

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Прикладные информационные технологии» |

**ОТЧЕТ О ВЫПОЛНЕНИИ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ №4**

**В РАМКАХ ДИСЦИПЛИНЫ «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ И СИСТЕМ»**

Выполнил:

Студент 2-ого курса

Учебной группы БИСО-02-22

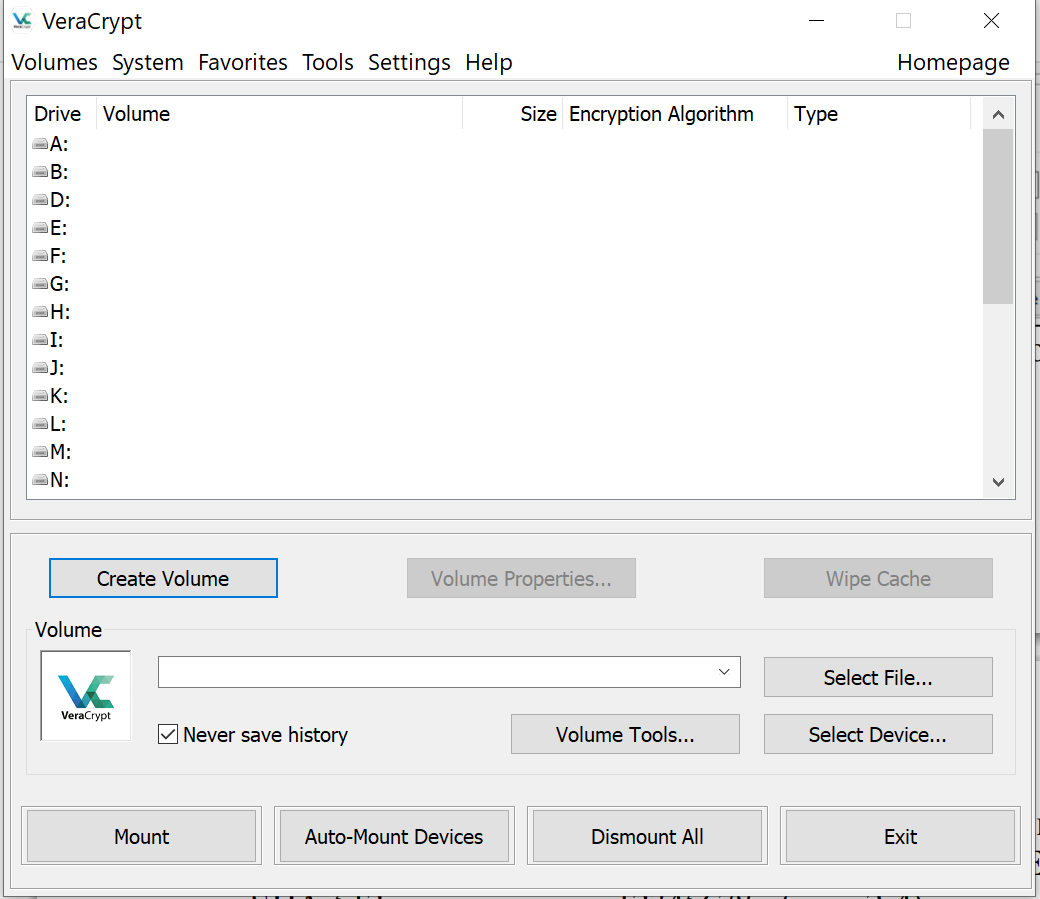
Зубарев В.С.

