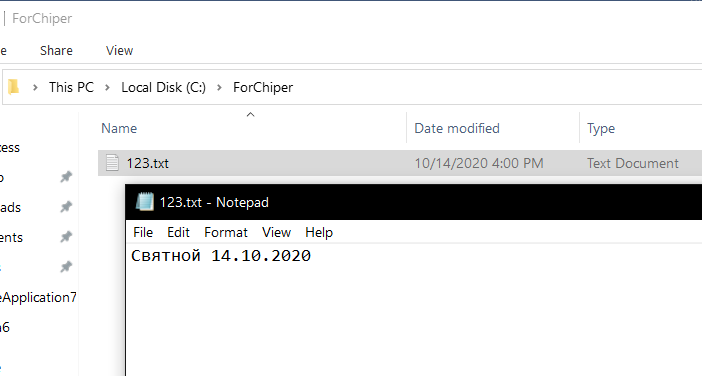
Святной Александр БАСО-02-20

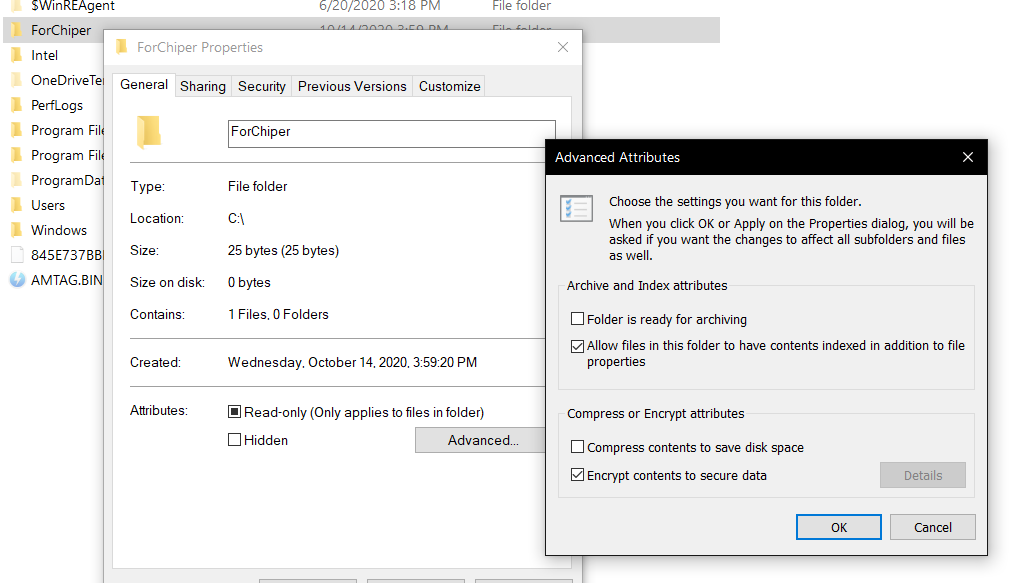
**Электронный отчет по практической работе 4**

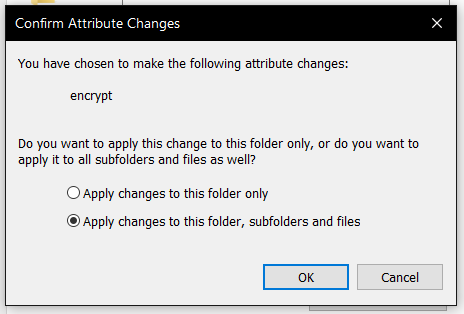
# Шифрование в Windows

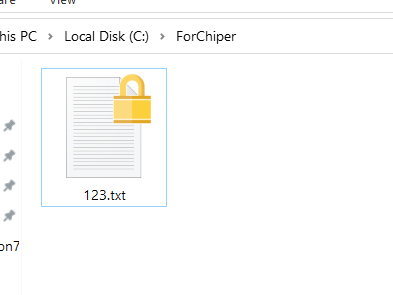
Создадим папку на диске C:\ и поместим туда текстовый документ:



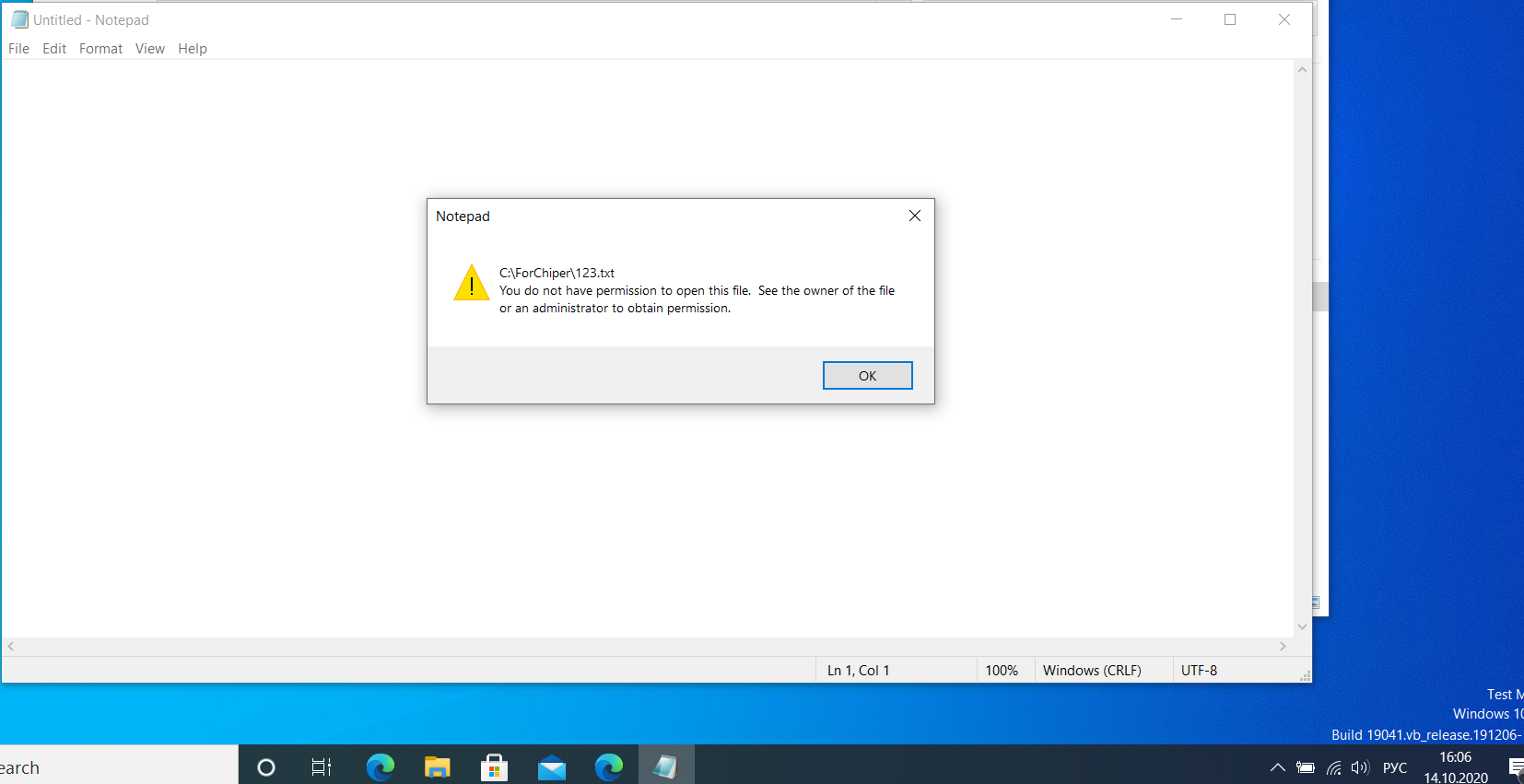
Затем зашифруем содержимое этой папки:







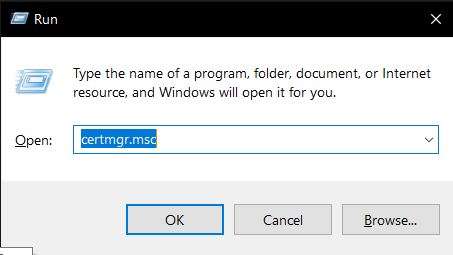
Затем, сменим пользователя и попробуем открыть данный текстовый документ:



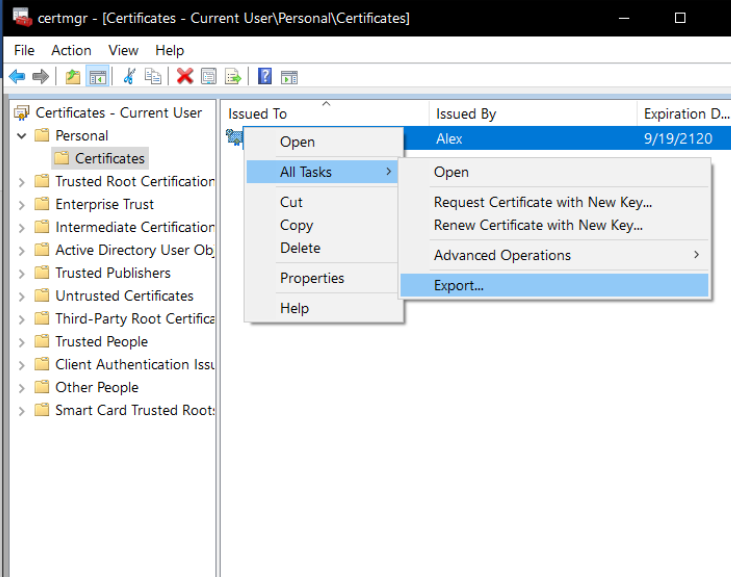
Предупреждение о том, что у данного пользователя отсутствуют права для открытия данного файла

