Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Студент: Костюкова А.О.

ФИТ 2 курс 4 группа

Преподаватель: Буснюк Н. Н.

Минск 2020

**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.

**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.

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.

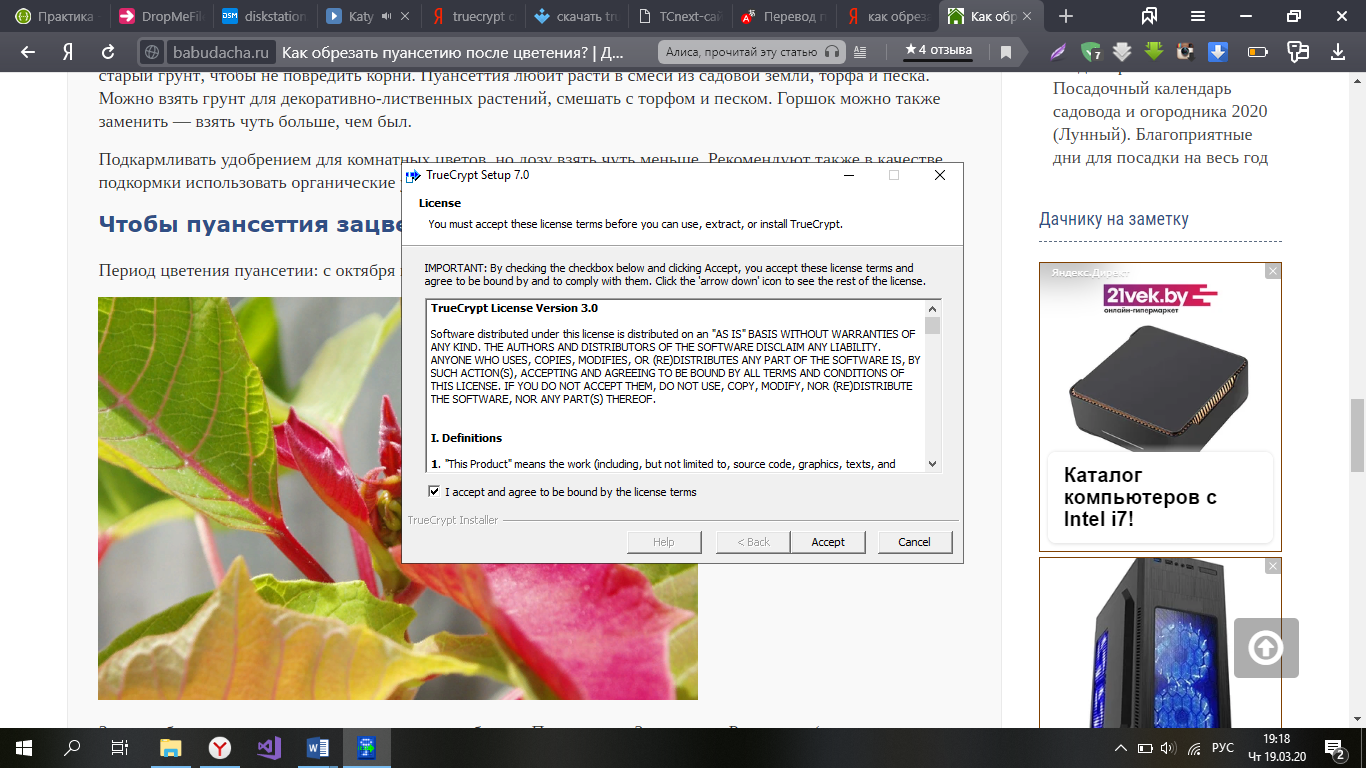
В рассматриваемом продукте реализовано несколько алгоритмов шифрования: AES, Serpent и Twofish. Владелец информации может сам выбрать, какой из них он хочет использовать в данный момент. Аутентификации пользователей в TrueCrypt может производиться с помощью обычных паролей. Однако есть и другой вариант – 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.