Оглавление

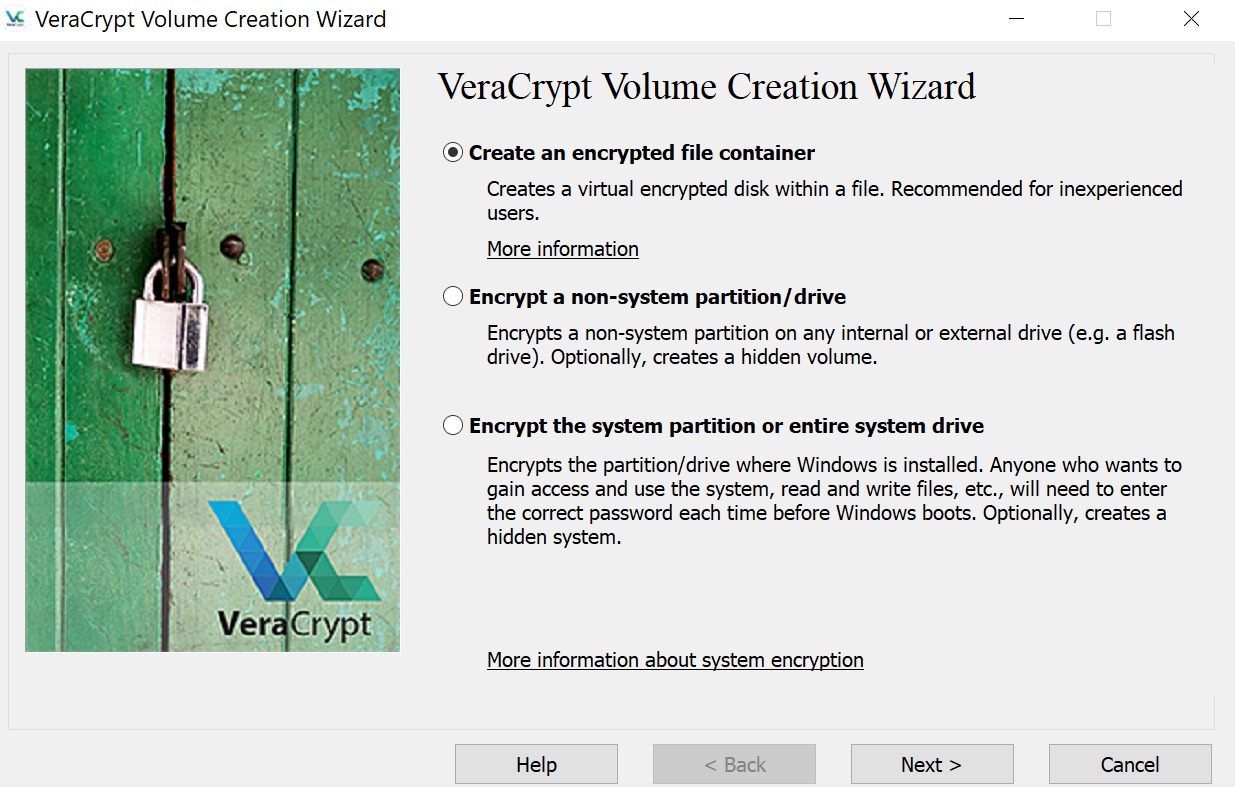
**Элементы оглавления не найдены.**

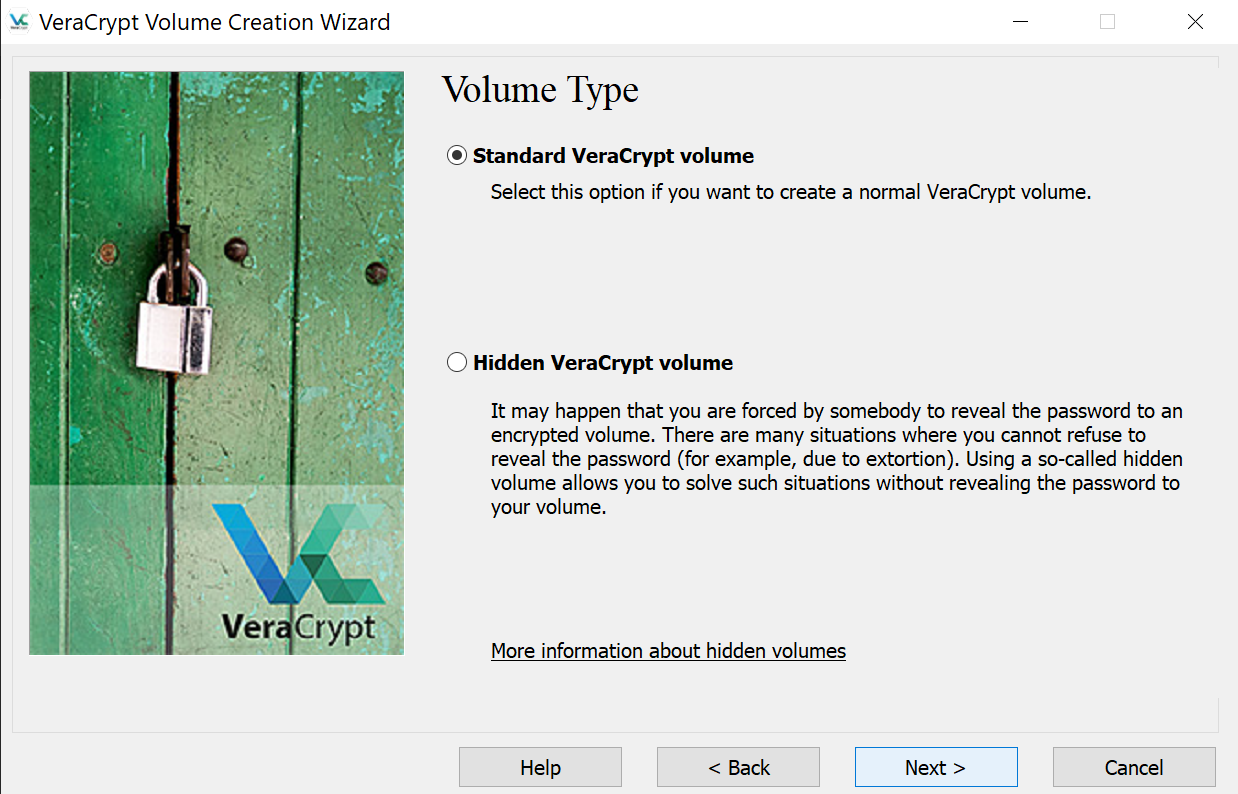
# Сохранение данных в криптографическом контейнере VeraCrypt

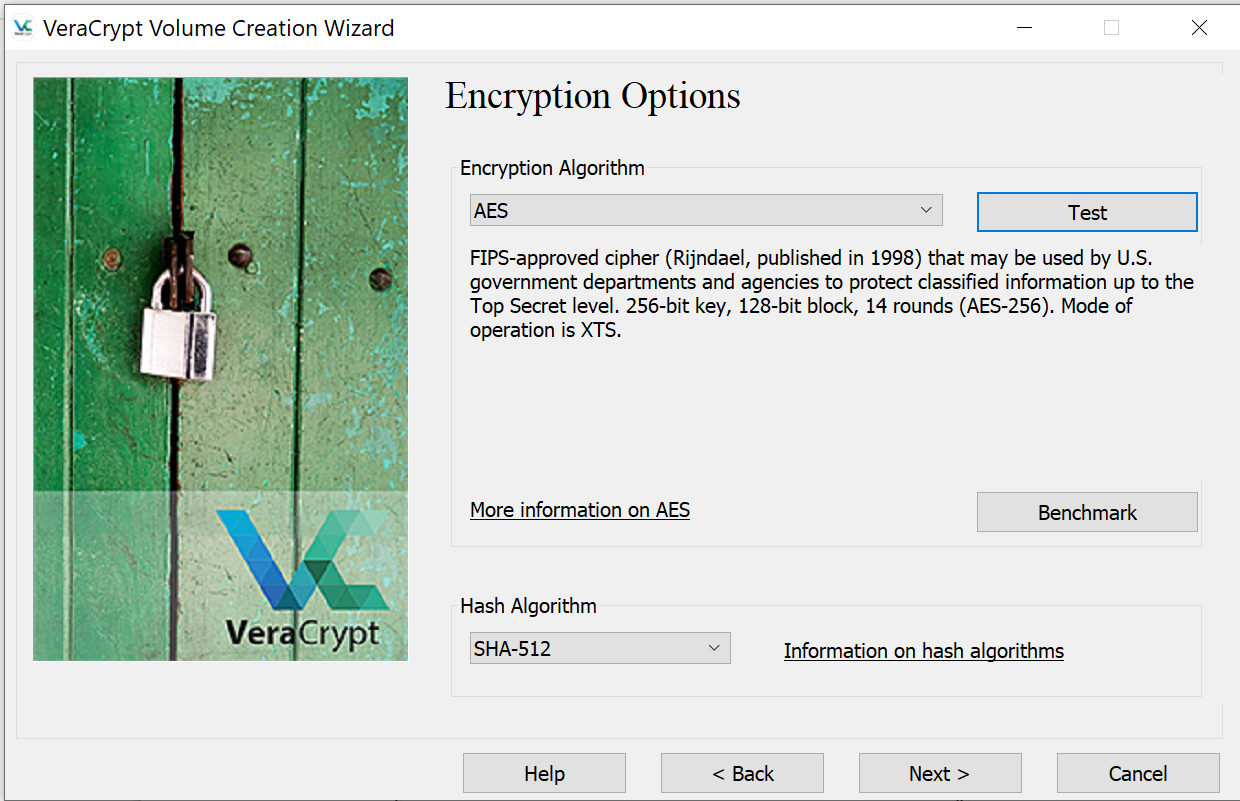
Запустите программу VeraCrypt через ярлык на Рабочем столе операционной системы Windows 10.

