Программно-аппаратный комплекс  
«ЛИССИ-УЦ»

Руководство администратора

ООО «ЛИССИ-Софт»  
\_\_ января 2018 г.

Оглавление

[Первичная настройка УЦ 3](#_Toc504406314)

[Основные опции 3](#_Toc504406315)

[Настройка web-сервера 5](#_Toc504406316)

[Настройка базы данных 6](#_Toc504406317)

[Интерфейсы УЦ 7](#_Toc504406318)

[Ролевая система 7](#_Toc504406319)

[Создание корневого сертификата 8](#_Toc504406320)

[Выпуск сертификатов 10](#_Toc504406321)

[Отзыв сертификатов 11](#_Toc504406322)

[Автоматический выпуск и отзыв сертификатов 12](#_Toc504406323)

# Первичная настройка УЦ

config.xml, центральным конфигурационным файлом УЦ. Он представляет собой набор тэгов, со следующей структурой:

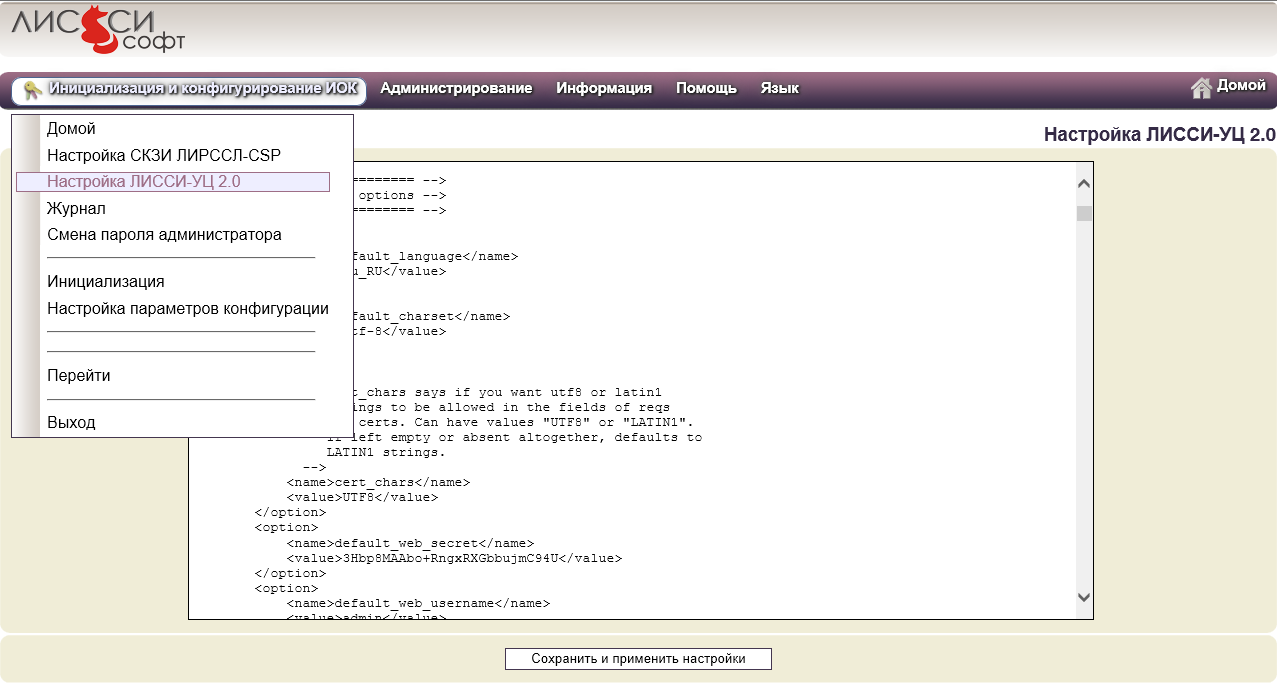
**<option>**

**<name>название параметра</name>**

**<value>значение параметра</value>**

**</option>**

Настройка файла конфигурации config.xml осуществляется через WEB интерфейс ЦР в разделе Общие->Настройка ПАК ЛИССИ-УЦ 2.0 и через WEB интерфейс ЦС в разделе Инициализация и конфигурирование ИОК->Настройка ПАК ЛИССИ-УЦ 2.0.

В следующих разделах описаны основные параметры config.xml, служебные параметры, не охваченные руководством, менять не следует.

## Основные опции

Секция “general options”.

default\_language задает язык локализации УЦ (ru или en), формирует первую часть идентификатора языка ru\_RU.UTF-8.

<option>

<name>default\_language</name>

<value>ru</value>

</option>

default\_charset задает кодировку страниц веб-интерфейса УЦ, формирует последнюю часть идентификатора языка ru\_RU.UTF-8.

