МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования

«Белорусский государственный технологический университет»

Отчет по дисциплине «Основы защиты информации»

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

Сдала: Керезь Екатерина, 2 курс, 4 группа

Принял: Буснюк Николай Николаевич

г. Минск, 2020

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.

**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.

**Порядок выполнения**

Этап 1:

Установили и запустили.

Этап 2:

Открыли окошко TrueCrypt (рисунок 6.1).

Рисунок 6.1 – Окно программы TrueCrypt

Далее нажали на кнопку «Create Volume» (Рисунок 6.2).

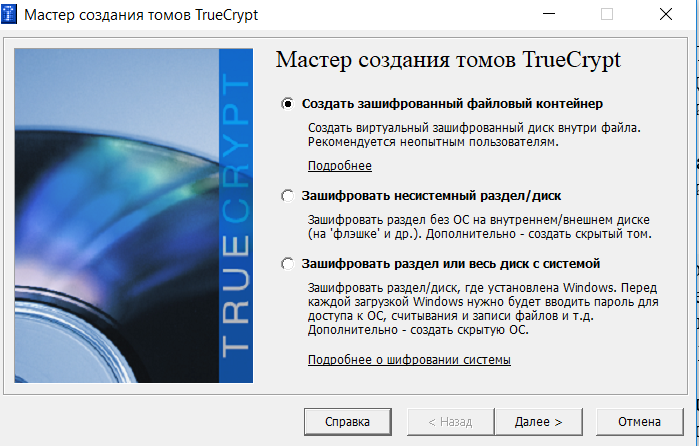


Рисунок 6.2 – Мастер создания томов

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».

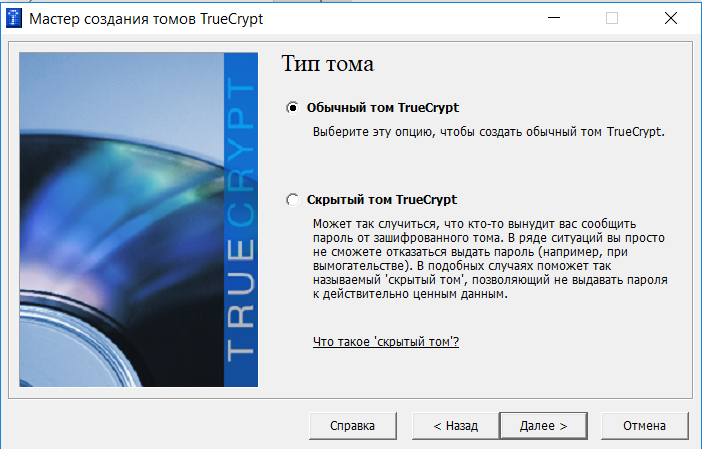


Рисунок 6.3 – Тип тома

Тут (Рисунок 6.3) вам необходимо определится, какой раздел вы создадите: скрытый или обычный. Руководство покажет создания обычного раздела. Опция уже выставлена. Поэтому нажимаем «Next».

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. (Рисунок 6.4)

