

Упрощенная пошаговая инструкция по установке и настройке программного комплекса «Центр Сертификации» из состава программного комплекса «Сигнатура-сертификат L» версия 6 в рамках тестового удостоверяющего центра на Astra Linux

Данный документ содержит пошаговую упрощенную инструкцию по установке и настройке программного комплекса (ПК) «Центр сертификации» (далее — ПК ЦС), входящего в состав ПК ВАМБ.00128-06 «Сигнатура-сертификат L» версия 6» (далее — ПК «Сигнатура-сертификат L») в рамках тестового удостоверяющего центра (УЦ) на операционную систему специального назначения (ОС СН) «Astra Linux Special Edition» РУСБ.10015-16 исполнение 1 («Смоленск»).

Данная инструкция предназначена **только для тестирования** и не применима для установки и настройки аккредитованного УЦ.

Шаг 1. Установка необходимых пакетов

Для корректной установки ПК «Сигнатура-сертификат L» необходимо установить все необходимые для его работы пакеты и ODBC-драйвер с дистрибутива Astra Linux Special Edition следующей командой в терминале FLY (выполненной с правами пользователя **root**):

```
sudo apt-get install libccid pcscd libcurl3 libsasl2-modules-gssapi-mit odbc-postgresql
```

Для корректной установки и настройки СУБД PostgreSQL в дистрибутиве Astra Linux Special Edition необходимо установить СУБД PostgreSQL в процессе установки ОС, пометив для установки **программное обеспечение СУБД** в диалоговом окне «**Выбор программного обеспечения**» процедуры установки ОС.

Если во время установки ОС СУБД PostgreSQL не был установлен, можно выполнить его установку вручную командой (выполненной с правами пользователя **root**):

```
sudo apt-get install postgresql-astra
```

или

```
sudo apt-get install postgresql
```

Шаг 2. Установка ПО компании Валидата

После установки всех необходимых пакетов можно приступить к процессу установки ПК «Сигнатура-сертификат L». Перед установкой ПК «Сигнатура-сертификат L» на ЭВМ необходимо предварительно установить ПК «Сигнатура-клиент L» версия 6 следующей командой (выполненной с правами пользователя **root**):

```
sudo dpkg -i spki-6.0.451.0-0.amd64.deb
```

Установка ПК «Сигнатура-сертификат L» выполняется следующей командой (выполненной с правами пользователя **root**):

```
sudo dpkg -i scara-6.0.452.0-0.amd64.deb
```

Примечание: необходимо указывать полные пути до установочных пакетов.

После установки ПО машину необходимо будет **перезагрузить**, чтобы изменения, внесенные во время установки, вступили в силу для всех пользователей машины, в том числе пользователя **postgres**, с помощью которого осуществляется настройка СУБД PostgreSQL.

Шаг 3. Настройка СУБД PostgreSQL

Перед началом работы с ПК ЦС необходимо провести настройку ОС и развернуть базу данных.

Примечание: Для ОС Astra Linux Special Edition версии 1.8 на уровне защищенности <<Смоленск>> необходимо назначить высокий уровень целостности для пользователя **postgres** командой вида:

```
sudo pdpl-user -i 63 postgres
```

Для настройки СУБД PostgreSQL необходимо переключиться на пользователя **postgres** следующей командой (выполненной с правами пользователя **root**):

```
sudo su postgres
```

Далее необходимо запустить утилиту **psql** СУБД PostgreSQL, выполнив следующую команду:

```
psql
```

Для функционирования подчиненного Центра Сертификации (ЦС) в режиме администратора необходимо создать две базы данных для локального хранилища и базы сертификации УЦ следующими SQL-запросами:

```
CREATE DATABASE "CALOC" WITH ENCODING='WIN1251' LC_COLLATE='ru_RU.cp1251'  
LC_CTYPE='ru_RU.cp1251' CONNECTION LIMIT=-1 TEMPLATE template0;
```

```
CREATE DATABASE "CABASE" WITH ENCODING='WIN1251' LC_COLLATE='ru_RU.cp1251'  
LC_CTYPE='ru_RU.cp1251' CONNECTION LIMIT=-1 TEMPLATE template0;
```

Далее необходимо создать пользователя базы данных и задать для него пароль. **Внимание:** поскольку в данном варианте ОС пользователь СУБД должен одновременно быть пользователем ОС, **имя пользователя базы данных обязательно должно совпадать с именем пользователя ОС** (далее для пример будем использовать имя пользователя **adminca**). Для создания пользователя СУБД необходимо выполнить SQL-запрос вида:

```
CREATE USER adminca WITH PASSWORD '1qaz2wsx';
```

Для разрешения полного доступа пользователя СУБД к схеме **public** созданных ранее БД необходимо выполнить SQL-запросы вида:

```
GRANT CONNECT ON DATABASE "CALOC" TO adminca;
```

```
GRANT CONNECT ON DATABASE "CABASE" TO adminca;
```

Примечание: Для корректной работы с СУБД PostgreSQL/Postgres Pro версий 15 и выше необходимо дать пользователю СУБД доступ к схеме **public** созданных баз данных выполнив SQL-запросы вида:

```
\c "CALOC";
```

```
GRANT USAGE, CREATE ON SCHEMA public TO adminca;
```

```
\c "CABASE";
```

```
GRANT USAGE, CREATE ON SCHEMA public TO adminca;
```

После успешного выполнения всех вышеописанных SQL-запросов пользователь может выйти из утилиты **psql** следующей командой:

```
\q
```

Чтобы выйти из сеанса пользователя **postgres**, необходимо выполнить следующую команду:

```
exit
```

Шаг 4. Настройка мандатного разграничения доступа

У пользователя СУБД (и, следовательно, ОС) должны присутствовать права на чтение атрибутов мандатного разграничения доступа (Mandatory Access Control, MAC). Дать пользователю СУБД права на чтение атрибутов MAC можно вручную следующей командой (выполненной с правами пользователя **root**):

```
sudo pdpl-user -l 0:0 adminca
```

Примечание: Эти права выдаются автоматически, если пользователь был создан с помощью программы управления политикой безопасности ОС («Приложения» - «Панель управления» - «Безопасность» - «Политика безопасности» - «Пользователи» - «Создать новый элемент»).

Шаг 5. Настройка ODBC подключения к СУБД

После задания всех необходимых настроек БД и пользователя ОС, необходимо создать **ODBC** имя источника данных (Data Source Name, DSN), используемых для хранения персонального и локального справочников Центра Сертификации. DSN представляет собой секцию (с именем данного DSN) конфигурационного INI-файла, полностью описывающую подключение к БД сервера СУБД.

Создавать пользовательские (т.е. доступные конкретному пользователю ОС) DSN следует посредством создания и редактирования конфигурационного INI-файла **\$HOME/.odbc.ini**.

Внимание: имя файла обязательно должно содержать точку в начале, что помечает его в файловой системе как скрытый. Создать пустой файл в домашней папке пользователя можно следующими командами:

```
cd
```

```
kate .odbc.ini
```

Пример описания DSN для доступа к БД под управлением СУБД PostgreSQL в файле **.odbc.ini** приведен ниже:

```
[CALOC]
```

```
Driver = /usr/lib/x86_64-linux-gnu/odbc/psqlodbcw.so
```

```
Servername = 127.0.0.1
```

```
Port = 5432
```

```
Database = CALOC
```

```
ConnSettings = SET CLIENT_ENCODING TO 'Windows-1251'
```

[CABASE]

Driver = /usr/lib/x86_64-linux-gnu/odbc/psqlodbcw.so

Servename = 127.0.0.1

Port = 5432

Database = CABASE

ConnSettings = SET CLIENT_ENCODING TO 'Windows-1251'

После внесения изменений сохраните изменения в файл.

