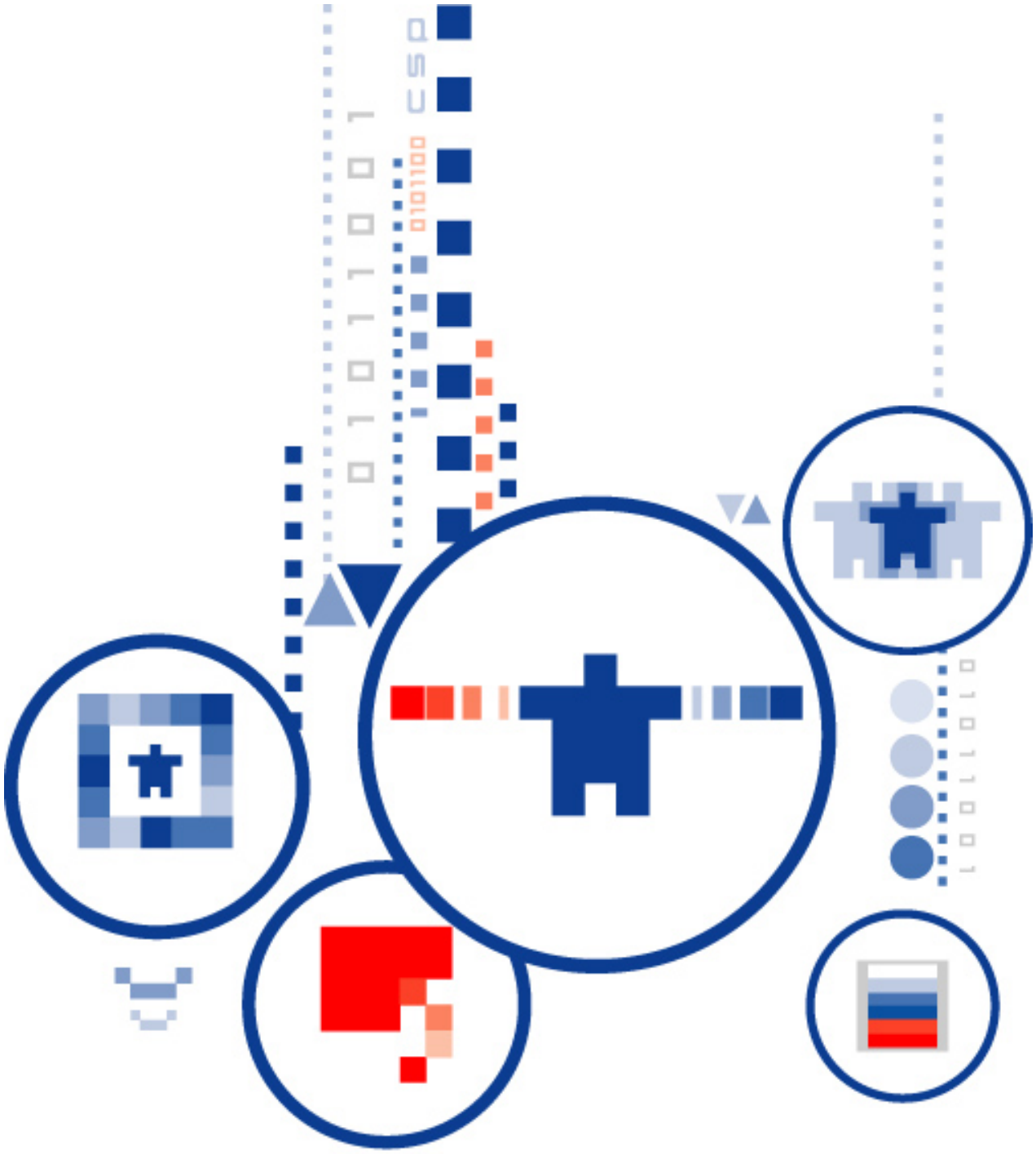
УТВЕРЖДЕН
ЖТЯИ.00035-01 90 05-ЛУ

ЖТЯИ.00035-01 90 05



КриптоПро УЦ

программно–аппаратный комплекс
удостоверяющий центр

Центр Регистрации

Руководство по эксплуатации

АННОТАЦИЯ

Настоящий документ содержит описание процесса настройки и конфигурации программного компонента Центр Регистрации, входящего в состав программно-аппаратного комплекса «Удостоверяющий Центр «КриптоПро УЦ» (ПАК «КриптоПро УЦ»).

Конфигурация программного обеспечения Центра регистрации осуществляется в следующих случаях:

- после первоначальной установки ПО ЦР;
- для изменения режима работы ЦР в процессе эксплуатации.

Настоящий документ предназначен для администраторов как руководство по настройке и конфигурации Центра Регистрации.

Информация о разработчике ПК «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

СОДЕРЖАНИЕ

1. Архитектура и схема взаимодействия компонентов Центра регистрации 5

1.1. Компоненты Центра регистрации 5

1.2. Схема взаимодействия компонентов Центра регистрации 5

1.3. Схемы размещения компонентов Центра регистрации на программно-технических средствах 5

2. Параметры настройки Центра Регистрации 7

2.1.1. Окно настройки параметров Центра Регистрации 7

2.2. Перечень и описание параметров Центра Регистрации 8

2.2.1. Настройка параметров компонент УЦ, рассылающих почтовые сообщения 23

3. Установка и конфигурация нескольких Центров Регистрации на одном выделенном сервере 25

3.1. Создание виртуального Web-узла Web-сервера MS IIS Центра Регистрации 25

3.2. Выпуск и инсталляция сертификата серверной аутентификации Web-сервера ЦР 26

3.3. Установка модуля доступа ЦР 27

3.4. Настройка ПО Центра Регистрации 29

3.5. Удаление модуля доступа ЦР 29

4. Настройка и изменение параметров программного обеспечения Центра Регистрации 32

4.1. Смена размещения базы данных Центра регистрации 32

4.2. Политики обработки запросов 33

4.3. Пользователи Центра Регистрации 35

4.4. Настройка разрешений к допустимым действиям Центра регистрации 37

4.5. Настройка регламентных Заданий 44

4.6. Настройка параметров Центра Регистрации для выпуска сертификатов открытых ключей уполномоченных лиц подчиненных УЦ 49

4.7. Настройка заданий публикации СОС 49

4.8. Настройка политики имени пользователя при создании запроса на регистрацию 54

4.9. Настройка модуля экспорта пользователей и сертификатов в Active Directory 54

5. Использование SQL 2000 Server 57

6. Отправка почтовых сообщений 62

7. Подключение привилегированных пользователей 64

8. Настройка Центра Регистрации для регистрации и обработки запросов на сертификат ЦС подчиненных УЦ 68

9. Использование и управление списком отозванных сертификатов на Центре Регистрации 69

9.1. Установка нового CRL в связи с истечением его срока действия 70

9.2. Установка нового CRL в связи с отзывом сертификата до истечения срока действия старого CRL 71

9.3. Действия администратора при несоблюдении срока установки нового CRL по истечению срока его действия 71

10. Сроки действия ключей Центра Регистрации и Web-сервера Центра Регистрации 73

11. Смена ключей Web-сервера Центра регистрации 74

11.1. Генерация новых ключей и создание запроса на сертификат Web-сервера Центра Регистрации 74
11.2. Выпуск и установка нового сертификата Web-сервера Центра Регистрации 74
11.3. Смена сертификата на Web-узле MS IIS 74
11.4. Уничтожение старых ключей на Центре регистрации 76
12. Смена ключей Центра регистрации 78
12.1. Генерация новых ключей и создание запроса на сертификат Центра Регистрации 78
12.2. Выпуск нового сертификата Центра Регистрации 79
12.3. Добавление нового сертификата в список доверенных ЦР на Центре сертификации 79
12.4. Удаление старого сертификата из списка доверенных ЦР на Центре сертификации 79
12.5. Установка нового сертификата Центра Регистрации 79
12.6. Изменение параметра настройки Центра регистрации 80
12.7. Уничтожение старых ключей на Центре регистрации 81
13. Обеспечение целостности программных средств Центра Регистрации 82
14. Приложение «Параметры Центра Регистрации» 83
14.1. Запуск приложения 83
14.2. Удаление виртуального каталога веб-интерфейса 83
14.3. Создание новой (пустой) базы данных Центра Регистрации 84
14.3.1. Создание новой базы данных в экземпляре CPCC для MSDE 84
14.3.2. Создание новой базы данных в экземпляре MS SQL Server 2000 86
14.4. Изменение базы данных 86
14.5. Установка (ввод параметров) лицензии 87
15. Настройка репликации базы данных Центра Регистрации КриптоПро УЦ 89
15.1. Предварительное конфигурирование издателя 89
15.1.1. Настройка публикации и распространения 89
15.1.2. Настройка учетной записи службы SQL Server Agent 91
15.2. Предварительное конфигурирование подписчика 91
15.3. Настройка репликации 91
16. Удаление программного обеспечения Центра регистрации 93
17. Перечень сокращений 95
18. Перечень рисунков 96
19. Перечень таблиц 99
20. Перечень ссылочных документов 100

1. Архитектура и схема взаимодействия компонентов Центра регистрации

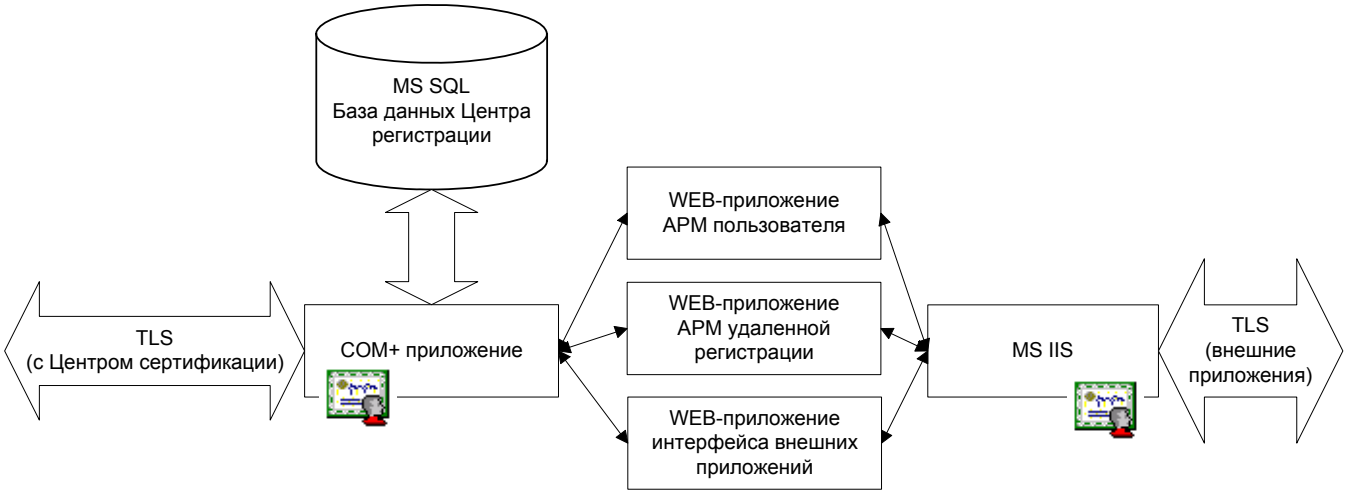
1.1. Компоненты Центра регистрации

В состав Центра регистрации входят следующие компоненты:

- База данных SQL-сервера (БД SQL 200 Server MSDE)
- COM+приложения
- Web-приложение интерфейса внешних приложений
- Web-приложение АРМ пользователя ЦР, включающее в себя:
  - АРМ регистрации пользователя (АРМ регистрации пользователя)
  - АРМ зарегистрированного пользователя с маркерным доступом
  - АРМ зарегистрированного пользователя с ключевым доступом
- Приложение настройки параметров Центра регистрации
- Приложения Мастеров:
  - Мастер создания запроса на клиентский сертификат ЦР
  - Мастер создания запроса на сертификат Web-сервера ЦР
  - Мастер установки клиентского сертификата ЦР
  - Мастер установки сертификата Web-сервера ЦР

1.2. Схема взаимодействия компонентов Центра регистрации

Рисунок 1. Схема взаимодействия компонентов Центра регистрации



1.3. Схемы размещения компонентов Центра регистрации на программно-технических средствах

Схема 1. Все программные компоненты Центра регистрации размещаются на одном выделенном сервере с использованием MSDE.

Данная схема предназначена для эксплуатации по стандартной или расширенной Лицензии производителя. В качестве сервера базы данных ЦР используется MSDE. Рекомендуемое ограничение на число пользователей - до 10 000 пользователей.

Схема 2. Все программные компоненты Центра регистрации размещаются на одном выделенном сервере с использованием MS SQL Server 2000 Enterprise или Standard Edition.

Данная схема предназначена для эксплуатации по расширенной Лицензии производителя. В качестве сервера базы данных ЦР используется редакция Enterprise или Standard Edition MS SQL Server 2000. Рекомендуемое ограничение на число пользователей - до 100 000 пользователей.

Схема 3. База данных размещается на выделенном SQL-сервере редакции Enterprise или Standard Edition.

Данная схема предназначена для эксплуатации по расширенной Лицензии производителя и обеспечивает более высокую производительность системы (баланс загрузки). Ограничений на число пользователей нет.

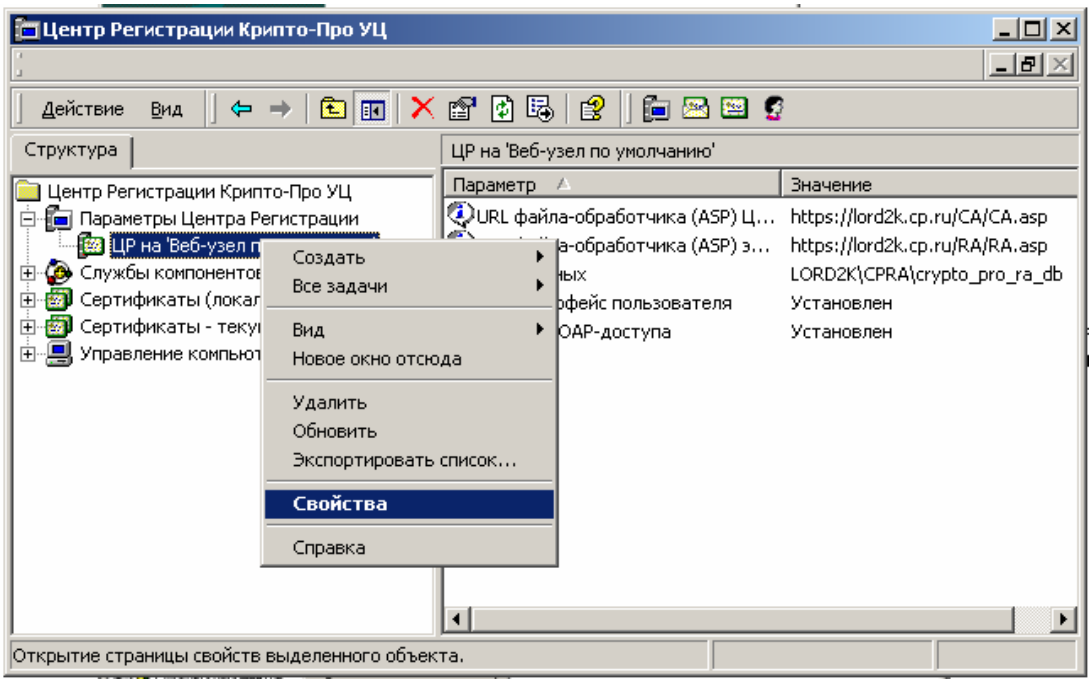
Для расчета размеров баз данных и выделения свободного пространства на жестких дисках серверов ЦР рекомендуется учитывать следующий показатель – на 1 пользователя ежегодно расходуется около 10Кбайт в базе данных ЦР.

2. Параметры настройки Центра Регистрации

2.1.1. Окно настройки параметров Центра Регистрации

Настройка параметров программного обеспечения Центра Регистрации осуществляется в свойствах узла **Центр Регистрации** приложения **Параметры Центра Регистрации** (см. Рисунок 2).

Рисунок 2. Пункт "Свойства" узла Центра Регистрации



2.2. Перечень и описание параметров Центра Регистрации

Наименование параметра	Описание параметра	Место его настройки	Комментарий
Адрес URL файла-обработчика Центра Регистрации	определяет местоположение и протокол доступа к файлу обработчику программного интерфейса Центра Регистрации, с которым будут взаимодействовать внешние (по отношению к ЦР) приложения (в том числе АРМ пользователя и АРМ администратора ЦР)	вкладка **Общие** свойств модуля доступа Центра регистрации	Как правило, дополнительной корректировки после установки ПО Центра Регистрации данный параметр не требует. По умолчанию - https://доменное_имя_ЦР/RA/RA.asp
Адрес URL файла-обработчика Центра Сертификации	определяет местоположение и протокол доступа к файлу обработчику программного интерфейса Центра сертификации, с которым будет взаимодействовать установленный Центр регистрации	вкладка **Общие** свойств модуля доступа Центра регистрации	В шаблоне параметра необходимо заменить имя localhost на доменное имя Web-сервера Центра сертификации По умолчанию - https://localhost/CA/CA.asp
Сертификат подписи и аутентификации Центра регистрации	Определяет клиентский сертификат Центра Регистрации, который используется для взаимодействия с Центром Сертификации	вкладка **Общие** свойств модуля доступа Центра регистрации	Этот сертификат должен быть включен в список доверенных Центров Регистрации на Центре Сертификации. По умолчанию – не задан
Очередь сообщений	определяет имя существующей частной транзакционной очереди сообщений, в которую будут помещаться сообщения, формируемые ЦР, для последующей отправки по почте	вкладка **Общие** свойств модуля доступа Центра регистрации	Как правило, дополнительной корректировки после установки ПО Центра Регистрации данный параметр не требует. Рекомендуется осуществлять смену очереди сообщений только квалифицированными сертифицированными специалистами. По умолчанию - ra_1_mail
AdminEMailAddress	определяет адрес электронной почты, от которого будут отправляться почтовые сообщения	вкладка **Политики** свойств модуля доступа Центра регистрации, группа **Дополнительные**	По умолчанию - postmaster

		параметры	
KeyValidityPeriod	определяет срок действия закрытых ключей пользователей, зарегистрированных на данном ЦР. Используется для оповещения пользователей и изменения статуса сертификатов открытых ключей в реестре Центра Регистрации	вкладка **Политики** свойств модуля доступа Центра регистрации, группа **Дополнительные параметры**	По умолчанию – 1 год 3 месяца
DenyDuplicateRegRequests	определяет политику проверки уникальности имен пользователей при постановке в очередь запросов на регистрацию.	вкладка **Политики** свойств модуля доступа Центра регистрации, группа **Дополнительные параметры**	0 – ставить в очередь запрос на регистрацию, даже если имя пользователя в этом запросе совпадает с именем пользователя в ранее поданном запросе не регистрацию. 1 – отвергать (не ставить в очередь) запрос на регистрацию, в котором имя пользователя совпадает с именем пользователя в ранее поданном запросе не регистрацию. По умолчанию – 0
PendingRegRequestLimit	определяет максимальное число необработанных запросов на регистрацию	вкладка **Политики** свойств модуля доступа Центра регистрации, группа **Дополнительные параметры**	0 – ограничений нет. 1-10000 – не ставить в очередь запросы на регистрацию (поданные через веб-интерфейс ЦР) при достижении заданного лимита необработанных запросов на регистрацию. По умолчанию – 0. Примечание. Для запросов, поданных не через веб-интерфейс ЦР ограничений нет в любом случае.
SendCertToUser	определяет необходимость прикрепления к письму, формируемого в адрес пользователя, изготовленного сертификата открытого ключа.	вкладка **Политики** свойств модуля доступа Центра регистрации, группа **Дополнительные параметры**	0 – не прикреплять, 1 – прикреплять. По умолчанию - 0
SendAcceptCertReqWithTokenNotification	определяет отправку почтового сообщения, при одобрении (принятии) запроса на сертификат, поступившего от пользователя с	вкладка **Политики** свойств модуля доступа Центра регистрации, группа	0 – не отправлять почтового сообщения, 1 – отправлять почтовое сообщение. По умолчанию - 0

	использованием АРМ зарегистрированного пользователя с маркерным доступом.	**Дополнительные параметры**	
SendAcceptCertReqNotification	определяет отправку почтового сообщения, при одобрении (принятии) любого запроса на сертификат, за исключением запросов, поступивших от пользователя с использованием АРМ зарегистрированного пользователя с маркерным доступом.	вкладка **Политики** свойств модуля доступа Центра регистрации, группа **Дополнительные параметры**	0 – не отправлять почтового сообщения, 1 – отправлять почтовое сообщение. По умолчанию - 0
SendDenyCertReqWithTokenNotification	определяет отправку почтового сообщения, при отклонении запроса на сертификат, поступившего от пользователя с использованием АРМ зарегистрированного пользователя с маркерным доступом.	вкладка **Политики** свойств модуля доступа Центра регистрации, группа **Дополнительные параметры**	0 – не отправлять почтового сообщения, 1 – отправлять почтовое сообщение. По умолчанию - 0
SendDenyCertReqNotification	определяет отправку почтового сообщения, при отклонении любого запроса на сертификат, за исключением поступивших запросов, от пользователя с использованием АРМ зарегистрированного пользователя с маркерным доступом.	вкладка **Политики** свойств модуля доступа Центра регистрации, группа **Дополнительные параметры**	0 – не отправлять почтового сообщения, 1 – отправлять почтовое сообщение. По умолчанию - 0
SendAcceptRegReqWithTokenNotification	определяет отправку почтового сообщения, при одобрении (принятии) запроса на регистрацию, поступившего от пользователя с использованием АРМ регистрации пользователя.	вкладка **Политики** свойств модуля доступа Центра регистрации, группа **Дополнительные параметры**	0 – не отправлять почтового сообщения, 1 – отправлять почтовое сообщение. По умолчанию - 0
SendAcceptRegReqNotification	определяет отправку почтового сообщения, при одобрении (принятии) любого запроса на регистрацию, за исключением запросов, поступивших от пользователя с использованием АРМ	вкладка **Политики** свойств модуля доступа Центра регистрации, группа **Дополнительные параметры**	0 – не отправлять почтового сообщения, 1 – отправлять почтовое сообщение. По умолчанию - 0

	регистрации пользователя.		
SendDenyRegReqWithTokenNotification	определяет отправку почтового сообщения, при отклонении запроса на регистрацию, поступившего от пользователя с использованием АРМ регистрации пользователя.	вкладка **Политики** свойств модуля доступа Центра регистрации, группа **Дополнительные параметры**	0 – не отправлять почтового сообщения, 1 – отправлять почтовое сообщение. По умолчанию - 0
SendDenyRegReqNotification	определяет отправку почтового сообщения, при отклонении любого запроса на регистрацию, за исключением запросов, поступивших от пользователя с использованием АРМ регистрации пользователя.	вкладка **Политики** свойств модуля доступа Центра регистрации, группа **Дополнительные параметры**	0 – не отправлять почтового сообщения, 1 – отправлять почтовое сообщение. По умолчанию - 0
TokenPeriod	Определяет срок действия («жизни») маркера временного доступа (логина) для входа на АРМ зарегистрированного пользователя с маркером временного доступа	вкладка **Политики** свойств модуля доступа Центра регистрации, группа **Дополнительные параметры**	Как правило, этот срок делают равным времени пересылки документов от пользователя к администратору ЦР и рассмотрения запроса администратором ЦР. По умолчанию – 1 месяц
Модуль экспорта сертификатов	определяет внешний модуль экспорта сертификатов во внешние системы (типа MS Active Directory) и параметры его работы	вкладка **Политики** свойств модуля доступа Центра Регистрации	При установке Центра Регистрации устанавливается один модуль экспорта сертификатов производства КРИПТО-ПРО, который позволяет осуществлять экспорт в MS Active Directory. Имеется возможность разрабатывать свои модули и подключать их согласно интерфейсу, описанному в Руководстве программиста. По умолчанию данный модуль не настроен.
Обработка запросов на отзыв (улучшенный ключ)	список, определяющий политику постановки в очередь на обработку запросов на отзыв (приостановление/возобновление действия) сертификатов открытого ключа, поступающих на Центр Регистрации, основанную на	вкладка **Политики** свойств модуля доступа Центра Регистрации	Политика определяется разрешениями на допустимые области использования сертификатов открытых ключей для соответствующей роли, присвоенной после аутентификации пользователя.

