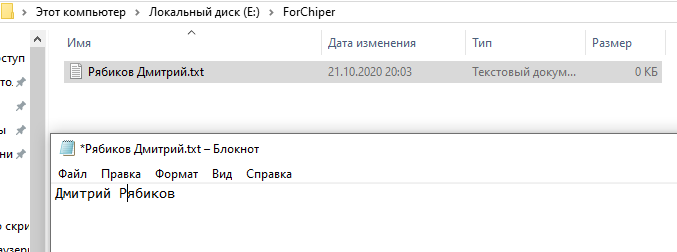
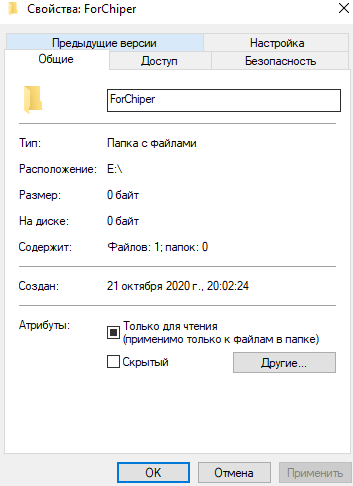
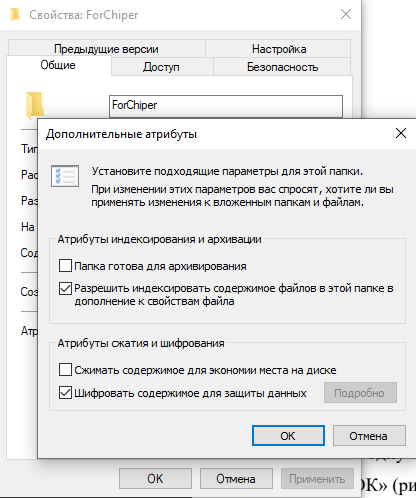
Шифрование в windows. EFS

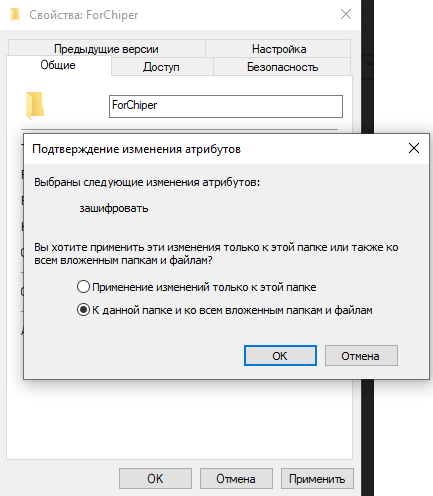
Для начала создадим папку и файл, что будем шифровать:

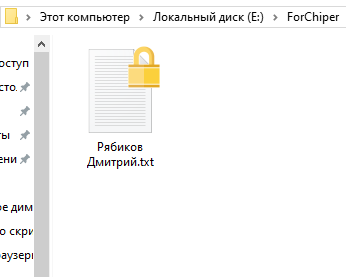


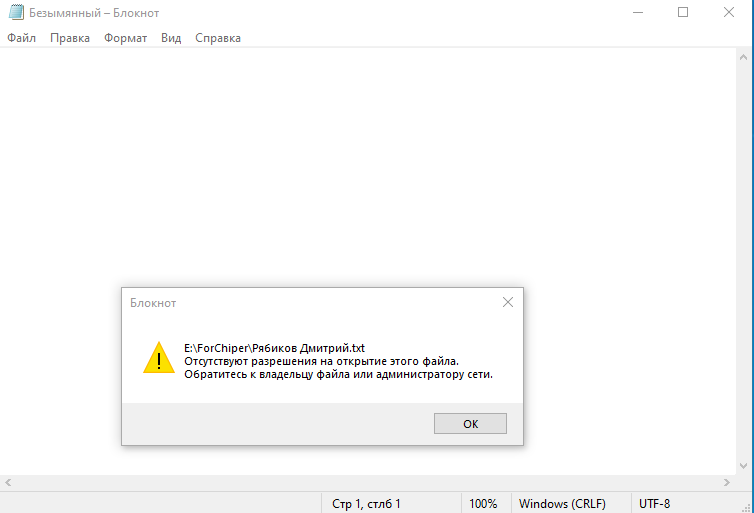


Далее Шифруем папку, создаем нового пользователя в ПК для теста нашего шифра:



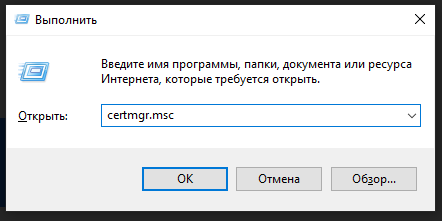


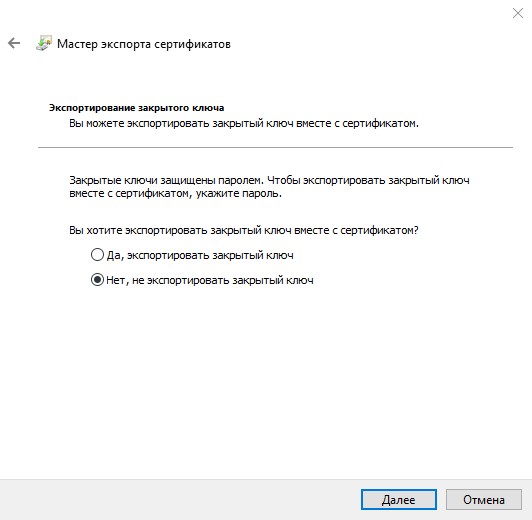


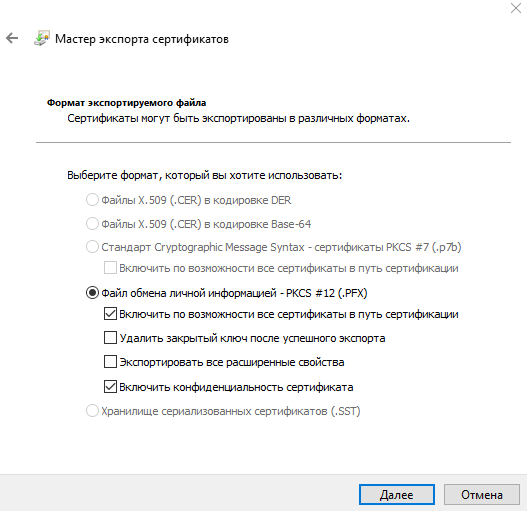


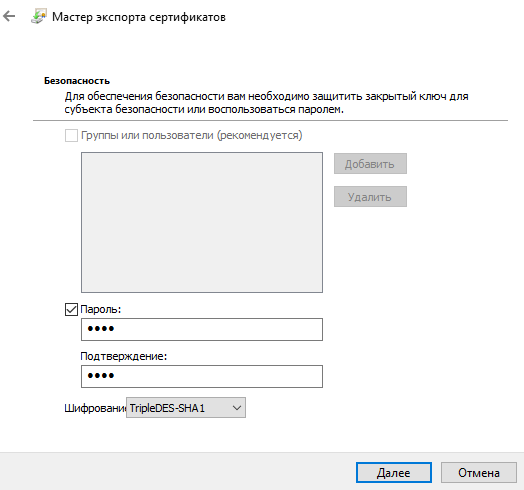
Успешно мы не получаем доступ к файлу(Неплохая вышла фраза)

Дальше перейдем к экспорту сертификата:

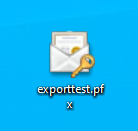
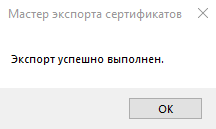
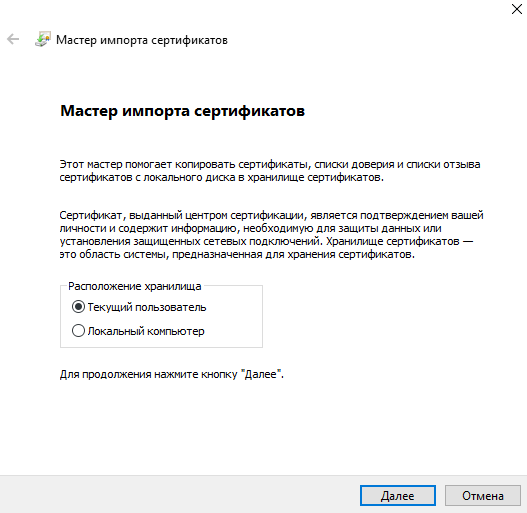