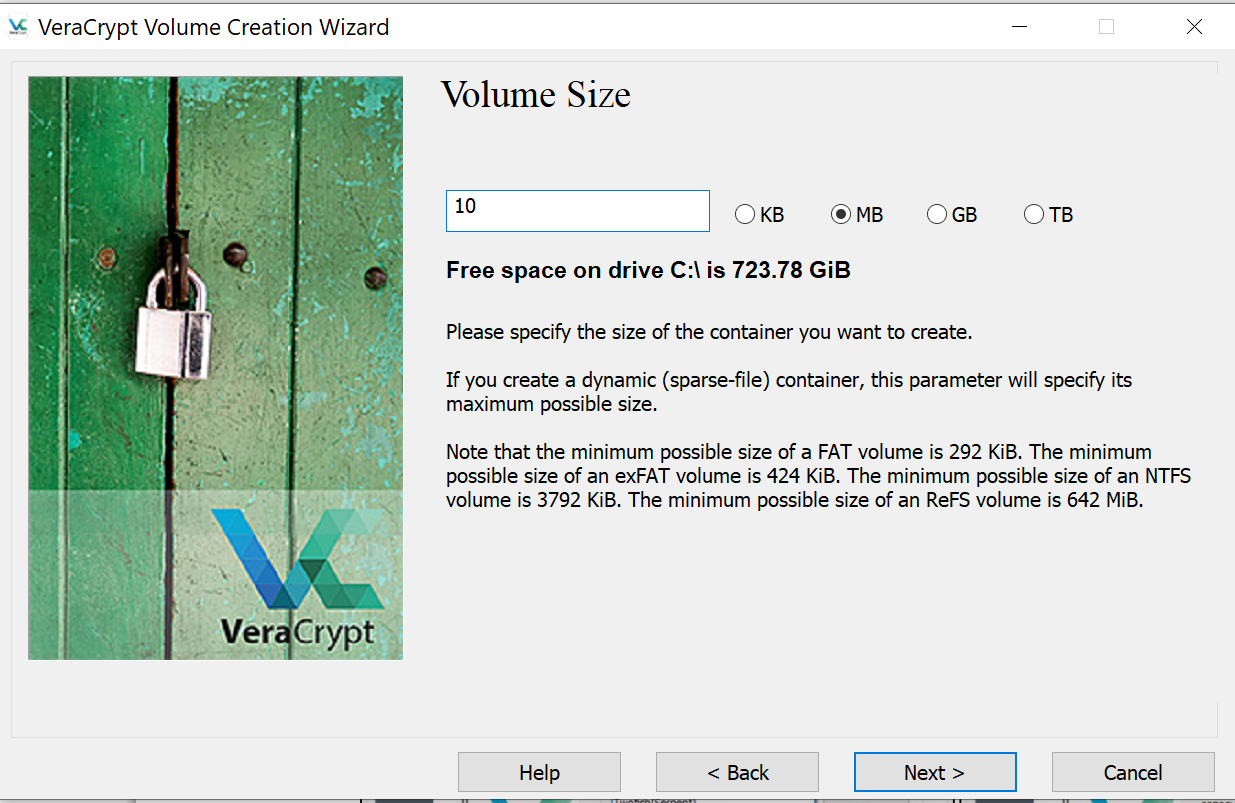


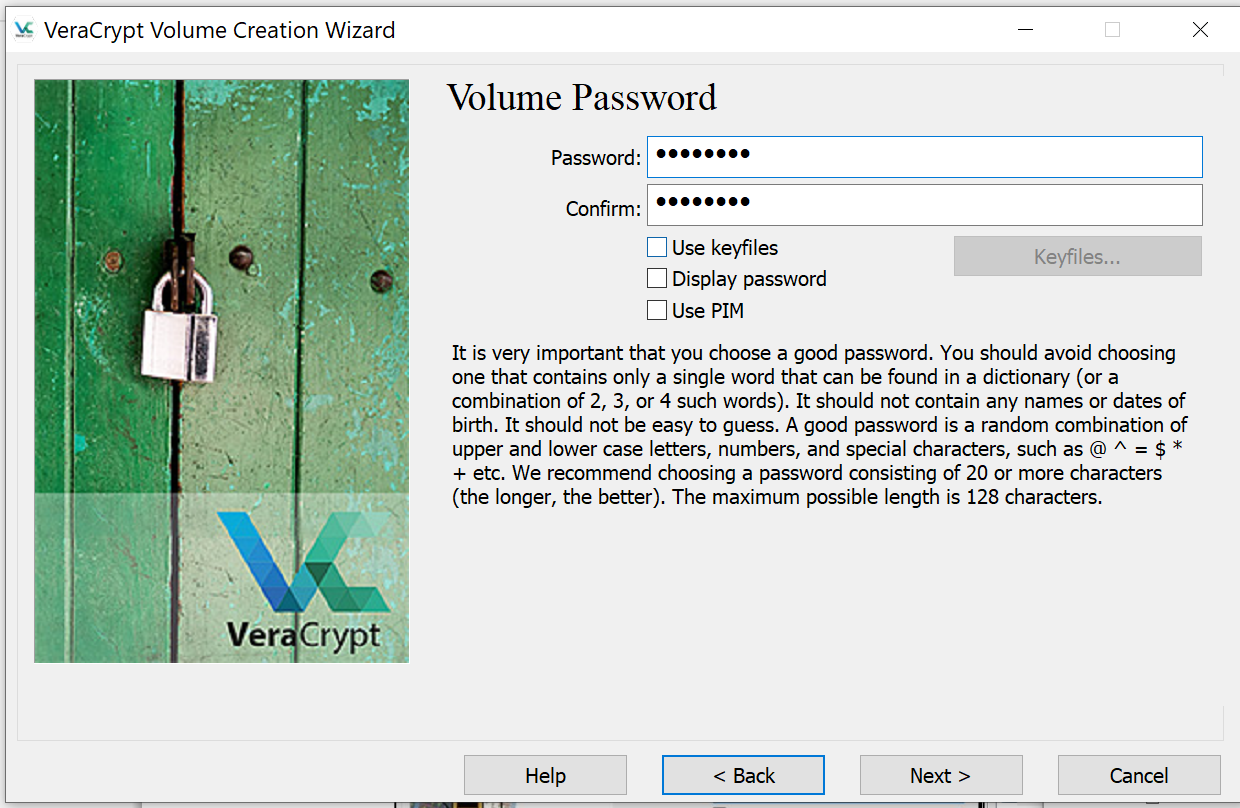
Создайте новый том (криптографический контейнер) размером 10 Мб, тип – обычный, алгоритм шифрования – AES, функция хеширования – SHA-512, с паролем – «12345678» (рис. 2-4). Кнопка «Create Volume» или «Создать том». Выберете создание контейнера в виде файла (Create an encrypted file container) и обычный том (Standard VeraCrypt volume). Место размещения файла – Рабочий стол, имя файла – ФИО.bin, тип файловой системы – FAT.