	анализе EKU сертификата, соответствующего запросу на отзыв.		
Обработка неподписанных запросов (улучшенный ключ)	список, определяющий политику постановки в очередь на обработку неподписанных (самоподписанных) запросов на сертификат открытого ключа (PKCS#10), поступающих на Центр Регистрации, основанную на анализе EKU запроса на сертификат.	вкладка **Политики** свойств модуля доступа Центра Регистрации	Политика определяется разрешениями на допустимые области использования сертификатов открытых ключей для соответствующей роли, присвоенной после аутентификации пользователя.
Обработка неподписанных запросов (расширения)	список, определяющий политику постановки в очередь на обработку неподписанных (самоподписанных) запросов на сертификат открытого ключа (PKCS#10), поступающих на Центр Регистрации, основанную на анализе расширений, указанных в запросе на сертификат.	вкладка **Политики** свойств модуля доступа Центра Регистрации	Политика определяется разрешениями на расширения сертификатов открытых ключей для соответствующей роли, присвоенной после аутентификации пользователя.
Обработка подписанных запросов (улучшенный ключ)	список, определяющий политику постановки в очередь на обработку подписанных запросов на сертификат открытого ключа (PKCS#7), поступающих на Центр Регистрации, основанную на анализе EKU запроса на сертификат.	вкладка **Политики** свойств модуля доступа Центра Регистрации	Политика определяется разрешениями на допустимые области использования сертификатов открытых ключей для соответствующей роли, присвоенной после аутентификации пользователя.
Обработка подписанных запросов (расширения)	список, определяющий политику постановки в очередь на обработку подписанных запросов на сертификат открытого ключа (PKCS#7), поступающих на Центр Регистрации, основанную на анализе расширений, указанных в запросе на сертификат.	вкладка **Политики** свойств модуля доступа Центра Регистрации	Политика определяется разрешениями на расширения сертификатов открытых ключей для соответствующей роли, присвоенной после аутентификации пользователя.
Политика имен	список параметров, определяющий ограничения на использование идентификаторов имен владельцев	вкладка **Политики** свойств модуля доступа Центра	Согласно этому списку формируются поля ввода при создании запроса на регистрацию пользователя в АРМ

	(SubjectDN) в обрабатываемых запросах на сертификат открытого ключа и запросов на регистрацию пользователей.	Регистрации	администратора ЦР и АРМ пользователя (подробнее см. ниже данной таблицы)
Системные роли	Список объектных идентификаторов, определяющих состав системных ролей для ЦР	вкладка **Политики** свойств модуля доступа Центра Регистрации	Для системных ролей, указанных в списке, можно давать разрешения на доступ к методам ЦР на вкладке **Безопасность** По умолчанию определены следующие системные роли: • Администратор • Оператор • Пользователь • Временный сертификат • Прошедший проверку
Шаблоны писем	список шаблонов писем, высылаемых по событиям Центром регистрации в адрес получателей.	вкладка **Политики** свойств модуля доступа Центра Регистрации	Список шаблонов писем предопределен, но формат и текст почтовых сообщений может быть изменен.
Шаблоны сертификатов	список, содержащий перечень шаблонов для областей применения сертификатов открытых ключей (EKU) при формировании запросов на сертификат	вкладка **Политики** свойств модуля доступа Центра Регистрации	При создании запроса на сертификат в АРМ администратора ЦР и АРМ пользователя предоставляется возможность выбрать шаблон, а не задавать области использования самостоятельно
Разрешения к допустимым действиям Центра регистрации	список действий, допустимых для выполнения на Центре регистрации, с настройками прав доступа к нему системными ролями.	вкладка **Безопасность** свойств модуля доступа Центра Регистрации	На каждое действие из списка можно определить разрешения (права доступа) для соответствующей роли в системе. (подробнее см. ниже данной таблицы)
Оповещение администратора о количестве необработанных запросов	Пакет заданий, анализирующее очередь запросов и формирующее сообщение администратору о состоянии очереди	вкладка **Задачи** свойств модуля доступа Центра Регистрации	Пакет включает в себя и задание на выполнение задачи рассылки сообщения 1 - посылать сообщения в случае, если в очереди нет необработанных запросов, 0

			– не посылать сообщение. По умолчанию – 1 Расписание на выполнение **не настроено**
Оповещение о превышении количества запросов на сертификат	Задание, анализирующее очередь запросов на сертификат на предмет превышение установленного лимита запросов на сертификат в течение заданного периода	вкладка **Задачи** свойств модуля доступа Центра Регистрации	Настройки задания определяют допустимый предел количества запросов на сертификат в течение указанного периода Расписание на выполнение **настроено: ежесуточно в 21 час**
Оповещение об истечении срока действия сертификата	Задание, анализирующее реестр сертификатов на предмет окончания действия сертификата на момент выполнения задания	вкладка **Задачи** свойств модуля доступа Центра Регистрации	Настройки задания режима отправки уведомлений Расписание на выполнение **настроено: ежесуточно в 00 часов**
Удаление неактивных пользователей	Задание, анализирующее реестр пользователей и удаляющее из базы данных Центра Регистрации всю информацию о неактивных пользователях	вкладка **Задачи** свойств модуля доступа Центра Регистрации	Неактивным считается пользователь, не имеющий ни одного действующего сертификата, ни одного не обработанного запроса на сертификат и не имеющий действующего маркера временного доступа Расписание на выполнение **не настроено**
Рассылка сообщений, стоящих в очереди	Задание, обрабатывающее **всю** очередь сообщений Центра Регистрации и формирующее почтовые сообщения.	вкладка **Задачи** свойств модуля доступа Центра Регистрации	Настройки задания определяют имя частной транзакционной очереди сообщений Расписание на выполнение **настроено: ежесуточно каждые 10 минут**
Оповещение о скором истечении срока действия секретного ключа	Задание, анализирующее реестр сертификатов на предмет окончания действия соответствующего закрытого ключа в устанавливаемом периоде	вкладка **Задачи** свойств модуля доступа Центра Регистрации	Настройки задания определяют временной интервал анализа сертификатов Расписание на выполнение **настроено: ежесуточно в 00 часов**
Оповещение об окончании действия секретных ключей	Задание, анализирующее реестр сертификатов на предмет	вкладка **Задачи** свойств модуля	Настройки задания режим отправки уведомлений

	окончания действия закрытых ключей соответствующих сертификатов на момент выполнения задания	доступа Центра Регистрации	Расписание на выполнение **настроено: ежесуточно в 00 часов**
Отзыв сертификатов с истекшим сроком приостановления действия	Задание, анализирующее реестр запросов на отзыв (приостановление действия) сертификатов на предмет окончания приостановления действия сертификата на момент выполнения задания	вкладка **Задачи** свойств модуля доступа Центра Регистрации	Настройки задания режим отправки уведомлений Расписание на выполнение **настроено: ежесуточно каждый 1 час**
Оповещение о скором истечении срока приостановления действия сертификата	Задание, анализирующее реестр запросов на отзыв (приостановление действия) сертификатов на предмет окончания приостановления действия сертификата в устанавливаемом периоде	вкладка **Задачи** свойств модуля доступа Центра Регистрации	Настройки задания определяют временной интервал анализа запросов на приостановление действия сертификатов Расписание на выполнение **настроено: ежесуточно в 00 часов**
Перенос COC из локальной папки CDP на дискету	Задание осуществляет перенос файлов COC из папки CDP, расположенной на Центре Регистрации, на дискету	вкладка **Задачи** свойств модуля доступа Центра Регистрации	Расписание на задание не настраивается, выполняется только вручную с помощью кнопки **Выполнить**
Публикация COC из сетевого ресурса CDP ЦР вышестоящего ЦС на сетевой ресурс incoming своего ЦС	Пакет заданий, которые осуществляют перенос файлов COC с Центра Регистрации вышестоящего УЦ на Центр Сертификации своего УЦ	вкладка **Задачи** свойств модуля доступа Центра Регистрации	Настройка задания определяет размещение папок CDP источника и приемника и перечень COC, которые надо перенести Расписание на выполнение **не настроено**
Получение COC из сетевого ресурса CDP своего ЦС в локальную папку CDP	Задание осуществляет перенос файлов COC из папки CDP, расположенной на Центре Сертификации, в папку CDP, расположенную на Центре Регистрации	вкладка **Задачи** свойств модуля доступа Центра Регистрации	Пакет включает в себя и задание на выполнение задачи рассылки сообщения Настройка задания определяет размещение папок CDP источника и приемника и перечень COC, которые надо перенести Расписание на выполнение **не настроено**

Публикация COC с дискеты на сетевой ресурс incoming своего ЦС	Задание осуществляет перенос файлов COC с дискеты на Центре Регистрации в папку CDP, расположенную на Центре Сертификации	вкладка **Задачи** свойств модуля доступа Центра Регистрации	Расписание на задание не настраивается, выполняется только вручную с помощью кнопки **Выполнить**
Сообщение действующим пользователям	Задание формирует сообщение в очередь сообщений для каждого пользователя ЦР, имеющего действующий сертификат	вкладка **Задачи** свойств модуля доступа Центра Регистрации	Текст сообщения оформляется в шаблоне письма **Оповещение действующего пользователя УЦ о событии** Рекомендуется расписание не настраивать, т.к. это задание предназначено для отправки разовых или редких сообщений (например, о факте смены ключей и сертификата ЦС) Расписание на выполнение **не настроено**
База данных			

Особенности настройки политики имён.

1. Можно разрешить использование нескольких одноимённых компонентов имени.

2. Можно пометить некоторые (или все) компоненты имени как обязательные для заполнения (при создании запроса на регистрацию пользователя на АРМе администратора или через веб-интерфейс ЦР). По умолчанию обязательным является только поле «Общее имя».

3. Если сервер ЦР включён в домен Windows 2000 (2003), то можно настроить соответствие между компонентами имени пользователей ЦР и атрибутов Active Directory (AD). Изменения может делать пользователь домена, который обладает правами администратора на сервере ЦР. По умолчанию выбранные компоненты имени (Общее имя, Подразделение, Организация, Город, Область, Страна, Электронная почта) связаны с аналогичными атрибутами AD – соответственно, cn, ou, company, l, st, c, mail. При добавлении нового компонента имени можно выбрать атрибут AD, который будет соответствовать этому компоненту (или оставить поле атрибута пустым).

При создании пользователя ЦР на АРМе администратора ЦР вместо ручного ввода информации о пользователе можно указать пользователя AD, и информацией из AD будут заполнены компоненты имени пользователя.

При этом:

1) если атрибут AD, связанный с конкретным компонентом имени, не заполнен – то этот компонент имени пользователя ЦР не будет заполнен;

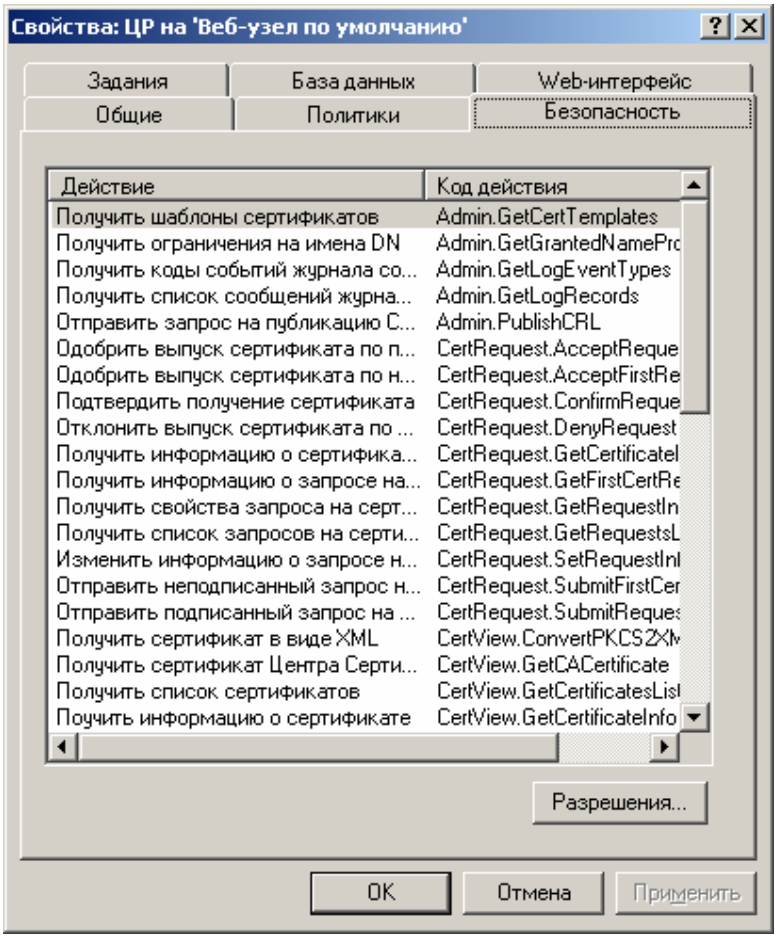
2) если атрибут AD не связан с каким-либо компонентом имени, то информация из него не будет добавлена.

Разрешения к допустимым действиям Центра регистрации – это список действий, допустимых для выполнения на Центре регистрации.

На каждое действие из списка можно определить разрешения (права доступа) для соответствующей роли в системе.

Изменения разрешений осуществляется на вкладке **Безопасность** свойств узла Центра регистрации (см. Рисунок 3).

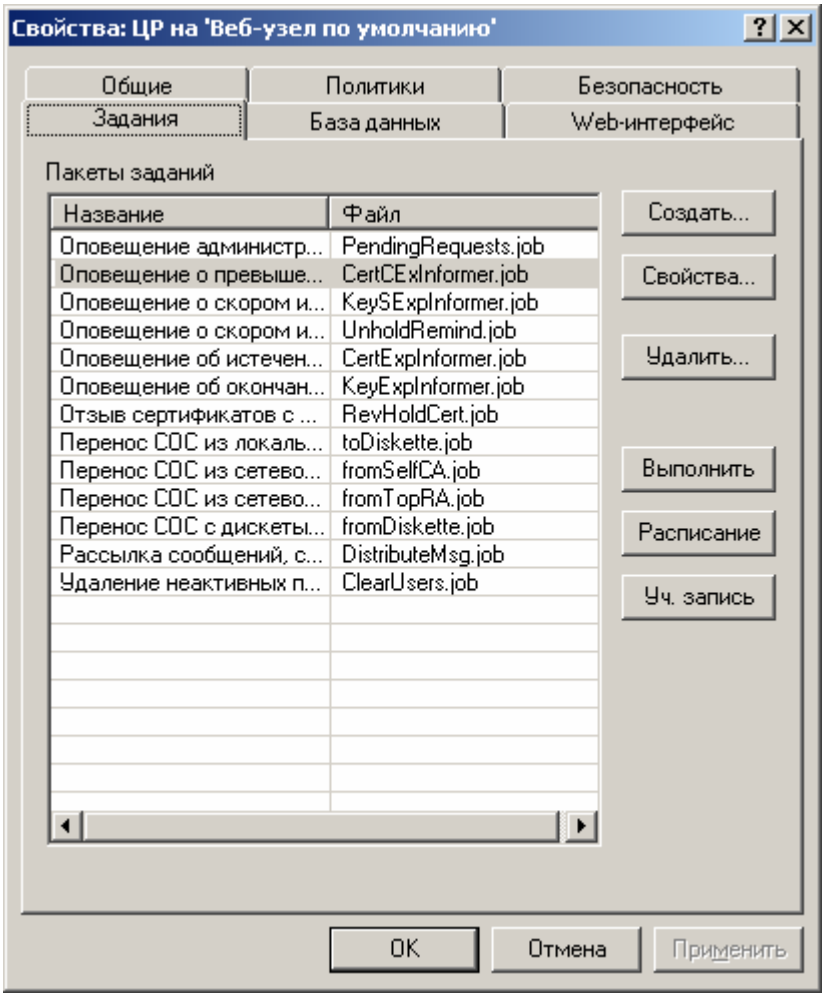
Рисунок 3. Вкладка "Безопасность" свойств узла Центра регистрации



Регламентные задания – это список задач, исполняемых на Центре Регистрации в автоматическом режиме.

Управление регламентными заданиями осуществляется на вкладке **Задания** свойств узла Центра регистрации (см. Рисунок 4).

Рисунок 4. Вкладка "Задания" свойств узла Центра регистрации

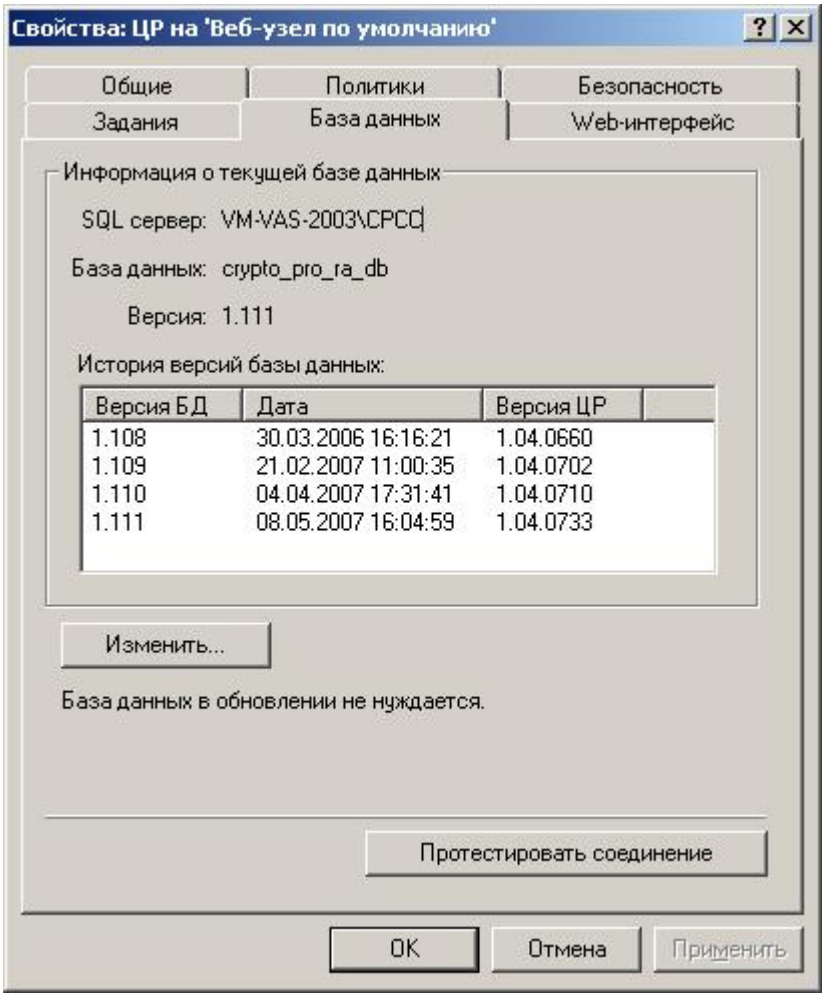


Используемая база данных Центра Регистрации – параметры, определяющие местоположение и параметры доступа к базе данных Центра Регистрации, размещаемой на SQL 2000 (2005) Server.

Настройка параметров осуществляется на вкладке **База данных** свойств узла Центра регистрации (см. Рисунок 5).

Как правило, дополнительной корректировки после установки ПО Центра Регистрации данные параметры не требуют.

