которого все отсчеты равны нулю). На рисунке 4.39 показан результат работы программы *Invisible Secrets*-4 на тестовых контейнерах при оцифровке 8 бит на отсчет.

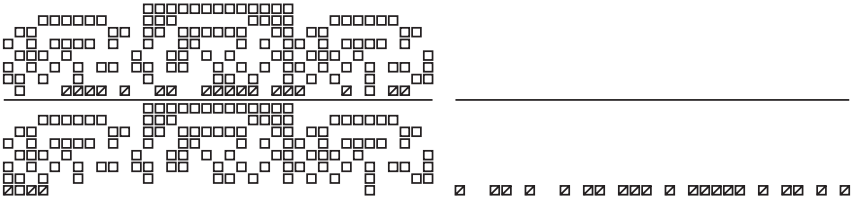

Рис. 4.39. Результат работы программы на тестовых контейнерах

На рисунке по горизонтали указываются отсчеты сигнала, по вертикали — разряды при записи отсчетов в двоичном виде. При наличии прямоугольника в соответствующем разряде соответствующего сэмпла стоит единица, в противном случае ноль. В верхней половине рисунка (выше разделительной линии) изображены отсчеты исходного сигнала контейнера, в нижней половине — отсчеты модифицированного сигнала контейнера. Перечеркнутые прямоугольники соответствуют несовпадающим битам в исходном и модифицированном контейнерах. На левом рисунке показан тональный сигнал, на правом — сигнал, содержащий тишину.

Программа *Invisible Secrets*-4 при внедрении данных в аудио контейнер использует наиболее распространенный в настоящее время метод модификации младшего бита (LSB-метод). Более того, при внедрении не производится никакого анализа содержимого контейнера, что видно из рисунка, где программа внедрила информацию в файл, содержащий тишину. Существенным недостатком данного программного продукта также является то, что при внедрении небольшого количества информации вся информация внедряется в начало контейнера, а не распределяется равномерно по всему контейнеру. Таким образом, возможно обнаружение наличия скрытого сообщения на основе анализа локальных различий статистик в разных частях контейнера.

На рисунке 4.40 приведен вид главного меню программы *Invisible Secrets*-4.

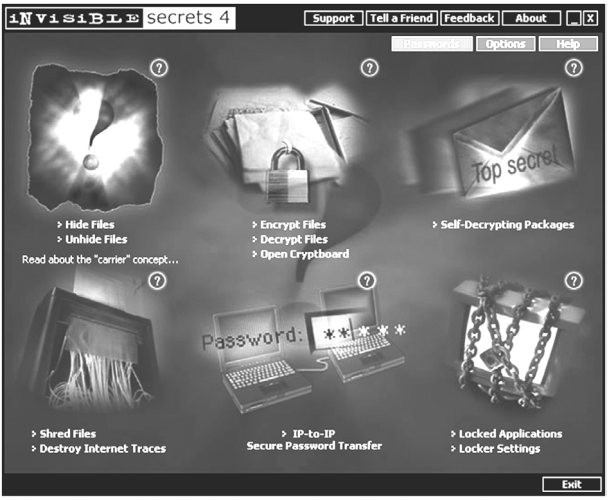

Рис. 4.40. Главное меню программы *Invisible Secrets*-4

Программа *Invisible Secrets*-4 состоит из шести функциональных модулей. Рассмотрим каждый из них отдельно.

Стеганография

Программа позволяет зашифровать и спрятать данные в таких местах, которые на поверхности выглядят совершенно безобидными, например в картинку, файлы с музыкой или веб-страницы. Такие типы контейнеров — прекрасная маскировка для секретной информации.

