Лабораторная работа

«Применение программных продуктов в шифровании»

Цель работы: Ознакомиться с некоторыми программными продуктами, предназначенными для зашиты информации на компьютере.

Теоретические сведения:

Стеганография (это слово происходит от греческих слов steganos (секрет, тайна) и graphy (запись) и, таким образом, означает буквально "тайнопись") обеспечивает обмен информацией таким образом, что скрывается сам факт существования секретной связи. Она не заменяет криптографию (шифрование данных), а дополняет ее еще одним уровнем безопасности. При обработке данных стеганографическими методами происходит скрытие передаваемой информации в других объектах таким образом, что бы постороннее лицо не догадывалось о существовании скрытого секретного сообщения. При этом, обнаружить такое сообщение довольно сложно, но если это и произойдет, то сообщение может быть к тому же еще и надежно зашифровано.

Современный прогресс в области глобальных компьютерных сетей и средств мультимедиа привел к разработке новых методов, предназначенных для обеспечения безопасности передачи данных по каналам телекоммуникаций и использования их в необъявленных целях. Эти методы, учитывая естественные неточности устройств оцифровки и избыточность аналогового видео или аудио сигнала, позволяют скрывать сообщения в компьютерных файлах (контейнерах). Причем, в отличие от криптографии, данные методы скрывают сам факт передачи информации.

Существуют множество программных продуктов, реализующих методы стеганографии. В данной лабораторной работе используются следующие программные средства: S-Tools, Masker, VipNet SafeDisk.

Выполнение работы:

1. Работа с программой S-Tools

S-Tools - Программа для скрытия данных от посторонних глаз. Работает без инсталляции. Использует метод стеганографии - данные прячутся в файлах графики (BMP или GIF) или музыкальном WAV-файле, которые внешне не отличаются от аналогичных файлов, не несущих спрятанной информации (картинку можно посмотреть, музыку можно послушать). Дело в том, что оцифрованные файлы (те же *.bmp или *.wav) могут быть в определенной степени изменены, и это не повлияет на качество звука или изображения (вернее, эти изменения будут практически не

заметны). Кроме этого, программа позволяет не только спрятать информацию во внешне ничем не примечательном файле, но и зашифровать ее.

Задание: Спрятать и зашифровать текстовый файл в файлы формата gif, bmp, wav

Для выполнения задания необходимо выполнить следующее:

1. Откройте программу S-Tools. Появится окно как показано на рис 1:

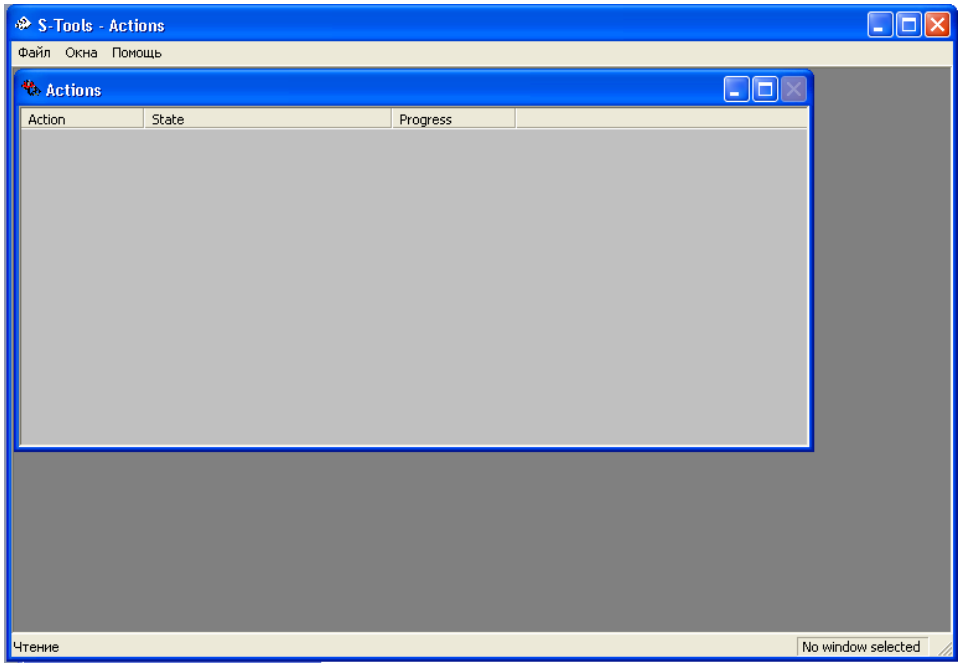

Рис 1. Окно программы S-Tools

2. Для того, чтобы скрыть любой текстовый файл в файл формата bmp, gif или wav, вам необходимо перетащить сначала файл-контейнер, а затем на него текстовый файл. В результате этого появиться окно как показано на рис 2:

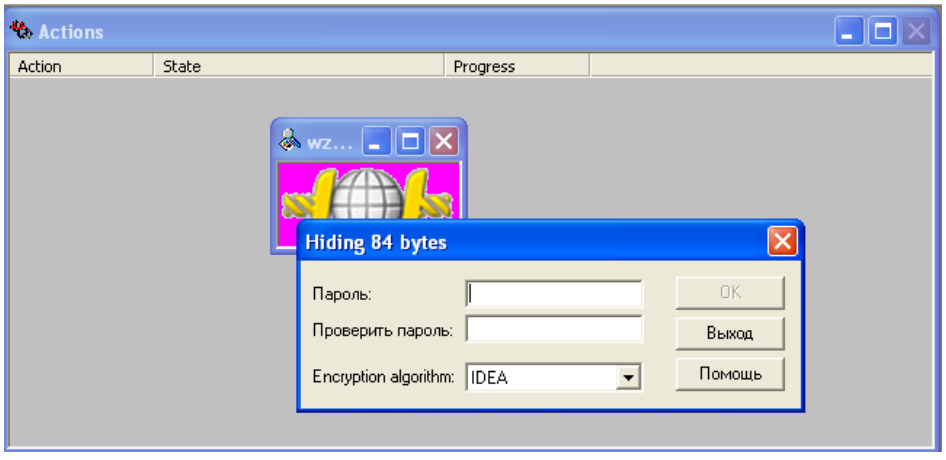

Рис 2. Скрытие файла

3. Введите пароль и выберите алгоритм шифрования; нажмите OK.

