Частное учреждение образования

Колледж бизнеса и права

|  |
| --- |
| УТВЕРЖДАЮ  Заместитель директора  по учебной работе  \_\_\_\_\_\_\_\_\_\_Е.В.Фалей  «\_\_\_»\_\_\_\_\_\_\_\_\_2016 |

|  |  |
| --- | --- |
| Специальность: 2-40 01 01 Программное обеспечение информационных технологий | Дисциплина: «Защита компьютерной информации» |
| Составлена на основании учебной программы, утвержденной директором Колледжа бизнеса и права 02.02.2016, и в соответствии с образовательным стандартом ОС РБ 2-40 01 01 -2014 | |

# Лабораторная работа №14

**Инструкционно-технологическая карта**

Тема: ***«***Создание зашифрованных виртуальных дисков с помощью программного средства TrueCrypt***»***

Цель работы: формирование умений шифрования жесткого диска или его частей и работы с виртуальными образами зашифрованной области.

Время выполнения: 2 часа

СОДЕРЖАНИЕ РАБОТЫ

1. Теоретические сведения для выполнения работы
2. Порядок выполнения работы
3. Контрольные вопросы (вопросы для проверки изученного материала)
4. Литература
5. ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ ДЛЯ ВЫПОЛНЕНИЯ РАБОТЫ

TrueCrypt – это программная система для создания и использования шифруемого «на лету» тома (устройства хранения данных). Шифрование «на лету» означает, что данные автоматически шифруются или расшифровываются прямо во время их считывания или записи без участия пользователя. Данные, сохраненные на зашифрованном томе, невозможно прочесть (расшифровать) без использования правильных пароля/ключевого файла или без правильных ключей шифрования. Шифруется вся файловая система, включая имена папок и файлов, содержимое файлов, пустое пространство, метаданные и т. п.).

Файлы могут копироваться с/на подключенный том TrueCrypt также, как они копируются с/на любой диск (к примеру, с помощью технологии перетаскивания – drag-n-drop). Файлы автоматически расшифровываются «на лету» (в память) во время чтения или копирования с зашифрованного тома TrueCrypt. Верно и обратное – файлы, записываемые или копируемые на том TrueCrypt, шифруются «на лету» в памяти прямо перед записью на диск. Однако это не значит, что весь файл, предназначенный для шифрования/расшифрования, должен целиком попасть в память перед шифрованием/расшифрованием. Для TrueCrypt не требуется дополнительная память.

Например, есть файл .avi, хранящийся на томе TrueCrypt и поэтому целиком зашифрованный. Пользователь, используя правильный пароль (и/или ключевой файл), подключает (открывает) том TrueCrypt. Когда пользователь дважды кликает по иконке видеофайла, операционная система запускает программу, связанную с этим типом файла, как правило, – медиаплеер. Медиаплеер начинает загружать в память небольшую начальную часть видеофайла с зашифрованного TrueCrypt-тома, чтобы проиграть его. В процессе загрузки этой небольшой части TrueCrypt автоматически расшифровывает ее в памяти. Расшифрованная часть видео, хранящаяся теперь в памяти, проигрывается медиаплеером. После проигрывания этой части медиаплеер начнет загружать следующую небольшую часть видеофайла с зашифрованного тома TrueCrypt в память, и процесс повторится. Этот процесс и называется шифрованием/расшифрованием «на лету», и он работает со всеми типами файлов, не только с видео.

TrueCrypt никогда не сохраняет никакие данные в незашифрованном виде на диск, он их временно хранит в памяти. Даже когда том подключен, данные на нем хранятся в зашифрованном виде. Когда вы перезапускаете Windows или выключаете компьютер, том отключается, и файлы, хранимые на нем, становятся недоступными, оставаясь зашифрованными. То же самое происходит в случае непредвиденного отключения электроэнергии (без правильного завершения работы системы). Чтобы получить к ним доступ снова, вы должны подключить том, используя правильные пароль и/или ключевой файл.

Разработка TrueCrypt закончена в 2014 году. На официальном сайте программы опубликовано заявление, что система не является безопасной и может содержать уязвимости. Финальный релиз TrueCrypt 7.2 можно использовать только как промежуточное звено при миграции на другие системы.

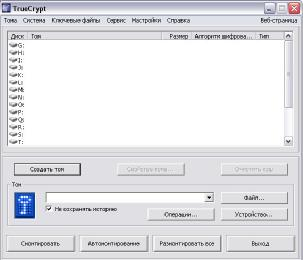
Шифрование и использование несистемного раздела диска

*Шаг 1*

Запустите TrueCrypt, дважды щелкнув по значку TrueCrypt.exe, или вызовите его из меню Пуск.

