

Министерство науки и высшего образования Российской Федерации  
Федеральное государственное автономное образовательное учреждение  
высшего образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ  
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

Кафедра автоматизированных систем управления (АСУ)

## ЗНАКОМСТВО С КРИПТОСИСТЕМАМИ

**Отчет по лабораторной работе №4**

**По дисциплине**

**«Информационная безопасность»**

Студент гр. 431-3

\_\_\_\_\_ Д.П. Андреев

«\_\_»\_\_\_\_\_ 2024 г.

Проверил: старший преподаватель кафедры  
АСУ.

\_\_\_\_\_ Я.В. Яблонский

«\_\_»\_\_\_\_\_ 2024 г.

Томск 2024

## 1 Цель работы

Познакомиться с работой программы. Внимательно изучите процессы создания ключей, распространения открытых и сохранения в тайне закрытых ключей, схему разделения и сборки ключей.

## 2 Задание на лабораторную работу

Вариант 3. Установите программу GPG4Win. Создайте свою собственную пару ключей (открытый и закрытый). Осуществите последовательно действия;

- подготовить документ (файл), который необходимо переслать другому пользователю;
- подпись файла цифровой подписью;
- зашифровать подписанный файл с помощью открытого ключа другого пользователя;
- передать зашифрованный файл пользователю, чей ключ использовался при шифровании;
- получатель должен расшифровать файл и проверить достоверность ЭЦП;

Напишите отчет по работе (если какие-либо из заданных пунктов выполнить в выбранной вами программе не возможны, отобразите это в отчете).

Прикрепите к отчету полученные в ходе работы файлы. Кратко поясните их назначение.

## 3 Ход работы

При запуске программы нас встречает окно с выбором действий (рисунок 3.1).

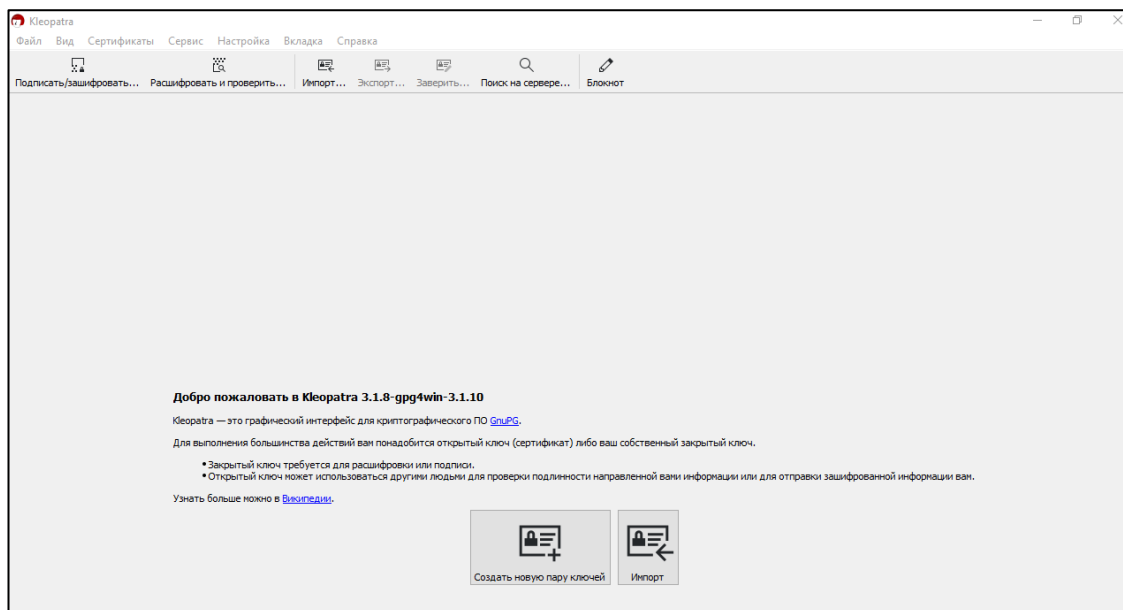


Рисунок 3.1 – Стартовое окно программы

Для начала нам нужно создать пару ключей. Запускаем мастер создания пары ключей и вводим персональные данные пользователя (рисунок 3.2).

