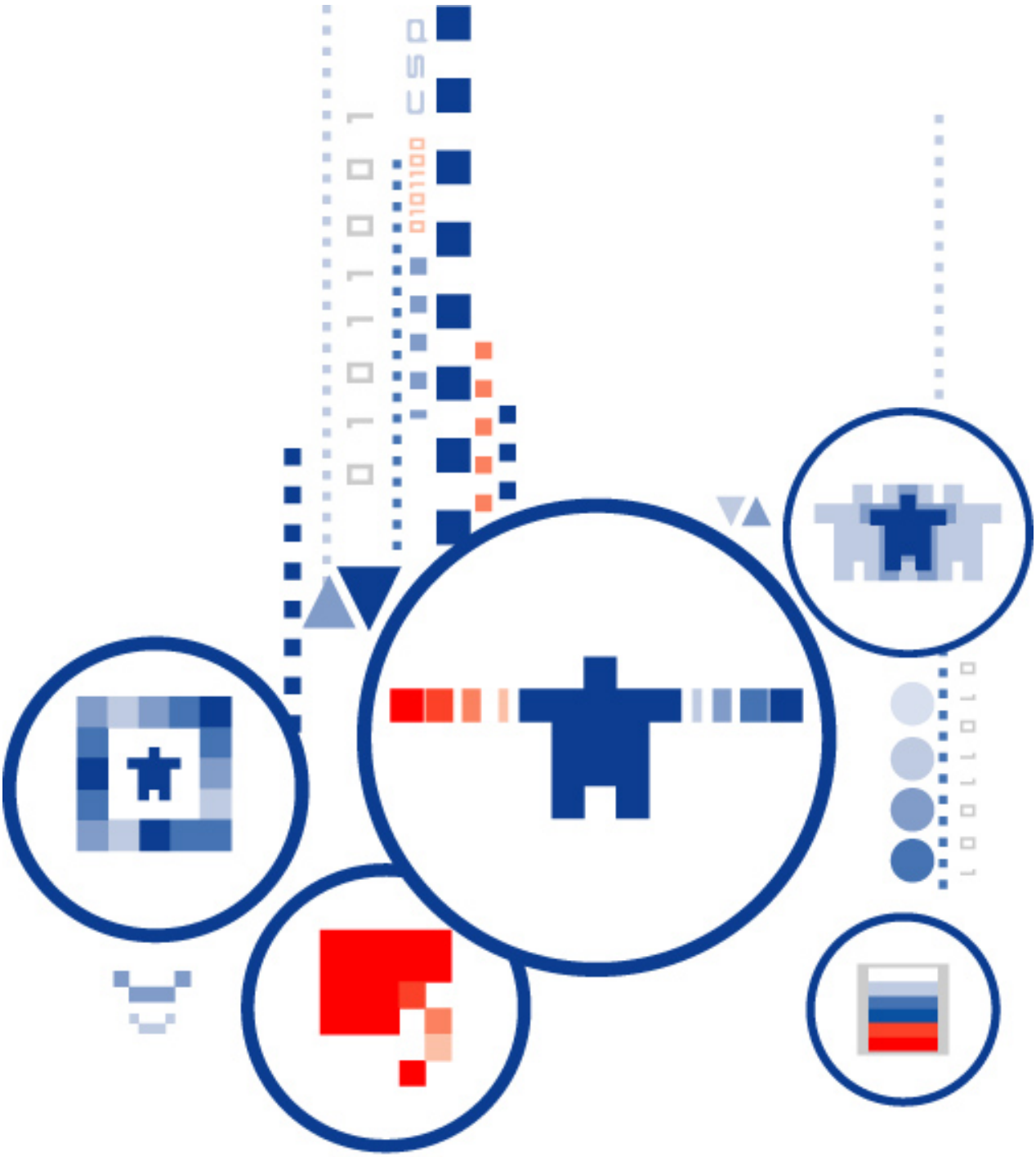
УТВЕРЖДЕН
ЖТЯИ.00035-01 90 18-ЛУ

ЖТЯИ.00035-01 90 18



КриптоПро УЦ

программно-аппаратный комплекс
удостоверяющий центр

Регламентные задания

АННОТАЦИЯ

Настоящий документ содержит описание настройки регламентных заданий, выполняемых на компьютере, не являющемся сервером ЦР.

Документ предназначен для администраторов Удостоверяющих Центров, администраторов доменов Windows, в которых используются сертификаты открытых ключей, выданные Удостоверяющим Центром «КриптоПро УЦ».

Информация о разработчике ПАК «КриптоПро УЦ»:

ООО "КРИПТО-ПРО"

127 018, Москва, улица Сущевский вал, 16 строение 5

Телефон: (495) 780 4820

Факс: (495) 780 4820

http://www.CryptoPro.ru

E-mail: info@CryptoPro.ru

Общее описание.

Приложение «КриптоПро УЦ. Регламентные задания» предназначено для выполнения задания переноса и публикации списков отозванных сертификатов (далее Задание переноса СОС) и задания рассылки писем-уведомлений об ошибках в работе.

Задание переноса СОС:

1) копирует список отозванных сертификатов с заданного адреса в локальную или сетевую папку,
2) устанавливает его в хранилище локального компьютера «Промежуточные Центры Сертификации» - «Список отзыва сертификатов» и
3) при необходимости может опубликовать СОС в Active Directory.

Таким образом, Задание переноса СОС, помимо непосредственного переноса СОС, может использоваться для публикации СОС в Active Directory, либо для установки списков отзыва на сервер, где требуется, чтобы СОС был установлен в хранилище локального компьютера (например, TSP или OCSP-сервер).

