Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Основы Защиты Информации**

**Практическое занятие №6**

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

Студент: Городилов М. П.

ФИТ 2 курс 4 группа

Преподаватель: Буснюк Н. Н.

Минск 2020

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

**Выполнение**

**Криптография** — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства.

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.

В данном практическом занятии демонстрируется работа с бесплатной утилитой TrueCrypt, которая предназначена для создания защищенных виртуальных дисков, шифрования системных разделов.

**Порядок работы с программой TrueCrypt.**

1. После установки программы, запускаем её и нажимаем на кнопку Create Volume.

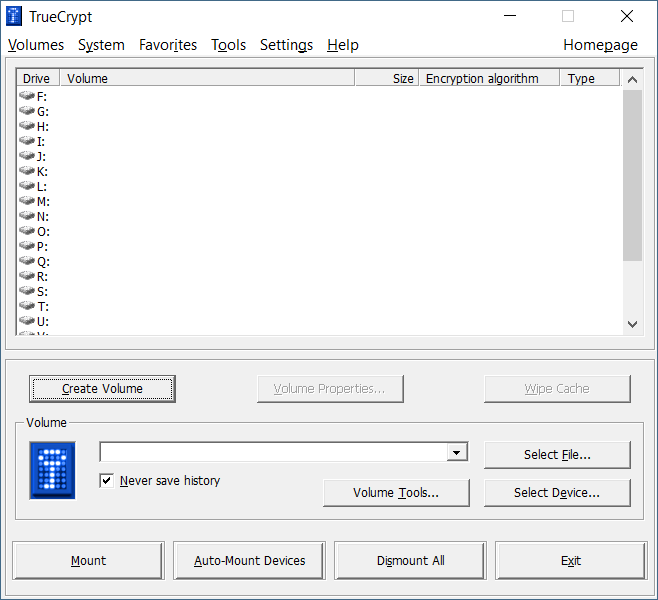


Рисунок 6.1 − Окно TrueCrypt

2. Выбираем место для создания раздела (может быть в файле, в разделе диска либо внутри дискового устройства).

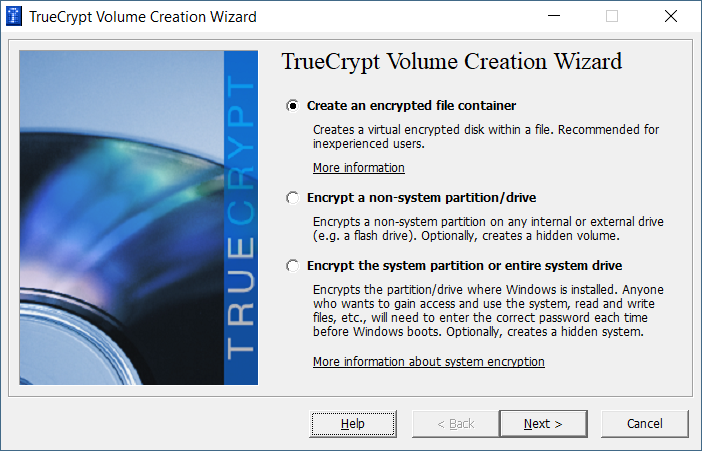


Рисунок 6.2 − Создание раздела

3. Определение типа раздела: обычный или скрытый. Выбираем обычный.

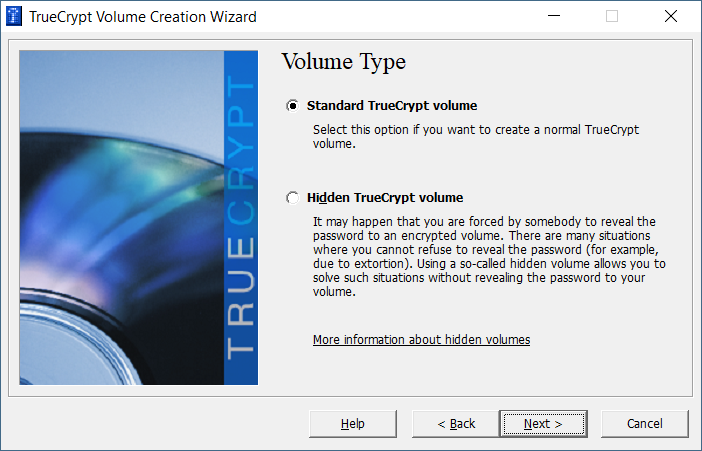


Рисунок 6.3 − Определение типа раздела

4. На следующем этапе выбираем место для создания раздела.