4. Для обнаружения файла, нажмите правой кнопкой мыши по появившемуся изображению и выберите обнаружить, как показано на рис 3:

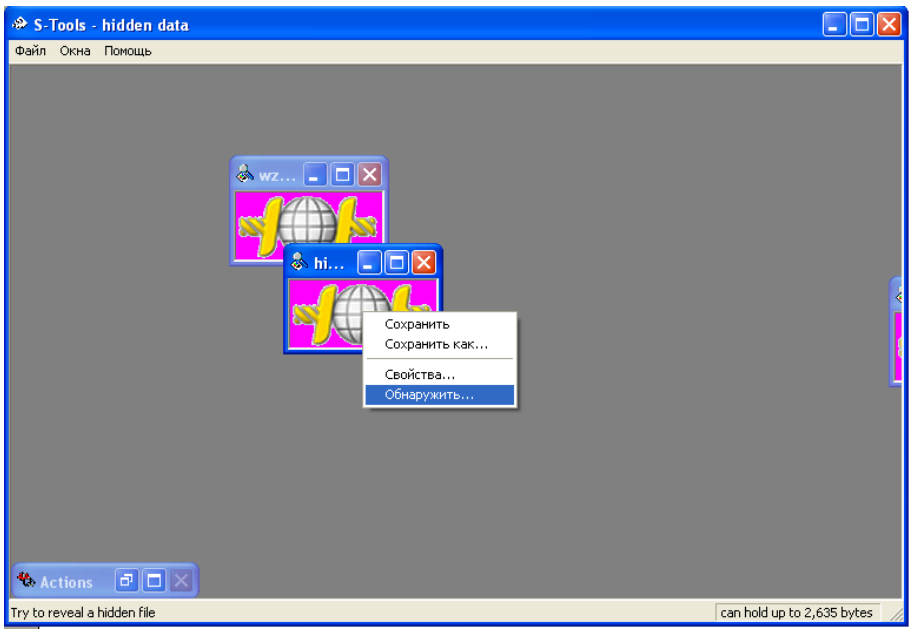

Рис 3. Обнаружение файла

2. *Работа с программой Masker 7.0*

Masker 7.0 - Программа для защиты данных, использующая стеганографию - скрытие зашифрованных данных во внешне безобидных файлах - графических (bmp, gif, jpg, tif), музыкальных (wav, mid, snd, mp3), видео (avi, mov, mpg) и даже в *.exe или *.dll, при этом файлы, в которых "прячутся" зашифрованные сведения, остаются полностью функциональны. Например, картинка, в которой спрятаны конфиденциальные сведения, при просмотре будет практически ничем не отличаться от такой же, но без внедренных в нее зашифрованных данных, разве что размером - он будет побольше. Зашифрованные таким способом данные можно не только хранить на своем компьютере, но и пересылать в виде приложения к письму - даже в случае его перехвата в нем будет обнаружена всего-навсего обычная картинка.

Задание: Спрятать и зашифровать текстовый файл в файлы формата gif, bmp, wav

Для выполнения задания необходимо выполнить следующее:

1. Откройте программу Masker 7.0. Появится окно, как показано на рис 4

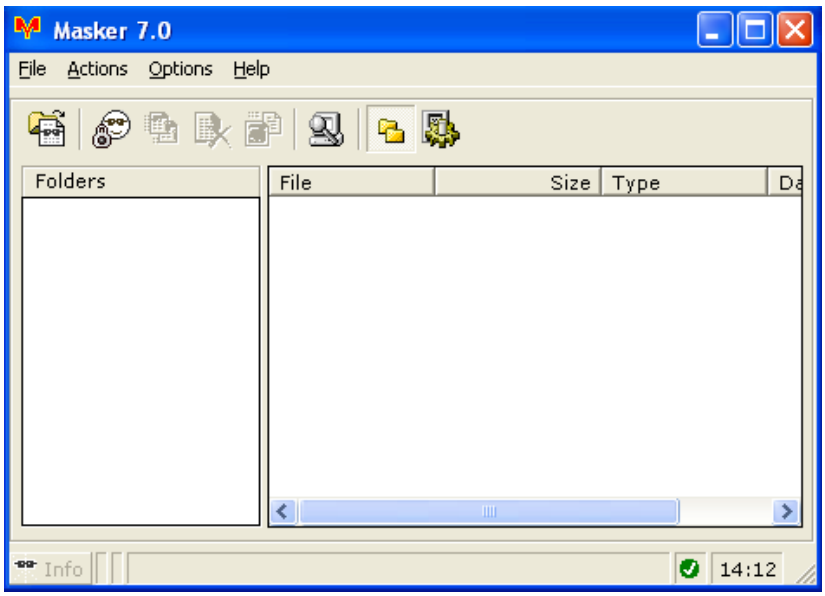

рис 4 Главное окно программы Masker 7.0

2. В меню File выберите Open Carrier File. В появившемся окне выберите файл-контейнер, в котором вы хотите скрывать файлы:

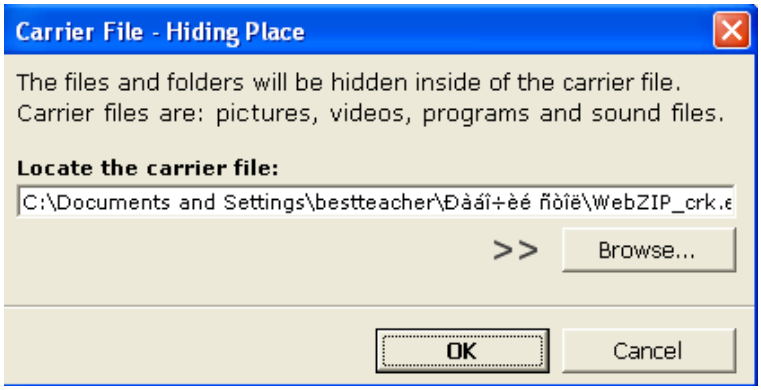

рис 5. Выбор файла-контейнера

3. Создайте новый контейнер, для чего введите его название, пароль и алгоритм кодирования, как показано на рис 6:

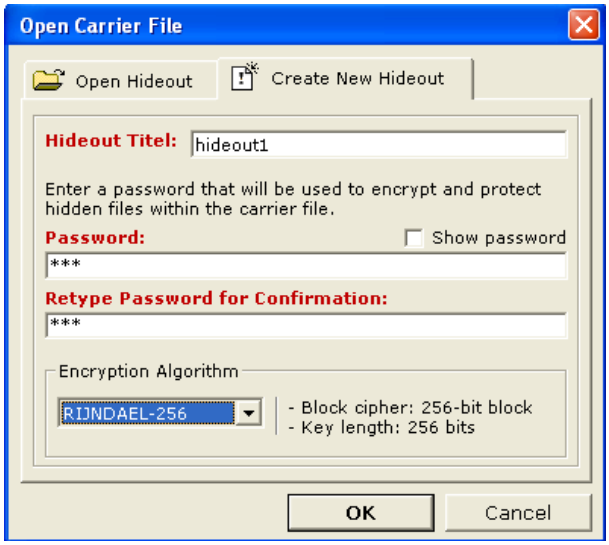

рис 6. Создание нового контейнера

4. Перейдите в меню Actions->Hide/add files. Выберите файлы и папки, которые вы хотите скрыть. Нажмите кнопку Hide для скрытия выбранных файлов и папок в файле-контейнере, как показано на рис. 7:

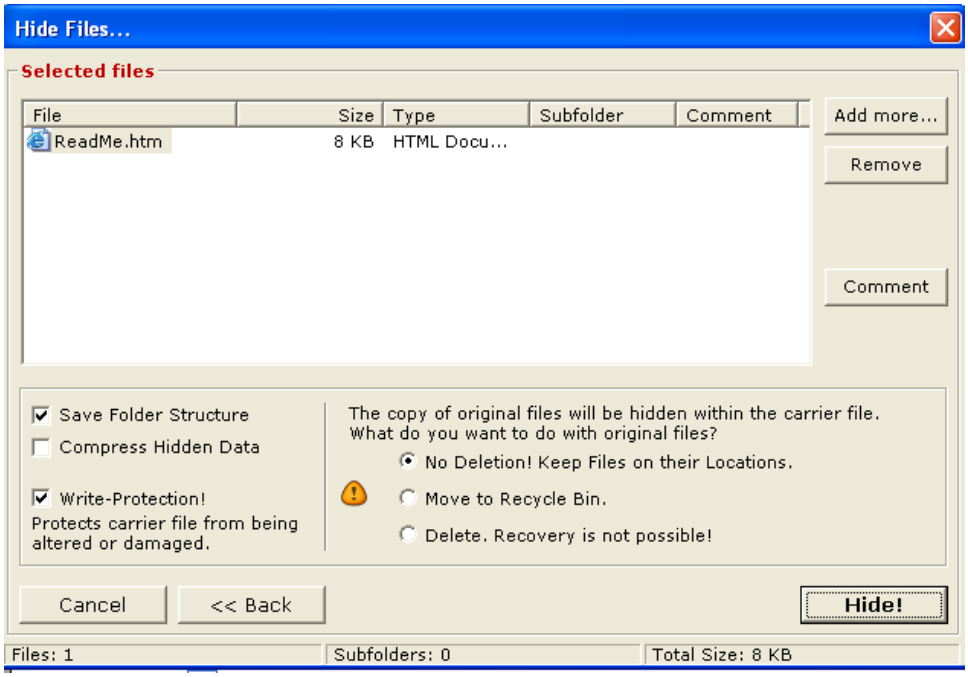

рис 7. Выбор файлов и папок для скрытия

Для извлечения скрытых файлов из контейнера, необходимо выполнить следующие действия:

1. В меню File выберите Open Carrier File. В появившемся окне выберите файл-контейнер, в котором содержаться скрытые файлы.

2. В появившемся окне укажите путь к файлу-контейнеру, где хранятся скрытые файлы.

3. Введите пароль

4. Выберите файл или папку, которую необходимо извлечь; правой кнопкой мыши нажмите на необходимый файл и выберите Extract.

3. Работа с программой VipNet Safe Disk

ViPNet Safe Disk предназначено для организации безопасного хранения конфиденциальной информации и удобной работы с ней на персональном компьютере.