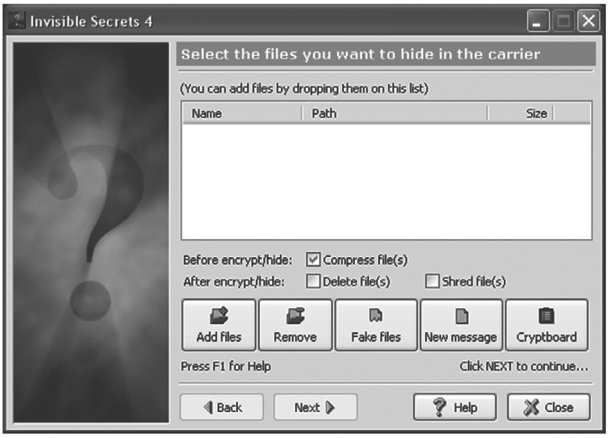

Рис. 4.41. Выбор файла, который необходимо встроить или зашифровать, и задание соответствующих параметров

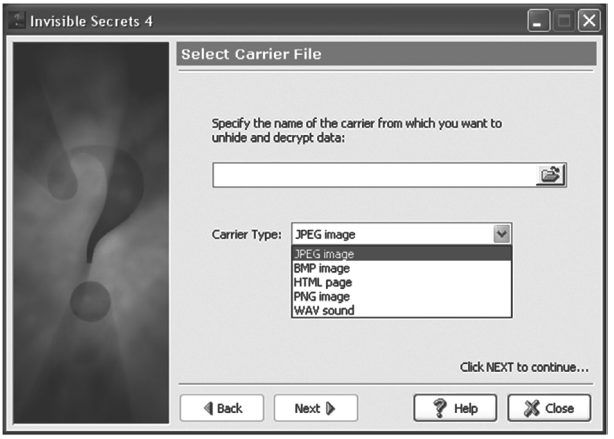

Рис. 4.42. Выбор файла для извлечения из файла-контейнера или расшифрования

Шифрование

Шифрование. В программе *Invisible Secrets*-4 предусмотрена защита файлов с использованием современных методов симметричного шифрования. Только владелец секретного пароля сможет прочесть их. Программа поддерживает такие алгоритмы шифрования, как: *Rijndael*, ГОСТ 28147—89, *Blowfish*, *Twofish*, *RC*4, *Cast*128, *Diamond* 2, *Sapphire II*. На рисунке 4.43 приведена панель шифрования файлов, а на рис. 4.44 панель расшифрования файлов.

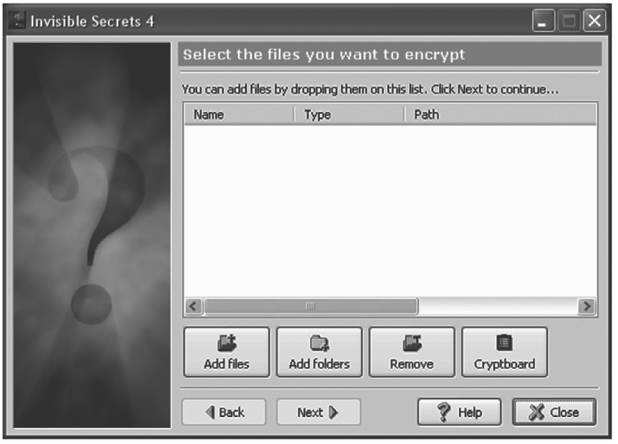

Рис. 4.43. Панель шифрования файлов

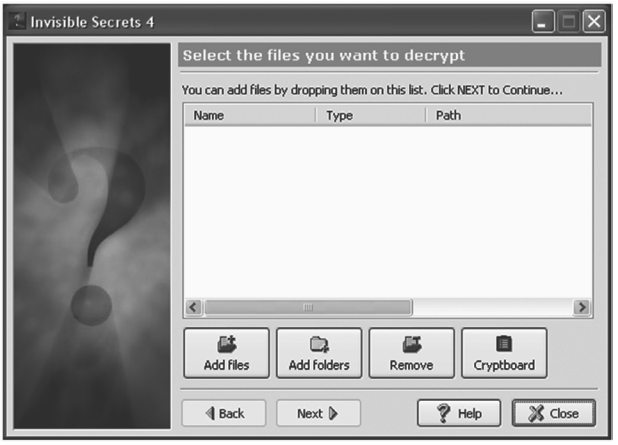

Рис. 4.44. Панель расшифрования файлов

Шифрование почтовых сообщений. Чрезвычайно актуальными являются процессы обмена конфиденциальной информацией в сети. При обмене личными сообщениями или коммерческими секретами возникает необходимость защищать конфиденциальную информацию от несанкционированного прочтения или модификации.. Программа *Invisible Secrets*-4 поможет отослать зашифрованное сообщение по *e-mail*, а получателю для его расшифрования необходимо будет знать только правильный пароль.