5. Далее выбираем алгоритм для шифрования, а также хеш алгоритма, предназначенного для раздела.

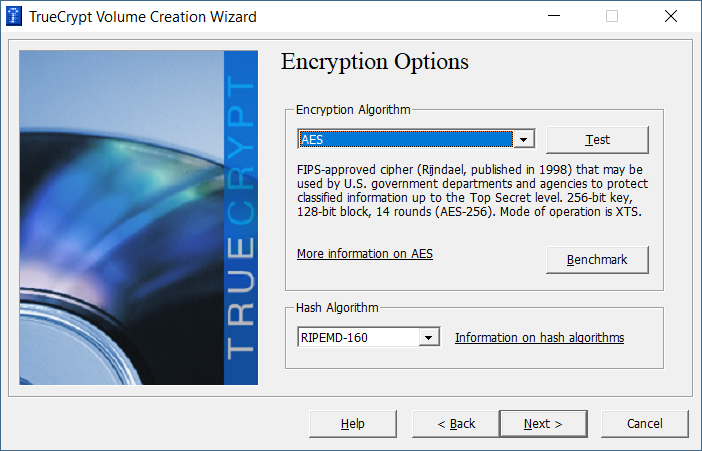


Рисунок 6.5 − Выбор алгоритма шифрования

6. Указываем предполагаемы размер контейнера в 10 мегабайт. Нажимаем «Next».

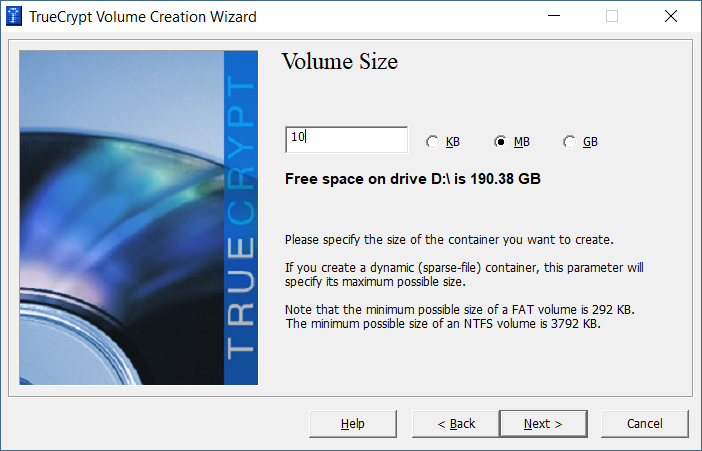


Рисунок 6.6 − Определение размера контейнера

7. Ввод пароля и его подтверждение. Игнорируем советы по составлению пароля, так как в дальнейшем этот раздел всё равно будет удалён.

