ЛАБОРАТОРНАЯ РАБОТА №3  
«ИЗУЧЕНИЕ ПРИНЦИПА ШИФРОВАНИЯ С ОТКРЫТЫМ КЛЮЧОМ»

**1. Цель работы**

Изучение принципа шифрования с открытым ключом, библиотеки ssl.

**2. Постановка задачи**

Необходимо сгенерировать сертификат УЦ, сгенерировать новый сертификат, подписать сертификат созданным УЦ. Импортировать созданный сертификат в вэб-сервер системы, установленной в лабораторной работе №2.

**3. Ход работы**

Для удобства использования был рассмотрен проект с открытым кодом XCA, в котором для криптографических преобразований используется библиотека OpenSSL.

Для создания сертификата удостоверяющего центра компании необходимо было во вкладке «Закрытые ключи» создать новый ключ (рисунок 1).

На рисунке 2 изображен список закрытых ключей.

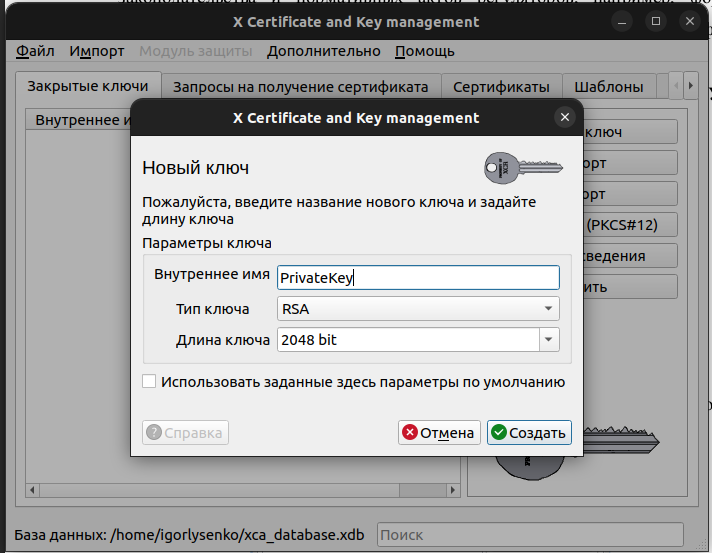


Рисунок 1 – Создание нового приватного ключа

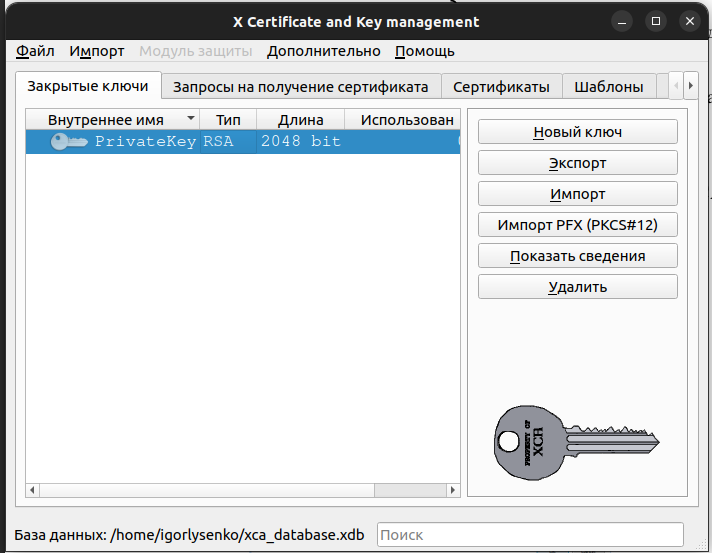


Рисунок 2 – Список приватных ключей

Далее необходимо было перейти во вкладку «Сертификаты» и создать сертификат УЦ компании. Далее необходимо нажать кнопку новый сертификат – вкладка «Первоисточник». Алгоритм подписи – SHA 256

Шаблон для нового сертификата – по умолчанию для УЦ (CA –Certificateauthority).

Все вышеописанные настройки изображены на рисунке 3.

