Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина» (УрФУ)

Институт радиоэлектроники и информационных технологий – РтФ

Школа профессионального и академического образования

Отчет по дисциплине   
«Криптографические методы защиты информации»

Лабораторная работа №6  
«Удостоверяющий центр (Certificate authority). OpenSSL.»

Студенты: Клоченко И.Е.

Преподаватель: Соколов И.П.

Группа: РИ-300024

Екатеринбург

2023

**Оглавление**

[1. Создание удостоверяющего центра (УЦ, Certificate Authority) 3](#_Toc135419933)

[1.1. Создание файловой иерархии. 3](#_Toc135419934)

[1.2. Корневой сертификат 4](#_Toc135419935)

[2. Создание промежуточного УЦ 5](#_Toc135419936)

[2.1. Создание файловой иерархии 5](#_Toc135419937)

[2.2. Создание сертификата промежуточного УЦ 5](#_Toc135419938)

[2.3. Выдача сертификата корневым УЦ 5](#_Toc135419939)

[2.4. Цепной сертификат 6](#_Toc135419940)

[3. Создание и подписывание сертификатов промежуточных УЦ 7](#_Toc135419941)

[3.1. Создание личного ключа веб-сервера 7](#_Toc135419942)

[3.2. Создание запроса на сертификат 7](#_Toc135419943)

[3.3. Издание сертификата промежуточным УЦ 8](#_Toc135419944)

[3.4. Сертификат. Просмотр. Проверка. 9](#_Toc135419945)

[3.5. Добавление сертификата в конфигурацию веб-сервера 11](#_Toc135419946)

[4. Отзыв сертификата 14](#_Toc135419947)

[4.1. Список отозванных сертификатов 14](#_Toc135419948)

[4.2. Создание сертификатов пользователя 16](#_Toc135419949)

[4.3. Отзыв сертификата пользователя 17](#_Toc135419950)

[4.4. Обновление списка отозванных сертификатов 18](#_Toc135419951)

[Вывод 19](#_Toc135419952)

**Цель работы:**

Знакомство с УЦ и библиотекой *OpenSSL*.

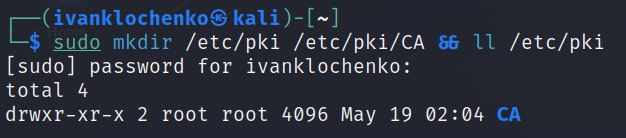
**Ход работы:**

# Создание удостоверяющего центра (УЦ, Certificate Authority)

## Создание файловой иерархии.

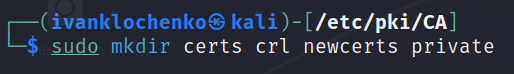
В лабораторной работе используется ОС *Kali* *Linux*, установленная на виртуальной машине *VMware* *Workstation*.

* + 1. Создаем директорию для файлов, связанных с УЦ.



**Рисунок 1**. Создание директории для файлов УЦ

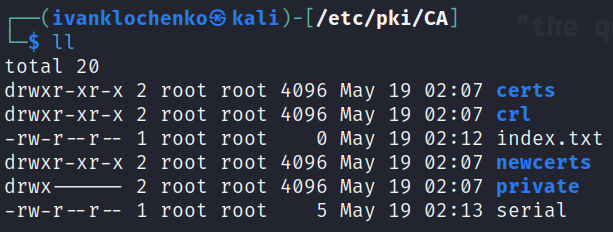
* + 1. Создаем иерархию в файловой системе.



**Рисунок 2**. Создание директорий для сертификатов

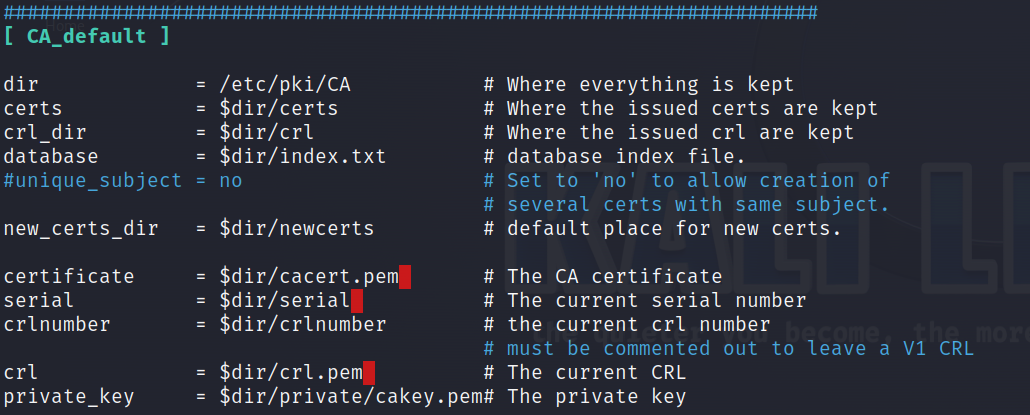
* + 1. Устанавливаем права доступа (700) к подкаталогу *Private*.
    2. Создаем БД для сертификатов в файле *index*.*txt* и файл *serial* для серийных номеров сертификатов.

Результат построения иерархии файловой системы:



**Рисунок 3**. Файловая система для УЦ

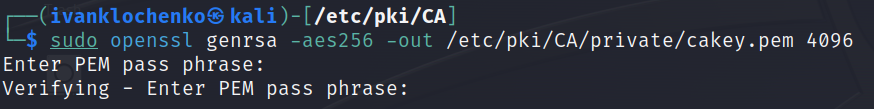
* + 1. Копируем файл *openssl*.*cnf* в каталог *CA* и изменим параметр *dir* на путь к каталогу *CA*.



