

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

Факультет Информатика и вычислительная техника

Кафедра Кибербезопасность информационных систем

**ОТЧЕТ ПО ЛАБОРАТОРЫМ РАБОТАМ №10,11**

«Асимметричная криптография и электронная цифровая подпись на

примере системы GnuPG»

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Автор |  | |  | Заболотный И.А. | |
|  | (подпись, дата) | |  |  | |
| Обозначение | ИиВТ.10.05.01 | | Группа | | ВКБ21 |
| Направление подготовки | | 10.05.01 Компьютерная безопасность | | | |
| Профиль | Математические методы защиты информации | | | | |
| Дисциплина | Основы ИБ | |  |
|  |  | |  |
| Проверил(а) |  | |  | доцент, Бурякова О.С. | |
|  | (подпись, дата) | |  |  | |

Ростов-на-Дону

2023

Содержание

[Цель 3](#_Toc146184996)

[Задания 3](#_Toc146184997)

[Вывод 7](#_Toc146184998)

# Цель

ознакомиться с принципами криптографической защиты информации с использованием алгоритмов асимметричного шифрования и электронной цифровой подписи, приобрести навыки практического применения указанных методов защиты информации на основе системы GnuPG

# Задания

Первое задание заключается в том, чтобы создать пару ключей в менеджере ключей Cleopatra. (Рис. 1)

#### 

#### Рисунок 1

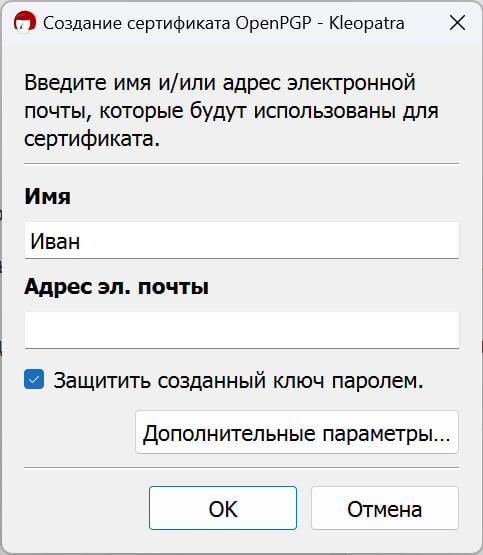
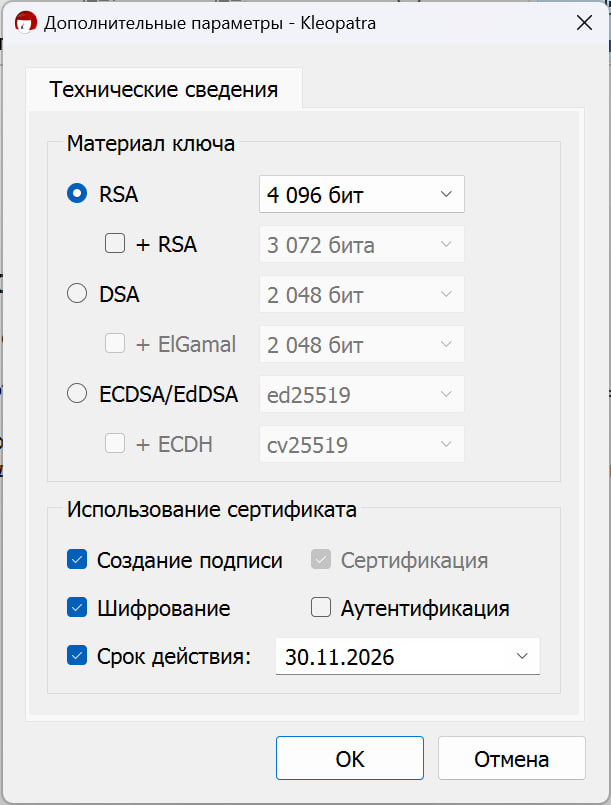


Рисунок 2

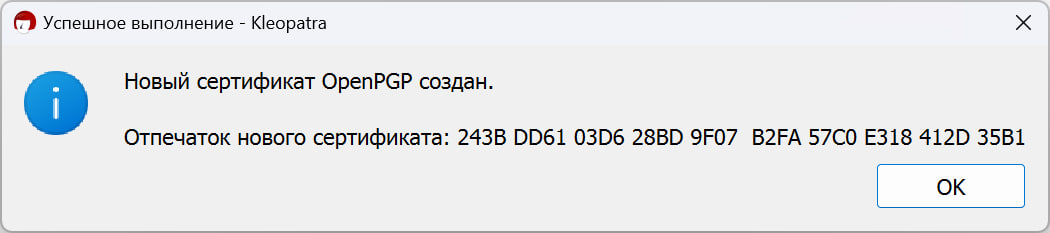
Вводим имя, которое будет использовано для сертификата. (Рис. 2)

Далее выбираем каким криптографическим алгоритмом будет зашифрован текст.



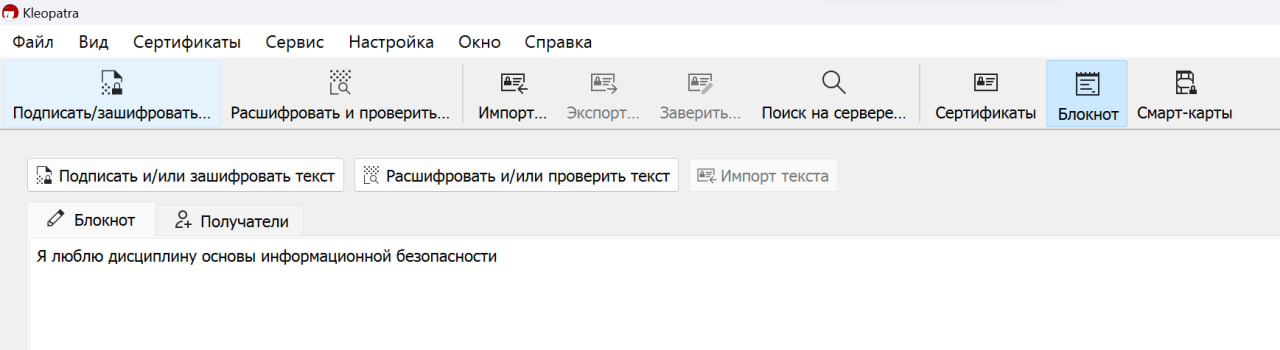
#### Рисунок 3

Нажимаем кнопку “OK”. Убеждаемся в том, что новый сертификат был создан. (Рис. 4)