Шаг 6. Настройка ПК ЦС

После установки ПК ЦС можно приступить к его настройке.

Для нормальной работы ПК ЦС необходимо задать настройки его сервиса. Запустите ПК ЦС из меню «**Приложения**» - «**Системные**» - «**Центр Сертификации**». В качестве режима работы выберите **режим администратора**. В главном окне приложения выберите пункт меню «**Настройки**» - «**Настройки Сервиса Центра Сертификации**» (Рисунок 1).

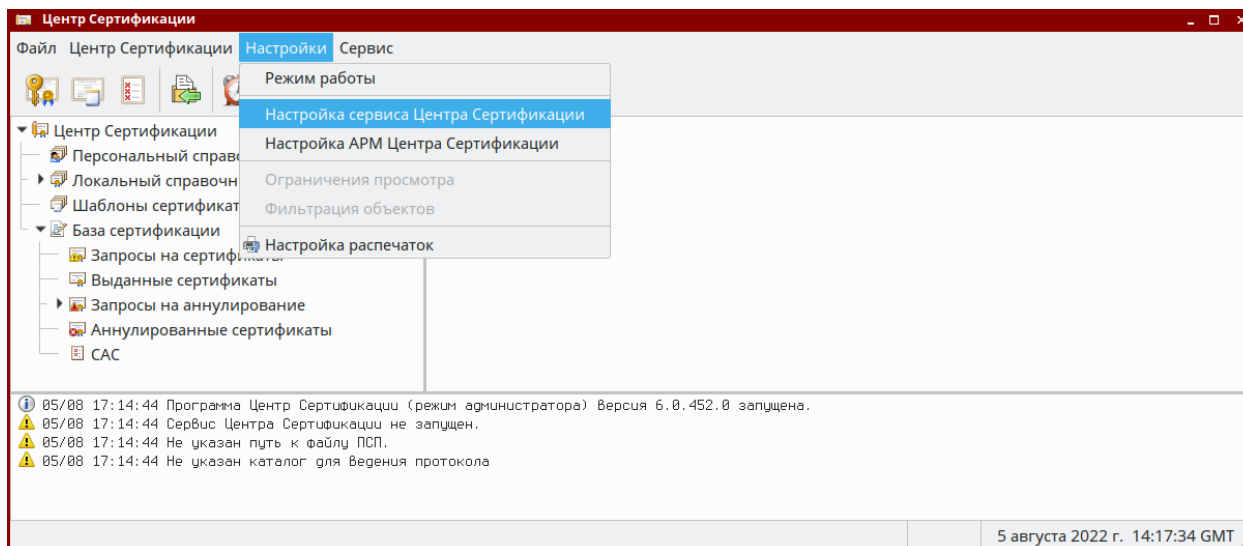


Рисунок 1 - Выбор пункта меню «Настройки Сервиса Центра Сертификации»

В окне настроек сервиса необходимо задать каталог ведения протокола во вкладке «**Общие настройки**» (Рисунок 2).

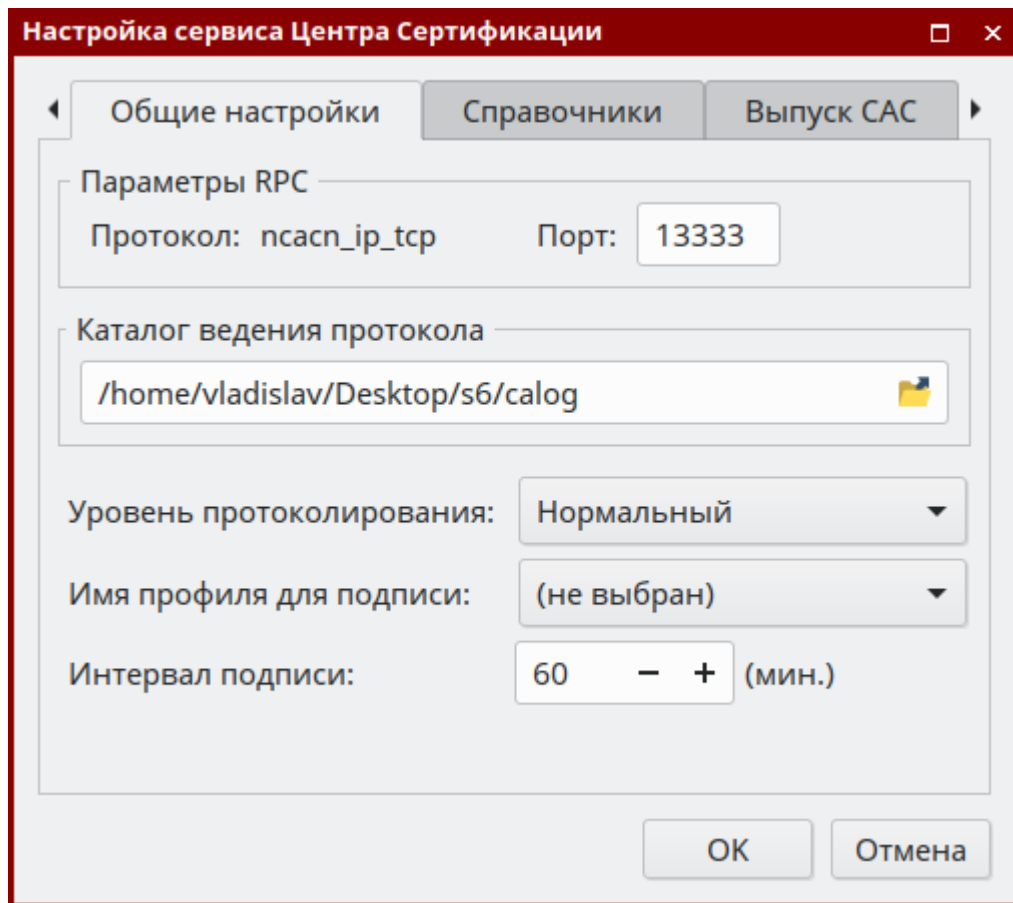


Рисунок 2 - Вкладка настроек сервиса «Общие настройки»

Далее во вкладке «**Справочники**» необходимо задать путь к каталогу, в котором будет создан Персональный Справочник Пользователя (ПСП) и имена ODBC подключений к базам данных локального хранилища сертификатов и базы сертификации (Рисунок 3).