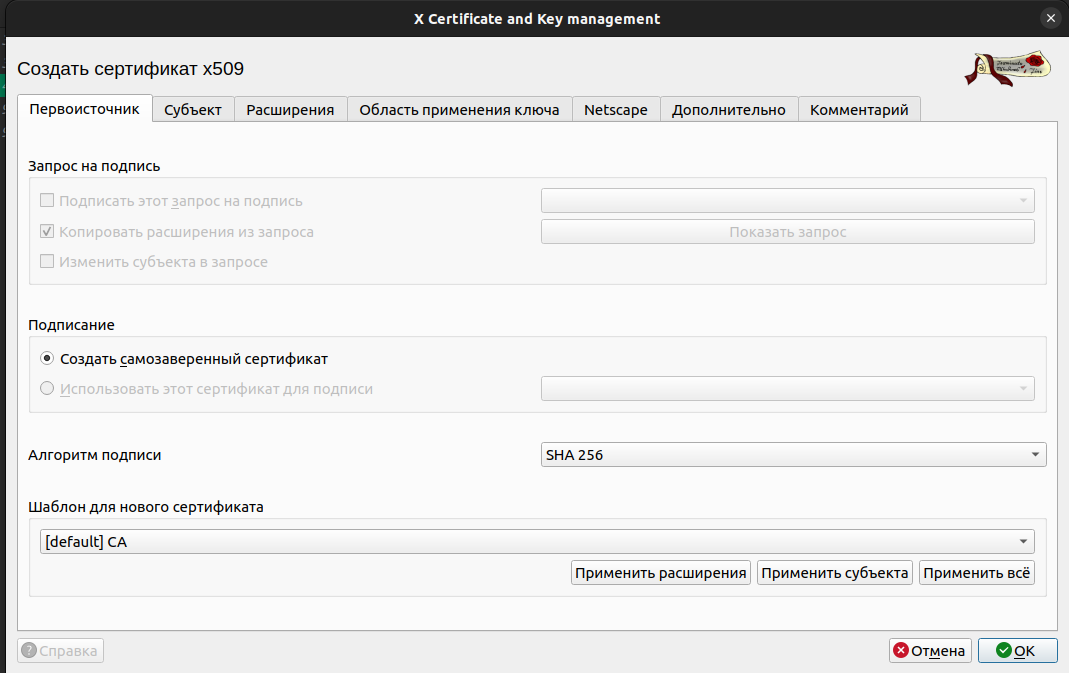


Рисунок 3 – Настройка во вкладке «Первоисточник» для создания сертификата

Далее были заполнены все поля во вкладке «Субъект» (рисунок 4).

Затем во вкладке «Расширение» был выбран тип базового контейнера – Центр Сертификации. Вид данной вкладки изображен на рисунке 5.

