

**Министр науки и высшего образования Российской
Федерации**

**Федеральное государственное автономное
образовательное учреждение высшего образования**

«Национальный исследовательский университет ИТМО»

Факультет информационных технологий и программирования

Лабораторная работа №2

Криптография

Выполнили студенты группы № М34041

Титов Даниил Ярославович
Иванов Алексей Александрович
Иванов Сергей Андреевич

Проверил:

Батоцыренов Павел Андреевич

Санкт-Петербург

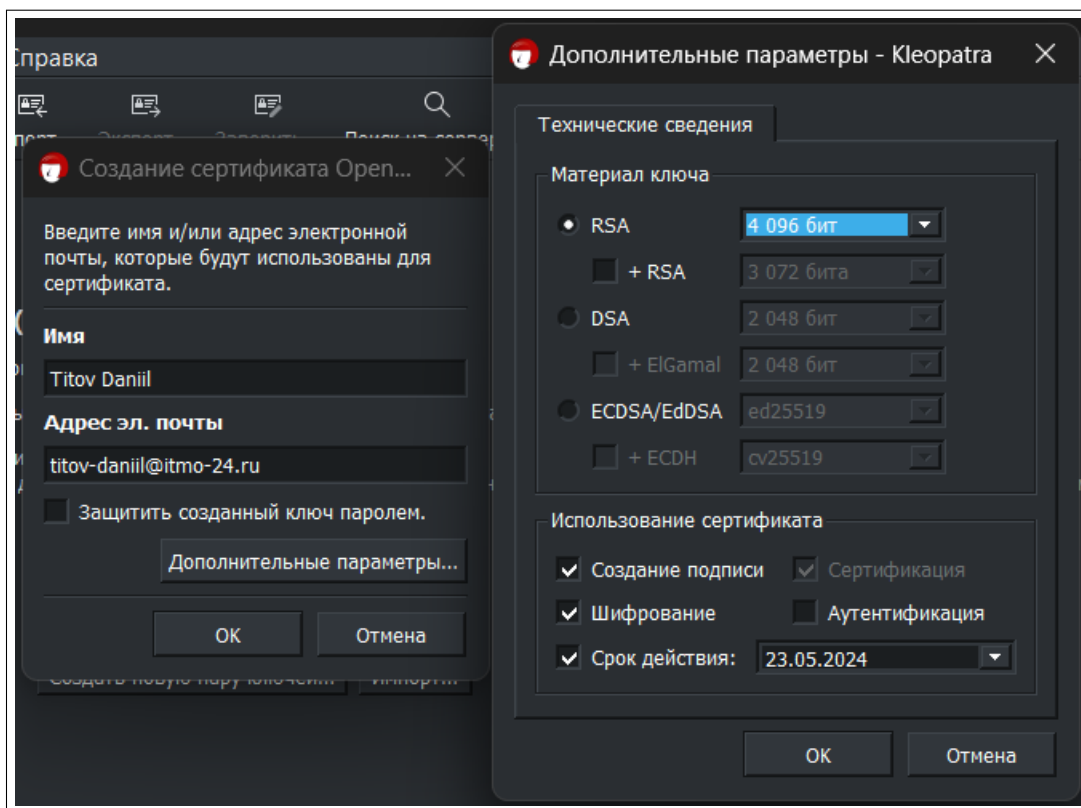
2024

Содержание

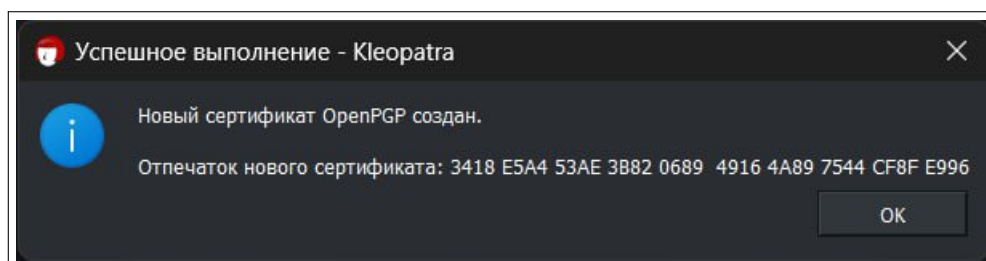
1	Создание ключевой пары	3
1.1	Создайте пару ключей RSA, которыми можно подписывать и шифровать файлы. Длину ключа укажите 4096 бит. Время жизни 3 месяца.	3
1.2	Запомните fingerprint своего публичного ключа.	3
1.3	Опубликуйте свой ключ на сервере ключей.	4
2	Шифрованный обмен	5
2.1	Узнайте fingerprint публичного ключа своего коллеги, которому Вы будете отправлять сообщение.	5
2.2	Создайте текстовый файл с секретным сообщением -> Зашифруйте файл и передайте шифрованный файл	6
2.3	Примите зашифрованный файл, который предназначается Вам и расшифруйте его с помощью своего ключа.	7
3	Электронная подпись	8
3.1	Создайте текстовый файл со списком дел на день -> Подпишите файл своей подписью	8
3.2	Примите файл и подпись от своего коллеги.	9
3.3	Сверьте подпись.	9
3.4	Внесите изменения в файл, сохраните и снова сверьте подпись.	10
4	Вопросы к защите	11
4.1	Какой ключ нужно использовать для шифрования файлов?	11
4.2	Какой ключ нужно использовать для подписывания файлов?	11
4.3	Предложите своё решение задачи, когда один документ должны подписать несколько человек. Например, PDF-файл с договором купли-продажи, который должны подписать продавец и покупатель.	11