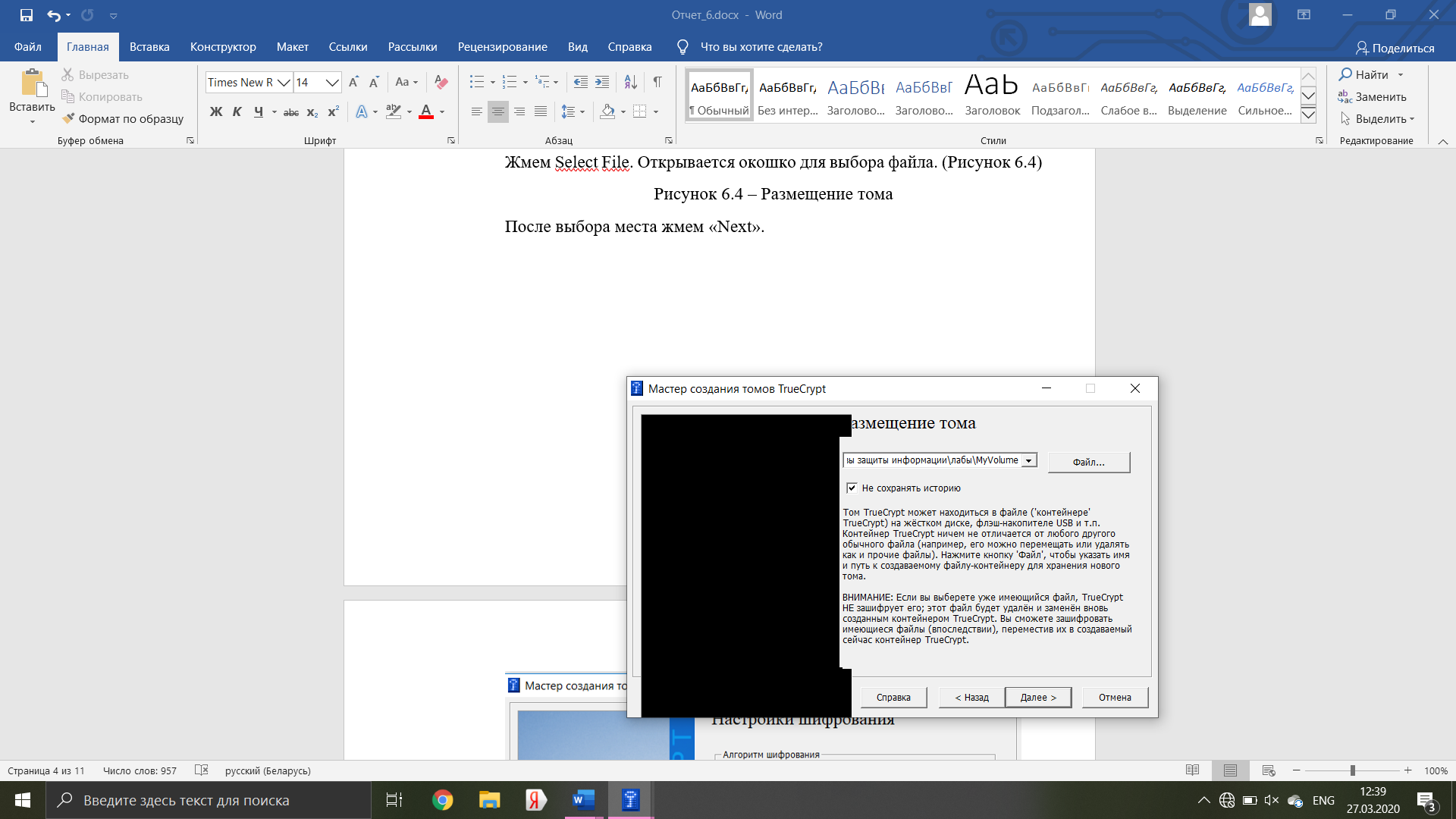


Рисунок 6.4 – Размещение тома

После выбора места жмем «Next».

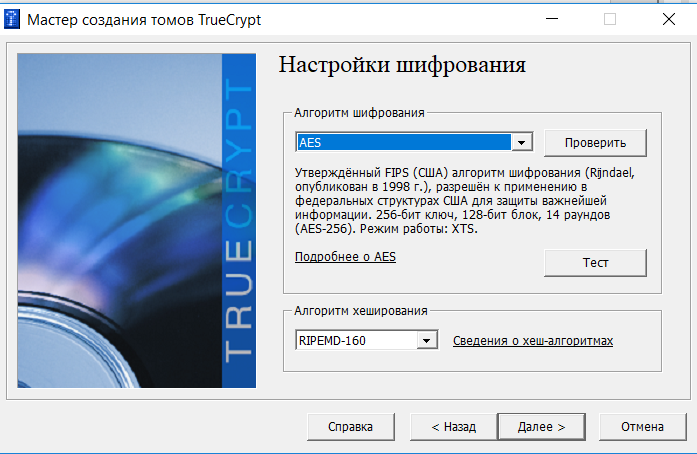


Рисунок 6.5 – Настройки шифрования

В данном разделе (Рисунок 6.5) 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 «Next».

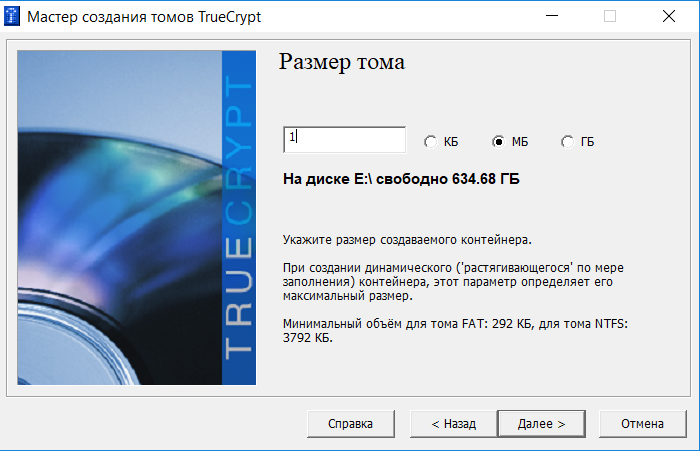
Далее в окне (Рисунок 6.6) мы указываем предполагаемый размер контейнера TrueCrypt в 1 мегабайт. Можно выбрать и другой размер, а затем нажимаем «Next».