<option>

<name>default\_charset</name>

<value>UTF-8</value>

</option>

organization задает название организации, которой принадлежит УЦ, и опреде­ляет параметр O в Distinguish Name (DN) корневого сертификата.

<option>

<name>organization</name>

< value>Ваша организация</value>

</option>

ca\_organization задает подразделение выше обозначенной организации и определяет параметр OU в Distinguish Name (DN) корневого сертификата.

<option>

<name>ca\_organization</name>

<value>Удостоверяющий центр</va1ue>

</option>

ca\_state (область) указывает на расположение УЦ и определяет параметр ST в Distinguish Name (DN) корневого сертификата.

<option>

<name>ca\_state</name>

<va1ue>Облaсть</va1ue>

</option>

ca\_locality (город) указывает на расположение УЦ и определяет параметр L в Distinguish Name (DN) корневого сертификата.

<option>

<name>ca\_locality</name>

<va1ue>Город</va1ue>

</option>

ca\_country представляет собой двухбуквенный код страны по стандарту ISO-3166­1, формирует среднюю часть идентификатора языка ru\_RU.UTF-8 и определяет па­раметр L в Distinguish Name (DN) корневого сертификата.

<option>

<name>ca\_country</name>

<value>RU</value>

</option>

service\_mail\_account будет автоматически подставляться в поле “From” каждого письма.

<option>

<name>service\_mail\_account</name>

<value>admin@organization.ru</value>

</option>

## Настройка web-сервера

Секция “web server configuration”.

httpd\_host имя хоста или IP-адрес, определяет параметр CN в Distinguish Name (DN) корневого сертификата.

<option>

<name>httpd\_host</name>

<value>organization.ru</value>

</option>

httpd\_protocol http или https протокол,

<option>

<name>httpd\_protocol</name>

<value>http</value>

</option>

httpd\_pub\_port порт для доступа к не защищенному интерфейсу пользователя, <option>

<name>httpd\_pub\_port</name>

<value>80</value>

</option>

httpds\_pub\_port порт для доступа к защищенному интерфейсу пользователя, <option>

<name>httpds\_pub\_port</name>

<value>8080</value>

</option>

httpds\_ra\_port порт для доступа к интерфейсу администратора Центра Реги­страции,

<option>

<name>httpds\_ra\_port</name>

<value>9443</value>

</option>

httpds\_ca\_port порт для доступа к интерфейсу администратора Центра Серти­фикации соответственно.

<option>

<name>httpds\_ca\_port</name>

<value>8443</value>

</option>

CRLDistributionPoints точки распространения CRL (CDP). Возможно задание нескольких точек распространения. Оптимально, чтобы каждому сертификату со­ответствовало, как минимум, две CDP.

<option>

<name>CRLDistributionPoints</name>

<value>

URI.1=<http://www.organization.ru/pub/crl/cacrl.crl>

URI.2=<http://www.organization2.ru/pub/crl/cacrl.crl>

</value>

</option>

## Настройка базы данных

Секция “database configuration”.

Вначале следует определиться, какой модуль БД (dbmodule) вы будете использо­вать. ПАК «ЛИССИ-УЦ»поддерживает два модуля - один для DBM файлов и один для MySQL баз данных. Флаг DB активирует поддержку DBM файлов, а DBI - под­держку MySQL. В случае использования MySQL базы данных, вам понадобиться установить еще несколько дополнительных параметров.

<option>

<name>dbmodule</name>

<value>DBI</value>

</option>

db\_type это тип DBD драйвера. В УЦ поддерживается два типа БД: MySQL.

<option>

<name>db\_type</name>

<value>MySQL</value>

</option>

db\_name имя используемой базы данных.

<option>

<name>db\_name</name>

<value>ca</value>

</option>

db\_host адрес хоста БД.

<option>

<name>db\_host</name>

<value>localhost</value>

</option>

db\_port порт доступа к БД.

<option>

<name>db\_port</name>

<value>3306</value>

</option>

db\_user пользователь БД.

<option>

<name>db\_user</name>

<value>lissica</value>

</option>

db\_passwd пароль для доступа к БД указанного выше пользователя.