**Рисунок 4**. Правка файла конфигурации OpenSSL

## Корневой сертификат

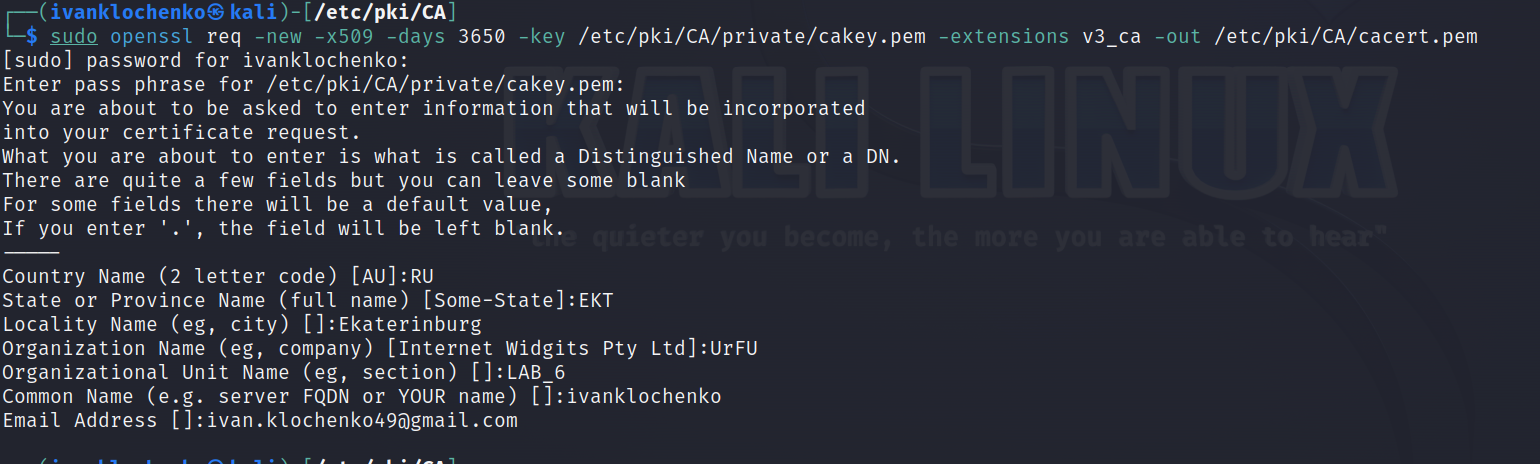
* + 1. Генерируем ключ *OpenSSL* с шифром *AES*-256.



**Рисунок 5**. Генерация ключа OpenSSL

Важно отметить, что длина *passphrase* должна быть от 4 до 1024 символов. Можно набрать меньше или больше и *OpenSSL* обязательно скажет об этом.

* + 1. Даем права 400 файлу *cakey*.*pem*.
    2. Издаем корневой самоподписанный сертификат, который будет действовать 10 лет.



**Рисунок 6**. Издание корневого сертификата

Используется стандарт для инфраструктуры открытого ключа и инфраструктуры управления привилегиями *X*.509 для издания корневого сертификата.

* + 1. Устанавливаем права на чтение для владельца, группы пользователей и других пользователей (444).

# Создание промежуточного УЦ

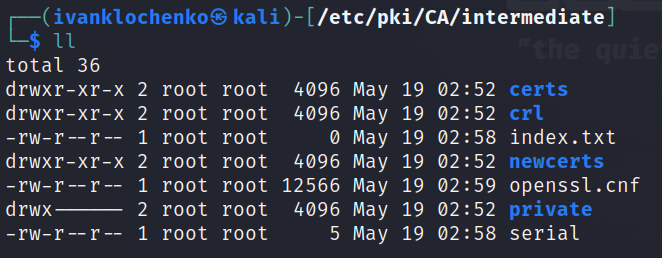
## Создание файловой иерархии

* + 1. Создаем в директории /*etc*/*pki*/*CA*/ директорию *intermediate* и в ней такую же иерархию, что и в *CA*.

Создаем БД и файл серийных номеров сертификатов.

Копируем файл конфигурации *opessl*.*cnf* в корень директории *intermediate*, изменив значение переменной *dir*.

Итог настройки ФС для промежуточного УЦ:



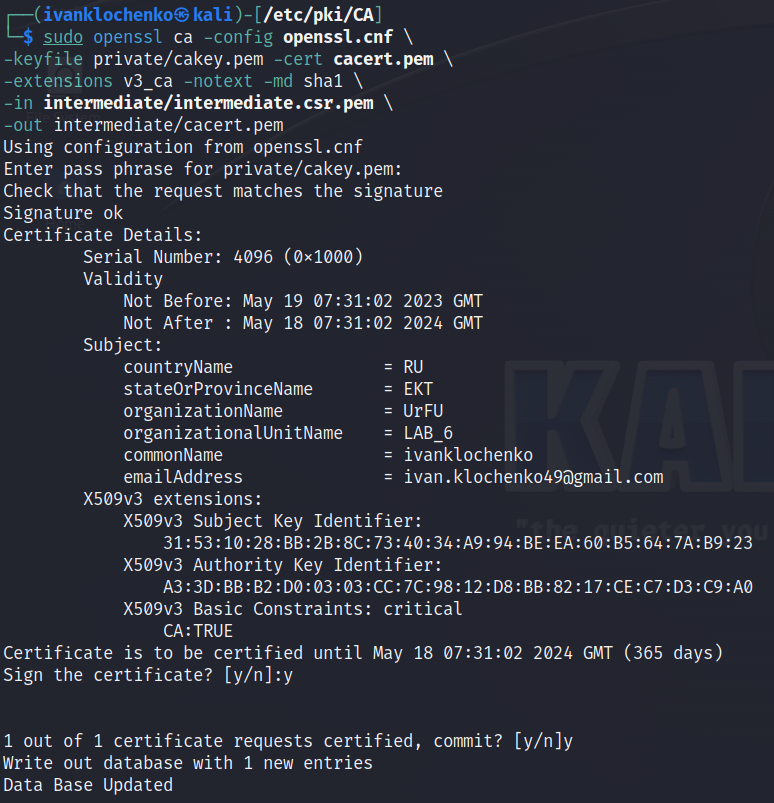
**Рисунок 7**. ФС для промежуточного УЦ

## Создание сертификата промежуточного УЦ

* + 1. Создаем сертификат промежуточного УЦ по аналогии с созданием корневого сертификата УЦ.