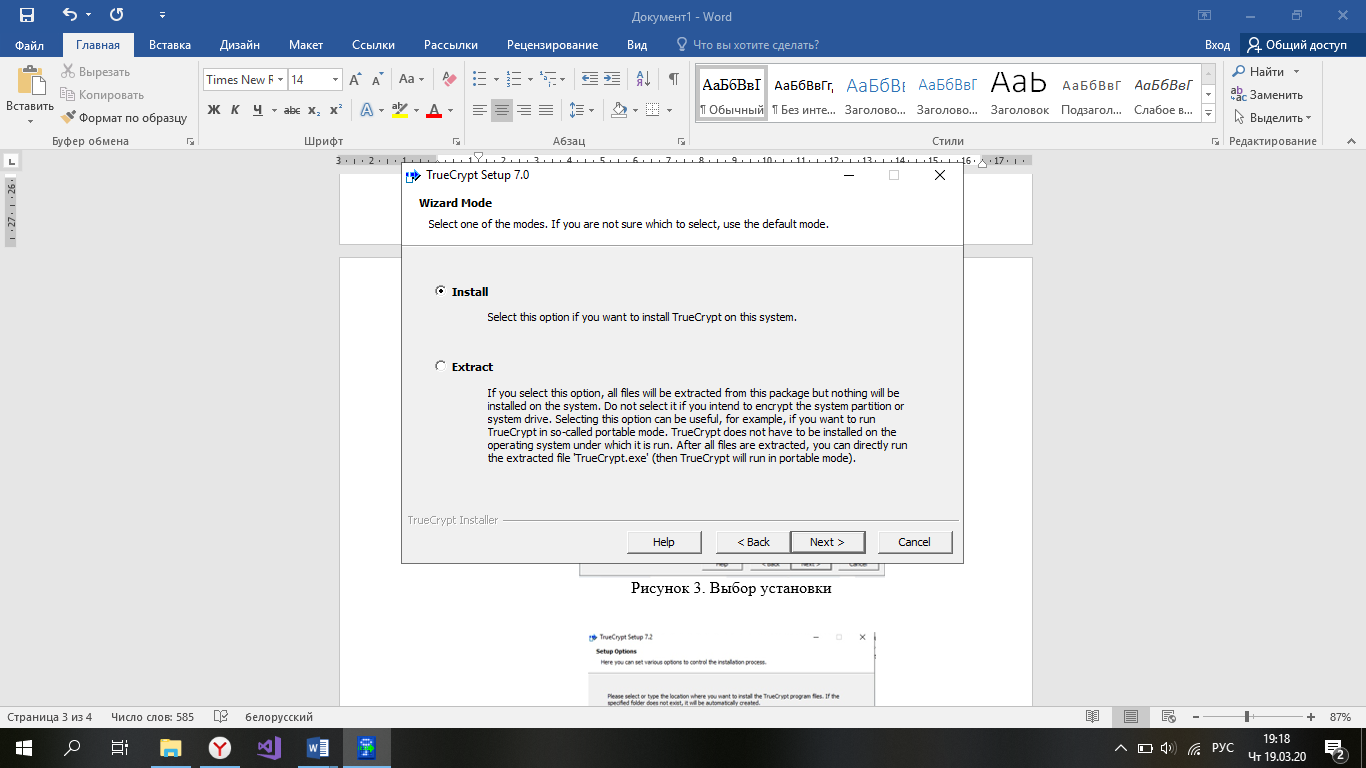
Из дополнительных функций рассматриваемой программы можно отметить возможность создания скрытых томов внутри основных. Она используется для сокрытия конфиденциальных данных при открытии диска под принуждением. Также в TrueCrypt реализована система резервного копирования заголовков томов для их восстановлении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

