Перевод действующего аккредитованного УЦ (использующего ПАК "КриптоПро УЦ" версии 1.5) из режима корневого в режим подчинённого.

Действующий аккредитованный УЦ, использующий ПАК "КриптоПро УЦ" версии 1.5 и работающий в режиме корневого ЦС может быть переведён в режим подчинённого ЦС с сохранением информации из баз данных серверов ЦС, ЦР, т.е. всех пользователей, запросов и выданных ранее сертификатов. При этом остаётся возможность отзыва ранее выданных сертификатов пользователей и публикации списков отозванных сертификатов.

Замечания.

1. Сроки действия всех сертификатов, которые будут выдаваться на УЦ после перехода в подчинённый режим, не могут превышать срок действия сертификата подчинённого ЦС, выдаваемого в УЦ Минкомсвязи.

2. После перехода УЦ в подчинённый режим для работы с сертификатами, выданными на этом УЦ будет требоваться доступ к актуальным спискам отозванных сертификатов (СОС) вышестоящих УЦ Минкомсвязи - ГУЦ и УЦ1 ИС ГУЦ (или УЦ2 ИС ГУЦ). Это касается как серверов самого УЦ, так и клиентских компьютеров или серверов, на которых будут использоваться выданные на этом УЦ сертификаты (в том числе для операций проверки подписи электронных документов).

На сервере ЦС служба сертификации может быть переведена из режима корневого ЦС в режим подчинённого ЦС путём изменения параметра реестра CAType в разделе реестра:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\CertSvc\Configuration\<имя ЦС>

Примечание. Название раздела <имя ЦС> совпадает со значением компонента имени Common Name в сертификате ЦС – в случае использования латинских букв непосредственно, для русских - каждая из них кодируется пятью символами – восклицательный знак и 4 шестнадцатеричные цифры.

Значение параметра CAType для режима "изолированный корневой ЦС" равно 3.

Значение параметра CAType для режима "изолированный подчинённый ЦС" равно 4.

Для перевода службы сертификации в подчинённый режим нужно задать значение 4.

Для создания запроса на сертификат подчинённого ЦС в соответствии с требованиями Минкомсвязи нужно добавить настройку для включения в запрос критического расширения "Основные ограничения" с заданием ограничения на длину пути со значением 0.

Это делается путём добавления в файл capolicy.inf в корневом каталоге Windows строк:

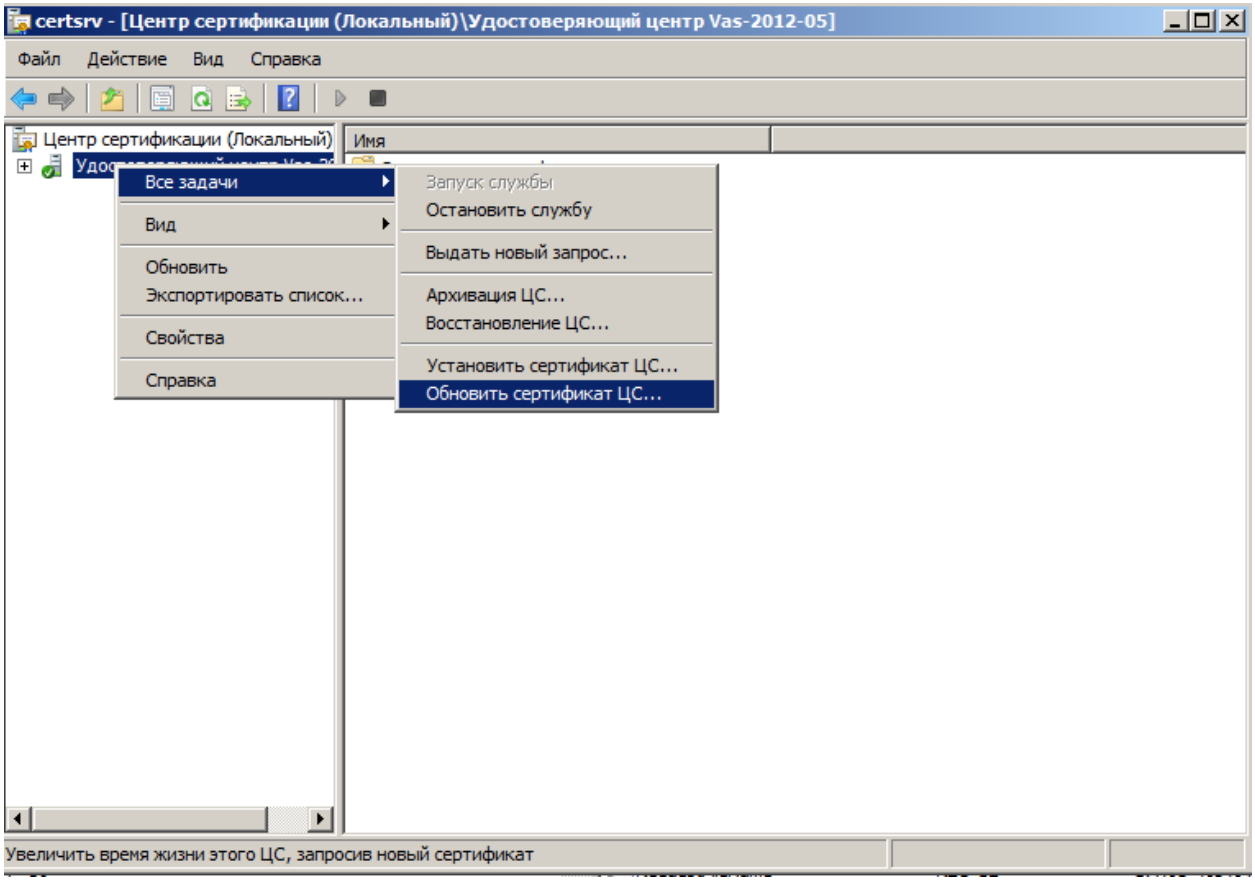
```
[BasicConstraintsExtension]
PathLength=0
Critical=True
```

Если в этом файле есть значение расширения 1.2.643.100.112 – то его нужно убрать (и OID, и его значение), поскольку данное расширение требуется только для неподчинённого режима работы УЦ.

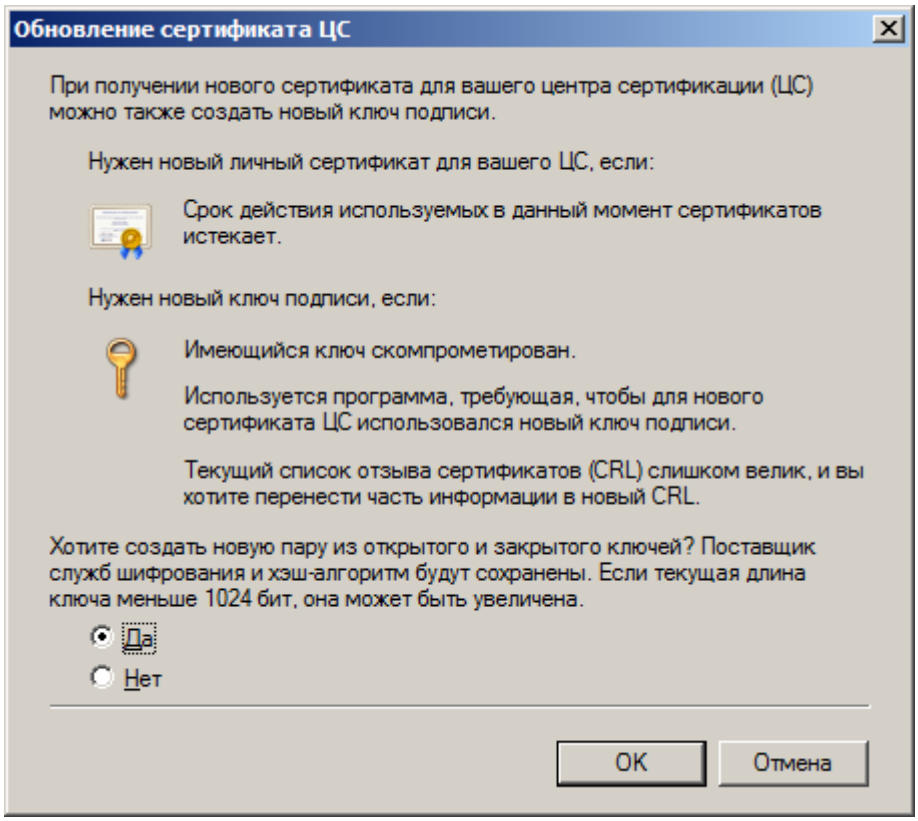
Пример файла capolicy.inf для варианта исполнения 1 КриптоПро УЦ (с КриптоПро CSP 3.6 по классу КС2):

```
[Version]
Signature="$Windows NT$"
[CRLDistributionPoint]
URL=""
[BasicConstraintsExtension]
PathLength=0
Critical=True
[PolicyStatementExtension]
Policies=PolicyKC1,PolicyKC2,PolicyAll
[PolicyKC1]
OID=1.2.643.100.113.1
[PolicyKC2]
OID=1.2.643.100.113.2
[PolicyAll]
OID=2.5.29.32.0
[Extensions]
1.2.643.100.111=DCsi0JrRgNC40L/RgtC+0J/RgNC+IENTUCIgKNCy0LXRgNGB0LjRjyAzLjYp
```