<option>

<name>db\_passwd</name>

<value>пароль</value>

</option>

## Интерфейсы УЦ

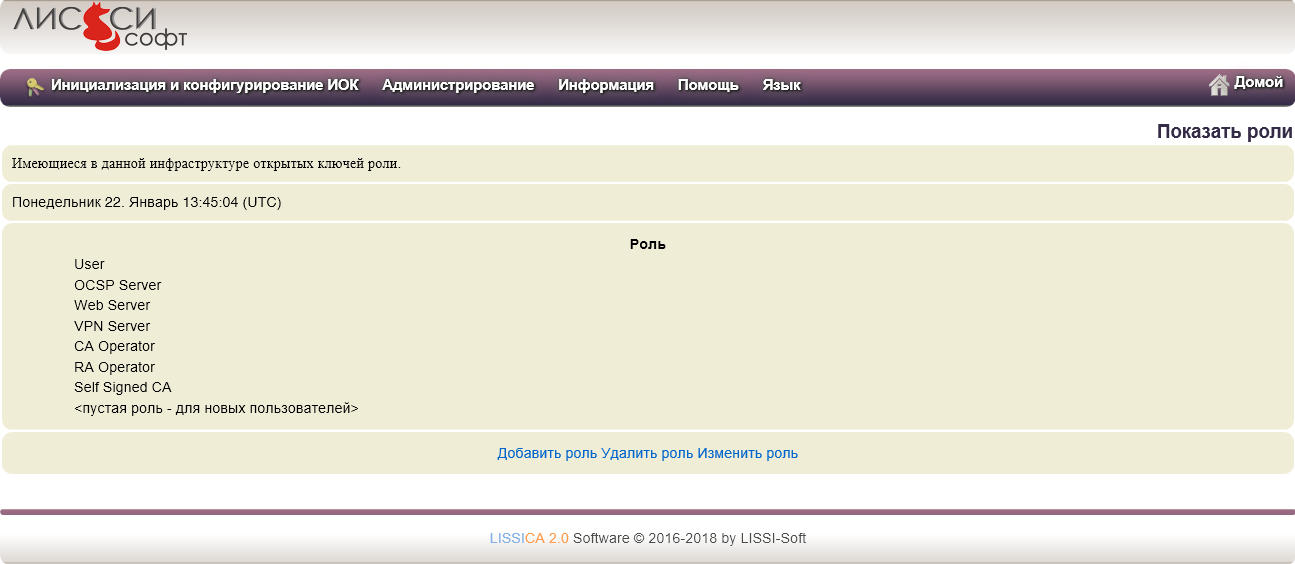
Каждый компонент УЦ располагает собственными интерфейсами:

* ЦР содержит публичный интерфейс и интерфейс администратора ЦР
* ЦС содержит интерфейс администратора ЦС

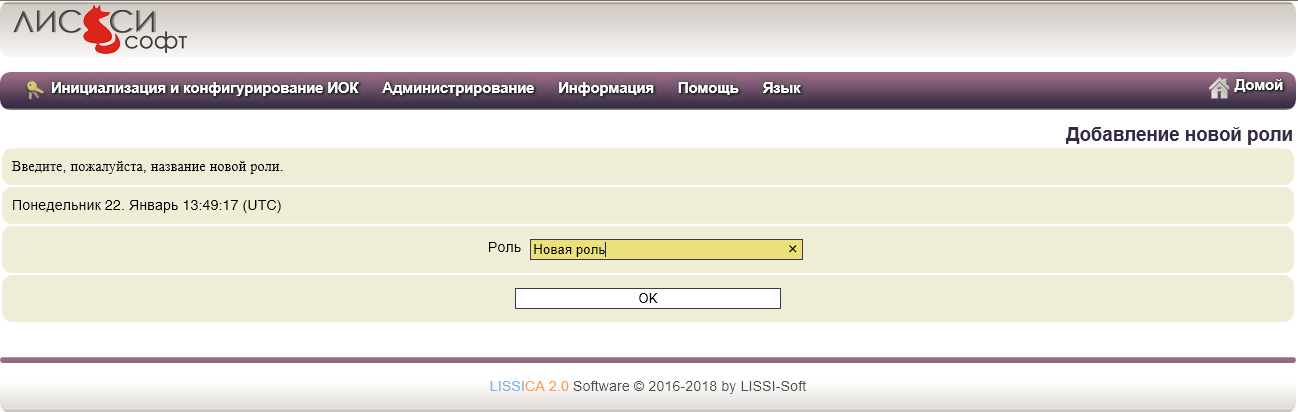
## Ролевая система

В представленном дистрибутиве УЦ по умолчанию задано 8 ролей (User, Web Server, CA Operator, RA Operator, Mail Server, VPN Server, OCSP, TSP Server), их можно редактировать в соответствии с требованиями заказчика.