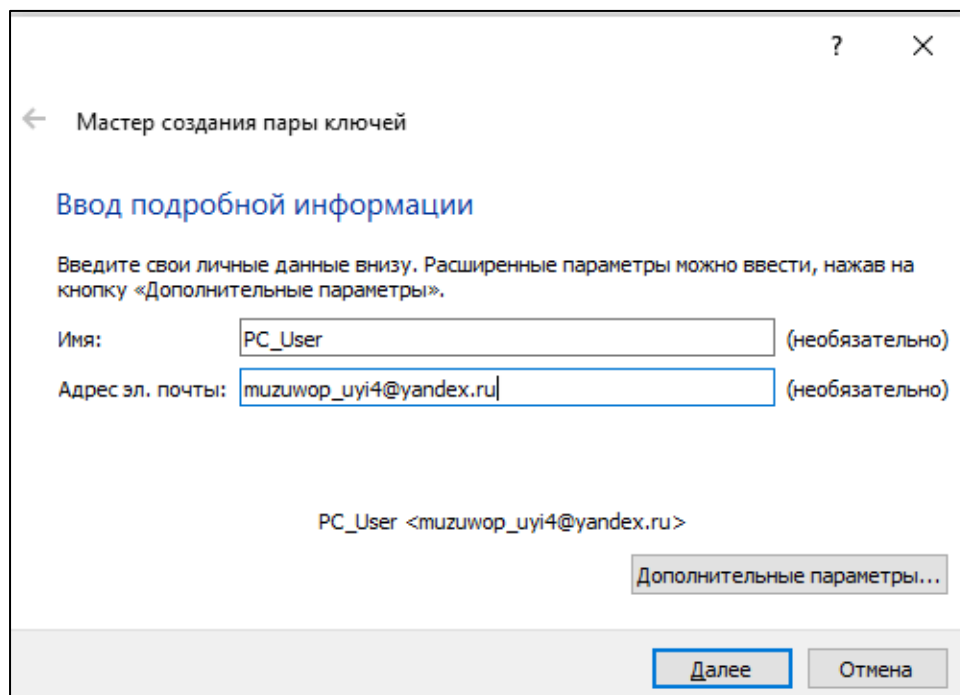


Рисунок 3.2 – Мастер создания пары ключей

Настраиваем подпись и сертификат (рисунок 3.3).

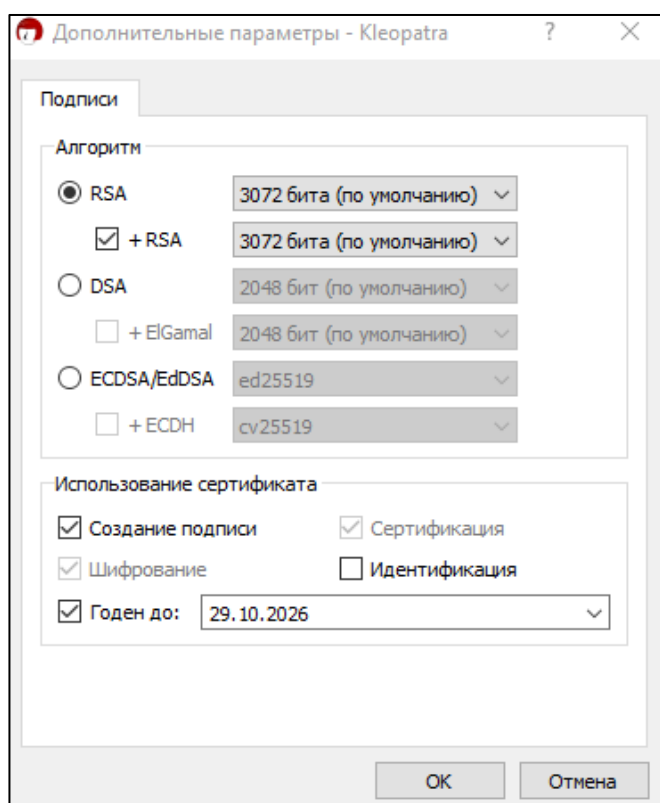


Рисунок 3.3 – Меню настройки подписи и сертификата

В конце вводим фразу-пароль и получаем нашу пару ключей (рисунок 3.4-3.6)