Рисунок 5. Вкладка "База данных" свойств узла Центра Регистрации



В случае подключения базы данных Центра Регистрации, созданной предыдущей версией ПО Центра регистрации может потребоваться обновление базы данных. Как правило, обновление происходит автоматически при подключении базы данных. Не рекомендуется прерывать начавшийся процесс обновления, поскольку это приведёт к неработоспособности базы данных ЦР.

Автоматически могут быть обновлены базы данных, созданные при помощи ПО Центра Регистрации следующих версий:

- 1.02.0212 (отображаемая версия БД – 1.80)

- 1.03.0429 (отображаемая версия БД – 1.90)

- 1.04.nnnn, т.е. все сборки версии 1.4.

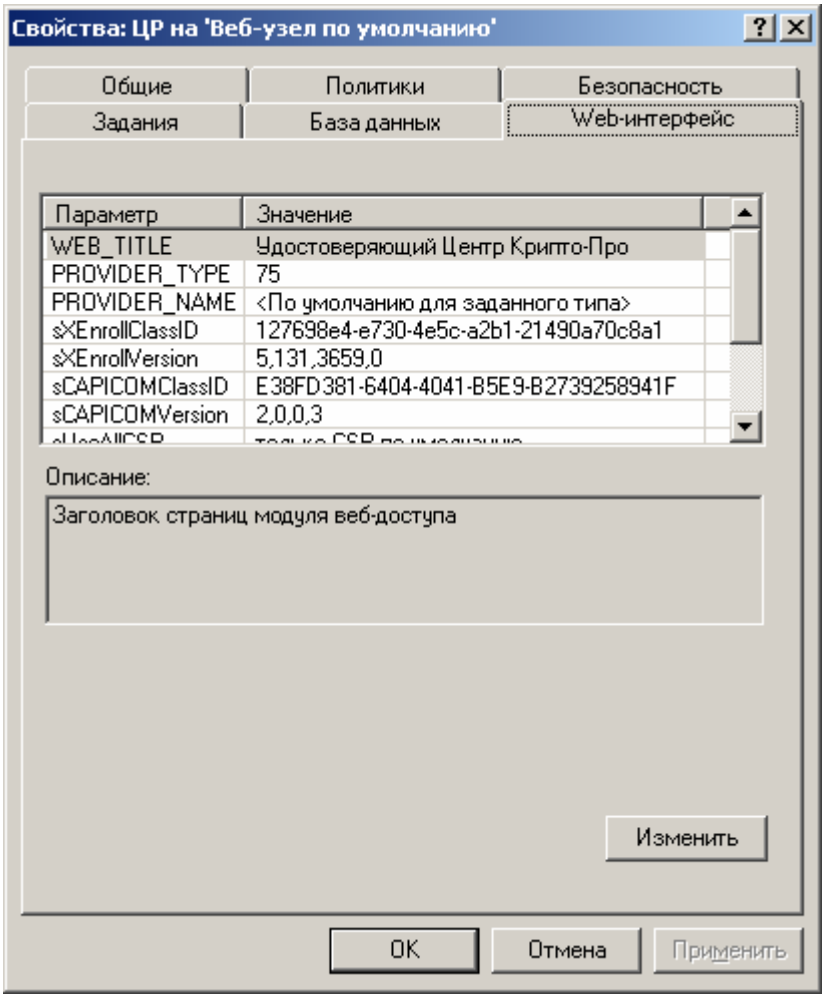
Параметры приложения пользователя – это параметры, определяющие функциональность веб-приложений, реализующих АРМы зарегистрированного пользователя.

К данным параметрам относятся:

- WEB_TITLE – параметр, определяющий название УЦ в заголовке страниц пользователя. Значение по умолчанию: "Удостоверяющий Центр Крипто-Про"
- PROVIDER_TYPE - идентификатор типа CSP. Значение по умолчанию: 75 (см. Microsoft Platform SDK, Crypto-API)
- PROVIDER_NAME - Имя CSP. Значение по умолчанию не присвоено (т.е. будет выбрано имя CSP, заданное по умолчанию для выбранного типа на компьютере пользователя)
- SXEnrollClassID - Идентификатор класса (ClassID) объекта Xenroll. Значение по умолчанию: "127698e4-e730-4e5c-a2b1-21490a70c8a1"
- SXEnrollVersion - Версия объекта Xenroll. Значение по умолчанию: "5,131,3659,0"
- SCAPICOMClassID - Идентификатор класса (ClassID) объекта CAPICOM. Значение по умолчанию: "E38FD381-6404-4041-B5E9-B2739258941F"
- sCAPICOMVersion - Версия (например, 2,1,0,1) объекта CAPICOM. Значение по умолчанию: "2,1,0,1"
- sUseAllCSP - При генерации ключей использовать только КриптоПро CSP или позволить пользователю выбирать любой CSP. Возможные значения: "" - только КриптоПро CSP, "1" - позволить выбирать CSP. Значение по умолчанию: "".
- UseFindCertMode - Поиск сертификатов в базе данных Центра Регистрации (для зарегистрированных пользователей ЦР). Возможные значения: 0 – отключен, 1 – доступен. Значение по умолчанию: 0.
- UseFindCertModeReg - Поиск сертификатов в базе данных Центра Регистрации (для пользователей с маркером временного доступа). Возможные значения: 0 – отключен, 1 – доступен. Значение по умолчанию: 0.
- RegReqAutoAccept - Автоматическое принятие запросов на регистрацию, поступающих от веб-приложения, реализующего АРМ регистрации пользователей. Возможные значения: 0 – отключено, 1 – включено. Значение по умолчанию: 0.
- CertReqAutoAccept - Автоматическое принятие запросов на сертификат, поступающих от веб-приложения, реализующего АРМ зарегистрированного пользователя с маркерным доступом. Возможные значения: 0 – отключено, 1 – включено. Значение по умолчанию: 0.
- WebCertReqAutoAccept - Автоматическое принятие заявлений на сертификат, поступающих от веб-приложения, реализующего АРМ зарегистрированного пользователя с ключевым доступом. Возможные значения: 0 – отключено, 1 – включено. Значение по умолчанию: 0.
- WebRevReqAutoAccept - Автоматическое принятие запросов на аннулирование и приостановление/возобновление действия сертификата, поступающих от веб-приложения, реализующего АРМ зарегистрированного пользователя с ключевым доступом. Возможные значения: 0 – отключено, 1 – включено. Значение по умолчанию: 0.

Установка параметров приложения осуществляется на вкладке **Web-интерфейс** окна свойств Центра Регистрации (см. Рисунок 6), путем выбора параметра и нажатия кнопки **Изменить**.

Рисунок 6. Вкладка "Web-интерфейс" свойств узла Центра Регистрации



Рекомендуем не изменять самостоятельно параметр PROVIDER_TYPE. Значение данного параметра автоматически изменяется на соответствующий тип при изменении параметра PROVIDER_NAME.

Если значение параметра **UseFindCertMode** равно 1 (единице), то режим поиска и импорта сертификатов открытых ключей будет доступен зарегистрированным пользователям, и в меню АРМ зарегистрированного пользователя появится соответствующий пункт **Поиск сертификатов**.

Если значение параметра **UseFindCertMode** равно любому другому значению, то возможности предоставления данного режима не будет. При этом доступ ко всем Web-страницам АРМ зарегистрированного пользователя, связанным с предоставлением возможности поиска и импорта сертификатов открытых ключей, будет блокирован, даже если производится попытка обращения к ним напрямую, не через соответствующий пункт меню АРМ.

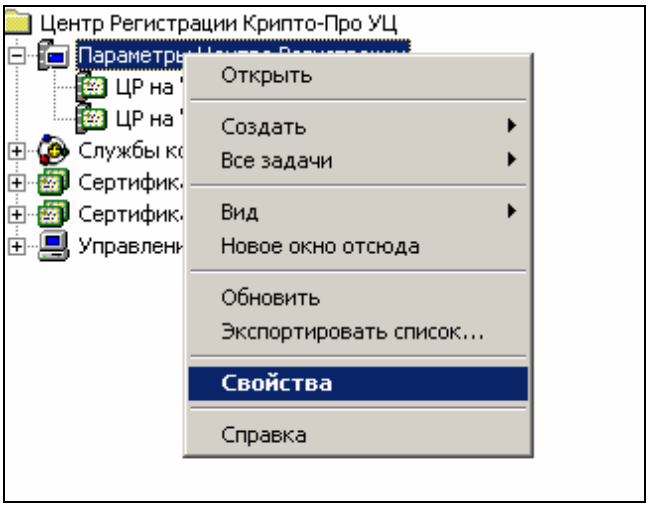
Если значение параметра **UseFindCertModeReg** равно 1 (единице), то режим поиска и импорта сертификатов открытых ключей будет доступен пользователям с маркером временного доступа, и в меню АРМ пользователя с маркером временного доступа появится соответствующий пункт **Поиск сертификатов**.

Если значение параметра **UseFindCertModeReg** равно любому другому значению, то возможности предоставления данного режима не будет. При этом доступ ко всем Web-страницам АРМ пользователя с маркером временного доступа, связанным с предоставлением возможности поиска и импорта сертификатов открытых ключей, будет блокирован, даже если производится попытка обращения к ним напрямую, не через соответствующий пункт меню АРМ.

2.2.1. Настройка параметров компонент УЦ, рассылающих почтовые сообщения

Настройка параметров компонент УЦ, рассылающих почтовые сообщения Центра регистрации, осуществляется в свойствах узла **Параметры Центра Регистрации** приложения **Параметры Центра Регистрации** (см. Рисунок 7).

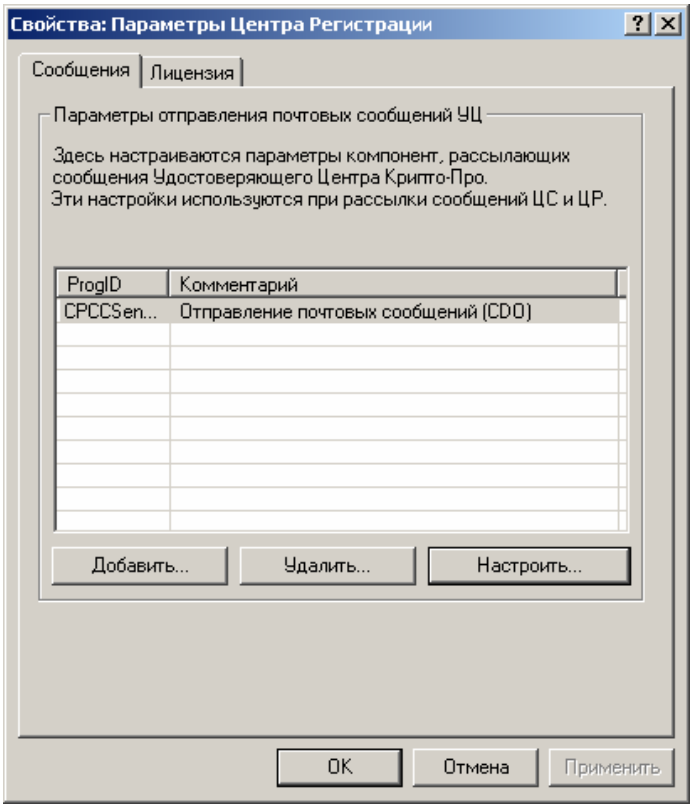
Рисунок 7. Пункт "Свойства" Параметры Центра Регистрации



При установке программного обеспечения Центра Регистрации устанавливается программная компонента отправки почтовых сообщений (CDO) (см. Рисунок 8).

Настройка параметров компоненты CDO осуществляется путем выбора компонент из списка и нажатия кнопки **Настроить**.

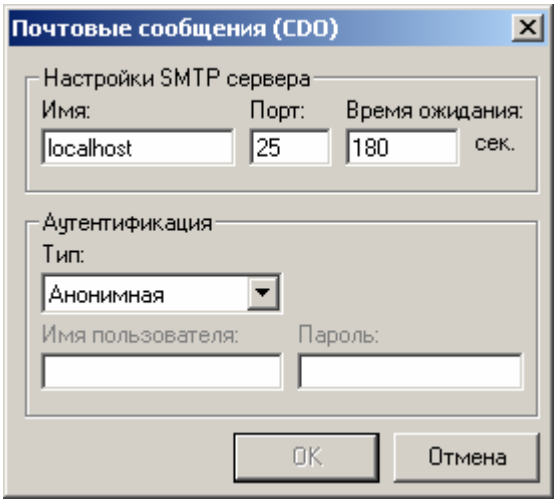
Рисунок 8. Окно компонент рассылки сообщений



К числу параметров настройки относятся:

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

Рисунок 9. Окно настройки параметров компоненты CDO



3. Установка и конфигурация нескольких Центров Регистрации на одном выделенном сервере

Программное обеспечение Центра Регистрации обеспечивает установку и эксплуатацию нескольких Центров Регистрации на одном выделенном сервере (локальном компьютере).

Установка второго и последующих ЦР производится аналогично установке первого (основного) Центра Регистрации на компьютере, выполняемой в соответствии с разделом 3 настоящего Руководства.

Дальнейшие действия по установке следующего Центра Регистрации выполняются в следующей последовательности:

1. Создание виртуального Web-узла Web-сервера MS IIS Центра Регистрации
2. Выпуск и инсталляция сертификата серверной аутентификации Web-сервера ЦР
3. Создание базы данных ЦР
4. Установка модуля доступа ЦР
5. Настройка ПО Центра Регистрации

Конфигурация программного обеспечения нового ЦР осуществляется в соответствии с разделом 4 настоящего Руководства.

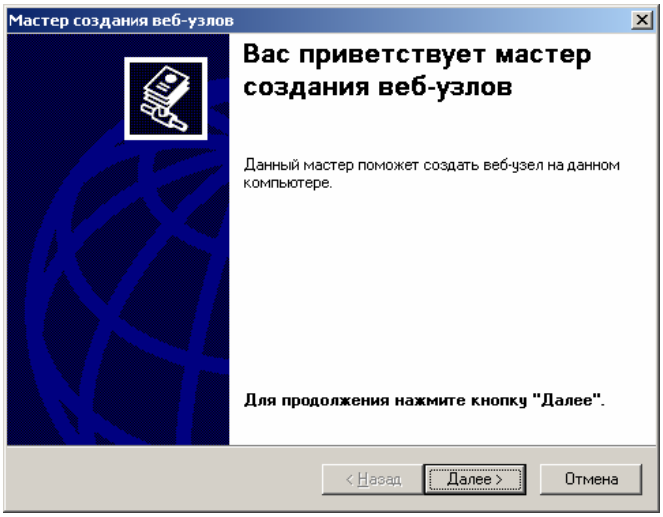
3.1. Создание виртуального Web-узла Web-сервера MS IIS Центра Регистрации

Создание виртуального Web-узла Web-сервера MS IIS осуществляется с использованием приложения «Диспетчер служб Интернет».

Для этого выполните следующие действия:

1. Запустите приложение Диспетчер служб Интернет
2. Выполните задачу **Создать Узел-Web**
3. Далее следуйте инструкциям Мастера создания Web-узлов (см. Рисунок 10)

Рисунок 10. Окно Мастера создания Web-узлов



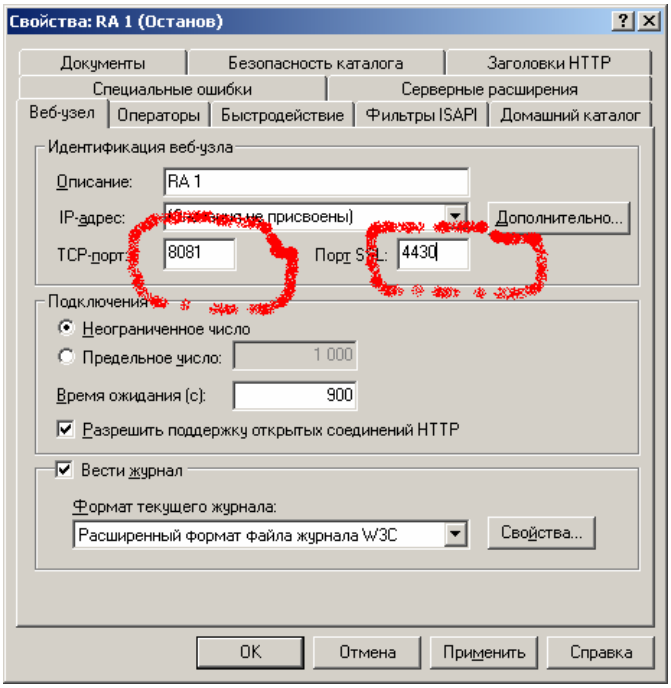
При размещении нескольких Центров Регистрации на одном компьютере необходимо заранее спланировать способ идентификации данного Web-узла. Поддерживается два способа идентификации:

- по IP-адресам;
- по портам.

При идентификации по портам необходимо:

1. Установить номер TCP-порта при создании Web-узла, отличный от номеров портов существующих Web-узлов;
2. После установки сертификата серверной аутентификации Web-узла Web-сервера Центра Регистрации, установить номер порта SSL, отличный от номеров портов SSL существующих Web-узлов.

Рисунок 11. Пример установки TCP-порта и порта SSL для Web-узла

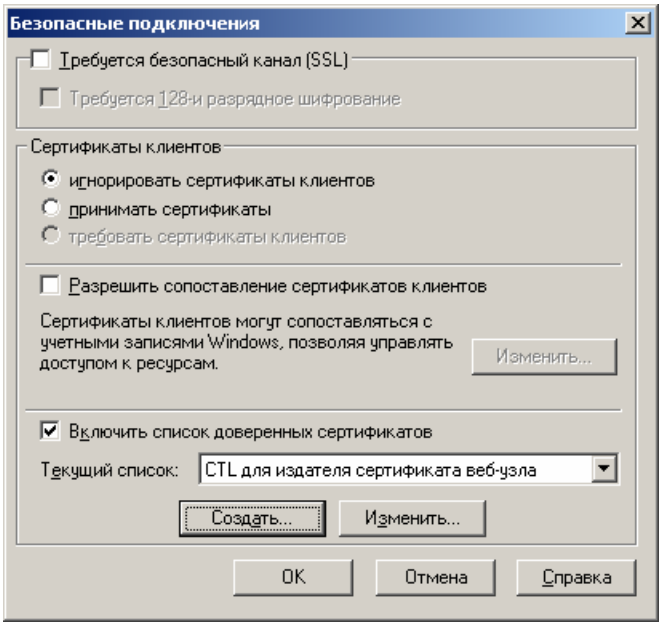


3.2. Выпуск и инсталляция сертификата серверной аутентификации Web-сервера ЦР

Выпуск и инсталляция сертификата серверной аутентификации Web-сервера ЦР осуществляется в соответствии с описанием, приведенном в разделе 3.2 настоящего Руководства.

При установке нескольких модулей доступа ЦР на одном компьютере с использованием сертификатов серверной аутентификации с разными алгоритмами (с разными криптопровайдерами), необходимо после инсталляции сертификата Web-сервера с алгоритмом, отличным от алгоритмов реализуемых СКЗИ КриптоПро CSP, создать и включить список доверенных сертификатов (CTL) для данного Web-узла. В этом списке должен содержаться сертификат Центра Сертификации, издавшего сертификат серверной аутентификации (см. Рисунок 12).

Рисунок 12. Окно свойств безопасных подключений Web-узла модуля доступа ЦР



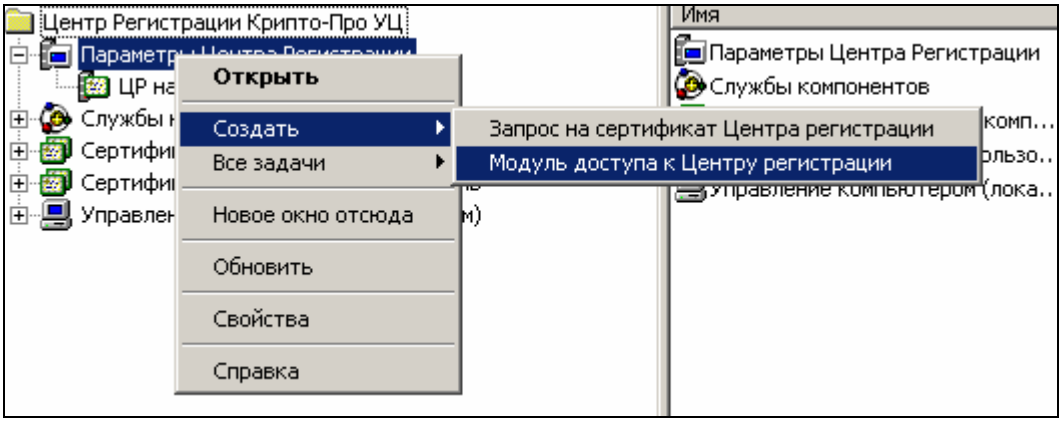
3.3. Установка модуля доступа ЦР

Установка нового модуля доступа к создаваемому Центру регистрации выполняется в приложении **Параметры Центра Регистрации** из группы **КриптоПро**.