На рисунке 4.45 приводится панель программы *Invisible Secrets*-4 для создания самораспаковывающегося пакета для его отправки по *e-mail*.

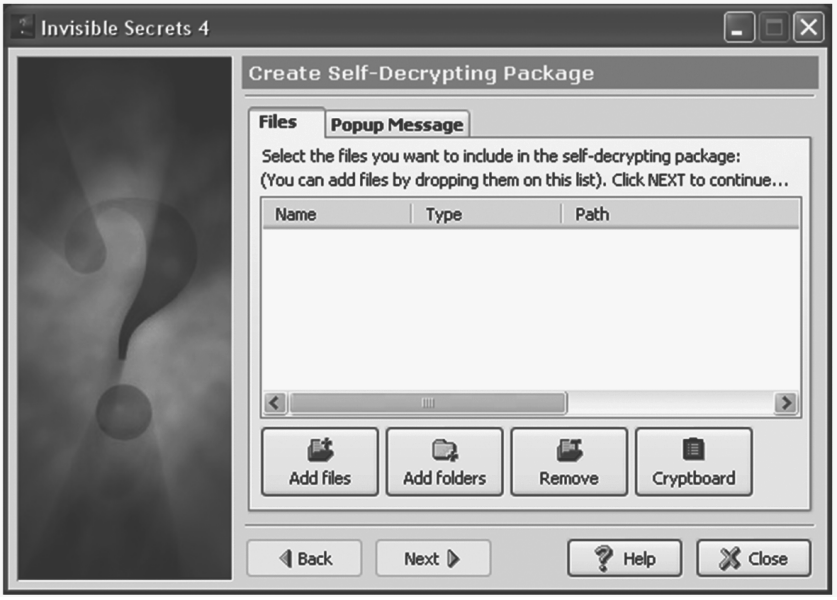

Рис. 4.45. Создание самораспаковывающегося пакета для его отправки по *e-mail*

Уничтожение папок, *файлов и ссылок*. Для уничтожения секретных папок или файлов без возможности их восстановления, а также различных ссылок в программе *Invisible Secrets*-4 используется модуль *DoD* 5220.22-*M Shredder*. Панель для уничтожения папок и файлов приведена на рис. 4.46, а для уничтожения ссылок на рис. 4.47.