*Шаг 2*

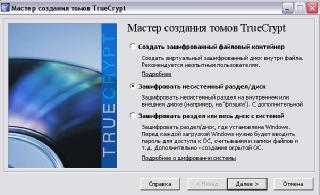
На экране появится главное окно TrueCrypt (рис. 12.1). Нажмите Создать том.

**

*Шаг* 3

На экране должно появиться окно Мастера создания раздела TrueCrypt.

Выберите место, где нужно создать раздел TrueCrypt. Раздел TrueCrypt может быть размещен в файле, который также называют контейнером, в разделе диска или на дисковом устройстве. Зашифруйте запоминающее USB-устройство, выбрав вторую опцию Зашифровать несистемный раздел/диск и кликнув кнопку Далее.



*Шаг 4*

На данном этапе предстоит выбрать, каким будет наш тип тома.

Возможны два варианта:

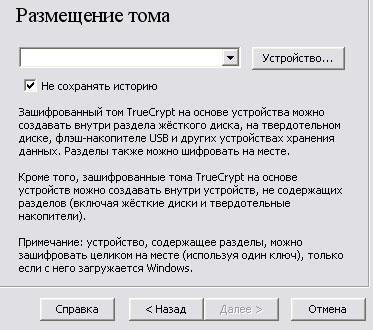
1. обычный том TrueCrypt;
2. скрытый том TrueCrypt.

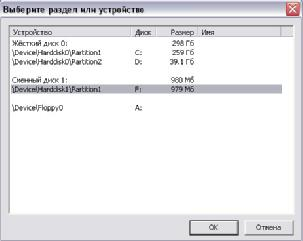
Выберите опцию Обычный том TrueCrypt.

П р и м е ч а н и е. Опцию Скрытый том TrueCrypt рассмотрим в шаге 12.

*Шаг 5*

Выберите устройство, которое будет зашифровано.

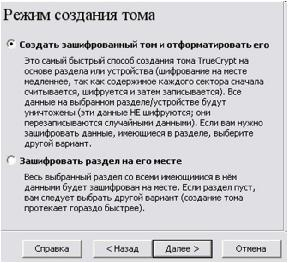


В данном случае выбран диск F. Затем перейдите к следующему шагу, нажав кнопку Далее.

*Шаг 6*

На данном этапе выберите одну из двух опций (рис. 12.6):

1. создать зашифрованный том и отформатировать его;
2. зашифровать раздел на его месте.



Если на устройстве, выбранном в шаге 5, имеется важная информация, которую вы хотите сохранить и зашифровать, то следует выбрать пункт Зашифровать раздел на его месте. Если на выбранном устройстве нет информации либо она отсутствует, выберите пункт Создать зашифрованный том и отформатировать его. В этом случае все данные, хранимые на выбранном устройстве, будут утеряны. После того, как вы выбрали опцию, кликните кнопку Далее.

*Шаг 7*

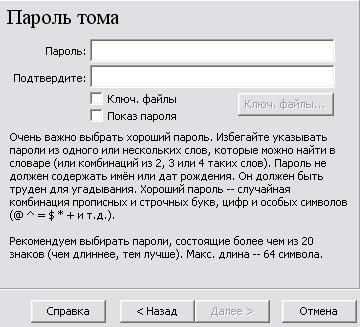
Здесь вы можете выбрать алгоритм шифрования и хэш-алгоритм для раздела. Если вы не уверены в том, что выбрать, то можете использовать настройки по умолчанию и нажать Далее.

*Шаг 8*

На восьмом шаге убедитесь в том, что вы выбрали именно то устройство, которое хотели, и нажмите кнопку Далее.

Шаг 9

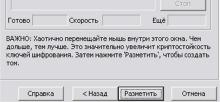
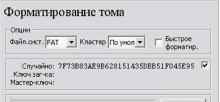
Это один из наиболее важных шагов. Здесь вы должны выбрать хороший пароль для тома. Внимательно прочитайте информацию, отображаемую в окне Мастера. После выбора, введите его в первое поле для ввода. Затем повторите его во втором поле и нажмите Далее.



П р и м е ч а н и е. Кнопка Далее будет неактивна пока пароли в обоих полях не будут совпадать.

*Шаг 10*

В окне Volume Creation Wizard как минимум 30 секунд случайно двигайте мышкой в разных направлениях, чем дольше вы будете ею двигать, тем значительно увеличите криптографическую силу ключей шифрования (которые, в свою очередь, усилят безопасность). Нажмите Разметить.



Согласитесь с форматированием выбранного раздела и ждите окончания процесса.Внимательно прочитайте и нажмите OK.

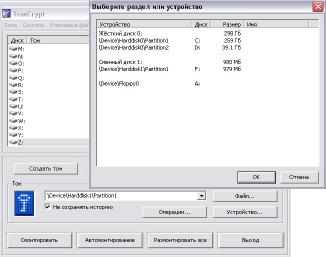
Итак, том создан.