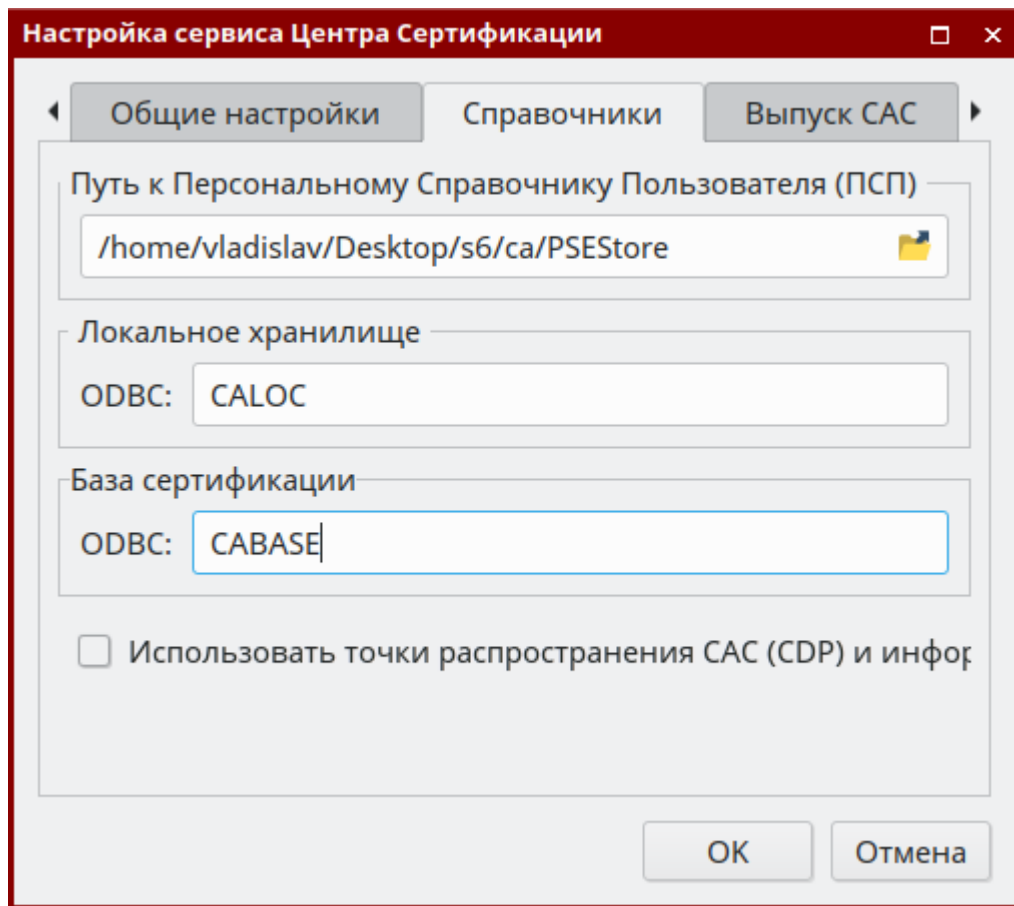


Рисунок 3 - Вкладка настроек сервиса «Справочники»

Шаг 7. Правка файла конфигурации ПК ЦС

После нажатия кнопки «**OK**» настройки ПК ЦС будут сохранены в файле `$HOME/.Validata/spki.ini`, находящемся в скрытой папке в домашнем каталоге пользователя ОС. Открыть этот файл для редактирования можно с помощью следующих команд:

```
cd
```

```
kate .Validata/spki.ini
```

В открытом файле необходимо задать имя и пароль пользователя СУБД, под учетной записью которого будет осуществляться доступ к БД. Для этого необходимо найти раздел «Parameters» и отредактировать строковые значения PkiODBCUsername и PkiODBCPassword.

```
[Parameters]
```

```
...
```

```
PkiODBCUsername = adminca
```

```
PkiODBCPassword = 1qaz2wsx
```

```
...
```

Шаг 8. Создание PKCS#10 запроса на получение сертификата Центра Сертификации

Подчиненный ЦС получает свой сертификат ключа проверки ЭП в вышестоящем УЦ.

При развертывании подчиненного УЦ для формирования запроса на получение сертификата ЦС, предназначенного для отправки в вышестоящий УЦ, необходимо выбрать пункт меню «**Центр Сертификации**» – «**Создать запрос на сертификат Центра Сертификации (в формате PKCS#10)**» (Рисунок 4).

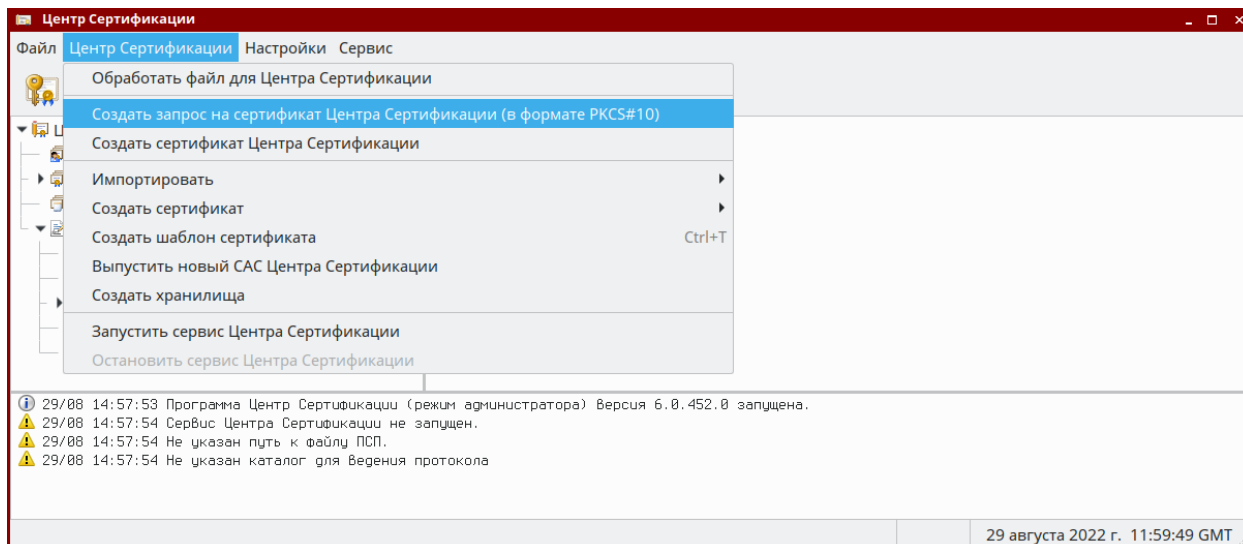


Рисунок 4 - Выбор пункта меню «Создать запрос на сертификат Центра Сертификации (в формате PKCS#10)»

Если у Администратора ЦС есть XML файл данных со всеми атрибутами, требуемыми для формирования сертификата ЦС, то в стартовом диалоге мастера создания запроса на сертификат ЦС (Рисунок 5) его можно указать с помощью кнопки «Выбрать», в противном случае все необходимые атрибуты нужно будет указать вручную в диалоговых окнах мастера создания запроса на сертификат. Нажмите кнопку «**Далее**» чтобы продолжить.