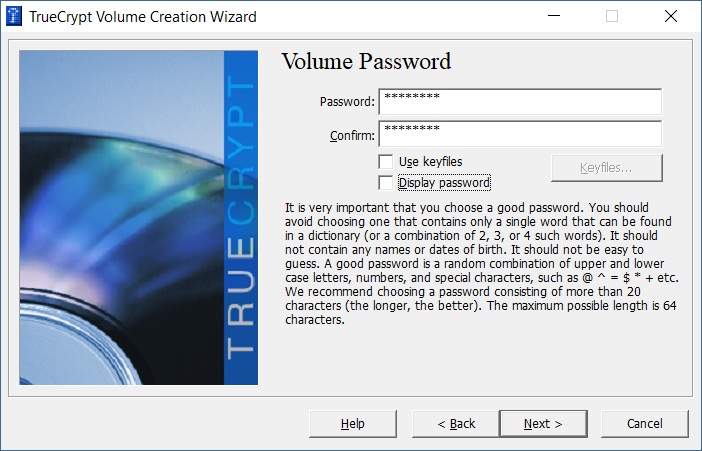


Рисунок 6.7 − Ввод пароля

8. Задаём тип файловой системы для нашего диска. Если планируется создавать файлы размером больше 2Gb рекомендуется выбирать NTFS. В противном случае можно обойтись и FAT. Жмём копку «Format» и по окончании процесса создания файла на месте этой кнопки появится «Next». Переходим к следующему шагу.

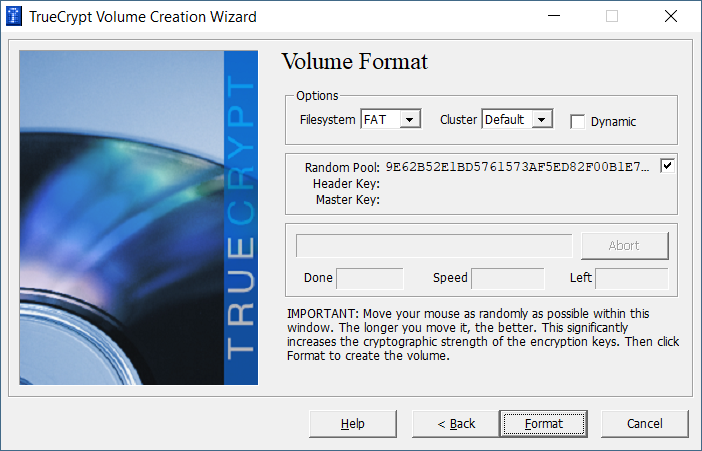


Рисунок 6.8 − Генерация ключа

9. Жмем «Exit». Окно пропадает. Возвращаемся к главному окну.

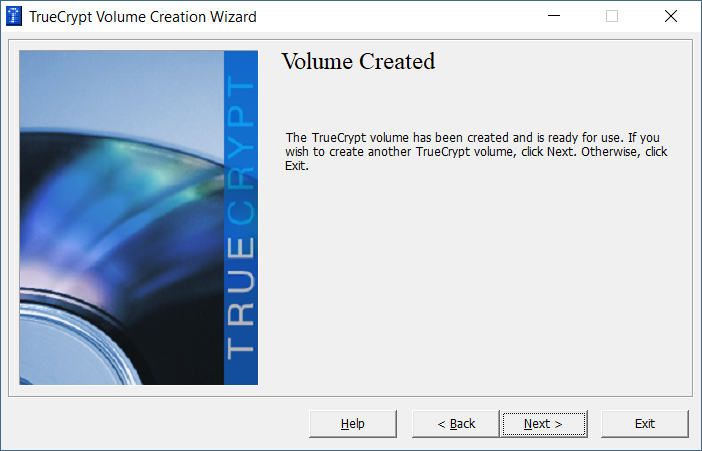


Рисунок 6.9 − Завершение создания раздела

10. Выбираем букву, которая будет являться названием диска, к которому монтируется контейнер.