Если при работе Задания переноса СОС возникают ошибки, можно настроить рассылку уведомлений об этом по указанным адресам e-mail. Непосредственно рассылкой писем занимается Задание для рассылки сообщений, которое по умолчанию входит в пакет заданий вместе с Заданием переноса СОС.

Установка приложения «КриптоПро УЦ. Регламентные задания».

Требования к программным и техническим средствам

В качестве аппаратной платформы для функционирования приложения должен использоваться компьютер типа IBM PC с процессором Pentium IV (и выше).
В качестве программной платформы могут использоваться операционные системы:

- Microsoft Windows Server 2000 с установленным пакетом обновлений SP4 и выше
- Microsoft Windows XP с установленным пакетом обновлений SP2 и выше
- Microsoft Windows Server 2003 с установленным пакетом обновлений SP2 и выше.

Операционные системы могут быть как английской версии, так и русской.

Последовательность установки

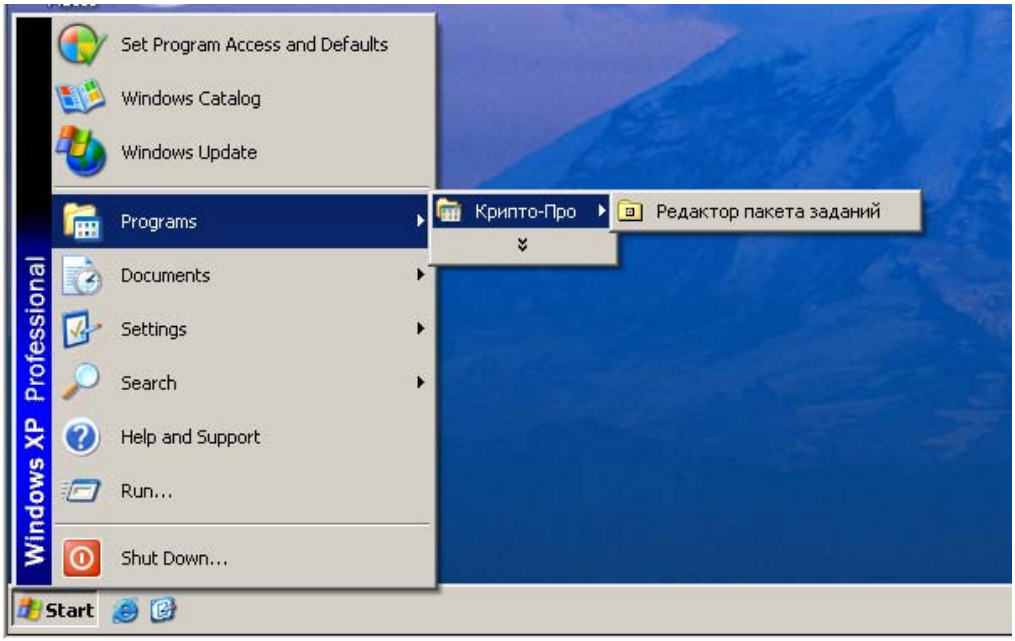
1. Установка СКЗИ КриптоПро CSP и КриптоПро TLS.

Примечание 1. Если известно, что алгоритм открытого ключа сертификата Центра Сертификации, издающего переносимые СОС, а также сертификатов всех вышестоящих ЦС не ГОСТ, то можно не устанавливать СКЗИ КриптоПро CSP и КриптоПро TLS.

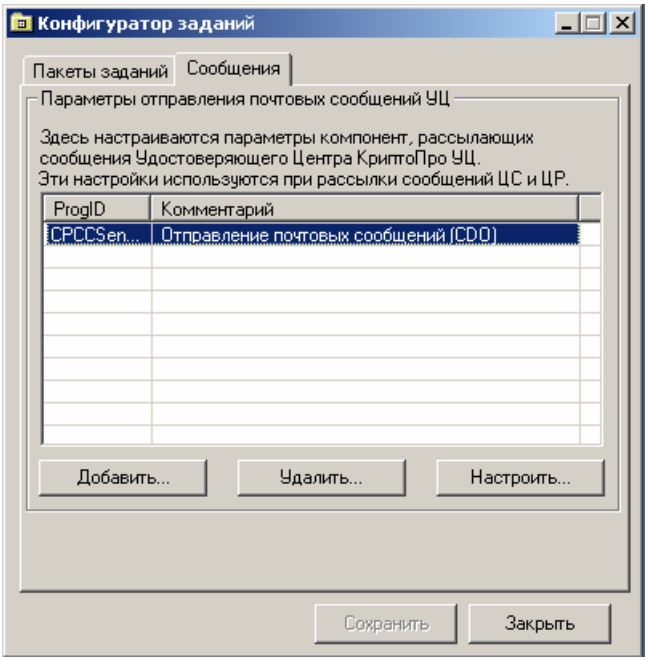
Примечание 2. В случае использования СКЗИ КриптоПро CSP версии 3.0 и выше пакет КриптоПро TLS отдельно устанавливать не нужно.

2. Установка службы очередей сообщений. Этот компонент выбирается в панели «Установка и удаление программ» - «Установка компонентов Windows». Достаточно выбрать подкомпонент «Общие» (для Windows XP и 2003). Для Windows 2000 подкомпонентов нет.
3. Установка программного обеспечения «КриптоПро УЦ. Регламентные задания» путем запуска файла **ScheduledTasks.msi.**

После установки в списке меню «**Пуск**» - «**Программы**» - «**Крипто-Про**» появится пункт «Редактор пакета заданий».