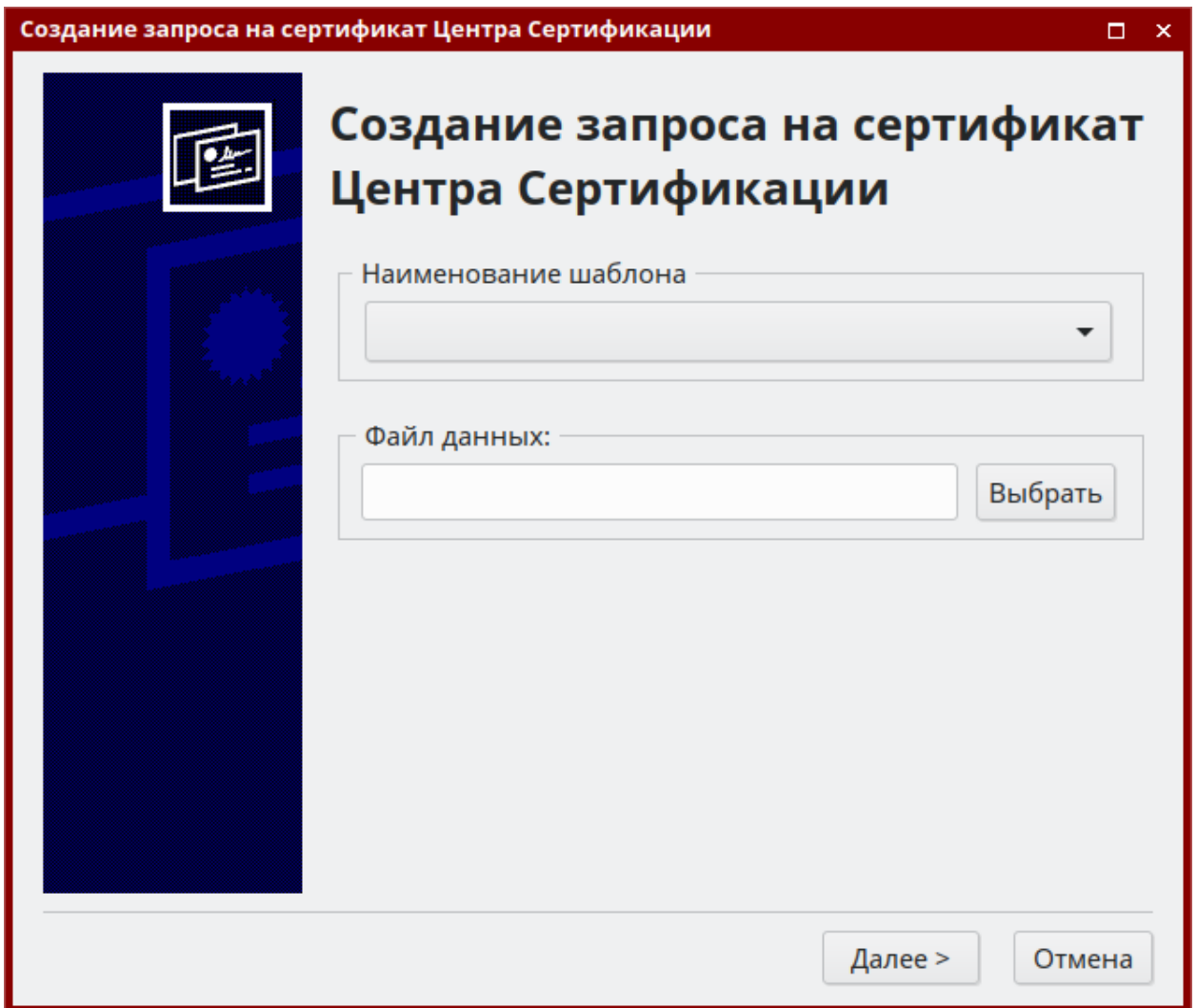


Рисунок 5 - Стартовый диалог мастера создания запроса на сертификат ЦС

Далее необходимо заполнить атрибуты сертификата. В первом диалоге (Рисунок 6) необходимо задать X.500-имя. При выпуске следующих сертификатов ЦС (смене ключа ЦС) X.500-имя останется таким же, как и при первом их задании. После ввода данных нажмите кнопку «**Далее**».

Создание запроса на сертификат Центра Сертификации

Имя владельца сертификата
Заполните атрибуты сертификата

Параметр	Значение
Должность (T)	
Неструктурированное имя (unstructuredName)	
Неструктурированный адрес (unstructuredAddress)	
ОГРН (OGRN)	
ОГРНИП (OGRNIP)	
СНИЛС (SNILS)	
ИНН (INN)	
ИНН юридического лица (INNLE)	
Фамилия (SN)	
Приобретенное имя (GN)	
Общее имя (CN)	
Общее имя (CN)	
Организация (O)	
Название улицы, номер дома (street)	
Населённый пункт (L)	
Город, Область (ST)	
Страна (C)	
Почтовый адрес RFC822 (Email)	
Доменное имя (DC)	
Подразделение (OU)	

< Назад Далее > Отмена

Рисунок 6 - Диалог заполнения X.500-имени

После этого необходимо задать срок действия сертификата и срок действия ключа ЭП Администратора (Рисунок 7). После нажмите кнопку «**Далее**».

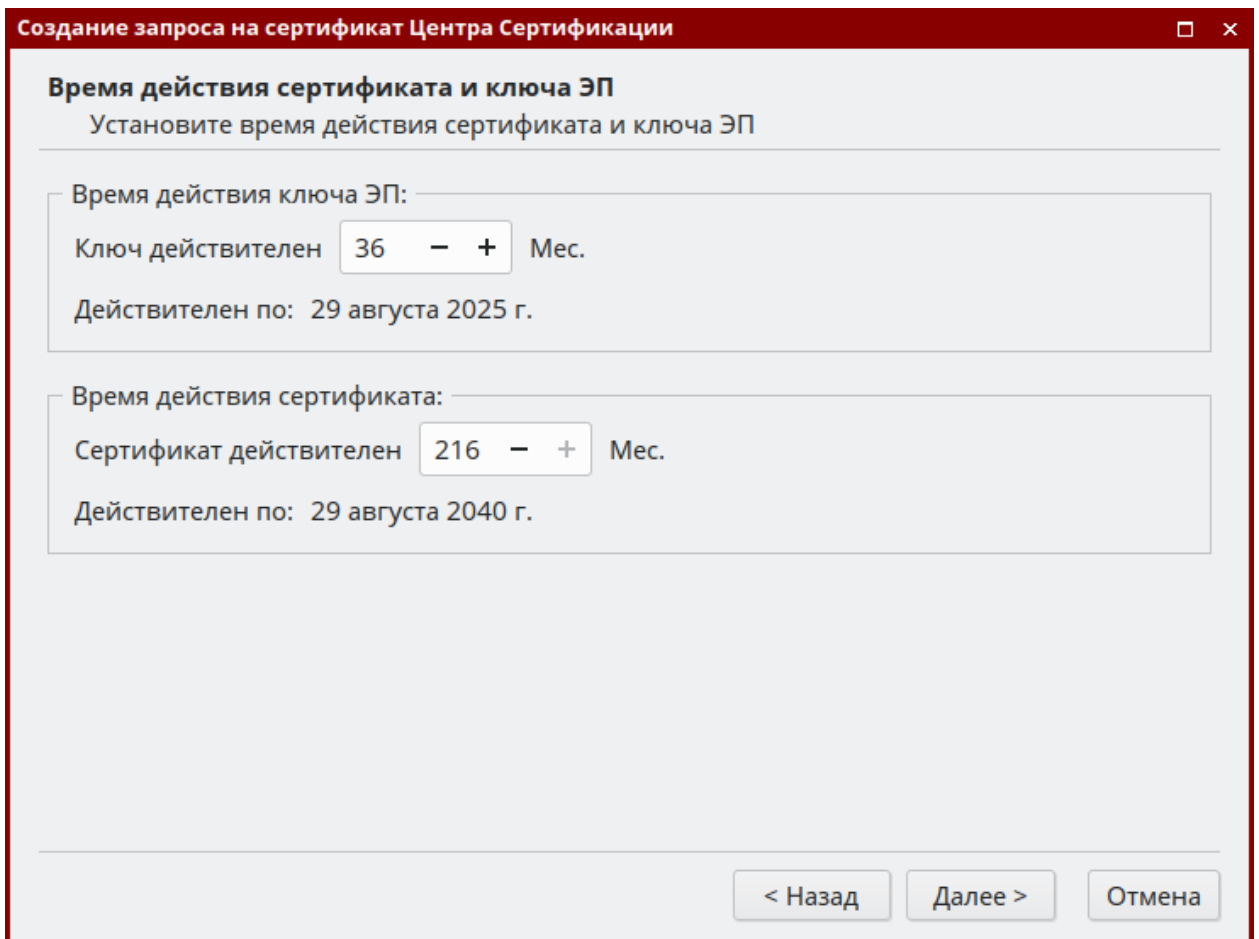


Рисунок 7 - Диалог выбора срока действия сертификата и срока действия ключа ЭП Администратора

