Практические задания
(криптографические средства защиты информации)

Используемое программное обеспечение:
1. Veracrypt
2. NBCrypt
3. Win4gpg/Kleopatra
4. EFS (Win10)
5. Bitlocker (Win10)

Подготовительные мероприятия:
Импортировать и запустить виртуальную машину Practic4_crypto с операционной системой Windows 10 и необходимыми программами в VirtualBox.
Параметры входа в ОС Windows:
Username: student
Password: 12345678

Можно использовать Portable версии программ в базовой ОС без VirtualBox.

Задание 1. Сохранение данных в криптографическом контейнере VeraCrypt.

Шаг 1. Запустите программу VeraCrypt через ярлык на Рабочем столе операционной системы Windows 10 (рис. 1)

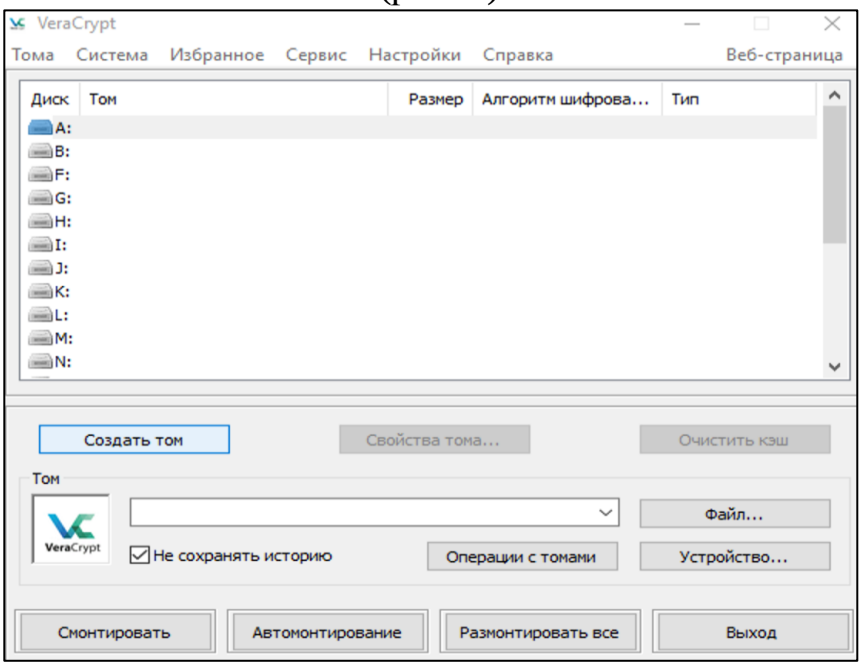


Рисунок 1 – Внешний вид интерфейса программы VeraCrypt

Шаг 2. 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.