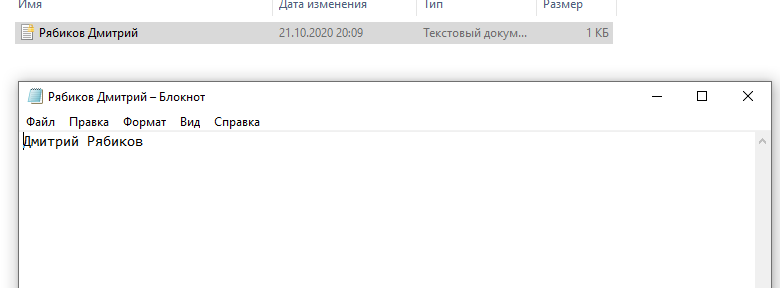
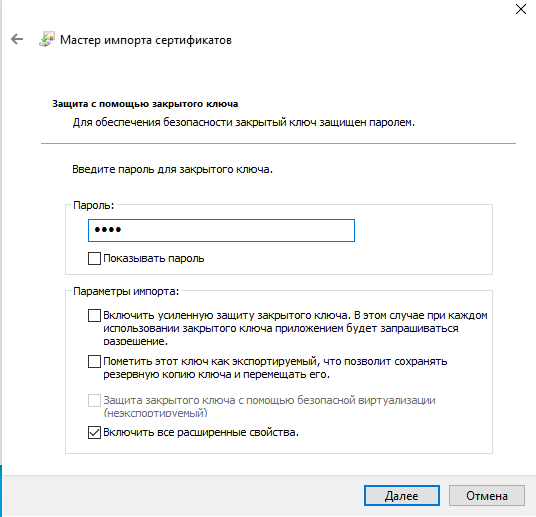






Дальше заходим под второй учеткой и проверяем:

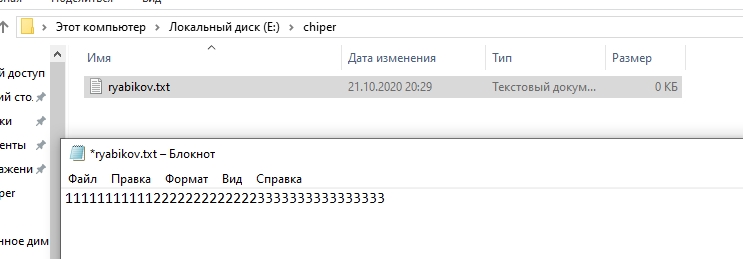
C:\Users\Admin\AppData\Local\Temp\Rar$DRa3740.41866\1шифрование\13логинимся с другой учетки.png



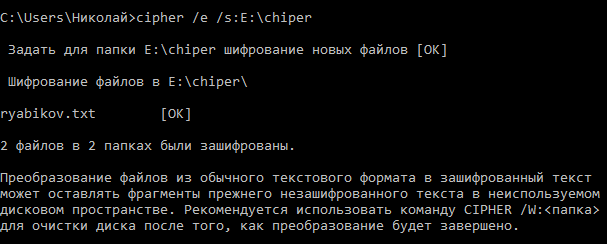
Все прошло успешно.

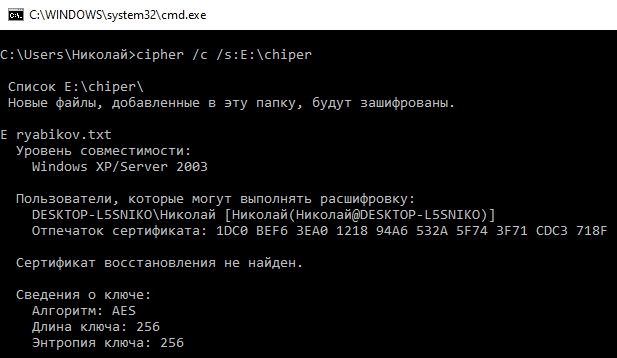
Cipher

Создадим новый файл для проверки:

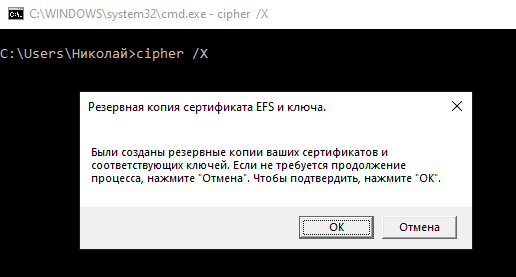


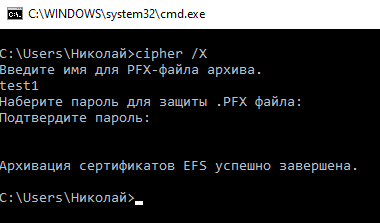
Шифруем их с помощью команды cipher /e /s:E:\shifr :



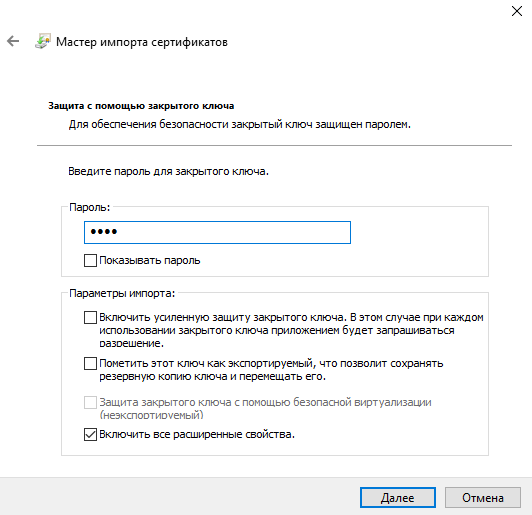
Посмотрим подробные сведения командой cipher /c /s:E:\shifr :

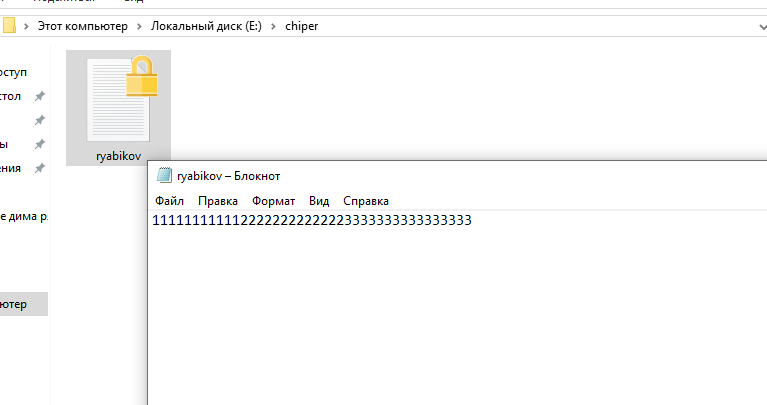
Теперь, командой cipher /X сохраним резервную копию сертификата EFS:





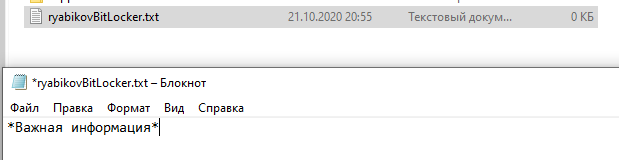
С другой учетки открываем данный файл:



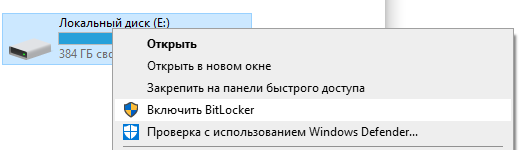


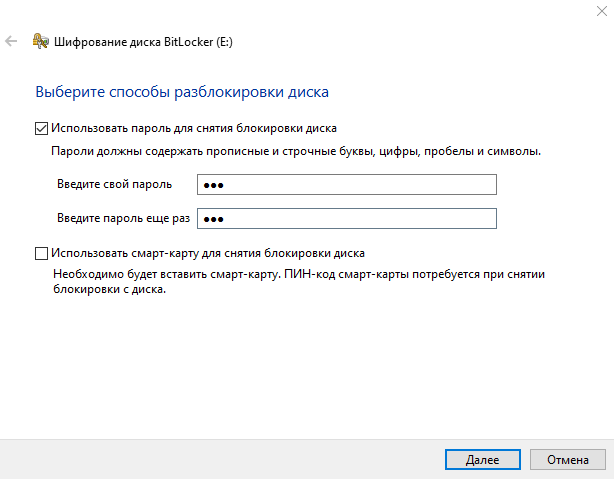
Succesful!