Затем необходимо установить максимальное количество уровней иерархии (Рисунок 8).
Рекомендуется установить уровень 0. После нажмите кнопку «**Далее**».

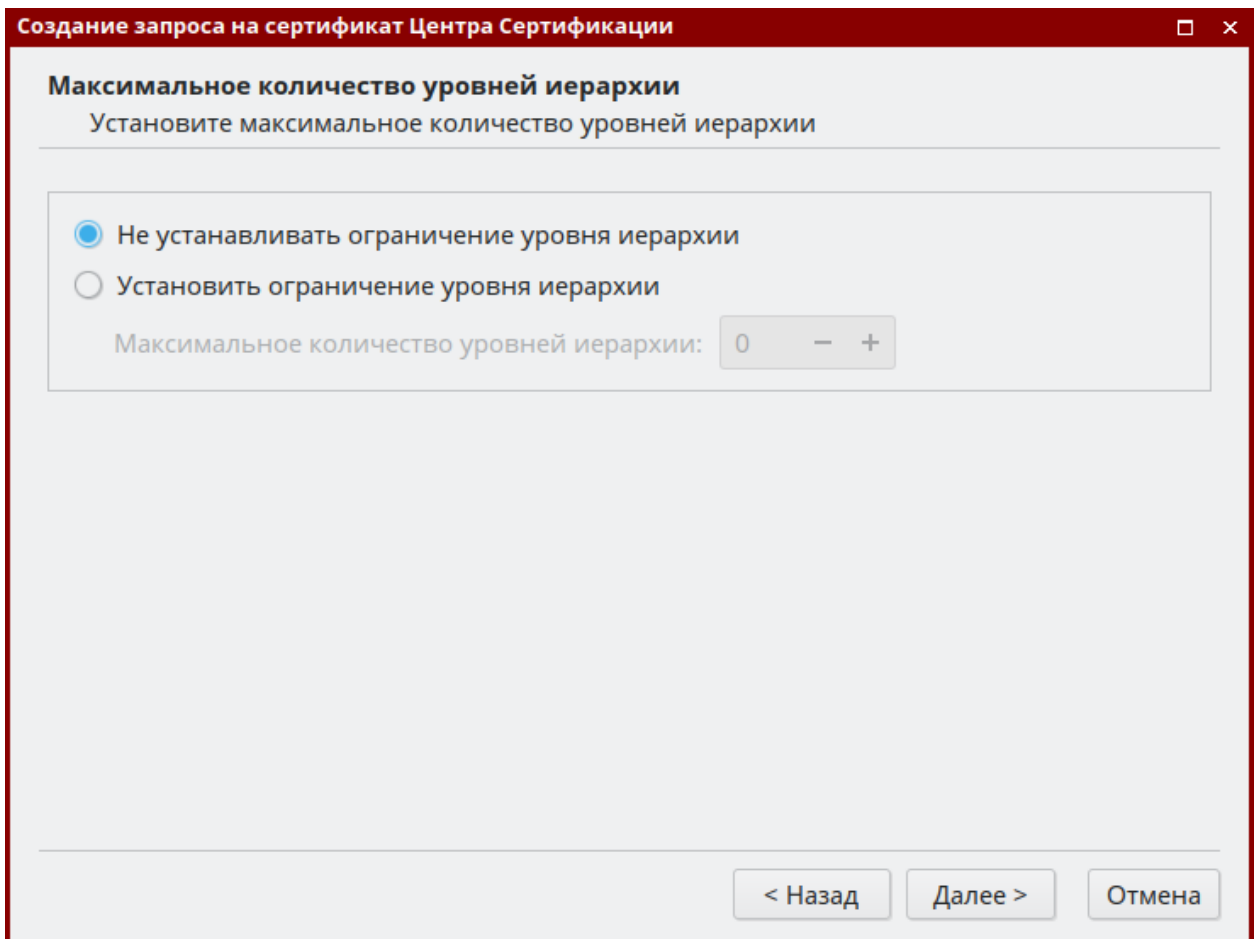


Рисунок 8 - Диалог выбора максимальное количество уровней иерархии

После этого необходимо задать дополнительные регламенты сертификата (Рисунок 9) и нажать кнопку «Далее».