1 Создание ключевой пары

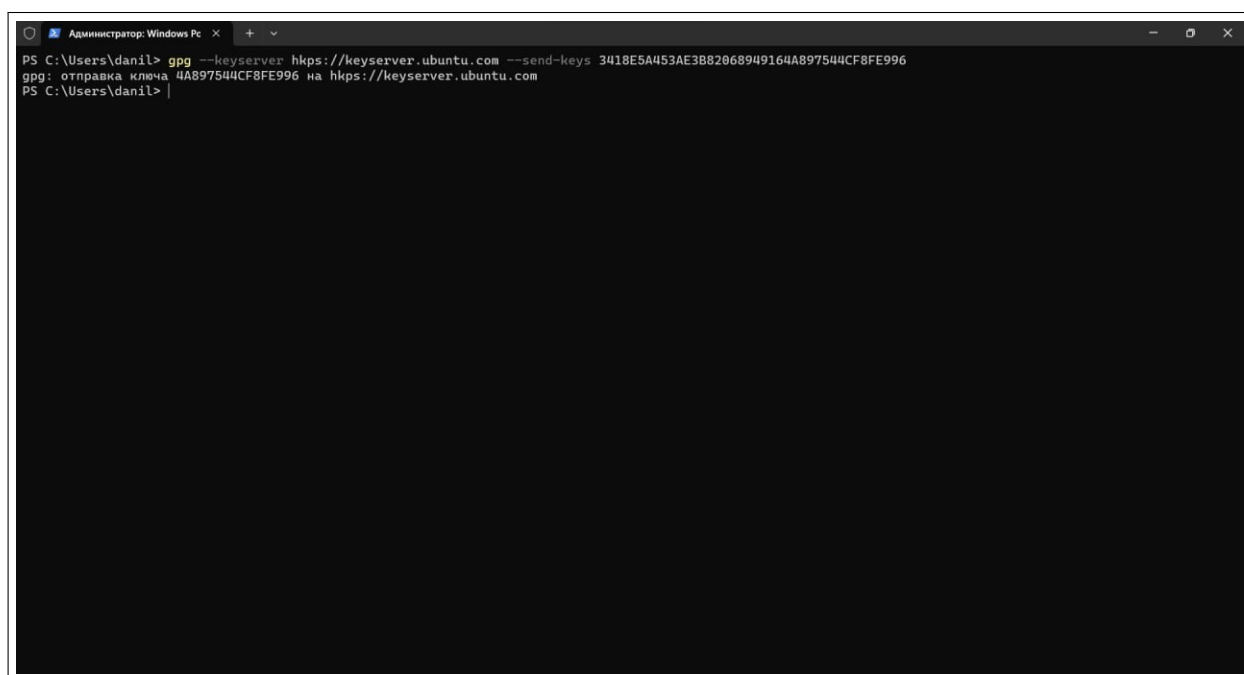
- 1.1 Создайте пару ключей RSA, которыми можно подписывать и шифровать файлы. Длину ключа укажите 4096 бит. Время жизни 3 месяца.



- 1.2 Запомните fingerprint своего публичного ключа.