Принципы работы ViPNet SafeDisk:

1. Создается контейнер в виде зашифрованного файла на диске или внешнем носителе и устанавливается способ его защиты: пароль, файл-ключ или электронный ключ;

2. При подключении контейнер отображается в системе как обычный диск, на который Вы можете сохранять конфиденциальную информацию;

3. При сохранении информации данные прозрачно шифруются, при считывании - расшифровываются. Этот процесс не отнимает времени. Вы работаете с документами в обычном режиме, но при этом Ваша информация надежно защищена;

4. При отключении контейнер перестает отображаться в системе, и установить сам факт наличия конфиденциальной информации и получить к ней доступ невозможно;

5. Чтобы восстановить доступ к ранее сохраненной в контейнере конфиденциальной информации и продолжить работу с ней, необходимо подключить контейнер. Для этого необходим пароль, файл-ключ или электронный ключ, в зависимости от выбранного Вами способа защиты.

Основные возможности программы:

- Создание контейнеров большого размера, ограниченного только возможностями используемой файловой системы;
- Дружественный интерфейс включает мастера, облегчающие выполнение всех основных действий пользователя;
- Экспорт и импорт контейнеров для передачи другому пользователю или резервного копирования;
- Режим экстренного отключения контейнеров и выхода из программы (режим "Паника");
- Подключение контейнеров в режиме "только для чтения";
- Автоматическое подключение выбранных контейнеров при старте программы;
- Автоматическое отключение контейнеров при выходе из программы;
- Шифрование данных производится по алгоритмам ГОСТ 28147-89 (длина ключа - 256 бит) и AES (длина ключа - 256 бит) по выбору пользователя;
- Использование одного из трех типов защиты контейнера: парольная защита, хранение ключей защиты в файле, аппаратный носитель ключа защиты;
- Возможность многопользовательской работы;

Задание:

1. Создать собственный контейнер для хранения конфиденциальной информации.
2. Подключить его и сохранить в нем секретные файлы.
3. Экспортировать контейнер
4. Создать нового пользователя
5. Импортировать контейнер новому пользователю
6. Включить режим «Паника» и экстренное размонтирование дисков

Выполнение задания

1. Запустите программу. Используйте значок  на **Рабочем столе** или в меню **Пуск.**

2. При первом запуске ViPNet SafeDisk откроется окно **Пароль пользователя.** Задайте пароль нового пользователя.

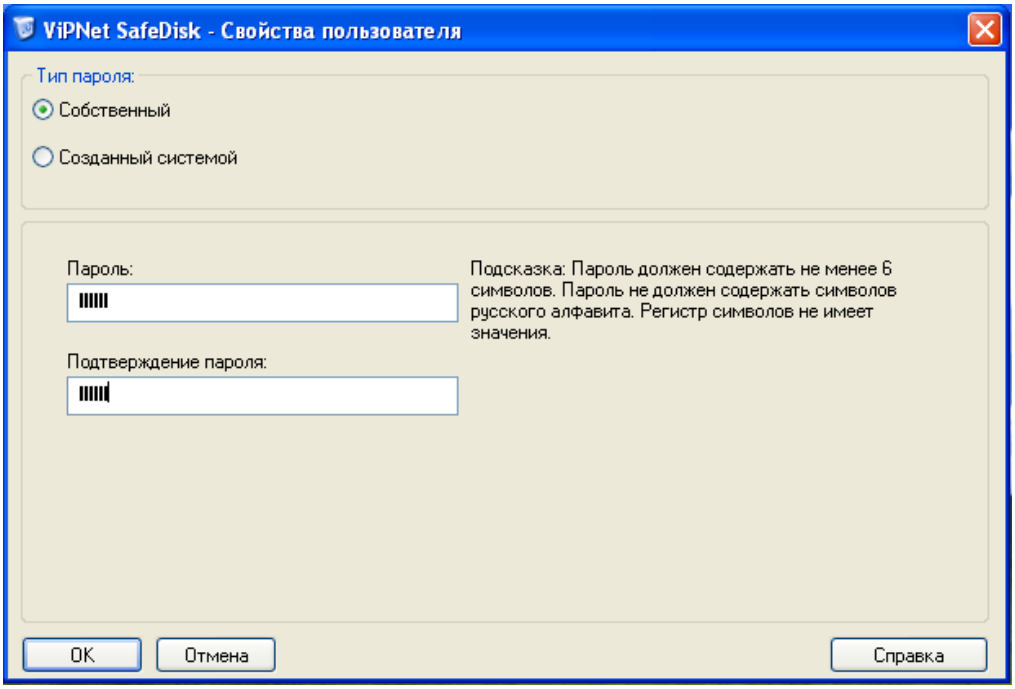

рис 8. Создание пароля нового пользователя

3. По умолчанию предлагается задать **Собственный** тип пароля. Задайте свой пароль и введите его подтверждение в соответствующих полях. Используйте заданный пароль для входа в программу при следующих запусках ViPNet SafeDisk.

После создания пароля нового пользователя откроется главное окно ViPNet SafeDisk; нажмите на кнопку создать, запустится мастер создания контейнера.

