**Практическое занятие №6**

**Тема «**Изучение принципов работы с компьютерными программами для криптографической защиты информации при передаче и хранении**»**

Цель: Овладение навыками работы с компьютерными программами для криптографической защиты информации при передаче и хранении.

**Теоретическое введение**

С задачей подбора программного обеспечения для криптографической защиты данных сталкивается каждый, кто всерьез задумывается о безопасности своей конфиденциальной информации. И в этом нет абсолютно ничего удивительного - шифрование на сегодняшний день является одним из самых надежных способов предотвратить несанкционированный доступ к важным документам, базам данных, фотографиям и любым другим файлам.

Проблема заключается в том, что для грамотного выбора необходимо понимать все аспекты работы криптографических продуктов. В противном случае можно очень легко ошибиться и остановиться на ПО, которое либо не позволит защитить всю необходимую информацию, либо не обеспечит должной степени безопасности. На что же нужно обращать внимание? Во-первых, это доступные в продукте алгоритмы шифрования. Во-вторых, способы аутентификации владельцев информации. В-третьих, способы защиты информации. В-четвертых, дополнительные функции и возможности. В-пятых, авторитет и известность производителя, а также наличие у него сертификатов на разработку средств шифрования.

## **Secret Disk 4 Lite**

Разработчиком продукта [Secret Disk 4 Lite](http://www.1csoft.ru/catalog/7627/4039257/4071068/) является компания **Aladdin** – один из мировых лидеров, работающих в области информационной безопасности. **Secret Disk 4 Lite** может использоваться для шифрования отдельных разделов винчестера, любых съемных накопителей, а также для создания защищенных виртуальных дисков. Таким образом, с помощью этого инструмента можно решить большую часть задач, связанных с криптографией. Отдельно стоит отметить возможность шифрования системного раздела. При этом сама загрузка ОС неавторизированным пользователем становится невозможной. Причем эта защита несоизмеримо надежнее, нежели встроенные средства защиты Windows.

В продукте **Secret Disk 4 Lite** нет встроенных алгоритмов шифрования. Эта программа для своей работы использует внешние криптопровайдеры. По умолчанию применяется стандартный модуль, интегрированный в Windows. В нем реализованы алгоритмы DES и 3DES. Однако сегодня они считаются уже морально устаревшими. Поэтому для лучшей защиты можно загрузить с сайта Aladdin специальный **Secret Disk Crypto Pack**. Это криптопровайдер, в котором реализованы наиболее надежные на сегодняшний день криптографические технологии, включая AES и Twofish с длиной ключа до 256 бит. Кстати, в случае необходимости в сочетание с Secret Disk 4 Lite можно использовать сертифицированных поставщиков алгоритмов Signal-COM CSP и «КриптоПро CSP”.

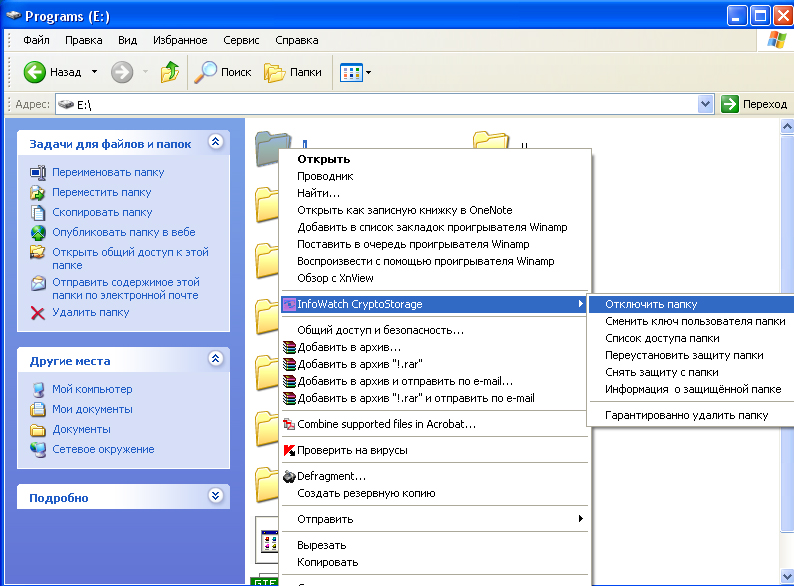
Отличительной особенностью **Secret Disk 4 Lite** является система аутентификации пользователей. Дело в том, что она построена на использовании цифровых сертификатов. Для этого в комплект поставки продукта включен аппаратный USB-токен eToken. Он представляет собой надежно защищенное хранилище для секретных ключей. Фактически, речь идет о полноценной двухфакторной аутентификации (наличие токена плюс знание его PIN-кода). В результате рассматриваемая система шифрования избавлена от такого "узкого" места, как использование обычной парольной защиты.

