**1. Цель работы**

Изучить принципы работы средств "прозрачного" шифрования.

**2. Порядок проведения работы**

2.1. Изучить лекционный материал (разделы [2.1-2.4](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\chapter2_1.html))  
2.2. Изучить теоретический материал по лабораторной работе  
2.3. Выполнить задание на лабораторную работу.   
2.4. Ответить на контрольные вопросы.

**3. Задание на лабораторную работу**

3.1. Создать файл-контейнер с помощью программы StrongDisk  
3.2. Подключить созданный контейнер как логический диск  
3.3. Скопировать файлы на этот диск и проверить их работоспособность (для исполняемых файлов - путем запуска, для текстовых - путем редактирования), кроме того, просмотреть содержимое файла-контейнера, убедившись, что оно зашифровано.  
3.4. Отключить логический диск и просмотреть содержимое файла-контейнера, убедившись, что оно зашифровано  
3.5. Создать файл-контейнер с помощью программы Steganos Security Suite.  
3.6. Подключить созданный контейнер как логический диск  
3.7. Скопировать файлы на этот диск и проверить их работоспособность (для исполняемых файлов - путем запуска, для текстовых - путем редактирования), кроме того, просмотреть содержимое файла-контейнера, убедившись, что оно зашифровано.  
3.8. Отключить логический диск и просмотреть содержимое файла-контейнера, убедившись, что оно зашифровано

**4. Теоретический материал и практические аспекты**

Для выполнения данной лабораторной работы необходимо знание учебного материала в объеме пп. [2.1-2.4.](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\chapter2_1.html)

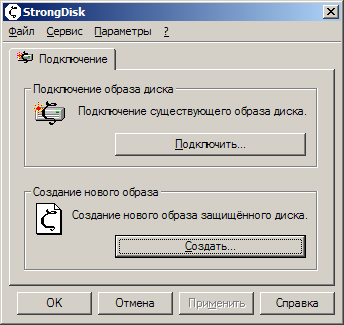
Традиционные средства криптографической защиты файлов позволяют хранить файлы в зашифрованном виде, но для работы с ними данные должны быть расшифрованы и храниться в открытом виде все время их обработки. При этом участки файлов могут оказаться и в файле подкачки, и во временных файлах используемых приложений. Кроме того, пользователь может забыть зашифровать заново измененный файл. Все это делает схему работы с файлами, зашифрованными с помощью традиционных схем, не очень надежной, и рекомендуется использовать такие средства только для архивного хранения информации.

Прозрачное шифрование позволяет работать с файлами и каталогами, которые хранятся на жестком диске в зашифрованном виде, расшифровываются только в память и только на время работы с очередным блоком файла. Такие системы предусматривают защиту от сбрасывания данных в файлы подкачки и временные файлы.

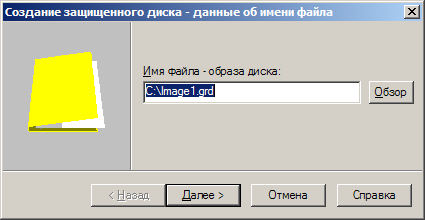
**ПРОГРАММА ДЛЯ ПРОЗРАЧНОГО ШИФРОВАНИЯ ФАЙЛОВ И КАТАЛОГОВ STRONGDISK**

StrongDisk для Windows 95/98/NT/2000 позволяет хранить конфиденциальные данные на шифрованных дисках. Шифрованный диск ничем не отличается от обычных дисков в системе, но всё его содержимое при записи шифруется. Для подключения шифрованного диска нужно указать пароль. Любые документы, таблицы, базы данных любого объема могут храниться на шифрованных дисках и открываться непосредственно с шифрованных дисков. Содержимое шифрованных диска физически располагается в одном обычном файле, что позволяет легко делать резервные копии и пересылать их по электронной почте. Подключенные шифрованные диски могут совместно использоваться в сети с распределением прав доступа стандартными средствами Windows.