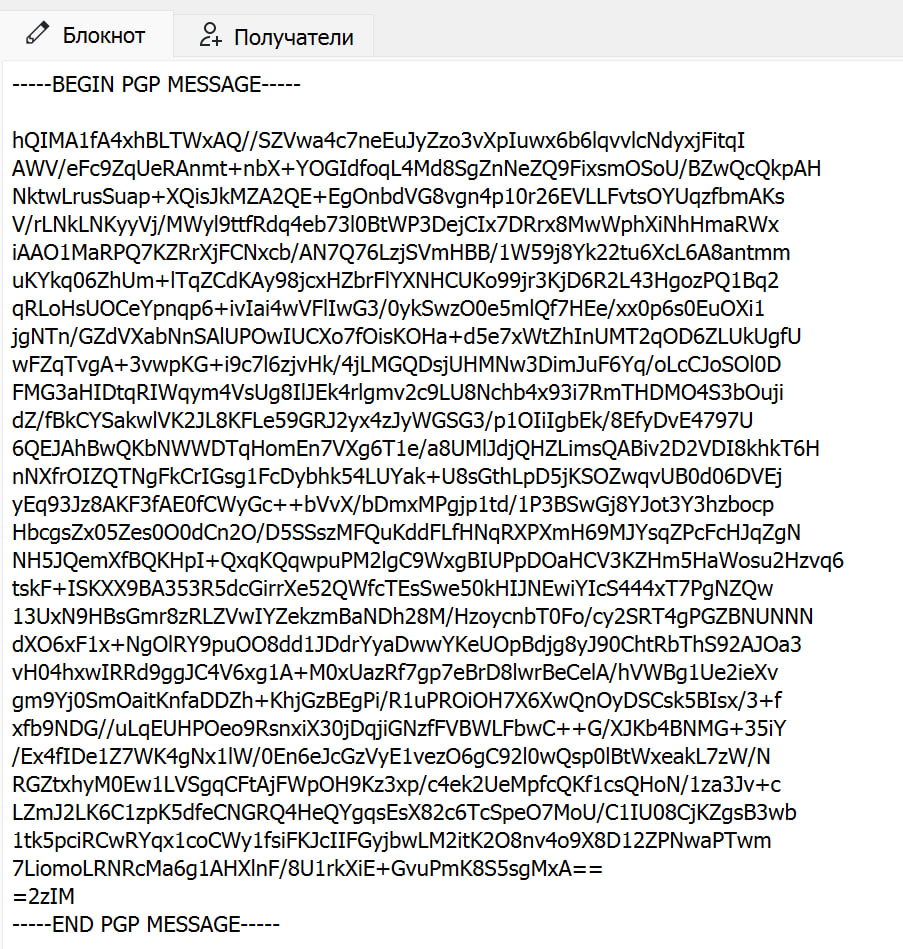
#### Рисунок 4

Следующее задание заключается в том, чтобы скопировать произвольный текст в буфер обмена. Зашифровать содержимое буфера обмена с помощью своего открытого ключа. Вставить содержимое буфера обмена в текстовый редактор, и убедится, что оно зашифровано. Для начала необходимо ввести в блокнот шифруемый текст и зашифровать (Рис. 5)



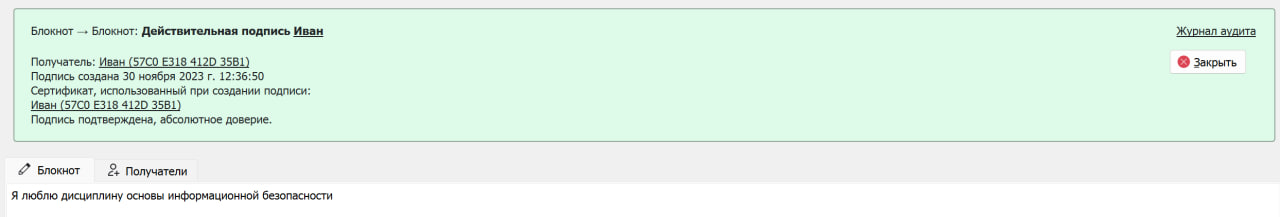
#### Рисунок 5

Далее необходимо убедиться, что оно зашифровано. (Рис. 6)



#### Рисунок 6

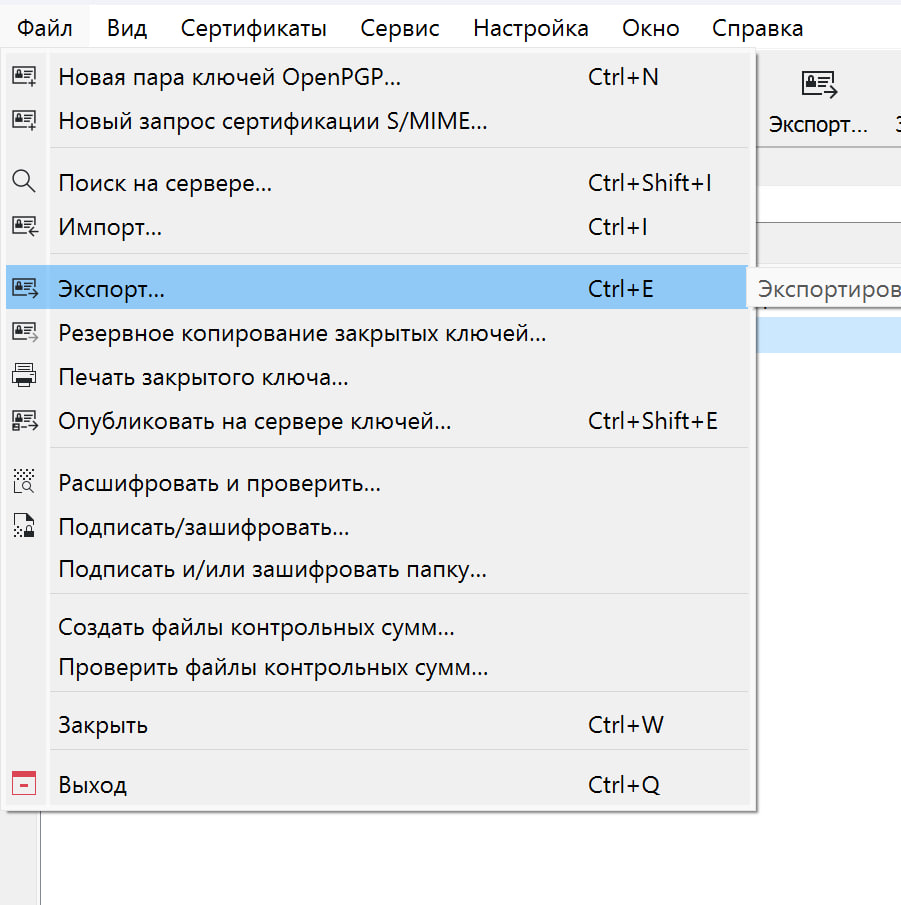
Теперь же нужно скопировать в буфер шифротекст, дешифровать его своим закрытым ключом, вновь вставить содержимое буфера обмена в текстовый редактор, и убедится, что текст был успешно расшифрован. Результат виден на Рис. 7