Рисунок 6.6 – Размер тома

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». (Рисунок 6.7)

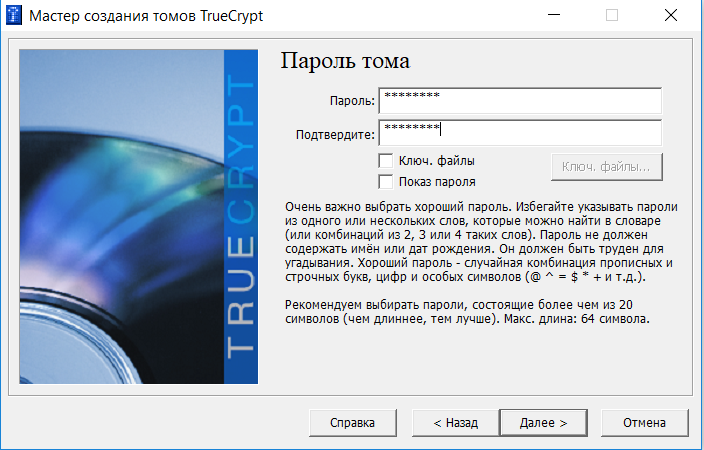


Рисунок 6.7 – Пароль тома

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:\4 СЕМЕСТР\Основы защиты информации\лабы появится файл MyVolume делал. Он будет выступать контейнером, в котором будет находится шифрованный раздел TrueCrypt. По окончанию вы увидите окно, показанное ниже.

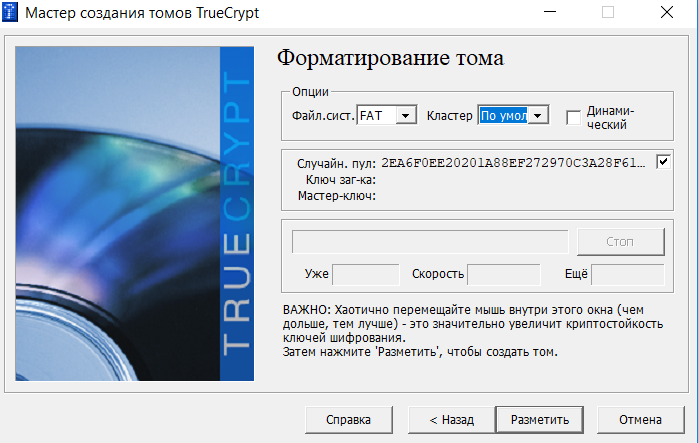


Рисунок 6.8 – Форматирование тома

**Жмем «ОК» для его закрепления. (Рисунок 6.9)**

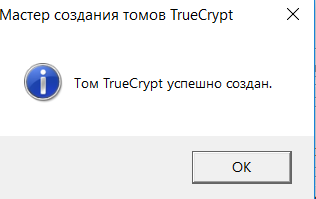


Рисунок 6.9 – Кнопка подтверждения

Мы создали раздел TrueCrypt. В окошке TrueCrypt Volume Creation Wizard жмем «Exit». (Рисунок 6.10) После этого окно пропадает. Возвращаемся к главному окну программы TrueCrypt, если оно исчезло повторяем 1 этап и приступаем к монтировке.