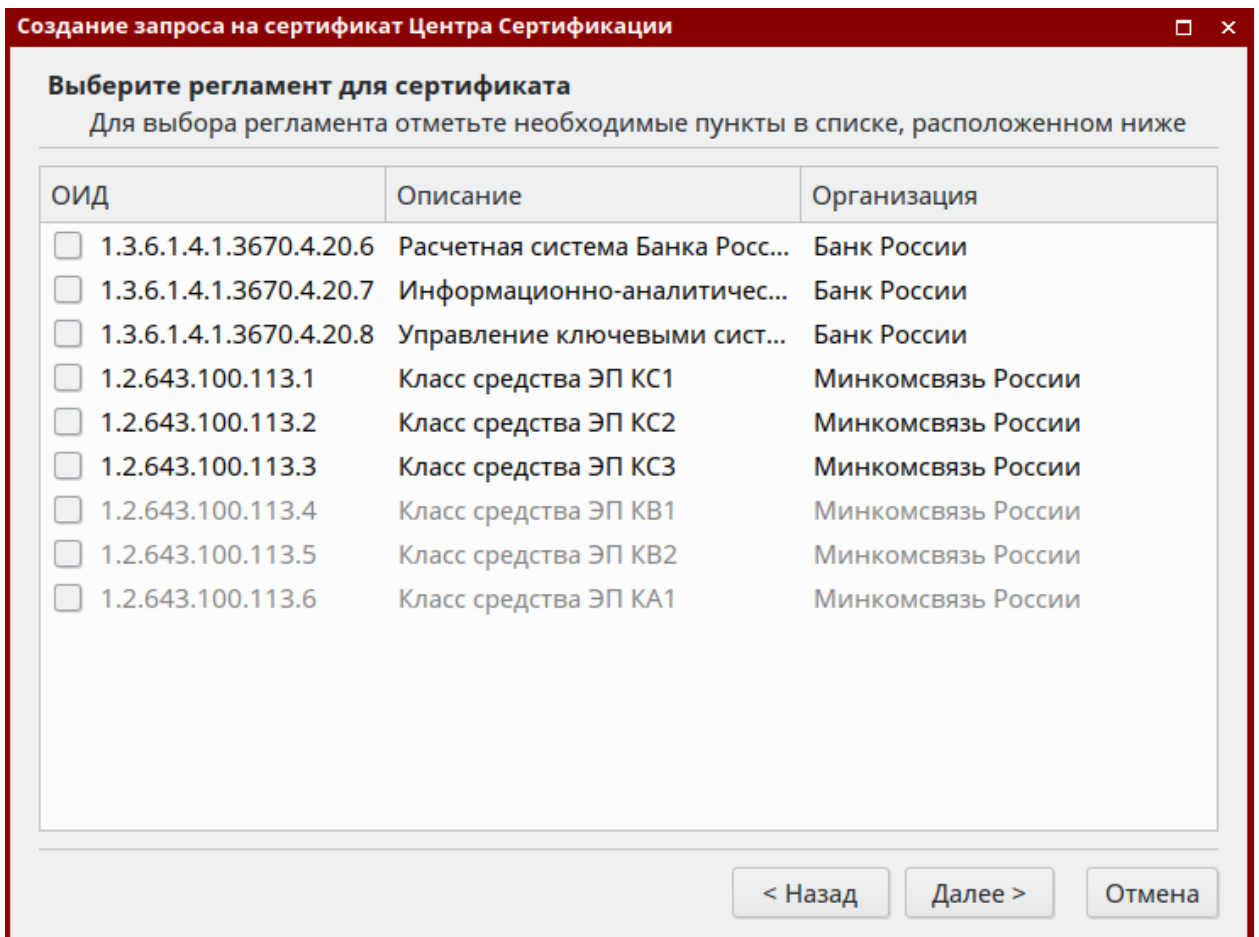


Рисунок 9 - Диалог выбора дополнительных регламентов сертификата

В следующем диалоге необходимо выбрать дополнения для сертификата и тип идентификации (Рисунок 10). После нажмите кнопку «**Далее**».

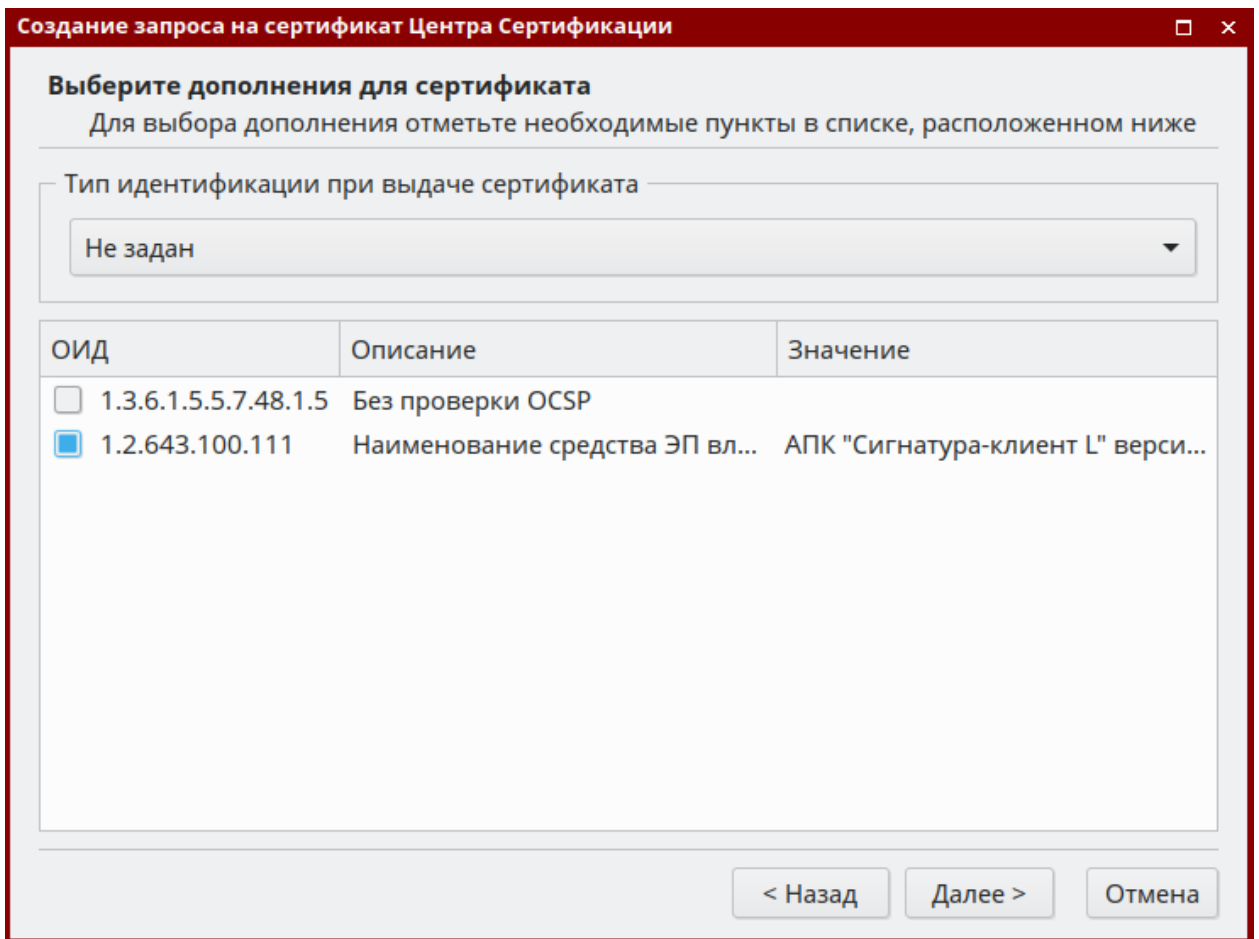


Рисунок 10 - Диалог выбора дополнений для сертификата и типа идентификации

Следующий диалог позволяет задать дополнительные атрибуты в дополнении Альтернативное Имя Владельца сертификата (Рисунок 11). В случае ЦС данное дополнение может быть не использовано или использоваться как информативное. После ввода и проверки всех введенных данных нажмите кнопку «**Готово**».