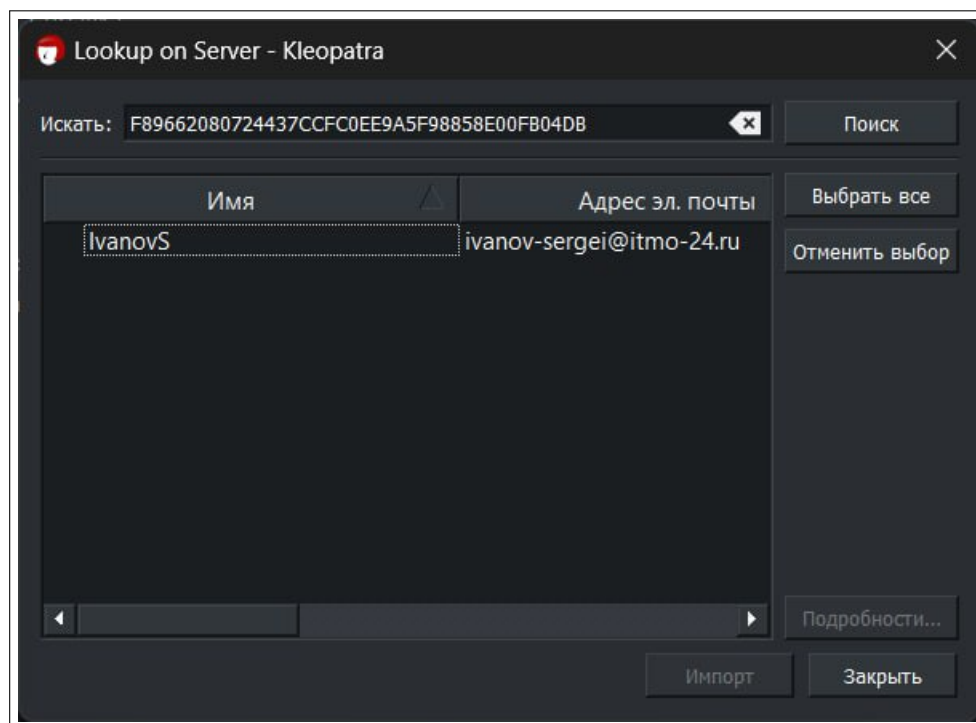
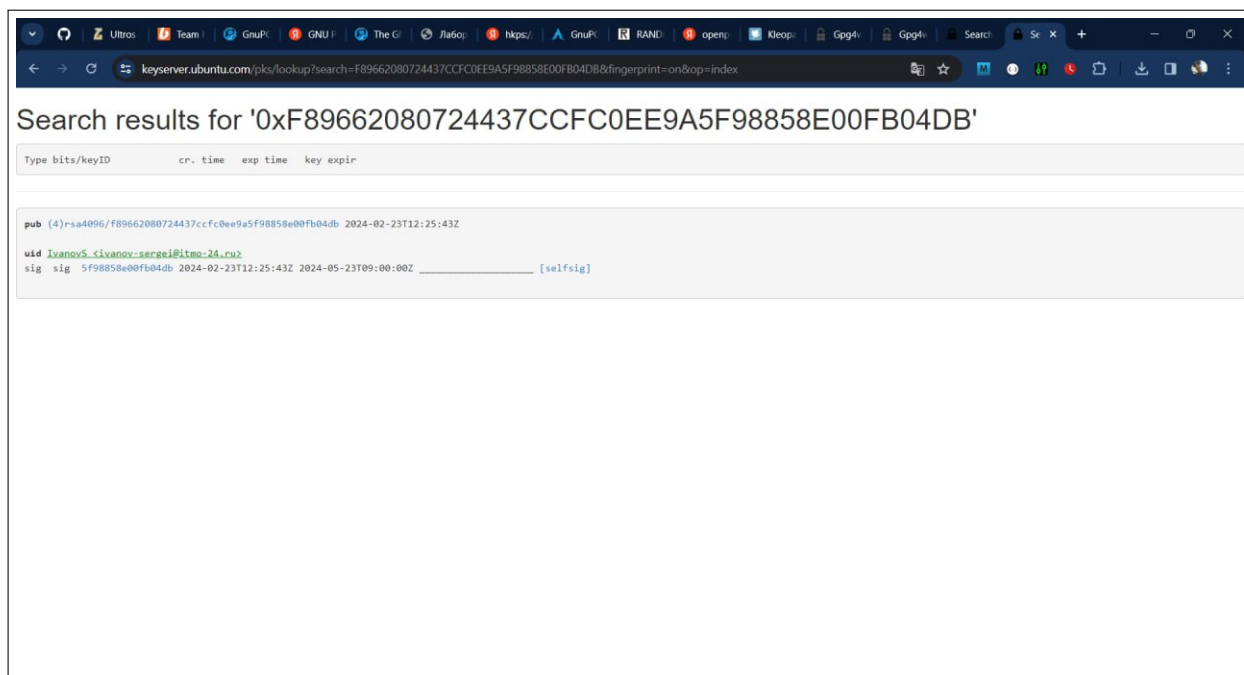
1.3 Опубликуйте свой ключ на сервере ключей.

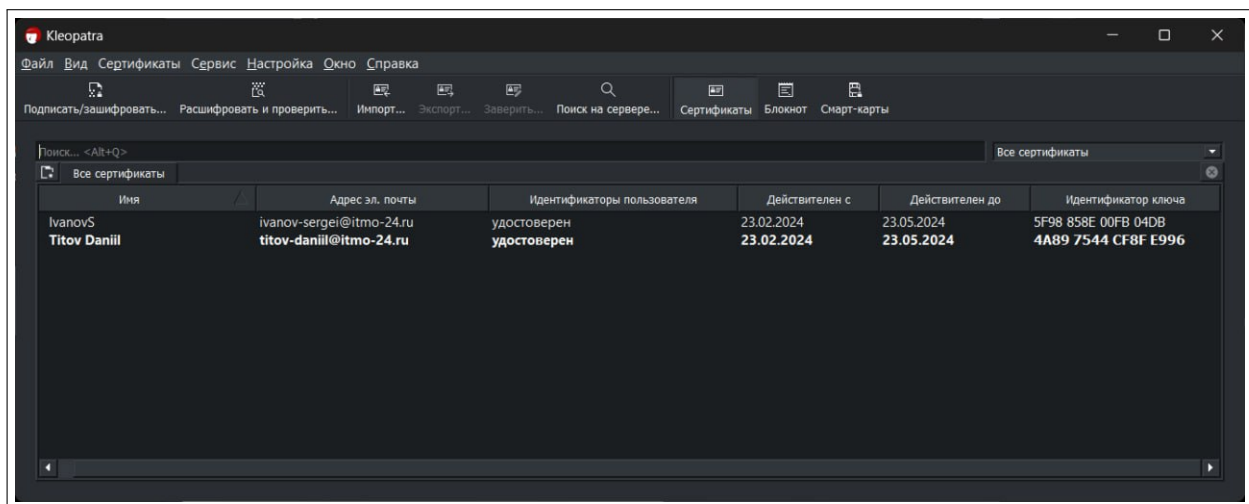


```
Администратор: Windows Po  X  +  -  X
PS C:\Users\danil> gpg --keyserver hkp://keyserver.ubuntu.com --send-keys 3418E5A453AE3B82068949164A897544CF8FE996
gpg: отправка ключа 4A897544CF8FE996 на hkp://keyserver.ubuntu.com
PS C:\Users\danil> |
```

