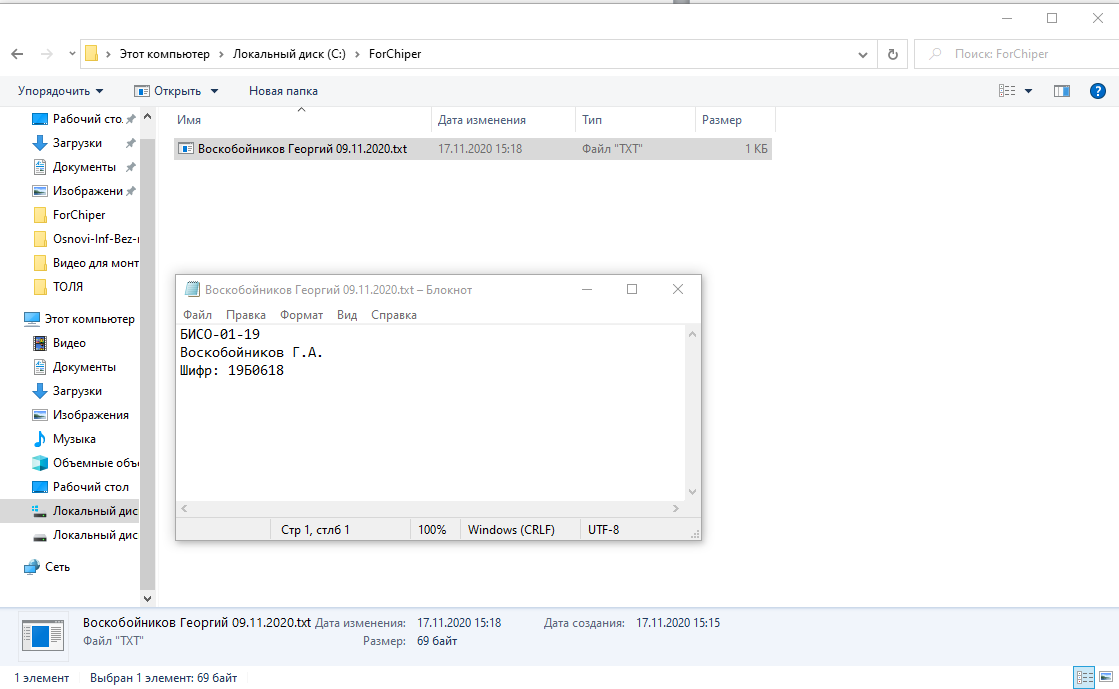
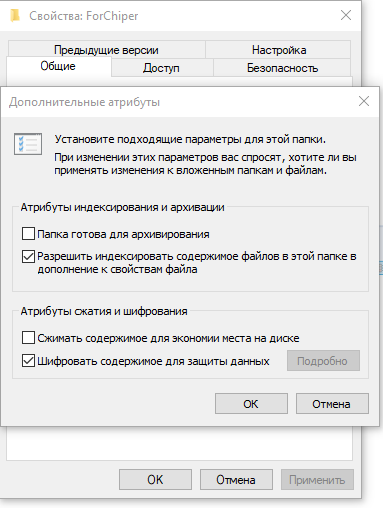
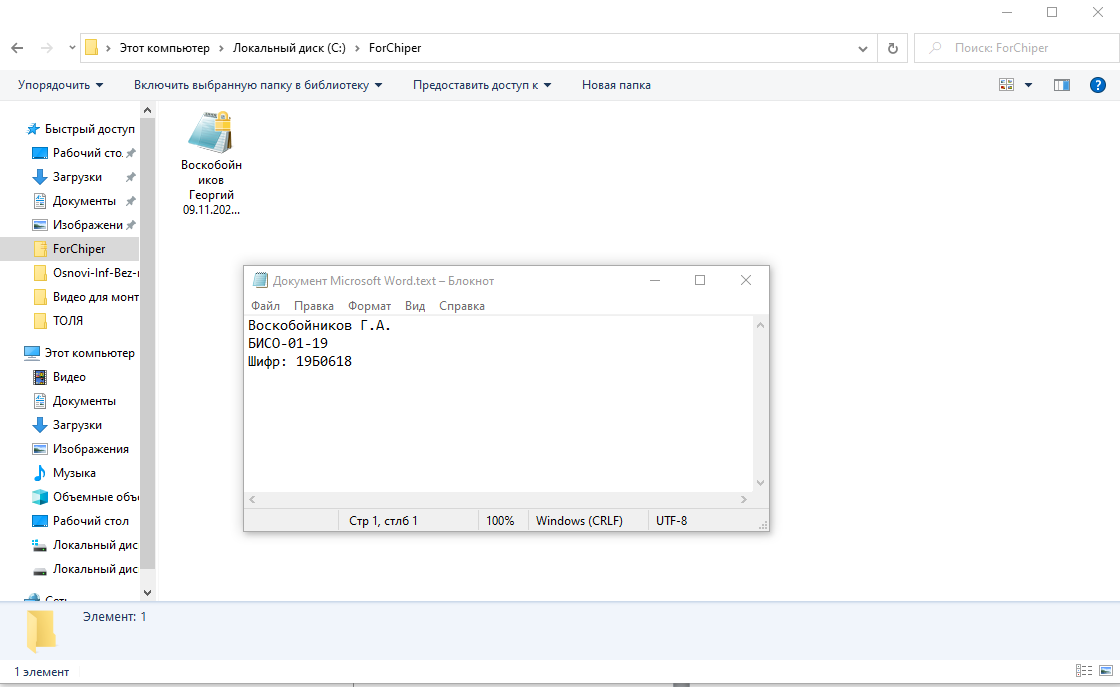
Практика 4