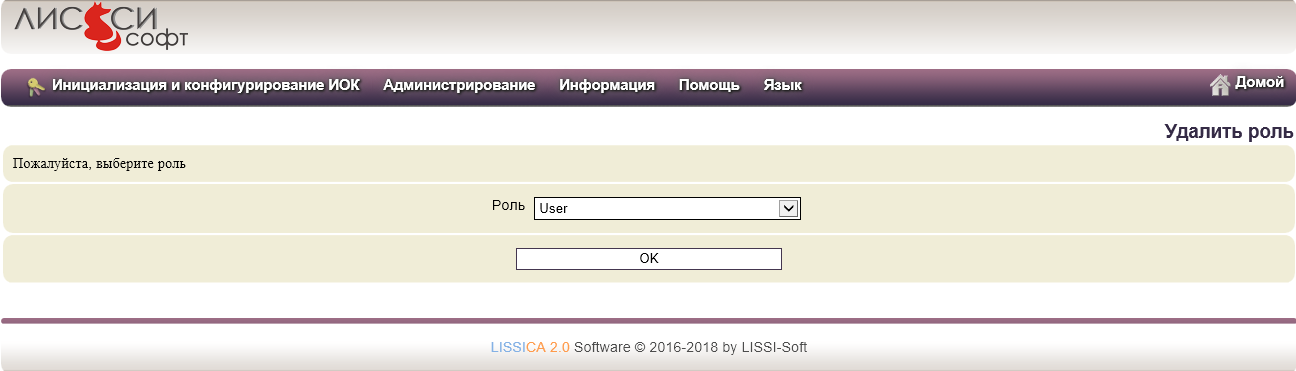
Добавление, удаление и редактирование ролей осуществляется через web интерфейс ЦС через соответствующее меню - Инициализация и конфигурирование ИОК->Настройки параметров конфигурации->Роли



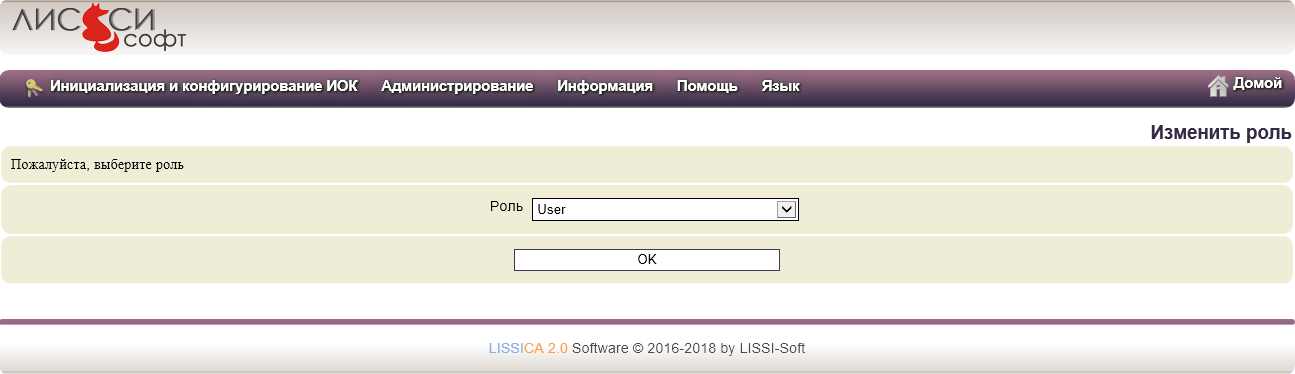
Для добавление роли необходимо нажать «Добавить роль» , откроется форма для добавления роли, где необходимо добавить наименование роли и нажать «ОК».



Для удаления роли необходимо нажать ссылку в окне«Удалить роль», в результате откроется форма для удаления роли , где необходимо выбрать из выпадающего списка наименование роли и нажать кнопку «ОК».



Для редактирования параметров роли необходимо нажать ссылку в окне«Изменить роль», в результате откроется форма для редактирования параметров роли , где необходимо выбрать из выпадающего списка наименование роли и нажать кнопку «ОК».Ввести необходимые параметры и нажать «Сохранить настройки».