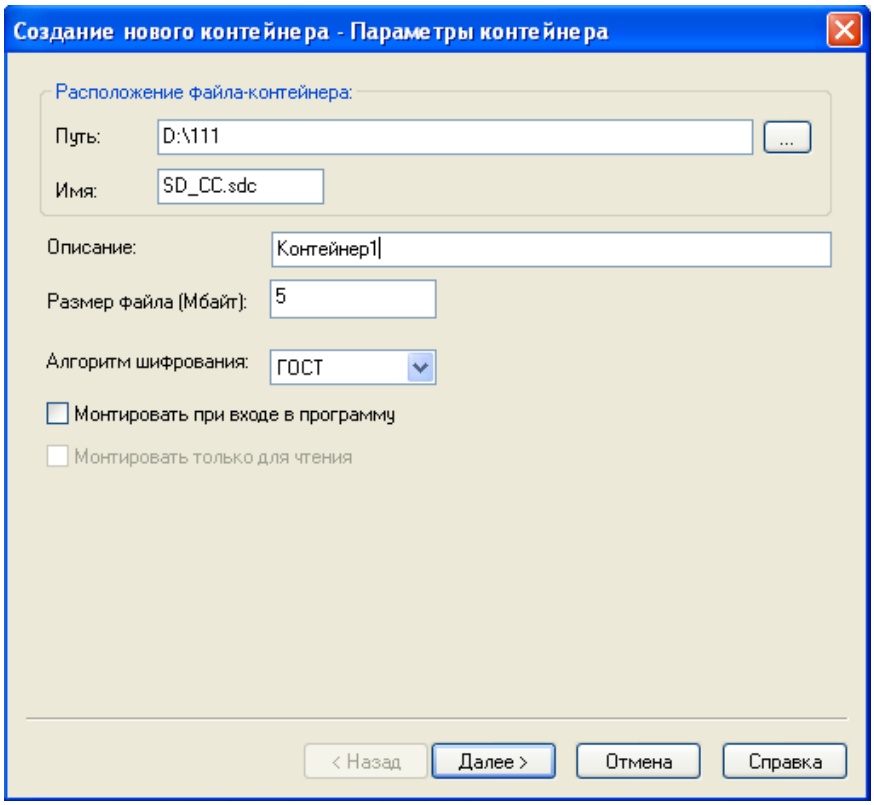

рис 9. Создание нового контейнера

4. На первой странице мастера создания контейнера задайте имя и расположение файла контейнера, его описание, размер и алгоритм шифрования. Нажмите кнопку Далее

5. В окне **Тип хранилища** выберите способ доступа к контейнеру.

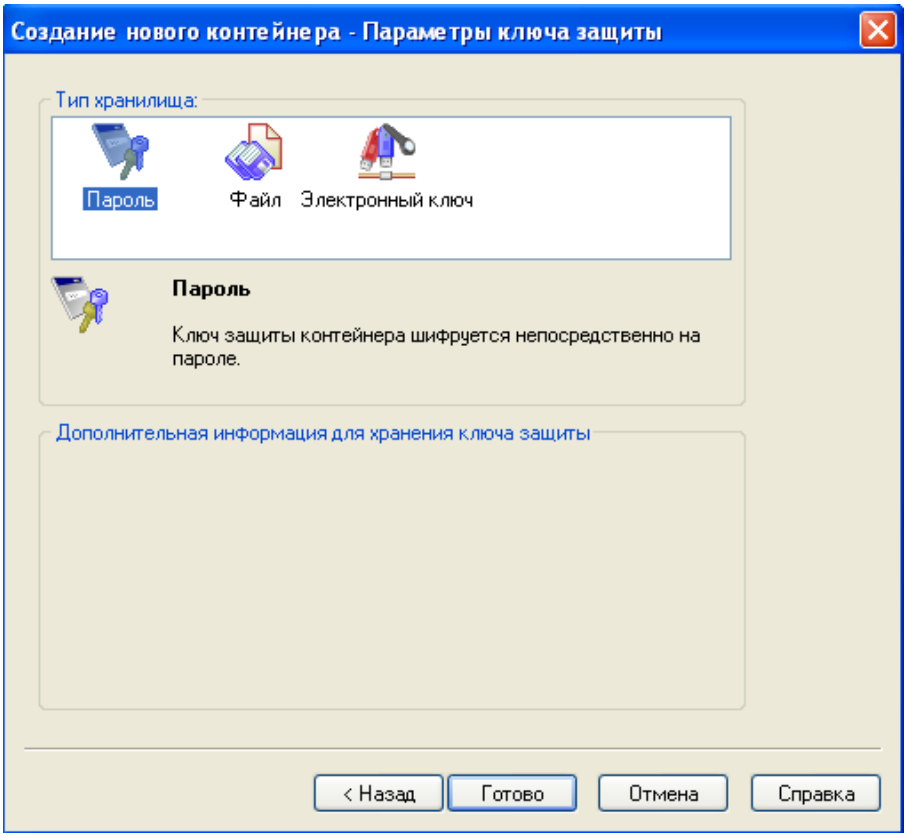

рис 10. Параметры ключа защиты

Пароль. Контейнер будет защищен только паролем, который используется для входа в программу.

Файл-ключ. Для доступа к контейнеру необходим пароль и файл-ключ. При выборе этого способа доступа задайте расположение и имя файла-ключа.

Для большей безопасности файл-ключ можно разместить на внешнем носителе.

Электронный ключ. Для доступа к контейнеру необходим пароль и электронный ключ. При выборе этого способа доступа вставьте электронный ключ в считыватель.

6. После выбора способа доступа к контейнеру нажмите **Готово.** Автоматически появится окно электронной рулетки.