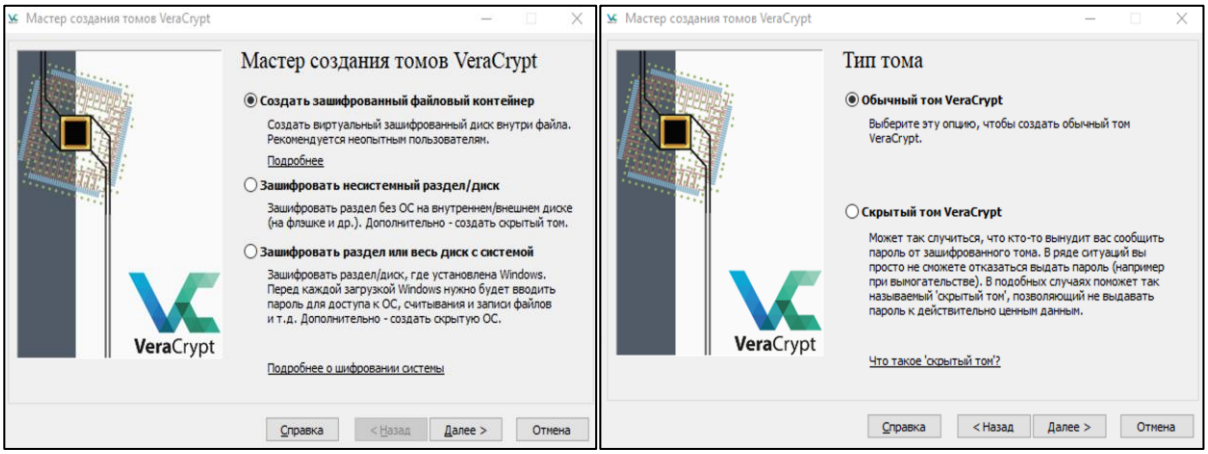


Рисунок 2 – Внешний вид мастера создания томов (тип)

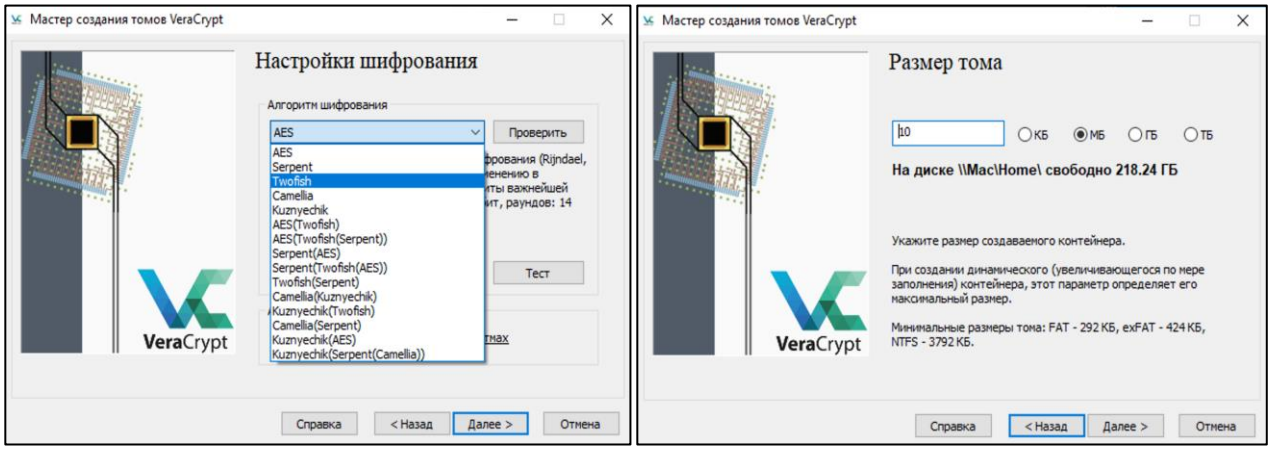


Рисунок 3 – Внешний вид мастера создания томов (шифр и размер)