Для этого выполните следующие действия:

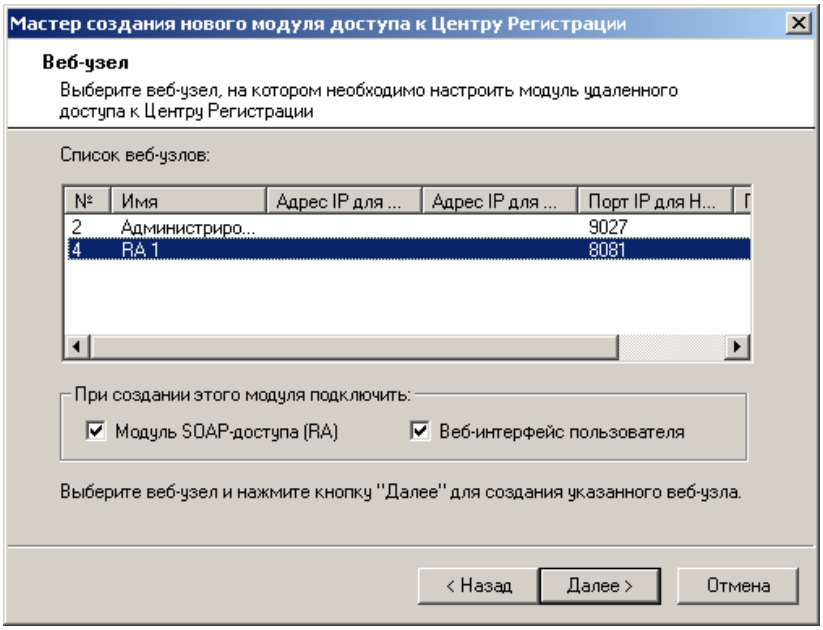
1. Запустите приложение **Параметры Центра Регистрации** из группы **КриптоПро**.
2. Установите курсор на раздел «Параметры Центра Регистрации» и нажмите правую кнопку мыши (см. Рисунок 13)

Рисунок 13. Запуск задачи создания модуля доступа ЦР



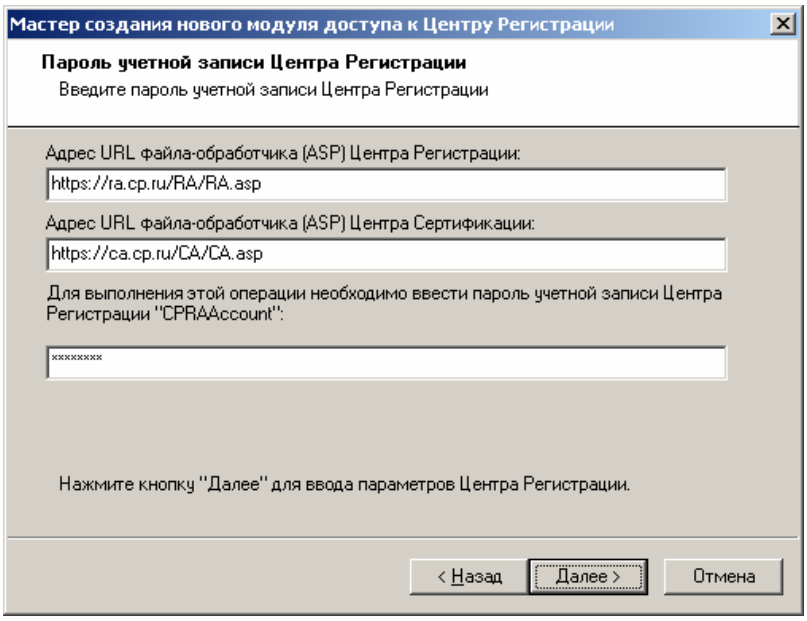
3. В Мастере создания нового модуля доступа к ЦР выберите Web-узел, созданный ранее (см. раздел 3.1)

Рисунок 14. Окно выбора Web-узла Мастера создания нового модуля доступа



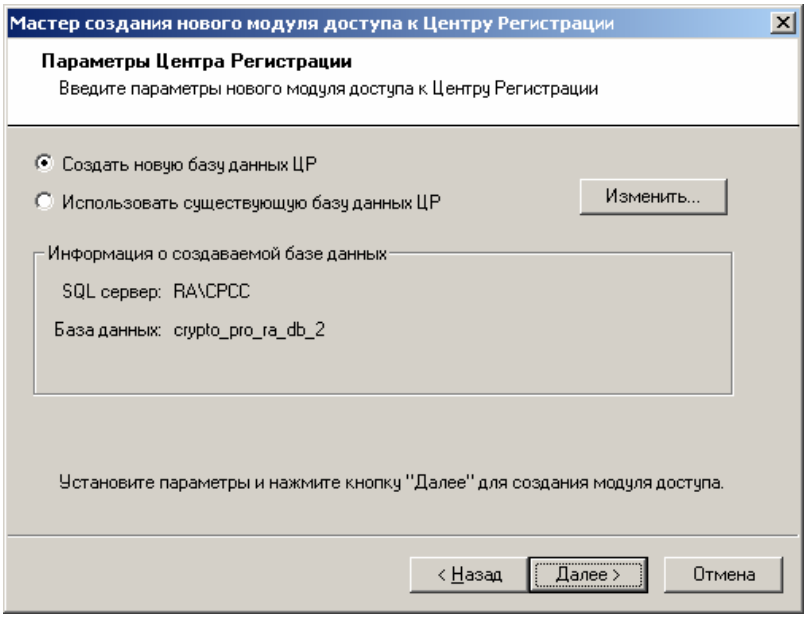
4. В окне ввода пароля учетной записи Центра Регистрации (см. Рисунок 15) необходимо ввести пароль, заданный во время установки программного обеспечения Центра Регистрации (см. страницу **44** документа **КриптоПро УЦ Руководство по установке**), а так же адреса URL файлов-обработчиков.

Рисунок 15. Окно ввода пароля учетной записи Центра Регистрации Мастера создания нового модуля доступа к ЦР



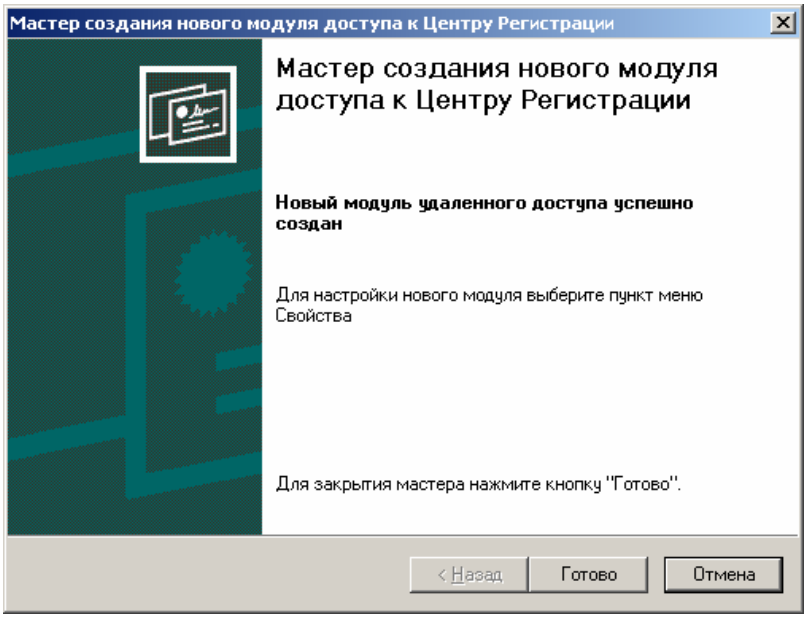
5. В следующем окне Мастера настройте базу данных Центра регистрации для нового модуля доступа (см. Рисунок 16). Есть возможность либо выбрать существующую базу данных ЦР, либо создать новую. Для настройки параметров базы данных воспользуйтесь описанием настройки **DataLink** из раздела 4.1.

Рисунок 16. Окно определения параметров в Мастере создания нового модуля доступа к ЦР



6. После нажатия кнопки **Далее** дождитесь завершения установки (см. Рисунок 17) и нажмите кнопку **Готово**.

Рисунок 17. Окно завершения работы Мастера создания нового модуля доступа к ЦР



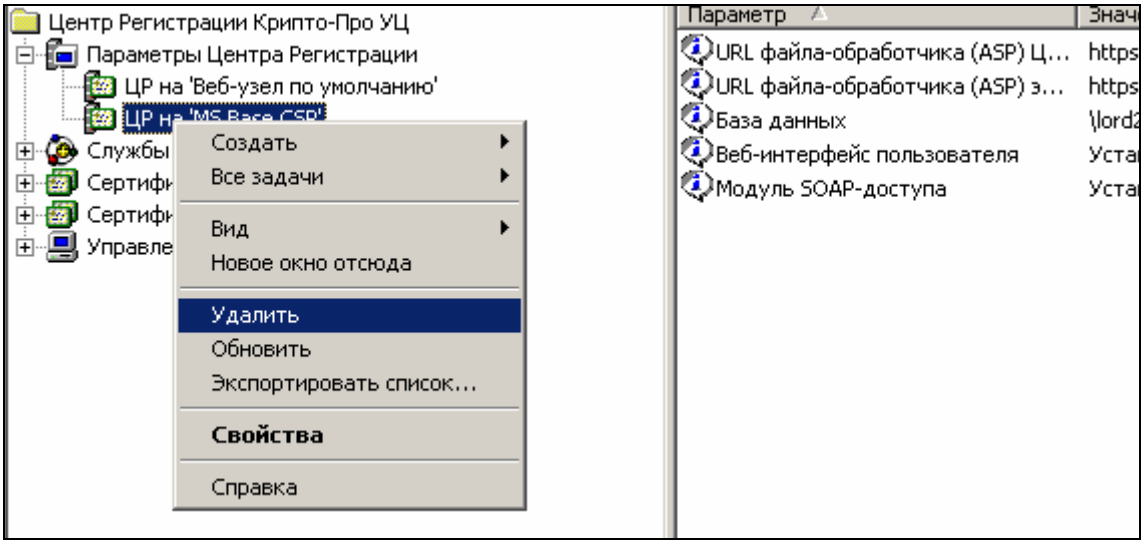
3.4. Настройка ПО Центра Регистрации

Настройка программного обеспечения созданного Центра Регистрации осуществляется в соответствии с описанием, приведенным в разделе 4 настоящего Руководства.

3.5. Удаление модуля доступа ЦР

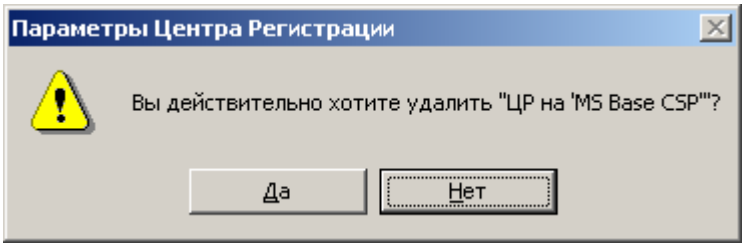
Удаление ранее созданного модуля доступа ЦР осуществляется путем выполнения задачи **Удалить** для выбранного модуля доступа из контекстного меню приложения **Параметры Центра Регистрации** (см. Рисунок 18).

Рисунок 18. Запуск задачи удаления модуля доступа Центра Регистрации



В следующем окне подтвердите выполнение операции удаления выбранного модуля доступа (см. Рисунок 19).

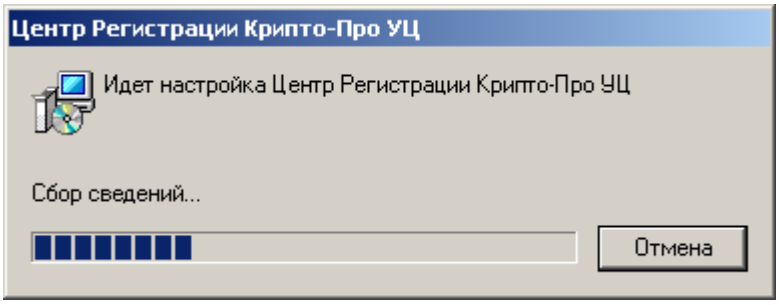
Рисунок 19. Окно подтверждения удаления модуля доступа ЦР



После подтверждения запускается программа Мастера установки Центра Регистрации Крипто-Про УЦ, которая выполнит удаление выбранного модуля доступа.

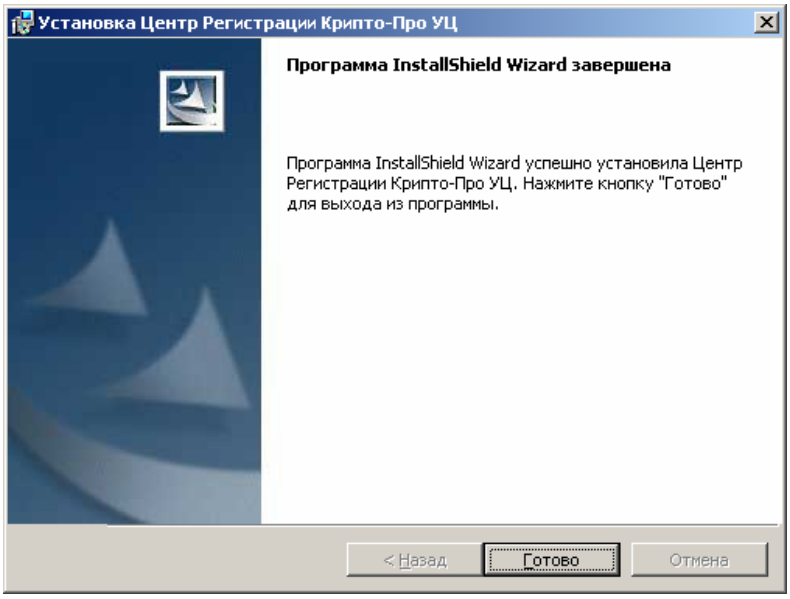
В процессе удаления отображается состояние работы (см. Рисунок 20).

Рисунок 20. Окно программы установки Центра Регистрации Крипто-Про УЦ при удалении модуля доступа



По завершении операции удаления отображается окно окончания работы Мастера (см. Рисунок 21).

Рисунок 21. Окно Мастера установки Центра Регистрации Крипто-Про УЦ при завершении удаления модуля доступа



4. Настройка и изменение параметров программного обеспечения Центра Регистрации

Настройка параметров Центра регистрации (конфигурация) осуществляется при вводе его в эксплуатацию. Настройка выполняется для обеспечения работы программного обеспечения в соответствии с регламентом Удостоверяющего Центра предприятия.

Изменение параметров Центра регистрации (реконфигурация) осуществляется в случае изменений регламента Удостоверяющего Центра, связанных с параметрами работы Центра регистрации. Изменение параметров настройки Центров регистрации осуществляется также при изменении схемы размещения программных компонентов Центра регистрации. Например, для оптимизации производительности Центра регистрации осуществляется переход со схемы 1 на схему 2 (см. раздел 1.3).

Изменение параметров настройки осуществляется в свойствах узла **Центр Регистрации** приложения **Параметры Центра Регистрации** (см. Рисунок 2). Перечень параметров настройки см. в разделе 2.

4.1. Смена размещения базы данных Центра регистрации

Смена параметров, определяющих место размещения базы данных, осуществляется на вкладке **База данных** свойств узла Центра регистрации.

Для смены строки нажмите кнопку **Изменить**. Откроется окно диалога "Изменение текущей базы данных". Используя его, можно либо выбрать существующую базу данных ЦР, либо создать новую. Для задания параметров базы данных нажмите кнопку **Выбрать** (**Настроить**). Появится окно определения свойств компонента **Связь с данными**.

Рисунок 22. Окно свойств компонента Связь с данными

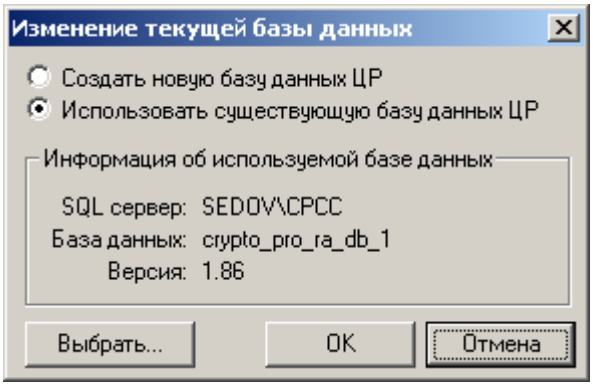
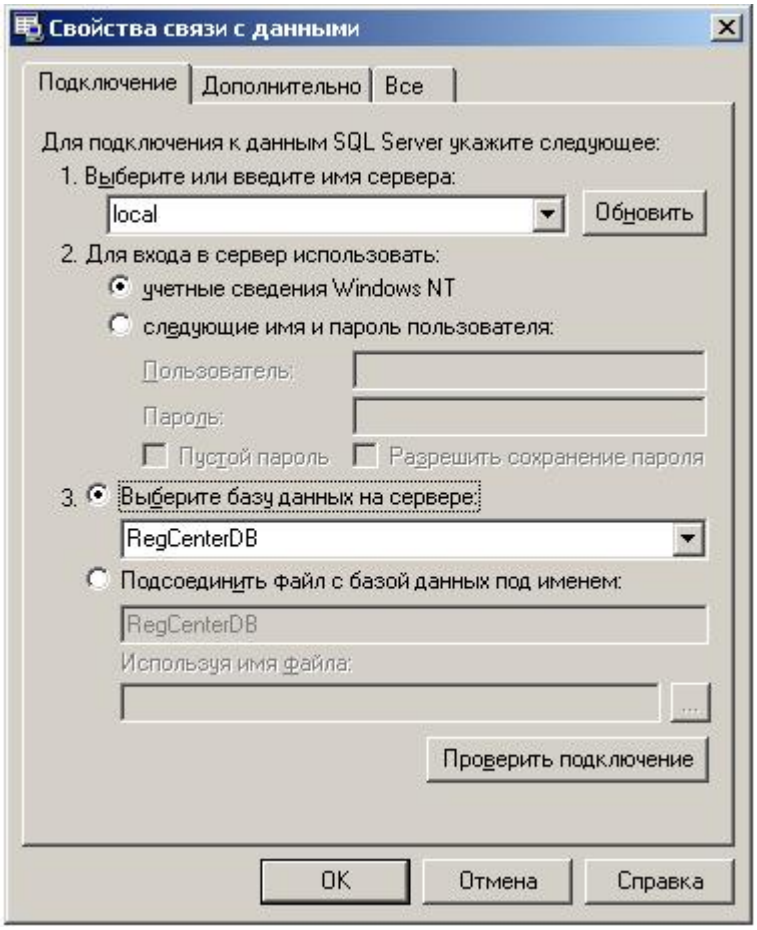


Рисунок 23. Окно свойств компонента Связь с данными



В этом окне выберите место размещения сервера SQL (пункт 1) и наименование базы данных, созданной/создаваемой на выбранном сервере (пункт 3).

После изменения параметров соединения нажмите кнопку **ОК**.

Перед изменением параметра, определяющего место размещения базы данных, необходимо осуществить перенос базы данных Центра регистрации в соответствии с руководством Администратора баз данных Удостоверяющего Центра.

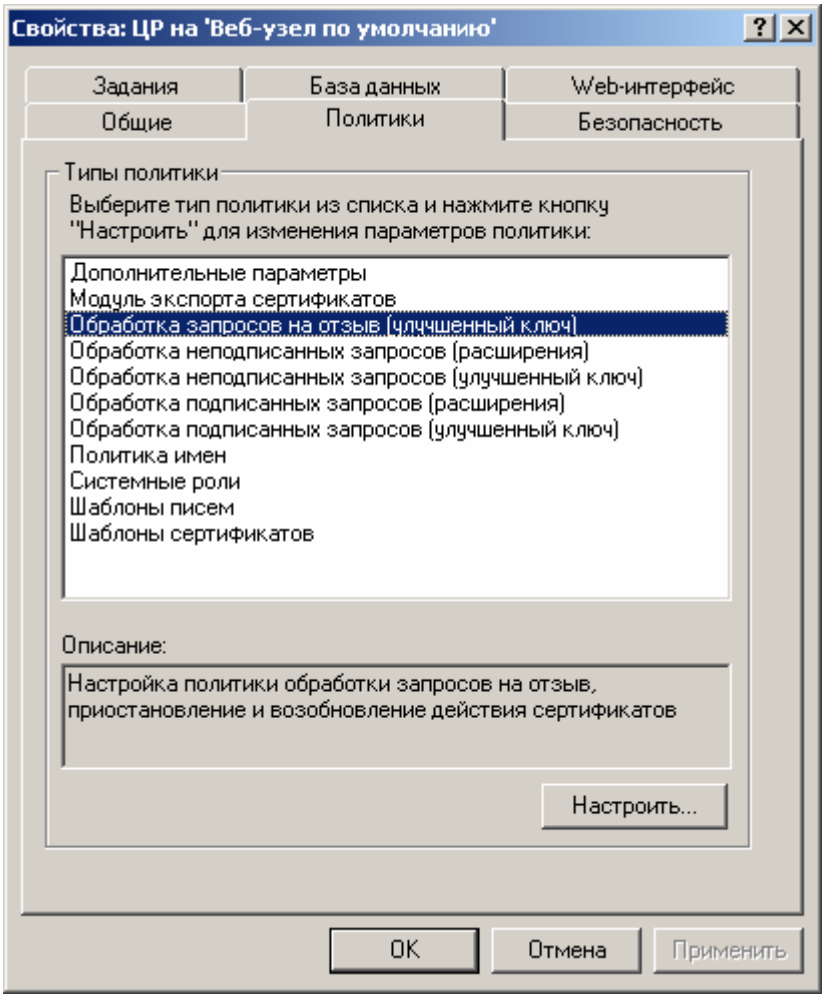
4.2. Политики обработки запросов

Политики обработки запросов включают в себя набор следующих типов политик:

- Обработка запросов на отзыв (улучшенный ключ);
- Обработка неподписанных запросов (расширения);
- Обработка неподписанных запросов (улучшенный ключ);
- Обработка подписанных запросов (расширения);
- Обработка подписанных запросов (улучшенный ключ).

Управление политиками обработки запросов осуществляется на вкладке **Политики** окна свойств модуля доступа Центра Регистрации в приложении **Параметры Центра Регистрации** (см. Рисунок 24).

Рисунок 24. Вкладка "Политики" свойств узла Центра Регистрации



Политика **Обработка запросов на отзыв (улучшенный ключ)** определяет разрешения для ролей Центра Регистрации при помещении запроса на отзыв сертификата (аннулирование, приостановление и возобновление действия) в очередь поступивших запросов на отзыв сертификатов Центра Регистрации.