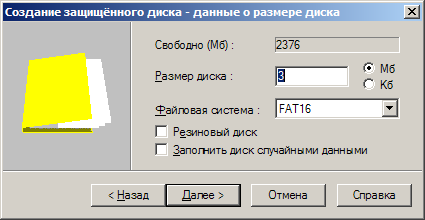
Прежде всего, нам необходимо создать образ диска, который в дальнейшем будет служить контейнером для хранения зашифрованных данных:



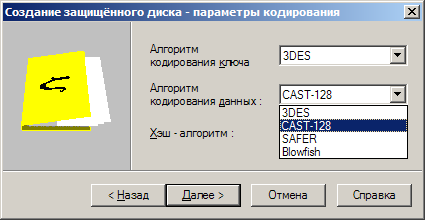
Необходимо выбрать имя файла-контейнера:



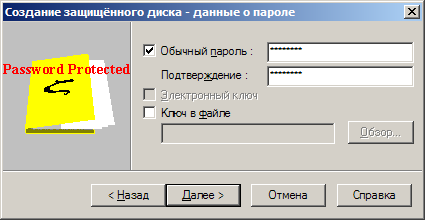
Далее настраиваем параметры контейнера: его размер и файловую систему. Кроме того, можно сделать диск "резиновым", когда изначально создается диск минимального размера, который затем изменяется в зависимости от количества хранимых данных. Если размер диска постоянен, то можно предварительно заполнить диск случайными данными - для того, чтобы затруднить криптоанализ на основе пустого текста.



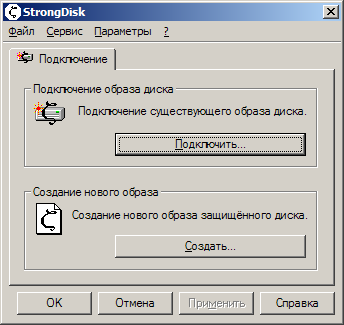
Далее можно выбрать алгоритмы кодирования ключа и данных, а также хеш-функцию:



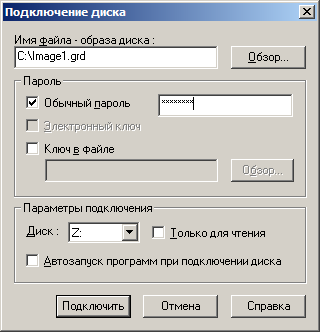
После этого задается пароль - либо вводом строки, либо заданием файла с паролем. Кроме того, может использоваться электронный ключ.



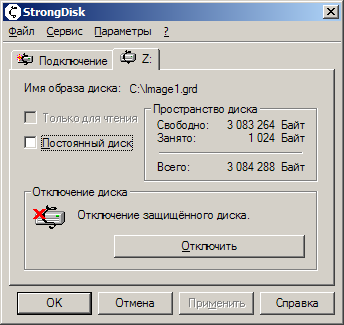
После этого создается диск с заданными параметрами. Для работы диск должен быть подключен:



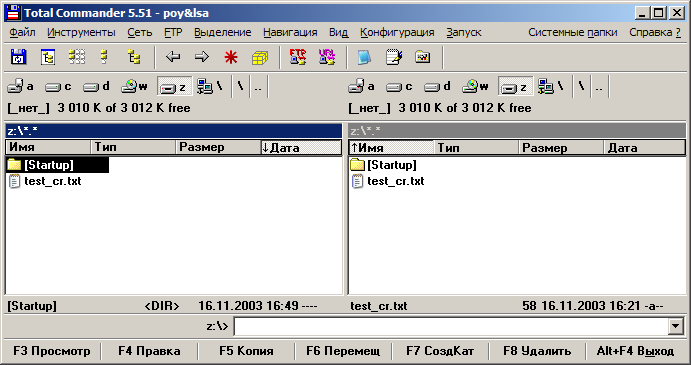
Для подключения необходимо выбрать файл с образом и указать его пароль, а также указать возможные параметры подключения (буква диска, подключение только для чтения):



После этого диск будет подключен как обычный локальный диск:



Операционная система ничем не отличает его от других дисков, что позволяет успешно работать с зашифрованными файлами и каталогами из любых программ:



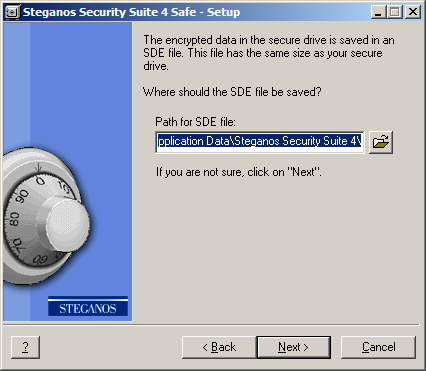
Загрузить пробную версию программы StrongDisk: [SDSETUP.EXE](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\soft\SDSETUP.EXE)