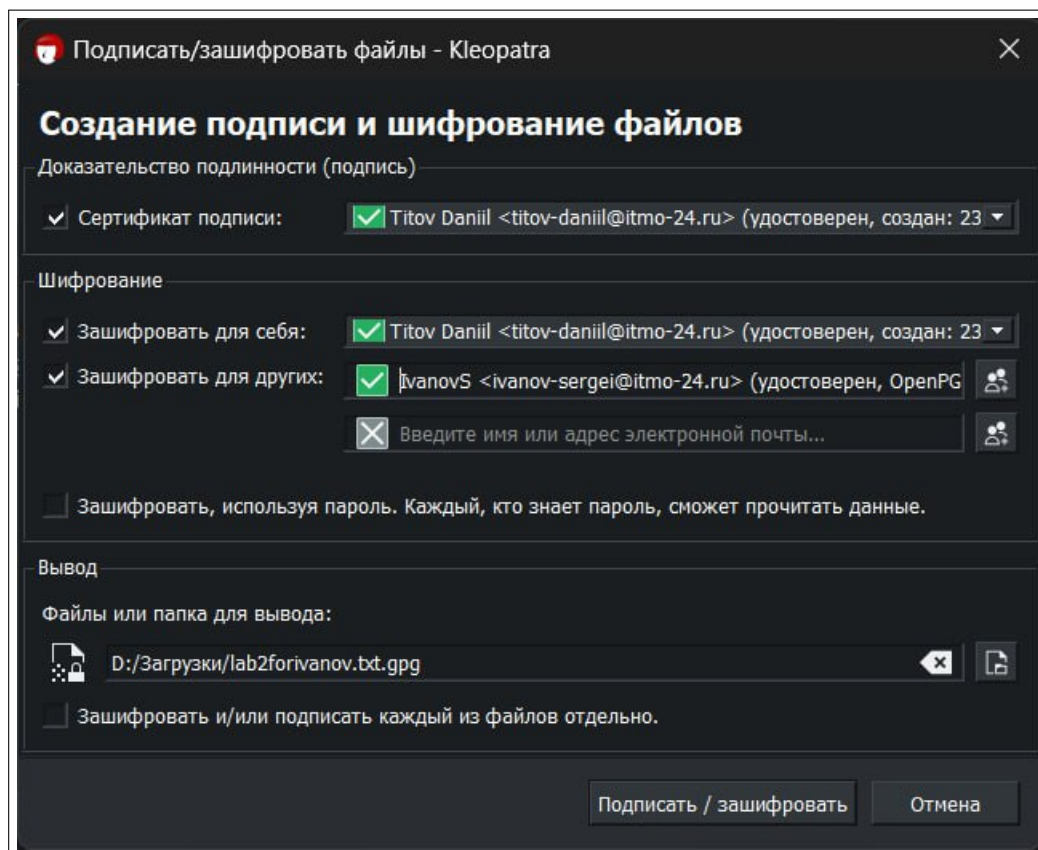
2 Шифрованный обмен

2.1 Узнайте fingerprint публичного ключа своего коллеги, которому Вы будете отправлять сообщение.