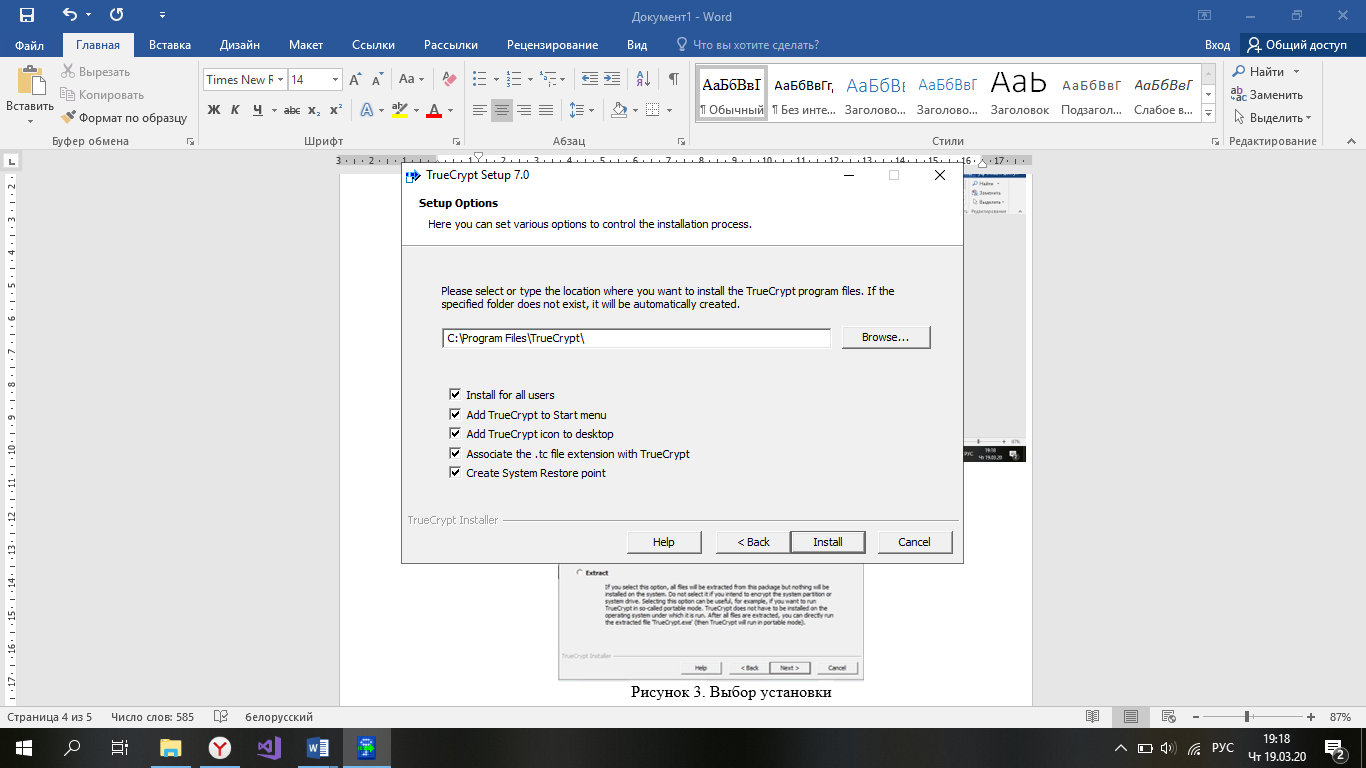
**Порядок работы с программой TrueCrypt**