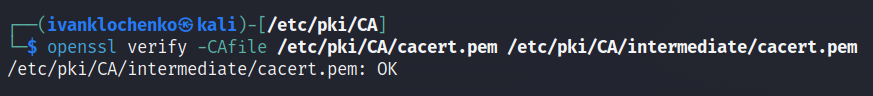
## Выдача сертификата корневым УЦ

* + 1. Переходим обратно в директорию *CA*. Издаем сертификат с расширением *v*3*\_ca*, используя созданные ранее ключ, корневой сертификат и сертификат промежуточного УЦ. В качестве формата криптографического хэширования используем *SHA*1.



**Рисунок 8**. Выдача сертификата корневым УЦ

* + 1. Устанавливаем права на чтение данного сертификата для владельца, группы пользователей и других пользователей (444).
    2. Проверяем действительность сертификата.

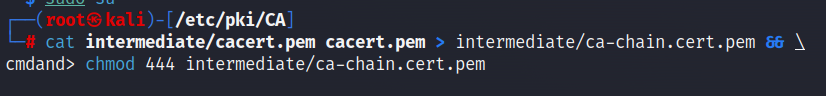


**Рисунок 9**. Проверка действительности созданного сертификата

Сертификат действителен.

## Цепной сертификат

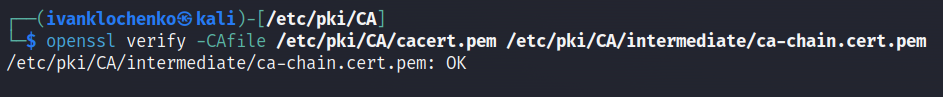
* + 1. Создаем цепной сертификат и устанавливаем права доступа 444.



**Рисунок 10**. Создание цепного сертификата

Примечание: команды выполнялись от лица суперпользователя, так как доступ был запрещен, даже с префиксом *sudo*.

* + 1. Проверяем действительность созданного цепного сертификата.



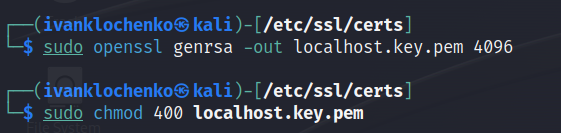
**Рисунок 11**. Проверка действительности цепного сертификата

Сертификат действителен.

# Создание и подписывание сертификатов промежуточных УЦ

## Создание личного ключа веб-сервера

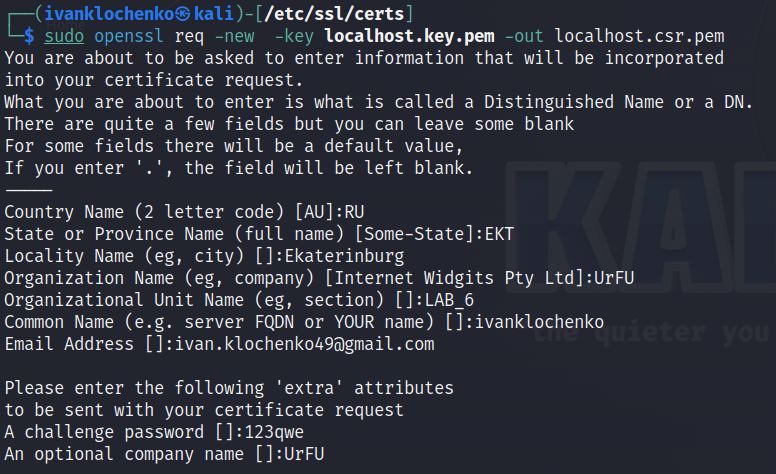
* + 1. Генерируем ключ веб-сервера *localhost*.*key*.*pem*.



**Рисунок 12**. Генерация ключа веб-сервера

## Создание запроса на сертификат

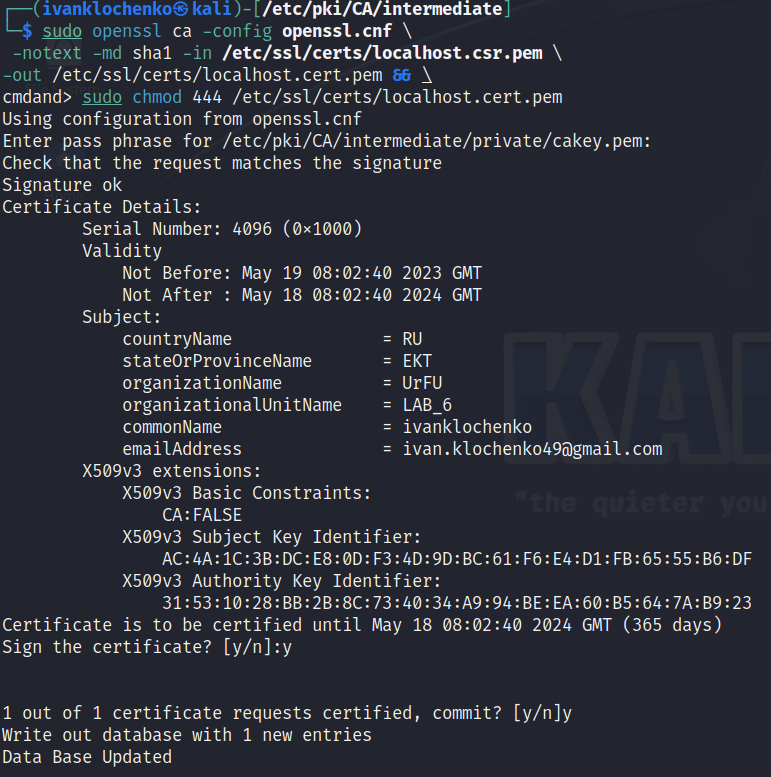
* + 1. Создаем запрос на сертификат.