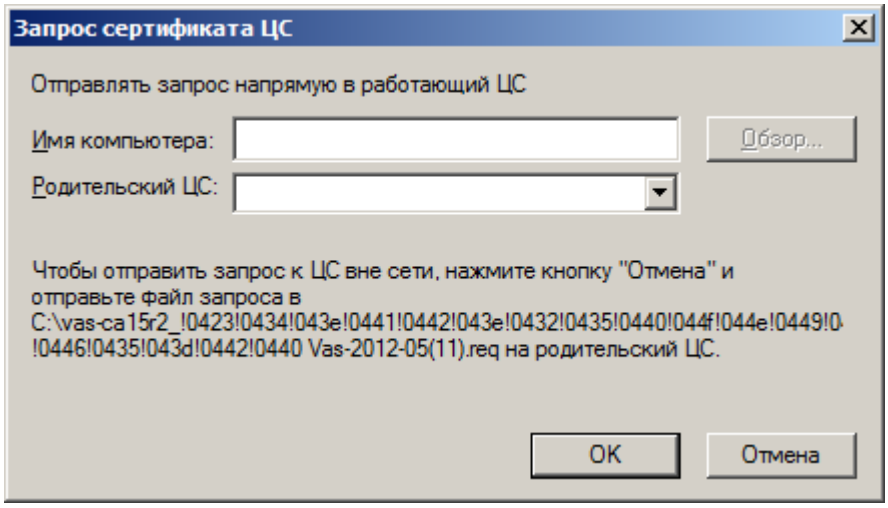
После проверки файла политик можно делать запрос на сертификат подчинённого УЦ. Для этого в оснастке управления службой сертификации нужно выбрать в контекстном меню "Все задачи" – "Обновить сертификат ЦС":



Далее после остановки службы сертификации выбрать вариант создания нового ключа ЦС:

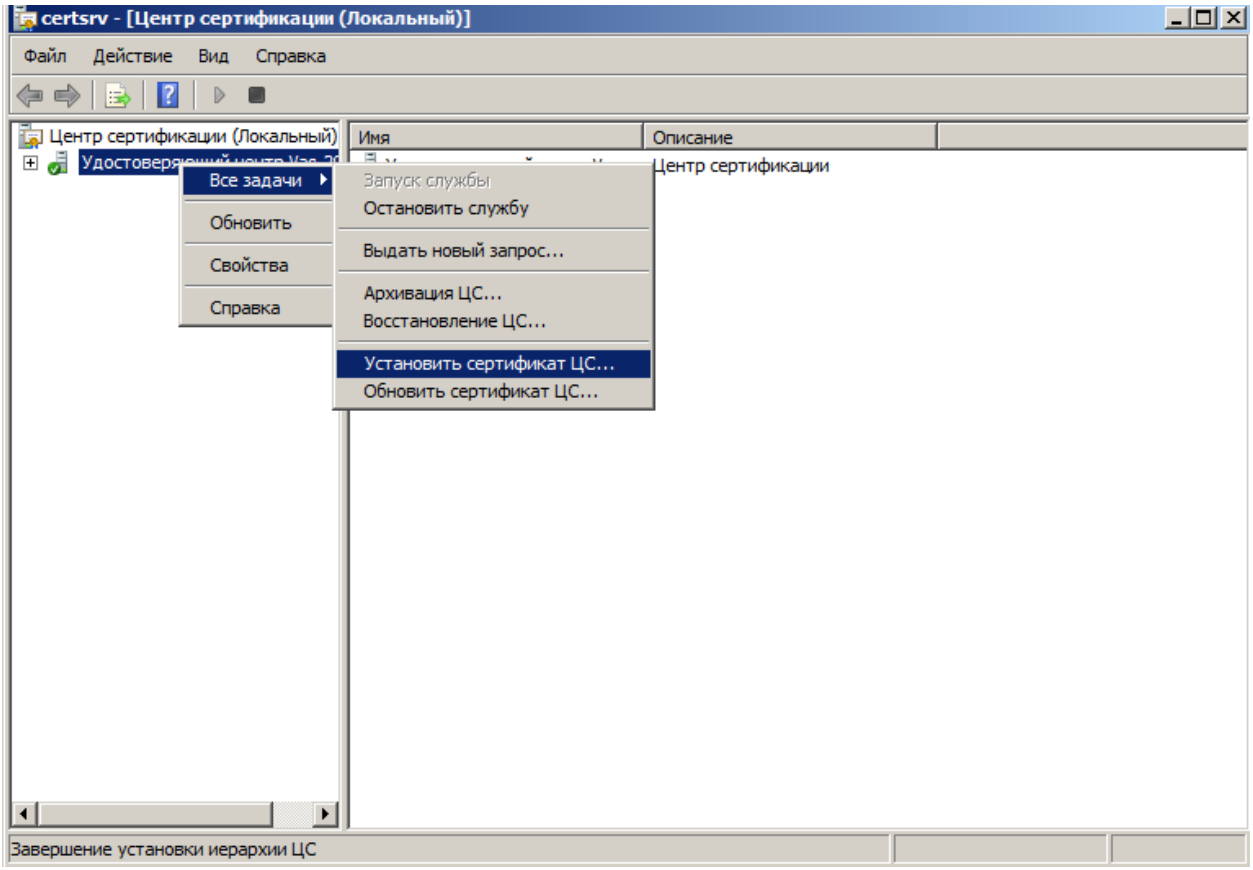


Затем после создания ключевого контейнера и записи его на выбранный носитель появится окно:



В нём написано имя файла (и полный путь на диске), куда будет сохранён файл запроса. Для завершения процесса формирования запроса нужно нажать кнопку Отмена, поскольку обработка файла запроса в УЦ Минкомсвязи не будет выполнена в онлайне.

Далее файл запроса с анкетой УЦ передаётся в Минкомсвязи для получения сертификата подчинённого УЦ. После получения сертификата установка его делается в оснастке управления службой сертификации:



Если в присланном файле имеется только сертификат подчинённого УЦ, то необходимо отдельно установить сертификат Головного удостоверяющего центра – в хранилище "Доверенные корневые ЦС" локального компьютера, сертификат выдающего УЦ (УЦ1 ИС ГУЦ или УЦ2 ИС ГУЦ) - в хранилище "Промежуточные ЦС" локального компьютера.