EFS

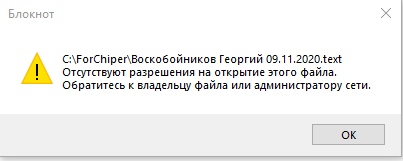






Создадим новую учётную запись на данном компьютере. Зашифруем файл.

Зайдем в аккаунт нового пользователя => файл не удалось открыть

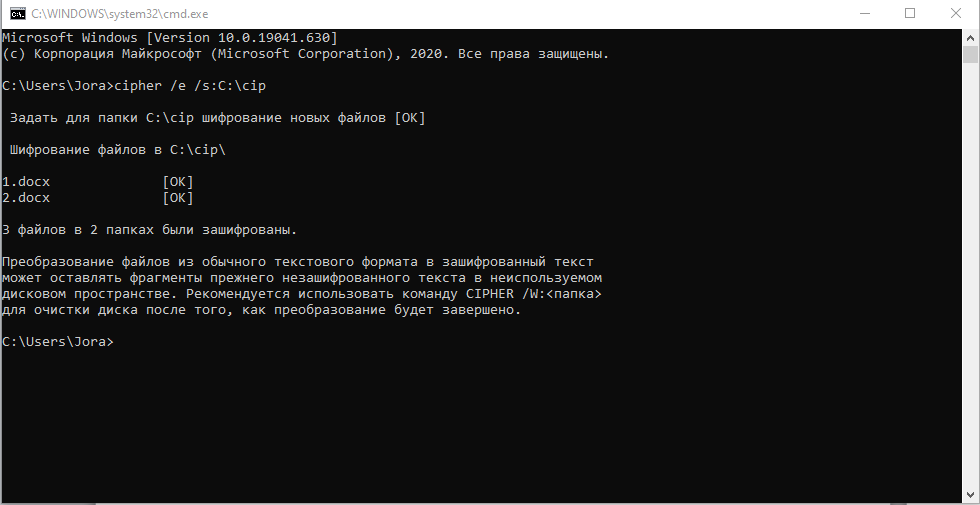


Зайдем на основную учетную запись и создадим резервную копию сертификатов , сохраним на другом диске.

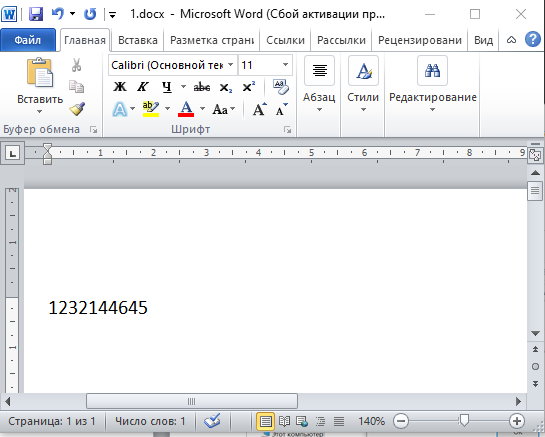
Перейдем на другую учётную запись и импортируем копию сертификатов и активируем ее.