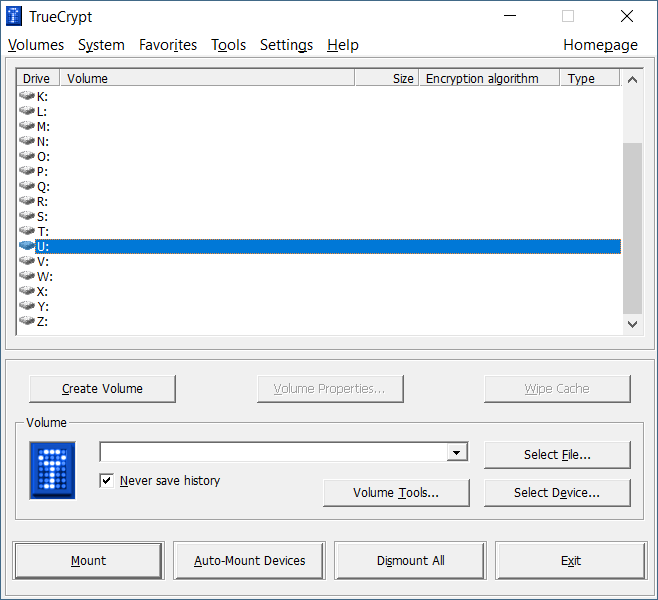


Рисунок 6.10 − Окно TrueCrypt

11. Жмем Select File, и видим открывшееся окно, в котором выбираем файл. Выбираем созданный ранее раздел.

12. В первоначальном окне жмем Mount. Появляется окно, запрашивающее пароль.

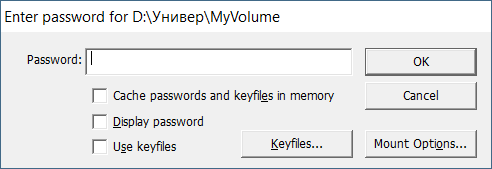


Рисунок 6.12 − Запрос пароля

13. Происходит монтировка на выбранный диск.

14. Зайдя в Мой компьютер, можно увидеть тот самый диск, созданный ранее.

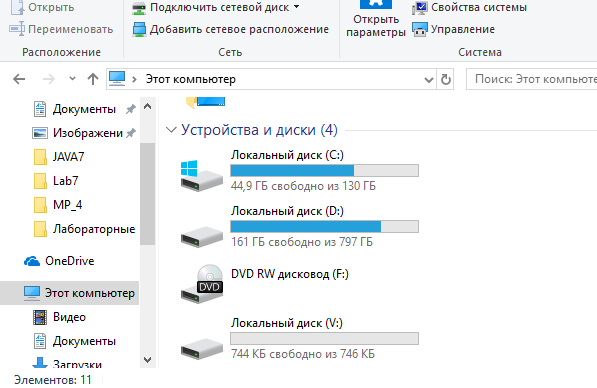


Рисунок 6.14 − Мой компьютер

13. Для закрытия и отказе в доступе к данным следует выбрать этот раздел и нажать кнопку Dismount.

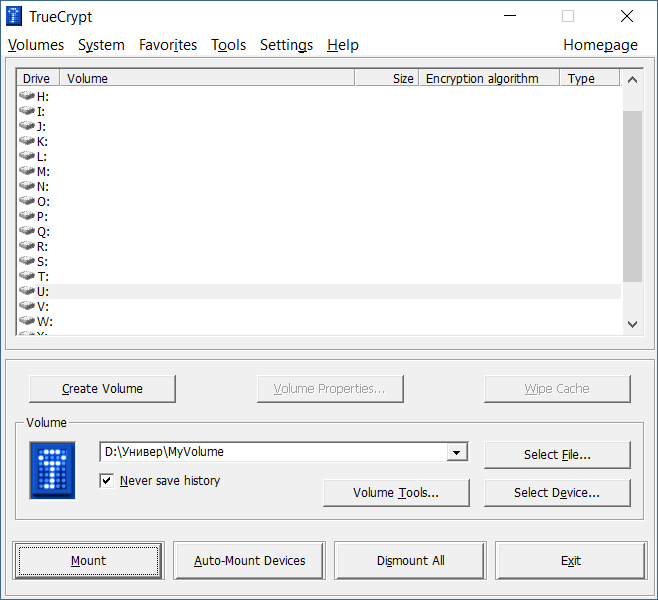


Рисунок 6.15 − Окно TrueCrypt

**Вывод**

В ходе работы в программе TrueCrypt создали зашифрованный том. В настоящее время существует множество программных обеспечений для криптографической защиты информации. В том числе платные и бесплатные, широко известные и не очень. Например, SecretDisk или InfoWatchCryptoStorage и многие другие. Правда, к использованию свободного ПО для защиты информации существует двоякое отношение. Дело в том, что многие утилиты пишутся программистами-одиночками или небольшими группами. 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, с которой мы познакомились.