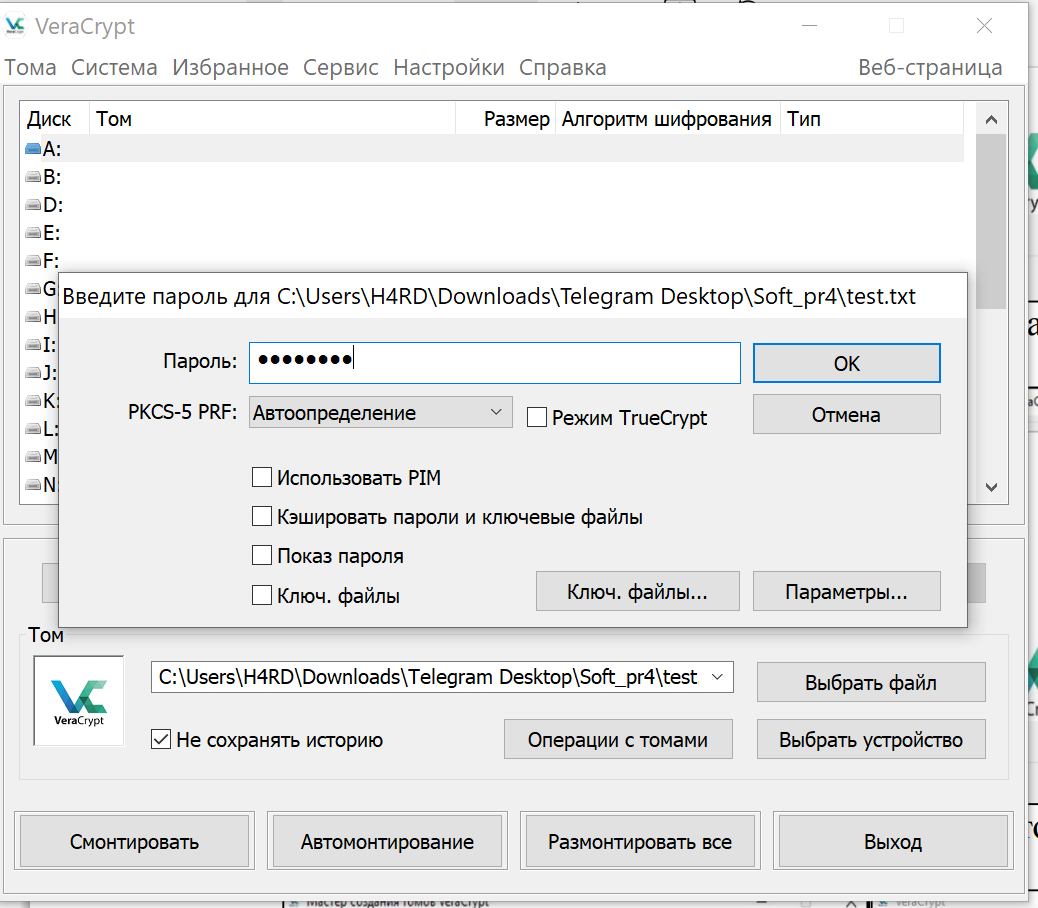


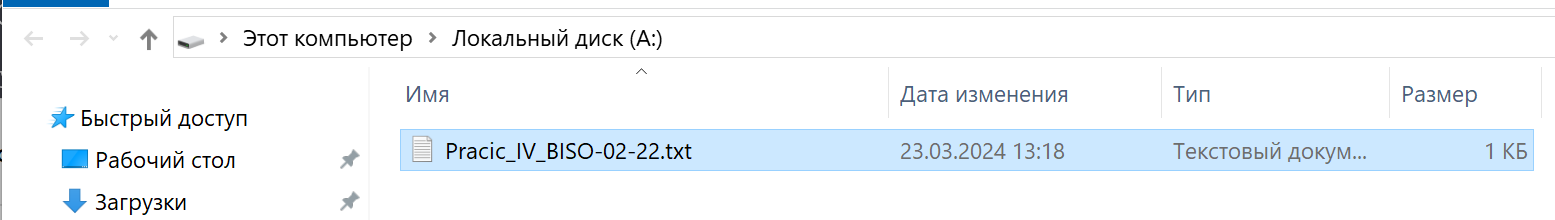


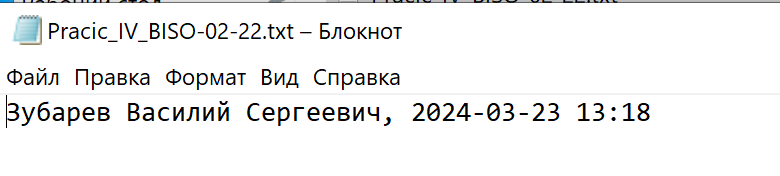






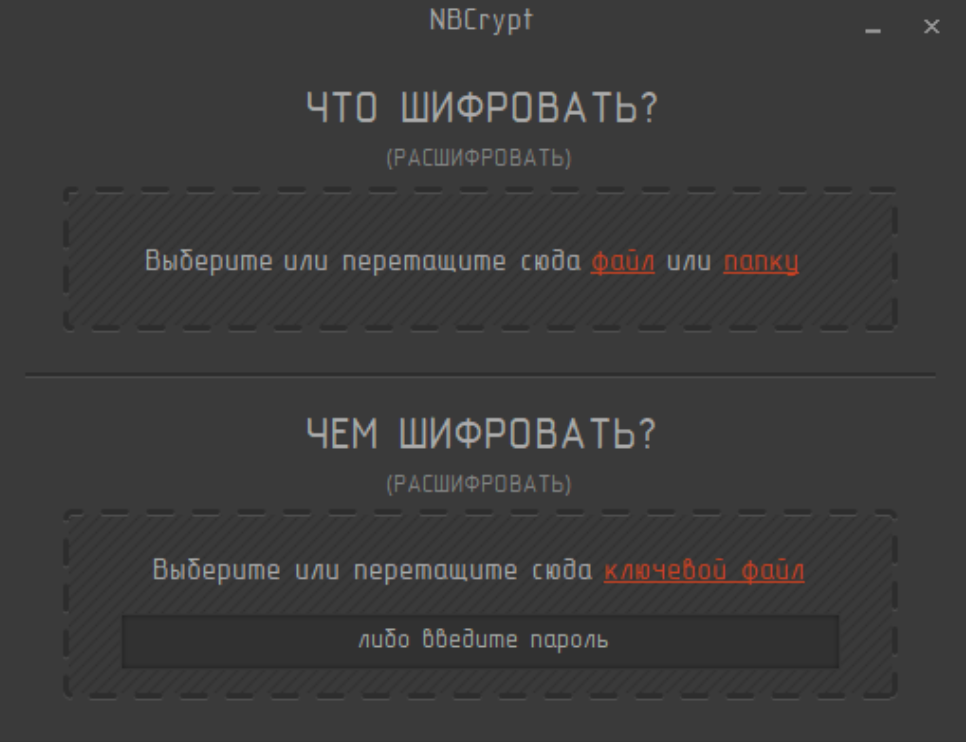