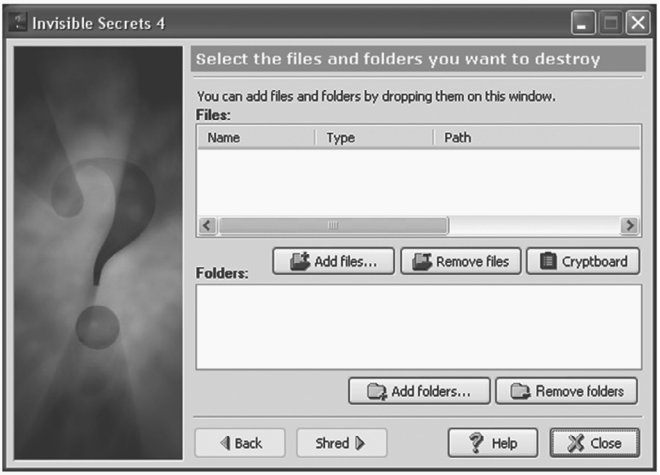

Рис. 4.46. Выбор папки или файла, которые необходимо уничтожить

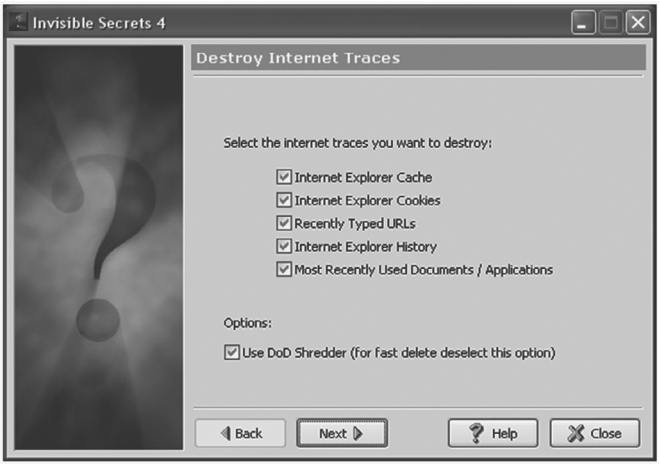

Рис. 4.47. Уничтожение ссылок

Передача паролей

Безопасная передача паролей. Одна из главных проблем, возникающих при организации защищенного обмена информацией, — это передача секретных паролей и ключей. *Invisible Secrets*-4 позволяет обмениваться паролями между двумя компьютерами при помощи создания безопасного соединения *IP*-к-*IP*.

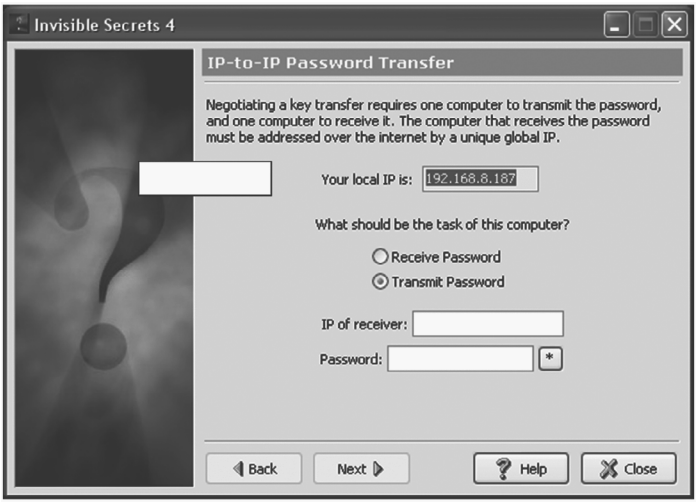

Рис. 4.48. Безопасная передача пароля

Задание

1. Установить на своем компьютере программу *Invisible Secrets*-4.
2. Ознакомиться со сведениями о программе *Invisible Secrets*, изложенными в разделе 1.
3. Запустить программу *Invisible Secrets*-4.
4. Изучить работу программы *Invisible Secrets* во всех шести возможных режимах:
   — стеганография;
   — шифрование;
   — шифрование почтовых сообщений;
   — уничтожение файлов;
   — передача паролей;
   — ограничение доступа к приложениям.
5. Сохранить в отчете экранные формы, демонстрирующие возможности программы *Invisible Secrets*-4 при работе в каждом из шести режимов.
6. Сделать выводы об эффективности используемого стеганографического пакета для каждого из рассмотренных режимов.
7. Включить в отчет о лабораторной работе ответы на контрольные вопросы, выбранные в соответствии с номером варианта из табл. 4.3.

Таблица 4.3

Номер варианта	Контрольные вопросы
1, 5, 7, 3, 9, 18, 28	Сформулируйте основные отличия стеганографических и криптографических методов защиты информационных ресурсов. В чем достоинства и недостатки каждого из методов?
2, 4, 6, 8, 20, 22, 24, 26, 30	Перечислите шесть основных режимов работы программы *Invisible Secrets*-4. В каких случаях вы можете порекомендовать использование каждого из режимов?
11, 13, 15, 10, 17, 19, 27	Оцените эффективность работы программы *Invisible Secrets*-4 с графическими и аудиофайлами различных типов. Для этого в режиме «стеганография» встройте данные в контейнеры различных форматов, сравните пустые и заполненные контейнеры, сделайте выводы
12, 14, 16, 21, 23, 25, 29	При встраивании данных в режиме «стеганография» используйте различные алгоритмы для шифрования встраиваемых данных. Сравните пустые и заполненные контейнеры, как изменяется размер заполненных контейнеров в зависимости от метода шифрования? Почему вы получили такие результаты, обоснуйте