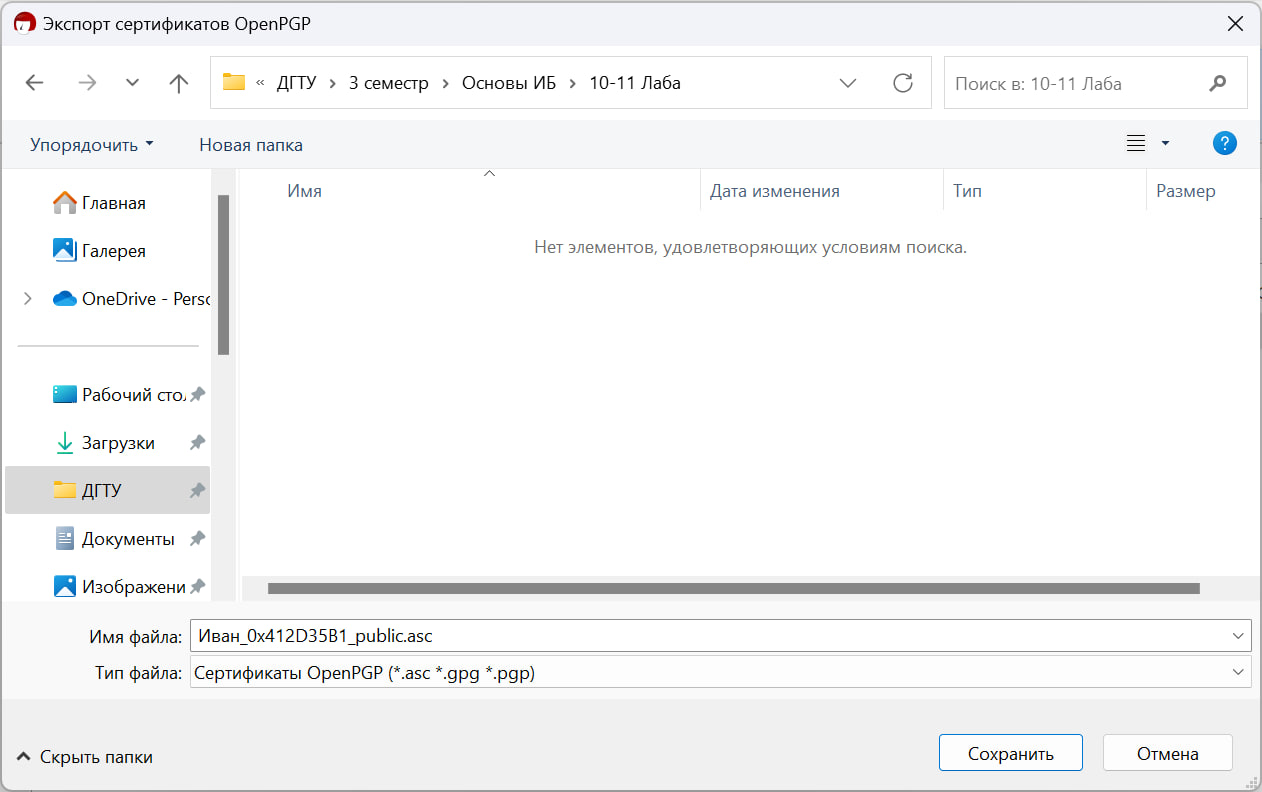
#### Рисунок 7

Следующее задание состоит в том, чтобы экспортировать сертификат открытого ключа из своей пары ключей в файл и передать его напарнику.

Первым делом надо экспортировать сертификат открытого ключа (Рис.8), предварительно сохранив его (Рис. 9).

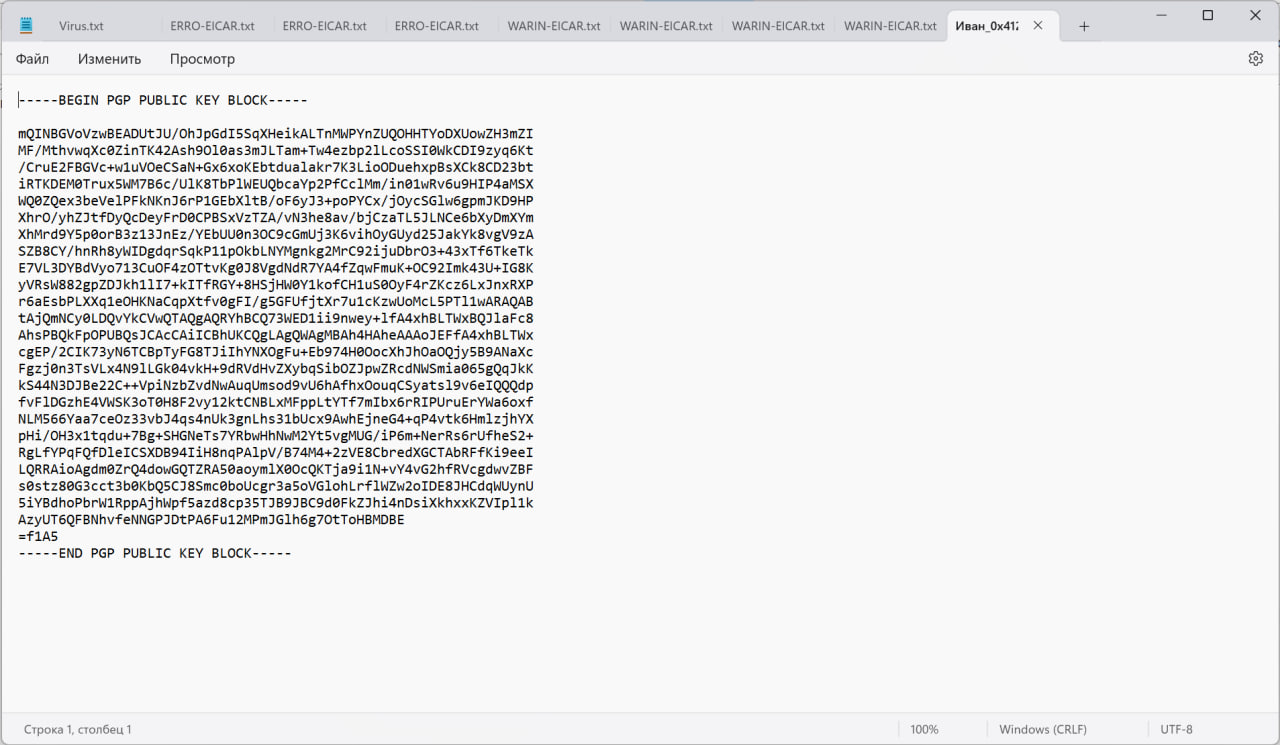


#### Рисунок 8



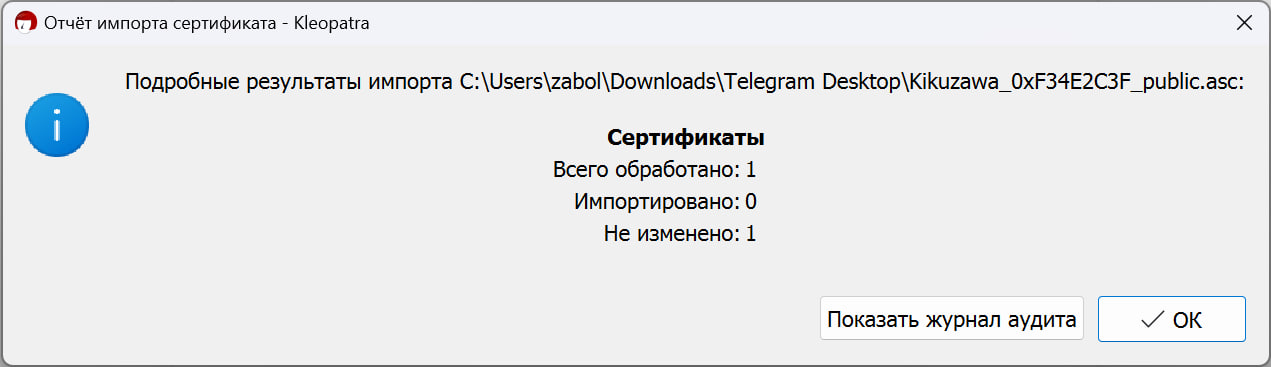
#### Рисунок 9

Проверяем, что текст зашифрован (Рис.10).