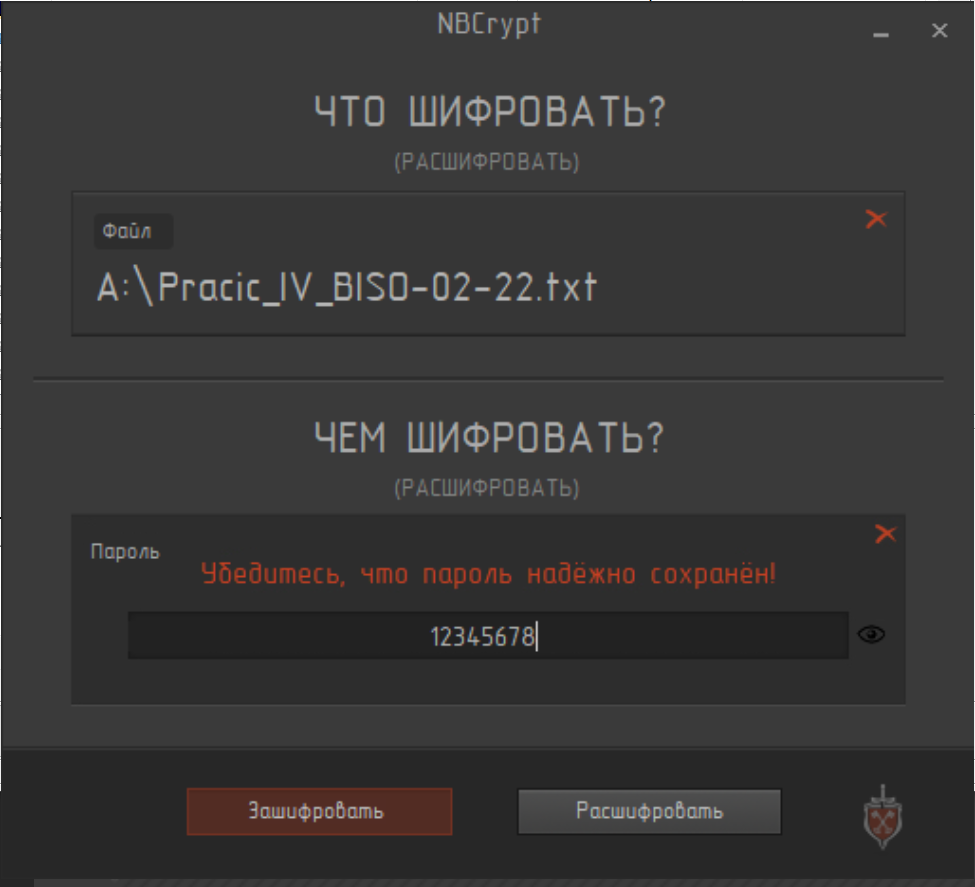


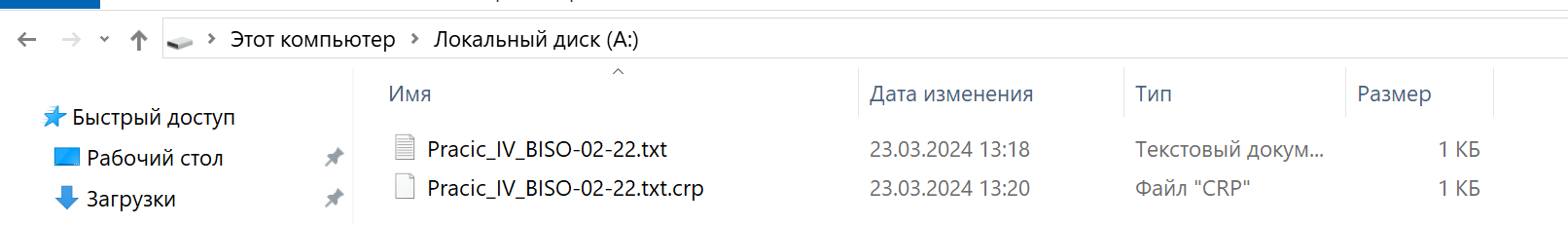
# Шифрование данных симметричным ключом с помощью программы NBCrypt