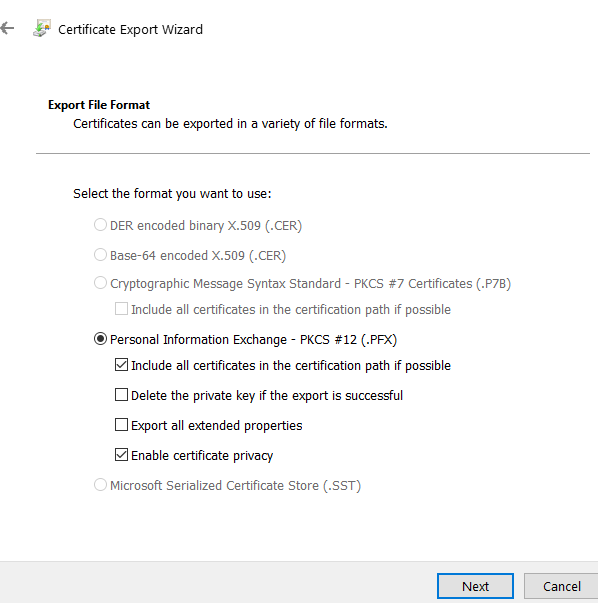
## Резервное копирование ключа шифрования EFS

Для резервного копирования ключа необходимо открыть диспетчер сертификатов:

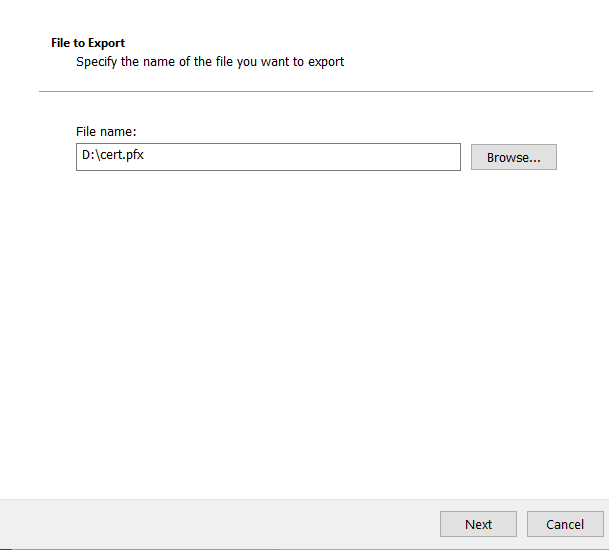


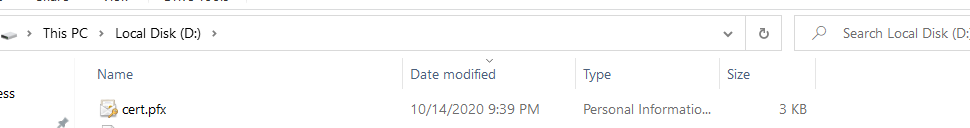
И экспортировать персональный сертификат:



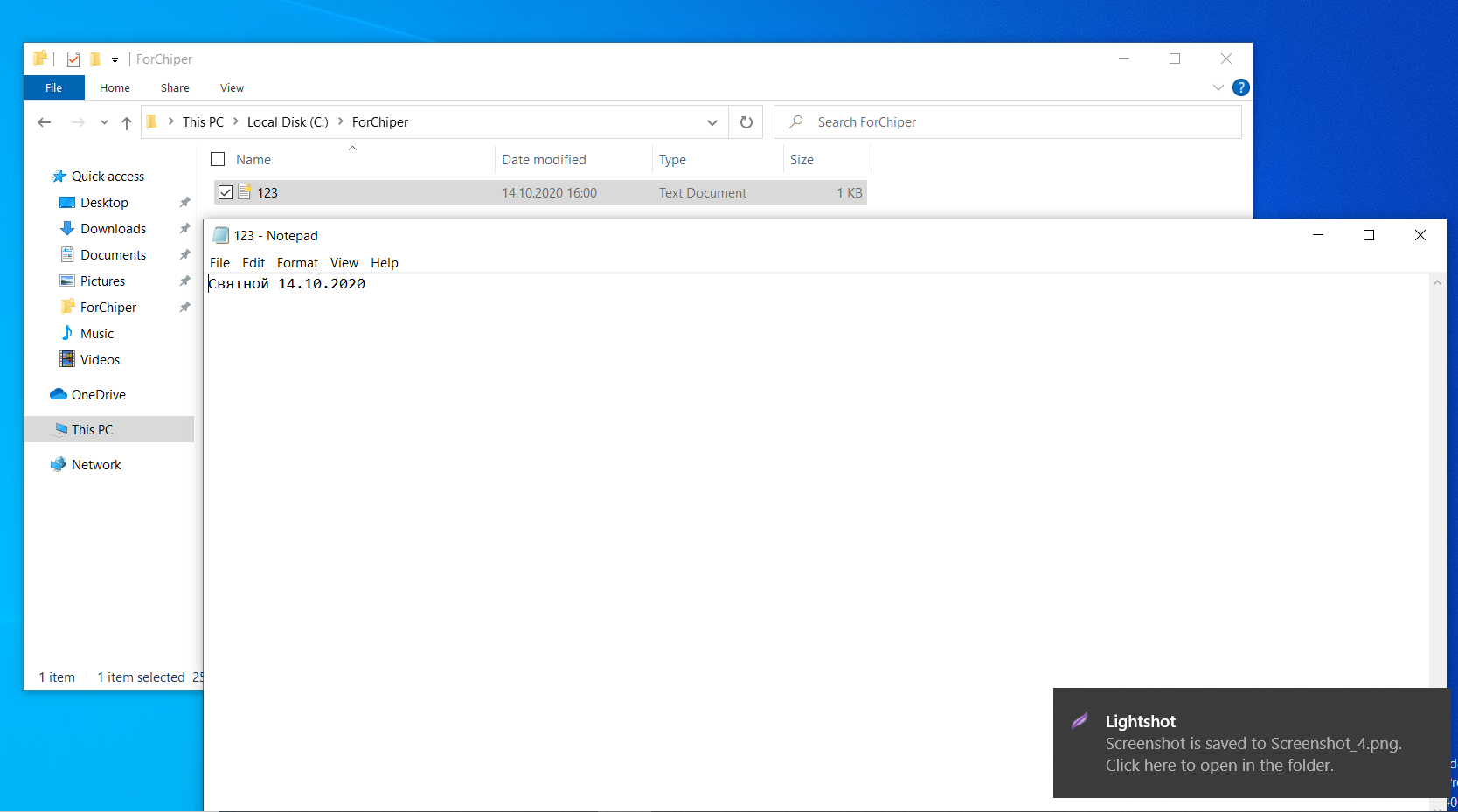
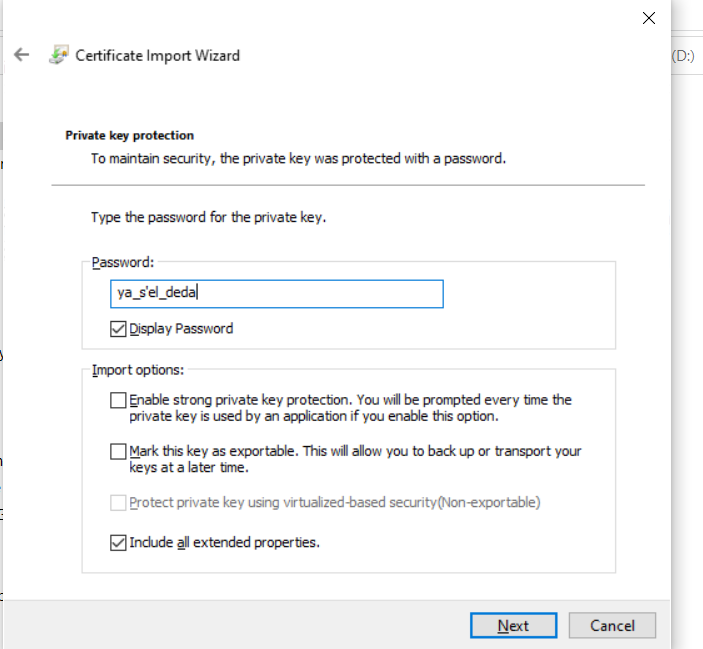
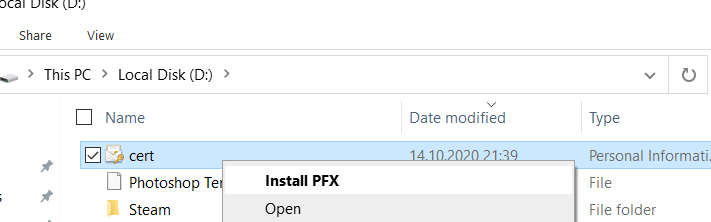


Установим пароль *ya\_s’el\_deda* и сохраним ключ на диске D:\:



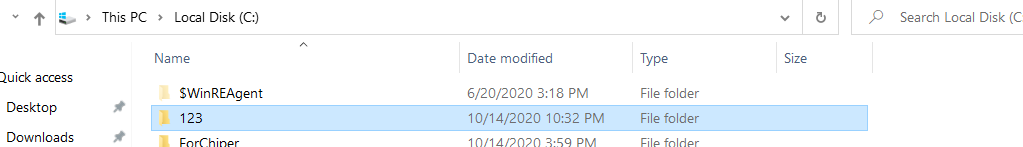
Получаем сообщение об успешном экспорте и наблюдаем, что ключ сохранился на диске D:\: 

Переключимся на другого пользователя, импортируем ключ и попробуем открыть файл:



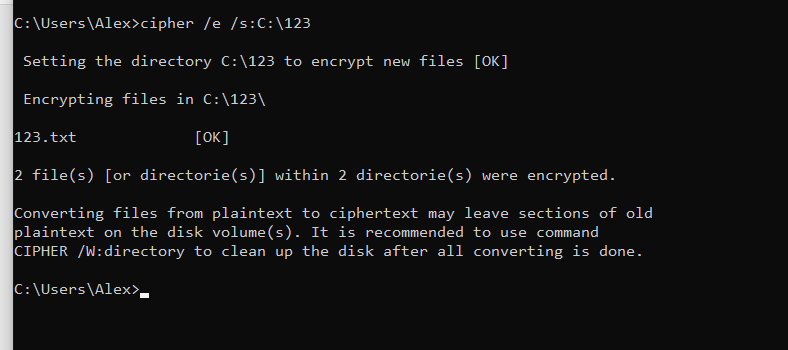
Всем ура! Мы открыли файл.