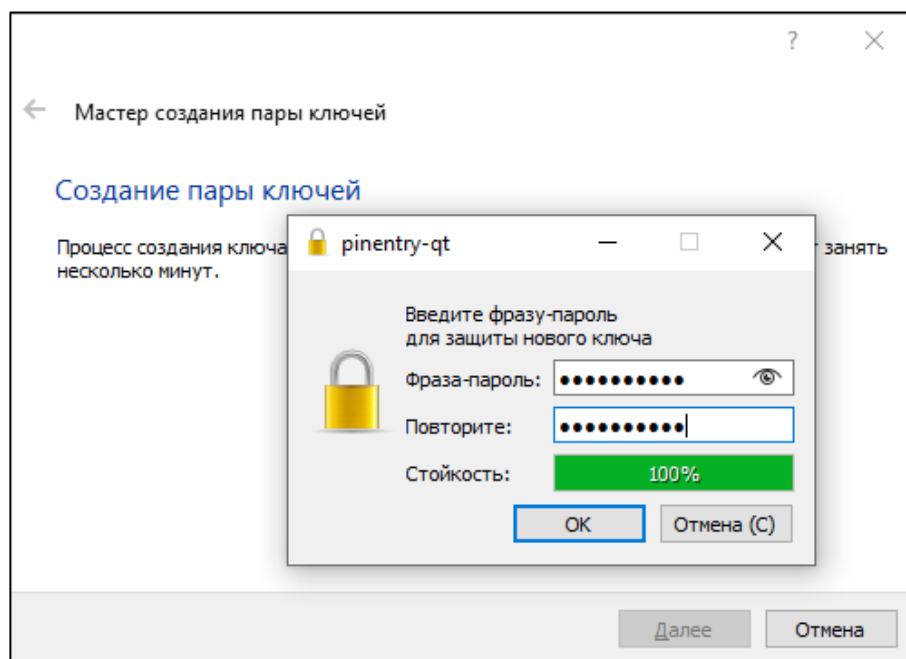


Рисунок 3.4 – Ввод фразы пароль

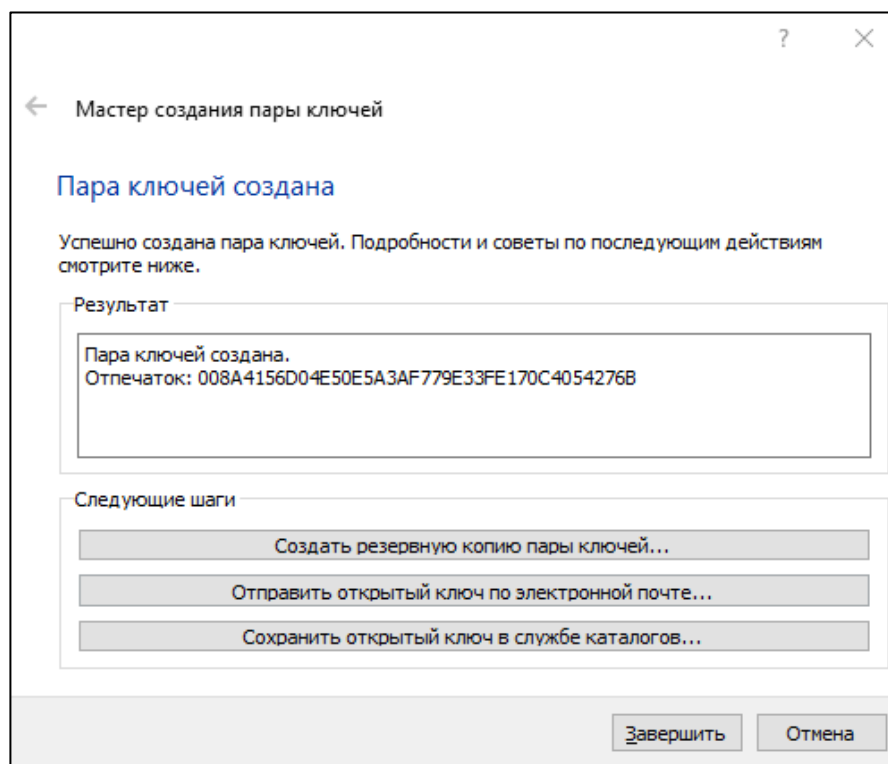


Рисунок 3.5 – Пара ключей

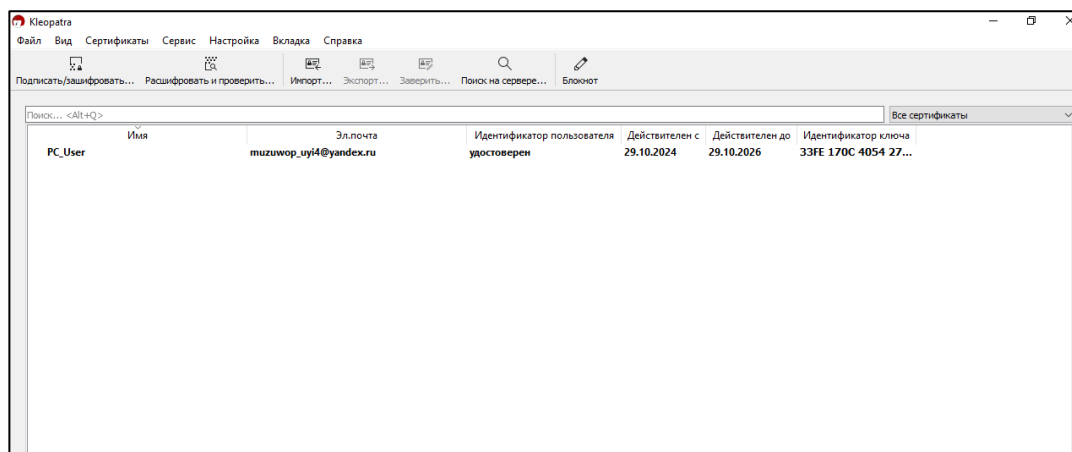


Рисунок 3.6 – Результат создания пары ключей

Делаем такую же процедуру на другом устройстве