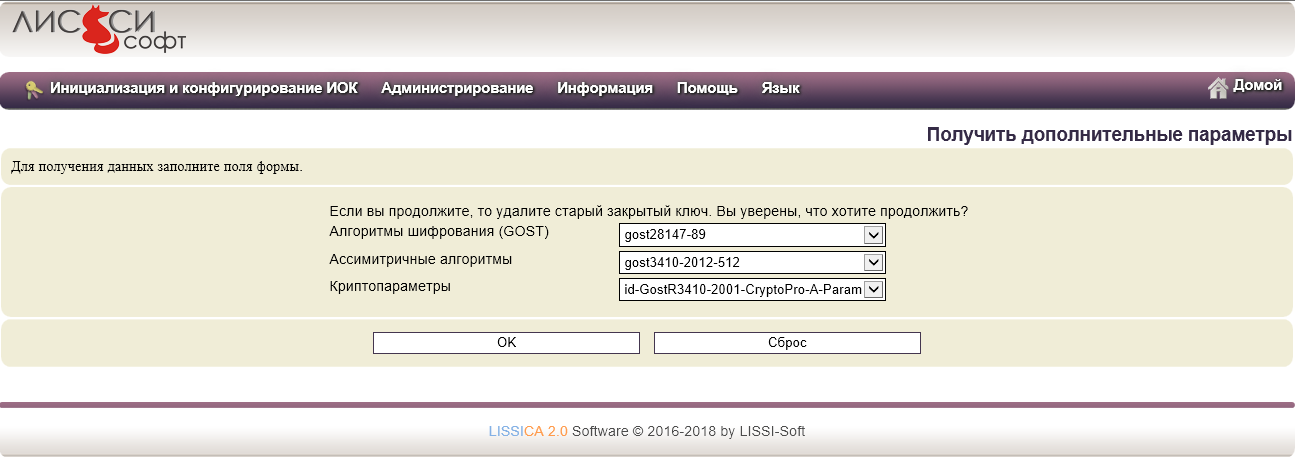
## Создание корневого сертификата

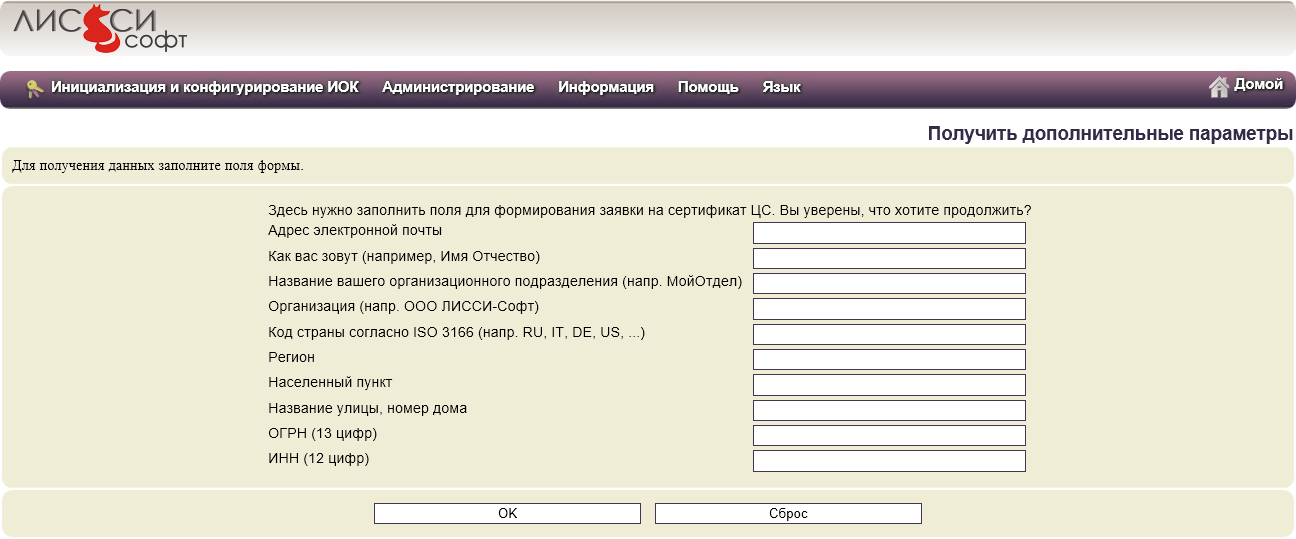
Выпуск корневого сертификата УЦ осуществляется через Web интерфейс ЦС. Для этого необходимо перейти в раздел Инициализация и конфигурирование ИОК->Инициализация.



Нажимаем на ссылку «Инициализация базы данных», после успешной инициализации возвращаемся назад и нажимаем «Генерировать новый секретный ключ УЦ».

Выбираем необходимые параметры закрытого ключа и нажимаем «ОК».