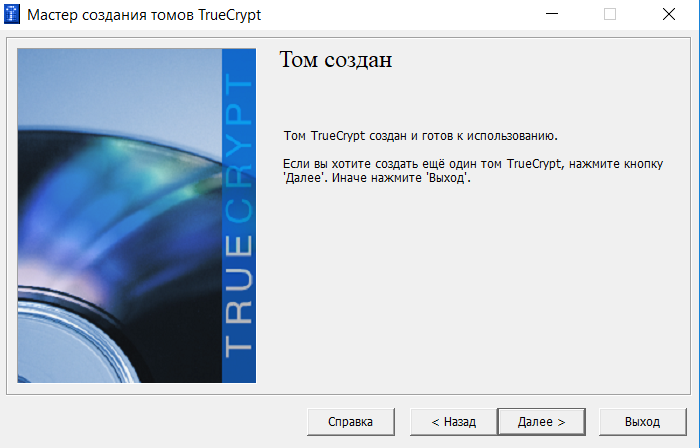


Рисунок 6.10 – Том создан

Выбираем одну из букв, представленных в списке, это будет буква диска, к которому вы примонтируете ваш контейнер. (Рисунок 6.11)

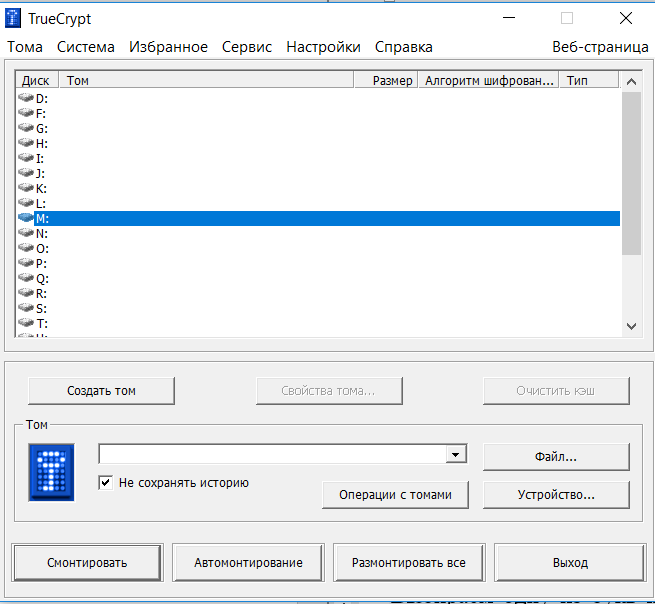


Рисунок 6.11 – Выбор буквы

Жмем Select File. При этом должна открыться стандартная версия окна в которой необходимо выбрать файл. (Рисунок 6.11)

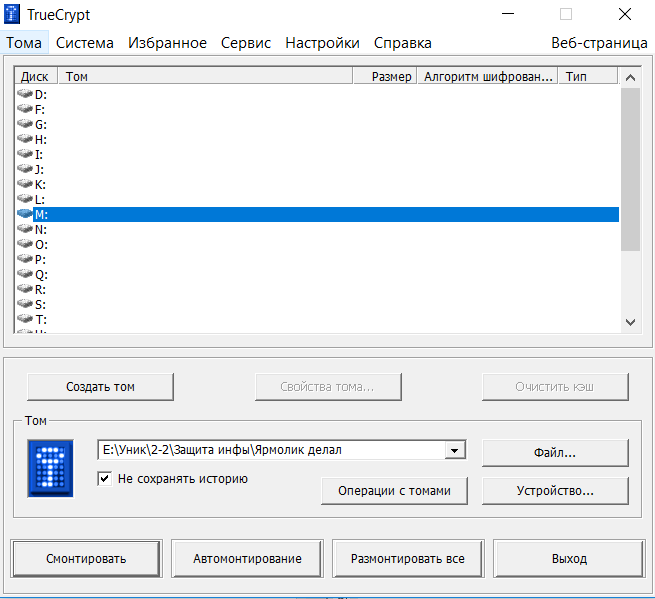
В данном окне находим файл, который вы создали с 6 по 11 этап и выбираем его. Жмем Open, после этого окно должно исчезнуть. (Рисунок 6.12).

Рисунок 6.12 – Выбор файла

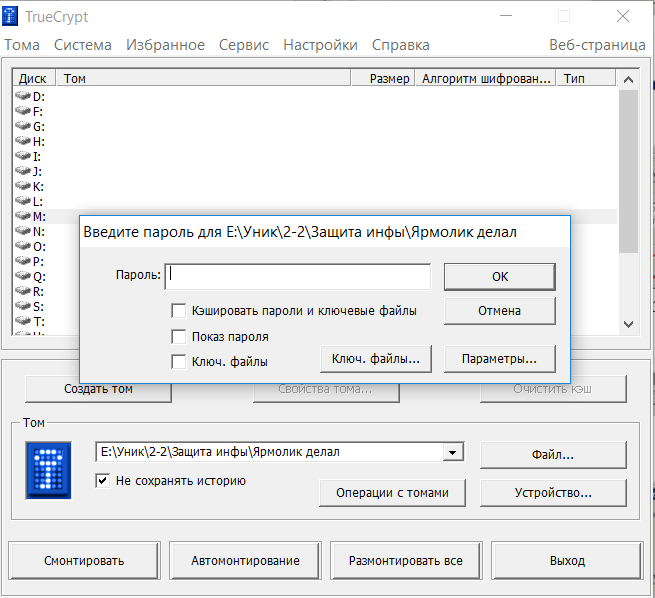
В оставшемся окошке TrueCrypt жмем Mount. Появляется окно, которое запрашивает ваш пароль. (Рисунок 6.13)