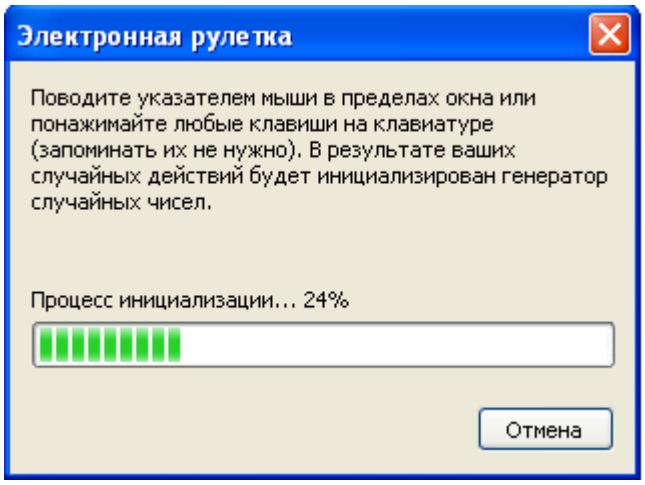

рис 11. Электронная рулетка

Для создания контейнера требуются случайные числа. Датчик случайных чисел запускается **Электронной рулеткой**, которая вызывается автоматически в момент, когда требуется получить случайное число**.**

При появлении **Электронной рулетки** до завершения процесса инициализации выполняйте действия: перемещайте указатель мыши в пределах окна или нажимайте клавиши клавиатуры.

7. Подключение контейнера. Для того чтобы в контейнер можно было сохранить данные, которые необходимо защитить, подключите контейнер. Для этого нажмите на кнопку **монтировать**. Откроется окно подключения контейнера.

Выберите настройки подключения. Используйте параметры, предложенные по умолчанию, или выберите свои.

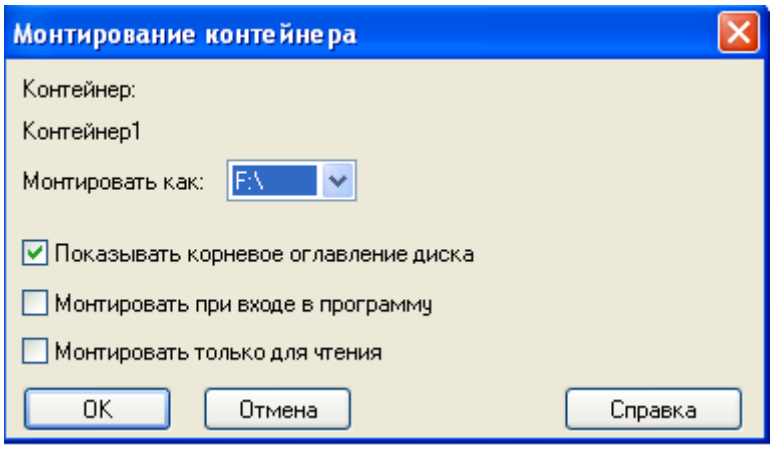

рис 12. Подключение контейнера

8. Подключаемый впервые контейнер необходимо отформатировать. Используйте параметры, предложенные по умолчанию, или задайте свои.

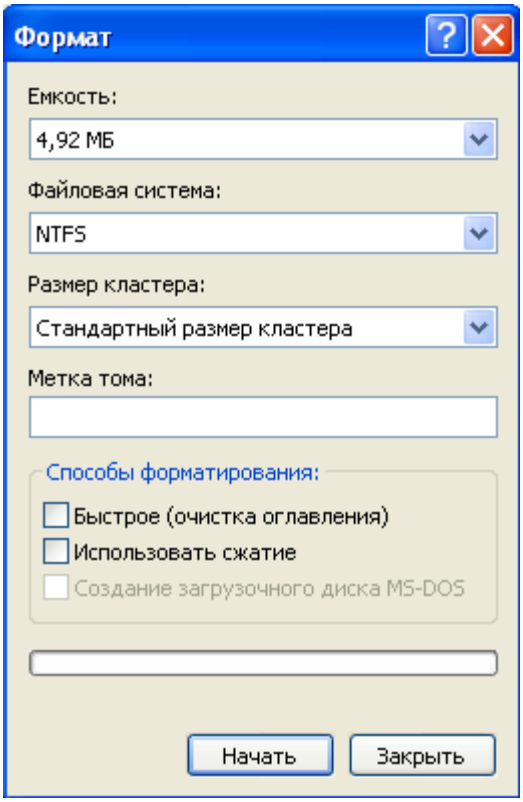

рис 13. Форматирование контейнера

Для начала форматирования нажмите **Начать**.

9. Появится предупреждающее сообщение о том, что диск будет отформатирован, и вся информация, хранящаяся на данном диске, будет потеряна. В данном случае происходит форматирование подключаемого контейнера, на котором еще не содержится никакой информации, поэтому для запуска процесса форматирования нажмите **OK**.

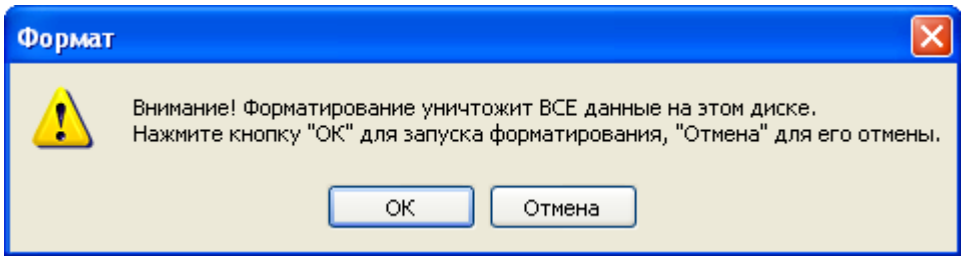

рис 14. Начало форматирования контейнера

Запустится процесс форматирования.

10. В окне с сообщением о завершении форматирования нажмите **ОК**.

11. Работа с защищенной информацией.

Подключенный контейнер отобразится как обычный диск Windows. Теперь Вы можете, например, перемещать файлы на этот диск или, работая в текстовом редакторе, сохранять на нем документы.

12. Завершение работы.