После того, как вы кликните ОК, TrueCrypt предложит вам создать еще один том (кнопка Далее). Если вы хотите прекратить работу Мастера создания томов, нажмите кнопку Выход.

*Шаг 11*

Теперь нужно научиться им пользоваться. При обычной попытке доступа к зашифрованному устройству (Мой компьютер – Зашифрованное устройство), Windows предложит его отформатировать (после процесса форматирования устройство окажется

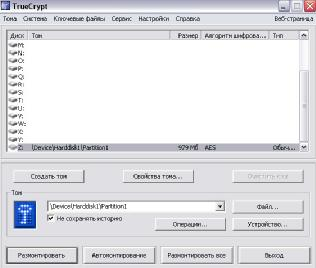
пустым и незашифрованным). Для доступа к созданному тому откройте TrueCrypt и на главной форме выберите устройство, которое шифровали (на нашем примере это диск F).



Далее выберите незанятую букву диска (например, Z) и нажмите кнопку Смонтировать.Введите пароль, который был придуман в шаге 9 и нажмите OK.

Если пароль неверный (например, вы его неправильно ввели), то TrueCrypt сообщит об этом; введите пароль заново и нажмите ОК. Если пароль правильный, то раздел будет смонтирован.

Зашифрованное устройство успешно смонтировано как виртуальный диск Z.



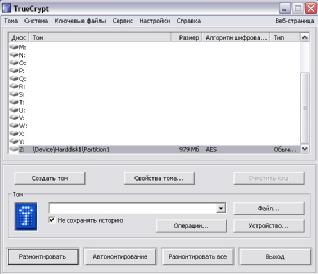
Виртуальный диск полностью зашифрован (включая имена файлов, таблицы размещения, свободное место и т. д.). Вы можете сохранять (копировать, перемещать и т. д.) файлы на этот виртуальный диск, и они будут зашифрованы «на лету» во время записи.Если откроете файл, хранящийся на разделе TrueCrypt, например, в медиаплеере, то он будет автоматически расшифрован «на лету» в ОЗУ (память) во время чтения.

П р и м е ч а н и е. Когда вы открываете файл, хранящийся на разделе TrueCrypt (или когда записываете/копируете файл с/на TrueCrypt раздел), запроса ввести пароль не будет. Ввести пароль потребуется только тогда, когда монтируете раздел.

Вы можете открыть смонтированный раздел, например, дважды кликнув на помеченной прямоугольником надписи, как ниже показано на снимке экрана (рис. 12.13).

Вы также можете найти и открыть смонтированный раздел, открыв Мой компьютер и дважды щелкнув кнопкой мыши по значку диска (в нашем случае это диск Z).

Выберите раздел из списка смонтированных разделов в главном окне TrueCrypt и затем нажмите Размонтировать.



Расшифровка устройства

Если потребуется обратно расшифровать устройство, выполните следующие действия:

1. проверьте, что зашифрованное устройство размонтировано;
2. зайдите в Мой компьютер;
3. найдите в списке дисков зашифрованный (тот, который хотите расшифровать);
4. кликните правой кнопкой по выбранному диску;
5. выберите из списка контекстного меню пункт Форматировать.

По окончании форматирования диск будет расшифрован и доступен так же, как и раньше.

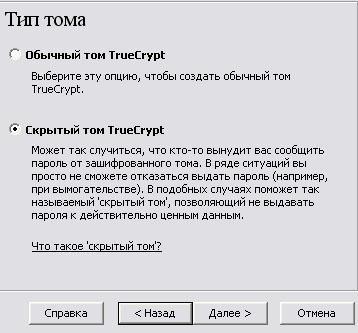
*Шаг 12*

Для создания скрытого тома повторите шаги один–три и на

четвертом выберите пункт Скрытый том TrueCrypt (рис. 12.15).

Что такое «скрытый том» можно узнать, кликнув по соответствующей ссылке. Представим общие сведения:

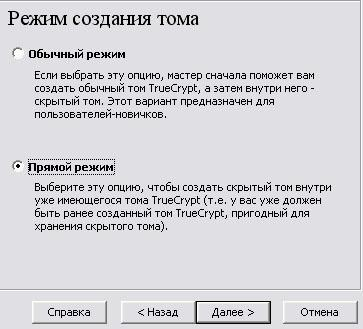
1. скрытый том создается внутри уже существующего обычного тома;
2. доступ к скрытому тому осуществляется так же, как и к обычному, только при монтировке обычного тома нужно ввести пароль скрытого;
3. о существовании скрытого тома невозможно узнать, что дает дополнительную защиту информации, хранимой на этом томе.