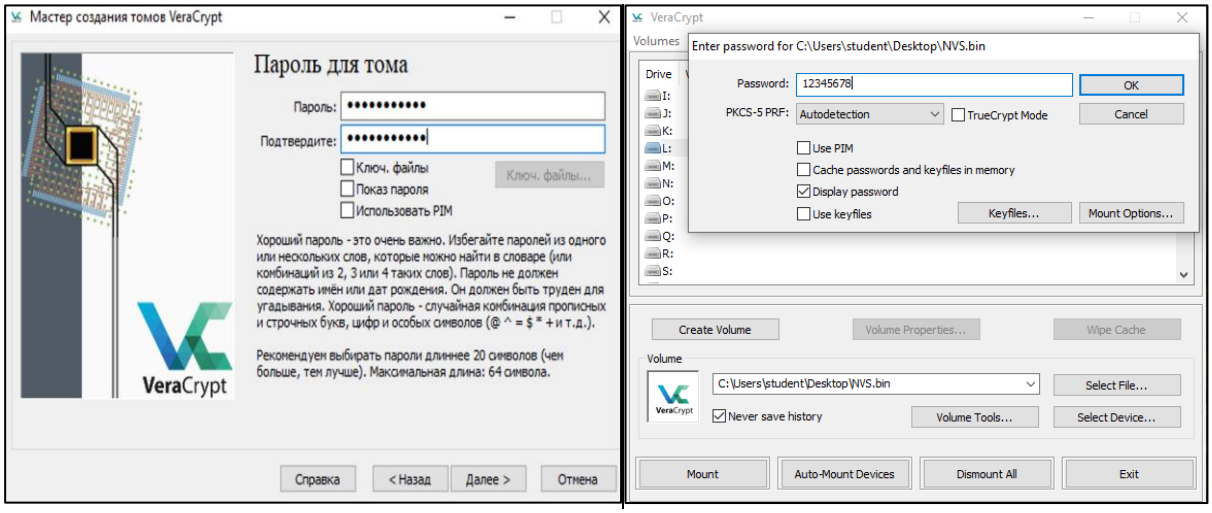


Рисунок 4 – Внешний вид мастера монтирования тома

Шаг 3. Примонтируйте том и создайте внутри него текстовый файл в кодировке UTF-8 с именем Practic_ФИО_Номер_группы.txt и запишите в него полные фамилию имя и отчество, а также текущую дату и время в формате YYYY-MM-DD hh:ss.

Например,

Practic_III_BISO-01-21.txt:

Иванов Иван Иванович, 2023-04-01 12:00

Задание 2. Шифрование данных симметричным шифром с помощью программы NBCrypt.

Шаг 1. Запустите программу NBCrypt, размещенную на рабочем столе.

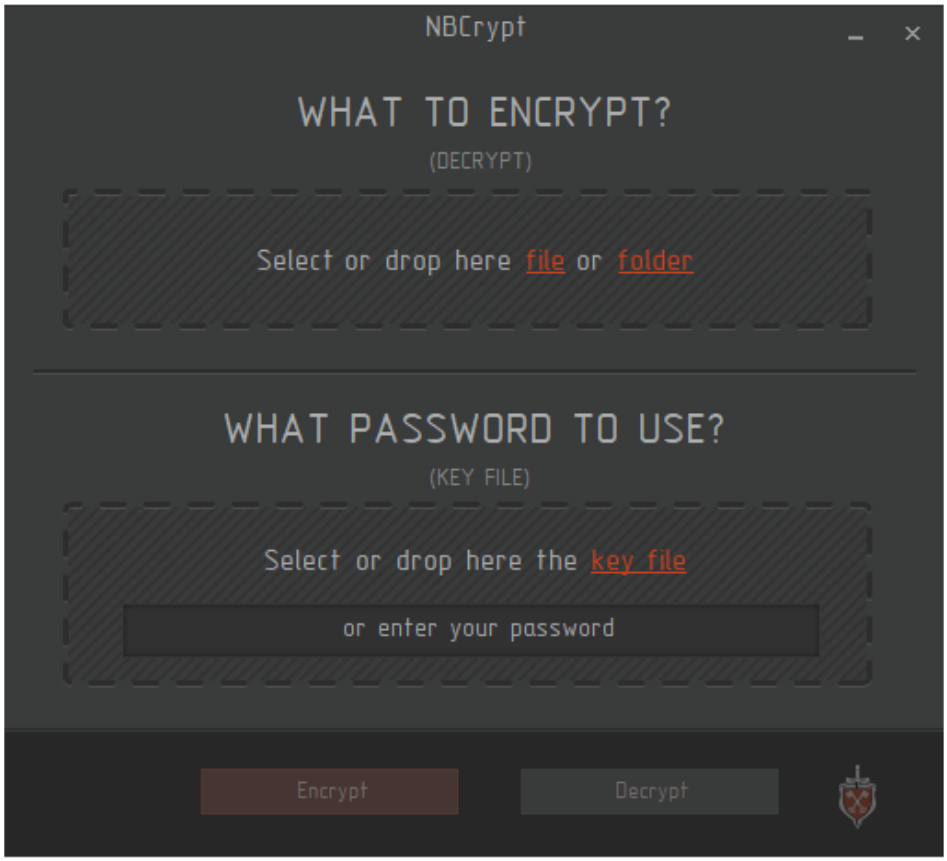


Рисунок 5 – Внешний вид программы NBCrypt

Шаг 2. Зашифруйте файл, полученный в задании №1 с помощью программы NBCrypt с паролем «12345678».