**Этап 1:**

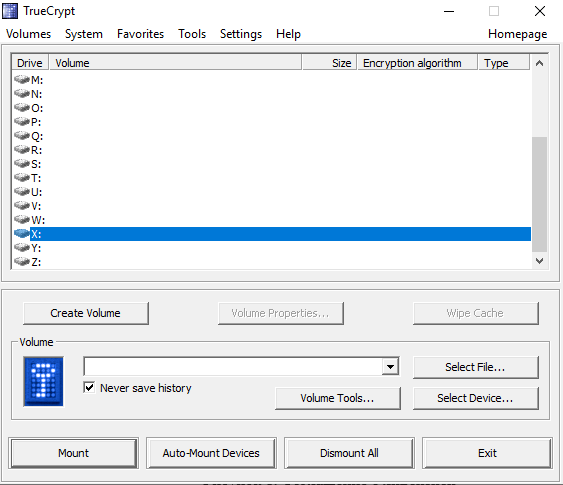
Установить и запустить





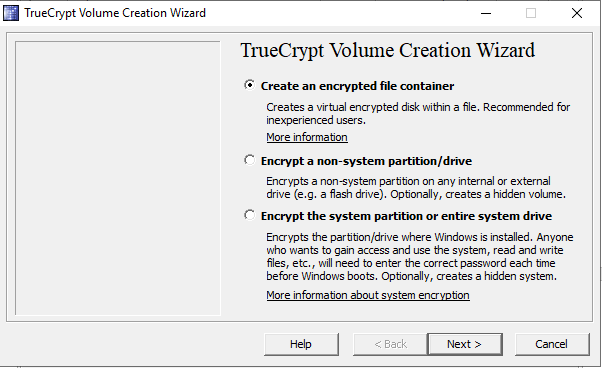


**Этап  2:**



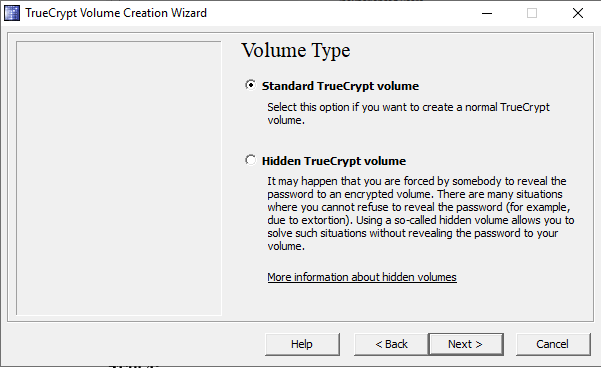
Откроется окошко TrueCrypt. Далее нажимайте на кнопку «Создать том»

**Этап 3:**

****

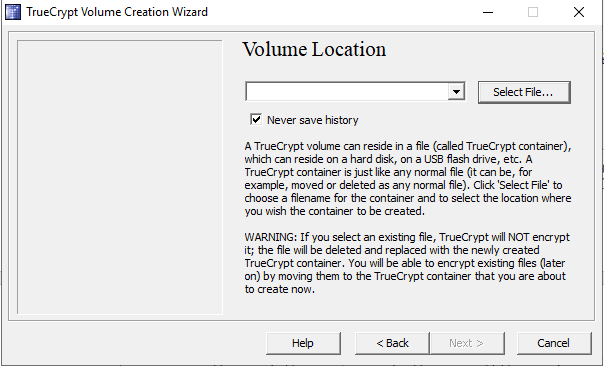
У вас на экране появится окошко для создания TrueCrypt раздела. На этом этапе вы выбираете место для создания раздела. Он может находится непосредственно в файле, в разделе диска либо внутри дискового устройства. Приступим к созданию раздела TrueCrypt в файле. Данное изображение имеет установку по умолчанию,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

**Этап 4:**

****

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

**Этап 5:**

****

Этап предполагает указание места расположения раздела TrueCrypt. При этом поведение контейнера идентичное с поведением самого обыкновенного файла. Жмем Файл. Открывается окошко для выбора файла.

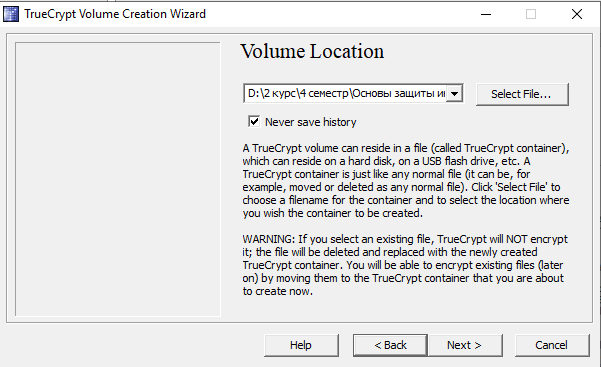
**Этап 6:**

Это руководство покажет вам как создать раздел TrueCrypt, который будет располагаться в папке D:\2 курс\4 семестр\Основы защиты информации, а файл будет иметь название ForLab6.  Вы в праве придумать любое другое название и место, однако запомните, что «ForLab6» 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.