Запустите программу NBCrypt, размещенную на рабочем столе



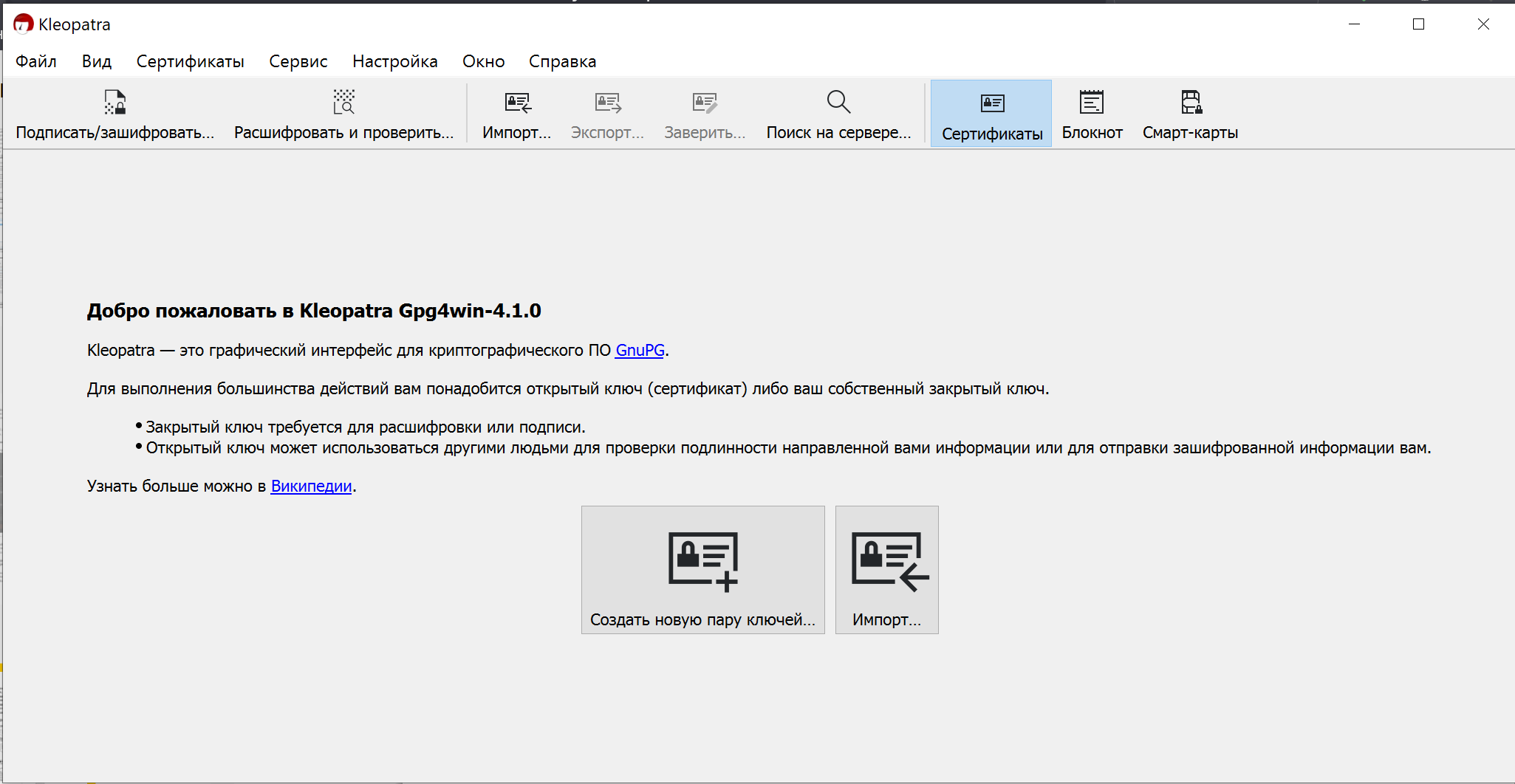
Зашифруйте файл, полученный в задании №1 с помощью программы NBCrypt с паролем «12345678». Должен появиться файл с аналогичным именем и расширением «.crp».