Должен появиться файл с аналогичным именем и расширением «.crp».

Задание 3. Асимметричное шифрование данных и электронная подпись с помощью программы Gpg4win/Kleopatra.

PGP (Pretty Good Privacy) – компьютерная программа, также библиотека функций, позволяющая выполнять операции шифрования и электронной подписи сообщений, файлов и другой информации, представленной в

электронном виде, в том числе прозрачное шифрование данных на запоминающих устройствах, например, на жёстком диске.

GNU Privacy Guard (GnuPG, GPG) – свободная программа для шифрования информации и создания электронных цифровых подписей. Разработана как альтернатива PGP и выпущена под свободной лицензией GNU General Public License. GnuPG полностью совместима со стандартом IETF OpenPGP. Текущие версии GnuPG могут взаимодействовать с PGP и другими OpenPGP-совместимыми системами.

Принцип работы GPG/PGP представлен на рисунке.

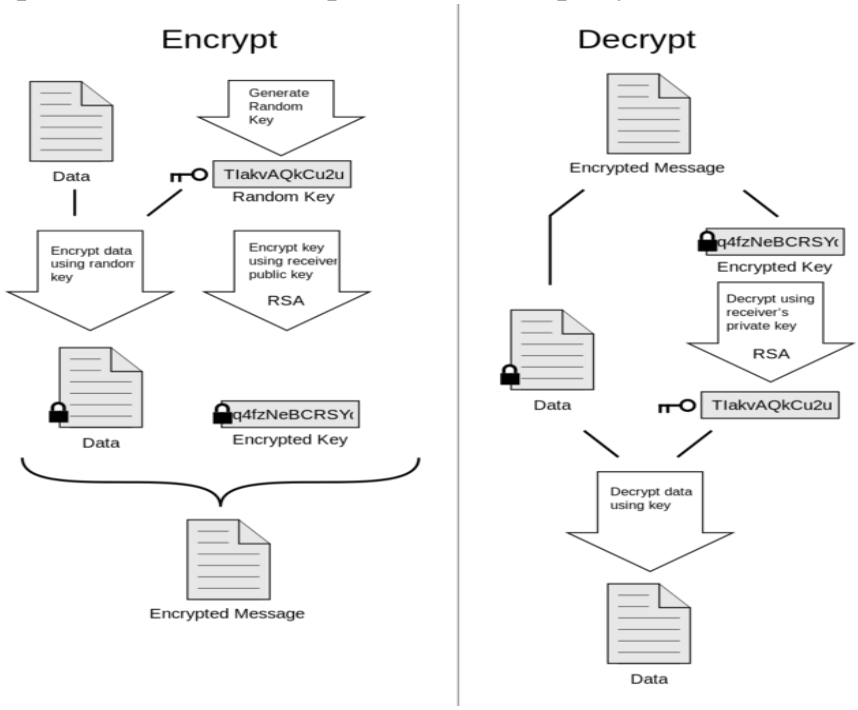


Рисунок 6 – Принцип работы PGP/GPG

В состав пакета GPG для ОС Windows входит программа с графическим интерфейсом – Kleopatra.

Шаг 1. Запустите программу Kleopatra через ярлык на Рабочем столе.