**Рисунок 13**. Создание запроса на сертификат

## Издание сертификата промежуточным УЦ

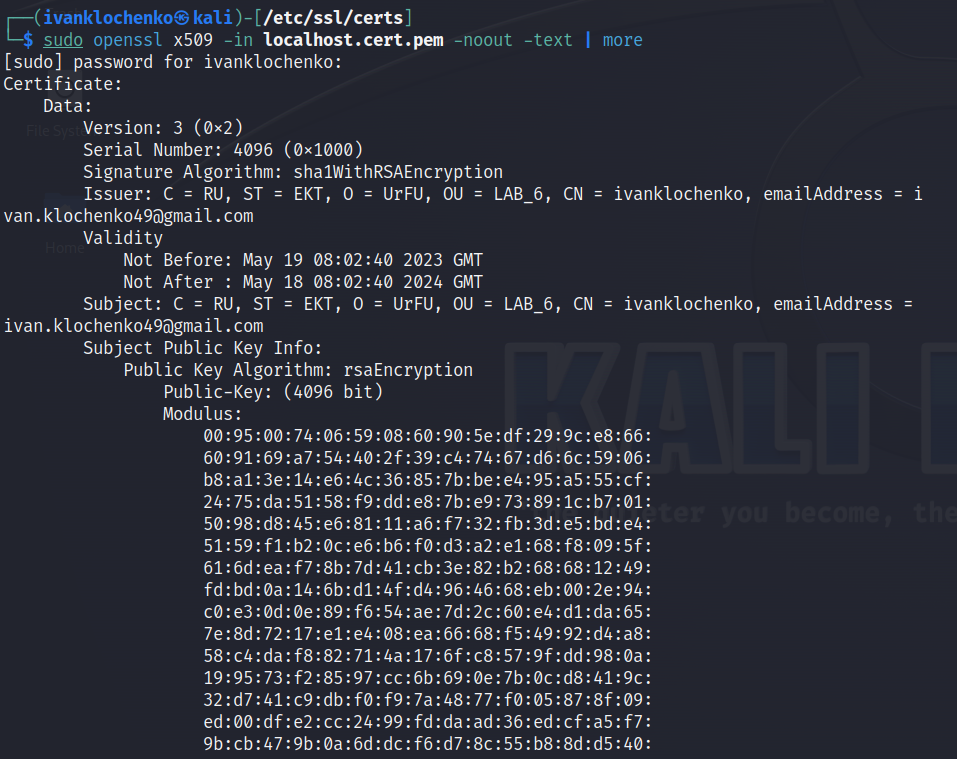
* + 1. Издаем сертификат от имени промежуточного УЦ. Для начала создаем файл сертификата и устанавливаем права доступа на него.



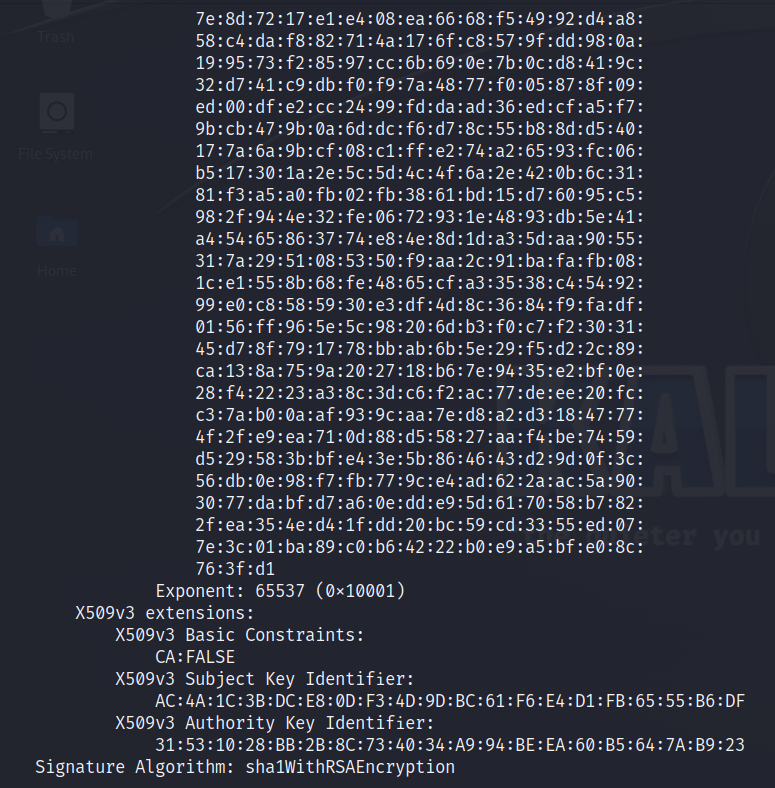
**Рисунок 14**. Создание файла сертификата и установка прав доступа

## Сертификат. Просмотр. Проверка.

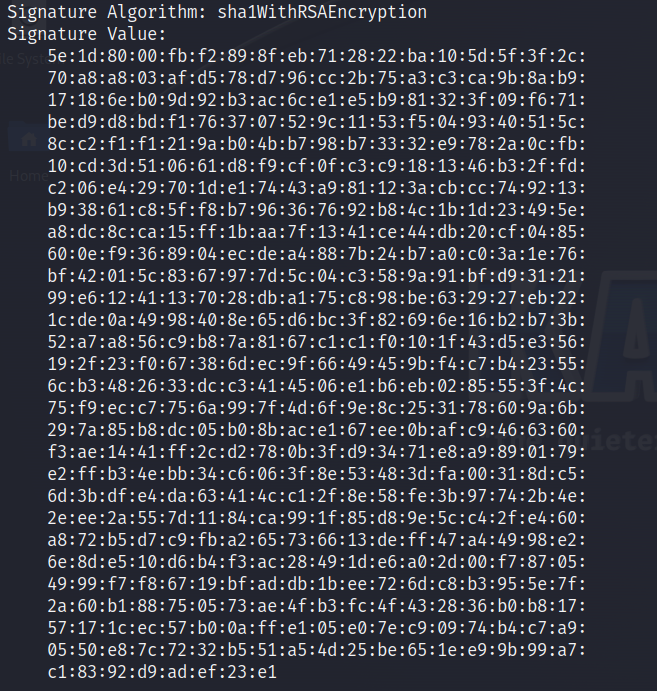
* + 1. Проверяем, верно ли заполнен сертификат.