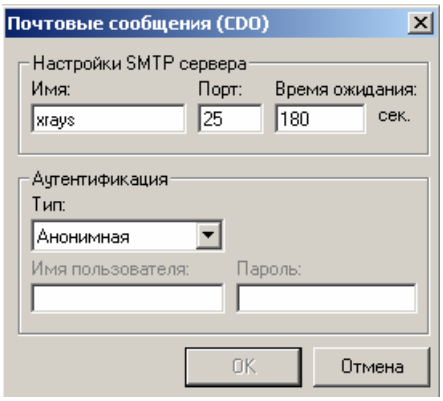


Настройка параметров рассылки почты осуществляется на вкладке «Сообщения» окна «Конфигуратор заданий»:



При нажатии на кнопку «Настроить» появится окно для ввода имени SMTP сервера и параметров.
К числу параметров настройки относятся:

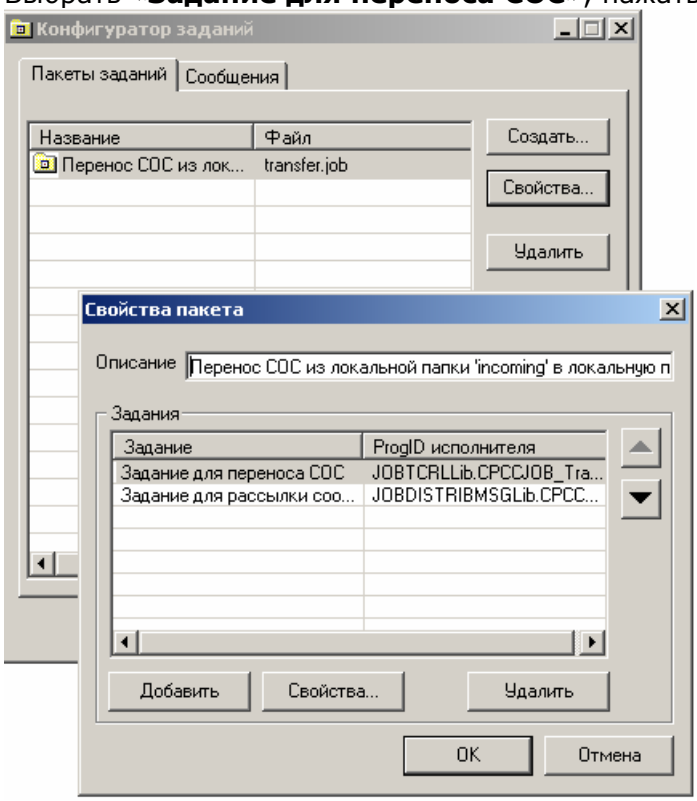
- Имя SMTP сервера;
- Номер порта SMTP сервера;
- Время ожидания ответа SMTP сервера;
- Тип и параметры аутентификации на SMTP сервере.



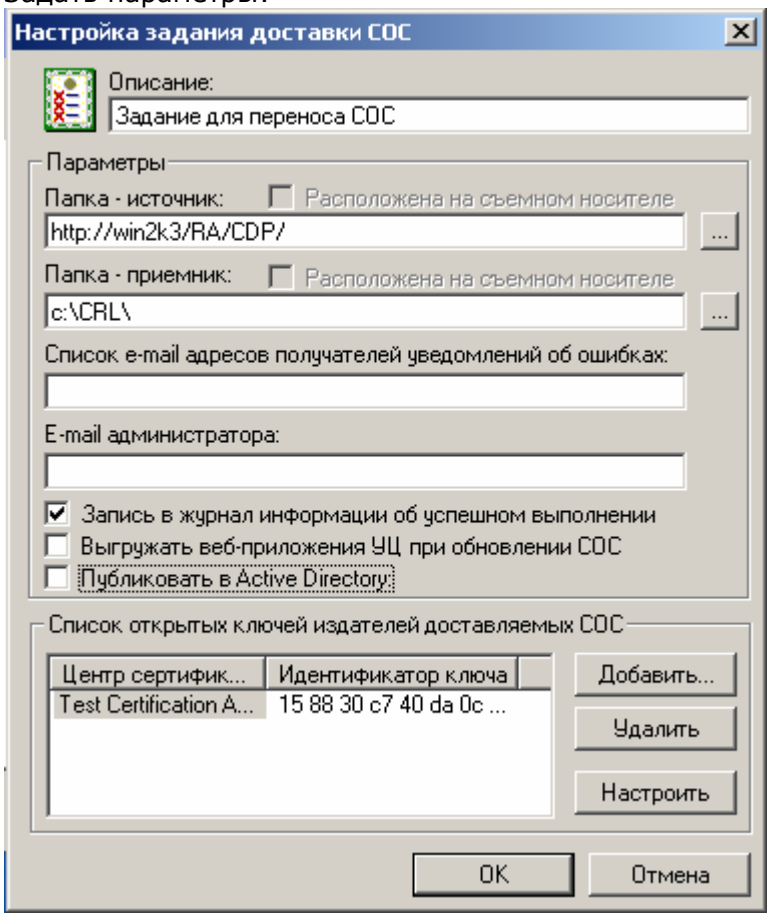
Непосредственную доставку почтовых сообщений до получателей выполняет SMTP сервер организации, где эксплуатируется программное обеспечение «КриптоПро УЦ. Регламентные задания».

Настройка «Задания переноса СОС» для переноса СОС (без использования съемных носителей).

Запустить конфигуратор заданий, в появившемся окне выбрать пакет заданий «**Перенос СОС...**», нажать «**Свойства**».
Выбрать «**Задание для переноса СОС**», нажать «**Свойства**».



Задать параметры:



Папка-источник – локальный или сетевой ресурс, с которого следует забирать СОС

Папка-приемник – локальный или общий сетевой ресурс, на котором следует разместить полученный СОС.

Список *e-mail адресов получателей уведомлений об ошибках* и *e-mail администратора* – в случае, если СОС не удастся забрать или опубликовать, на указанные адреса будут сформированы отчеты об ошибках, которые будут отправлены заданием «Рассылка почтовых сообщений» (если оно настроено).