Из дополнительных функция **Secret Disk 4 Lite** можно отметить возможность многопользовательской работы (владелец зашифрованных дисков может предоставить доступ к ним другим людям) и фоновую работу процесса шифрования.

Интерфейс **Secret Disk 4 Lite** прост и понятен. Он выполнен на русском языке, точно так же, как и подробная справочная система, в которой расписаны все нюансы использования продукта.

## **InfoWatch CryptoStorage**

[InfoWatch CryptoStorage](http://www.1csoft.ru/catalog/7627/4039257/5634393/) – продукт достаточно известной компании **InfoWatch**, обладающей сертификатами ФСБ РФ на разработку, распространение и обслуживание шифровальных средств. Они не обязательны, но могут играть роль своеобразного индикатора серьезности компании и качества выпускаемой ею продукции.

[](http://www.1csoft.ru/upload/1csoft/cryptostorage.jpg)

В **InfoWatch CryptoStorage** реализован только один алгоритм шифрования – AES с длиной ключа 128 бит. Аутентификация пользователей реализована с помощью обычной парольной защиты. Ради справедливости стоит отметить, что в программе есть ограничение минимальной длины ключевых слов, равное шести символам. Тем не менее, парольная защита, безусловно, сильно уступает по своей надежности двухфакторной аутентификации с использованием токенов.

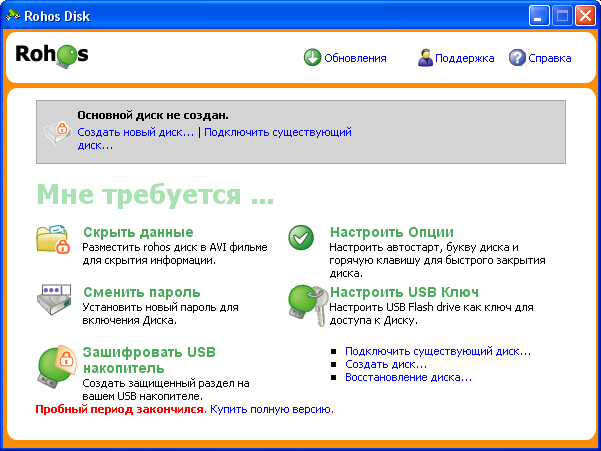
Особенностью программы **InfoWatch CryptoStorage** является ее универсальность. Дело в том, что с ее помощью можно зашифровывать отдельные файлы и папки, целые разделы винчестера, любые съемные накопители, а также виртуальные диски. Кстати, данный продукт, как и предыдущий, позволяет защищать системные диски, то есть он может использоваться для предотвращения несанкционированной загрузки компьютера. Фактически, **InfoWatch CryptoStorage** позволяет решить весь спектр задач, связанных с использованием симметричного шифрования.

Дополнительной возможностью рассматриваемого продукта является организация многопользовательского доступа к зашифрованной информации. Кроме того, в **InfoWatch CryptoStorage** реализовано гарантированное уничтожение данных без возможности их восстановления.

**InfoWatch CryptoStorage** – русскоязычная программа. Ее интерфейс, выполнен на русском языке, однако достаточно необычен: главное окно как таковое отсутствует (есть только небольшое окошко конфигуратора), а практически вся работа реализована с помощью контекстного меню. Такое решение непривычно, однако нельзя не признать его простоту и удобство. Естественно, русскоязычная документация в программе также имеется.