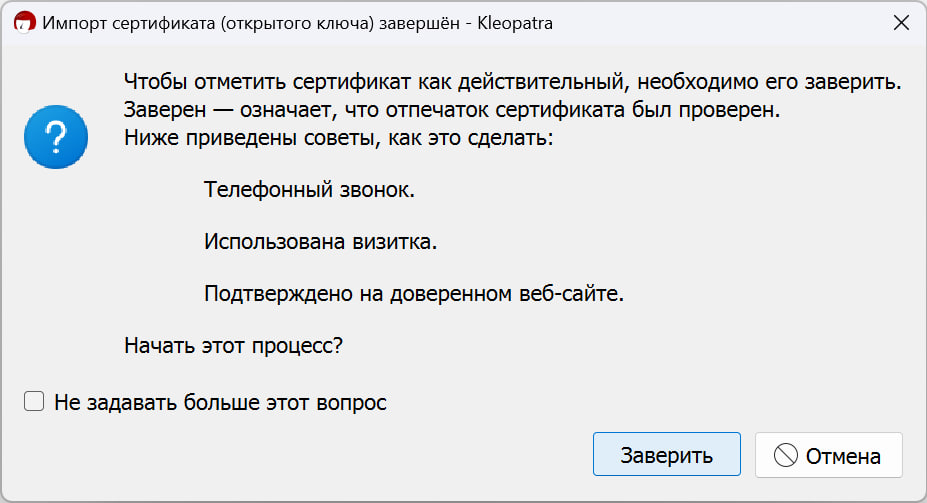
#### Рисунок 10

Далее, получив файл с экспортированным ключом от напарника, нужно импортировать его в менеджер ключей. Установить для импортированного ключа полное доверие. Поэтому импортируем файл напарника (Рис. 11)

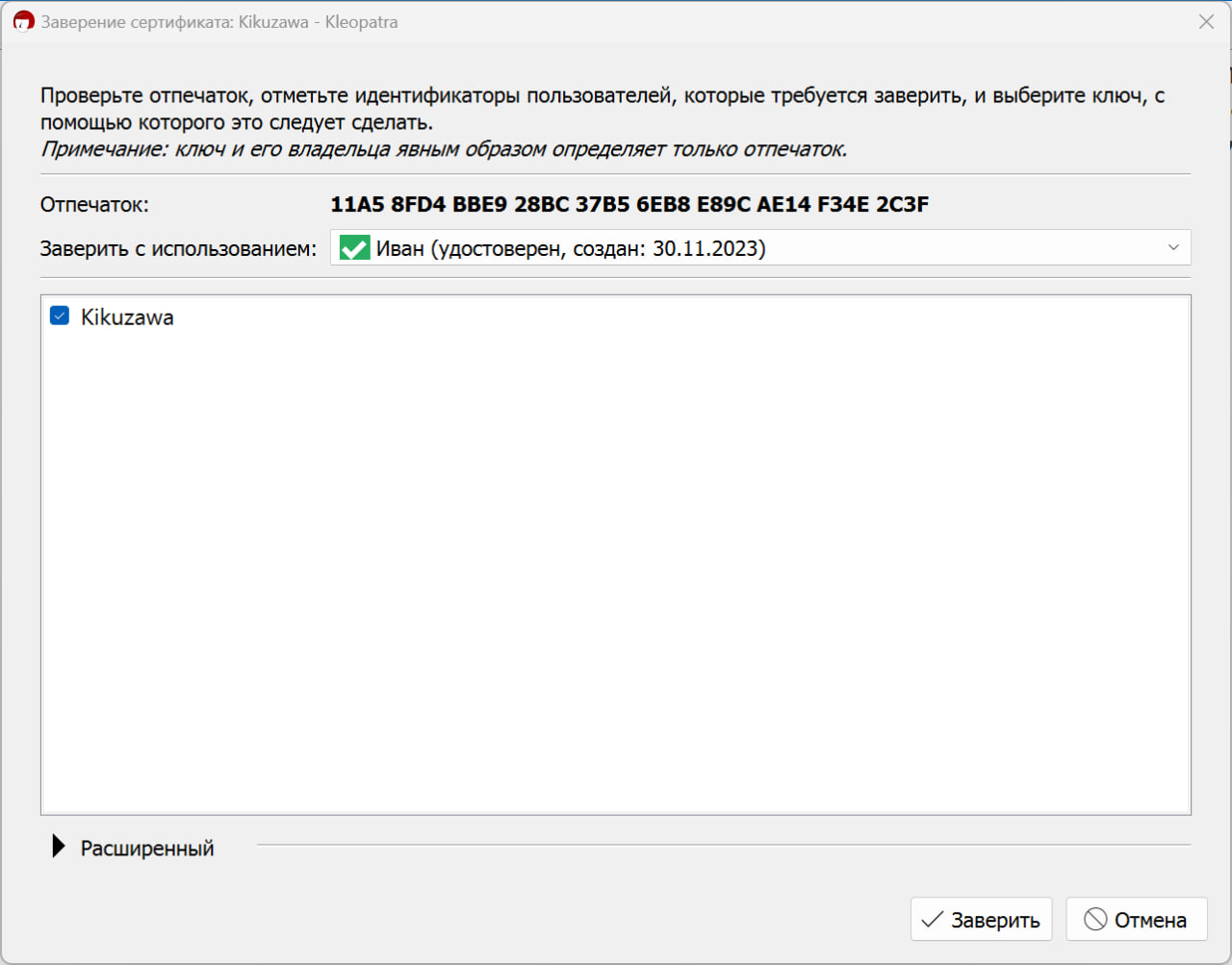


#### Рисунок 11

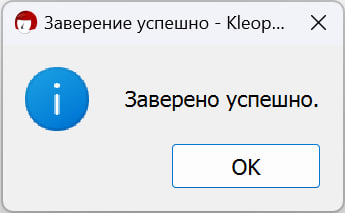
И заверяем полученный сертификат напарника (Рис. 12-14)