и получаем ещё одну пару ключей (рисунок 3.7)

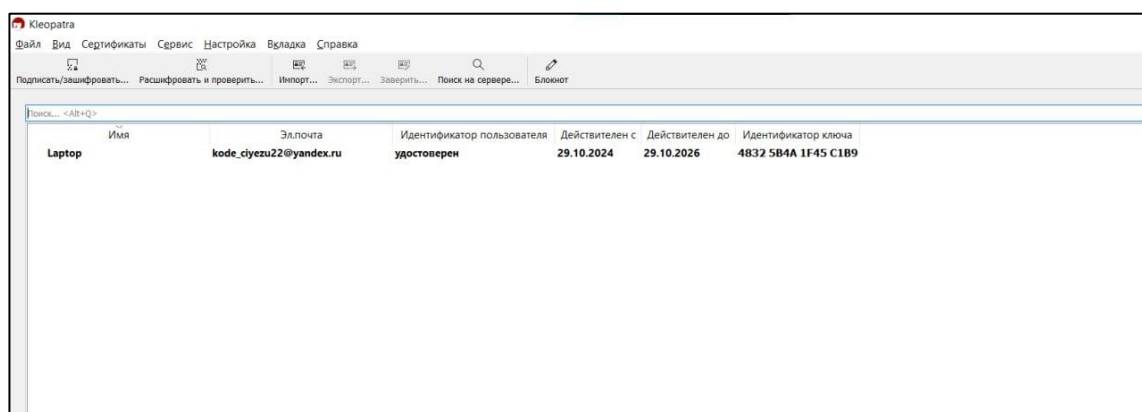


Рисунок 3.7 – Результат создания пары ключей на другом устройстве

Для шифрования и передачи сообщений сохраним сертификаты. Теперь обмениваемся с устройством сертификатами (рисунок 3.8-3.9).