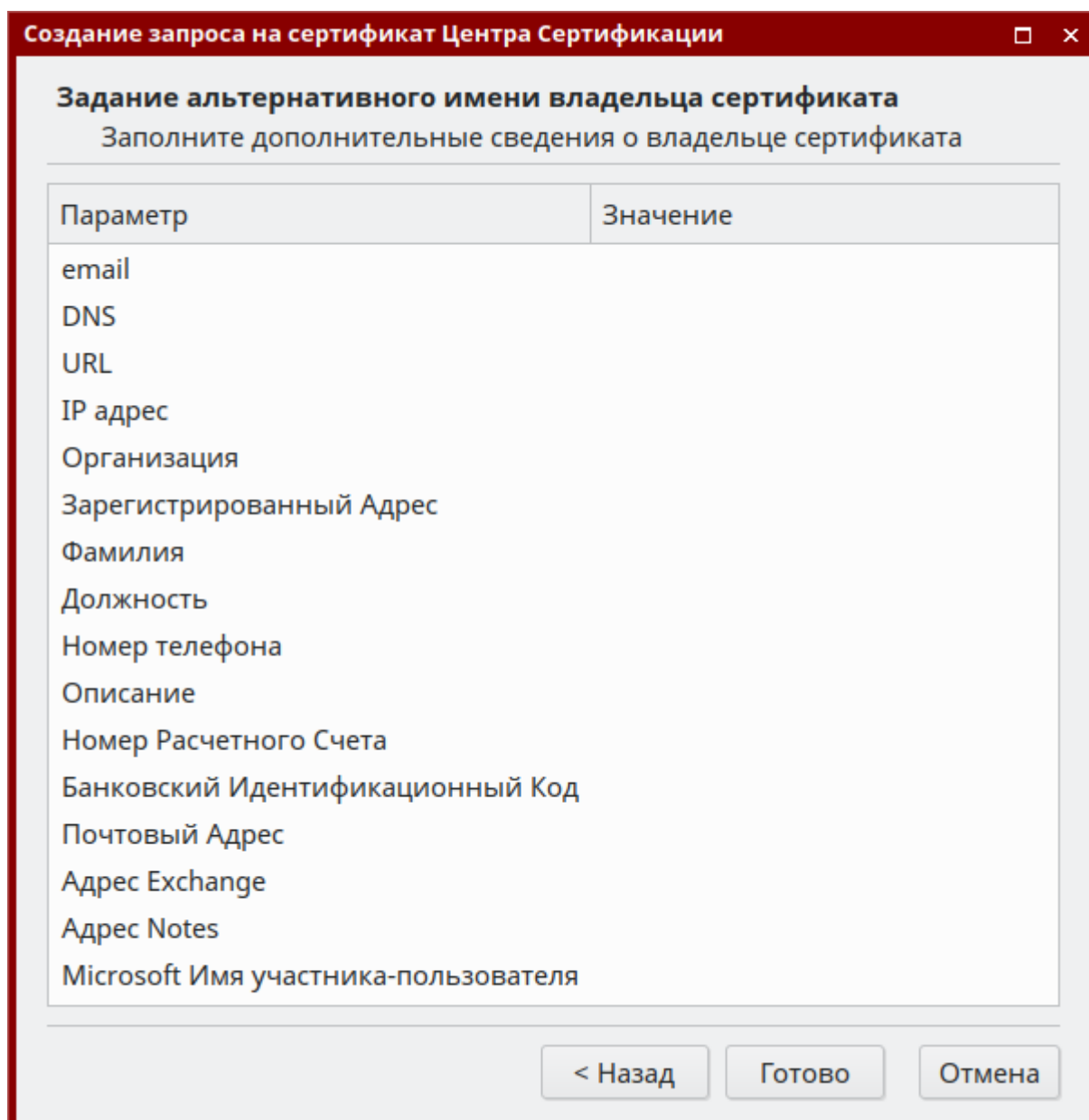


Рисунок 11 - Диалог выбора дополнительных атрибутов в дополнении Альтернативное Имя
Владельца сертификата

Примечание: При плановом переходе УЦ на новый ключ ЭП формирование нового ключа ЭП Администратора ЦС и запроса на сертификат ЦС, предназначенного для отправки в вышестоящий УЦ, выполняется аналогичным образом.

Шаг 9. Формирование ключа ЭП Администратора ЦС

После заполнения атрибутов сертификата ПК ЦС предлагает создать ключ ЭП Администратора ЦС (рисунок 12).

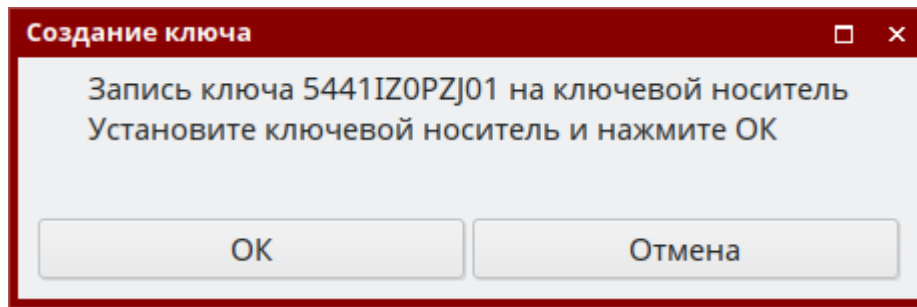


Рисунок 12 - Диалог создания ключа ЭП Администратора ЦС

Далее необходимо установить ключевой носитель и выбрать тип считывателя (рисунок 13).

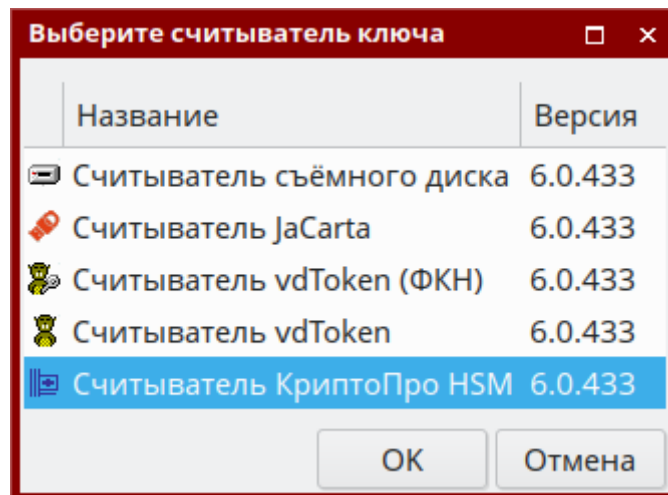


Рисунок 13 - Диалог выбора ключевого носителя

После завершения создания запроса на сертификат ЦС будет показано диалоговое окно с содержанием запроса (рисунок 14).