Кроме этого, требуется установить списки отозванных сертификатов (СОС) ГУЦ и УЦ1 ИС ГУЦ (или УЦ2 ИС ГУЦ) - в хранилище "Промежуточные ЦС" локального компьютера.

В дальнейшем нужно следить за сроками действия этих СОС, поскольку работа подчинённого УЦ будет невозможна без актуальных СОС вышестоящих УЦ.

Вместо помещения СОС в хранилище можно настроить доступ к ним по точкам публикации из сертификатов УЦ1 ИС ГУЦ (или УЦ2 ИС ГУЦ) и полученного сертификата подчинённого УЦ.

Сервер ЦС не рекомендуется подключать к сетям общего пользования (интернет), поэтому доступ к СОС вышестоящих УЦ в онлайне невозможен. Но можно организовать на любом доступном с сервера ЦС веб-сервере (в качестве него можно использовать сервер ЦР) виртуальную папку с именем cdp в корневом каталоге IIS и настроить по расписанию задание для помещения в эту папку актуальных файлов СОС вышестоящих УЦ. Тогда на сервере ЦС достаточно будет в файле hosts (%windir%\system32\drivers\etc\hosts) поместить строку:

<ip-адрес веб-сервера> <DNS-имя (имена) сервера cdp из сертификатов УЦ>

Пример, когда в качестве веб-сервера с СОС выступает сервер ЦР:

если ЦС имеет ip-адрес 192.168.1.1 и подключен только к серверу ЦР с ip-адресом 192.168.1.2, то в файл hosts нужно поместить:

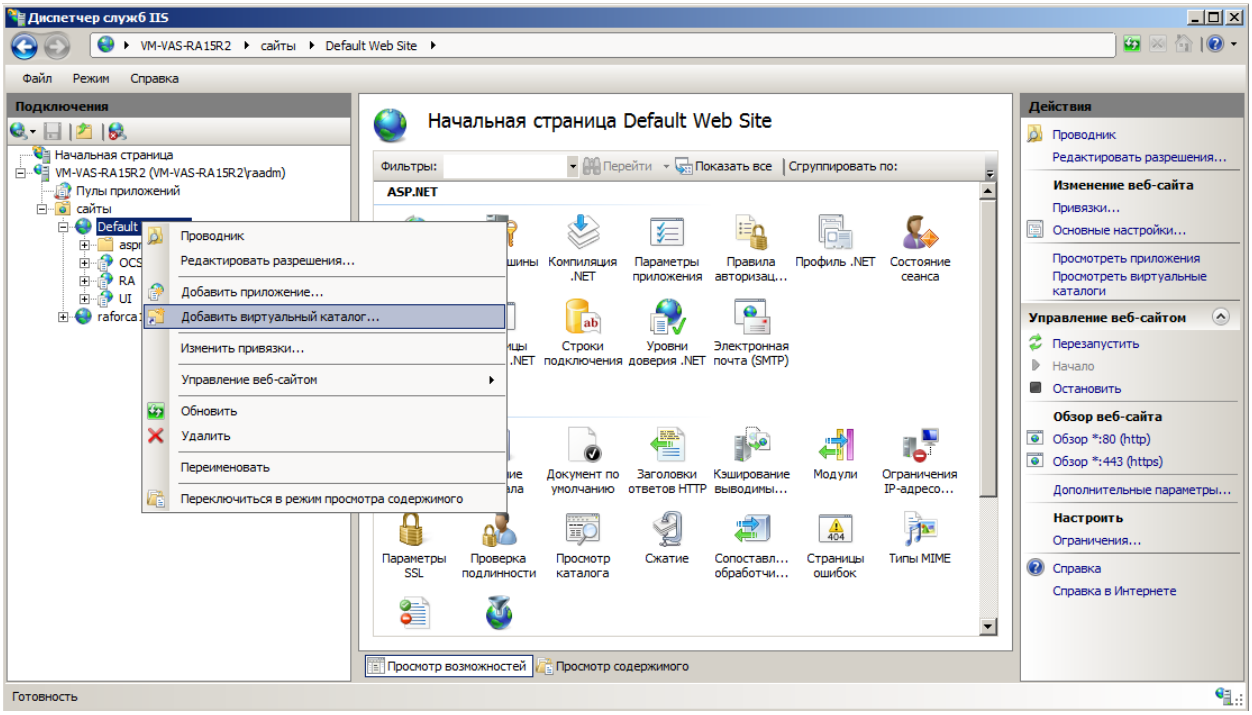
192.168.1.2 rostelecom.ru reestr-pki.ru

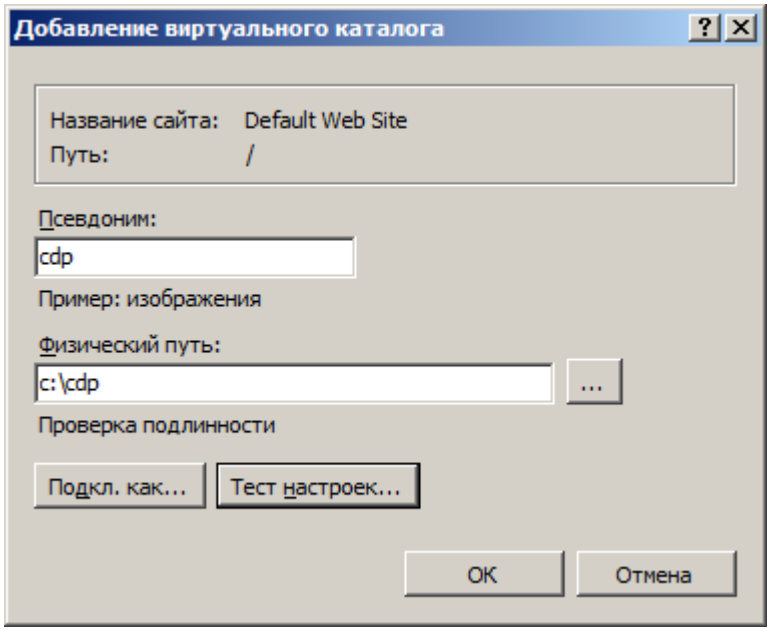
Тогда ЦС сможет в автоматическом режиме получать доступ к СОС по адресам из сертификатов, например:

http://rostelecom.ru/cdp/guc.crl
http://reestr-pki.ru/cdp/guc.crl
http://reestr-pki.ru/cdp/vguc1_4.crl
http://rostelecom.ru/cdp/vguc1_4.crl

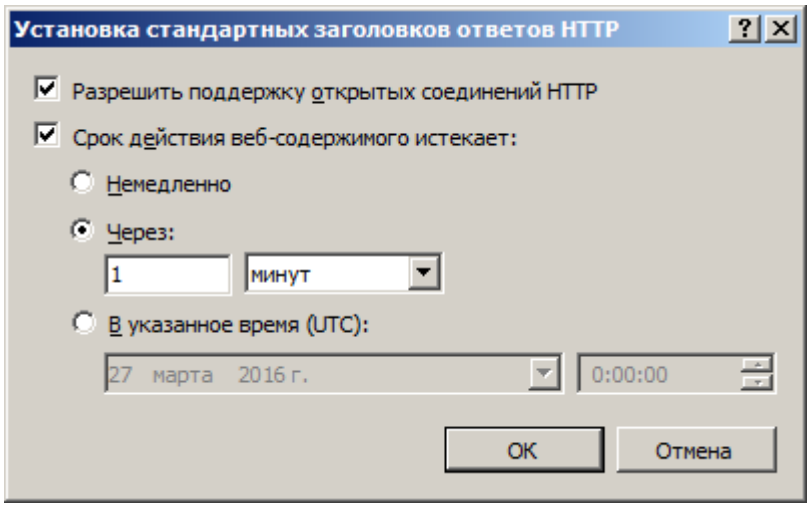
На сервере ЦР нужно установить сертификаты вышестоящих УЦ и полученный сертификат подчинённого УЦ и следить за сроками их действия. Если сервер ЦР имеет подключение к интернету – то СОС вышестоящих УЦ могут быть автоматически получены по адресам точек распространения СОС из сертификатов УЦ1 ИС ГУЦ (или УЦ2 ИС ГУЦ) и полученного сертификата подчинённого УЦ. Для организации доступа к файлам СОС вышестоящих УЦ с сервера ЦС на сервере ЦР нужно создать виртуальную папку:

1. Создать на локальном диске папку, например, c:\cdp
2. В IIS создать в корневом каталоге веб-узла виртуальную папку с именем cdp





Рекомендуется настроить для этой папки срок действия веб-содержимого в функции "Заголовки ответов HTTP" – "Настроить стандартные заголовки" (для исключения ненужного кеширования файлов со стороны IIS):



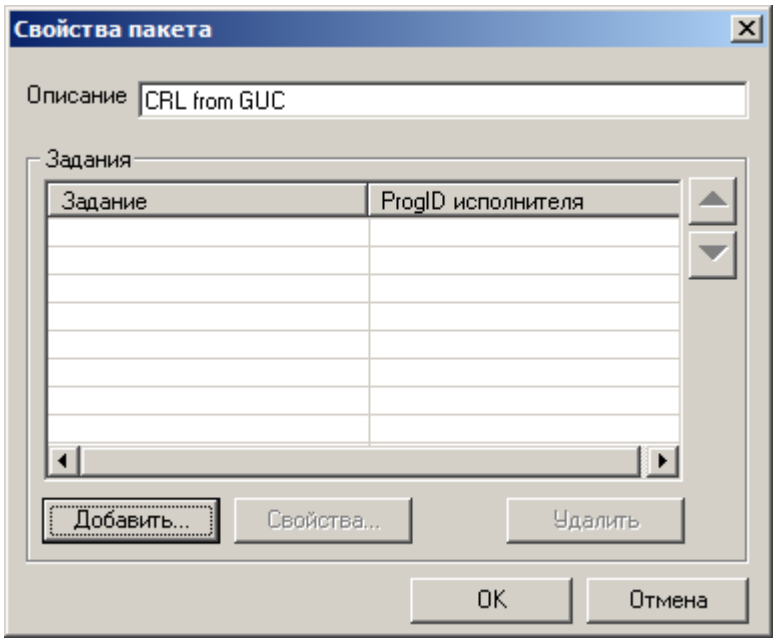
Далее осталось настроить задания, которые будут брать файлы COC вышестоящих УЦ из интернета и помещать их в эту папку cdp на диске.

Для этого можно использовать специально модифицированный файл задания переноса COC JOBTCRLLib.dll. Этот файл размещён в ftp://ftp.cryptopro.ru/pub/CRLfromGUC

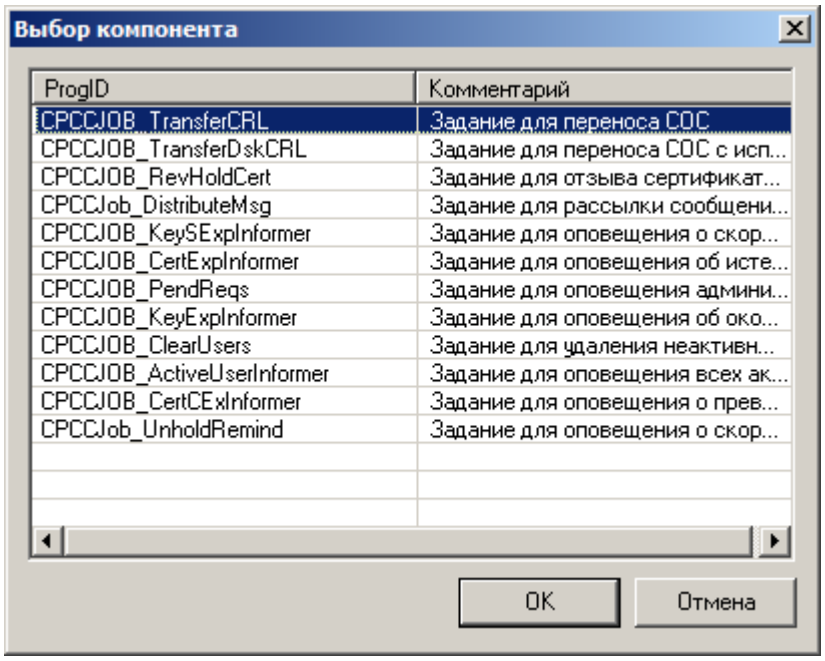
Его нужно поместить в папку на сервере ЦР вместо существующего там:

c:\Program Files (x86)\Common Files\Crypto Pro\Shared\JOBTCRLLib.dll

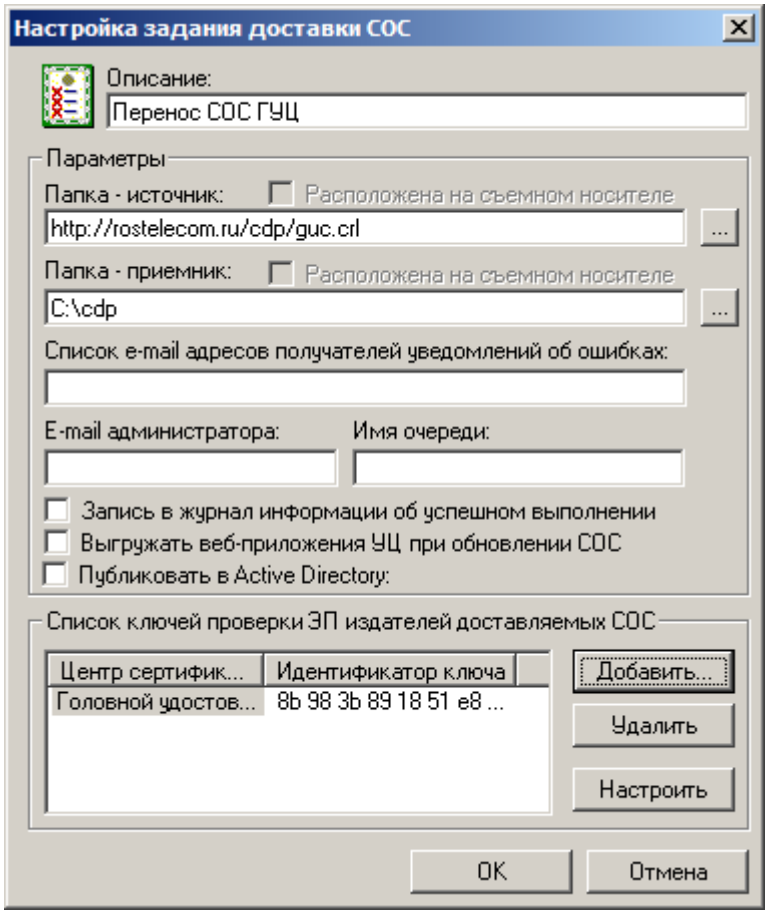
После этого для каждого адреса, с которого будет доставляться COC, в оснастке управления ЦР (Пуск – Программы – КриптоПро – Параметры Центра регистрации, Свойства на "ЦР на … веб-узле") на вкладке Задания нужно создать новое задание:



Имя можно задать любое, затем нажать Добавить:



И настроить его:



При необходимости можно настроить оповещение администратора об ошибках переноса COC.

Затем нужно задать учётную запись, под которой будет выполняться задание (рекомендуется CPRAComPlusAcct&) и расписание его работы.

Для каждого из остальных адресов COC вышестоящих УЦ нужно сделать отдельное задание и настроить его.