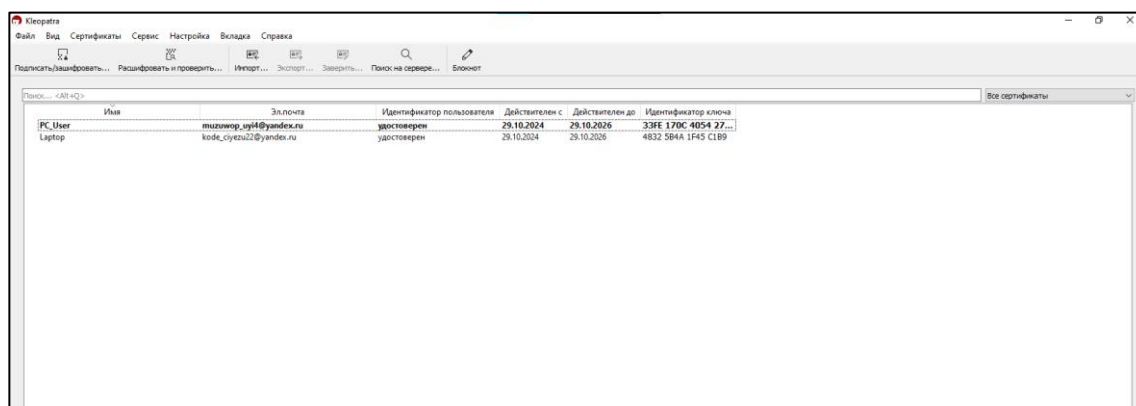


Рисунок 3.8 – Сертификаты на первом устройстве

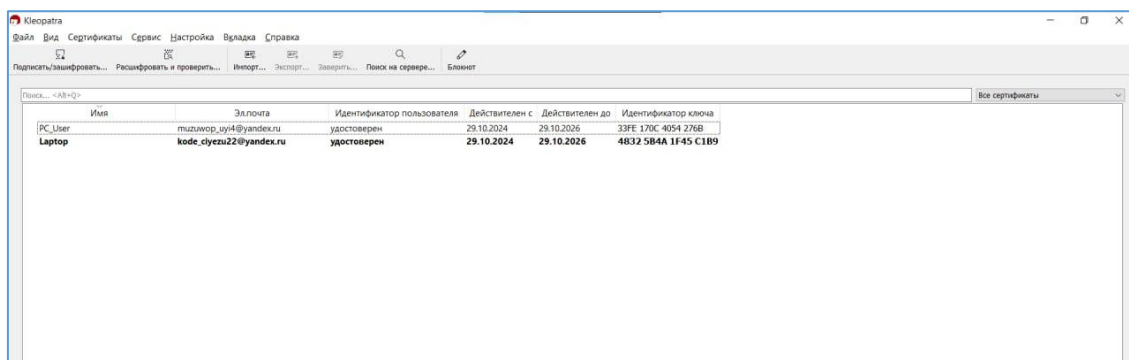


Рисунок 3.9 – Сертификаты на втором устройстве

В первом примере мы будем подписывать и шифровать фото и отправим его на другое устройство. Для этого мы выбираем наше фото и вводим данные получателя. Получаем зашифрованный файл с нашим изображением (рисунок 3.10-3.11).



Рисунок 3.10 – Входное изображение

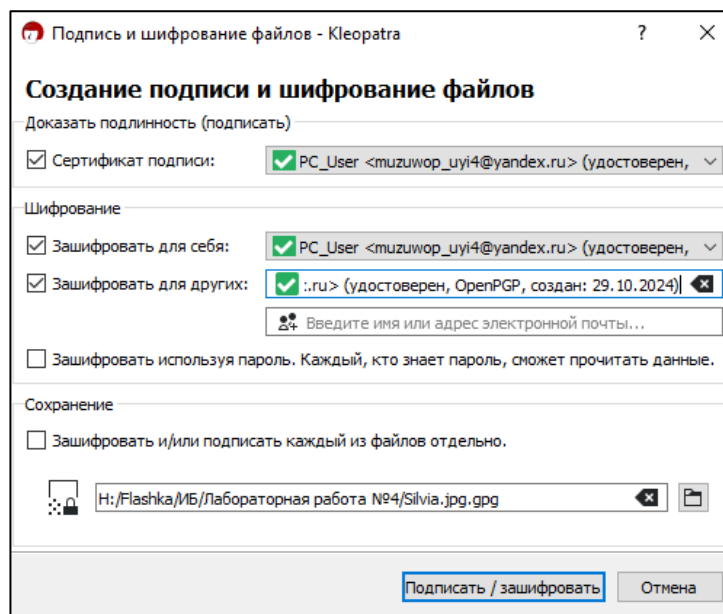


Рисунок 3.11 – Создание подписи и шифрование файла

Теперь пробуем расшифровать его на другом устройстве. Выбираем зашифрованный файл и начинаем расшифровку. Вводим фразу-пароль и получаем расшифрованное изображение. Также видим информацию об подленности подписи(рисунок 3.12-3.13).