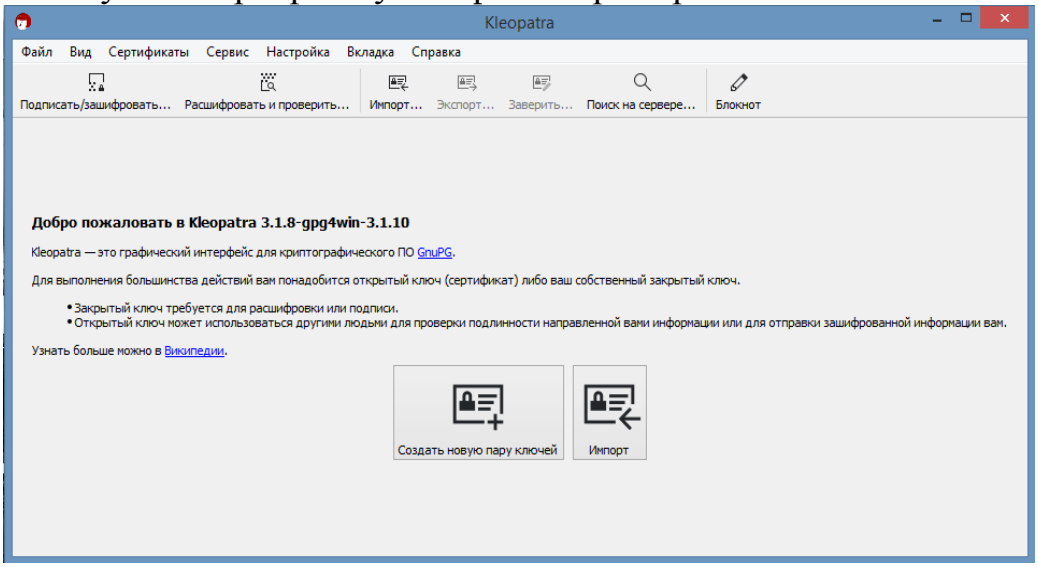


Рисунок 7 – Внешний вид программы Kleopatra

Шаг 2. Создайте новую пару RSA-ключей с именем student_ФИО для шифрования и подписи, размером 4096 бит и сроком действия до 31.12.2035.