**Рисунок 15**. Просмотр и визуальная проверка сертификата (1)

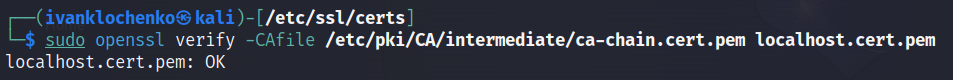


**Рисунок 16**. Визуальная проверка сертификата (2)



**Рисунок 17**. Визуальная проверка сертификата (3)

* + 1. Проверяем сертификат.

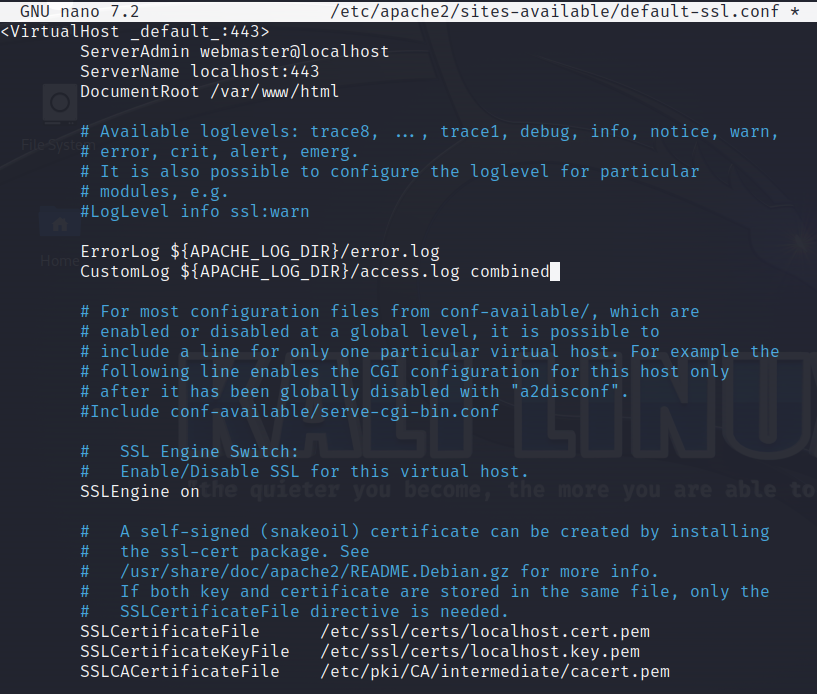


**Рисунок 18**. Проверка сертификата

## Добавление сертификата в конфигурацию веб-сервера

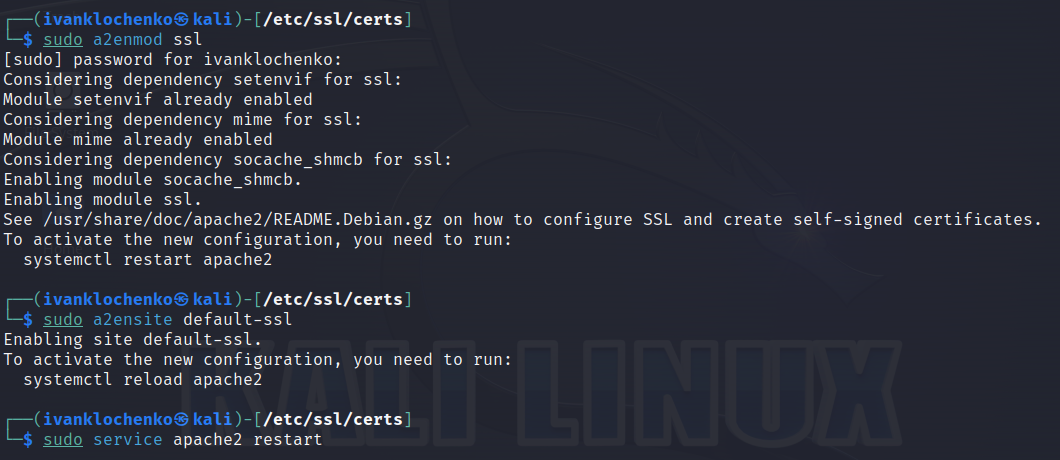
* + 1. Редактируем конфигурационный файл *SSL* для *Apache*2.

Примечание: файл конфигурации *SSL* для *Apache*2 - /*etc*/*apache*2/*sites*-*available*/*default*-*ssl*.*conf*.



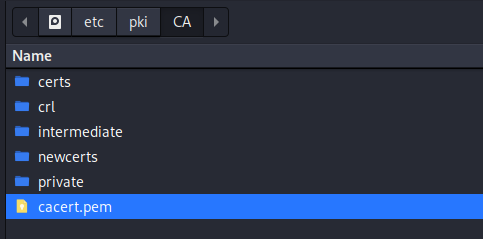
**Рисунок 19**. Редактирование файла конфигурации OpenSSL для Apache2

* + 1. Запускаем веб-сервер с включенной поддержкой защищенных соединений.