При завершении работы с защищаемой информацией, необходимо закрыть к ней доступ. Для этого завершите работу со всеми файлами, которые хранятся в контейнере, а также закройте окно **Проводника**, отображающее файлы контейнера. В главном окне нажмите кнопку размонтировать. При отключении контейнера доступ к защищаемой информации будет закрыт и скрыт сам факт наличия такой информации на Вашем компьютере.

13. Для завершения сеанса работы используйте пункт **Выход** в меню **SafeDisk.**

Резервное копирование защищенной информации.

ViPNet SafeDisk позволяет создавать резервные копии защищенной информации, чтобы при необходимости обеспечить возможность восстановления информации. Для создания резервной копии защищенных данных используется процедура **Экспорта** контейнера. В результате процедуры экспорта будет создан файл экспорта контейнера. Файл экспорта контейнера является резервной копией защищенной информации и содержит в себе файл контейнера и резервную копию ключей контейнера.

Для того чтобы произвести процедуру **Экспорта** контейнера и создать резервную копию защищенной информации, выполните следующее:

1. В главном окне ViPNet SafeDisk выберите контейнер с данными, для которых необходимо сделать резервную копию.
2. Если контейнер подключен, его необходимо отключить.
3. Выберите пункт **Экспорт** в меню **Контейнер**. Откроется окно мастера экспорта контейнера.

4. Выберите папку и укажите имя файла экспорта контейнера. В целях безопасности файл экспорта рекомендуется хранить отдельно от защищенной информации, например, на внешнем носителе

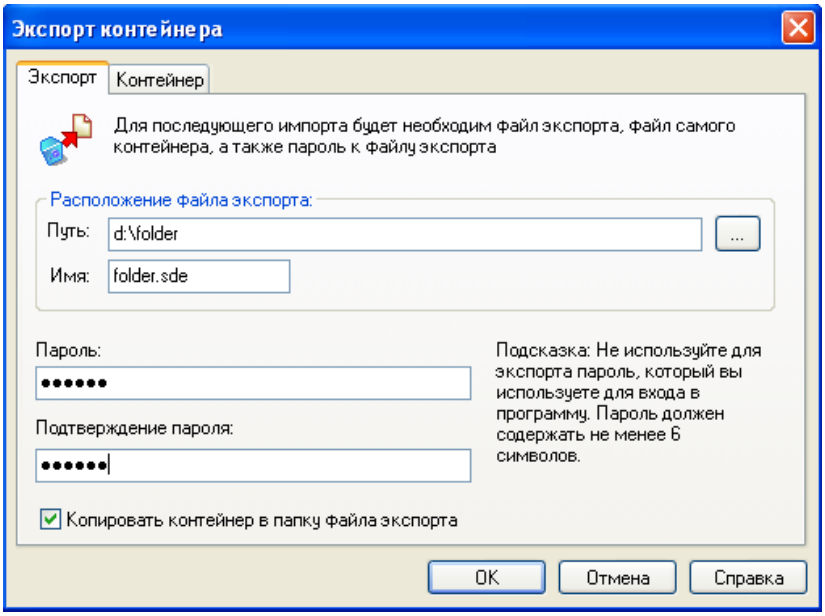

рис 15. Экспорт компьютера

Заполните поля и нажмите кнопку OK

Регистрация нового пользователя

ViPNet SafeDisk является многопользовательской программой, что позволяет работать каждому пользователю со своими защищенными данными, независимо друг от друга. Для того чтобы начать сеанс работы нового пользователя необходимо выполнить следующее:

1. Если программа уже запущена, завершите сеанс работы текущего пользователя. Для этого выберите пункт **Выход** в меню **SafeDisk**.
2. Запустите программу. Выберите **Войти как > Новый пользователь**

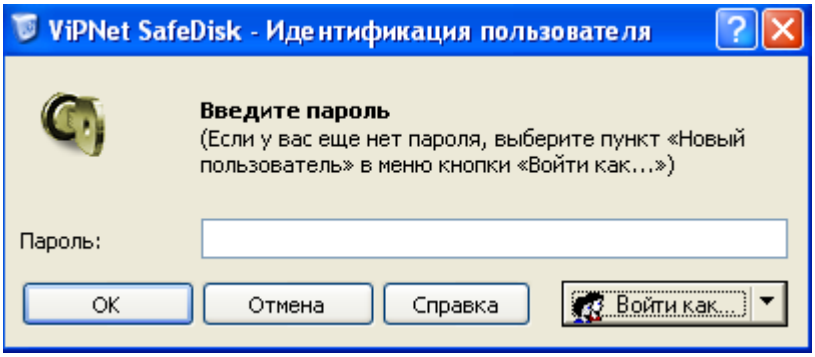

рис 16 Создание нового пользователя

3. Откроется окно **Пароль пользователя SafeDisk**.

4. В окне **Пароль пользователя SafeDisk** по умолчанию выбран **Собственный** тип пароля. Задайте пароль нового пользователя, введите подтверждение пароля и нажмите **ОК**. Начнется сеанс работы вновь зарегистрированного пользователя.

При последующих запусках ViPNet SafeDisk для начала работы зарегистрированного пользователя в окне ввода пароля необходимо ввести созданный пароль.

Смена пароля пользователя

В целях повышения безопасности рекомендуется периодически изменять свой пароль.

1. Выберите пункт **Сменить пароль** в меню **Безопасность**. Появится окно создания пароля пользователя.

2. В окне **Пароль пользователя SafeDisk** по умолчанию выбран **Собственный** тип пароля. Задайте пароль нового пользователя, введите подтверждение пароля и нажмите **ОК**.