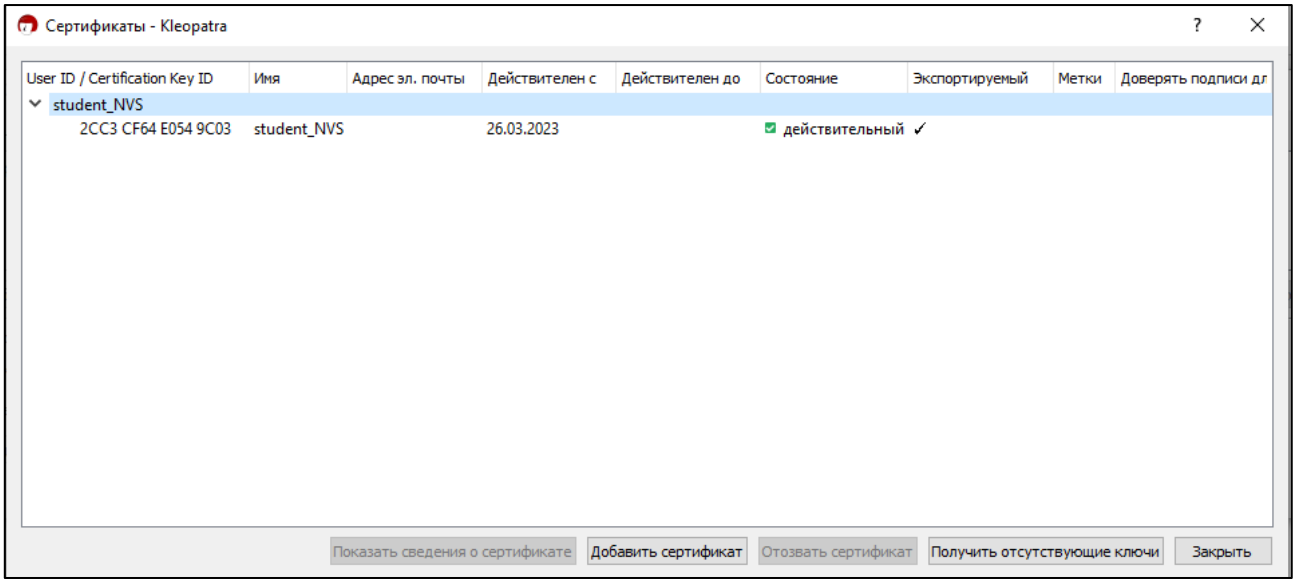


Рисунок 8 – Внешний вид программы Kleopatra

Шаг 3. Проверьте подпись файла.

Сохраните скриншот результата проверки в контейнер с именем «task3_1.png».