#### Рисунок 12



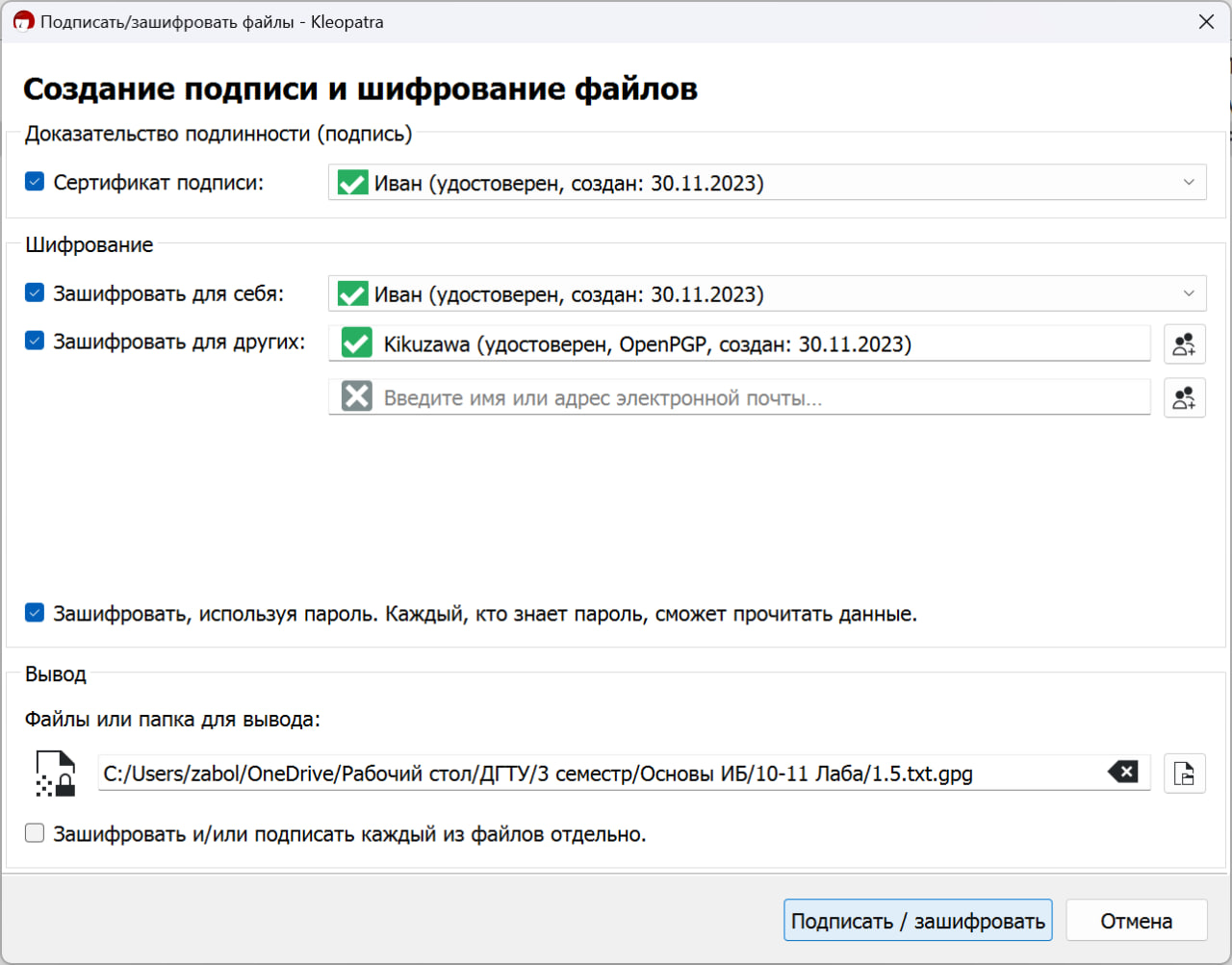
#### Рисунок 13



#### Рисунок 14

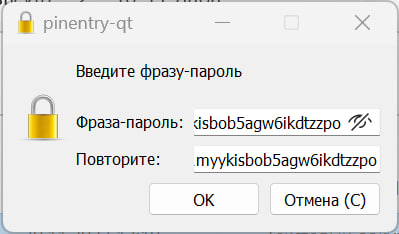
По требованию следующего задания необходимо зашифровать с использованием импортированного ключа напарника произвольный текст на диске. Передать зашифрованный текст напарнику.

Шифруем текст используя импортированный ключ напарника (Рис. 15).

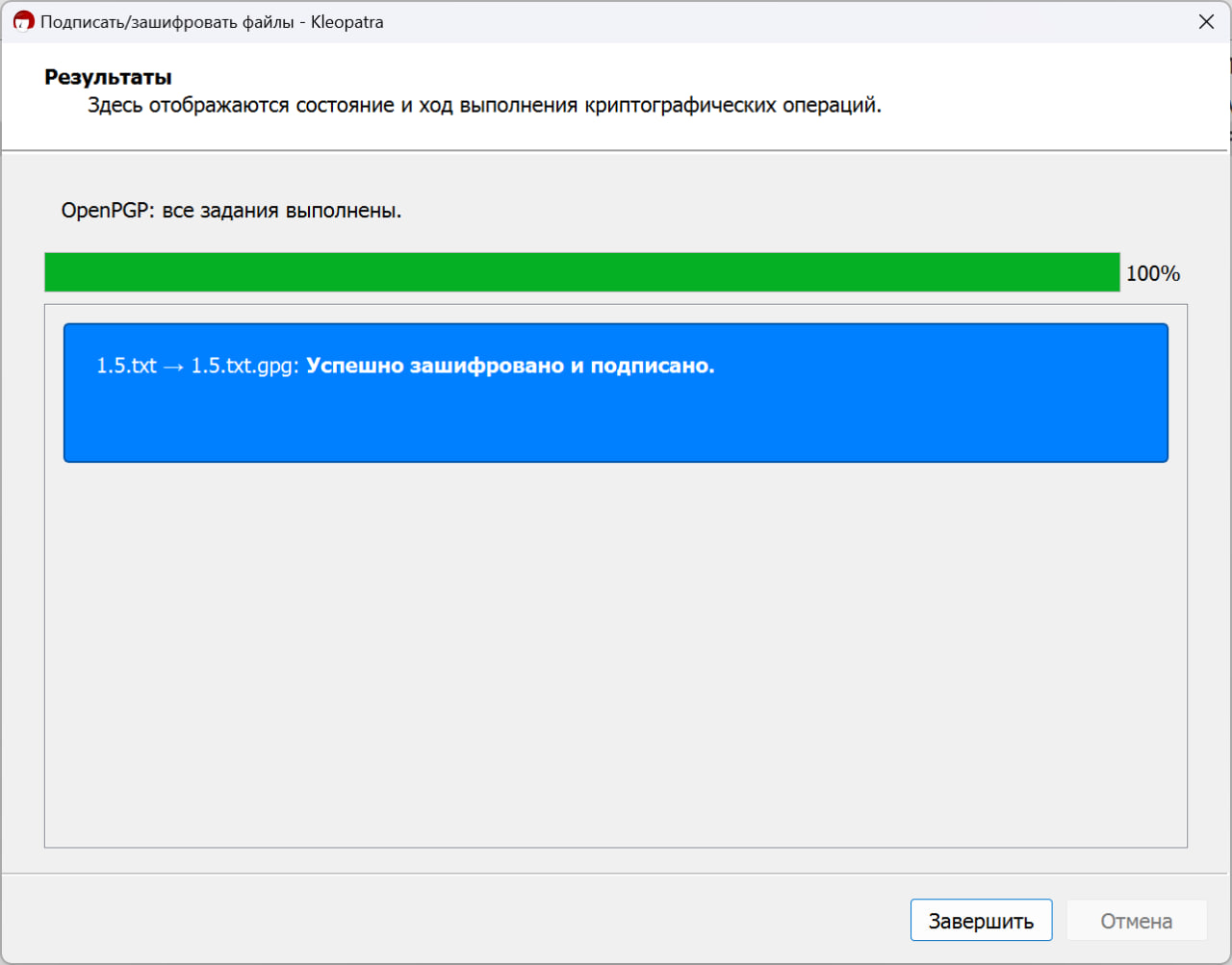


#### Рисунок 15

Вводим фразу-пароль и ожидаем (Рис. 16, Рис. 17)