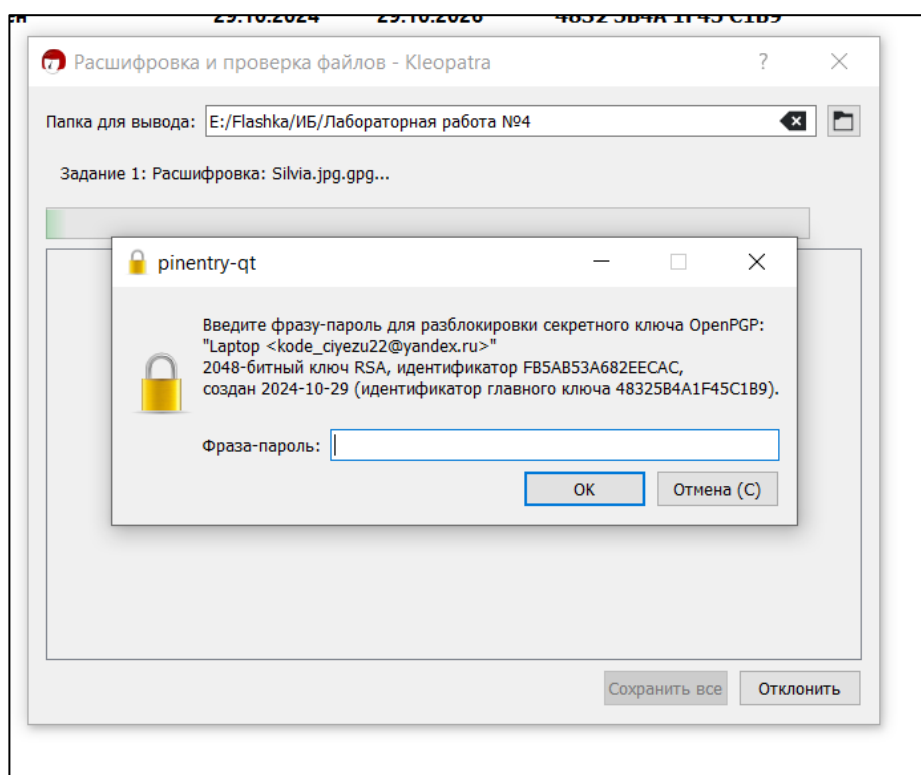


Рисунок 3.12 – Ввод фразы-пароль

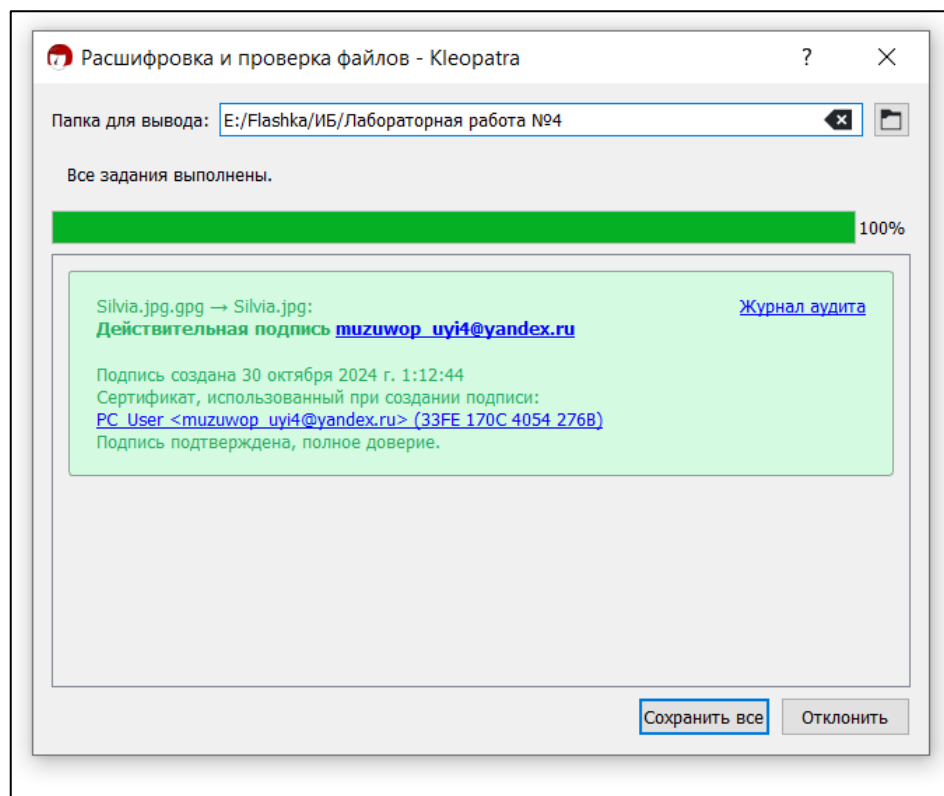


Рисунок 3.13 – Информационное окно

В результате получаем такое изображение (рисунок 3.14).