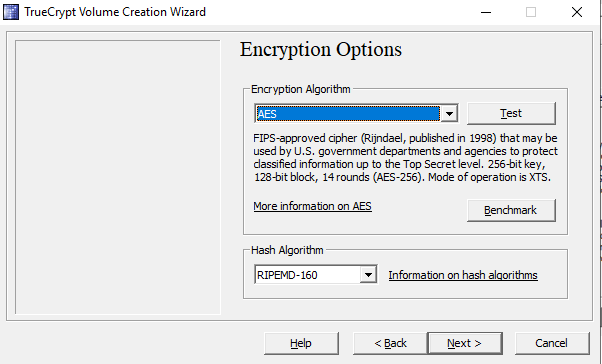
Выбираем место в окне для выбора, где будущий контейнер будет располагаться. Вводим любое имя и жмем «Save». После этого окошко должно исчезнуть.

**Этап 7:**



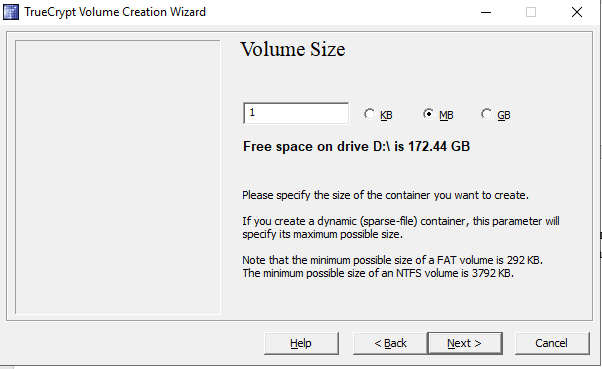
После выбора места нажмем «Далее».

**Этап 8:**

****

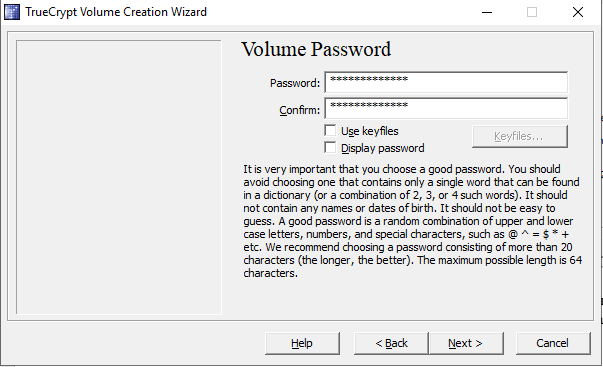
В данном разделе вам предлагается сделать выбор алгоритма для шифрования, а также хеш – алгоритма, предназначенного для раздела. Если вы не в состоянии что-то выбрать, оставляем всё как есть и жмем «Далее».