## **Rohos Disk**

**Rohos Disk** – продукт компании Tesline-Service.S.R.L. Он входит в линейку небольших утилит, реализующих различные инструменты по защите конфиденциальной информации. Разработка этой серии продолжается с 2003 года.

[](http://www.1csoft.ru/upload/1csoft/rohos.jpg)

Программа **Rohos Disk** предназначена для криптографической защиты компьютерных данных. Она позволяет создавать зашифрованные виртуальные диски, на которые можно сохранять любые файлы и папки, а также устанавливать программное обеспечение. Для защиты данных в данном продукте используется криптографический алгоритм AES с длиной ключа 256 бит, который обеспечивает высокую степень безопасности.

В **Rohos Disk** реализовано два способа аутентификации пользователей. Первый из них – обычная парольная защита со всеми ее недостатками. Второй вариант – использование обычного USB-диска, на который записывается необходимый ключ. Откровенно говоря, данный вариант также не является очень надежным. При его использовании утеря "флешки" может грозить серьезными проблемами.

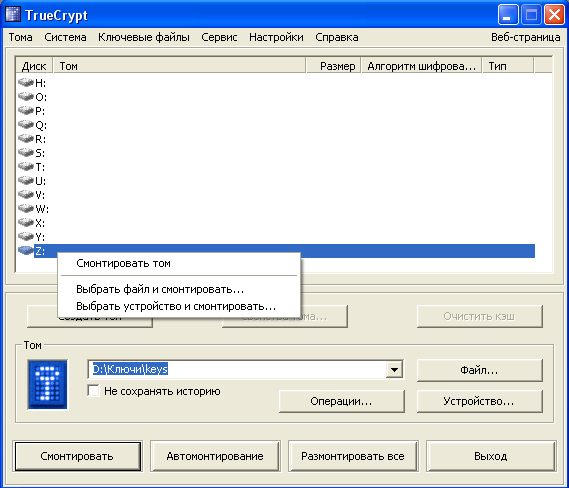
**Rohos Disk** отличается широким набором дополнительных возможностей. В первую очередь стоит отметить защиту USB-дисков. Суть ее заключается в создании на "флешке" специального зашифрованного раздела, в котором можно без опасений переносить конфиденциальные данные. Причем в состав продукта входит отдельная утилита, с помощью которой можно открывать и просматривать эти USB-диски на компьютерах, на которых не инсталлирован Rohos Disk.

Следующая дополнительная возможность – поддержка стеганографии. Суть этой технологии заключается в сокрытии зашифрованной информации внутри мультимедиа-файлов (поддерживаются форматы AVI, MP3, MPG, WMV, WMA, OGG). Ее использование позволяет скрыть сам факт наличия секретного диска путем его размещения, например, внутри фильма. Последней дополнительной функцией является уничтожение информации без возможности ее восстановления.

Программа **Rohos Disk** обладает традиционным русскоязычным интерфейсом. Кроме того, она сопровождена справочной системой, может быть, не столь подробной, как у двух предыдущих продуктов, однако достаточной для освоения принципов ее использования.

## **TrueCrypt**

Говоря о криптографических утилитах, нельзя не упомянуть и про бесплатное программное обеспечение. Ведь сегодня практически во всех областях есть достойные продукты, распространяющиеся совершенно свободно. И защита информации не является исключением из этого правила.

[](http://www.1csoft.ru/upload/1csoft/truecrypt.jpg)

Правда, к использованию свободного ПО для защиты информации существует двоякое отношение. Дело в том, что многие утилиты пишутся программистами-одиночками или небольшими группами. При этом никто не может поручиться за качество их реализации и отсутствии "дыр", случайных или намеренных. Но криптографические решения сами по себе весьма сложны для разработки. При их создании нужно учитывать огромное множество различных нюансов. Именно поэтому рекомендуется применять только широко известные продукты, причем обязательно с открытым кодом. Только так можно быть уверенным, что они избавлены от "закладок" и протестированы большим количеством специалистов, а значит, более-менее надежны. Примером такого продукта является программа **TrueCrypt**.

