# 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 центра сертификации с поддержкой списков отозванных сертификатов 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](#_Toc102684694)

[**Ход работы.** 3](#_Toc102684695)

[**Результаты лабораторной работы и выводы.** 6](#_Toc102684696)

## **Цель работы.**

Получить навык применения программного продукта OpenSSL для создания центра сертификации, выпуска, верификации и отзыва сертификатов, изучить формат списков отзыва сертификатов.

## **Ход работы.**

1. Создадим с помощью OpenSSL новый центр сертификации:

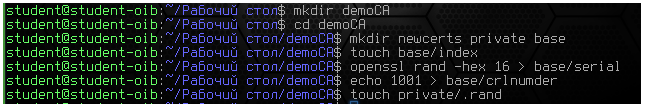
1.1 Создадим структуру каталогов:

Рисунок 1: структура каталога CA.

* Каталог newcerts содержит новые сертификаты
* Каталог base содержит базу данных сертификатов
* Каталог private содержит закрытый ключ центра сертификации

1.2 Создадим закрытый ключ и запрос на подписывание сертификата (CSR) в каталоге demoCA:

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

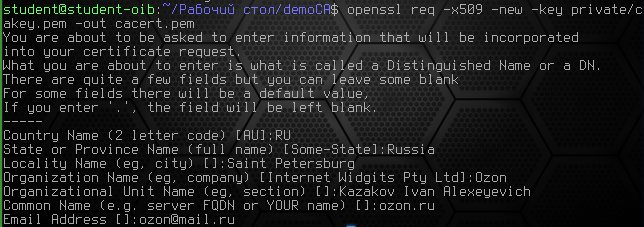


Рисунок 3: создание сертификата cacert.pem в каталоге demoCA.

2. Выпустим два сертификата «A» и «B»:

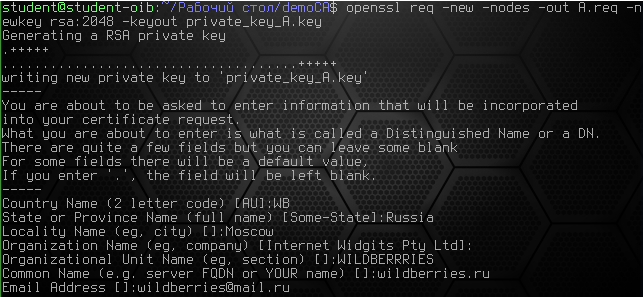


Рисунок 4:сертификат A.

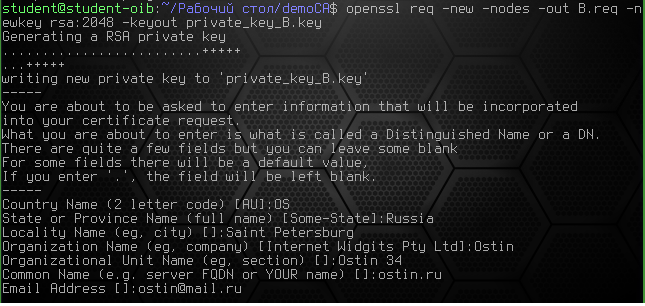


Рисунок 5: сертификат B.

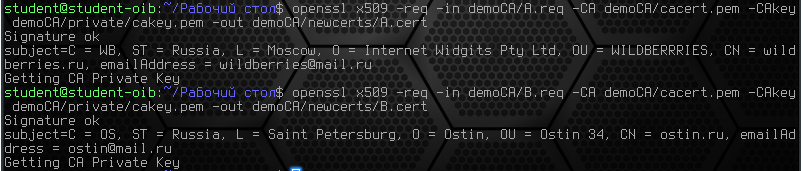
2.1 Подпишем два сертификата «A» и «B»:

Рисунок 6: подпись сертификатов.

3. Проверим подлинность сертификата «А» с помощью сертификата удостоверяющего центра:



Рисунок 7: проверка подлинности сертификата А (положительно)

4. Изменим сертификат «А» и заново проверим подлинность сертификата «А», убедимся, что сертификат не проходит проверку:



Рисунок : изменённый сертификат A не прошёл провеку подлинности.

5. Внесём сертификат «В» в список отзыва:

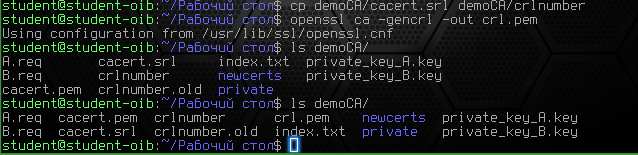
5.1 Создадим список отзыва (CRL):

Рисунок 9: создан список отзыва (CRL) crl.pem.

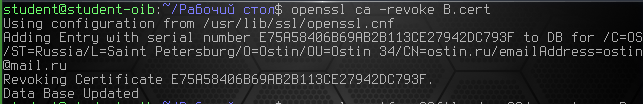
5.2 Внесём сертификат «B» в список отзыва и проверим его:

Рисунок 10: проверка сертификата на подлинность и через список отзыва.

Рисунок : сертификат "B" добавлен в список отзыва.

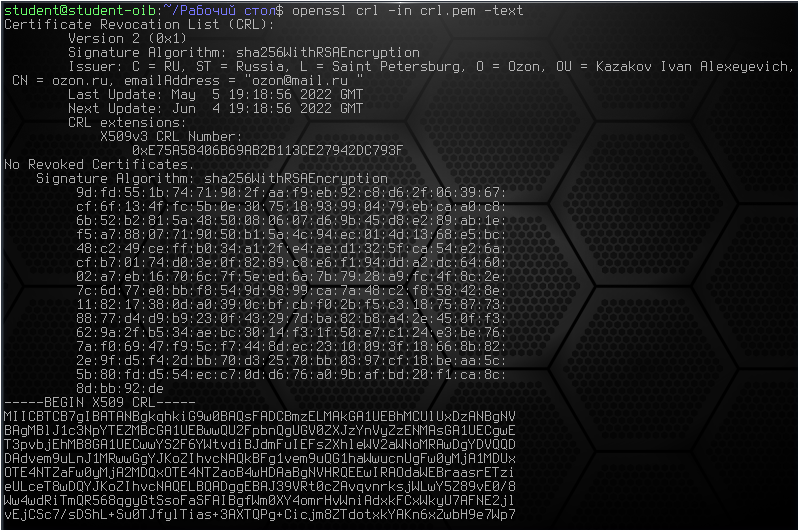
6. Формат CRL:

Рисунок 12: формат CRL.

Список отзыва сертификатов представлен в PEM формате. Показаны прямым текстом личные данные владельца сертификата, а также информация представлена в кодировке Base64 между строками "-BEGIN X509 CRL-" и "- END X509 CRL-".

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

Получил навык применения программного продукта OpenSSL для создания центра сертификации, выпуска, верификации и отзыва сертификатов, изучил формат списков отзыва сертификатов. При проведении проверки сертификата «B» в списке сертификатов результат был положителен, хотя он находится в списке CRL.