# МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

# федеральное государственное автономное образовательное учреждение высшего образования

# «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

# АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА № 34

ОТЧЕТ   
ЗАЩИЩЕН С ОЦЕНКОЙ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ПРЕПОДАВАТЕЛЬ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| доцент, кандидат технических наук |  |  |  | Мыльников В.А. |
| должность, уч. степень, звание |  | подпись, дата |  | инициалы, фамилия |

|  |
| --- |
| ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ |
| **Применение электронной цифровой подписи для проверки авторства и неизменности файла** |
| по курсу: ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ |
|  |

РАБОТУ ВЫПОЛНИЛ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| СТУДЕНТ ГР. № | 3143 |  |  |  | Казаков И.А. |
|  |  |  | подпись, дата |  | инициалы, фамилия |

Санкт-Петербург 2022 г.

Оглавление

[**Цель работы.** 2](#_Toc104386758)

[**Ход работы.** 3](#_Toc104386759)

[**Результаты лабораторной работы и выводы.** 6](#_Toc104386760)

## **Цель работы.**

Получить навыки применения программного продукта OpenSSL для электронного подписывания документов и проверки подписи, изучить принципы ЭЦП.

## **Ход работы.**

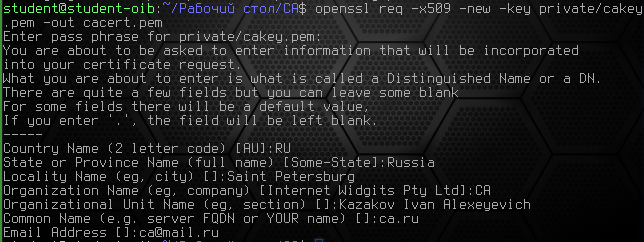
1. С помощью OpenSSL создадим новый центр сертификации и выпустим сертификат:

Рисунок 3: создание сертификата cacert.pem в каталоге CA.

Рисунок 2: создание закрытого ключа cakey.pem в каталоге private.

Рисунок 1: структура каталога CA.

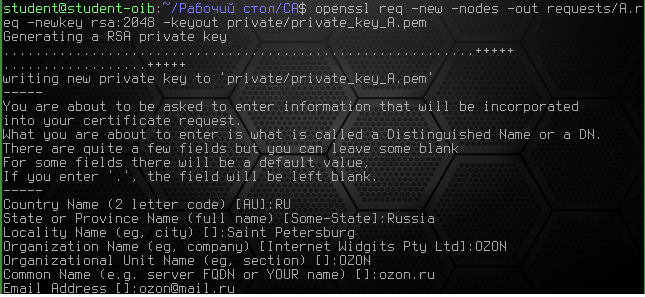
1. Создадим запрос на сертификацию и подпишем его ключом нового центра сертификации:

Рисунок 4: создание запроса на сертификацию.

1. Создадим текстовый файл и создадим для него ЭЦП новой парой ключей:

Рисунок 6: проверка подлинности сертификата A.cert.

Рисунок 5: подписанный сертификат A.cert.

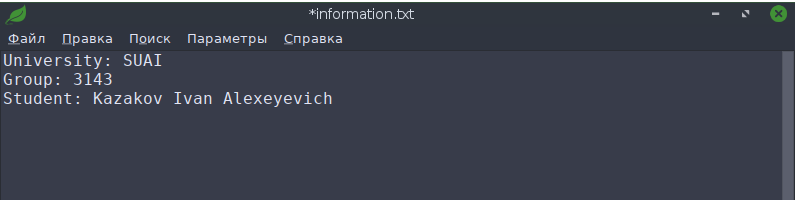


Рисунок 7: содержание созданного файла information.txt.



Рисунок 8: генерация закрытого ключа алгоритма RSA.



Рисунок 9: извлекаем открытый ключ из закрытого.



Рисунок 10: подписание и хеширование файла с помощью закрытого ключа.

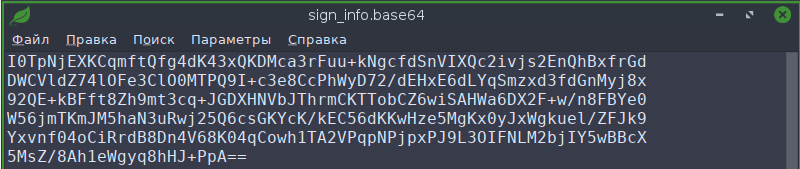


Рисунок 11: электронная цифровая подпись information.txt.



Рисунок 12: проверка подписи.

1. Изменим исходный файл и проверим подпись заново, убедимся, что проверка оканчивается неудачей:

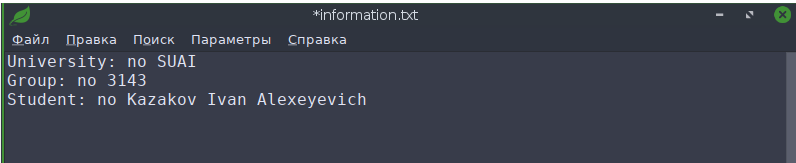
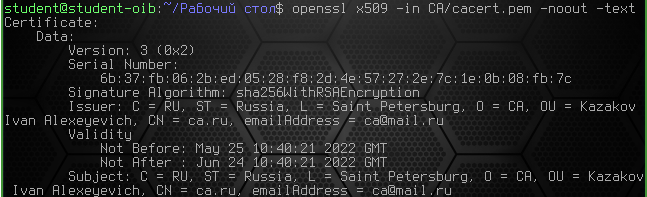


Рисунок 23: изменённый текстовый файл.

Рисунок 14: подпись не прошла проверку.

1. Распечатаем сертификат и укажем, из какого поля можно узнать владельца сертификата, которым подписан текст:

Узнать информацию о владельце сертификата можно из поля Subject.

## **Результаты лабораторной работы и выводы.**

Получил навыки применения программного продукта OpenSSL для электронного подписывания документов и проверки подписи, изучил принципы ЭЦП.