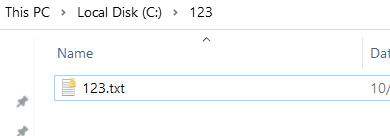
## Cipher

Создадим новую папку на диске C:\ 

Воспользуемся утилитой cipher:

cipher /e /s:C:\123

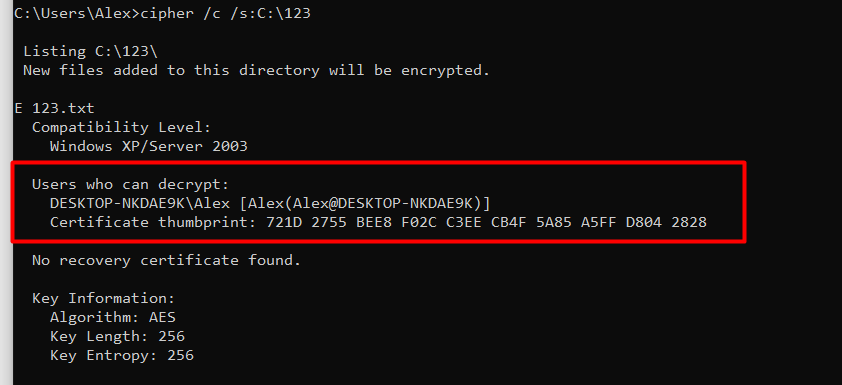




Мы успешно зашифровали подкаталог

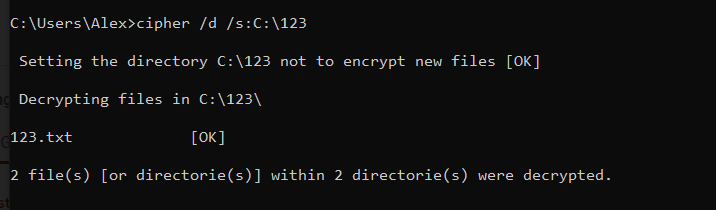
Далее проверим возможность чтения данного файла другими пользователями:

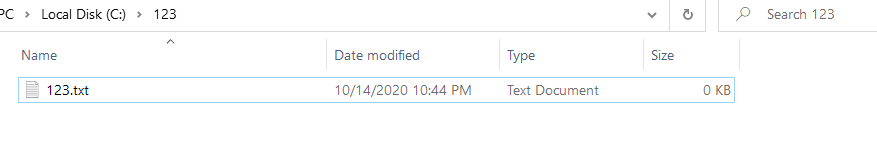
cipher /c /s:C:\123



Теперь расшифруем данный подкаталог:

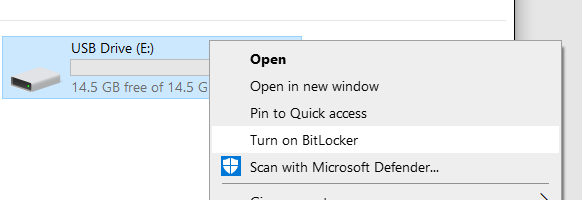
cipher /d /s:C:\123

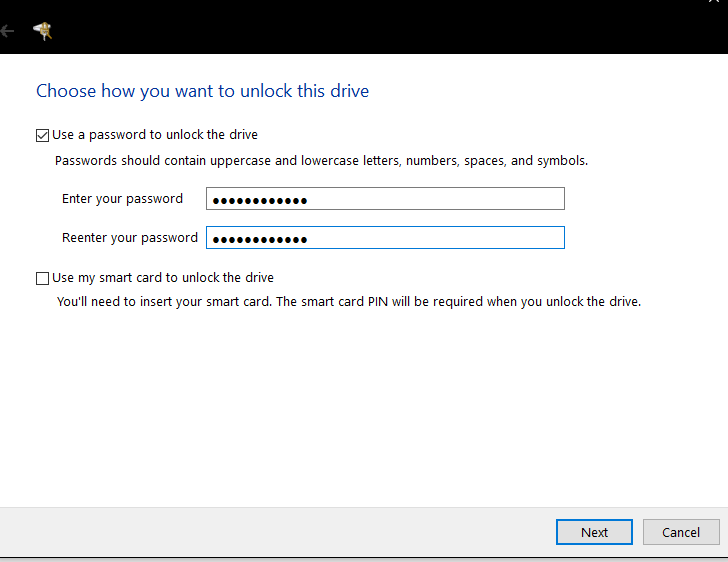


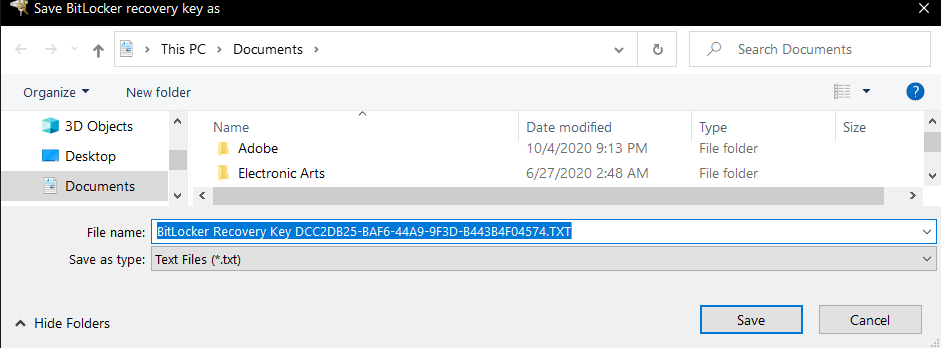


# Создание зашифрованного USB носителя и его использование

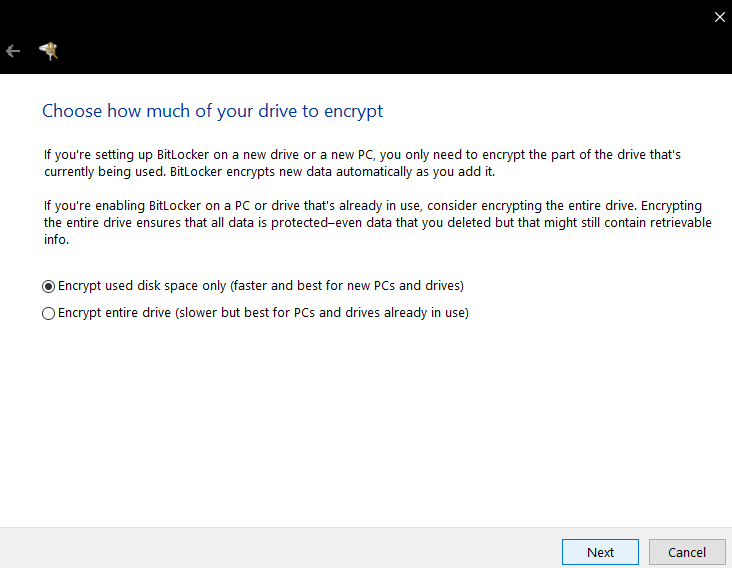
Необходимо включить BitLocker для данного накопителя:

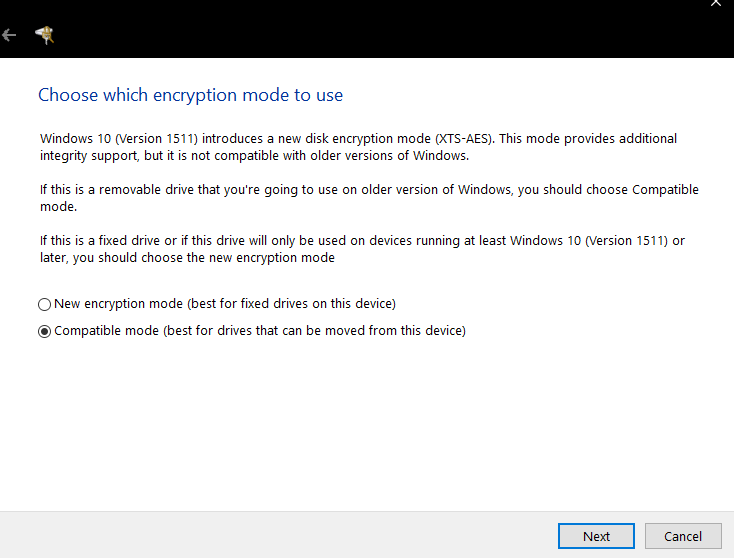


Устанавливаем пароль *ya\_s’el\_deda* и выбираем место сохранения в файл:



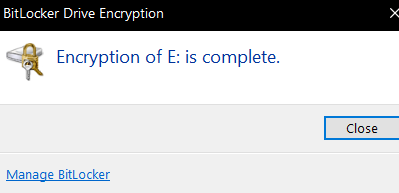
Затем выбираем оптимальные опции шифрования:



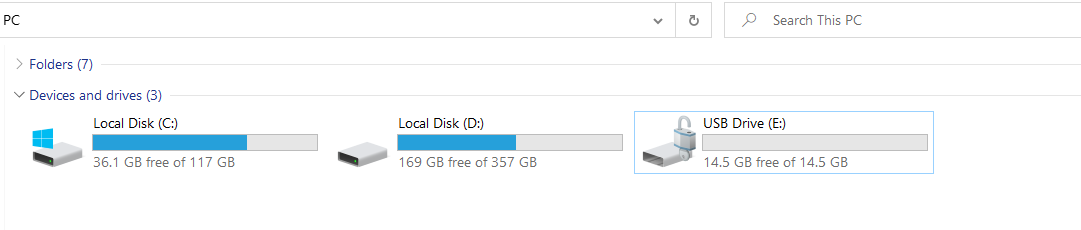


Происходит процесс шифрования:



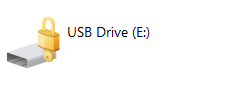


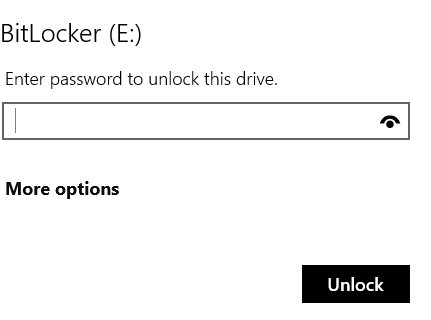
Как видно, флешка действительно зашифрована:



## Использование зашифрованного USB устройства

При извлечении и повторном подключении накопителя необходимо ввести пароль, чтобы получить доступ к диску:





После правильного введения пароля содержимое шифрованного раздела будет

доступно в обычном режиме. Также появится возможность управления параметрами

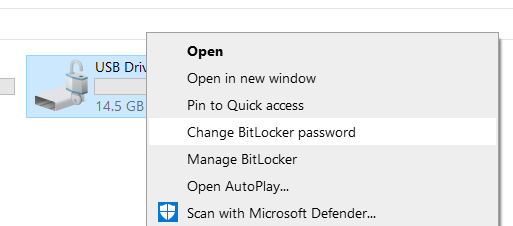
шифрования. В частности, возможно заменить пароль, сохранить ключ

восстановления, а также включить автоматическую разблокировку шифрованного

диска именно на данном компьютере. Для доступа к этим функциям нужно вызвать

контекстное меню для шифрованного диска, и выбрать пункт «Управление

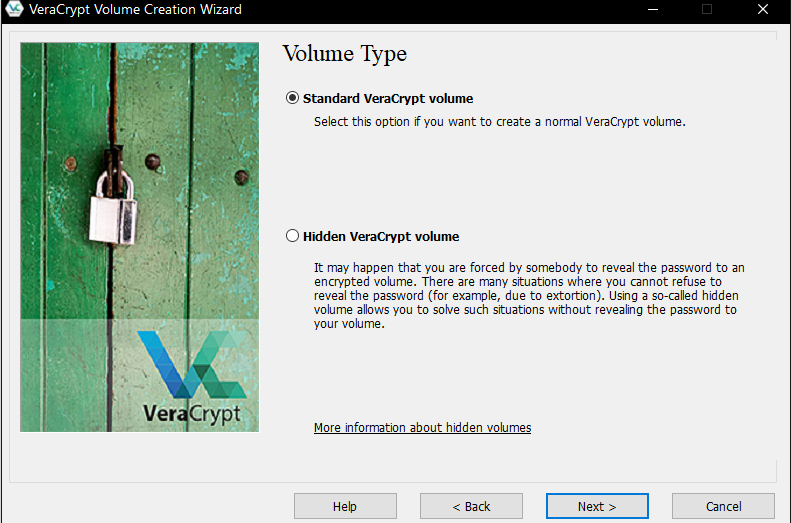
BitLocker»:

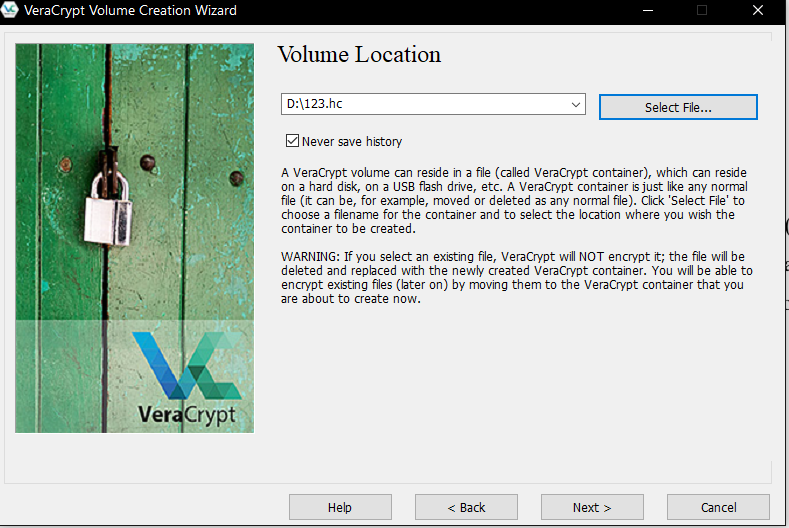


# Создание шифрованного контейнера с помощью VeraCrypt

## 

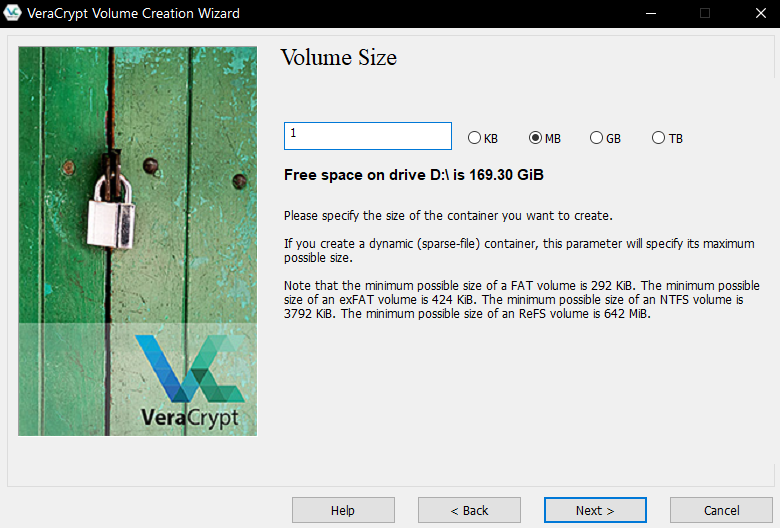




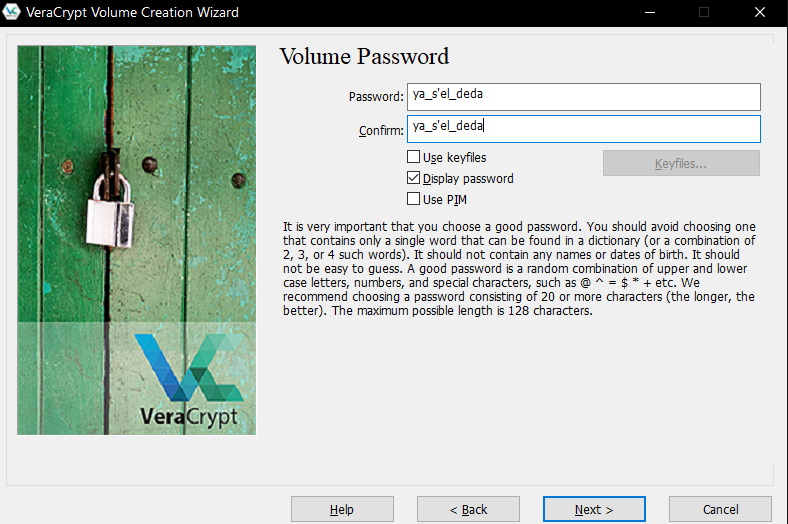




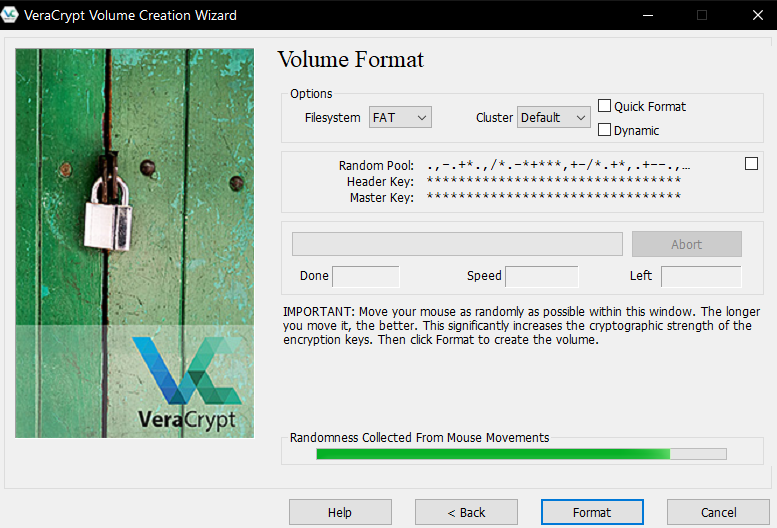
Создаем том размером 1 Мб:

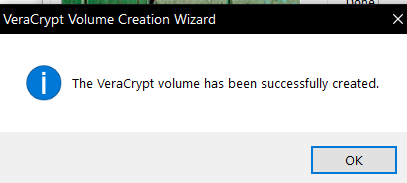


Устанавливаем пароль:

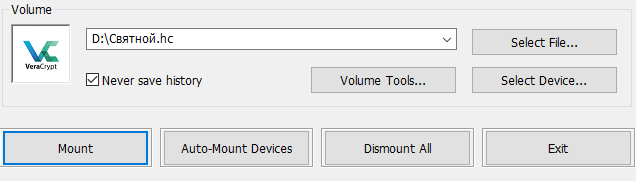


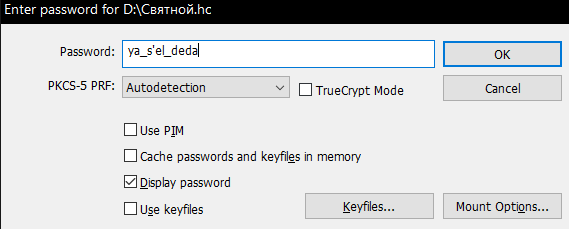
Происходит процесс формирования тома:

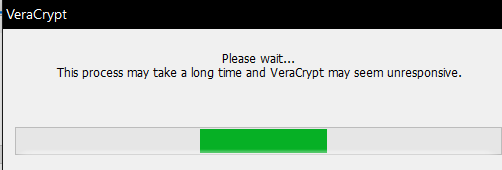


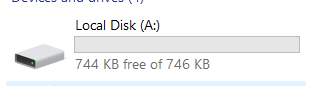


## Монтирование тома









p.s. Получается, что в процессе создания контейнера на скринах я назвал файл не своей фамилией, следовательно, на гитхабе будет этот же файл, но переименованный.