**TrueCrypt** является, пожалуй, одной из самых функционально богатых бесплатных криптографических утилит. Изначально она использовалась только для создания защищенных виртуальных дисков. Все-таки для большинства пользователей это наиболее удобный способ защиты различной информации. Однако со временем в ней появилась функция шифрования системного раздела. Как мы уже знаем, она предназначается для защиты компьютера от несанкционированного запуска. Правда, шифровать все остальные разделы, а также отдельные файлы и папки TrueCrypt пока не умеет.

В рассматриваемом продукте реализовано несколько алгоритмов шифрования: AES, Serpent и Twofish. Владелец информации может сам выбрать, какой из них он хочет использовать в данный момент. Аутентификации пользователей в **TrueCrypt** может производиться с помощью обычных паролей. Однако есть и другой вариант – с использованием ключевых файлов, которые могут сохраняться на жестком диске или любом съемном накопителе. Отдельно стоит отметить поддержку данной программой токенов и смарт-карт, что позволяет организовать надежную двухфакторную аутентификацию.

Из дополнительных функций рассматриваемой программы можно отметить возможность создания скрытых томов внутри основных. Она используется для сокрытия конфиденциальных данных при открытии диска под принуждением. Также в **TrueCrypt** реализована система резервного копирования заголовков томов для их восстановлении при сбое или возврата к старым паролям.

Интерфейс **TrueCrypt** привычен для утилит подобного рода. Он многоязычен, причем есть возможность установить и русский язык. С документацией дела обстоят гораздо хуже. Она есть, причем весьма подробная, однако написана на английском языке. Естественно, ни о какой технической поддержки речи идти не может. Максимум, на что можно рассчитывать – ответ на вопрос на форуме.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Secret Disk 4 Lite** | **InfoWatch CryptoStorage** | **Rohos Disk** | **TrueCrypt** |
| Алгоритмы шифрования | DES, 3DES, AES, TwoFish | AES | AES | AES, Serpent, Twofish |
| Максимальная длина ключа шифрования | 256 | 128 | 256 | 256 |
| Подключение внешних криптопровайдеров | + | - | - | - |
| Строгая аутентификация с использованием токенов | + | - | - | +(токены приобретаются отдельно) |
| Шифрование файлов и папок | - | + | - | - |
| Шифрование разделов | + | + | - | - |
| Шифрование системы | + | + | - | + |
| Шифрование виртуальных дисков | + | + | + | + |
| Шифрование съемных накопителей | + | + | + | - |
| Поддержка многопользовательской работы | + | + | - | - |
| Гарантированное уничтожение данных | - | + | + | - |
| Сокрытие зашифрованных объектов | - | - | + | - |
| Работа "под принуждением" | - | - | - | + |
| Русскоязычный интерфейс | + | + | + | + |
| Русскоязычная документация | + | + | + | - |
| Техническая поддержка | + | + | + | - |

Рассмотренные продукты различаются достаточно сильно. Так какой же из них выбрать? Ответ на этот вопрос зависит от того, для чего планируется использовать программу. Если речь идет о защите каких-то файлов в домашних условиях, то вполне можно обойтись бесплатным программным обеспечением.

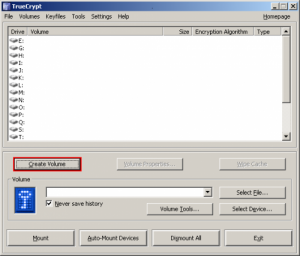
Для корпоративных клиентов выбор также нужно осуществлять, исходя из конкретных потребностей. Хотя, можно сказать, что в большинстве случаев бесплатные программы тут не подойдут из-за отсутствия некоторого функционала, в частности, возможности многопользовательской работы. Кроме того, отдельно нужно учесть необходимость строгой аутентификации (она, безусловно, надежнее, однако продукты с ней стоят дороже из-за включения в их состав токенов или смарт-карт) и использования более надежных алгоритмов шифрования.