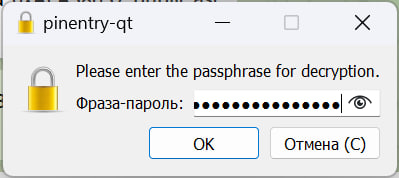
#### Рисунок 16



#### Рисунок 17

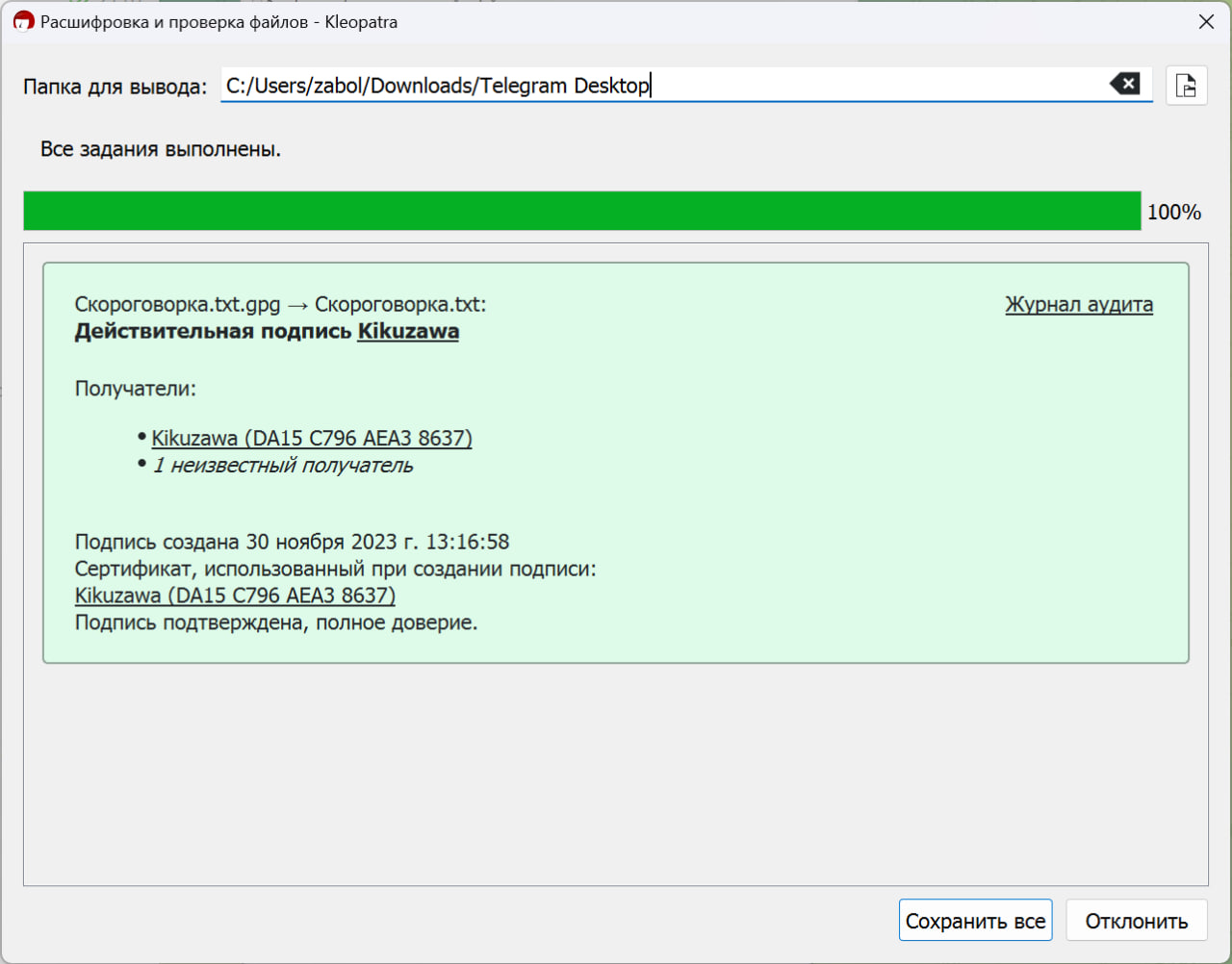
Далее по заданию получив зашифрованный файл от напарника, дешифровать его своим закрытым ключом. Убедится, что файл был успешно дешифрован.

Для этого нужно ввести закрытый ключ для дешифровки (Рис. 18).



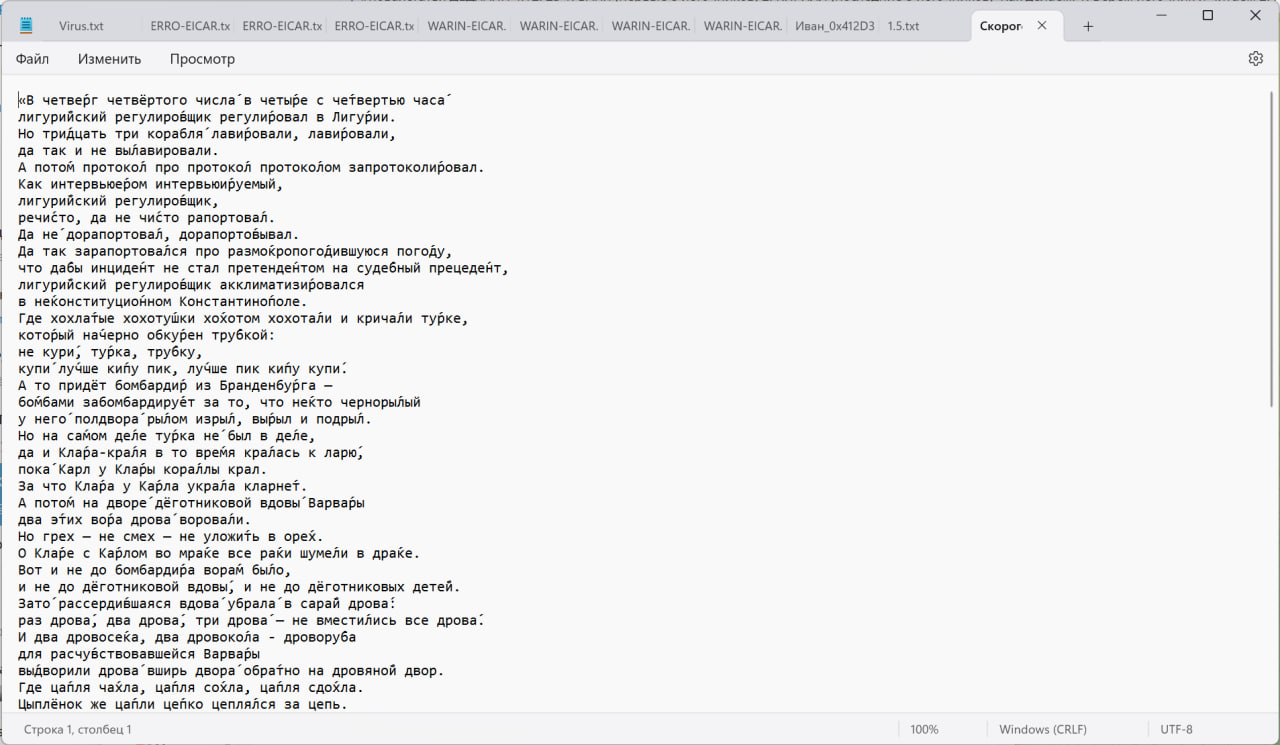
#### Рисунок 18

Далее необходимо ожидать процесс дешифровки. (Рис. 19).