Bitlocker:

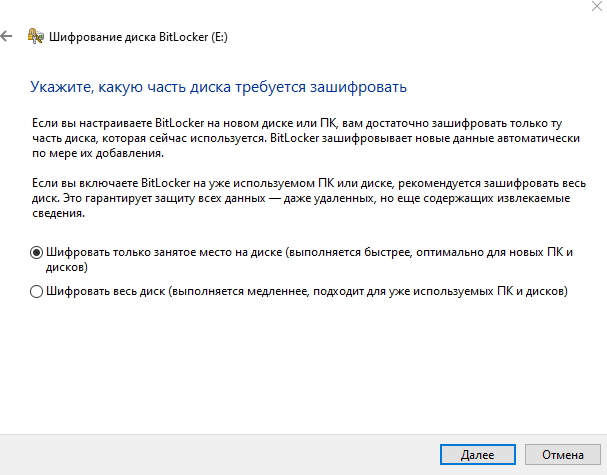
Создаем очередной файл…

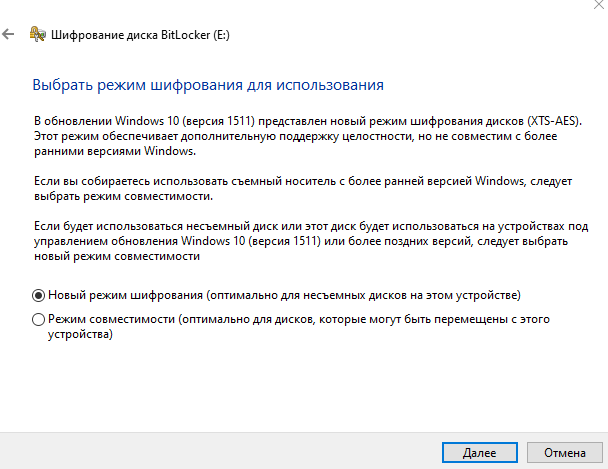
Включаем битлокер:

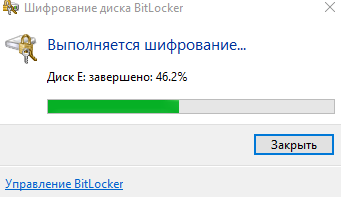




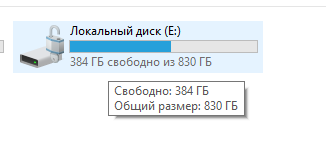
Шифруем:



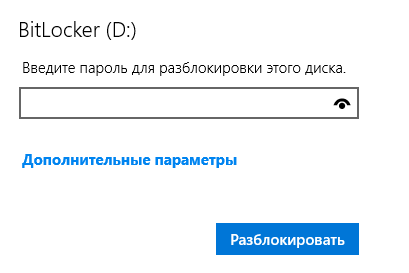




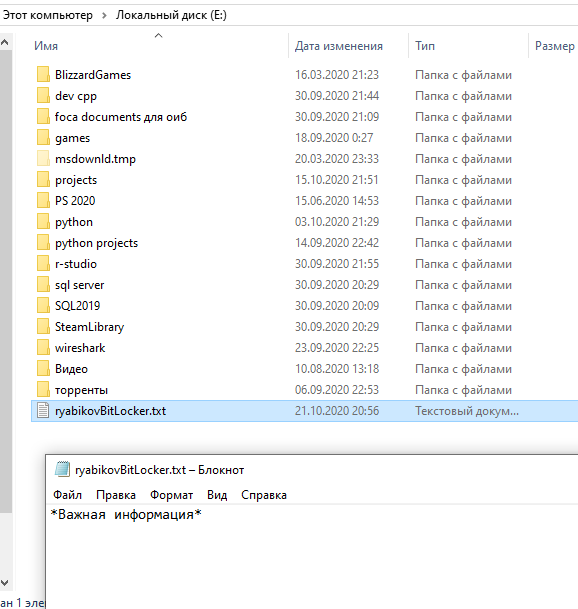
Как мы видим диск успешно зашифрован.