Рисунок 3.14 – Итоговое изображение на втором устройстве

Во втором пример мы передадим изображение (рисунок 3.15) со второго устройства.





Рисунок 3.15 – Входное изображение для шифрования

Подпишем и зашифруем данное изображение. Для этого мы выбираем наше фото в программе и вводим данные получателя (рисунок 3.16).

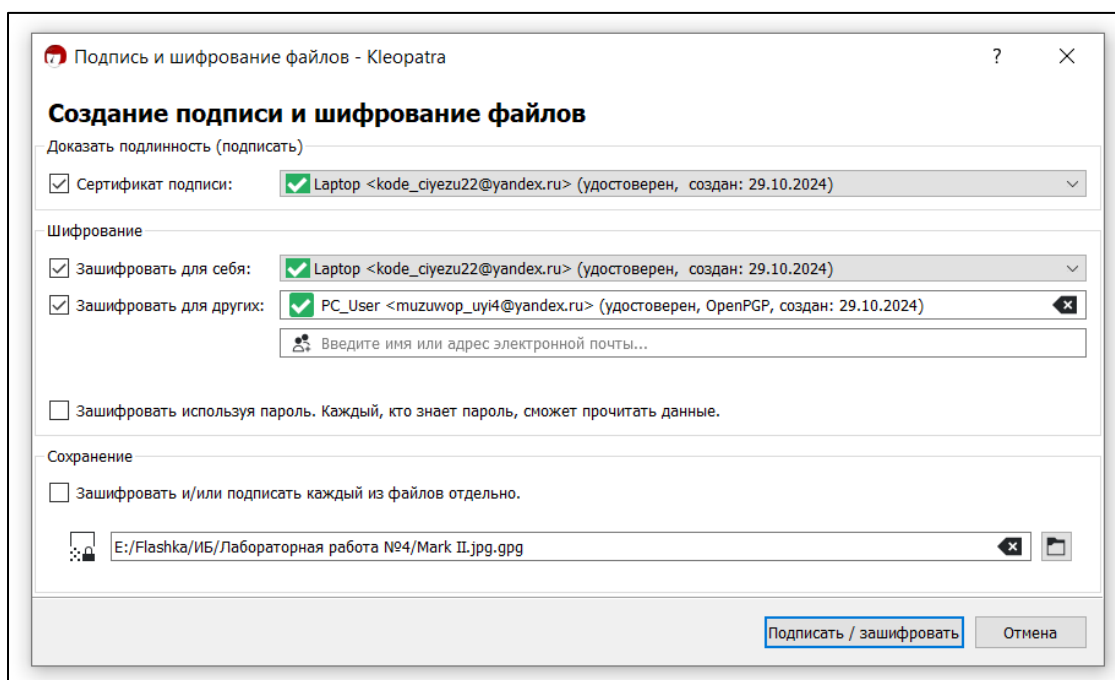


Рисунок 3.16 – Создание подписи и шифрование файла

Получаем зашифрованный файл с нашим изображением. Теперь передаём его на первое устройство. На первом устройстве начинаем расшифровку изображения и получаем окно с

информацией об выполнении расшифровки и сведениях об подлинности подписи (рисунок 3.17).