Эта политика означает следующее:

- пользователь, помещающий запрос на отзыв сертификата в очередь поступивших запросов на отзыв сертификатов, ассоциирован с ролью Центра Регистрации;
- совокупность областей применения, содержащаяся в отзываемом сертификате, является подмножеством областей применения роли, с которой пользователь ассоциирован.

С помощью этой политики можно управлять правами привилегированных пользователей (администраторов и операторов) Центров Регистрации на отзыв сертификатов определенного вида.

Политики **Обработки неподписанных запросов** и политики **Обработки подписанных запросов** являются политиками обработки запросов на сертификат и определяют разрешения для ролей Центра Регистрации при помещении неподписанного запроса на сертификат (PKCS#10) или подписанного (PKCS#7 с PKCS#10 в данных для подписи) в очередь поступивших запросов на сертификат Центра Регистрации.

Неподписанные запросы на сертификат порождаются администратором/оператором при выполнении задач регистрации пользователей или при выпуске зарегистрированным пользователям нового сертификата с использованием АРМ администратора ЦР. Также неподписанные запросы порождаются прошедшим проверку пользователем в процессе прохождения регистрации в распределенном режиме с выпуском первого сертификата

открытого ключа пользователя (через АРМ зарегистрированного пользователя с маркерным доступом).

Подписанные запросы порождаются при выполнении задачи плановой смены ключей и сертификатов администраторов/операторов с использованием АРМ администратора ЦР и при выполнении задачи запроса на новый сертификат в АРМе зарегистрированного пользователя с ключевым доступом.

Политики обработки запросов на сертификат делятся на две группы по типу применения:

- **улучшенный ключ** - применяющиеся к информации в областях применения в расширении Extended Key Usages (EKU) запроса. Название пошло от перевода корпорацией Microsoft данного расширения EKU;
- **расширения** – применяющиеся к информации

Политики обработки запросов на сертификат означают следующее:

- пользователь, помещающий запрос на сертификат в очередь поступивших запросов на сертификаты, ассоциирован с ролью Центра Регистрации;
- совокупность областей применения, содержащаяся в запросе на сертификат (в PKCS#10), является подмножеством областей применения роли, с которой пользователь ассоциирован.

Если последнее условие истинно, то запрос на сертификат будет помещен в очередь **Поступившие** на Центре Регистрации. В противном случае, действие будет отвергнуто с диагностическим сообщением об ошибке «*Действие не может быть выполнено на данном сертификате*».

4.3. Пользователи Центра Регистрации

Все пользователи Центра Регистрации делятся на три типа:

- зарегистрированные пользователи;
- активные пользователи;
- пользователи, проходящие процедуру регистрации в распределенном режиме;

Зарегистрированным пользователем является физическое лицо, учетная информация о котором внесена в Базу Данных Центра Регистрации, но не имеющее ни одного действующего сертификата открытого ключа, выданного Удостоверяющим Центром и содержащего идентификаторы ролей в области применения сертификата.

Пользователи указанного типа появляются в Центре Регистрации в следующих случаях:

1. Когда регламентом Удостоверяющего Центра определена процедура централизованной регистрации сотрудником из группы администраторов УЦ пользователей (владельцев сертификатов открытых ключей) без выдачи пользователю ключей и сертификатов открытых ключей. Генерация ключей и выдача пользователю ключей и сертификатов открытых ключей, как правило, осуществляется другим сотрудником из группы администраторов УЦ.
2. Когда у пользователя, относящегося к типу **Активные пользователи**, истекли сроки действия и/или отозваны все его сертификаты открытого ключа.

Активным пользователем является физическое лицо, учетная информация о котором внесена в Базу Данных Центра Регистрации, и имеющее действующий сертификат (сертификаты) открытого ключа, содержащий (содержащие) идентификаторы ролей в области применения сертификата

Пользователь, проходящий процедуру регистрации в распределенном режиме, является физическим лицом, выполняющим регламентные действия по регистрации в Центре Регистрации со своего рабочего места.

В программном обеспечении Центра Регистрации реализована ролевая модель взаимодействия пользователей с Центром Регистрации в части выполнения на нем действий. Перечень действий приведен в Таблица 1.

Пользователи, относящиеся к типу **Зарегистрированные пользователи**, не имеют средств аутентификации (действующих сертификатов открытых ключей) и, следовательно, не могут выполнять никакие действия на Центре Регистрации с использованием программного обеспечения, предоставляемого Центром Регистрации. Для получения возможности использовать программное обеспечение, предоставляемое Центром Регистрации, пользователю необходимо стать владельцем действующего сертификата открытого ключа, способом, определяемым Регламентом УЦ.

Пользователи, относящиеся к типу **Пользователи, проходящие процедуру регистрации в распределенном режиме**, ассоциированы с набором определенных ролей из списка предустановленных. Эти роли пользователи данного типа получают, последовательно проходя стадии регистрации.

Пользователи, относящиеся к типу **Активные пользователи**, ассоциированы с любыми ролями из списка предустановленных ролей и могут быть ассоциированы с другими ролями, расширяющими список предустановленных ролей.

На Центре Регистрации имеются следующие предустановленные роли:

- **Администратор** – администратор Центра Регистрации,
- **Оператор** – оператор Центра Регистрации
- **Пользователь Центра Регистрации** – пользователь, имеющий действующий сертификат открытого ключа, содержащий идентификатор этой роли в области применения сертификата, и информация о котором внесена в Базу Данных Центра Регистрации
- **Временный сертификат** – владелец временного сертификата пользователя Центра Регистрации
- **Прошедший проверку** – прошедший проверку пользователь, имеющий маркер доступа

Пользователи, проходящие процедуру регистрации в распределенном режиме, получают роль **Прошедший проверку** - пользователь, успешно прошедший аутентификацию по паролю до момента получения первого сертификата открытого ключа;

Пользователи, относящиеся к типу **Активные пользователи**, в свою очередь делятся на два класса по типу регистрации их учетной информации в Базе Данных Центра Регистрации:

- обычные пользователи;
- привилегированные пользователи.

Привилегированные пользователи регистрируются в Базе Данных Центра Регистрации с помощью задачи **Создать Привилегированного пользователя** приложения **Параметры Центра Регистрации**.

Для привилегированных пользователей используются роли **Администратор** и **Оператор** из списка предустановленных ролей.

Рекомендуется использовать данные роли (и это определено предустановленными правами доступа к допустимым действиям Центра Регистрации) для обеспечения выполнения следующих организационно-технических мероприятий:

1. Администратор
   1.1. Генерация рабочих и служебных ключей пользователей
   1.2. Получение сертификата открытых ключей пользователей
   1.3. Отзыв сертификатов открытых ключей пользователей
   1.4. Опубликование списка отозванных сертификатов
   1.5. Обработка запросов на сертификаты открытых ключей пользователей

1.6. Обработка запросов на отзыв сертификатов открытых ключей пользователей
2. Оператор
   2.1. Регистрация пользователей в Базе Данных Центра Регистрации
   2.2. Обработка запросов на регистрацию пользователей

Обычные пользователи регистрируются пользователями из класса привилегированных пользователей.

Аутентификация и авторизация пользователей, относящихся к типу **Активный пользователь**, осуществляется по ролям, определенным в сертификате открытого ключа (по области применения), предъявленного для аутентификации.

Сертификат открытого ключа пользователя может содержать идентификаторы одной или нескольких ролей, в том числе и роль **Владелец временного сертификата**.

Права доступа к информационным ресурсам Центра Регистрации для каждой роли определяются настройками разрешений к действиям Центра Регистрации (см. раздел 4.4).

4.4. Настройка разрешений к допустимым действиям Центра регистрации

Допустимые действия Центра Регистрации, к которым может быть осуществлена настройка прав доступа, приведены в следующей таблице.

Таблица 1. Таблица допустимых действий Центра Регистрации

№	Наименование объекта	Наименование действия ЦР
1	Admin.GetCertTemplates	Получить шаблоны сертификатов
2	Admin.GetGrantedNameProperties	Получить ограничения на имена DN
3	Admin.GetLogEventTypes	Получить коды событий журнала событий
4	Admin.GetLogRecords	Получить список сообщений журнала событий
5	Admin.PublishCRL	Отправить запрос на публикацию СОС
6	CertRequest.AcceptRequest	Одобрить выпуск сертификата по подписанному запросу на сертификат
7	CertRequest.AcceptFirstRequest	Одобрить выпуск сертификата по неподписанному запросу на сертификат
8	CertRequest.ConfirmRequest	Подтвердить получение сертификата
9	CertRequest.DenyRequest	Отклонить выпуск сертификата по запросу
10	CertRequest.GetCertificateInfo	Получить информацию о сертификате по коду запроса на сертификат
11	CertRequest.GetFirstCertRequestInfo	Получить информацию о запросе на сертификат по коду запроса на регистрацию
12	CertRequest.GetRequestInfo	Получить свойства запроса на сертификат
13	CertRequest.GetRequestsList	Получить список запросов на сертификат
14	CertRequest.SetRequestInfo	Изменить информацию о запросе на сертификат
15	CertRequest.SubmitFirstCertRequest	Отправить неподписанный запрос на сертификат

16	CertRequest.SubmitRequest	Отправить подписанный запрос на сертификат
17	CertView.ConvertPKCS2XML	Получить сертификат в виде XML
18	CertView.GetCACertificate	Получить сертификат Центра Сертификации
19	CertView.GetCertificatesList	Получить список сертификатов
20	CertView.GetCertificateInfo	Получить информацию о сертификате
21	CertView.GetCRL	Получить список отозванных сертификатов (СОС)
22	Registration.AcceptRequest	Одобрить создание пользователя по запросу на регистрацию
23	Registration.CreateCertRequest	Извлечь запрос на сертификат из запроса на регистрацию
24	Registration.CreateRequest	Отправить запрос на регистрацию пользователя самим пользователем
25	Registration.CreateRequestByAdmin	Отправить запрос на регистрацию пользователя администратором
26	Registration.DenyRequest	Отклонить запрос на регистрацию
27	Registration.GetRequestInfo	Получить информацию о запросе на регистрацию
28	Registration.GetRequestsList	Получить список запросов на регистрацию
29	Registration.SetRequestInfo	Изменить информацию о запросе на регистрацию
30	RevokeRequest.AcceptRequest	Одобрить запрос на отзыв сертификата
31	RevokeRequest.DenyRequest	Отклонить запрос на отзыв сертификата
32	RevokeRequest.GetRequestInfo	Получить информацию о запросе на отзыв сертификата
33	RevokeRequest.GetRequestsList	Получить список запросов на отзыв сертификата
34	RevokeRequest.SetRequestInfo	Изменить информацию о запросе на отзыв сертификата
35	RevokeRequest.SubmitRequest	Отправить запрос на отзыв сертификата
36	RevokeRequest.SubmitHoldRequest	Отправить запрос на приостановление действия сертификата
37	RevokeRequest.SubmitUnHoldRequest	Отправить запрос на возобновление действия сертификата
38	UserView.AddDocument	Добавить документ пользователя
39	UserView.GetDocumentInfo	Получить информацию о документе пользователя
40	UserView.GetDocumentsList	Получить список документов пользователя
41	UserView.GetUserByCertificate	Найти идентификатор пользователя по сертификату
42	UserView.GetUserInfo	Получить информацию о пользователе

43	UserView.GetUsersList	Получить список пользователей
44	UserView.RemoveDocument	Удалить документ пользователя
45	UserView.SetUserInfo	Изменить информацию о пользователе
46	UserView.DeleteUser	Удалить пользователя
47	Admin.CreateTokenForUser	Создать маркер временного доступа

На допустимые действия Центра Регистрация могут быть назначены права доступа.

Права доступа различаются на два типа:

- выполнение;
- делегация.

Выполнение – это тип действия, определяющий, что пользователь с соответствующей ролью в системе может или не может выполнить действие Центра регистрации, для которого определяется элемент разрешений.

Делегация – это тип действия, определяющий, что пользователь с соответствующей ролью в системе может или не может не только выполнить действие Центра регистрации, для которого определяется элемент разрешений, но и выполнить его от имени другого пользователя системы. Например, таким образом определяются права администратора от имени пользователя сформировать и поставить в очередь на обработку запрос на сертификат открытого ключа.

Соответственно, тип действия Центра Регистрации может находиться в двух состояниях:

- разрешено;
- запрещено.

Для каждой предустановленной роли имеются стандартные (предустановленные) права доступа к действиям, обеспечивающие типовой режим работы программного обеспечения Центра Регистрации (конфигурация по лицензии на стандартную версию).

Таблица 2. Таблица прав доступа для роли Администратор

Номер действия по таблице допустимых действий (Таблица 1)	**Выполнение**	**Делегация**
1	**X**	
2	**X**	
3	**X**	
4	**X**	
5	**X**	
6	**X**	**X**
7	**X**	**X**
8	**X**	**X**
9	**X**	**X**
10	**X**	**X**
11	**X**	**X**
12	**X**	**X**
13	**X**	**X**
14	**X**	**X**

15	**X**	**X**
16	**X**	**X**
17	**X**	
18	**X**	
19	**X**	**X**
20	**X**	**X**
21	**X**	
22		
23		
24		
25		
26		
27	**X**	**X**
28	**X**	
29		
30	**X**	**X**
31	**X**	**X**
32	**X**	**X**
33	**X**	**X**
34	**X**	**X**
35	**X**	**X**
36	**X**	**X**
37	**X**	**X**
38	**X**	**X**
39	**X**	
40	**X**	
41	**X**	**X**
42	**X**	**X**
43	**X**	
44	**X**	
45	**X**	
46	**X**	
47	**X**	

Таблица 3. Таблица прав доступа для роли Оператор

Номер действия по таблице допустимых действий (Таблица 1)	**Выполнение**	**Делегация**
1	**X**	

2	**X**	
3	**X**	
4	**X**	
5		
6	**X**	
7	**X**	**X**
8	**X**	**X**
9		
10	**X**	**X**
11	**X**	**X**
12	**X**	**X**
13	**X**	**X**
14	**X**	**X**
15	**X**	**X**
16	**X**	
17	**X**	
18	**X**	
19	**X**	**X**
20	**X**	**X**
21	**X**	
22	**X**	**X**
23	**X**	**X**
25	**X**	
26	**X**	**X**
27	**X**	**X**
28	**X**	
29	**X**	**X**
30		
31		
32	**X**	**X**
33	**X**	**X**
34		
35	**X**	**X**
36	**X**	**X**
37	**X**	**X**
38	**X**	**X**
39	**X**	
40	**X**	
41	**X**	**X**

42	**X**	**X**
43	**X**	
44	**X**	
45	**X**	**X**
46		
47		

Таблица 4. Таблица прав доступа для роли Пользователь Центра Регистрации

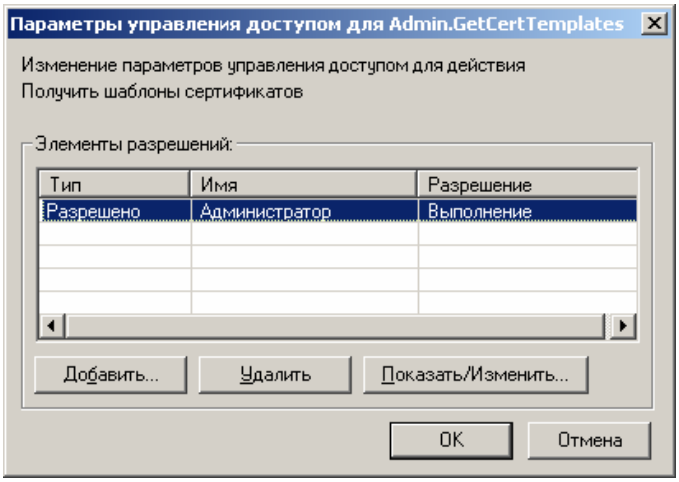
Номер действия по таблице допустимых действий (Таблица 1)	**Выполнение**	**Делегация**
1	**X**	
2	**X**	
6	**X**	
8	**X**	
10	**X**	
13	**X**	
16	**X**	
17	**X**	
18	**X**	
19	**X**	
20	**X**	
21	**X**	
33	**X**	
34	**X**	
35	**X**	
37	**X**	
41	**X**	
42	**X**	

В процессе эксплуатации Центра Регистрации возможно изменение настроек разрешений с целью построения режимов работы Центра Регистрации в соответствии с корпоративными регламентами.

Настройка разрешений (прав) осуществляется на вкладке **Безопасность** свойств узла Центра регистрации (см. Рисунок 3).

Для каждого действия, которое может быть выполнено на Центре регистрации (через интерфейс внешних приложений, АРМ администратора, АРМ пользователя и т.д.) определяется список элементов разрешений (см. Рисунок 25).

Рисунок 25. Окно элемента разрешений для действия Центра регистрации



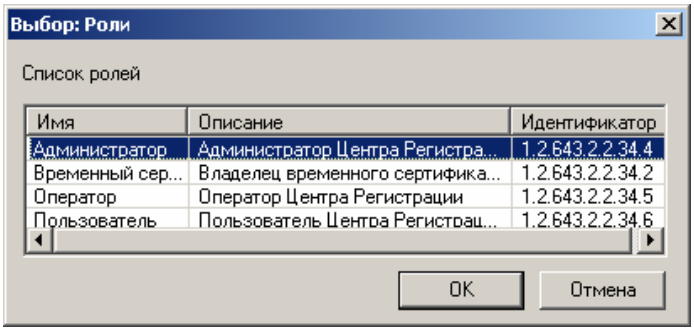
Каждый элемент разрешений определяет права и тип права для одной из ролей доступа к действию Центра регистрации.

В список элементов можно добавить элемент путем нажатия кнопки **Добавить**, удалить элемент нажатием кнопки **Удалить**, или изменить ранее созданный элемент путем нажатия кнопки **Показать/Изменить**.

Добавление элемента разрешений в список

При нажатии кнопки **Добавить** отображается диалоговое окно, в котором необходимо выбрать из списка роль доступа, для которой будет создан новый элемент разрешений (см. Рисунок 26).

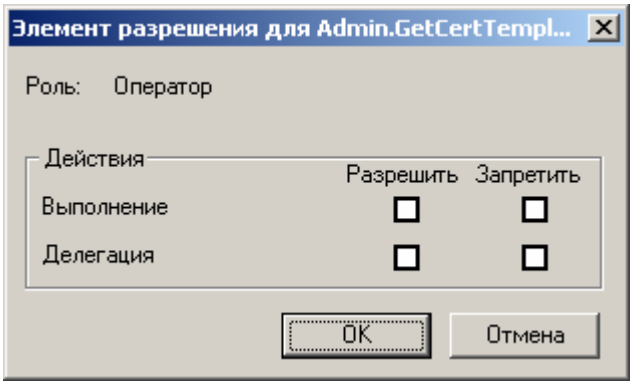
Рисунок 26. Окно выбора роли при создании элемента разрешений



После выбора роли из списка ролей, отображается окно определения свойств создаваемого элемента разрешений (см. Рисунок 27). В этом окне необходимо определить права доступа (разрешить/запретить) для двух типов действий:

- Выполнение
- Делегация

Рисунок 27. Окно свойств элемента разрешений



Изменение элемента разрешений в списке

При нажатии кнопки **Показать/Изменить** отображается диалоговое окно определения свойств элемента разрешений (см. Рисунок 2727). В этом окне можно переопределить права доступа (разрешить/запретить) для типов действий.

4.5. Настройка регламентных Заданий

Регламентные Задания – это совокупность заданий, исполняемых на Центре Регистрации в автоматическом режиме согласно установленному им расписанию.

При установке ПО Центра Регистрации устанавливаются следующие задания:

1. Оповещение о превышении количества запросов на сертификат
2. Оповещение об истечении срока действия сертификата открытого ключа
3. Удаление неактивных пользователей
4. Отправка сообщений, стоящих в очереди
5. Оповещение о скором истечении срока действия секретного ключа
6. Оповещение об окончании действия секретного ключа
7. Отзыв сертификатов с истекшим сроком приостановления действия
8. Оповещение о скором истечении срока приостановления действия сертификата
9. Оповещение администратора о количестве необработанных запросов
10. Копирование COC из локальной папки CDP на дискету
11. Публикация COC из сетевого ресурса CDP ЦР вышестоящего ЦС на сетевой ресурс incoming своего ЦС
12. Получение COC из сетевого ресурса CDP своего ЦС в локальную папку CDP
13. Публикация COC с дискеты на сетевой ресурс incoming своего ЦС

Задания №№ 10-13 относятся к заданиям публикации COC и их настройка описывается в разделе 4.7 настоящего Руководства.

Программное обеспечение Центра Регистрации включает пять базовых программных модулей:

- Перевод сертификатов, у которых истек срок действия, в состояние **Просроченные**;
- Уведомление о скором прекращении действия секретного ключа за устанавливаемый период времени до окончания;
- Перевод сертификатов, у которых истек срок действия секретного ключа, в состояние **Просроченный Ключ**;
- Очистка очереди отправленных сообщений с указанного периода;
- Превышение лимита запросов на сертификат в течение заданного периода.

Каждый базовый модуль имеет программный идентификатор обработчика и параметры, определяющие периодичность и режим работы их исполнения.