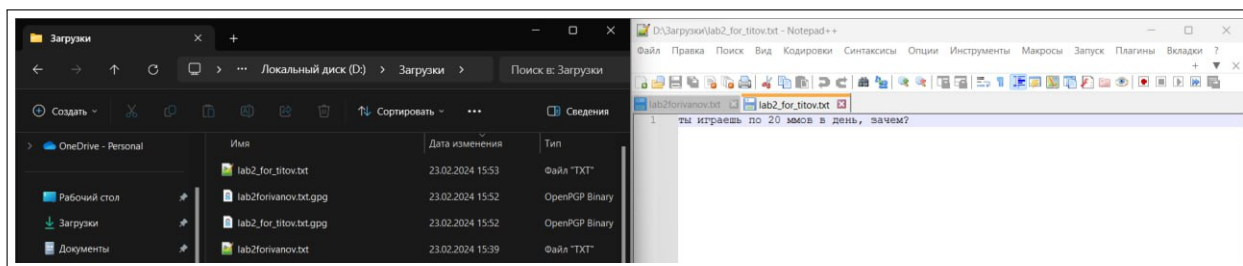
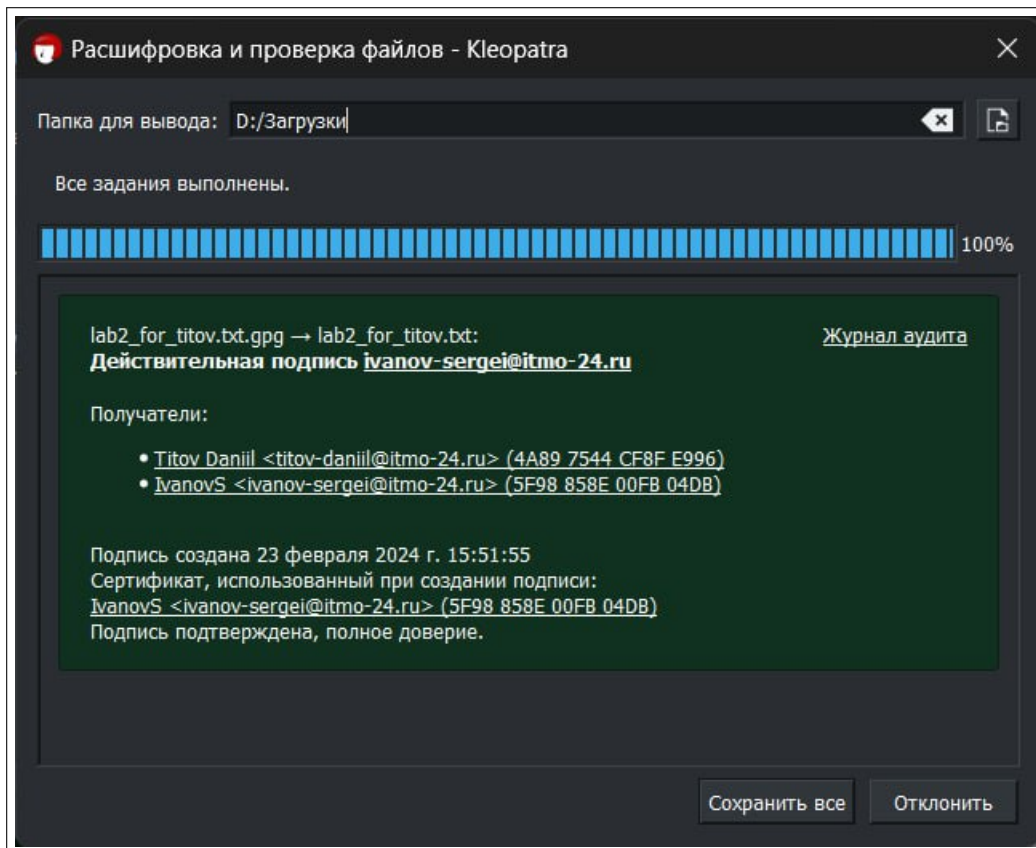




2.2 Создайте текстовый файл с секретным сообщением -> Зашифруйте файл и передайте зашифрованный файл

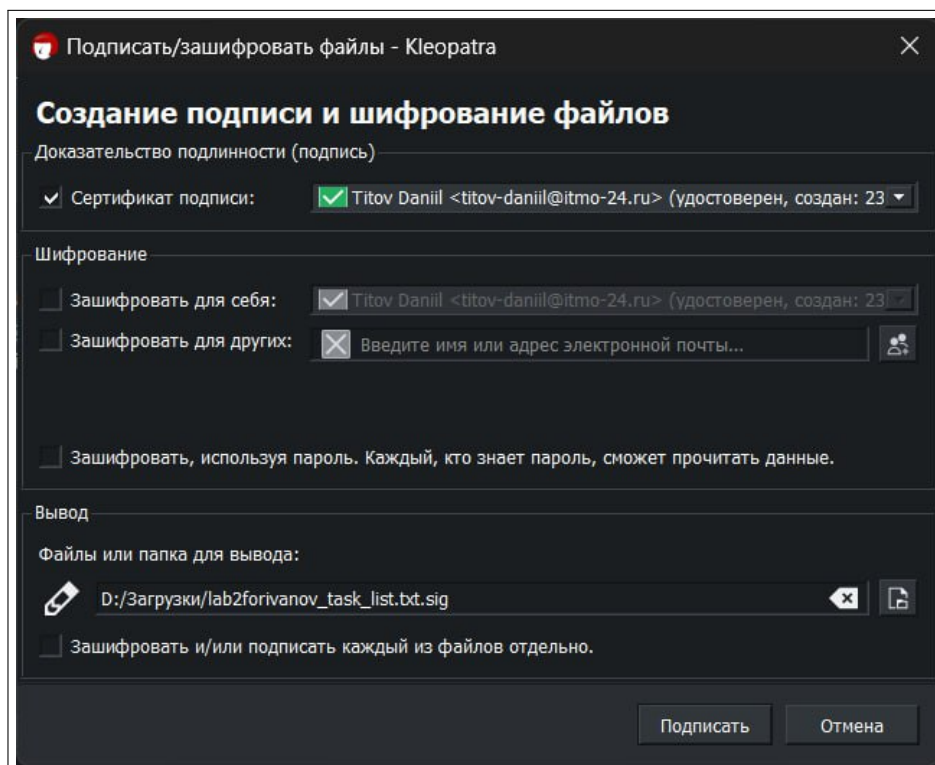
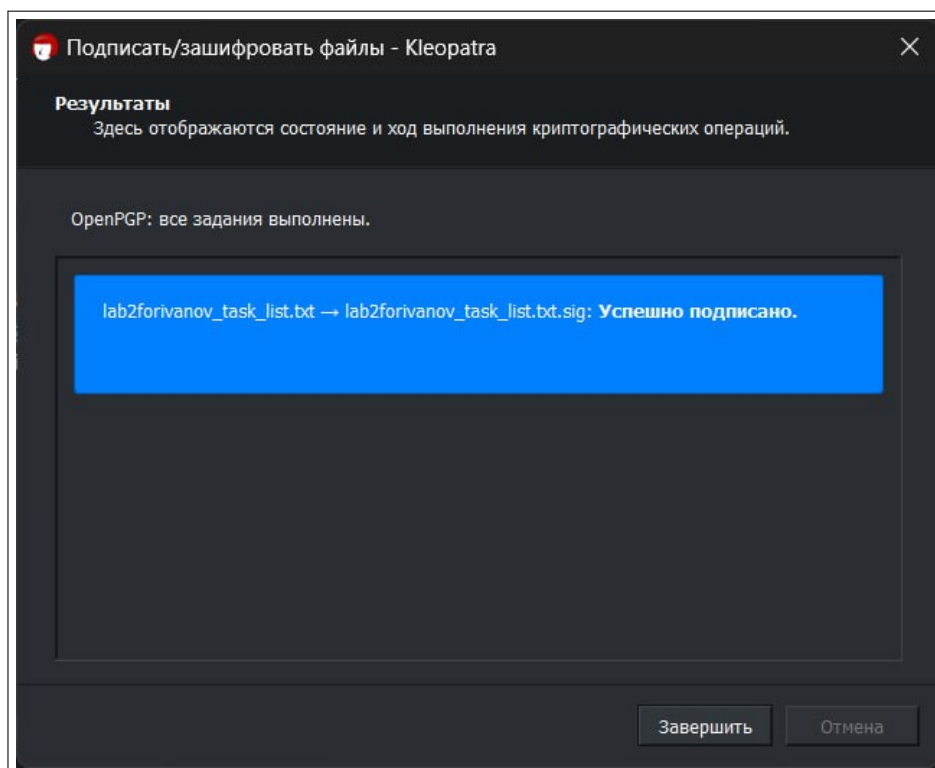