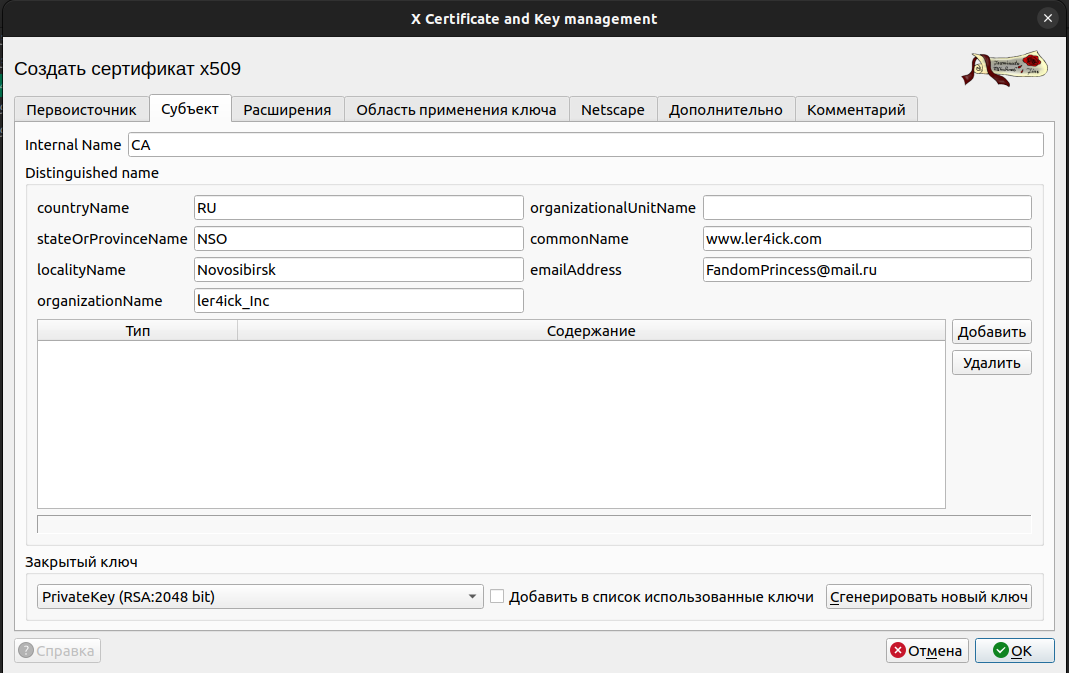


Рисунок 4 – Настройки во вкладке «Субъект»

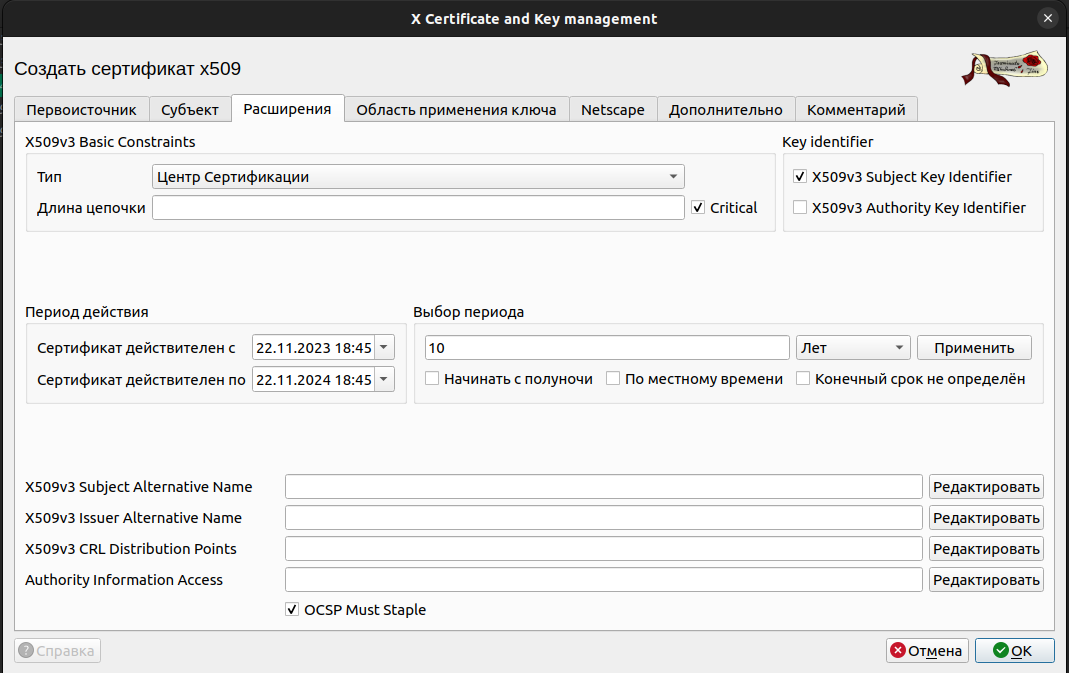


Рисунок 5 – Настройки во вкладке «Расширения»

Во вкладке «Область применения ключа» были выбраны пункты «Certificate Sign» и «CRL Sign» (рисунок 6).

