# 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 |
| **Создание цифровых сертификатов Х.509 и преобразование их форматов с применением пакета OpenSSL** |
| 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](#_Toc101818669)

[**Ход работы** 3](#_Toc101818670)

[**Результат лабораторной работы.** 6](#_Toc101818671)

## **Цель работы**

Получить навык применения программного продукта OpenSSL для создания сертификатов Х.509 и их преобразования, изучить структуру сертификата Х.509 и форматы DER и PEM.

## **Ход работы**

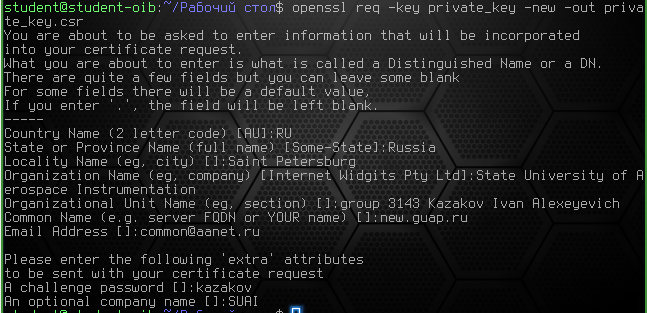
1.Создадим запрос на сертификацию:

Рисунок 1:создание запроса сертификата (private\_key.csr) для существующего ключа (private\_key)

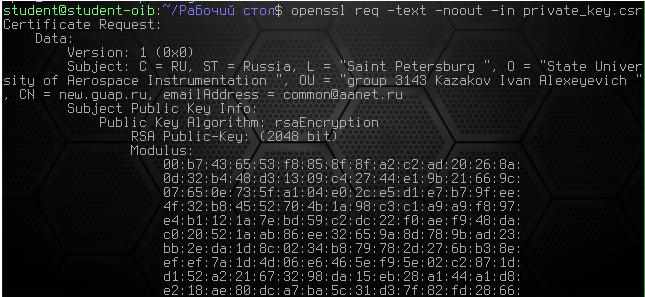
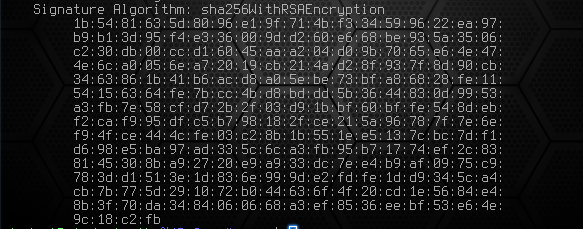
2. Выведем запрос на сертификацию в текстовом виде: 

Рисунок 2:содержимое сертификата в виде простого текста.

Рисунок 3: содержимое сертификата в виде простого текста.

**Version**: Данное поле описывает версию представления сертификата. Если используются расширения, то версия должна быть 3 (значение - 2) Если расширения не указаны, но Unqueldentifer представлен, версия может быть 2 (значение - 1), но версия может быть и 3. Если представлены только базовые поля, версия может быть 1 (значение в сертификате опущено как значение по умолчанию), но версия может быть 2 или 3.

**Subject:** Поле subject идентифицирует участника, который является собственником сертификата и соответствующего закрытого ключа.

**signature Algorithm:** Поле signatureAlgorithm содержит идентификатор криптографического алгоритма, используемого СА для подписывания данного сертификата.

**Subject Public Key Info:** Поле содержит информацию открытого ключа.

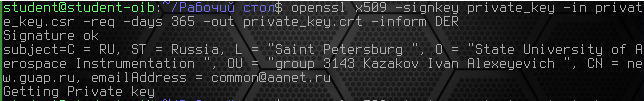
 3. Сгенерируем ключ RSA и подпишите им созданный запрос, с указанием формата сертификата DER:

Рисунок 4:создание сертификата (private\_key.crt) на основе существующего запроса (private\_key.csr) и закрытого ключа (private\_key).

4. Выведем полученный сертификат в текстовом виде:

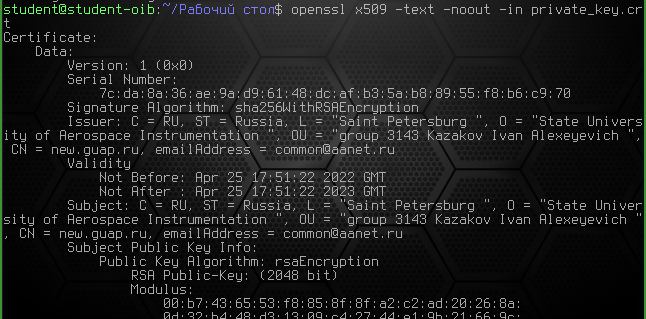


Рисунок 5: содержимое сертификата в виде простого текста.

**Serial number**: серийный номер должен быть положительным целым, назначаемым СА для каждого сертификата. Он должен быть уникальным для каждого сертификата, выпущенного данным СА. Таким образом, имя выпустившего и серийный номер однозначно определяют сертификат CAs должны обеспечивать. чтобы серийные номера были неотрицательными целыми. Считается, что серийные номера могут иметь длину до 20 октетов.

**Issuer:** поле issuer идентифицирует того, кто подписал и выпустил сертификат.

**Validity:** срок действия сертификата.

**Modulus**: длина открытого ключа.

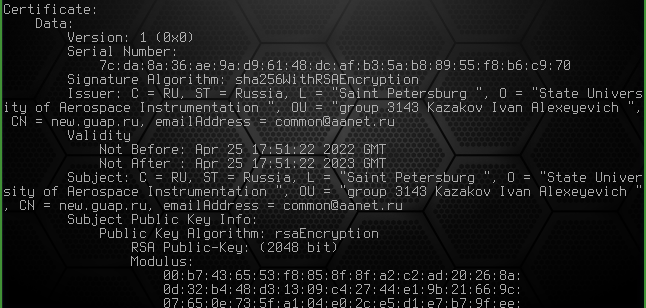
5. Преобразуем формат сертификата из DER в PEM:

Рисунок 7: DER формат.

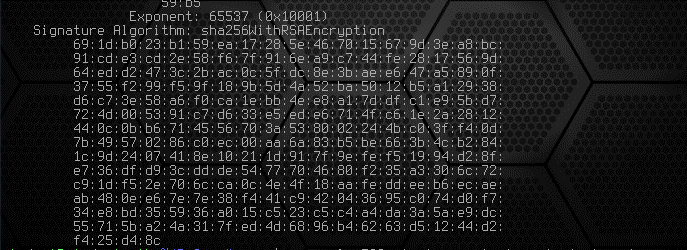


Рисунок 8: DER формат.

Рисунок 6: преобразование из DER в PEM.



Рисунок 9: формат PEM.

Формат DER предполагает хранение данных прямым текстом, а формат PEM предполагает хранение сертификата и ключа в кодировке Base64 между строками "-BEGIN CERTIFICATE" и "- END CERTIFICATE-"

## **Результат лабораторной работы.**

Получил навык применения программного продукта OpenSSL для создания сертификатов Х.509 и их преобразования, изучил структуру сертификата Х.509 и форматы DER и PEM.