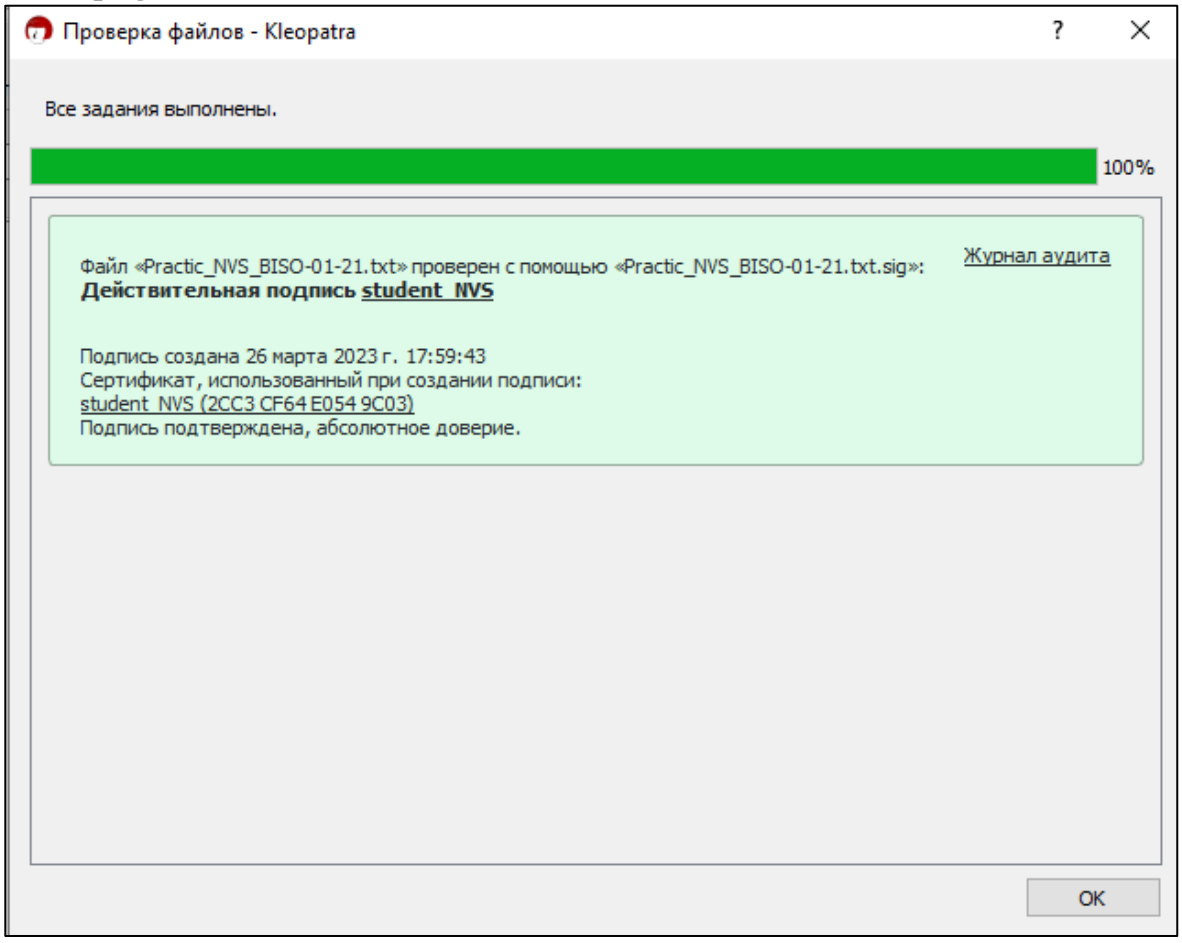


Рисунок 9 – Результат проверки цифровой подписи

Шаг 4. Внесите изменения в исходный файл (добавьте пробел). Снова проверьте подпись файла.

Сохраните скриншот результата проверки в контейнер с именем «task3_2.png».

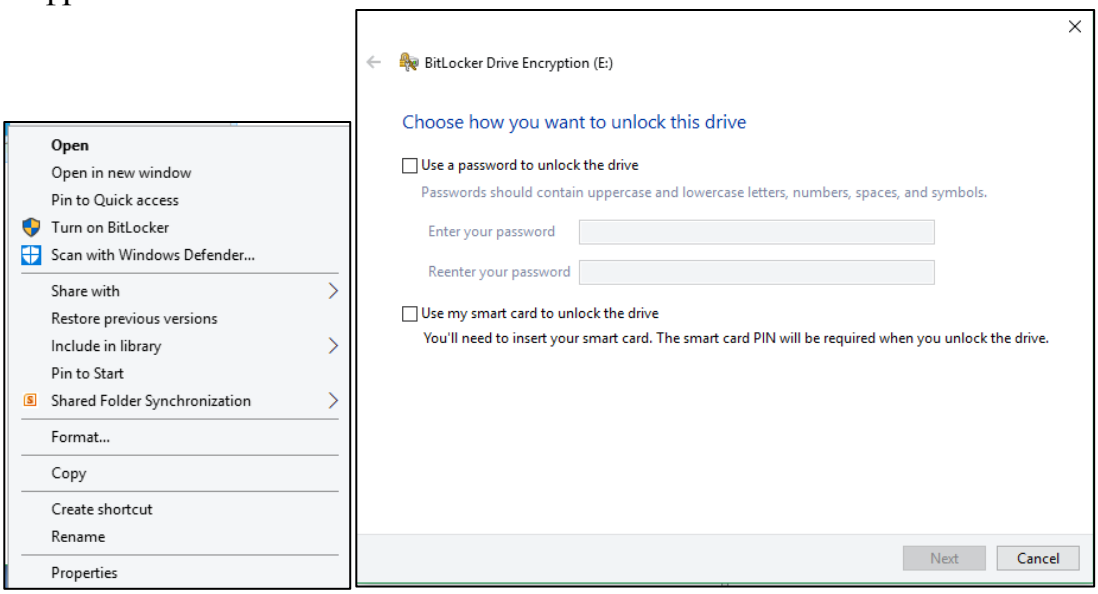
Шаг 5. Зашифруйте исходный файл из Задания №1 для пользователя student_NVS, открытый ключ которого уже находится в хранилище сертификатов, и результат сохраните в контейнере.

Задание 4. 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:



Шаг 1. Включить BitLocker для диска «C».