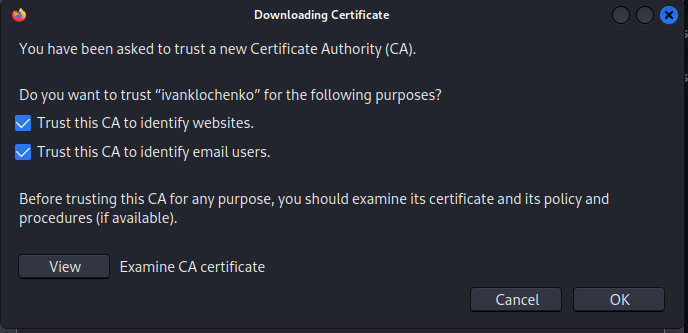


**Рисунок 20**. Запуск веб-сервера с включенной поддержкой защищенных соединений

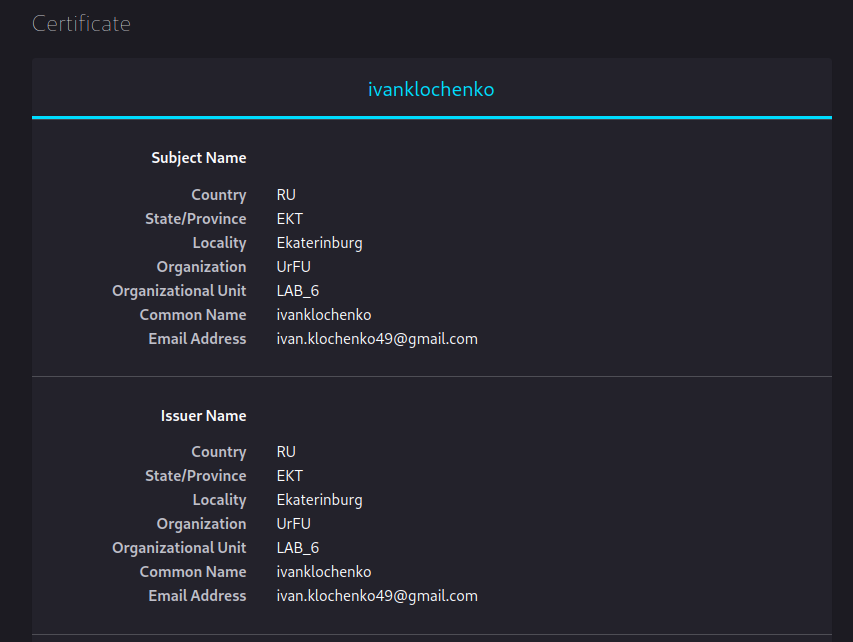
* + 1. Импортируем сертификат УЦ в браузер и проверим защищенное соединение.



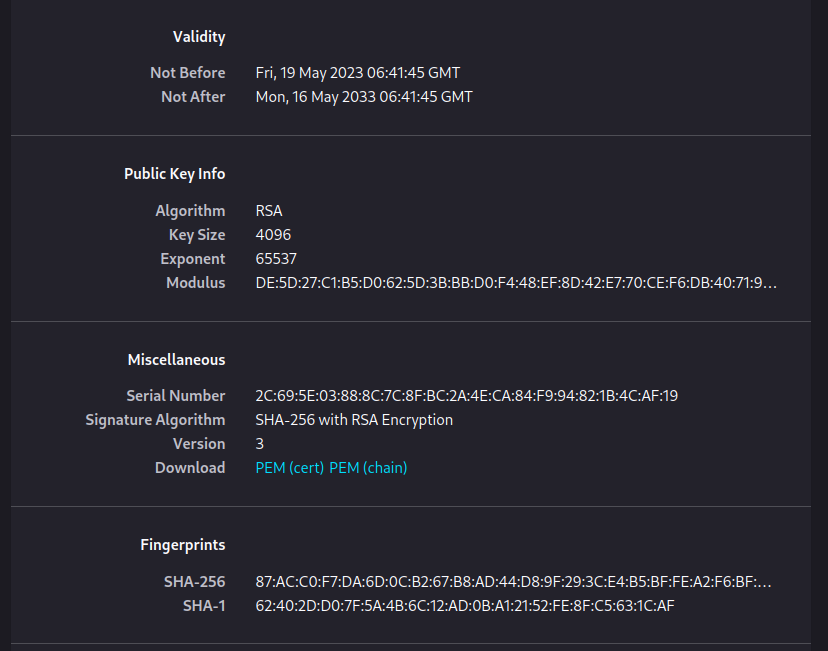
**Рисунок 21**. Выбор сертификата для импорта



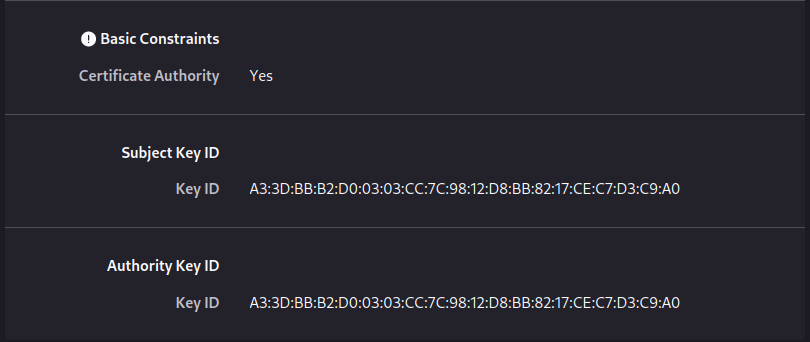
**Рисунок 22**. Импорт сертификата



**Рисунок 23**. Описание сертификата (1)



**Рисунок 24**. Описание сертификата (2)



**Рисунок 25**. Описание сертификата (3)

# Отзыв сертификата

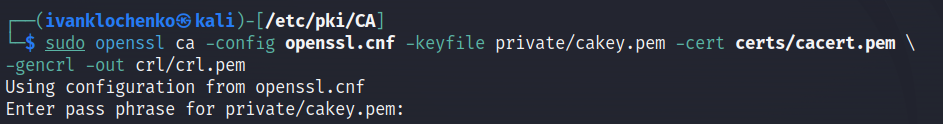
## Список отозванных сертификатов

* + 1. Создадим список отозванных сертификатов.

Для начала нужно инициализировать файл *crlnumber*



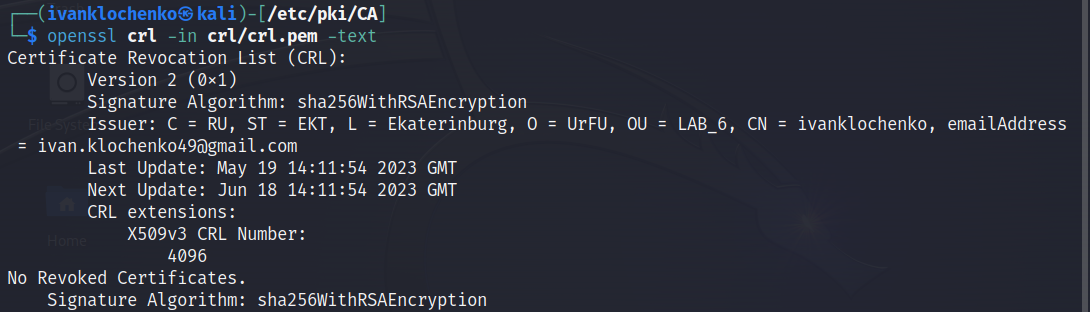
**Рисунок 26**. Инициализация файла crlnumber