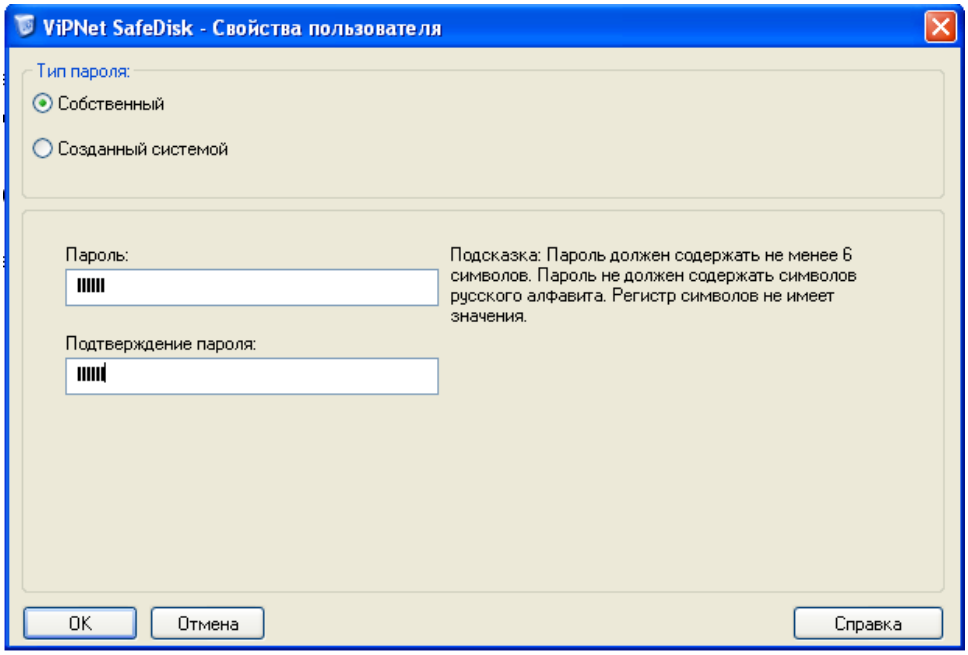

рис 17. Смена пароля пользователя

При последующих запусках ViPNet SafeDisk для начала сеанса работы используйте вновь созданный пароль.

Если при использовании ViPNet SafeDisk до смены пароля были созданы резервные копии конфигурации, которые будут необходимы в дальнейшем, запомните предыдущий пароль

Перенос защищенной информации с одного компьютера на другой

Если необходимо обеспечить защищенный перенос конфиденциальной информации на другой компьютер, например, с рабочего компьютера на домашний, ViPNet SafeDisk позволяет сделать это с помощью экспорта и импорта контейнера.

Экспорт контейнера

1. В главном окне **ViPNet SafeDisk** выберите контейнер с данными, которые необходимо перенести.
2. Если контейнер подключен, его необходимо отключить.
3. Выберите пункт **Экспорт** в меню **Контейнер**. Откроется окно мастера экспорта контейнера.
4. Укажите расположение и имя создаваемого файла экспорта контейнера
5. Для последующего доступа к файлу экспорта задайте пароль и его подтверждение.
6. Задайте свойства экспортируемого контейнера.
7. На внешнем носителе, например флеш-накопителе или диске, перенесите файл экспорта контейнера на другой компьютер.

Импорт контейнера на другом компьютере

1. Запустите ViPNet SafeDisk и введите пароль.
2. Произведите процедуру импорта с использованием перенесенного файла экспорта. Для этого выберите пункт **Импорт** в меню **Контейнер**. Откроется мастер импорта контейнера.
3. Укажите расположение на внешнем носителе созданного файла экспорта контейнера
4. Задайте расположение и имя файла импортируемого контейнера
5. Выберите способ доступа к контейнеру: файл-ключ, пароль или электронный ключ
6. После импорта контейнер появится в главном окне ViPNet SafeDisk**.**

Срочное отключение доступа к защищенной информации. Режим «Паника»

Если существует потенциальная опасность, что к Вашему компьютеру могут подойти злоумышленники, выполните следующее:

1. Заранее включите режим **Паника**, нажав кнопку  на панели инструментов в главном окне**.**

2. При приближении злоумышленников, нажмите кнопку  или комбинацию клавиш **Ctrl+Alt+P**.

Произойдет срочное отключение всех подключенных контейнеров, доступ к защищенной информации будет закрыт, сами диски в Windows отображаться не будут. Также исчезнет с экрана Вашего монитора главное окно программы и исчезнет значок в

области уведомлений. В результате, сам факт Вашей работы с конфиденциальной информацией будет сложно установить.

Если в течение 60 секунд ViPNet SafeDisk не сможет отключить контейнеры, произойдет перезагрузка компьютера.

Ход работы:

1. Зашифровать и спрятать текстовый файл в файлы формата .bmp, .gif или .wav с помощью программы S-TOOLS.
2. Зашифровать и спрятать текстовый файл с помощью программы MASKER.
3. Создать собственный контейнер для хранения секретной информации с помощью программы VipNet Safe Disk. Изучить возможности программы.
4. Подготовить отчет в электронном виде, содержащий краткие сведения о каждой из изученных программ.

Контрольные вопросы:

1. Что такое стеганография?
2. Программные продукты для реализации методов стеганографии
3. С какими файлами работает программа S-Tools? Преимущества и недостатки программы
4. С какими файлами работает программа Masker 7.0? Преимущества и недостатки программы
5. Применение программного продукта VipNet Safe Disk
6. Для чего нужен экспорт и импорт контейнера?
7. Что такое режим работы «Паника»?