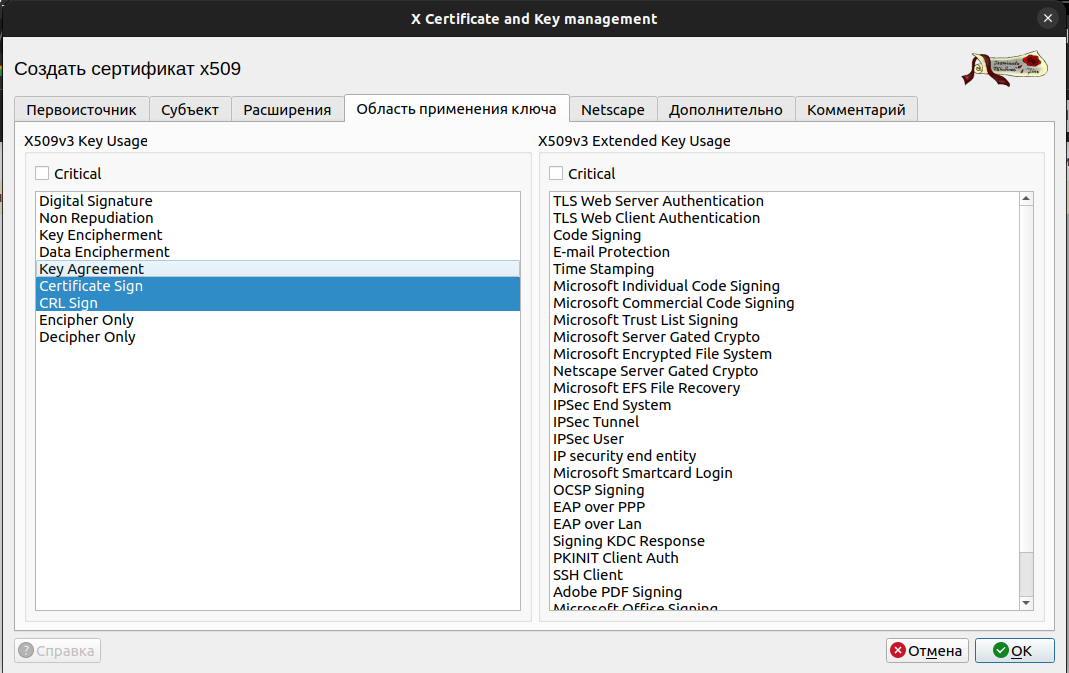


Рисунок 6 – Настройки во вкладке «Область применения ключа»

Вид вкладки «Netscape» представлен на рисунке 7.