Флаги:

Запись в журнал информации об успешном выполнении – в случае успешного переноса СОС в системный журнал приложений будет внесена соответствующая запись.

Выгружать веб-приложения при обновлении СОС –в случае отдельного от УЦ задания этот флаг не производит никаких действий, поскольку такие приложения ему не доступны. Сохранён для единообразия интерфейса настройки аналогичного задания переноса СОС на сервере ЦР.

Публиковать СОС в Active Directory – см. «Настройка приложения для публикации СОС в AD» на стр. 10 этого документа.

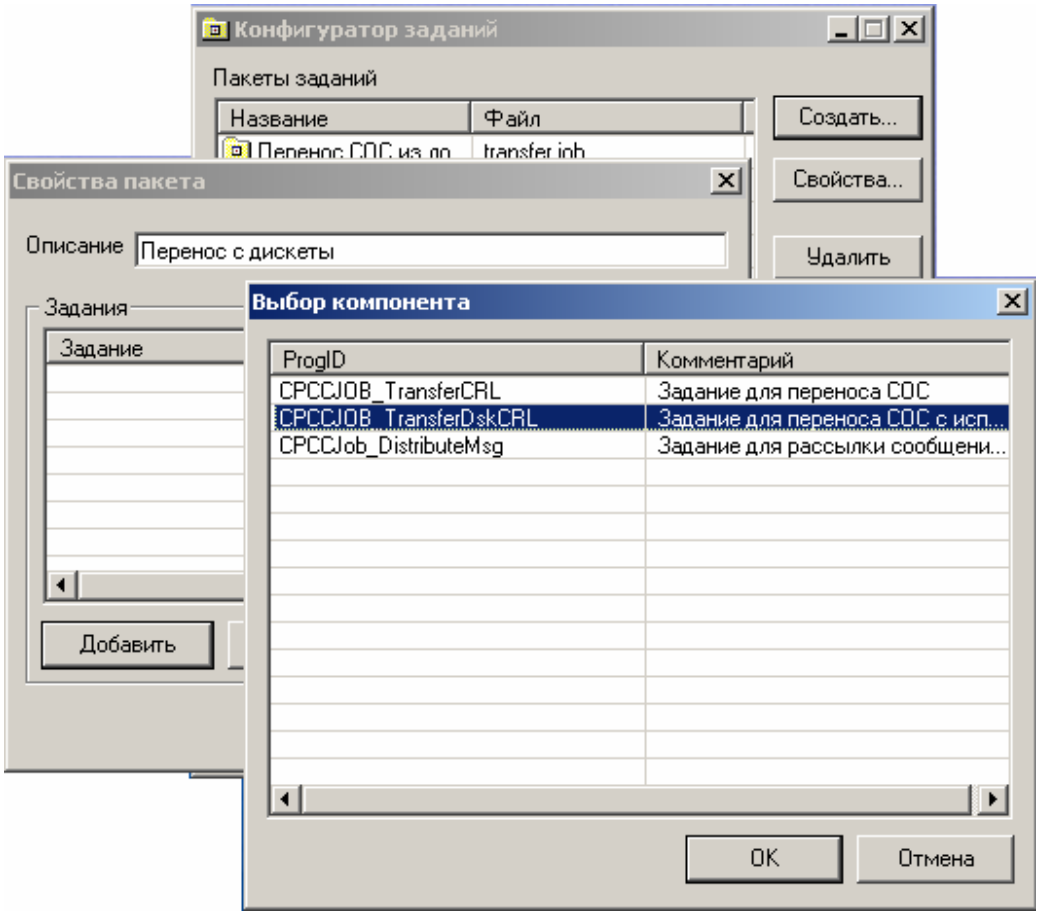
Окно «*Список открытых ключей издателей доставляемых СОС*» - для выбора только тех СОС, открытые ключи издателей которых добавлены в этот список. Для добавления нужного ключа в список нажмите «**Добавить**» и выберите издателя из появившегося списка (список формируется из сертификатов Центров Сертификации, которые установлены в хранилище «Доверенные корневые Центры Сертификации»).

Далее в конфигураторе заданий настраивается расписание выполнения пакета заданий и задается учетная запись, от имени которой будут выполняться задания.

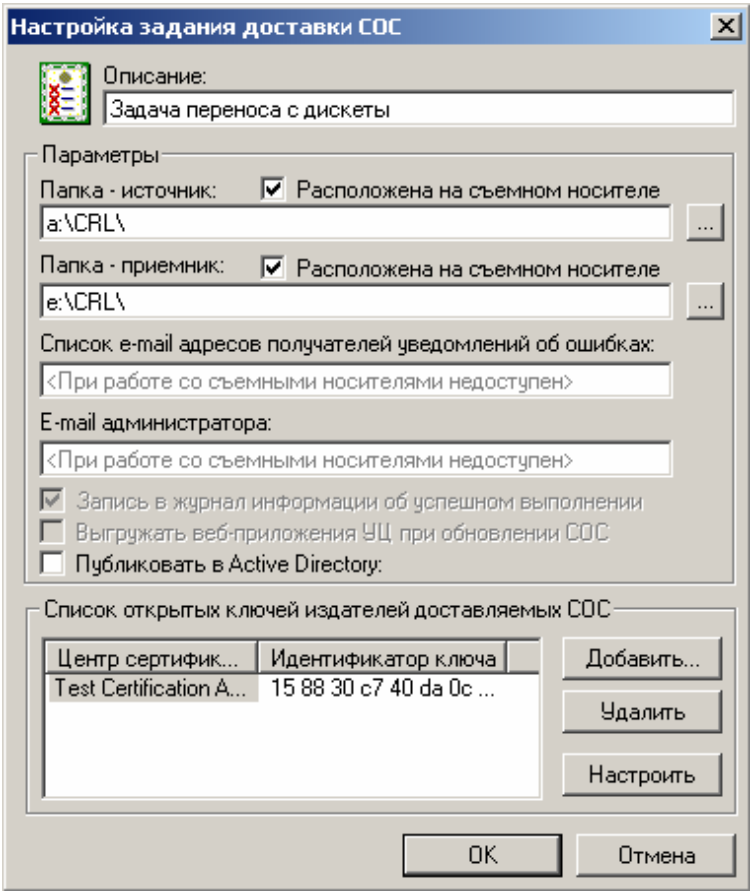
Примечание. Если на компьютере установлена ОС Windows XP, и компьютер не входит в домен, то, перед заданием учетной записи, от имени которой будут выполняться задания, необходимо установить в **0** значение параметра **forceguest** в разделе реестра **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa** и перезагрузить компьютер.