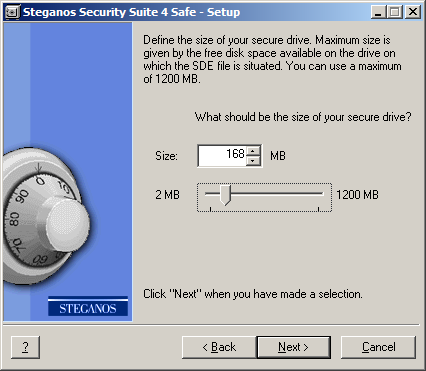
Просмотреть видеозаписи настройки и работы с программой: [sd\_1.avi](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\video\sd_1.avi), [sd\_2.avi](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\video\sd_2.avi)

**STEGANOS SECURITY SUITE**

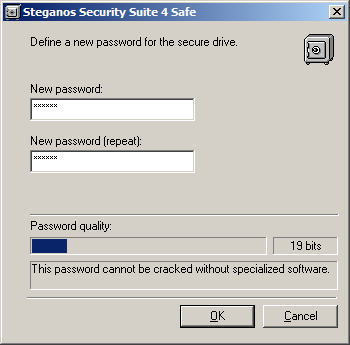
Эта программа, в числе прочего, позволяет создать на компьютере виртуальный шифрованный диск, доступ к которому без знания пароля невозможен.

Перед созданием диска необходимо указать каталог, где будет храниться соответствующий файл-образ, и его размеры:

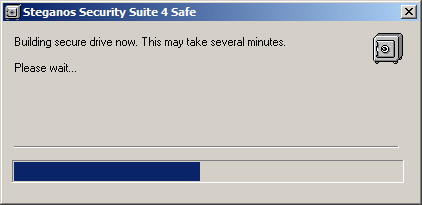




После этого программа запросит задать пароль для доступа к диску (при вводе пароля отображается его качество и характеристика возможности взлома):

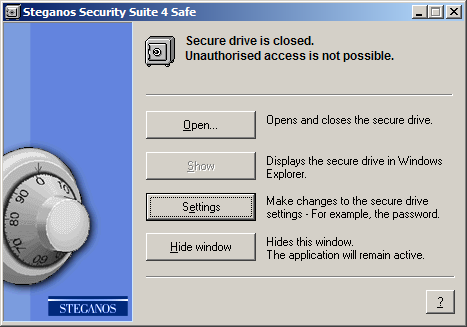


После этого будет создан диск с заданными характеристиками:

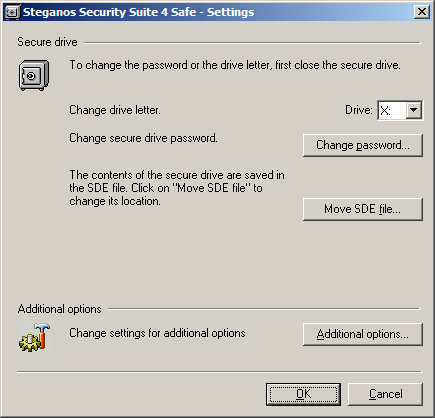




Теперь можно работать с созданным "сейфом" (именно так называется шифродиск в этой программе:



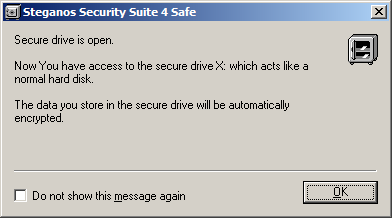
Можно изменить его пользовательские характеристики, например, букву, под которой он будет зарегистрирован в системе:



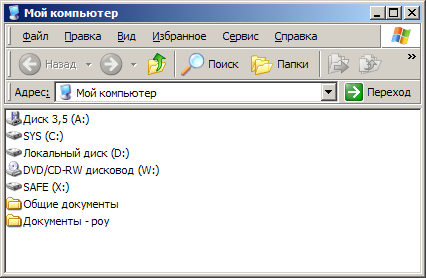
Для доступа к диску необходимо ввести пароль:



Если пароль введен правильно, то диск будет открыт:



Он виден в системе как обычный логический диск:



И может быть использован любыми системными и прикладными программами.

Загрузить пробную версию программы Steganos Security Suite: [sss4int.exe](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\soft\sss4int.exe)

Просмотреть видеозаписи настройки и работы с программой: [sss\_1.avi](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\video\sss_1.avi), [sss\_2.avi](file:///C:\Users\student\Desktop\учебник%20Сане\Защ_ин\video\sss_2.avi).