## **Порядок работы с программой TrueCrypt**

**Этап  1:**

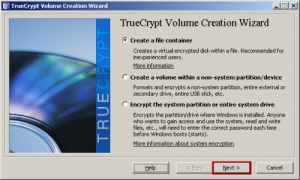
Установить и запустить

**Этап  2:**

**[](http://www.truecryptrussia.ru/images/stories/images_st/2.png)**

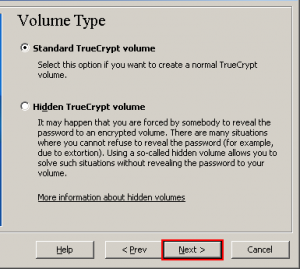
Откроется окошко TrueCrypt. Далее нажимайте на кнопку «Create Volume»

**Этап 3:**

[](http://www.truecryptrussia.ru/images/stories/images_st/3.png)

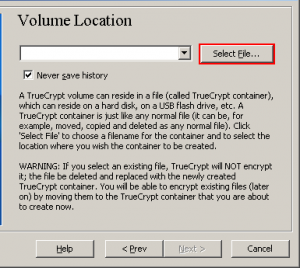
У вас на экране появится окошко для создания TrueCrypt раздела. На этом этапе вы выбираете место для создания раздела. Он может находится непосредственно в файле, пользователи называют его контейнером, в разделе диска (партиции) либо внутри дискового устройства. Приступим к созданию раздела TrueCrypt в файле. Данное изображение имеет установку по умолчанию, поэтому жмем «Next».

**Этап 4:**

**[](http://www.truecryptrussia.ru/images/stories/images_st/4.png)**

Тут вам необходимо определится, какой раздел вы создадите: скрытый или обычный. Руководство покажет создания обычного раздела. Опция уже выставлена. Поэтому нажимаем «Next».

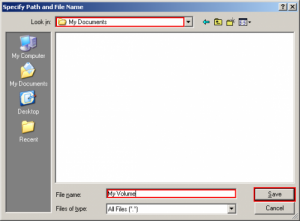
**Этап 5:**

[](http://www.truecryptrussia.ru/images/stories/images_st/5.png)

Этап предполагает указание места расположения раздела TrueCrypt. При этом поведение контейнера идентичное с поведением самого обыкновенного файла.

Жмем Select File. Открывается окошко для выбора файла.

**Этап 6:**

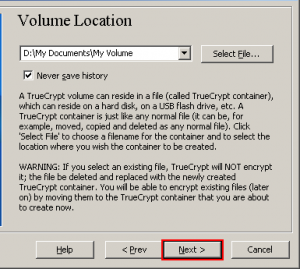
[](http://www.truecryptrussia.ru/images/stories/images_st/6.png)

Это руководство покажет вам как создать раздел TrueCrypt, который будет располагаться в папке D:\My Documents\, а файл будет иметь название My Volume.  Вы в праве придумать любое другое название и место, однако запомните что «My Volume» не будет пока TrueCrypt его не создаст.

ВАЖНО: Запомните, что TrueCrypt не может зашифровать существующие документы, если вы попробуете это сделать, то вы просто на просто потеряете свои данные. Шифровать файлы можно будет немного позже, путем размещения их на шифрованном разделе TrueCrypt.

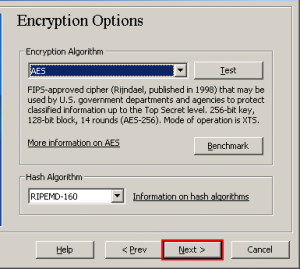
Выбираем место в окне для выбора, где будущий контейнер будет располагаться. Вводим любое имя и жмем «Save». После этого окошко должно исчезнуть.

**Этап 7:**

[](http://www.truecryptrussia.ru/images/stories/images_st/7.png)

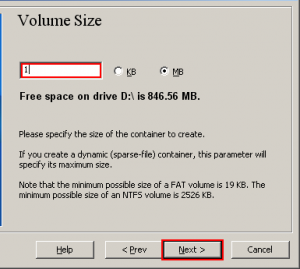
После выбора места жмем «Next».

**Этап 8:**

[](http://www.truecryptrussia.ru/images/stories/images_st/8.png)

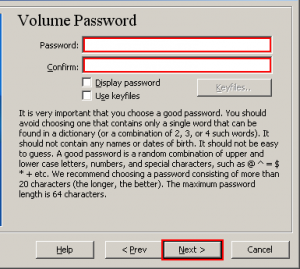
В данном разделе вам предлагается сделатиь выбор алгоритма для шифрования, а так же хеш – алгоритма предназначенного для раздела. Если вы не в состоянии что то выбрать, оставляем всё как есть и жмем  «Next».