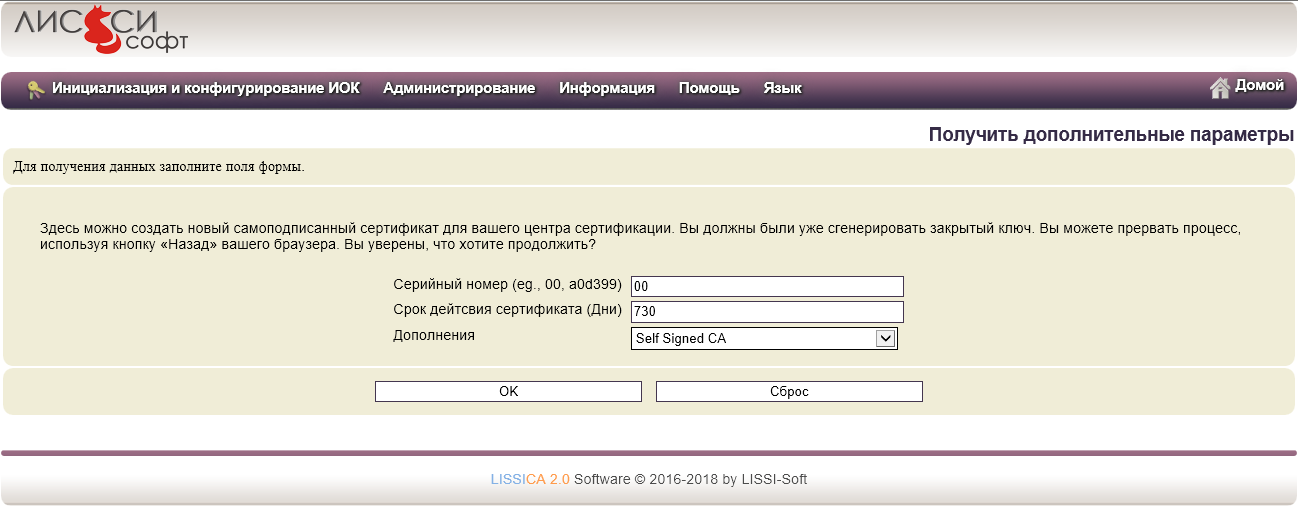


Переходим в раздел Инициализация и конфигурирование ИОК->Инициализация и нажимаем «[Генерировать новую заявку на сертификат УЦ (используя созданный секретный ключ)](http://lissicatest.lissi.lan/cgi-bin/pki/ca/ca?cmd=getParams;GET_PARAMS_CMD=genCAReq;xsrf_protection_token=79328b30a4fb57ea0488c45093614d8c7cd749c7)».

Вводим соответствующие данные (в поле ОРГАНИЗАЦИЯ название организации должно быть заключено в кавычки вида «...»; если ИНН меньше 12 символов, то необходимо перед ИНН добавить нулей; в поле НАЗВАНИЕ УЛИЦЫ, НОМЕР ДО­МА не должно быть запятых) и нажимаем «OK».

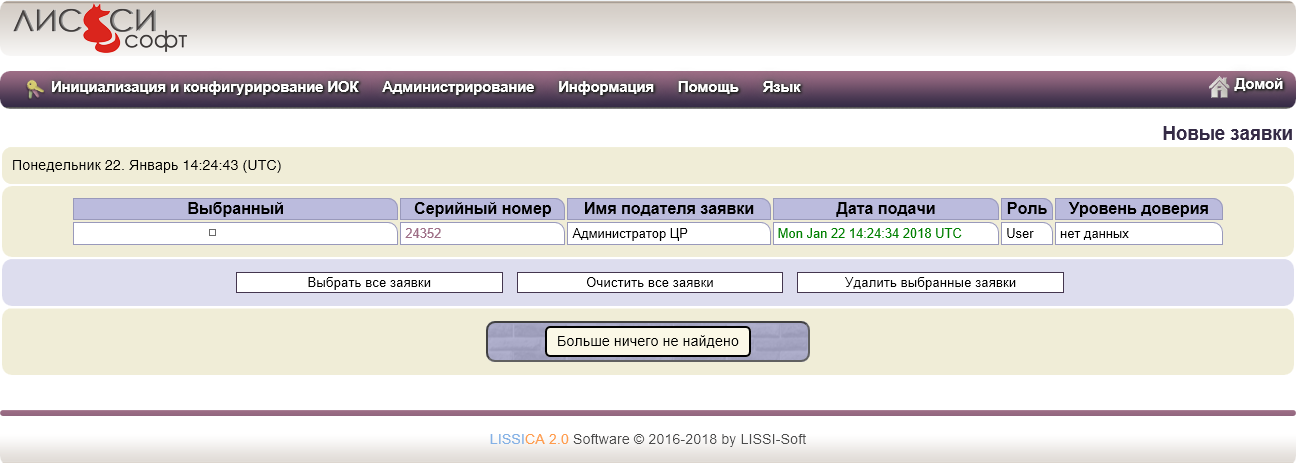
Заявка создана, теперь её можно использовать для создания самоподписанного корневого сертификата, либо экспортировать для отправки в Минкомсвязь.