Теперь требуется ввести пароль:

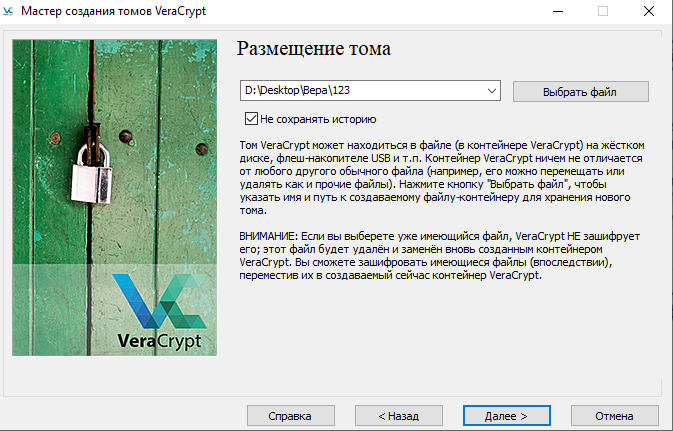


После ввода пароля все вновь работает:

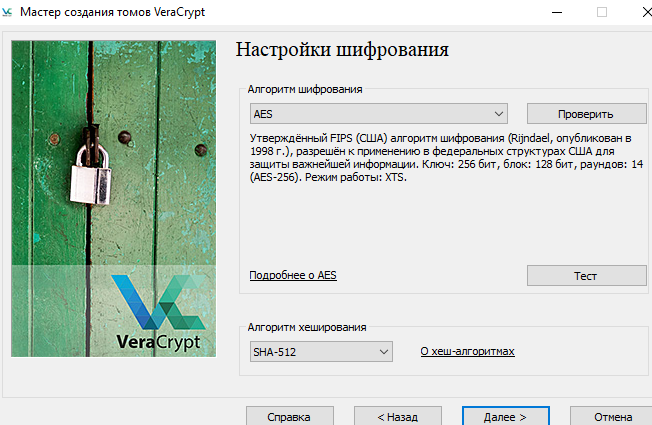


VeraCrypt

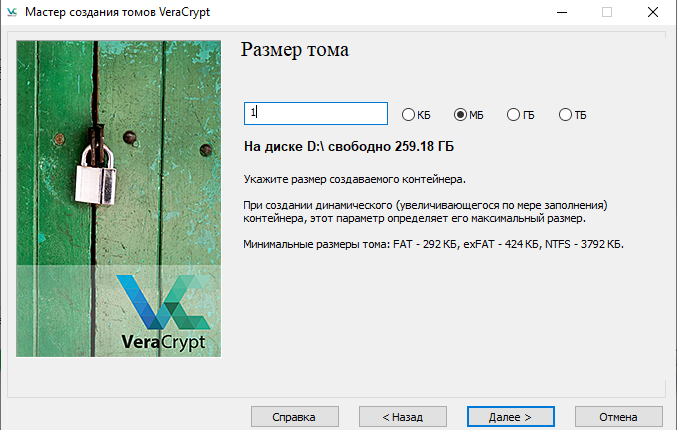
Создаем очередную папку с текстовиком и шифруем:

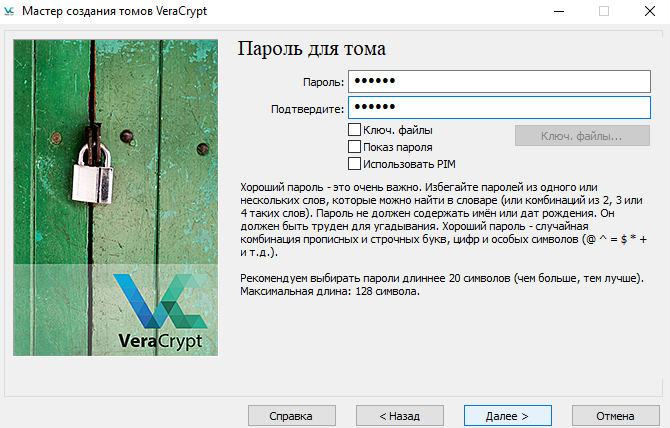


Используем шифр AES:

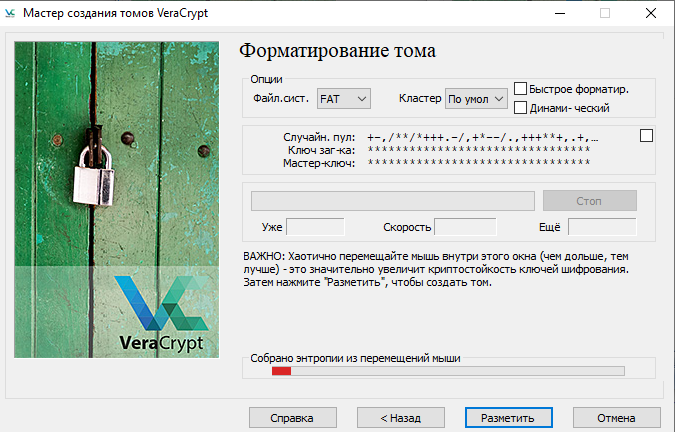


Выбираем размер и пароль:

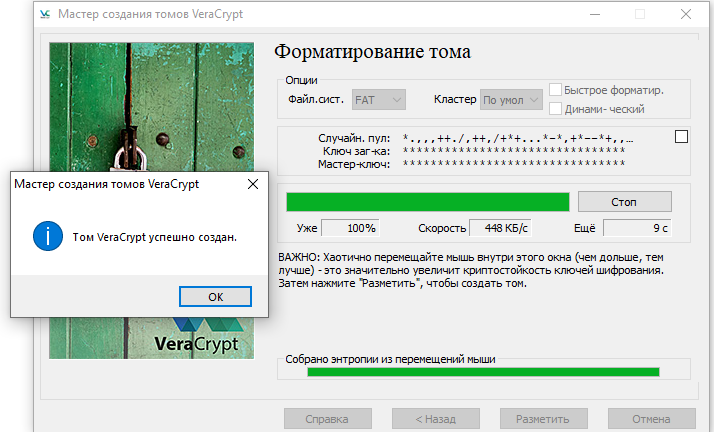




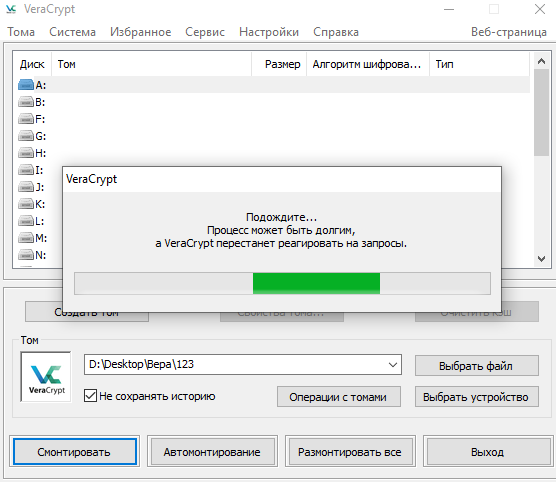
Ожидаем….



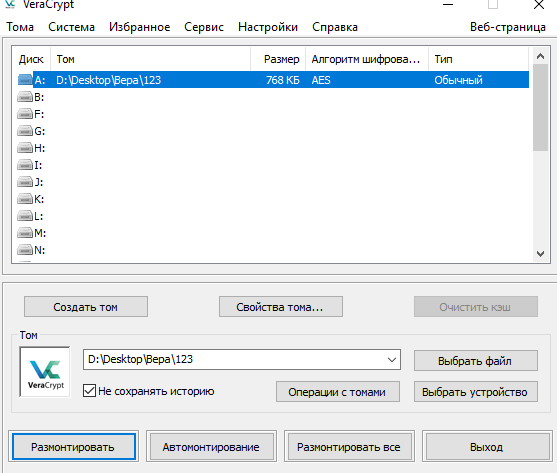
Готово:



Смонтируем том:



Успешно смонтировали



Пароль от файла будет 228322