**Этап 9:**

[](http://www.truecryptrussia.ru/images/stories/images_st/9.png)

Далее в окне мы указываем предполагаемый размер контейнера TrueCrypt в 1 мегабайт. Можно выбрать и другой размер, а затем нажимаем «Next».

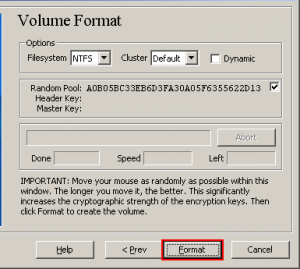
**Этап 10:**

[](http://www.truecryptrussia.ru/images/stories/images_st/10.png)

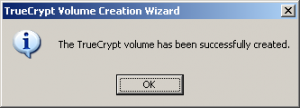
Этот этап самый основной. Тут необходимо определится с паролем для раздела. Стоит ознакомится с информацией, которое дает определение качественного пароля.

После того как вы определитесь введите пароль в первое поле, а затем продублируйте его во второе и нажмите «Next».

**Этап 11:**

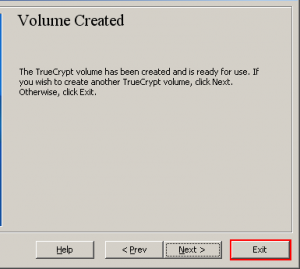
[](http://www.truecryptrussia.ru/images/stories/images_st/11.png)

В открывшемся окне следует двигать мышкой в случайном порядке не менее 30 секунд. Чем дольше будет продолжаться процесс – тем лучше. Это повлияет на увеличение криптографических свойств ключей. Жмем Format. Далее начинается процесс создания раздела. На диске D:\My Documents\ появится файл My Volume. Он будет выступать контейнером в котором будет находится шифрованный раздел TrueCrypt. По окончанию вы увидите окно показанное ниже.

[](http://www.truecryptrussia.ru/images/stories/images_st/11_1.png)

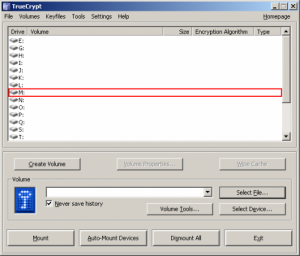
**Жмем «ОК» для его закрепления.**

**Этап 12:**

[](http://www.truecryptrussia.ru/images/stories/images_st/12.png)

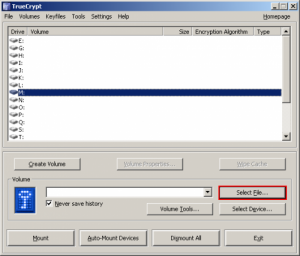
Вы создали раздел TrueCrypt. В окошке TrueCrypt Volume Creation Wizard жмем «Exit». После этого окно пропадает. Возвращаемся к главному окну программы TrueCrypt, если оно исчезло повторяем 1 этап и приступаем к монтировке.

**Этап 13:**

[](http://www.truecryptrussia.ru/images/stories/images_st/13.png)

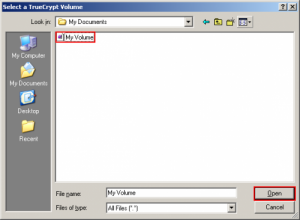
Выбираем одну из букв представленных в списке, это будет буква диска к которому вы примонтируете ваш контейнер.

**Этап 14:**

[](http://www.truecryptrussia.ru/images/stories/images_st/14.png)

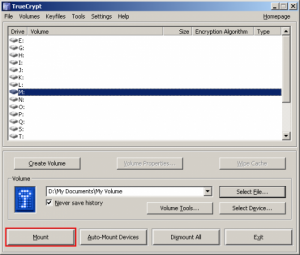
Жмем Select File. При этом должна открыться стандартная версия окна в которой  необходимо выбрать файл.