Настройка «Задания переноса СОС» для работы со съемными носителями.

В конфигураторе заданий нажать «**Создать**», ввести в строке «**Описание**» название нового пакета заданий, нажать «**Добавить**». Выбрать «**Задание для переноса СОС с использованием съемных носителей**».



После нажатия кнопки **ОК**, появится окно задания параметров.



Здесь *папка-источник* и *папка-приемник* могут располагаться на съемных носителях.
Как и в случае использования локальных или сетевых ресурсов, необходимо указать *открытый ключ издателя СОС*.
В случае использования съемных носителей недоступна часть опций (они отображаются как неактивные).
Публикация в Active Directory настраивается так же, как в случае работы без использования съемных носителей.

Для случая использования съемных носителей нельзя задать расписание и учетную запись, из-под которой будет выполняться задание – задание выполняется разово, при нажатии на кнопку «**Выполнить**» в конфигураторе заданий от имени текущего пользователя системы.

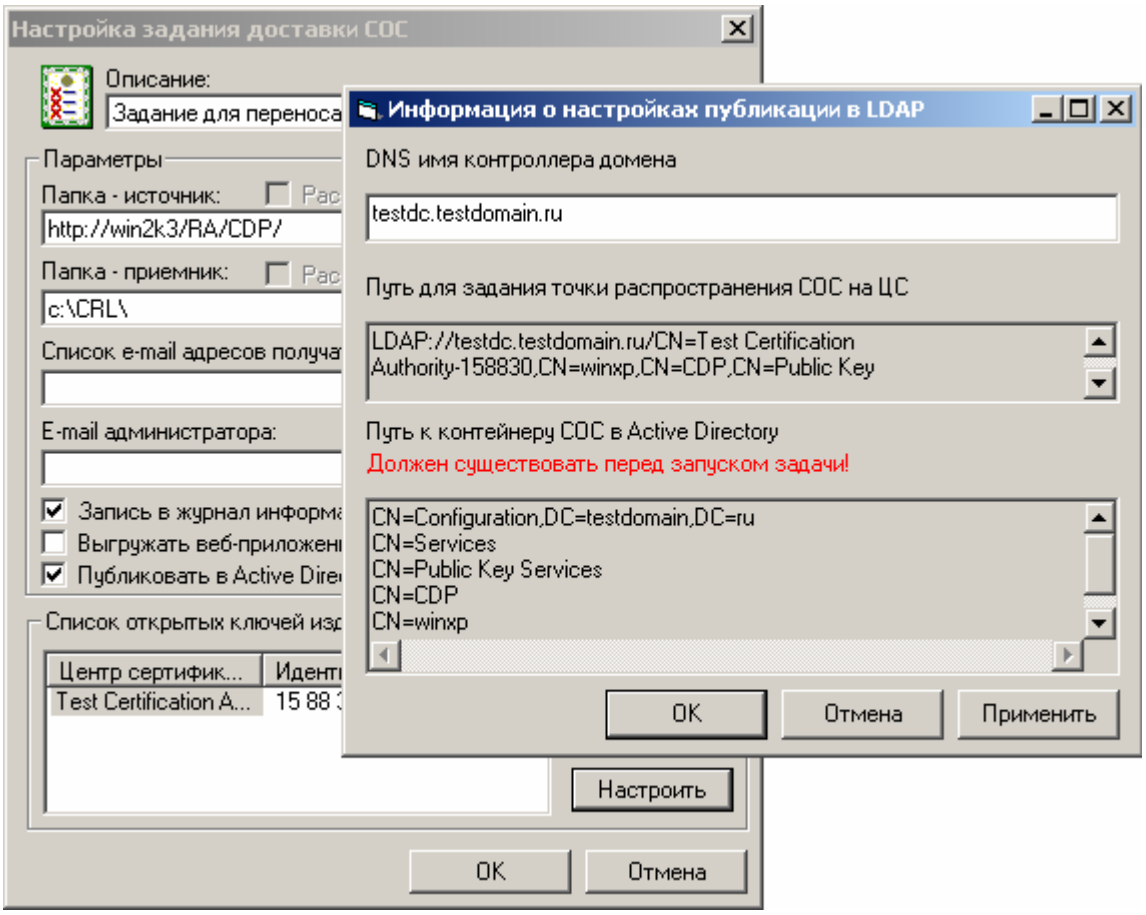
Примечание: при нажатии на кнопку «**Выполнить**», система предложит подготовить носитель с папкой-источником, затем – с папкой-приемником. Нужно убедиться, что носитель вставлен и нажать **ОК**.

Публикация списков отозванных сертификатов в Active Directory.

С компьютера, где выполняется Задание переноса СОС, должен быть доступен сервер Центра Регистрации (либо задание настраивается на самом сервере ЦР, если он включен в домен).