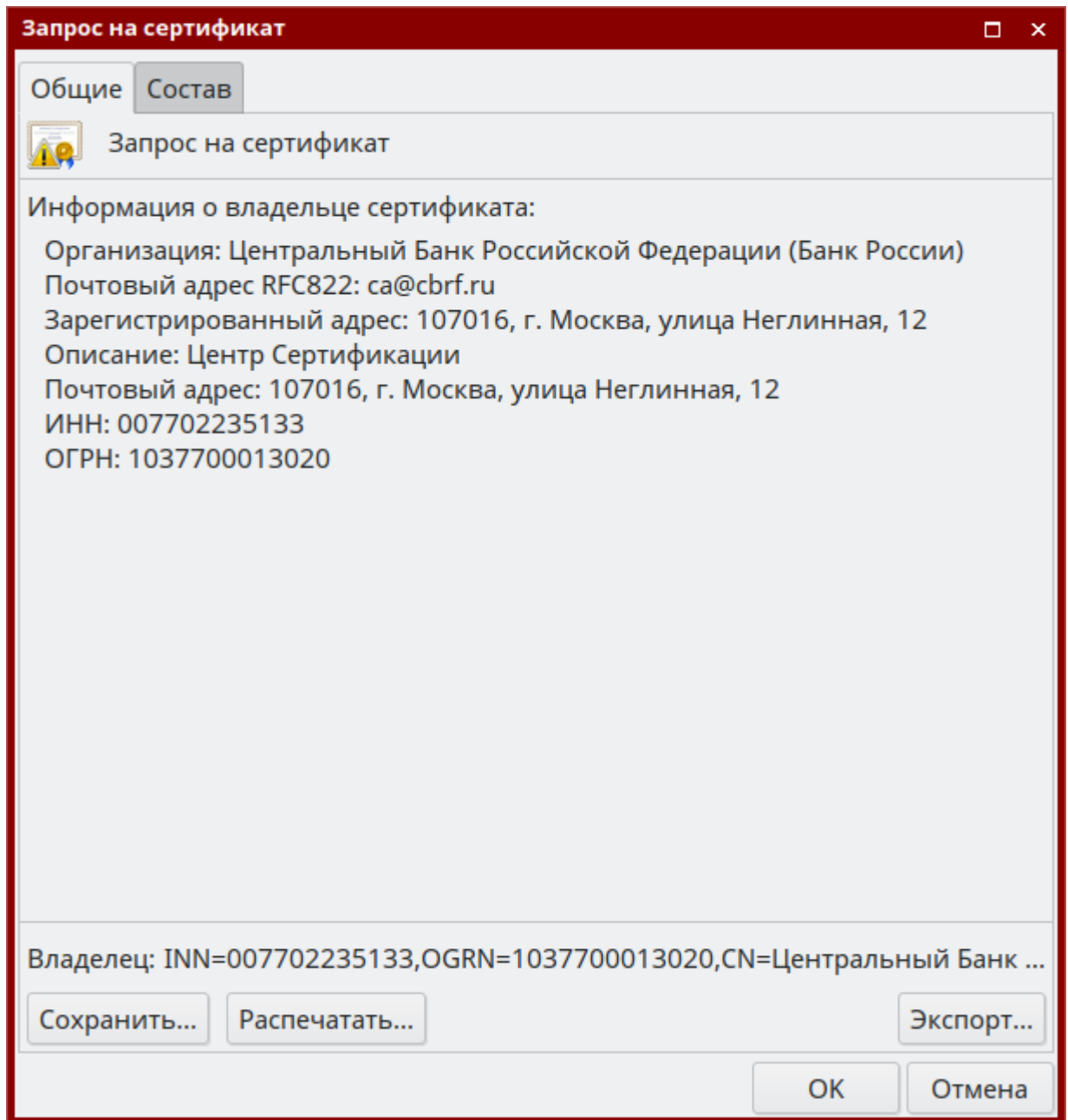


Рисунок 14 - Диалоговое окно с содержанием запроса

Далее АРМ ЦС предлагает сохранить созданный запрос на сертификат. Сохранённый запрос на сертификат должен быть передан в вышестоящий ЦС для получения сертификата.

Шаг 10. Создание хранилищ и запуск сервиса Центра Сертификации

После завершения настроек сервиса Центра Сертификации и получения сертификата от вышестоящего УЦ можно приступить к созданию хранилищ Центра Сертификации. Выберите пункт меню «**Центр Сертификации**» - «**Создать Хранилища**» (Рисунок 15).

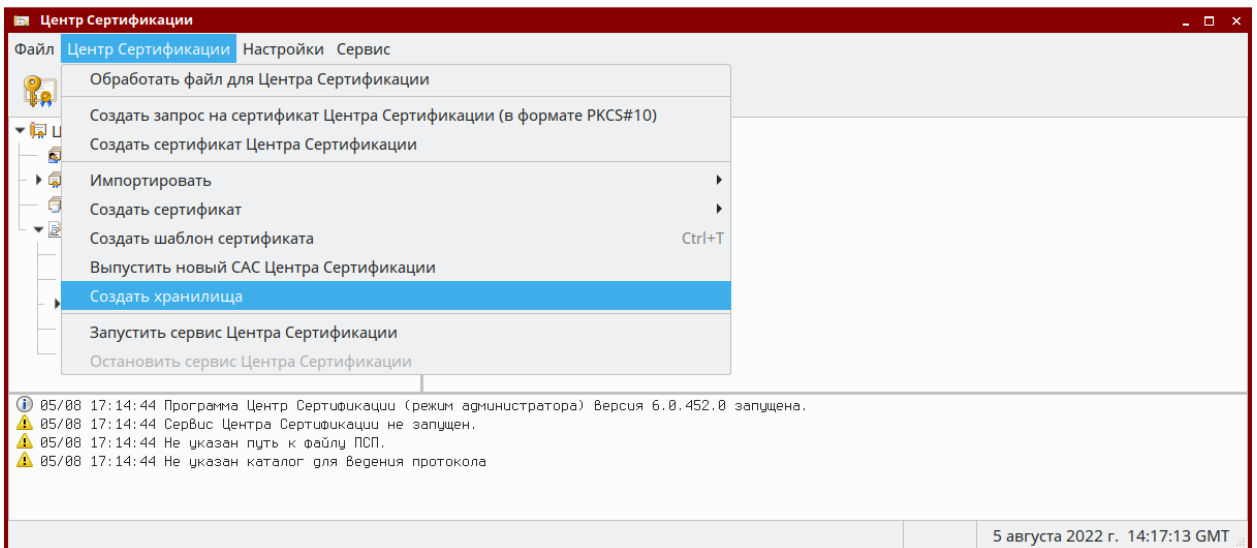


Рисунок 15 – Выбор пункта меню «Создать Хранилища»

В появившемся окне выберите каталог, содержащий выданные вам вышестоящим УЦ сертификаты с файловым расширением **.cer** и список аннулированных сертификатов с файловым расширением **.crl**.

В появившемся окне выберите рабочий сертификат Центра Сертификации (Рисунок 16).

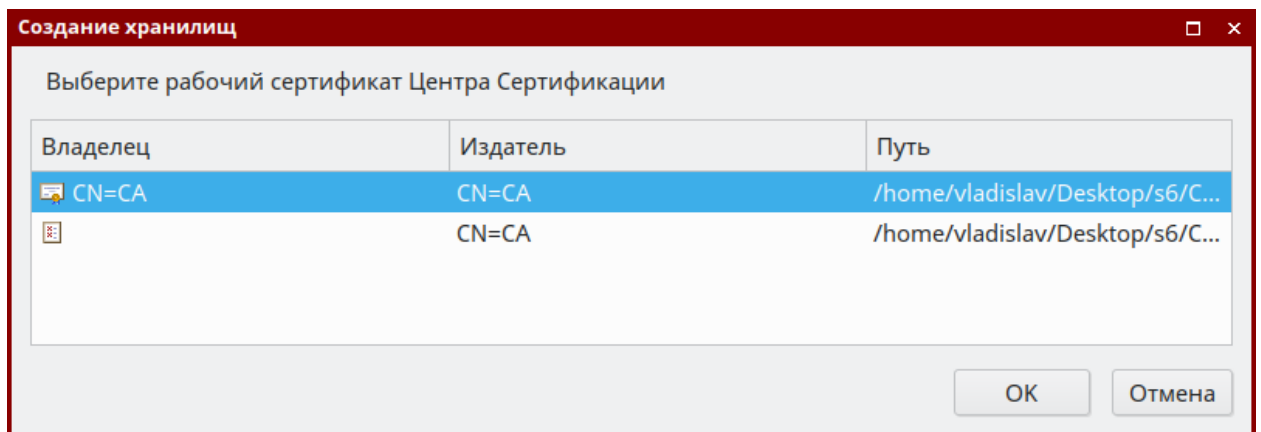


Рисунок 16 – Выбор рабочего сертификата Центра Сертификации

В случае если все вышеописанные операции были выполнены корректно, будут созданы хранилища Центра Сертификации и сервис Центра Сертификации должен автоматически запуститься. В окне «**Выберите Профиль**» можно нажать кнопку «**Отмена**» и не выбирать конкретный Профиль Справочника.