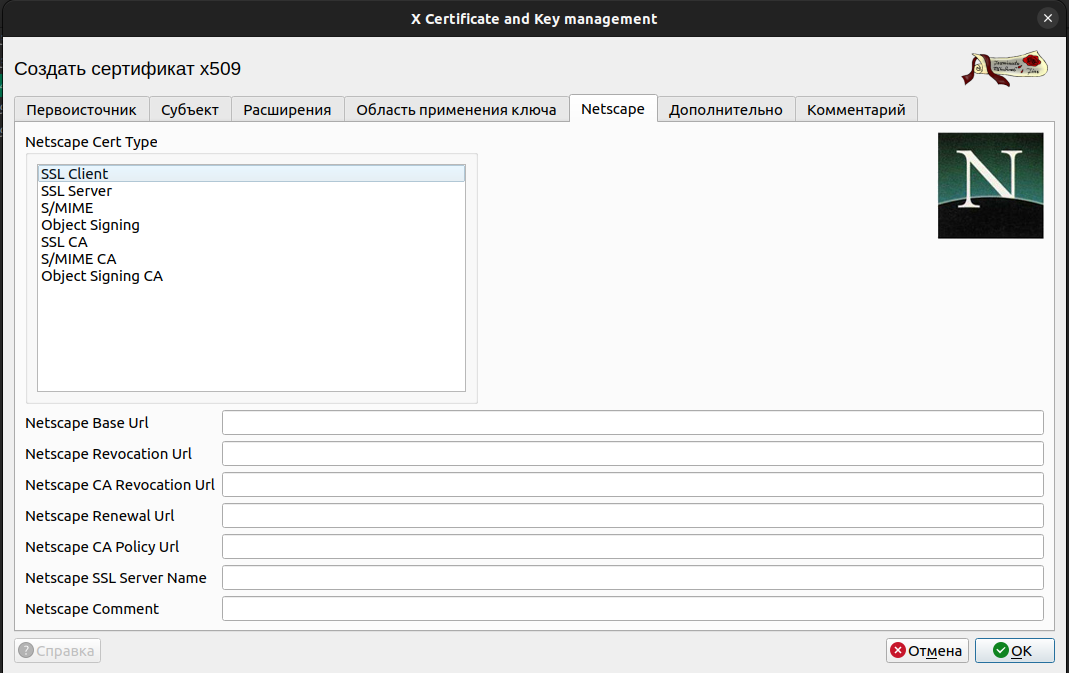


Рисунок 7 – Настройки во вкладке «Netscape»

На этом настройка была завершена и сертификат создан. Посмотреть созданный сертификат можно во вкладке «Сертификаты» (рисунок 8).

На рисунке 9 изображен экспорт сертификата.

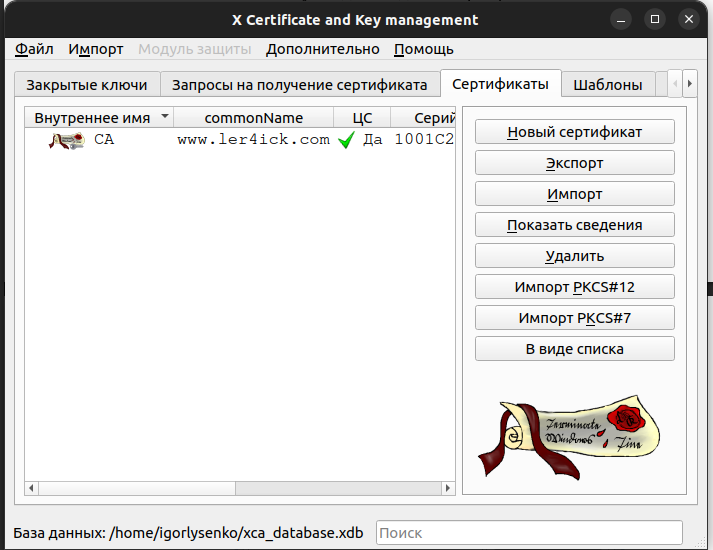


Рисунок 8 – Просмотр сертификатов

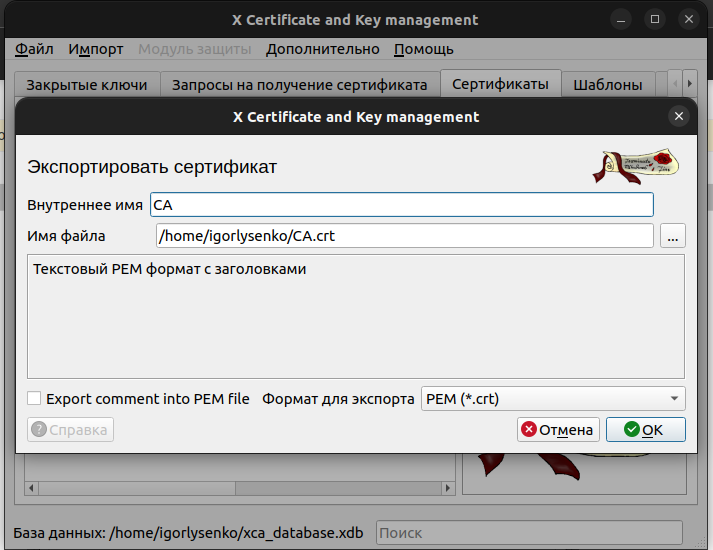


Рисунок 9 – Экспорт сертификата

ВЫВОДЫ

В ходе выполнения лабораторной работы был сгенерирован сертификат УЦ и новый сертификат, а также требовалось подписать сертификат созданным УЦ, что и было сделано.

Контрольные вопросы:

**1. Что такое Удостоверяющий центр?**

Удостоверяющий центр (УЦ) - это доверенная организация, которая выпускает и управляет цифровыми сертификатами. Он играет важную роль в системе публичного ключа (Public Key Infrastructure, PKI) и используется для проверки подлинности и целостности электронной информации.