На компьютере, где запускается задание переноса СОС, необходимо выполнить следующие настройки:

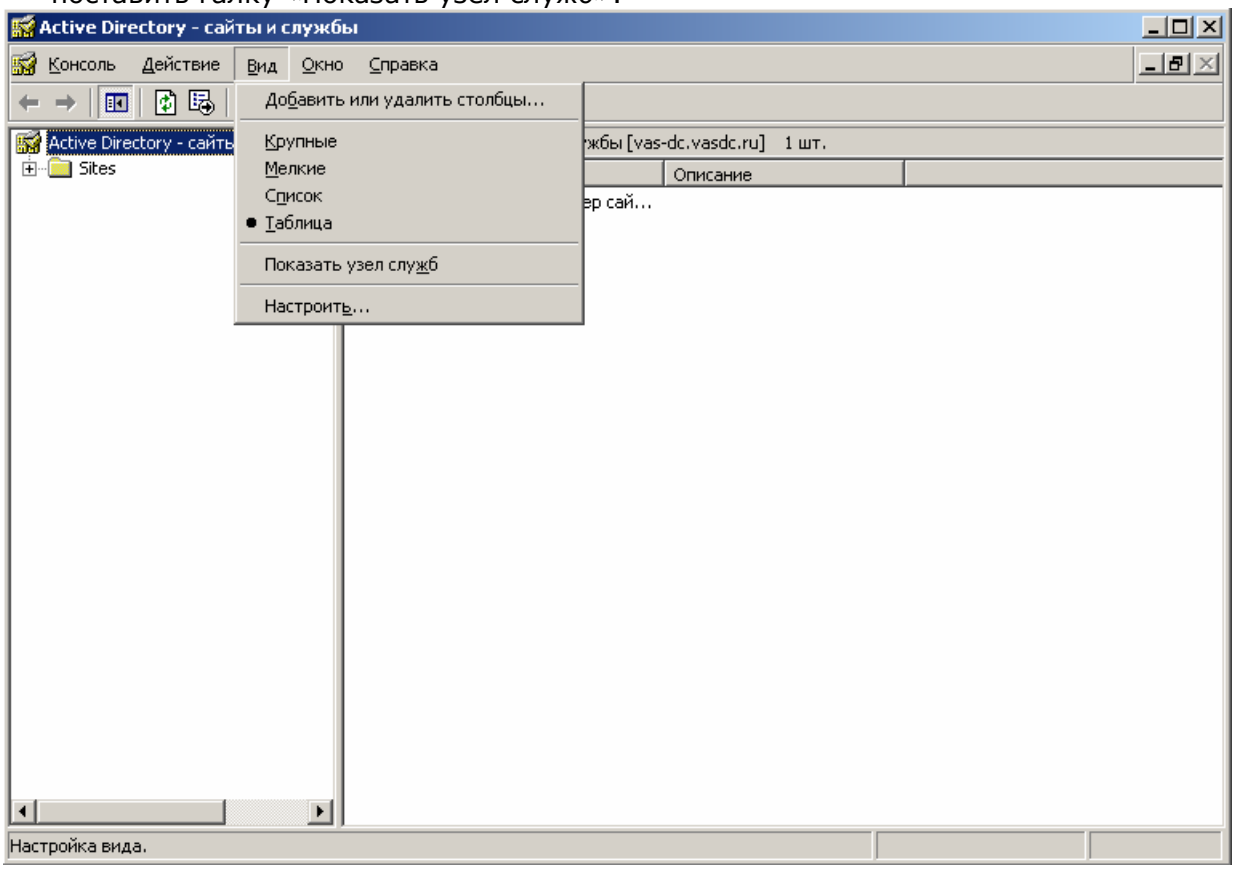
1) Настроить задание переноса (в соответствии с пунктом «Настройка задания переноса») с некоторыми дополнениями:
   - Необходимо включить галку "*Публиковать в Active Directory*";
   - Возле окна «*Список открытых ключей издателей СОС*» нажать кнопку «**Настроить**» и ввести имя контроллера домена.



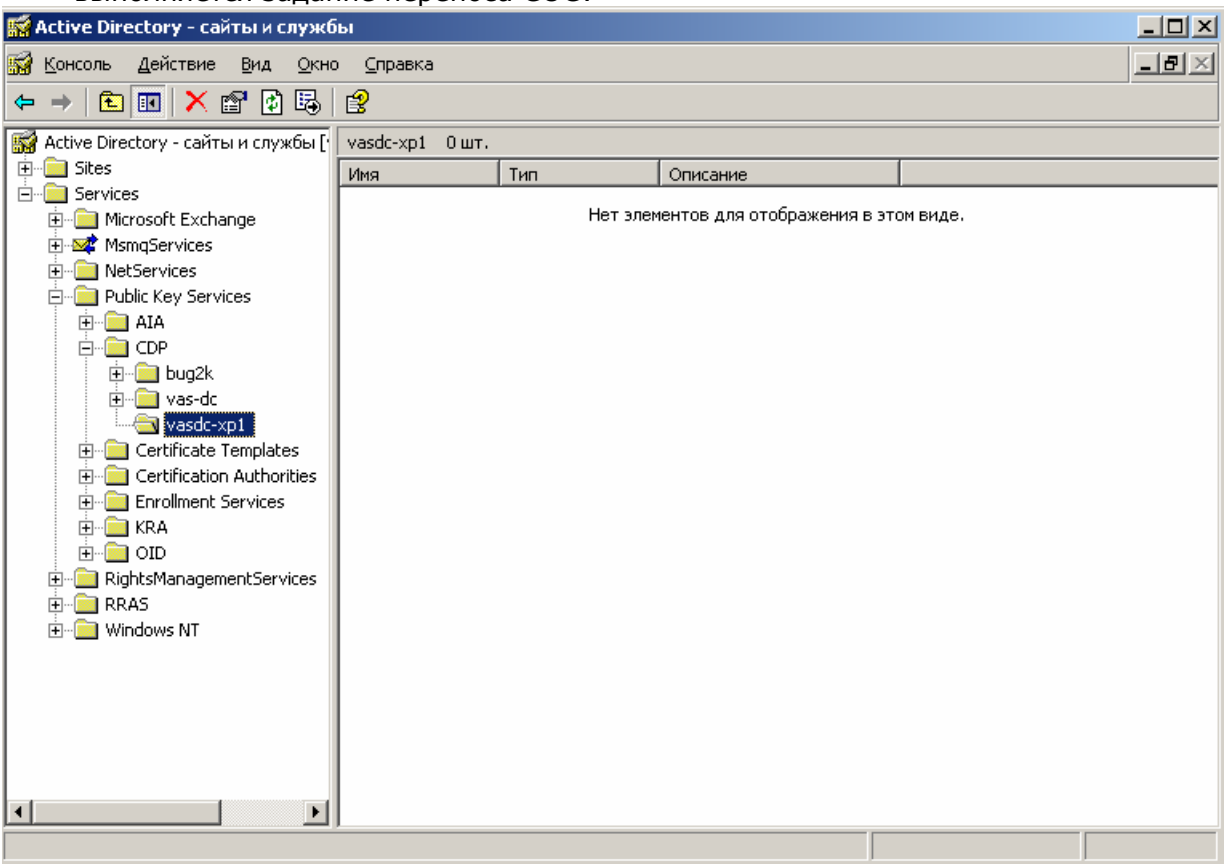
2) Задать учетную запись пользователя домена, под которой будет запускаться задание (см. ниже п. 7-8). Эта учетная запись должна обладать правами по записи CRL в локальное хранилище этого компьютера.
3) Задать расписание этого задания.