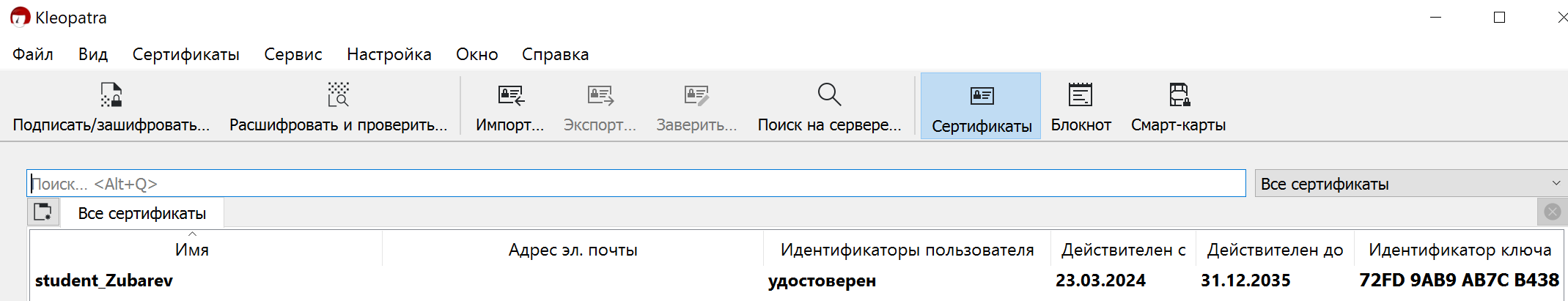


# Асимметричное шифрование данных и электронная подпись с помощью программы Gpg4win/Kleopatra.

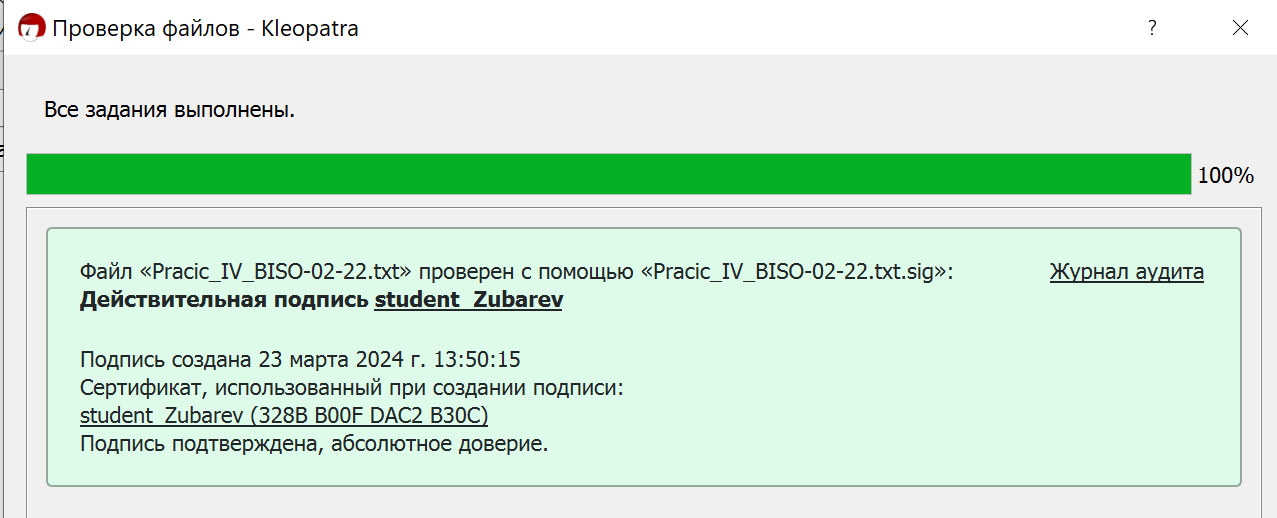
Запустите программу Kleopatra через ярлык на Рабочем столе



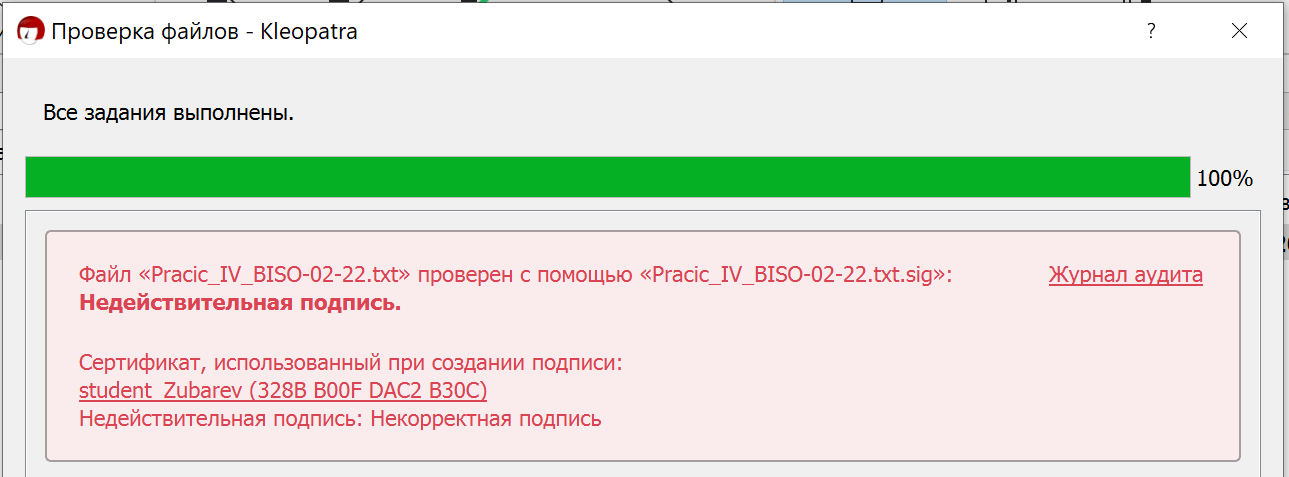
Создайте новую пару RSA-ключей с именем student\_ФИО для шифрования и подписи, размером 4096 бит и сроком действия до 31.12.2035.



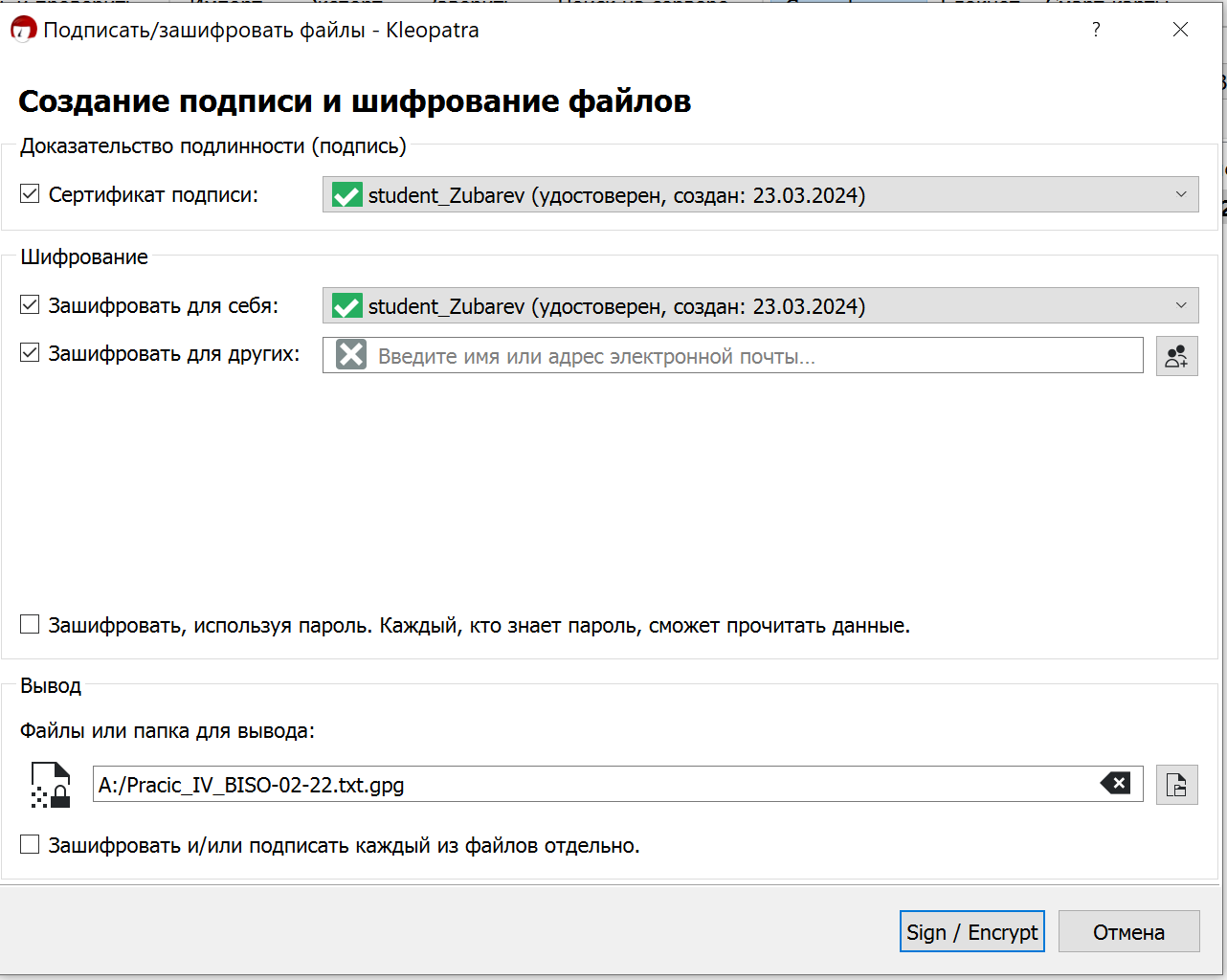
Проверьте подпись файла. Сохраните скриншот результата проверки в контейнер с именем «task3\_1.png».