**2. В чем отличие открытого ключа и сертификата?**

Открытый ключ (public key) - это криптографический ключ, который используется для шифрования данных или проверки цифровой подписи. Сертификат содержит открытый ключ, а также информацию о его владельце, выдавшем органе и сроке его действия. Отличие между открытым ключом и сертификатом заключается в том, что сертификат содержит дополнительные данные и информацию, подтверждающую подлинность открытого ключа.

**3. Какой функционал несет закрытый ключ?**

Закрытый ключ (private key) используется для расшифровки данных, создания цифровой подписи или установления безопасного соединения. Он должен быть хранен в секрете и не должен быть доступен посторонним лицам. Функционал закрытого ключа включает генерацию цифровых подписей, дешифрование зашифрованных данных и установление безопасного соединения с использованием протоколов шифрования.

**4. В чем особенности Формата сертификата \*.pfx?**

Формат сертификата \*.pfx (Personal Information Exchange) является одним из форматов для хранения и передачи сертификатов и соответствующих закрытых ключей. Файл формата \*.pfx обычно защищен паролем и может содержать цепочку сертификатов, закрытый ключ и дополнительные сведения.

**5. Какие УЦ являются доверенными?**

Доверенные удостоверяющие центры (Trusted Certificate Authorities) являются организациями, которым доверяют большинство клиентских устройств и программного обеспечения. Они выпускают сертификаты и гарантируют, что открытые ключи, содержащиеся в сертификатах, связаны с определенными субъектами. Некоторые известные доверенные УЦ включают VeriSign, Comodo, Let's Encrypt, Digicert и другие.

**6. Что такое список отозванных сертификатов?**

Список отозванных сертификатов (Certificate Revocation List, CRL) - это список сертификатов, которые были отозваны УЦ до истечения их срока действия. CRL содержит информацию о сертификатах, подлежащих отзыву, и используется для проверки подлинности сертификатов перед их использованием.

**7. Можно ли с помощью одного закрытого ключа создать несколько сертификатов?**

Нет, каждый сертификат обычно связан с конкретным открытым и закрытым ключом. Для каждого сертификата требуется пара ключей - открытый и закрытый.

**8. Какова основная уязвимость в шифровании с открытым ключом?**

Основная уязвимость в шифровании с открытым ключом связана с возможностью подмены открытого ключа. Если злоумышленник заменяет открытый ключ на свой собственный, то он может перехватывать и расшифровывать зашифрованные сообщения или создавать ложные цифровые подписи от имени других пользователей.

**9. Какие основные форматы файлов открытого ключа и сертификата?**

Основные форматы файлов открытого ключа включают X.509 (обычно с расширением .cer или .pem), PGP (Pretty Good Privacy, с расширением .asc или .pgp) и SSH(.pub). Форматы файлов сертификатов включают X.509 (обычно с расширением .cer или .pem), PKCS#12 (с расширением .pfx) и другие.

**10. Что такое цепочка сертификатов УЦ?**

Цепочка сертификатов УЦ (Certificate Chain) представляет собой иерархическую серию сертификатов, начиная от конечного сертификата и до корневого сертификата УЦ. Цепочка сертификатов позволяет проверить подлинность сертификата путем проверки подписей цепочки от конечного сертификата до доверенного корневого сертификата.

**11. Каким образом сертификаты попадают в список отозванных?**

Сертификаты попадают в список отозванных, когда УЦ обнаруживает, что сертификат больше не является доверенным или его закрытый ключ скомпрометирован. При обнаружении таких ситуаций УЦ отзывает сертификат и включает его в CRL или в список отозванных сертификатов, чтобы клиенты могли проверить его статус перед использованием.

**12. Как производится браузером проверка сертификата?**

Проверка сертификата браузером включает несколько шагов. Браузер проверяет цепочку сертификатов от конечного сертификата до доверенного корневого сертификата, проверяя подписи каждого сертификата. Он также проверяет действительность сертификата, срок его действия и его статус в списке отозванных сертификатов. Если сертификат прошел успешную проверку, браузер отображает зеленую пиктограмму или замок, указывая на безопасное соединение с веб-сайтом.