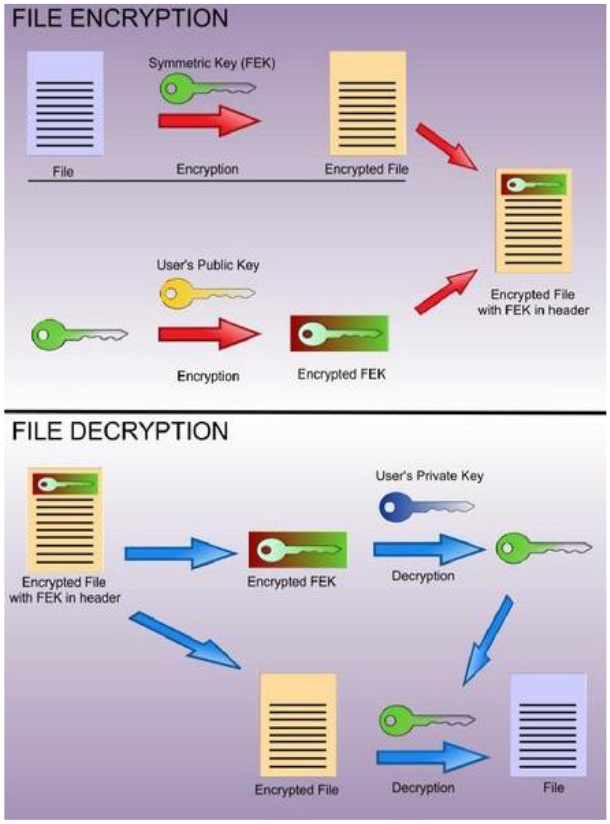
В виртуальной машине из-за недоступности модуля TPM использование BitLocker для шифрования системного диска не работает.

Сохраните в контейнер из задания №1 скриншот ошибки поиска TPM в виде файла task4_1.png.

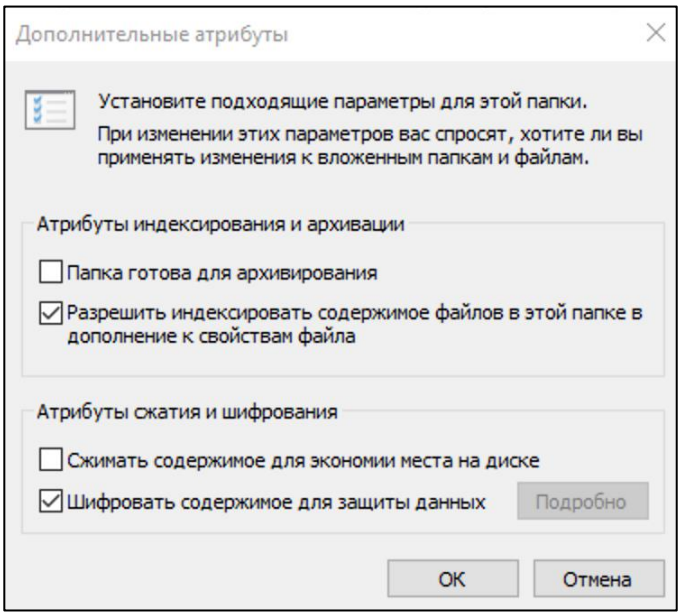
Задание 5. Шифрование каталогов с помощью EFS.

Encrypting File System (EFS) – система шифрования данных, реализующая шифрование на уровне файлов в операционных системах Microsoft WindowsNT (начиная с Windows 2000 и выше), за исключением «домашних» версий (Windows XP Home Edition, Windows Vista Basic, Windows Vista Home Premium, Windows 7 Starter (Home Basic и Premium), Windows 10 Pro, Enterprise, and Education editions, Windows Server 2016, Windows Server 2019.

Данная система предоставляет возможность «прозрачного шифрования» данных, хранящихся на разделах с файловой системой NTFS, для защиты потенциально конфиденциальных данных от несанкционированного доступа при физическом доступе к компьютеру и дискам.



Шифрование включается для каталога через контекстное меню «Свойства», далее в дополнительных атрибутах указывается соответствующая галочка.



Шаг 1. Создать на рабочем столе каталог с ФИО.

Шаг 2. Разместить в каталоге любой файл.

Шаг 3. Включить шифрование EFS для каталога с ФИО.

Шаг 4. Сделать скриншот каталога с замком.

Шаг 5. Разместить скриншот с именем task5_1.png в контейнере из задания № 1.

После выполнения всех заданий представить результат (контейнер) преподавателю.