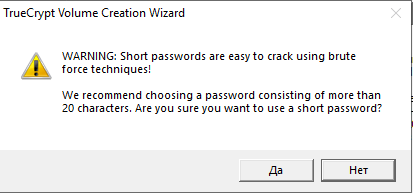
**Этап 9:**

****

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

**Этап 10:**

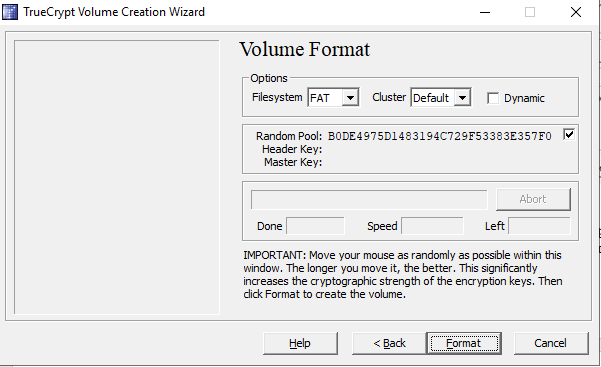
****

****

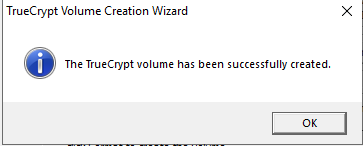
Этот этап самый основной. Тут необходимо определится с паролем для раздела. Стоит ознакомится с информацией, которое дает определение качественного пароля.

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

**Этап 11:**



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:\2 курс\4 семестр\Основы защиты информации\ появится файл ForLab6. Он будет выступать контейнером, в котором будет находится шифрованный раздел TrueCrypt. По окончанию вы увидите окно показанное ниже.



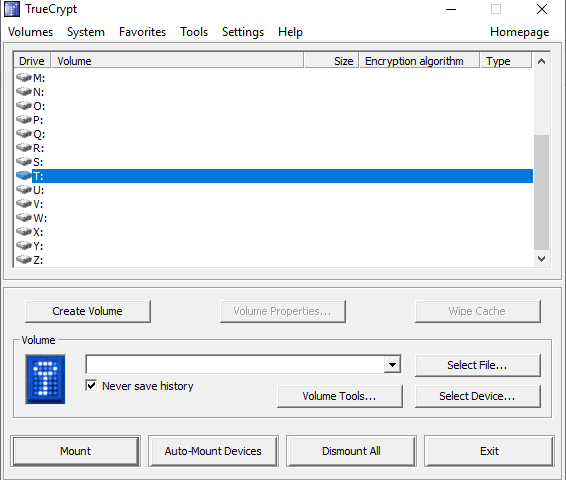
Жмем «ОК» для его закрепления.

**Этап 12:**

****

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:**



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

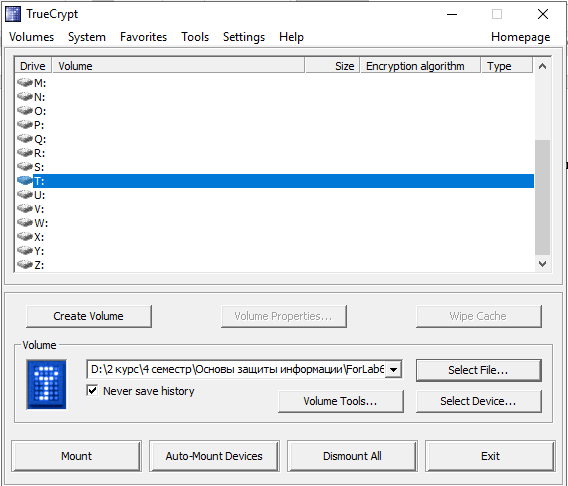
**Этап 14:**

Жмем «Файл…». При этом должна открыться стандартная версия окна в которой необходимо выбрать файл.

**Этап 15:**

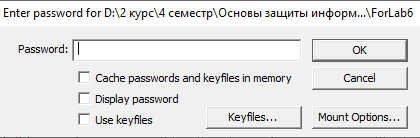
В данном окне находим файл, который вы создали с 6 по 11 этап и выбираем его. Жмем «Открыть», после этого окно должно исчезнуть.

**Этап 16:**

****

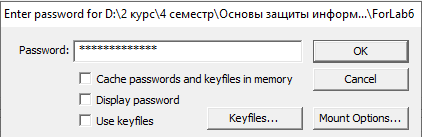
В оставшемся окошке TrueCrypt жмем «Смонтировать». Появляется окно, которое запрашивает ваш пароль.

**Этап 17:**



Вводим пароль, который вы установили на 10 этапе в поле «Пароль:».