**

*Шаг 13*

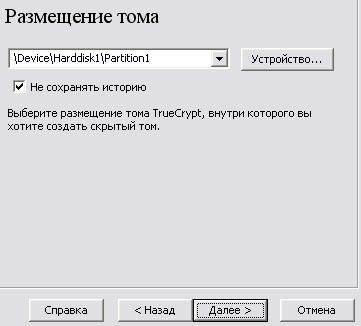
Мастер создания томов предлагает выбрать режим создания скрытого тома. Возможны два варианта:

* обычный режим (создание обычного тома, после чего появится возможность создания внутри него скрытого тома);
* прямой режим (создание скрытого тома на уже существующем обычном томе).
* Выберите Прямой режим, так как обычный том уже был создан.



*Шаг 14*

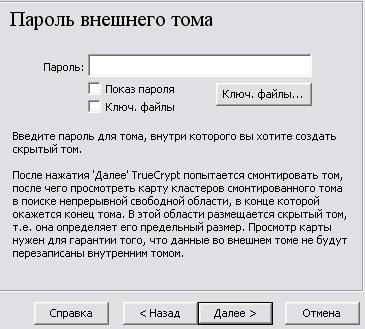
Выберите устройство (диск) или каталог, в котором нужно создать скрытый том.

**

*Так же можно выбрать пункт сохранения истории происходящих действий, но не рекомендуется это делать, чтобы злоумышленник не добрался до скрытой информации данного файла*.*Шаг 15*

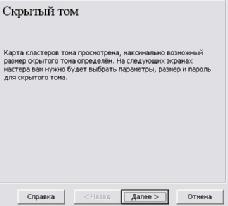
На этом шаге введите пароль, который применяется в обычном томе (этот пароль был использован в шаге 9).

После ввода пароля кликните Далее.

**

*Шаг 16*

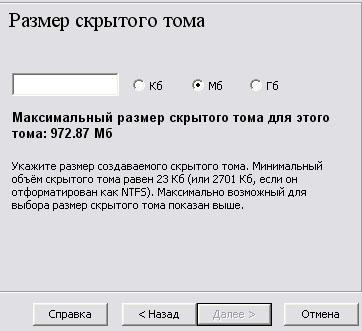
Внимательно прочитайте уведомление.

*Шаг 17*

Данный шаг аналогичен шагу 7.

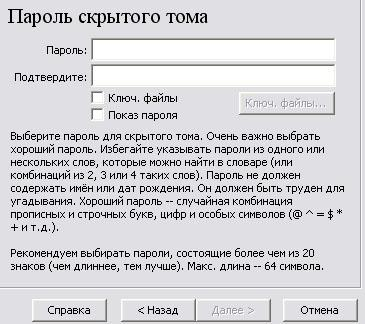
*Шаг 18*

На этом этапе выберите размер скрытого тома.

**

*П р и м е ч а н и е. Обратите внимание на максимально возможный размер*.*Шаг 19*

Этот шаг аналогичен шагу 9, но *пароль для скрытого тома должен отличаться от пароля внешнего*.

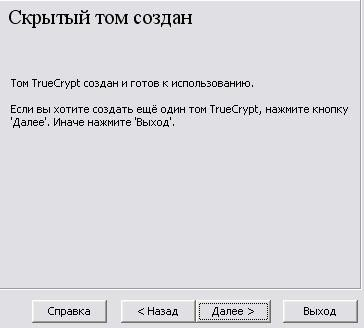


*Шаг 20*

Данный шаг аналогичен шагу 10.

Прочитайте уведомление.

Скрытый том готов. Для создания еще одного тома нажмите кнопку Далее. Для прекращения работы Мастера создания томов кликните Выход.

*Шаг 21*

Работа со скрытым томом аналогична работе с внешним. Отличие лишь в том, что для доступа к скрытому тому необходимо вводить пароль из шага 19, а не из шага 9.

1. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ.
2. Зашифруйте несистемный диск.
3. Зашифруйте часть диска.
4. Зашифруйте отдельные файлы разного формата.
5. Зашифруйте флешку.
6. Создайте виртуальные образы зашифрованных объектов и проверьте их работу.
7. Оформите отчет по проделанной работе.
8. В конце отчета ответьте на контрольные вопросы.
9. КОНТРОЛЬНЫЕ ВОПРОСЫ:
10. Что значит термин шифрование «на лету»?
11. Какие есть режимы работы программы TrueCrypt?
12. Как удалить зашифрованный раздел?
13. ЛИТЕРАТУРА
14. Тетерукова Н. А., Апанасевич С. А. Защита компьютерной информации (лабораторный практикум) - МГВРК, 2013.

Преподаватель А.Г. Тараренко

Рассмотрено на заседании цикловой комиссии

Программного обеспечения информационных технологий № 10

Протокол № \_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_ 2016

Председатель ЦК \_\_\_\_\_\_ Т.Г. Багласова