2.3 Примите зашифрованный файл, который предназначается Вам и расшифруйте его с помощью своего ключа.

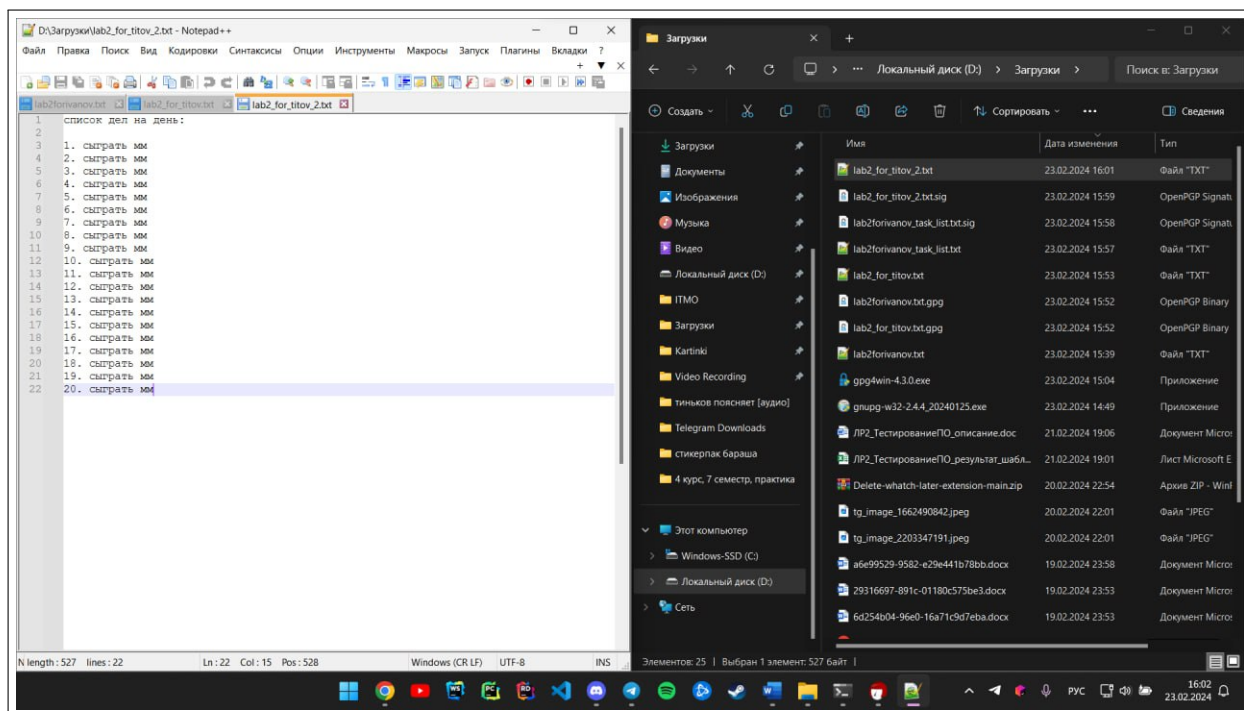


3 Электронная подпись

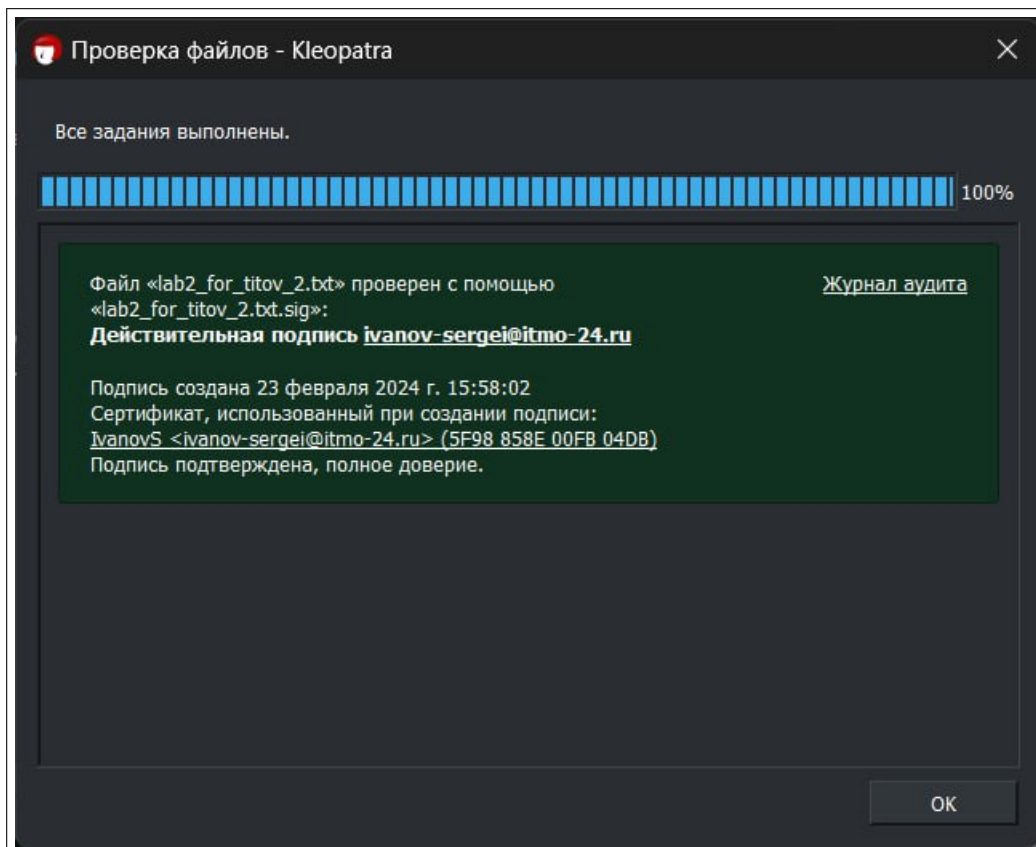
3.1 Создайте текстовый файл со списком дел на день -> Подпишите файл своей подписью