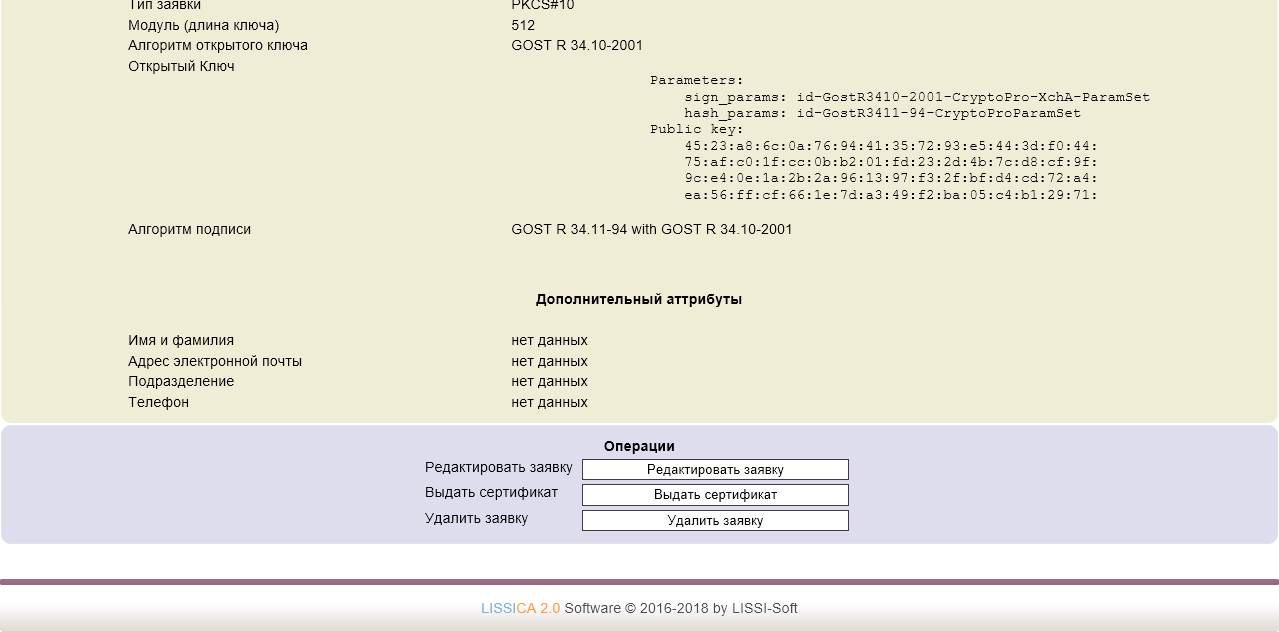
Для создания самоподписанного сертификата УЦ необходимо нажать «[Самоподписанный сертификат УЦ (созданный на основе уже сгенерированной заявки)](http://lissicatest.lissi.lan/cgi-bin/pki/ca/ca?cmd=getParams;GET_PARAMS_CMD=genCACert;xsrf_protection_token=79328b30a4fb57ea0488c45093614d8c7cd749c7)».



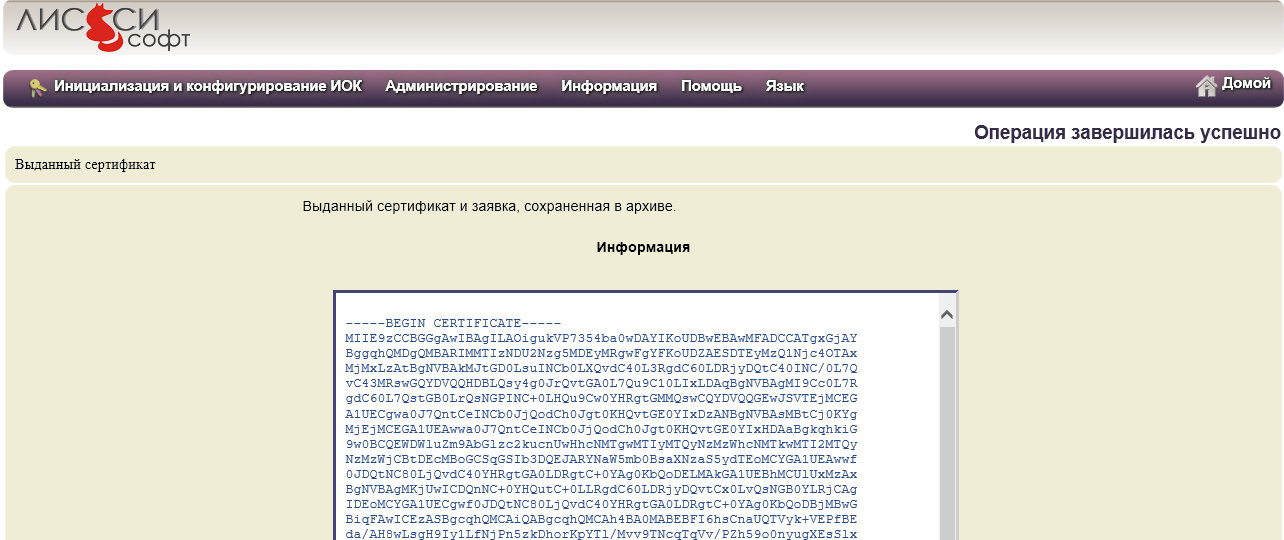
## Выпуск сертификатов

Выпуск сертификатов ключей проверки электронной подписи осуществляется через Web интерфейс ЦС через пункт Администрирование->Заявки на сертификат->Новые.