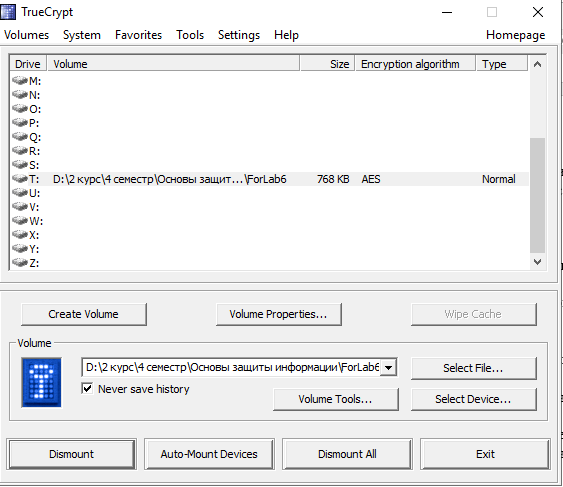
**Этап 18:**

****

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:

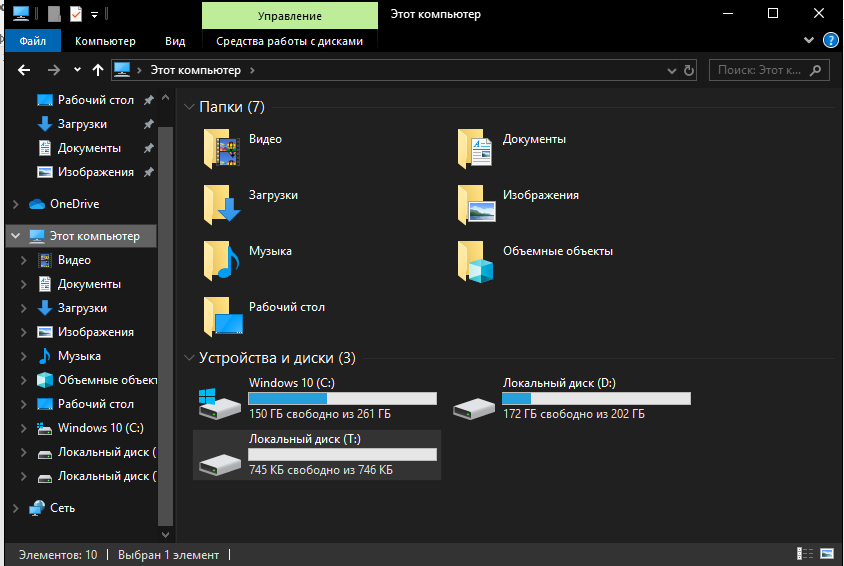


Только что успешно прошла монтировка на один из виртуальных дисков. Диск полностью зашифрован и при этом ничем не отличается от прочих дисков. Вы можете помешать данные на данный диск и при этом они автоматически будут зашифровываться.

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

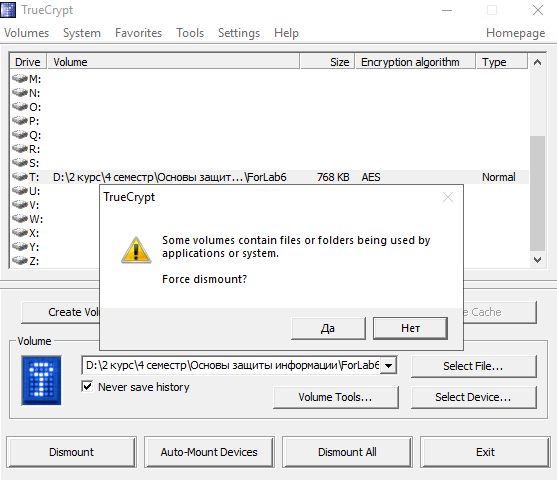
Важно: Обратите внимание, что при каждом открытие документа у вас будут требовать пароль.

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 с 13 по 18 этап.

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



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

**Вывод:**

Получила навыки работы с компьютерными программами для криптографической защиты информации при передаче и хранении.