Рисунок 6.13 – Монтирование

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

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. (Рисунок 6.14)

Финальный этап:

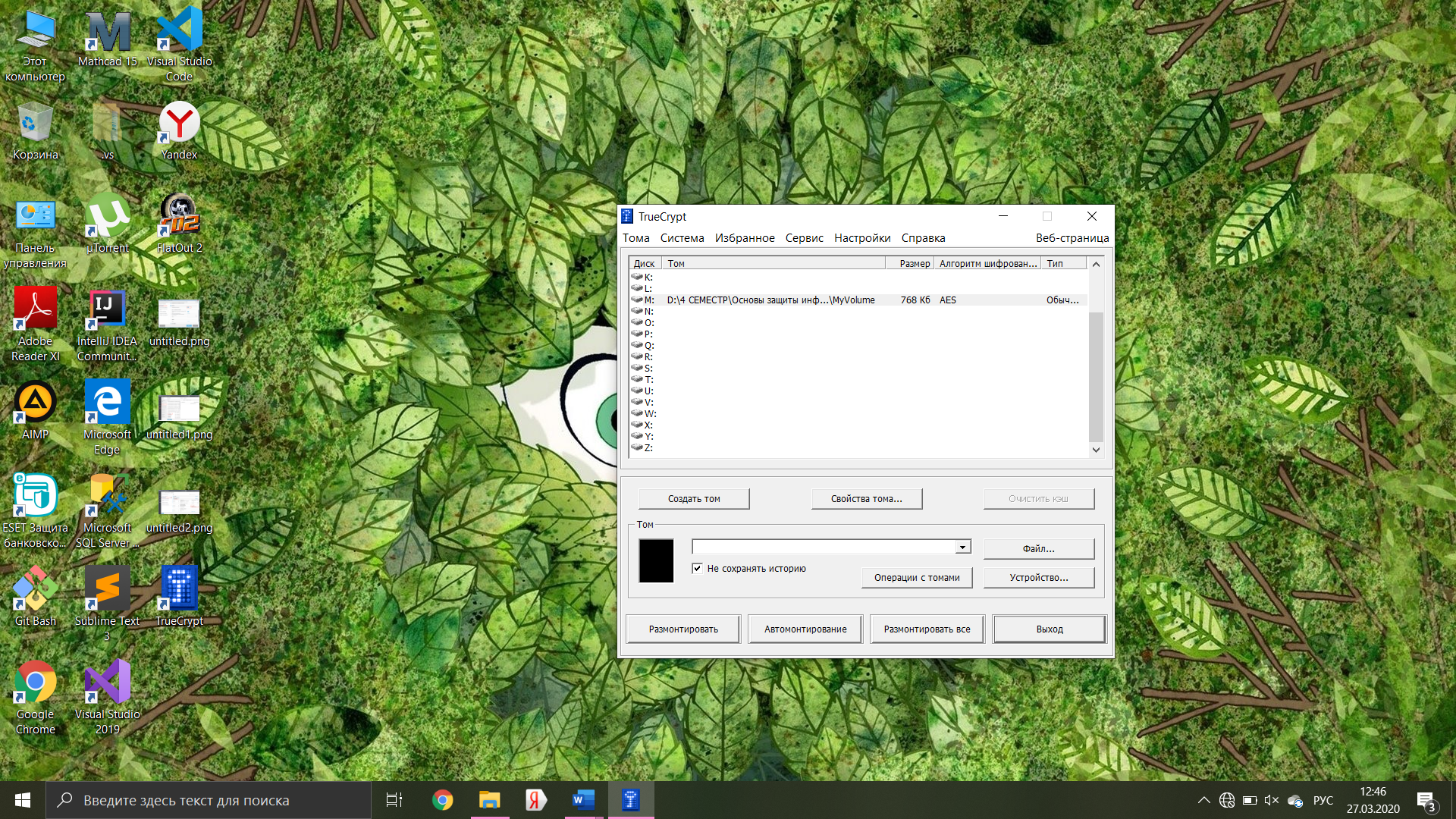


Рисунок 6.14 – Завершение операции

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». (Рисунок 6.15)