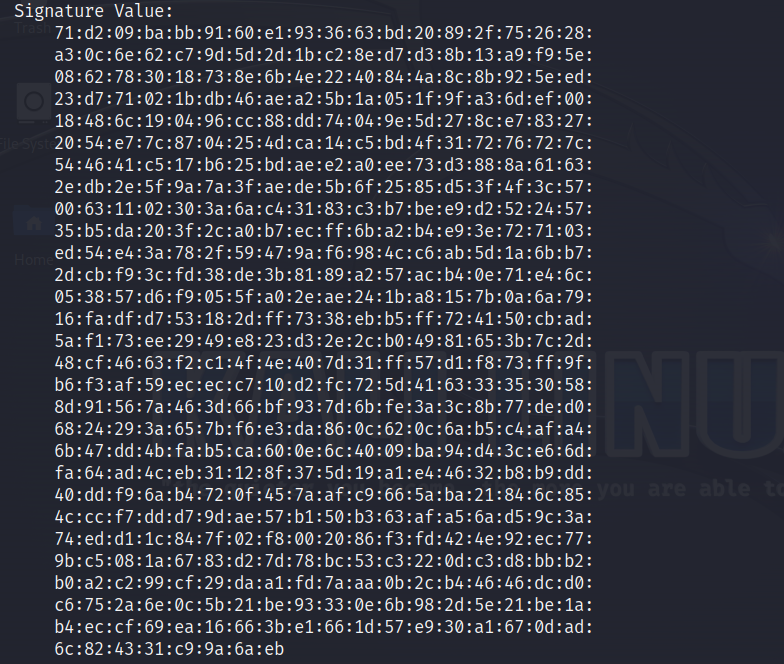
**Рисунок 27**. Создание списка отозванных сертификатов

Важно отметить, что в команде, указанной в методических указаниях, нет дополнительного параметра «-*config* *openssl*.*cnf*». Ее нужно добавить, чтобы избежать ошибок при выполнении команды. В противном случае будет обращение к /*etc*/*ssl*/*openssl*.*cnf*, в котором нет прописанных нами конфигурационных строк.

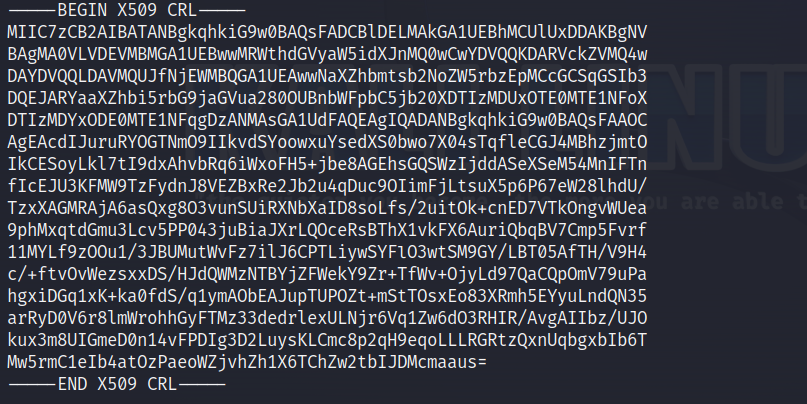
* + 1. Просмотрим получившийся список отозванных сертификатов



**Рисунок 28**. Просмотр отозванных сертификатов (1)



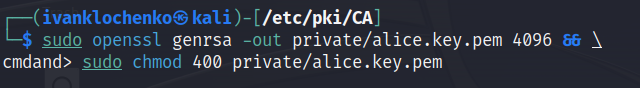
**Рисунок 29**. Просмотр отозванных сертификатов (2)



**Рисунок 30**. Просмотр отозванных сертификатов (3)

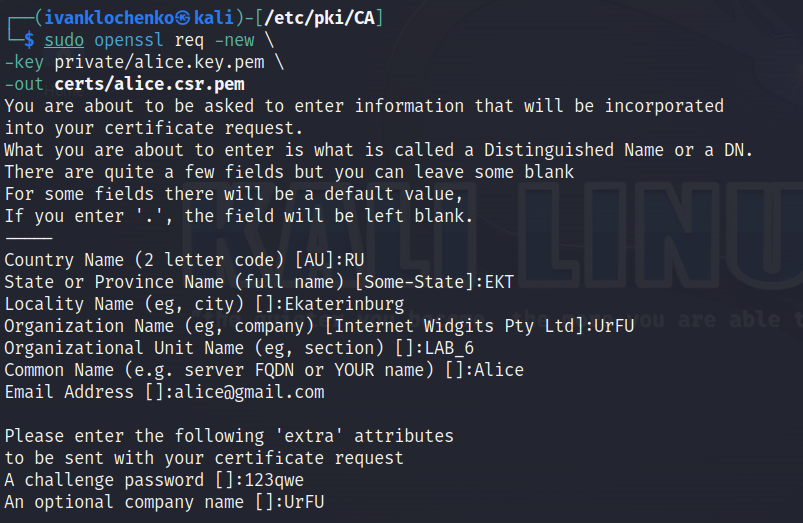
## Создание сертификатов пользователя

* + 1. Создаем ключ пользователя *Alice* и устанавливаем к нему ограниченные права доступа.



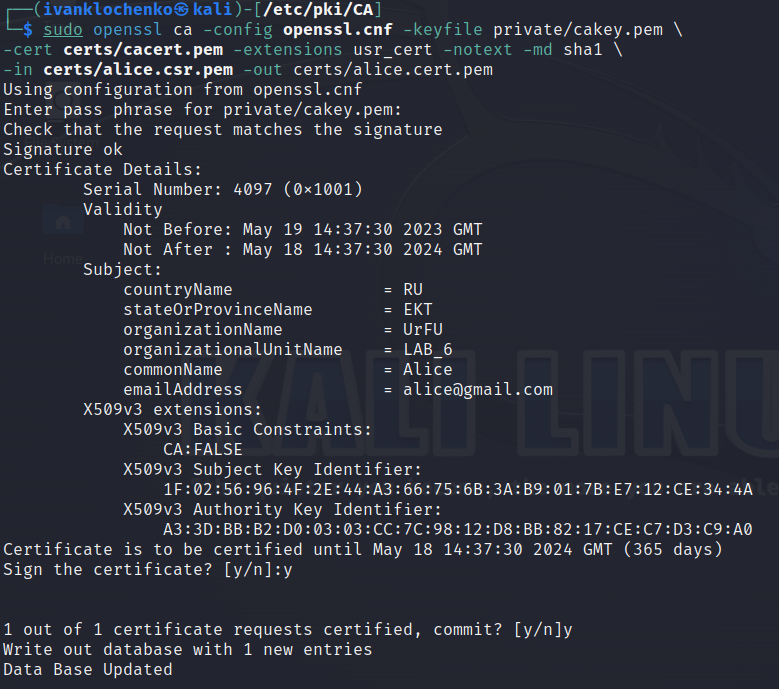
**Рисунок 31**. Создание ключа пользователя Alice