**Этап 15:**

[](http://www.truecryptrussia.ru/images/stories/images_st/15.png)

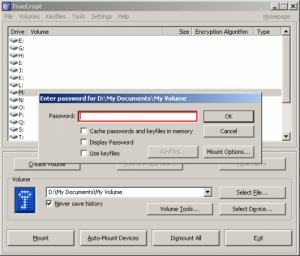
В данном окне находим файл, который вы создали с 6 по 11 этап и выбираем его. Жмем  Open, после этого окно должно исчезнуть.

**Этап 16:**

[](http://www.truecryptrussia.ru/images/stories/images_st/16.png)

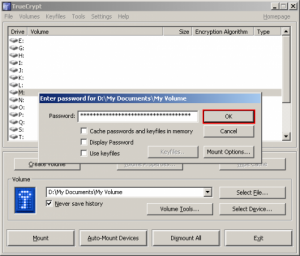
В оставшемся окошке TrueCrypt жмем Mount. Появляется окно, которое запрашивает ваш пароль.

**Этап  17:**

**[](http://www.truecryptrussia.ru/images/stories/images_st/17.png)**

Вводим пароль, который вы установили на 10 этапе в поле выделенное красным.

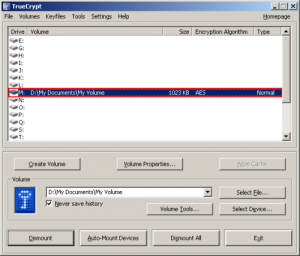
**Этап  18:**

[](http://www.truecryptrussia.ru/images/stories/images_st/18.png)

Жмем «ОК».

Далее TrueCrypt приступает к монтировке раздела. В случае неправильного введения пароля TrueCrypt запросит повторный ввод, если пароль введен верно монтировка раздела пройдет успешно.

Финальный этап:

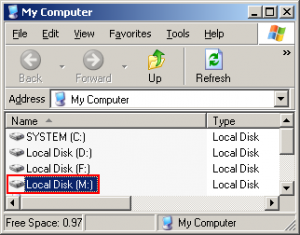
[](http://www.truecryptrussia.ru/images/stories/images_st/18_1.png)

Только что успешно прошла монтировка на один из виртуальных дисков. Диск полностью зашифрован и при этом ничем не отличается от прочих дисков. Вы можете помешать данные на данный диск и при этом они автоматически будут зашифровываться.

Если вы решите открыть файл, который размещен в TrueCrypt, то расшифровка будет производится автоматически через ОЗУ во время воспроизведения.

Важно: Обратите внимание, что при каждом открытие документа у вас будут требовать пароль.

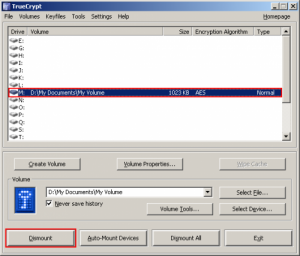
Открыть уже смонтированный раздел можно два раза нажав на него мышкой как указанно на картинке ниже. Открыть его так же можно как и все прочие диски, через вкладку «Мой компьютер».

[](http://www.truecryptrussia.ru/images/stories/images_st/18_2.png)

Вы имеете возможность осуществить копирование как с раздела TrueCrypt, так и на него. Все файлы автоматически расшифровываются или наоборот – зашифровываются.

Обратите внимание, что ни одна расшифрованная информация не подлежит сохранению, а лишь временно сохраняется в ОЗУ. Даже во время открытия файла данные по прежнему зашифрованные. Во время выключения или перезагрузки вашего компьютера, даже несанкционированного, раздел размонтируется и в доступе к файлам будет отказано. Для возобновления доступа необходимо произвести примонтировку описанную в с 13 по 18 этап.

Для закрытия раздела и отказа в доступе к данным вам следует выполнить следующие действия:

[](http://www.truecryptrussia.ru/images/stories/images_st/18_3.png)

Из списка разделов представленных в главном окне необходимо выбрать один раздел и нажать «Dismount».  Для открытия доступа к разделам необходимо повторить с 13 по 18 этап.

**Задание к выполнению**

1. Изучить программы, описанные в теоретическом введении.
2. Установить на рабочий компьютер программу TrueCrypt.
3. Выполнить этапы 1-18, описанные в теоретическом введении.

В электронный конспект поместить копии экрана с пояснениями проведенных действий.