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:

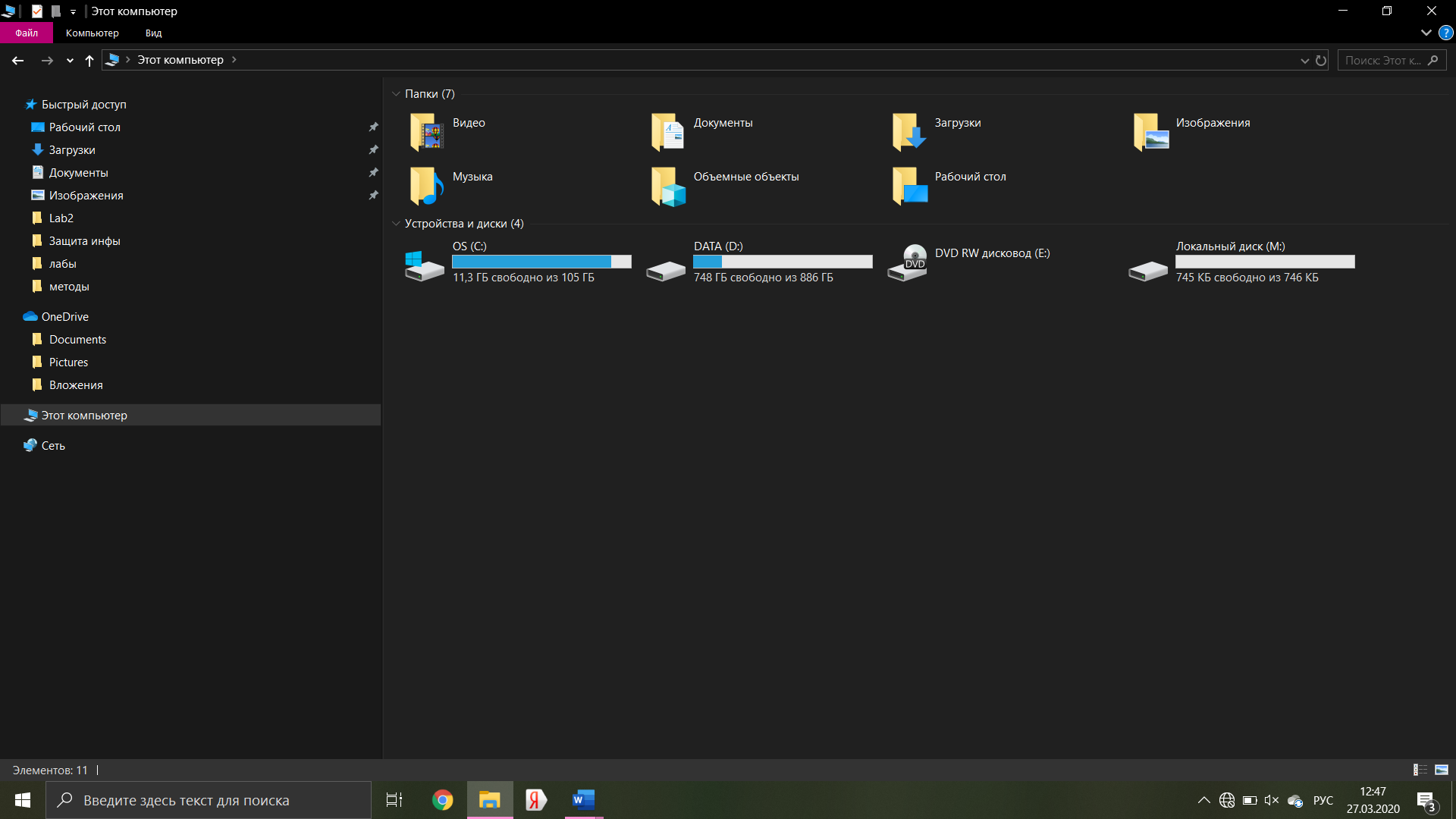


Рисунок 6.15 – Отображение нашего диска

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.

**Вывод:** Овладела навыками работы с компьютерными программами для криптографической защиты информации при передаче и хранении.