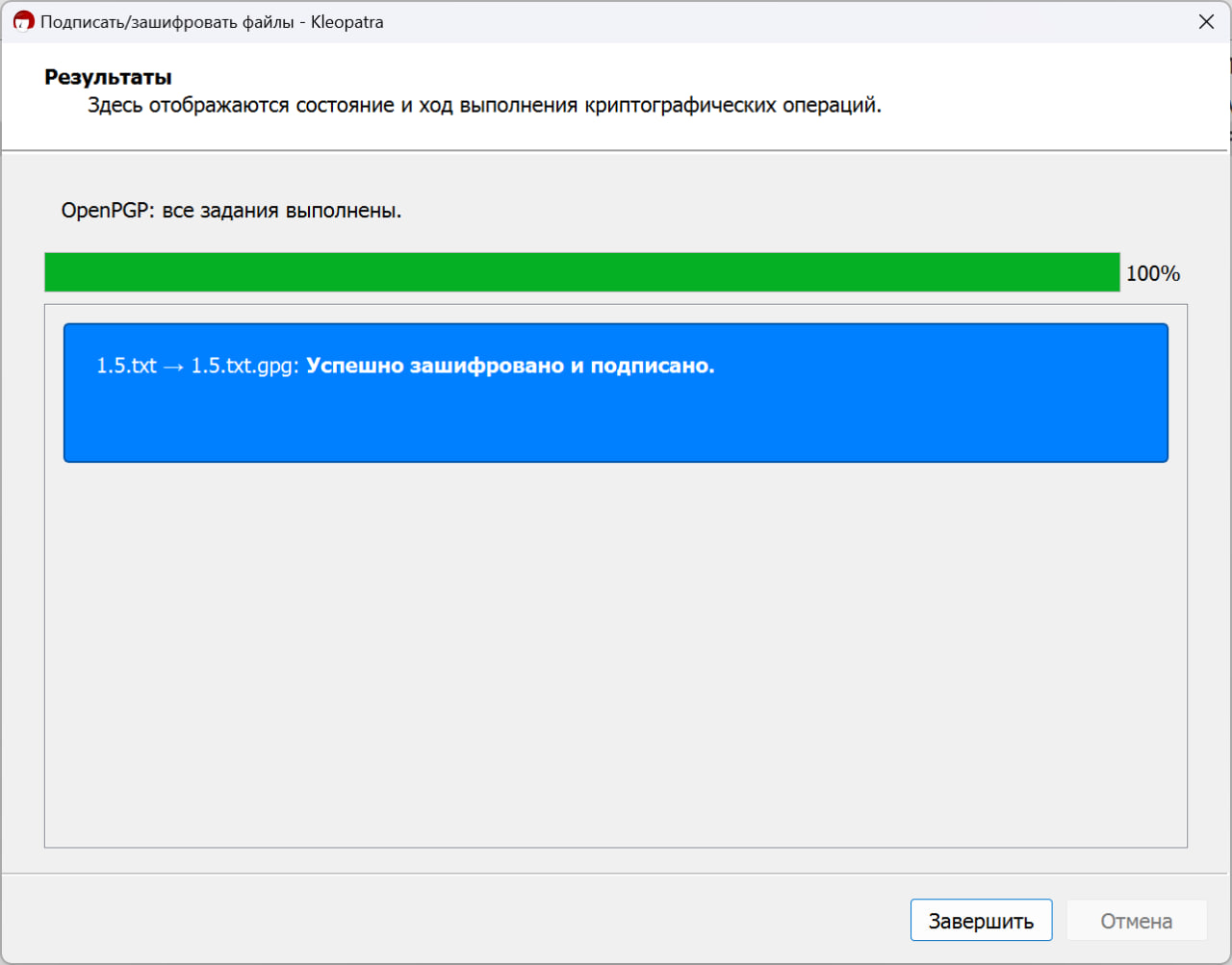
#### Рисунок 19

Проверим, что текст действительно был дешифрован (Рис. 20)



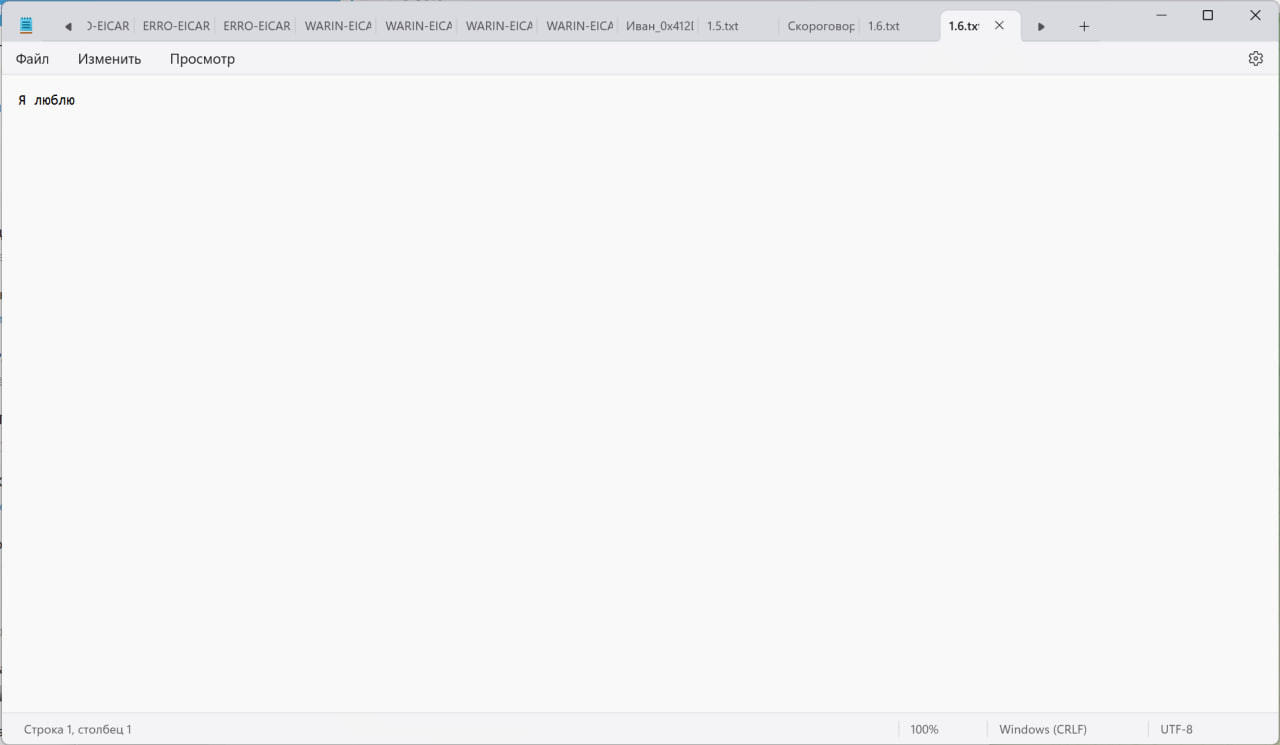
#### Рисунок 20

В следующем задании нужно, используя свой закрытый ключ, подписать произвольный файл на диске электронной подписью. И передать подписанный документ вместе с подписью напарнику. (Рис. 21)