* + 1. Создаем запрос на сертификат от пользователя *Alice*.



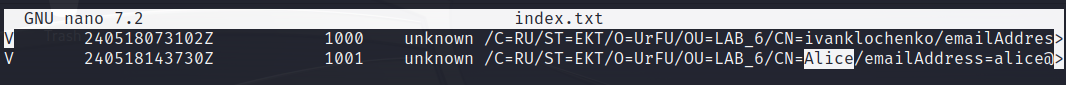
**Рисунок 32**. Создание запроса сертификата от пользователя Alice

* + 1. Выдаем сертификат по ранее сформированному запросу.



**Рисунок 33**. Выдача сертификата по ранее сформированному запросу

* + 1. Ограничиваем права доступа к сертификату.
    2. Проверяем базу данных сертификатов.

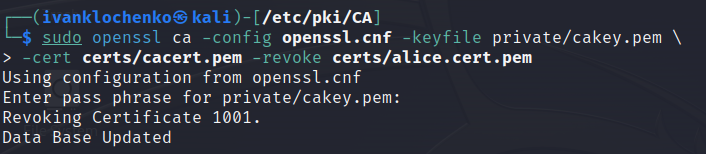


**Рисунок 34**. Проверка базы сертификатов

Созданный сертификат присутствует в БД сертификатов.

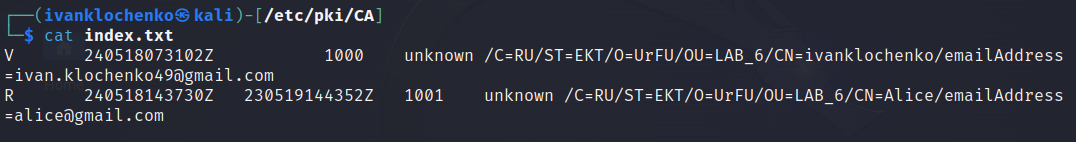
## Отзыв сертификата пользователя

* + 1. Проведем процедуру отозвания сертификата, выданного пользователю *Alice*.



**Рисунок 35**. Отзыв сертификата пользователя Alice

После проведения этой процедуры содержание БД сертификатов изменилось.

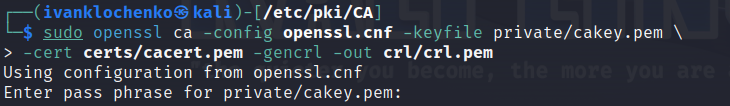


**Рисунок 36**. Содержание БД сертификатов после отзыва сертификата пользователя Alice

Буква, стоящая в начале строки сменилась с «*V*» (*Valid*) на «*R*» (*Revoke*).

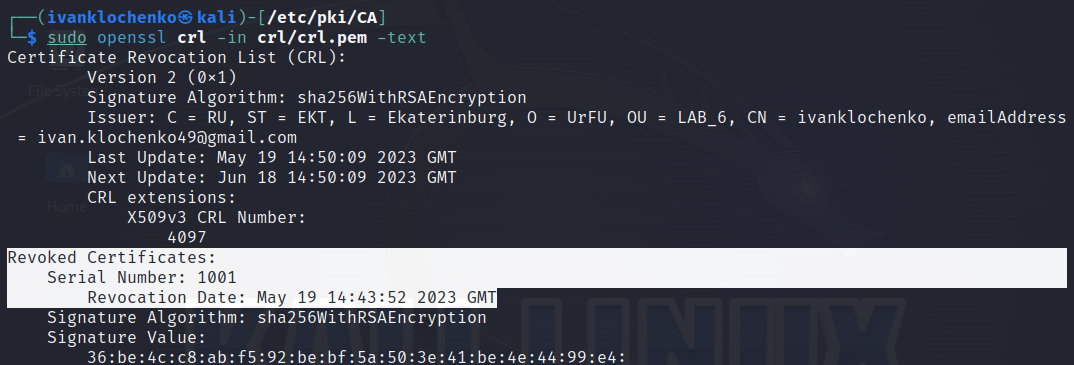
## Обновление списка отозванных сертификатов

* + 1. Производим обновление списка отозванных сертификатов.



**Рисунок 37**. Обновление списка отозванных сертификатов

* + 1. Просматриваем список отозванных сертификатов.



**Рисунок 38**. Список отозванных сертификатов после отзыва сертификатов Alice

Добавилась пометка об отзыве сертификата с указанием серийного номера сертификата *Alice* и даты отзыва сертификата.

# Вывод

В ходе выполнения лабораторной работы были освоены основные навыки работы с УЦ, запросами, изданием и отзывом сертификатов.

Были созданы УЦ, промежуточный УЦ (созданы файловые иерархии, корневой – для УЦ, промежуточный – для промежуточного УЦ, цепной сертификаты, выдан сертификат для промежуточного УЦ).

Проведено создание и подписывание сертификатов промежуточного УЦ: создание личного ключа веб-сервера, создание запроса на сертификат, издание сертификата, добавление сертификата в конфигурацию веб-сервера.

Изучена процедура отзыва сертификата. Был запрошен и издан сертификат для пользователя, после чего отозван. После отзыва сертификата было произведено обновление списка отозванных сертификатов. Проведен анализ содержания БД сертификатов, а также списка отозванных сертификатов, который был заранее создан.