Нажмите на серийный номер выбранной заявки

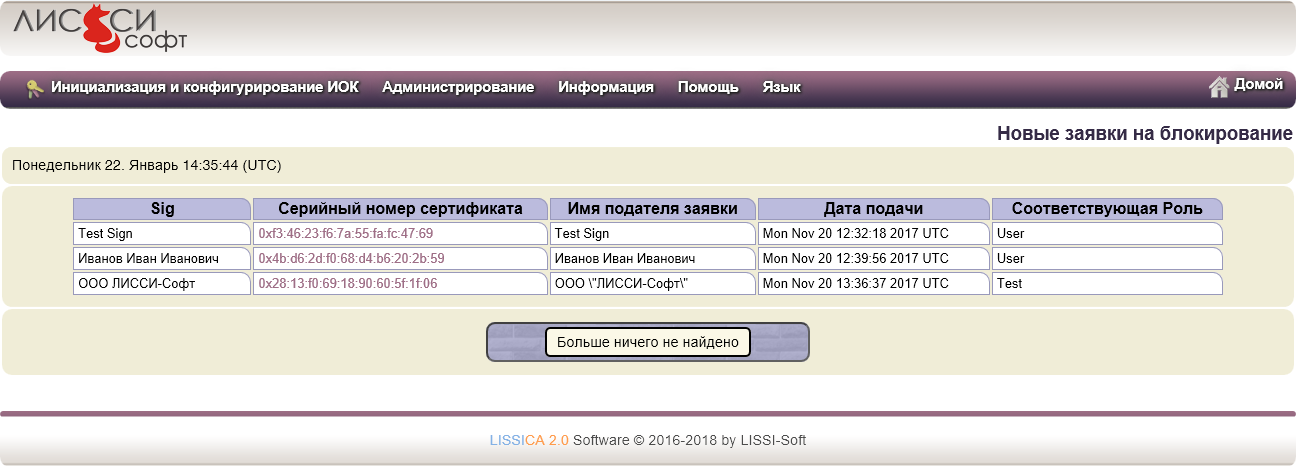


Нажмите «Выдать сертификат» и введите пароль на закрытый ключ УЦ.

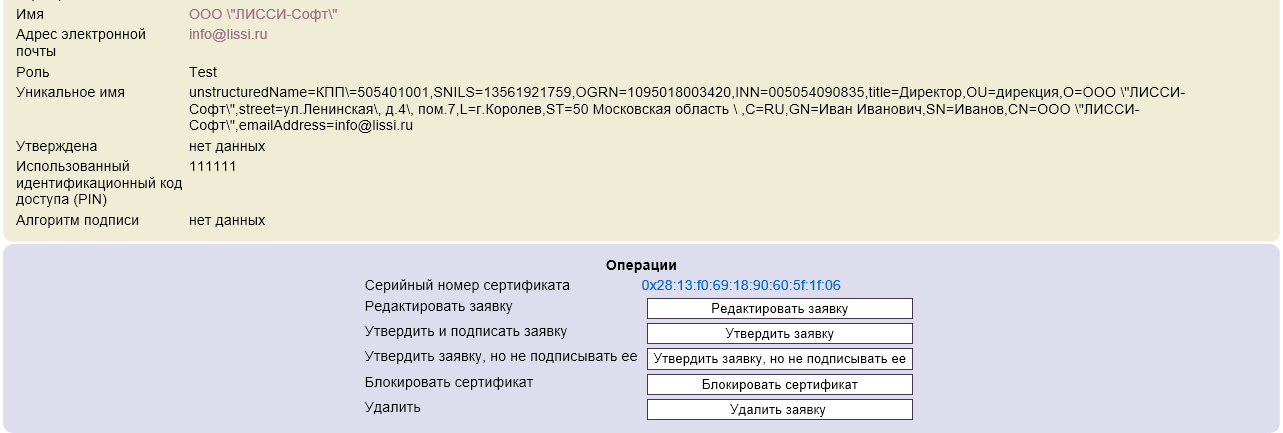


## Отзыв сертификатов

Выпуск сертификатов ключей проверки электронной подписи осуществляется через Web интерфейс ЦС через пункт Администрирование->Заявки на блокирование->Новые



Нажмите на серийный номер выбранной заявки



Нажмите «Блокировать сертификат и введите пароль на закрытый ключ УЦ.

## Автоматический выпуск и отзыв сертификатов

Для включения автоматического выпуска и отзыва сертификатов необходимо использовать пункты Администрирование->Автоматический выпуск сертификатов и Администрирование->Автоматический отзыв сертификатов соответственно.