1. Оповещение об истечении срока действия сертификата открытого ключа

1.1. Программный идентификатор: **JOBCEXPLib.CPCCJOB_CertExpInformer**

1.2. Параметры:

- посылать уведомления пользователю
  - Значение параметра: (1)-посылать, (0) – не посылать
- посылать уведомления администратору
  - Значение параметра: (1)-посылать, (0) – не посылать
- режим отправки уведомления администратору
  - Значение параметра: (1)- посылать общее уведомление администратору, (0) – посылать уведомление администратору по каждому сертификату

2. Оповещение об окончании действия секретного ключа

2.1. Программный идентификатор: **JOBKSEXPLib.CPCCJOB_KeySExpInformer**

2.2. Параметры:

- посылать уведомления пользователю
  - Значение параметра: (1)-посылать, (0) – не посылать
- посылать уведомления администратору
  - Значение параметра: (1)-посылать, (0) – не посылать
- режим отправки уведомления администратору
  - Значение параметра: (1)- посылать общее уведомление администратору, (0) – посылать уведомление администратору по каждому сертификату
- вид указанного периода
  - Значение параметра: (d)-в днях, (m)-в месяцах, (yyyy)-в годах
- временной интервал от текущей даты, вперед, до вычисляемой даты. Вычисление производится либо за весь период, либо за день вычисленной даты
  - Значение параметра: число
- режим отбора сертификатов
  - Значение параметра: (0) – отбирать сертификаты, у которых срок действия ключа заканчивается в указанном периоде, (1) - отбирать сертификаты, у которых срок действия ключа заканчивается в день вычисленной даты

3. Оповещение о скором истечении срока действия секретного ключа

3.1. Программный идентификатор: **JOBKEXPLib.CPCCJOB_KeyExpInformer**

3.2. Параметры:

- посылать уведомления пользователю
  - Значение параметра: (1)-посылать, (0) – не посылать
- посылать уведомления администратору
  - Значение параметра: (1)-посылать, (0) – не посылать
- режим отправки уведомления администратору
  - Значение параметра: (1)- посылать общее уведомление администратору, (0) – посылать уведомление администратору по каждому сертификату

4. Отправка сообщений, стоящих в очереди

4.1. Программный идентификатор: **JOBDISTRIBMSGLib.CPCCJob_DistributeMsg**

4.2. Параметры:

- Имя очереди
  - Значение параметра по умолчанию: \Private$\RA_1_Mail

- Прервать выполнение операции при возникновении ошибки
  - Значение параметра: (1)-да, (0)-нет

5. Превышение лимита запросов на сертификат в течение заданного периода

5.1. Программный идентификатор: **JOBCEXLib.CPCCJOB_CertCExInformer**

5.2. Параметры:

- посылать уведомления пользователю
  - Значение параметра: (1)-посылать, (0) – не посылать
- посылать уведомления администратору
  - Значение параметра: (1)-посылать, (0) – не посылать
- допустимый предел количества запросов на сертификат в течение указанного периода
  - Значение число
- вид указанного периода
  - Значение параметра: (d)-в днях, (m)-в месяцах, (yyyy)-в годах
- временной интервал от текущей даты, назад, до вычисляемой даты.
  - Значение параметра: число

6. Удаление неактивных пользователей

6.1. Программный идентификатор: **JOBCLEARUSERSLib.CPCCJOB_ClearUsers**

6.2. Параметры:

- посылать уведомления администратору
  - Значение параметра: (1)-посылать, (0) – не посылать

7. Отзыв сертификатов с истекшим сроком приостановления действия

7.1. Программный идентификатор: **JOBREVHOLDCERTLib.CPCCJOB_RevHoldCert**

7.2. Параметры:

- посылать уведомления пользователю
  - Значение параметра: (1)-посылать, (0) – не посылать
- посылать уведомления администратору
  - Значение параметра: (1)-посылать, (0) – не посылать
- режим отправки уведомления администратору
  - Значение параметра: (1)- посылать общее уведомление администратору, (0) – посылать уведомление администратору по каждому сертификату

Помимо рассылки уведомлений пользователю и администратору данная задача осуществляет изменение статуса сертификата из состояния «действие приостановлено» в «отозван».

При выполнении настоящей задачи осуществляется просмотр Базы данных Центра Регистрации и, если обнаруживается сертификат, действие которого было приостановлено, и срок приостановления действия этого сертификата истек, то данный сертификат отзывается. До выполнения указанной задачи статус настоящего сертификата не изменится, т.е. статус сертификата будет (останется) - «действие приостановлено».

8. Оповещение о скором истечении срока приостановления действия сертификата

8.1. Программный идентификатор:
JOBUNHOLDREMINDLib.CPCCJob_UnholdRemind

8.2. Параметры:

- посылать уведомления пользователю
  - Значение параметра: (1)-посылать, (0) – не посылать
- посылать уведомления администратору
  - Значение параметра: (1)-посылать, (0) – не посылать
- допустимый предел количества запросов на сертификат в течение указанного периода
  - Значение параметра: число
- вид указанного периода
  - Значение параметра: (dd)-в днях, (ww)-в месяцах, (mm)-в месяцах, (yyyy)-в годах
- временной интервал, выраженный в единицах вида указанного периода.
  - Значение параметра: число

9. Оповещение администратора о количестве необработанных запросов

9.1. Программный идентификатор: **JOBPENDREQSLib.CPCCJOB_PendReqs**

9.2. Параметры:

- посылать уведомление в случае, если нет необработанных запросов
  - Значение параметра: (1)-посылать, (0) – не посылать

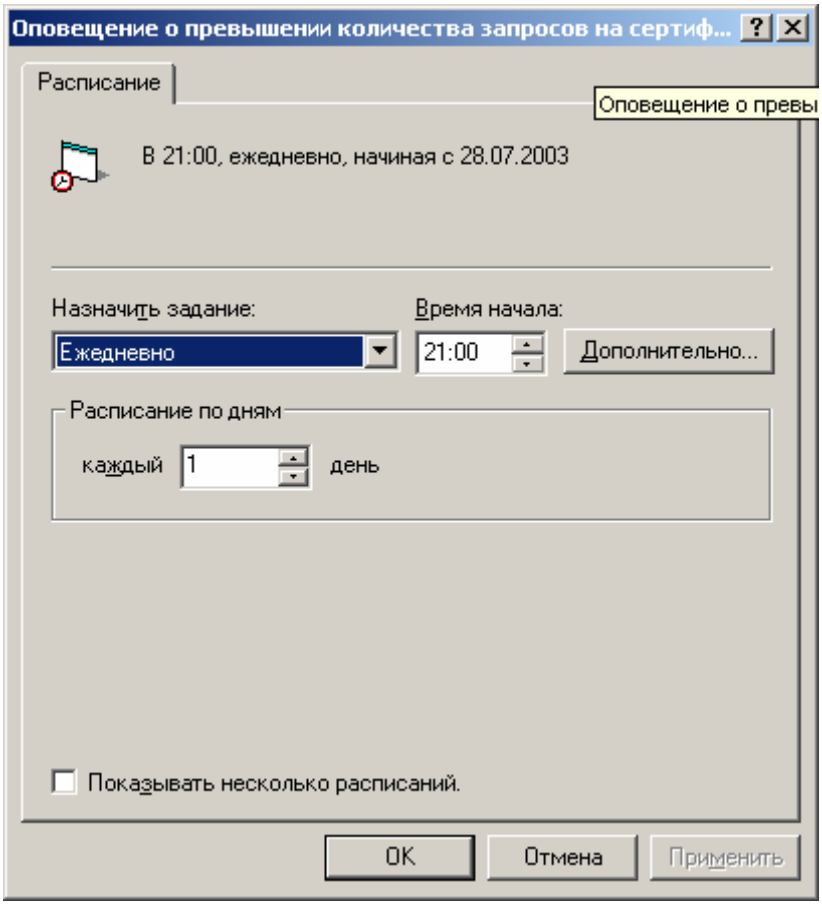
Таким образом, **регламентным заданием** является занесенное в список задание, содержащее информацию об исполняемом программном базовом модуле и значения его параметров.

Управление составом и параметрами заданий в списке осуществляется с помощью кнопок: **Создать**, **Свойства**, **Удалить** на вкладке Задания (см. Рисунок 4).

Для каждого задания должно быть определено расписание его выполнения. Расписание задается в окне свойств расписания при нажатии на кнопку **Расписание** (см. Рисунок 28).

Для каждого задания может быть определено несколько расписаний путем включения опции **Показывать несколько расписаний**.

Рисунок 28. Окно свойств расписания регламентного задания Центра Регистрации



Настройки параметров для каждого задания публикации COC сохраняются в отдельном файле в нотации XML. Файлы настройки размещаются в каталоге **..:\Documents and Settings\All Users\Application Data\Crypto Pro\RA\Inetpub\1\RA** и имеют расширение **job**.

Соответствие заданий и файлов настройки приведено в Таблица 5

Таблица 5. Таблица соответствия наименований заданий и файлов настройки

Наименование задания	Имя файла настройки
Оповещение о превышении количества запросов на сертификат	CertCExInformer.job
Оповещение об истечении срока действия сертификата открытого ключа	CertExpInformer.job
Удаление неактивных пользователей	ClearUsers.job
Отправка сообщений, стоящих в очереди	DistributeMsg.job
Оповещение о скором истечении срока действия секретного ключа	KeyExpInformer.job
Оповещение об окончании действия секретного ключа	KeySExpInformer.job
Отзыв сертификатов с истекшим сроком приостановления действия	RevHoldCert.job
Оповещение о скором истечении срока приостановления действия сертификата	UnholdRemind.job
Оповещение администратора о количестве необработанных запросов	PendingRequests.job

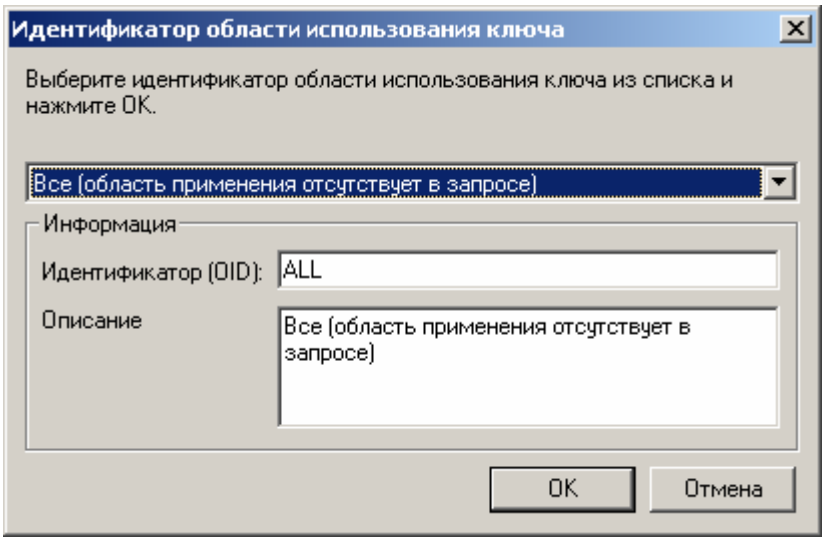
4.6. Настройка параметров Центра Регистрации для выпуска сертификатов открытых ключей уполномоченных лиц подчиненных УЦ

Сертификаты уполномоченных лиц подчиненных УЦ в программном комплексе «Удостоверяющий Центр» реализованы в виде сертификатов Центров Сертификации подчиненных УЦ по иерархической модели.

Для обеспечения обработки запросов на сертификат подчиненных ЦС администратором Центра Регистрации необходимо выполнить настройку политики обработки **неподписанных** запросов в параметрах Центра Регистрации.

Настройка политики заключается в добавлении в список допустимых областей применения для ролей, с которыми ассоциированы администраторы/операторы, выполняющие процедуры регистрации и выпуска сертификатов подчиненных УЦ, области применения, определяемой идентификатором **Все (область применения отсутствует в запросе)** (см. Рисунок 29).

Рисунок 29. Идентификатор области использования ключа подчиненных УЦ



Кроме того, в список допустимых расширений нужно добавить расширения 2.5.29.19 (Basic Constraints), 1.3.6.1.4.1.311.20.2 (Certificate Template Name), 1.3.6.1.4.1.311.21.1 (CA Version) и 2.5.29.14 (Subject Key Identifier).

4.7. Настройка заданий публикации COC

Для обеспечения автоматизации процедур распространения списков отозванных сертификатов (CRL, COC), издаваемых Центром Сертификации, в рамках одного Удостоверяющего Центра и по иерархии, в случае использования подчиненных УЦ, на Центре регистрации используются задания публикации COC.

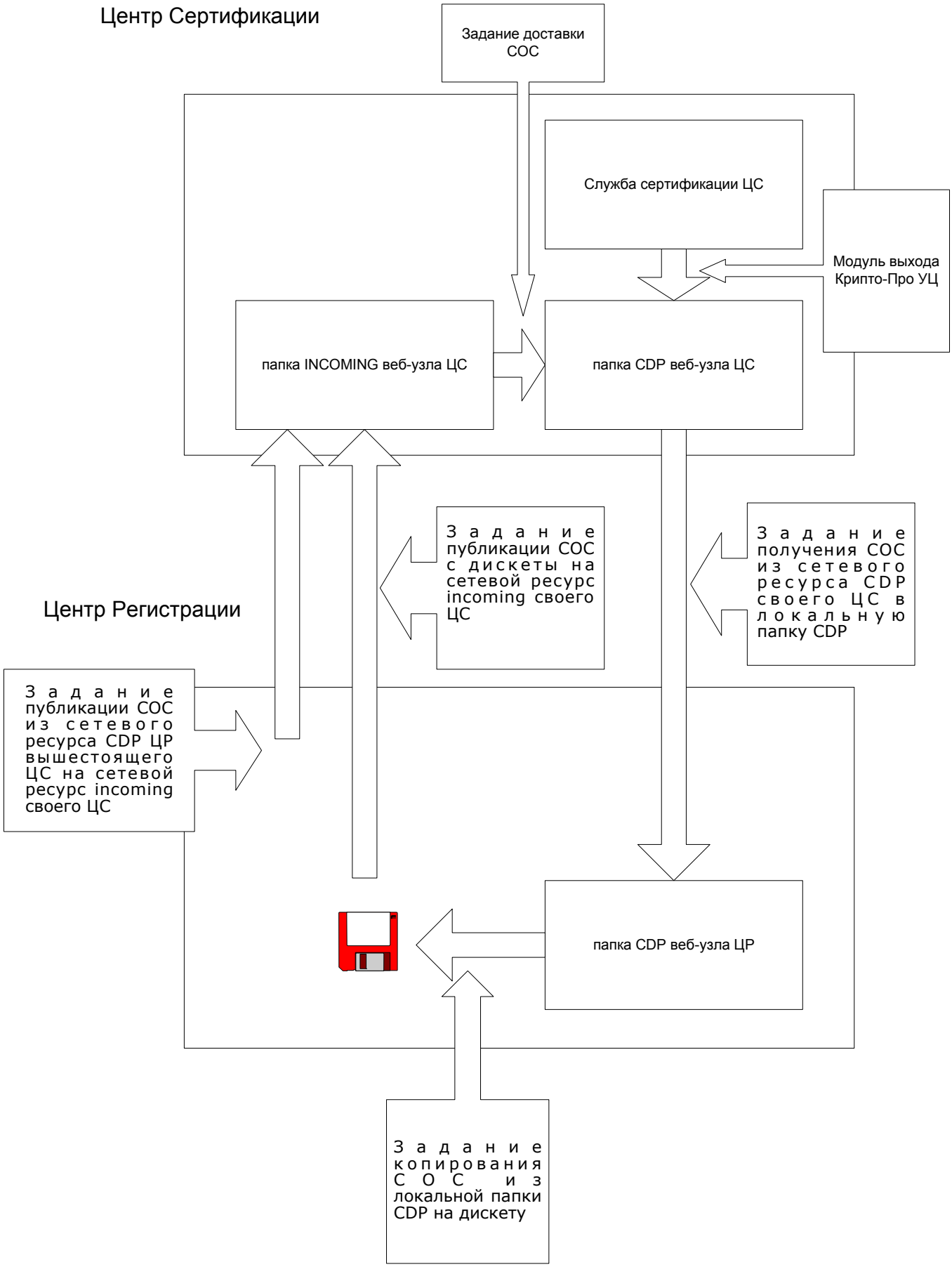
Задания публикации COC включают в себя следующие задания:

- Задание публикации COC с дискеты на сетевой ресурс incoming своего ЦС;
- Задание копирования COC из локальной папки CDP на дискету;
- Задание получения COC из сетевого ресурса CDP своего ЦС в локальную папку CDP;
- Задание публикации COC из сетевого ресурса CDP ЦР вышестоящего ЦС на сетевой ресурс incoming своего ЦС.

При этом задания публикации COC на ЦР должны использоваться совместно с заданиями и настройками модуля выхода на ЦС.

Общая схема взаимодействия задания публикации COC на Центре Сертификации и Центре Регистрации приведена на Рисунок 30.

Рисунок 30. Схема взаимодействия заданий публикации СОС на ЦС и ЦР



Применение заданий зависит от регламента и режима работы Удостоверяющего Центра.

Режим 1: Головной удостоверяющий центр без сетевого соединения с подчиненными УЦ.

Используются следующие задания на ЦР:

- *Задание получения СОС из сетевого ресурса CDP своего ЦС в локальную папку CDP*. Это задание будет доставлять на ЦР СОС, изданные «своим» ЦС.
- *Задание копирования СОС из локальной папки CDP на дискету*. Это задание будет копировать на магнитную дискету 3,5" файлы СОС, полученные предыдущим заданием.

Режим 2: Подчиненный УЦ, не имеющий сетевого соединения с вышестоящим УЦ (головным или вышестоящим по иерархии) и имеющий сетевое соединение с нижестоящими УЦ и/или предоставляющий сетевой доступ к файлам СОС, расположенным в сетевом ресурсе CDP Центра Регистрации, для пользователей.

Используются следующие задания на ЦР:

- *Задание публикации СОС с дискеты на сетевой ресурс incoming своего ЦС*. Это задание будет доставлять с ЦР СОС, расположенные на магнитной дискете 3,5" и полученные с вышестоящего УЦ.
- *Задание получения СОС из сетевого ресурса CDP своего ЦС в локальную папку CDP*. Это задание будет доставлять на ЦР СОС, изданные «своим» ЦС и полученные из вышестоящего УЦ.

Режим 3: Подчиненный УЦ, не имеющий сетевого соединения с вышестоящим УЦ (головным или вышестоящим по иерархии) и не имеющий сетевого соединения с нижестоящими УЦ и/или не предоставляющий сетевой доступ к файлам СОС, расположенным в сетевом ресурсе CDP Центра Регистрации, для пользователей.

Используются следующие задания на ЦР:

- *Задание публикации СОС с дискеты на сетевой ресурс incoming своего ЦС*. Это задание будет доставлять с ЦР СОС, расположенные на магнитной дискете 3,5" и полученные с вышестоящего УЦ.
- *Задание получения СОС из сетевого ресурса CDP своего ЦС в локальную папку CDP*. Это задание будет доставлять на ЦР СОС, изданные «своим» ЦС и полученные из вышестоящего УЦ.
- *Задание копирования СОС из локальной папки CDP на дискету*. Это задание будет копировать на магнитную дискету 3,5" файлы СОС, полученные предыдущим заданием.

Режим 4: Подчиненный УЦ, имеющий сетевое соединение с вышестоящим УЦ (головным или вышестоящим по иерархии) и не имеющий сетевого соединения с нижестоящими УЦ и/или не предоставляющий сетевой доступ к файлам СОС, расположенным в сетевом ресурсе CDP Центра Регистрации, для пользователей.

Используются следующие задания на ЦР:

- *Задание публикации СОС из сетевого ресурса CDP ЦР вышестоящего ЦС на сетевой ресурс incoming своего ЦС*. Это задание будет доставлять из ЦР вышестоящего УЦ файлы, содержащие СОС, и помещать их для обработки в «свой» ЦС.
- *Задание получения СОС из сетевого ресурса CDP своего ЦС в локальную папку CDP*. Это задание будет доставлять на ЦР СОС, изданные «своим» ЦС и полученные из вышестоящего УЦ.
- *Задание копирования СОС из локальной папки CDP на дискету*. Это задание будет копировать на магнитную дискету 3,5" файлы СОС, полученные предыдущим заданием.

Режим 5: Подчиненный УЦ, имеющий сетевое соединение с вышестоящим УЦ (головным или вышестоящим по иерархии) и имеющий сетевое соединение с нижестоящими УЦ и/или

предоставляющий сетевой доступ к файлам COC, расположенным в сетевом ресурсе CDP Центра Регистрации, для пользователей.

Используются следующие задания на ЦР:

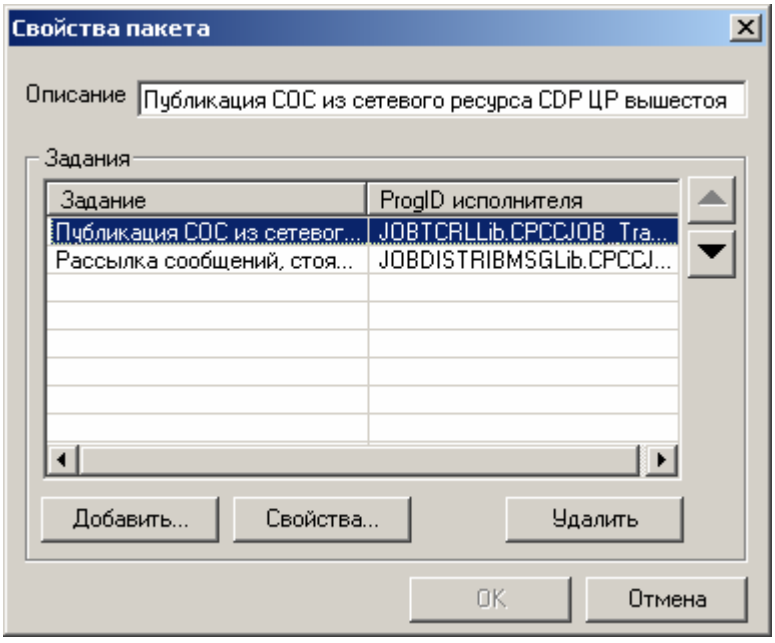
- *Задание публикации COC из сетевого ресурса CDP ЦР вышестоящего ЦС на сетевой ресурс incoming своего ЦС*. Это задание будет доставлять из ЦР вышестоящего УЦ файлы COC, и помещать их для обработки в «свой» ЦС.
- *Задание получения COC из сетевого ресурса CDP своего ЦС в локальную папку CDP*. Это задание будет доставлять на ЦР COC, изданные «своим» ЦС и полученные из вышестоящего УЦ.