Внесите изменения в исходный файл (добавьте пробел). Снова проверьте подпись файла. Сохраните скриншот результата проверки в контейнер с именем «task3\_2.png».

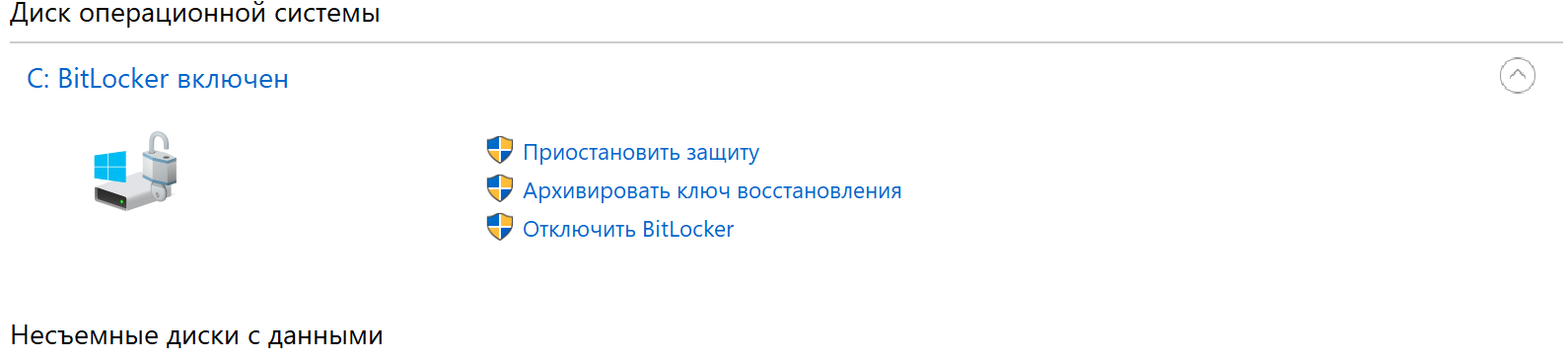


Зашифруйте исходный файл из Задания №1 для пользователя student\_NVS, открытый ключ которого уже находится в хранилище сертификатов, и результат сохраните в контейнере.



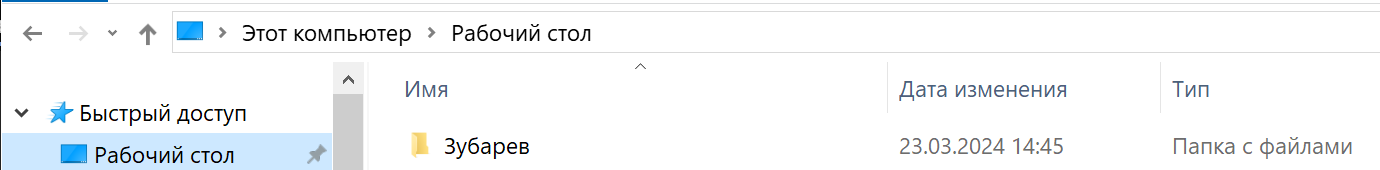
# Шифрование системного раздела ОС с помощью BitLocker.

BitLocker (точное название BitLockerDriveEncryption) – технология шифрования содержимого дисков компьютера, разработанная компанией Microsoft, впервые появившаяся в Windows Vista. С помощью BitLocker возможно было шифровать тома жестких дисков, но позже, уже в Windows 7 появилась похожая технология BitLockerToGo, которая предназначена для шифрования съемных дисков и флешек. Шифрование может быть включено из контекстного меню:

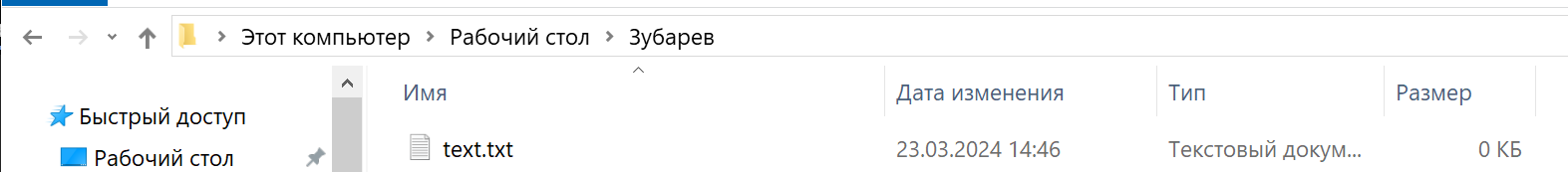


# Шифрование каталогов с помощью EFS

Создать на рабочем столе каталог с ФИО.



Разместить в каталоге любой файл.



Включить шифрование EFS для каталога с ФИО.