После этого файл удачно открылся

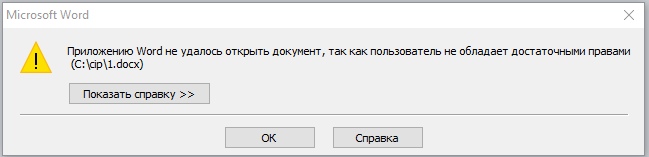
Cipher



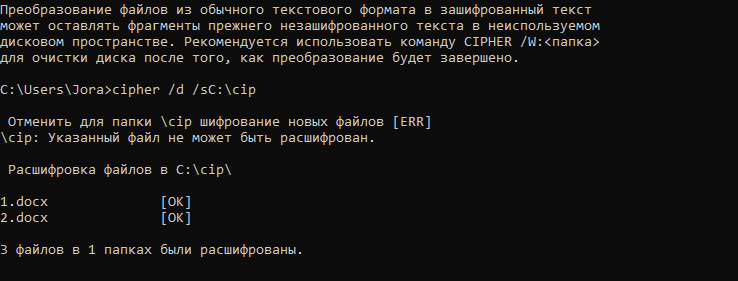
В основной учетной записи файл открывается:



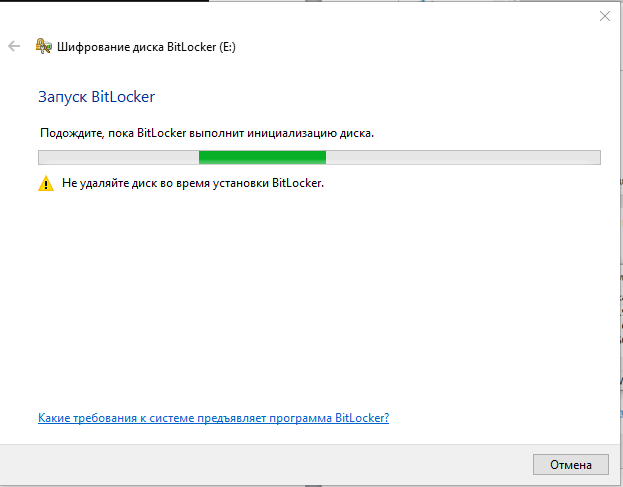
В дополнительной учетной записи не открывается ни один

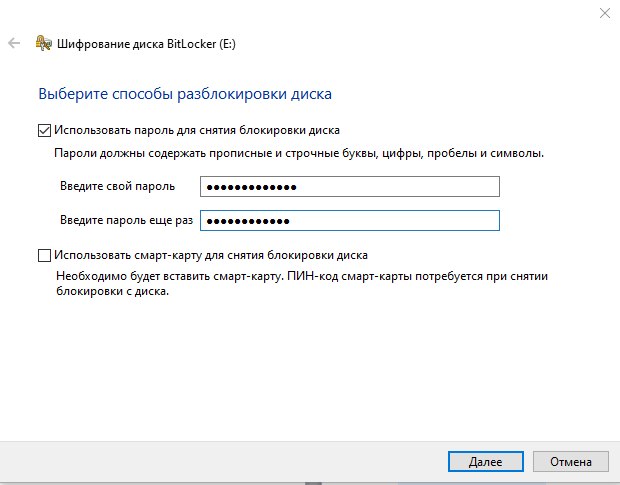


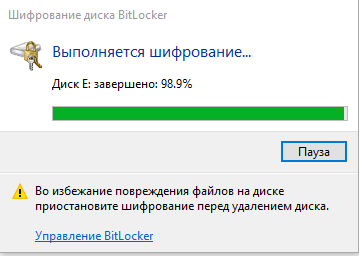
Расшифруем папку:

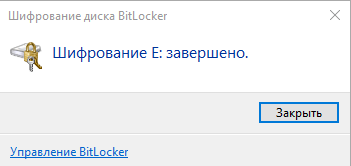


BitLocker

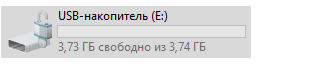




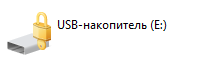


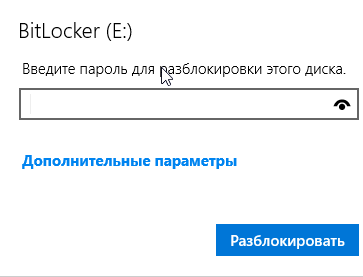


Получаем зашифрованный носитель:



Извлечем и снова вставим флеш-накопитель в устройство:





Теперь у нас есть абсолютно рабочий зашифрованный носитель наших данных.

VERACRYPT