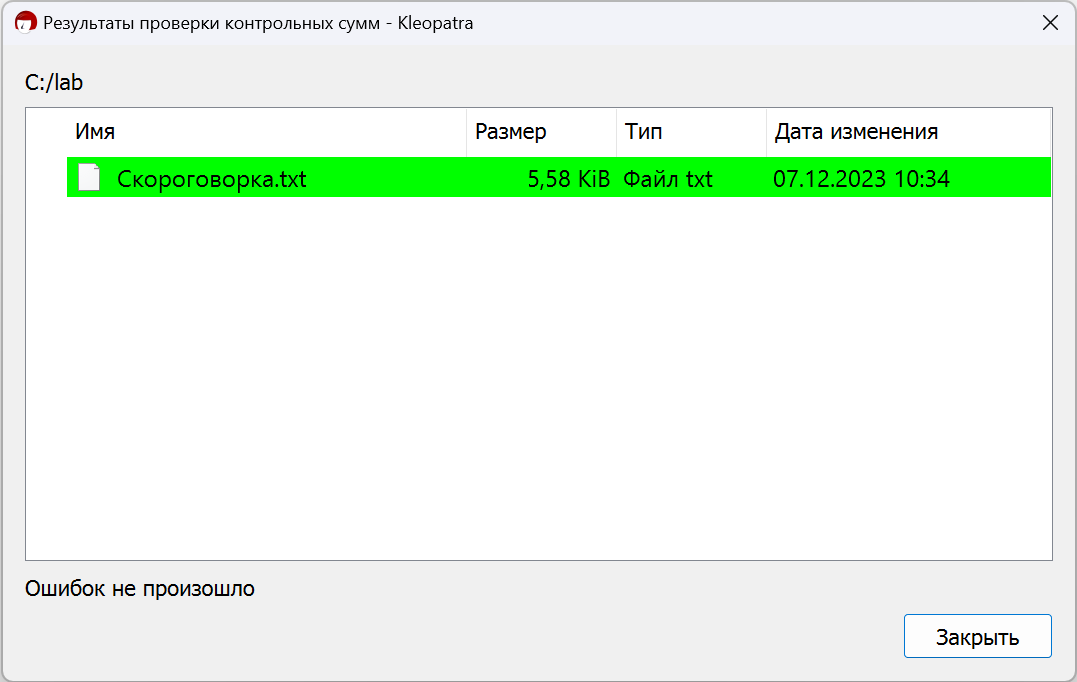


#### Рисунок 21

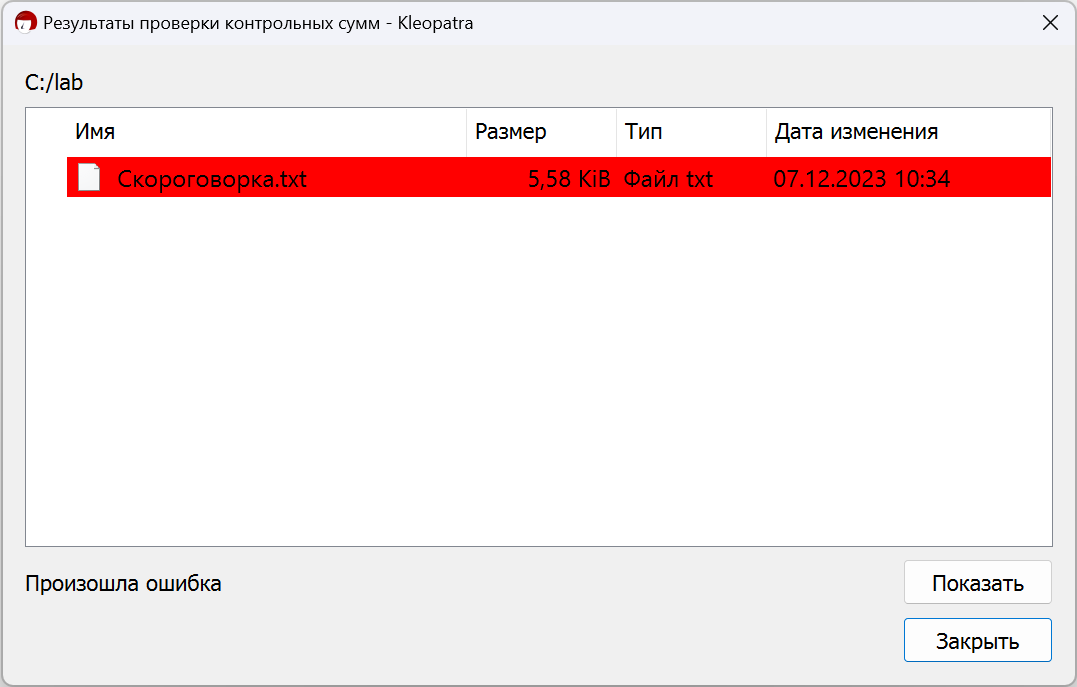
Получив от напарника документ с подписью, убедитесь, что подпись верна. Измените подписанный документ и убедитесь, что подпись стала неверна. Верните документ к первоначальному состоянию и вновь убедитесь, что подпись верна. (Рис. 22-25)



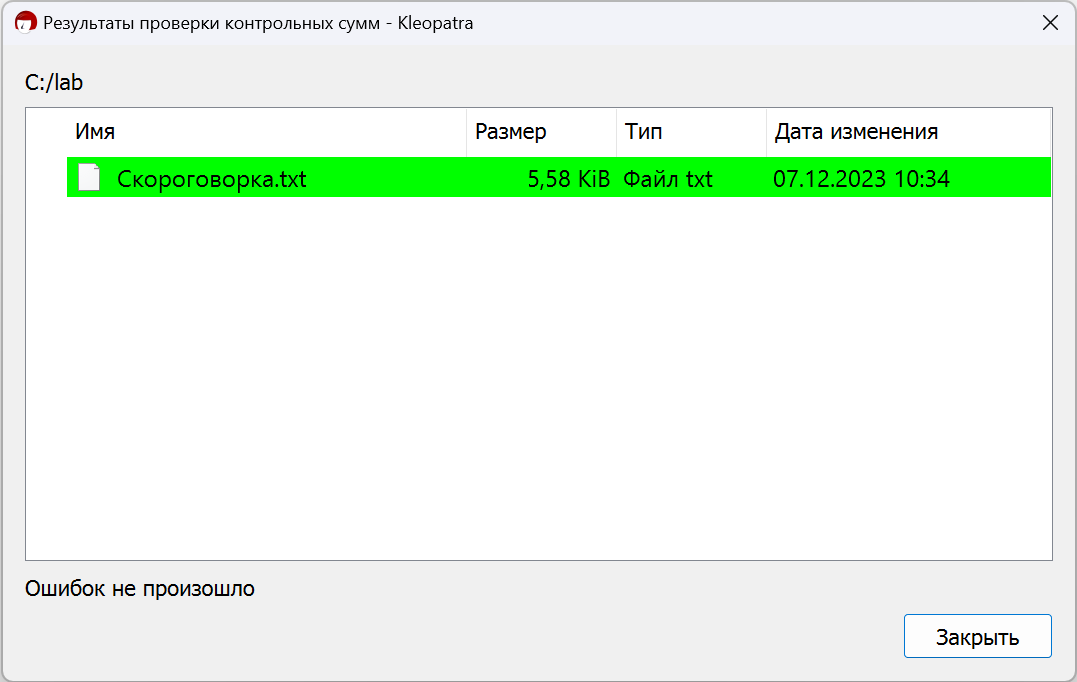
#### Рисунок 22



#### Рисунок 23



#### Рисунок 24



#### Рисунок 25

# Вывод

Я ознакомился с принципами криптографической защиты информации с использованием алгоритмов асимметричного шифрования и электронной цифровой подписи, а также приобрел практические навыки практического применения указанных методов защиты информации на основе системы GnuPG.