В каждом режиме возможна настройка ЦР для публикации списков отозванных сертификатов в Active Directory (см. документ «КриптоПро УЦ. Регламентные задания»)

Настройка каждого задания осуществляется путем выбора задания в списке на вкладке **Задания** окна свойств ЦР (см. Рисунок 4) и нажатия кнопки **Свойства**.

В окне свойств пакета заданий для каждого задания публикации COC подготовлено одно или два задания (см. Рисунок 31). Для настройки задания выберите первое задание из списка и нажмите кнопку **Свойства**.

Рисунок 31. Окно свойств заданий публикации COC



В появившемся окне настройки задания (см. Рисунок 32) необходимо определить параметры задания (смысловое наполнение параметров зависит от задания):

Задание активно – определяет, что если оно не активно, то задание выполняться не будет, даже если на выполнение настроен соответствующий планировщик заданий Windows.

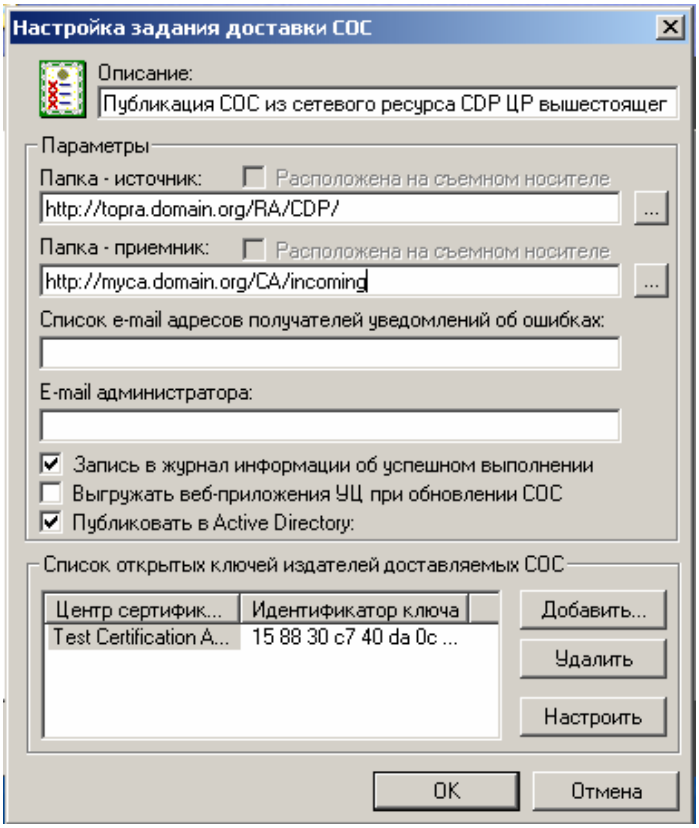
Папка-источник – определяет ресурс, содержащий файлы с CRL.

Папка-приемник – определяет ресурс, куда будут помещаться файлы с CRL, обрабатываемые из папки-источника.

Список e-mail адресов получателей уведомления – перечень адресов электронной почты, разделенных символом «точка с запятой», которым будет направляться уведомления о работе задания. Если данный параметр не задан, то уведомлений отправляться не будет. Если параметр задан, то необходимо выполнить настройку почты на соответствующей вкладке **Настройка почты**.

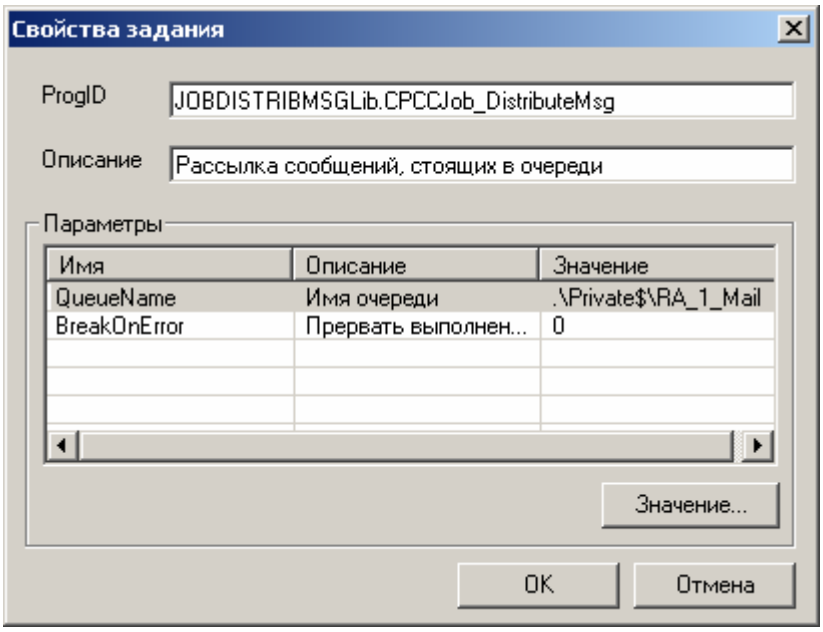
Список открытых ключей издателей доставляемых CRL – данный список содержит информацию об издателях COC (наименование и идентификатор ключа субъекта), списки отозванных сертификатов которых будут обрабатываться заданием.

Рисунок 32. Окно настройки задания публикации COC



Для настройки свойств задания рассылки сообщений из пакета задания публикации COC выберите второе задание из списка и нажмите кнопку **Свойства** (см. Рисунок 33).

Рисунок 33. Окно свойств задания рассылки сообщения из пакета задания публикации COC



Настройки параметров для каждого задания публикации COC сохраняются в отдельном файле в нотации XML. Файлы настройки размещаются в каталоге **..:\Documents and Settings\All Users\Application Data\Crypto Pro\RA\Inetpub\1\RA** и имеют расширение **job**.

Соответствие заданий и файлов настройки приведено в Таблица 6

Таблица 6. Таблица соответствия наименований заданий публикации COC и файлов настройки

Наименование задания	Имя файла настройки
Задание публикации COC с дискеты на сетевой ресурс incoming своего ЦС	fromDiskette.job
Задание копирования COC из локальной папки CDP на дискету	toDiskette.job
Задание получения COC из сетевого ресурса CDP своего ЦС в локальную папку CDP	fromSelfCA.job
Задание публикации COC из сетевого ресурса CDP ЦР вышестоящего ЦС на сетевой ресурс incoming своего ЦС	fromTopRA.job

Для того чтобы задания выполнялись в автоматическом режиме, нужно назначить расписание заданий на вкладке **Задания** окна свойств ЦР (см. Рисунок 4) путем нажатия кнопки **Расписание** и ввода параметров расписания.

4.8. Настройка политики имени пользователя при создании запроса на регистрацию

Программное обеспечение Центра Регистрации обеспечивает уникальность имен пользователей всех типов в Базе Данных Центра Регистрации.

Если Центр Регистрации работает в режиме поддержки регистрации пользователей в распределенном режиме, то программное обеспечение позволяет управлять политикой уникальности имени пользователя, проходящего процедуру регистрации, в запросах на регистрацию.

Данная политика определяется значением параметра **DenyDuplicateRegRequests** из типа политики **Дополнительные параметры** на вкладке **Политики** свойств Центра Регистрации приложения **Параметры Центра Регистрации**.

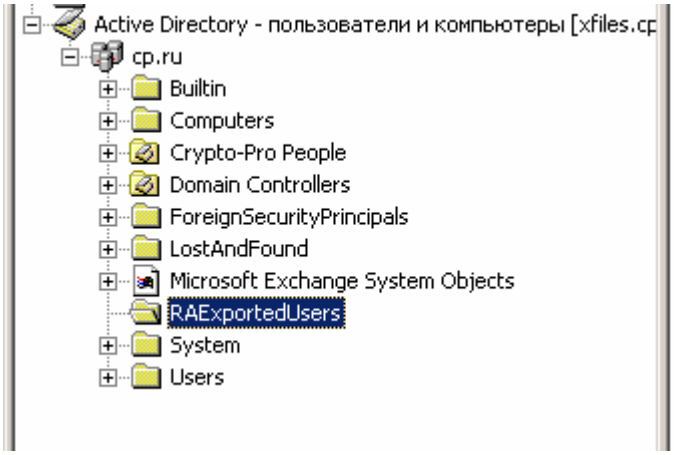
DenyDuplicateRegRequests = 0. При таком значении этого параметра Центр Регистрации будет принимать и ставить в очередь на обработку запросы на регистрацию пользователей, не проверяя уникальности имен пользователей.

DenyDuplicateRegRequests = 1. При таком значении этого параметра Центр Регистрации не будет принимать и ставить в очередь на обработку запросы на регистрацию пользователей, имена которых совпадают с именами пользователей в других запросах на регистрацию.

4.9. Настройка модуля экспорта пользователей и сертификатов в Active Directory

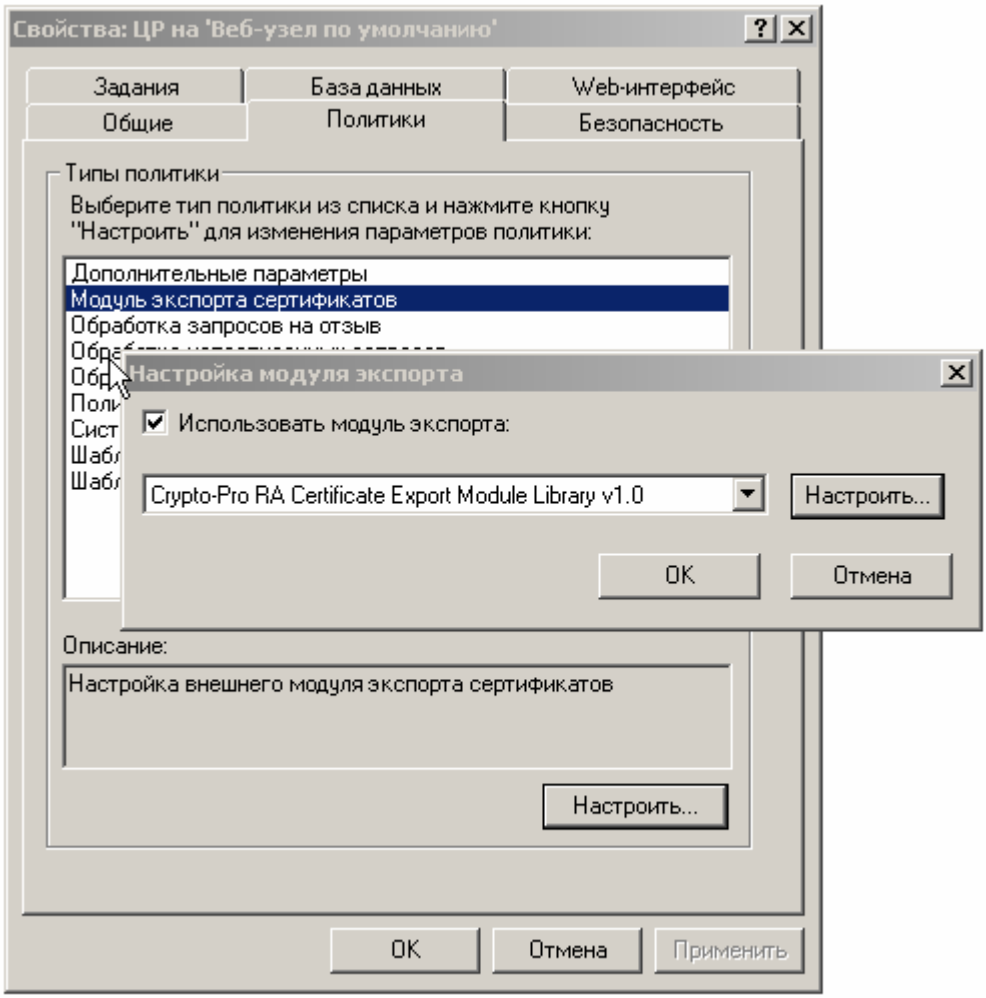
Создать, используя MMC консоль «Active Directory Users and Computers», отдельный контейнер (см. Рисунок 34), например, с именем RAExportedUsers (туда будут записываться (экспортироваться) все пользователи с выдаваемыми сертификатами).

Рисунок 34. Окно MMC консоли "Active Directory Users and Computers"



На вкладке **Политики** окна свойств модуля доступа Центра Регистрации вызвать окно настройки модуля экспорта сертификатов.

Рисунок 35. Вызов окна настройки модуля экспорта сертификатов

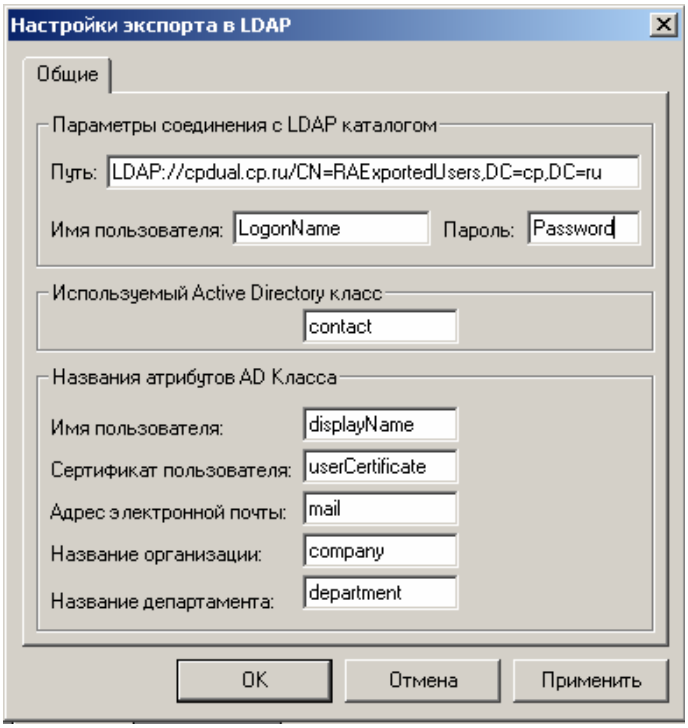


В поле «Путь» ввести LDAP адрес созданного контейнера в том виде как указано на рисунке (с тем именем контейнера, который создавали на предыдущем шаге).

В поле Имя пользователя ввести Account пользователя, имеющего права на запись в Active Directory в указанный контейнер, Например zAdmin (администратор). Соответственно в поле Password – его пароль для входа в домен.

Все остальные поля заполнить так, как указано ниже (см. Рисунок 36).

Рисунок 36. Окно настройки модуля экспорта сертификатов



5. Использование SQL 2000 Server

Как отмечалось в разделе установки ПО Центра Регистрации, по умолчанию используется Microsoft SQL 2000 Server Desktop Edition. Более подробно об этой редакции сервера баз данных можно прочитать в справочном руководстве компании Microsoft по данному продукту.

Если Вы желаете использовать полноценную СУБД SQL 2000 Server редакции Enterprise Edition или Personal Edition (в дальнейшем условимся называть MSDE – это экземпляр БД ЦР на SQL 2000 Server редакции MSDE 2000, а SQL 2000 Server – это экземпляр БД ЦР на SQL 2000 Server редакции Enterprise Edition или Personal Edition), то необходимо осуществить перенос БД с использованием сервиса Data Transformation Services, предоставляемого консолью SQL Server Enterprise Manager.

После подготовки БД на SQL 2000 Server, необходимо изменить строку соединения с базой данных Центра Регистрации в параметрах Центра Регистрации, в соответствии с разделом 4.1 настоящего Руководства. Для этого должна быть расширенная Лицензия на право установки и эксплуатации Центра регистрации, полученная от поставщика.

SQL 2000 Server должен быть установлен в следующей конфигурации:

Install database server:	Yes
Install upgrade tools:	Yes
Install replication support:	Yes
Install full-text search:	No
Install client management tools:	All
Install client connectivity:	Yes
Install online documentation:	Yes
Install development tools:	None
Install code samples:	None
Character Set:	1251 (Cyrillic)
Sort order:	Dictionary order, case-insensitive
Set Unicode collation:	General, case-insensitive

После установки ПО SQL 2000 Server необходимо создать новую базу данных на нем. Имя базы данных задается произвольно. Будем называть эту созданную базу данных «пустой» БД.

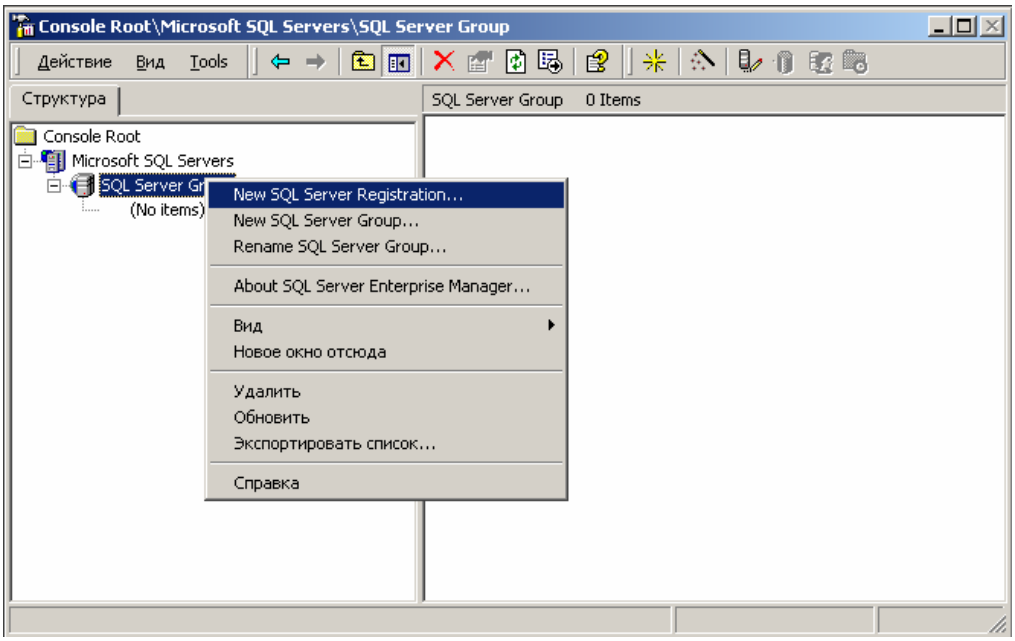
Выполните следующие действия:

Установите на сервере Центра Регистрации приложение консоли SQL Server Enterprise Manager из состава дистрибутива SQL 2000 Server.

Запустите приложение SQL Server Enterprise Manager.

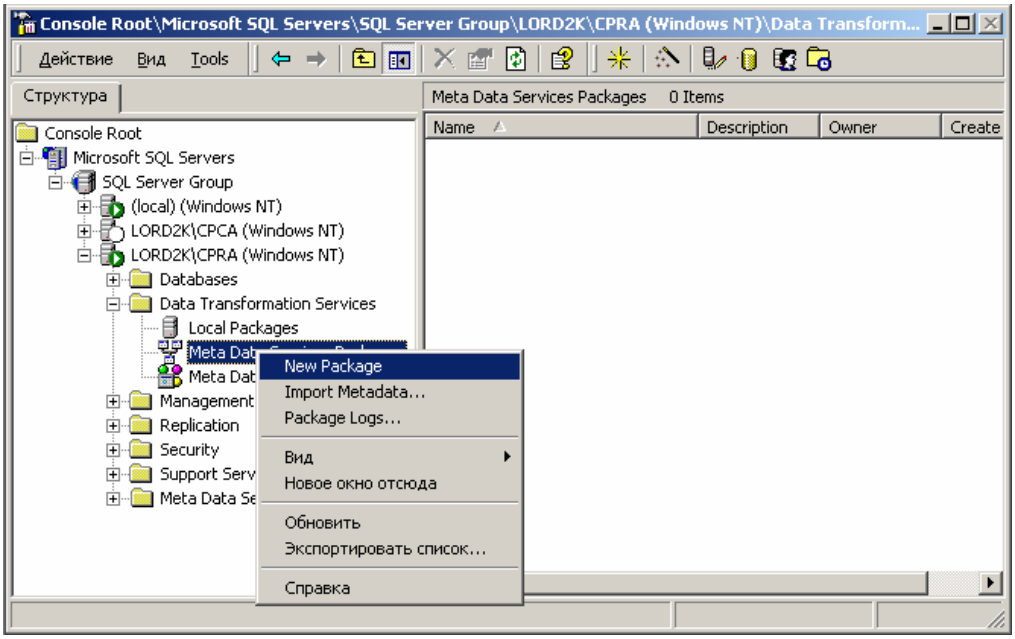
Зарегистрируйте экземпляр SQL сервера локального компьютера с именем CPRA в консоли с использованием Мастера регистрации SQL серверов (см. Рисунок 37). При регистрации укажите в качестве способа аутентификации Windows authentication.