Перед запуском задания в AD нужно подготовить место для публикации СОС.

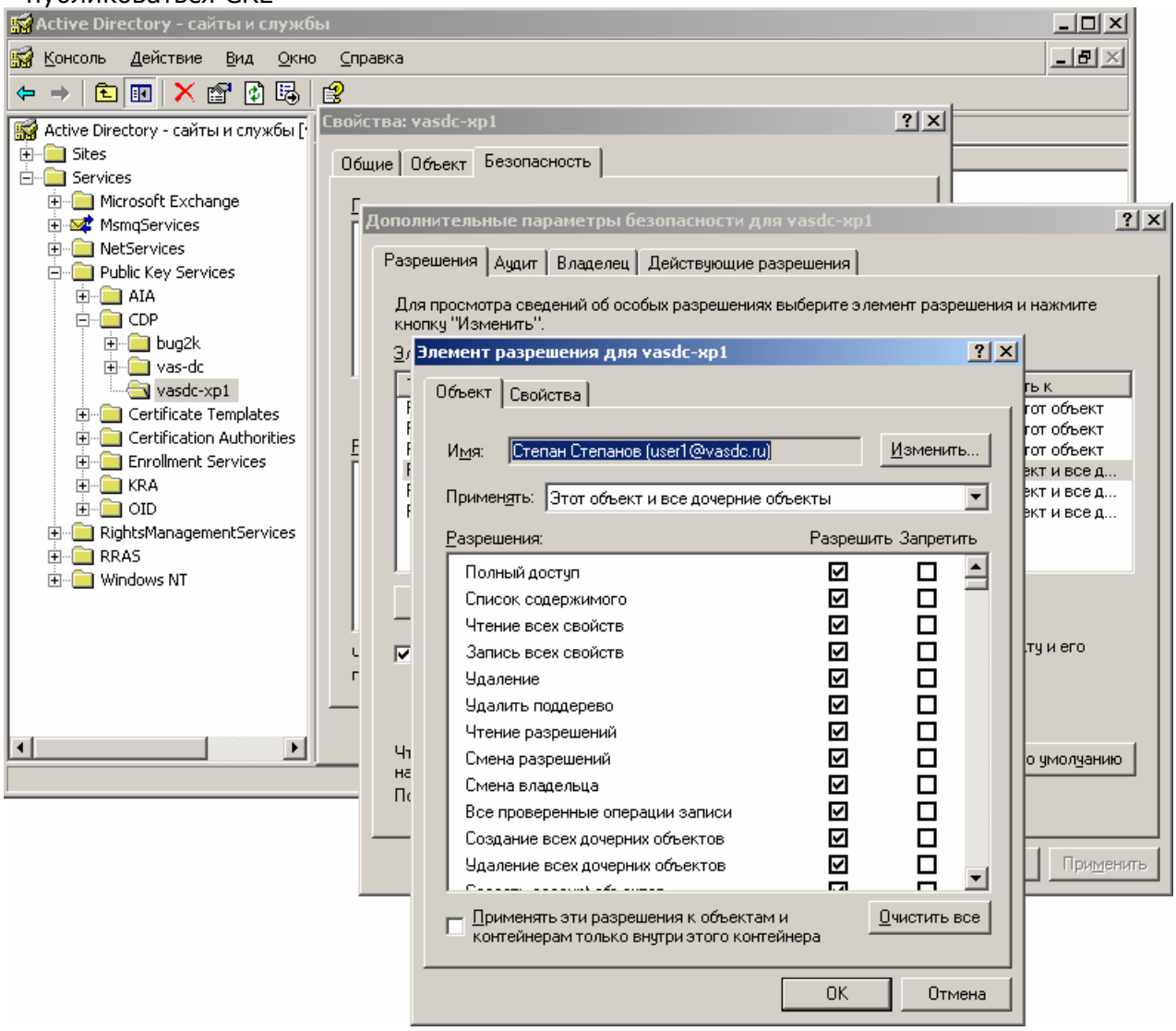
4) Запустить оснастку dssite.msc («Active Directory – сайты и службы»). В меню «Вид» поставить галку «Показать узел служб»:



5) Создать дерево контейнеров в каталоге Services. Дерево контейнеров создается на основании адреса CDP, отображаемого при нажатии на кнопку «**Настроить**» задания переноса СОС – см. п.1. Как правило, достаточно в нужном месте AD (Services – Public Key Services - CDP) создать контейнер с именем, совпадающим с именем компьютера, где выполняется задание переноса СОС:



6) Создать учетную запись и назначить ей полный доступ к контейнеру, в который будут публиковаться CRL



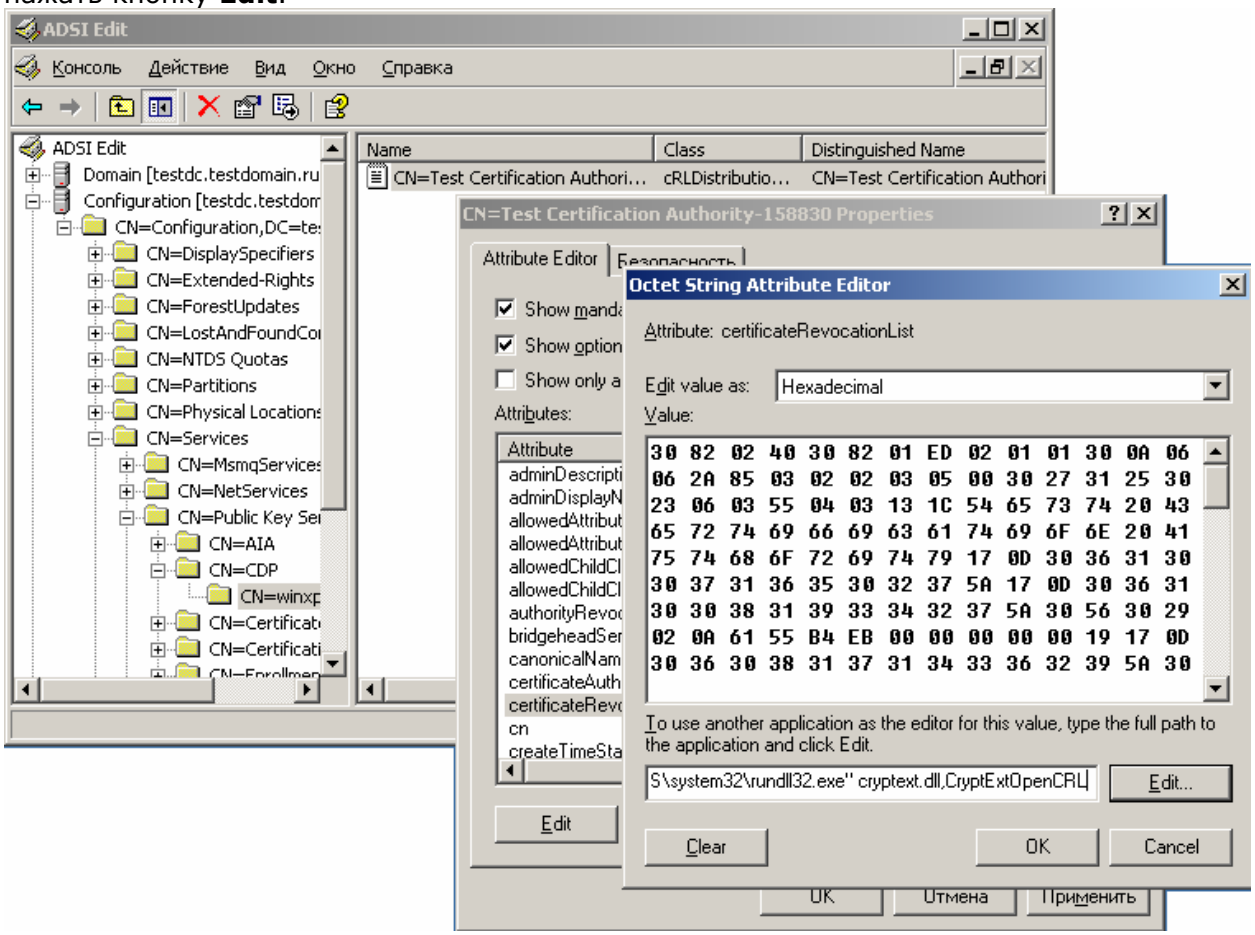
7) Обязательно исправить разрешение с «**Только этот объект**» на «**Этот объект и все дочерние объекты**»
8) На этот раздел AD требуется установить права на чтение для тех пользователей, которые будут обращаться за СОС по протоколу ldap.

Для того, чтобы убедиться в том, что после выполнения Задания переноса СОС в нужном месте AD действительно опубликован правильный СОС, можно открыть этот СОС из AD. Для этого необходимо:

1. Установить сервисные утилиты MS Windows SUPPORT\TOOLS\SUPTOOLS.MSI из дистрибутива Win2003.
2. Запустить оснастку C:\Program Files\Support Tools\adsiedit.msc (лучше с DC).
3. Перейти к разделу AD, содержащему контейнер публикации СОС, по контейнеру (в правой части окна) кликнуть правой кнопкой мыши и выбрать «**Свойства**». Выбрать атрибут **certificateRevocationList** и два раза кликнуть по нему левой кнопкой мыши. В строке **edit** ввести

"C:\WINDOWS\system32\rundll32.exe" cryptext.dll,CryptExtOpenCRL

нажать кнопку **Edit**.



Должен открыться список отозванных сертификатов.
Проверьте поля «Поставщик», «Идентификатор ключа ЦС», сроки начала и окончания действия СОС.