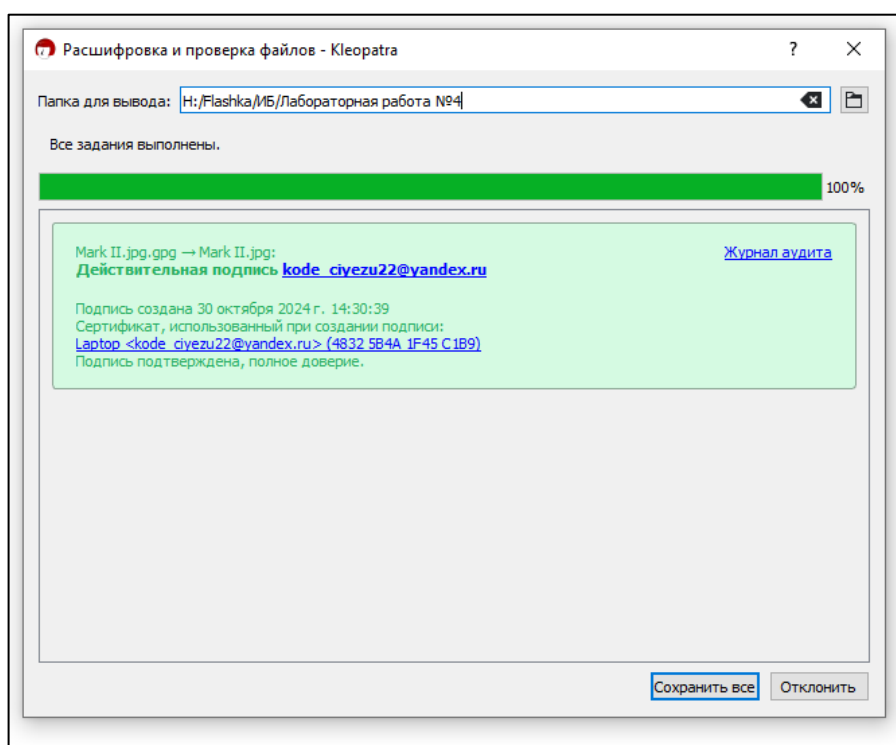


Рисунок 3.17 – Информационное окно

В итоге получаем изображение (рисунок 3.18).

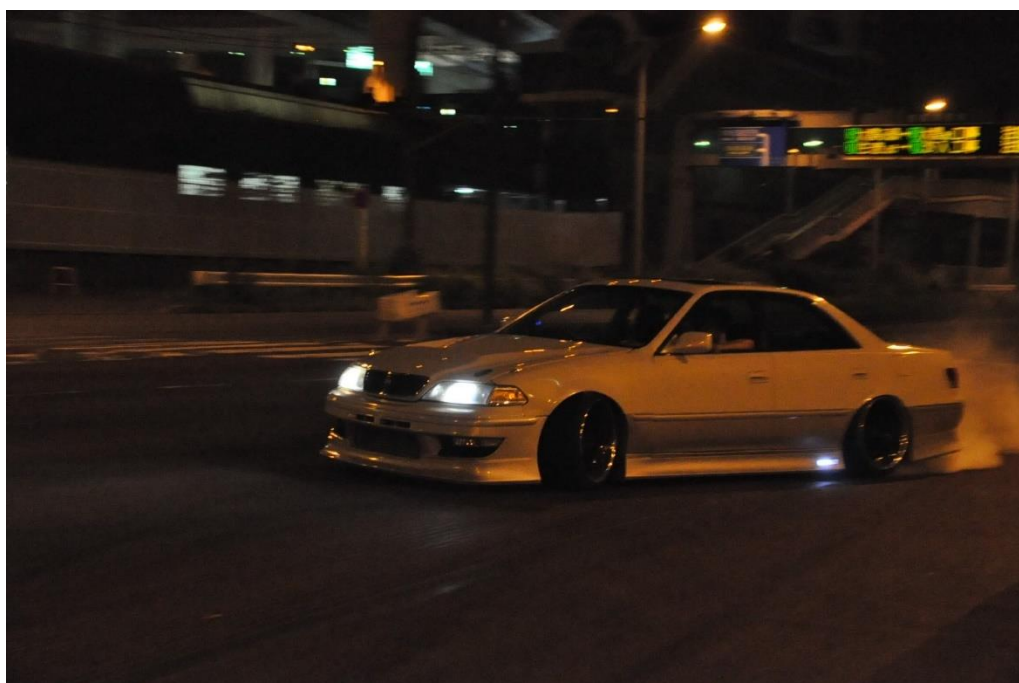


Рисунок 3.18 – Итоговое изображение на первом устройстве

## **4 Вывод**

В ходе выполнения лабораторной работы я познакомился с работой программ GPG4Win и Kleopatra. Изучил процессы создания ключей, распространения открытых и сохранения в тайне закрытых ключей, схему разделения и сборки ключей.