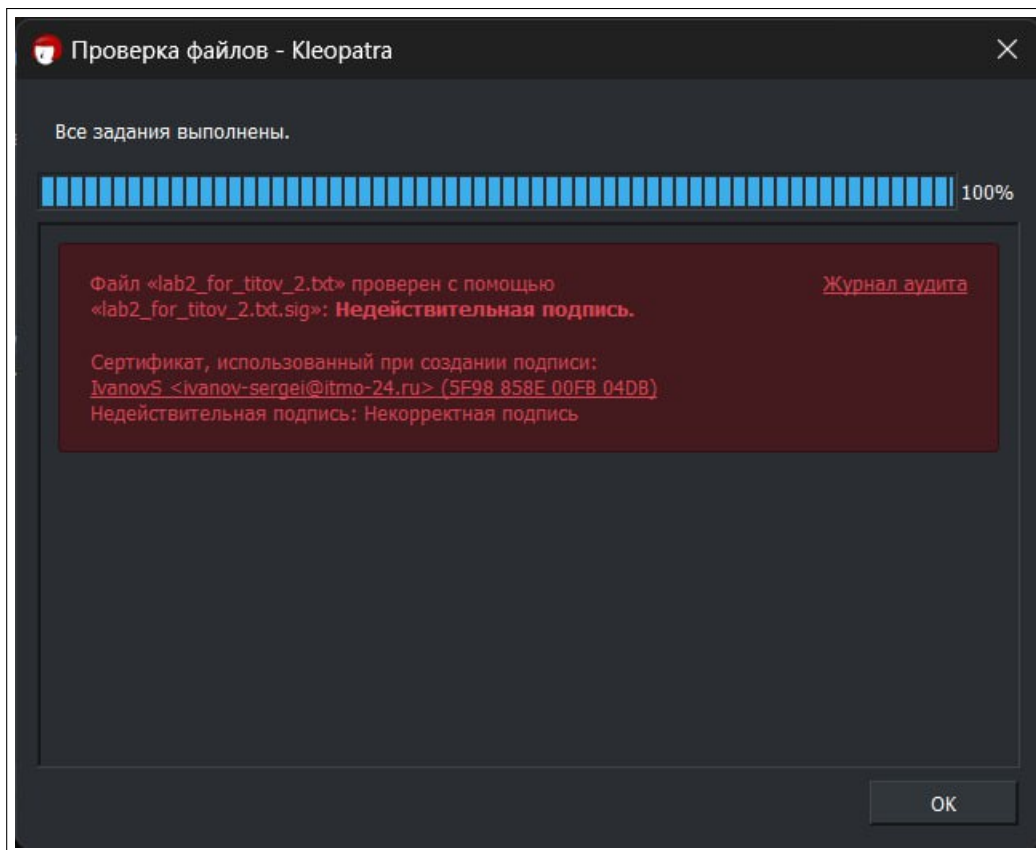
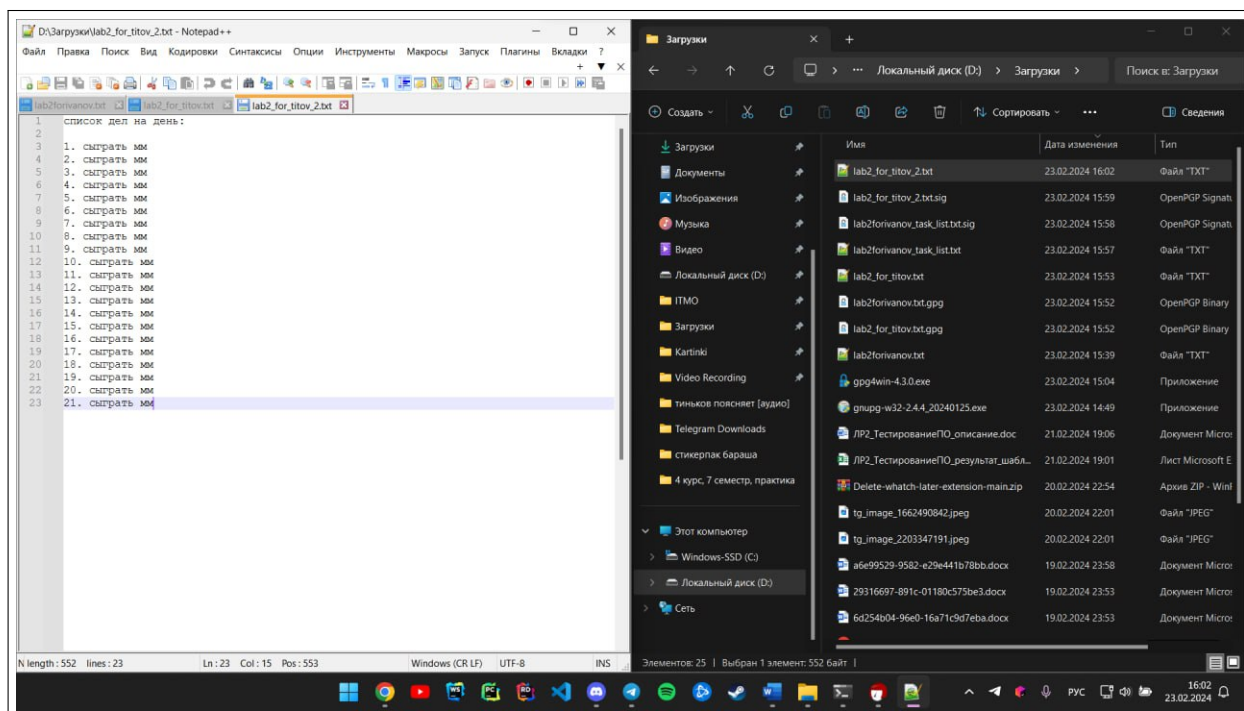
3.2 Примите файл и подпись от своего коллеги.



3.3 Сверьте подпись.



3.4 Внесите изменения в файл, сохраните и снова сверьте подпись.



4 Вопросы к защите

4.1 Какой ключ нужно использовать для шифрования файлов?

`-encrypt` + открытый ключ

4.2 Какой ключ нужно использовать для подписывания файлов?

`-detach-sig` + закрытый ключ

4.3 Предложите своё решение задачи, когда один документ должны подписать несколько человек. Например, PDF-файл с договором купли-продажи, который должны подписать продавец и покупатель.

Допустим, у нас есть два ключа подписи: автор и валидатор, автор всегда подписывает документ перед отправкой в валидатор, а валидатор подписывает его, как только получает:

Автор подписывает свой документ (doc.txt)
`gpg -u author -a --clearsign doc.txt`
в результате получается файл с именем doc.txt.asc

Проверяющий получает doc.txt.asc, проверяет, что у него есть действительный знак от автора, и подписывает его своим ключом.

`gpg --verify doc.txt.asc`
`gpg -u validator -a --clearsign doc.txt.asc`
в результате получается файл doc.txt.asc.asc

Теперь у вас есть файл doc.txt.asc.asc а с обеими подписями. Чтобы проверить обе подписи, надо выполнить:

`gpg --decrypt doc.txt.asc.asc 1>authors-file.txt.asc`
`gpg --decrypt authors-file.txt.asc 1>original-file.txt`

Важен порядок проведения проверки. Можно связать в цепочку столько подписей, сколько необходимо, используя этот метод, но при проверке надо следовать порядку, прямо противоположному порядку подписи.