Рисунок 37. Запуск Мастера регистрации SQL сервера в консоли Enterprise Manager



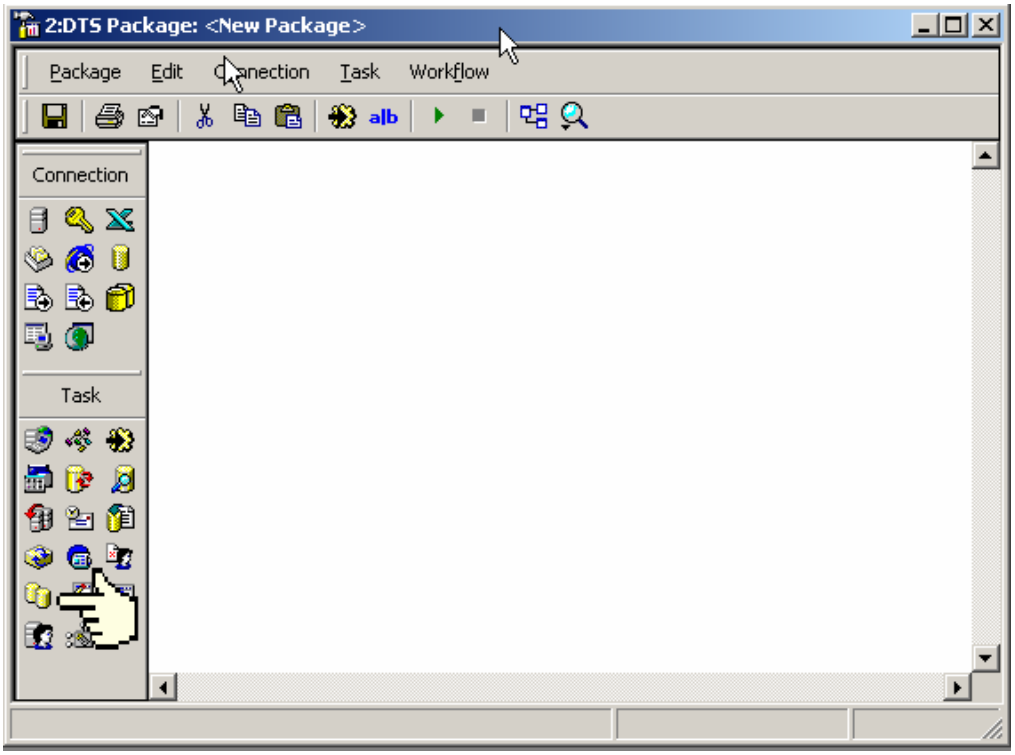
Запустите задачу создания нового Data Transformation Services (DTS) пакета для Meta Data Services (см. Рисунок 38).

Рисунок 38. Создание нового пакета Meta Data Services



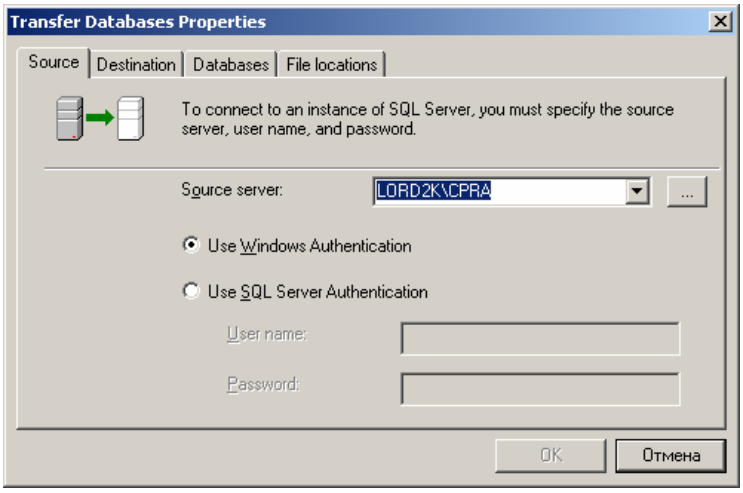
Запустите задание Transfer Database Task (см. Рисунок 39)

Рисунок 39. Запуск задания Transfer Database Task



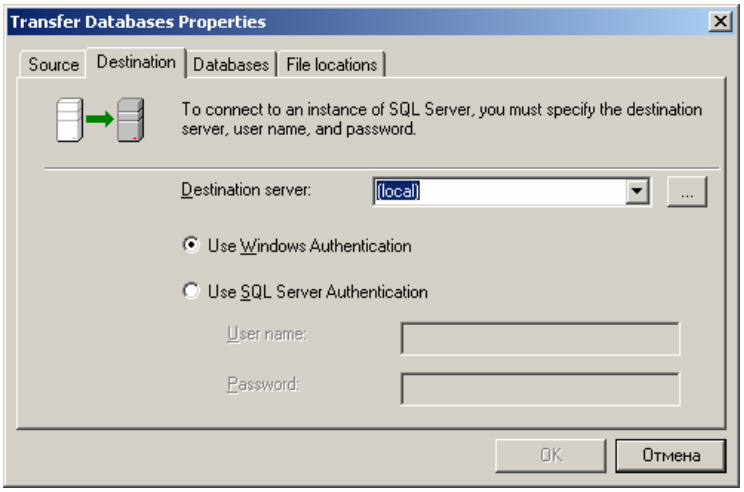
На вкладке **Source** в качестве сервера-источника выберите SQL сервер CPRA (см. Рисунок 40), который управляет базой данных с именем **crypto_pro_ra_db**.

Рисунок 40. Вкладка Source свойств задания Transfer Database Task



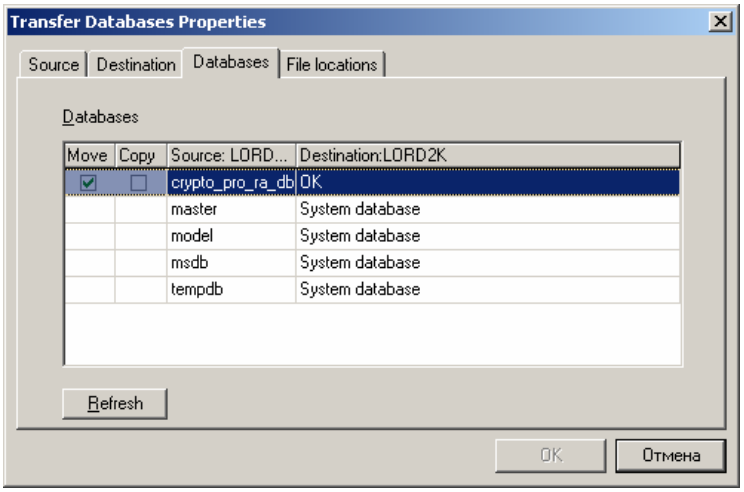
На вкладке **Destination** в качестве сервера-приемника выберите SQL 2000 Server (см. Рисунок 41), который будет управлять базой данных Центра Регистрации.

Рисунок 41. Вкладка Destination свойств задания Transfer Database Task



На вкладке **Databases** отметьте режим копирования или перемещения базы данных с именем **crypto_pro_ra_db** (см. Рисунок 42).

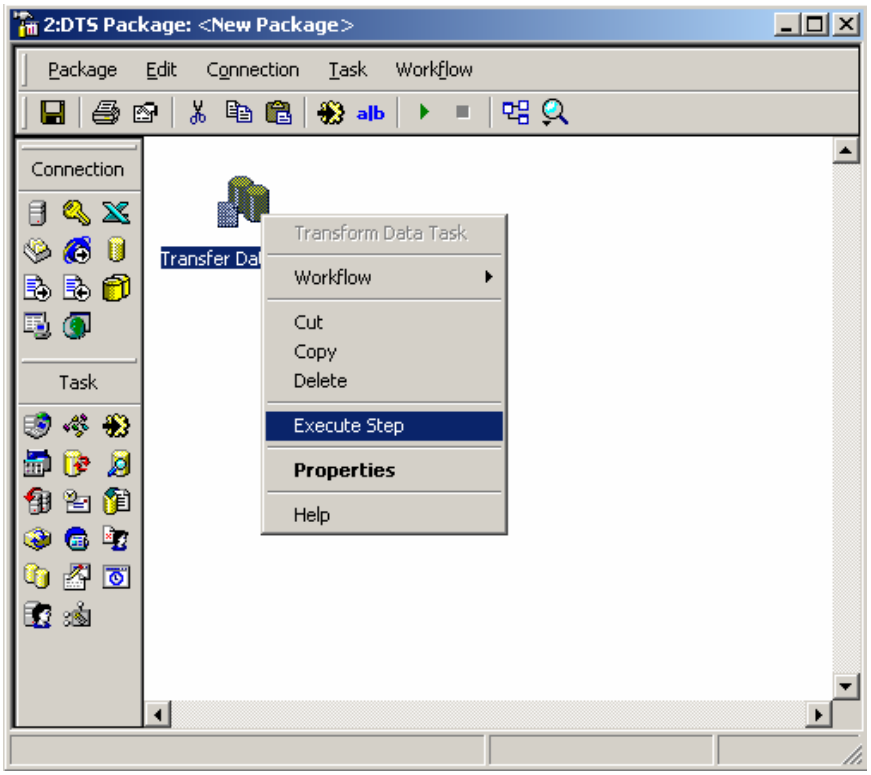
Рисунок 42. Вкладка Databases свойств задания Transfer Database Task



Перейдите на вкладку **File locations** и нажмите кнопку **OK** после установки свойств задания.

Вызовите контекстное меню правой кнопкой мыши и запустите выполнение сформированного задания, выбрав пункт **Executive Step** выпадающего меню (см. Рисунок 43).

Рисунок 43. Запуск исполнения задания переноса базы данных



6. Отправка почтовых сообщений

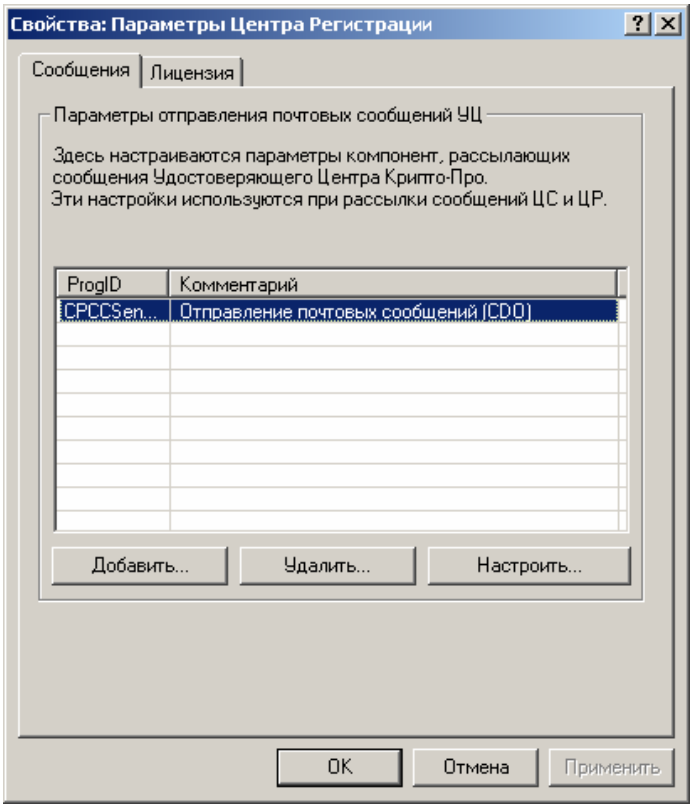
Программное обеспечение Центра Регистрации в процессе своей работы формирует и ставит в частную транзакционную очередь службы очередей сообщений почтовые сообщения в адрес пользователей и администратора Центра Регистрации.

Непосредственную доставку почтовых сообщений до получателей выполняет SMTP сервер организации, где эксплуатируется программное обеспечение Центра Регистрации.

Передача почтовых сообщений из очереди сообщений на SMTP сервер организации осуществляется с использованием регламентного задания Центра Регистрации с наименованием **Отправка почтовых сообщений, стоящих в очереди**.

Настройка программного обеспечения ЦР на выбранный почтовый сервер выполняется путем задания двух параметров в окне свойств приложения **Параметры Центра Регистрации** на вкладке **Сообщения** (см. Рисунок 7).

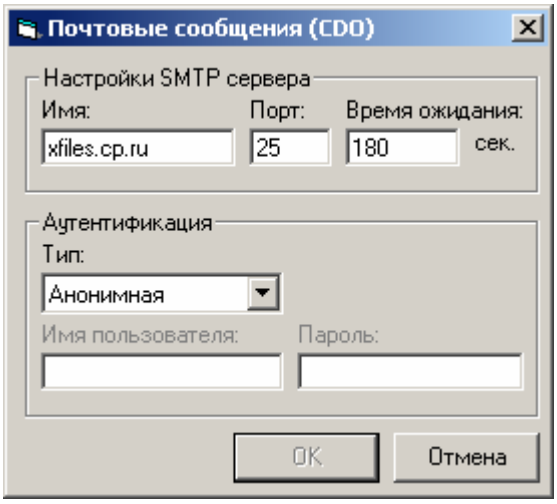
Рисунок 44. Окно свойств приложения Параметры Центра Регистрации



Для настройки параметров выберите из списка строку с комментарием **Отправление почтовых сообщений (CDO)** и нажмите кнопку **Настроить**.

В появившемся окне (см. Рисунок 45) введите параметры отправки почтовых сообщений.

Рисунок 45. Окно параметров отправки почтовых сообщений (CDO)



Отправка почты Центром Регистрации выполняется в **асинхронном** режиме.

Асинхронный режим отправки почтовых сообщений подразумевает, что транзакция, в которой формируется почтовое сообщение и инициируется его отправка, будет продолжаться и может быть завершена вне зависимости от результатов обработки почтовым сервером сообщения.

7. Подключение привилегированных пользователей

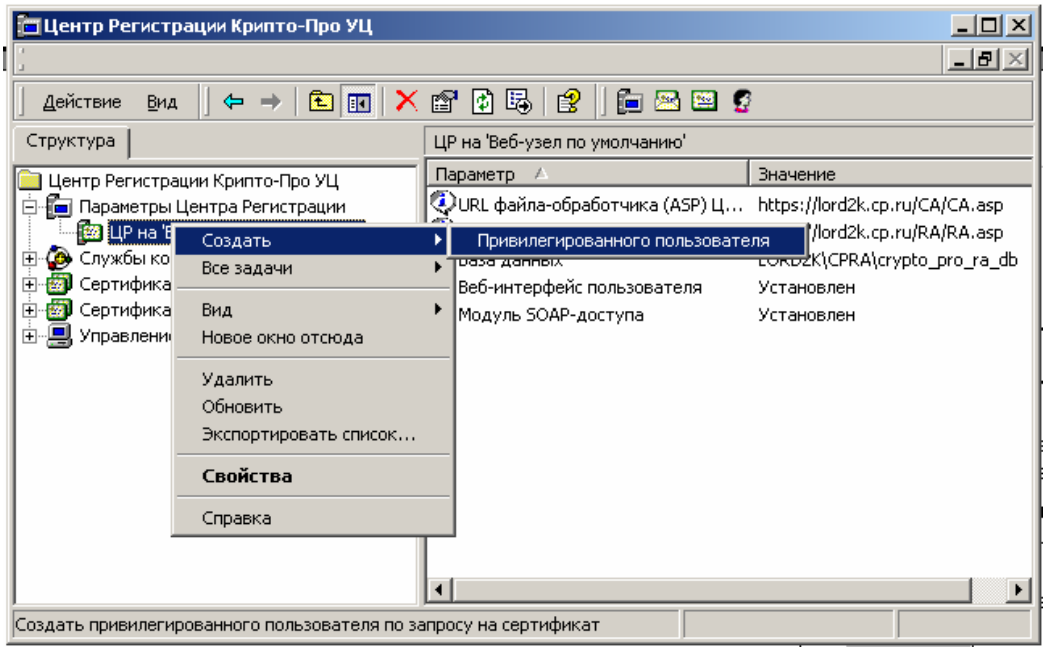
Под привилегированными пользователями Центра регистрации понимаются пользователи, входящие в группы администратора или операторов Центра регистрации. Взаимодействие привилегированных пользователей с Центром Регистрации осуществляется посредством программного обеспечения **АРМ администратора**.

Подключение привилегированных пользователей осуществляется на основании запроса на сертификат открытого ключа, сформированного с использованием АРМ администратора.

Данный запрос в виде файла должен быть доставлен сотруднику Удостоверяющего Центра, ответственному за выполнение регламентных процедур по конфигурированию Центра регистрации.

Подключение привилегированного пользователя выполняется с помощью задачи **Создать** и пункта **Привилегированного пользователя** узла **Центр Регистрации** в левом окне mmc-консоли приложения **Параметры Центра Регистрации** (см. Рисунок 46).

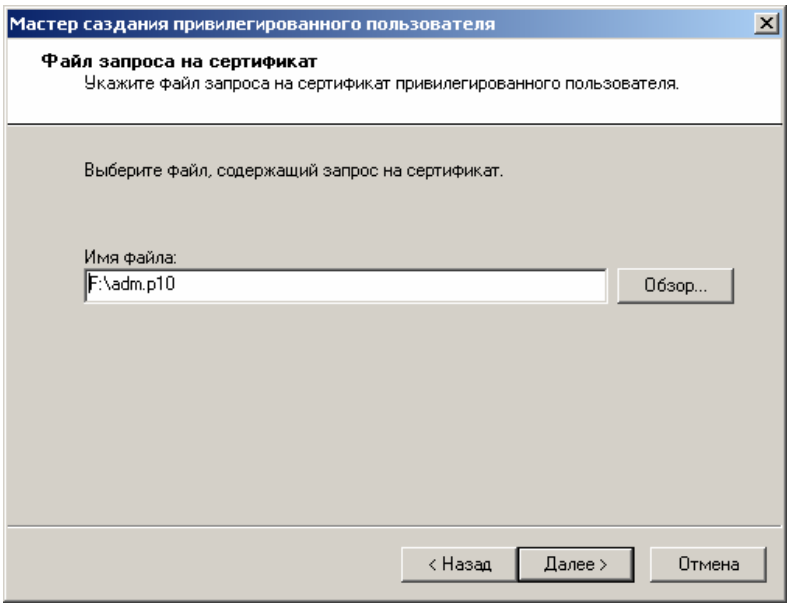
Рисунок 46. Задача Создать Привилегированного пользователя



При выполнении задачи выполните следующие действия в указанном порядке:

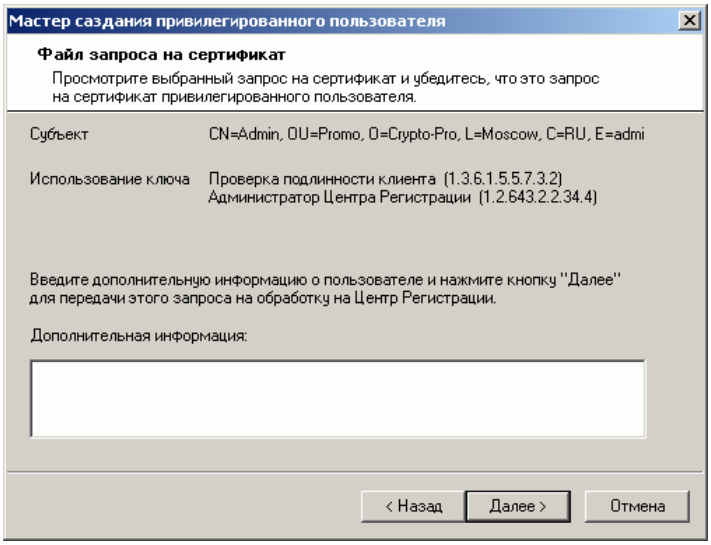
1. В диалоговом окне Мастера выберите файл с запросом на сертификат привилегированного пользователя (см. Рисунок 47).

Рисунок 47. Окно выбора файла с запросом в Мастере создания привилегированного пользователя



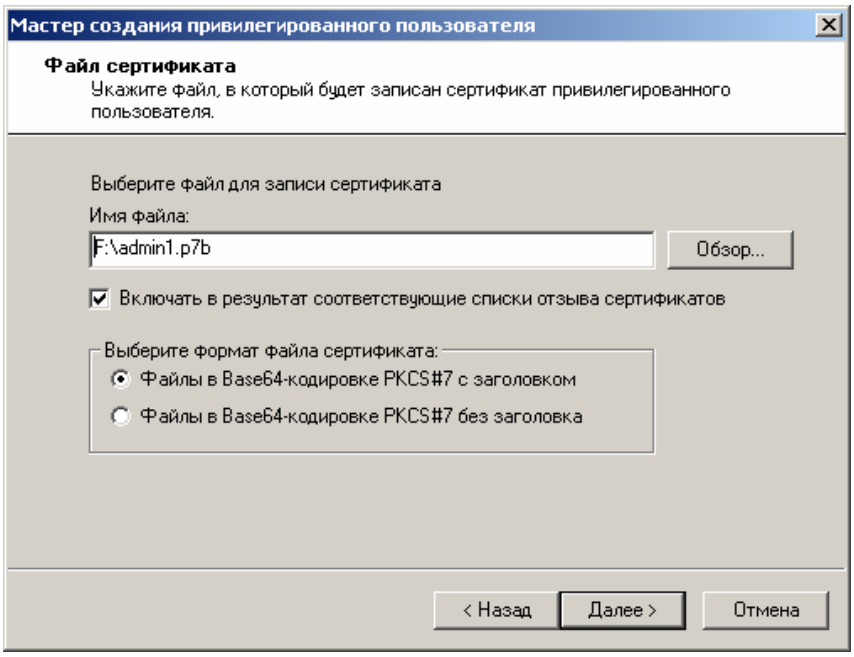
2. В следующем диалоговом окне Мастера отображается информация из запроса на сертификат привилегированного пользователя и для лица, осуществляющего обработку запроса, предоставляется возможность ввода дополнительной информации по данной процедуре (см. Рисунок 48).

Рисунок 48. Окно просмотра файла с запросом на сертификат привилегированного пользователя



3. В следующем окне Мастера создания привилегированного пользователя необходимо определить файл, куда будет сохранен выпущенный сертификат привилегированного пользователя, а также формат файла (см. Рисунок 49).

Рисунок 49. Окно выбора файла записи сертификата Мастера создания привилегированного пользователя



4. В случае положительной обработки запроса на Центре регистрации будет создан привилегированный пользователь. Мастером будет выдано соответствующее сообщение (см. Рисунок 50)

В противном случае будет отображено окно с диагностическим сообщением об ошибке (см. Рисунок 51).

Типичными причинами возникновения ошибки являются:

- отсутствие соединения с Центром сертификации;
- не запущена служба Microsoft Certificates Authority;
- запрос на сертификат привилегированного пользователя не содержит идентификаторы, определяющие роль привилегированного пользователя;
- настройки модуля политики Центра сертификации не позволяют выпустить сертификат в соответствии с запросом.

Рисунок 50. Окно сообщения о создании привилегированного пользователя

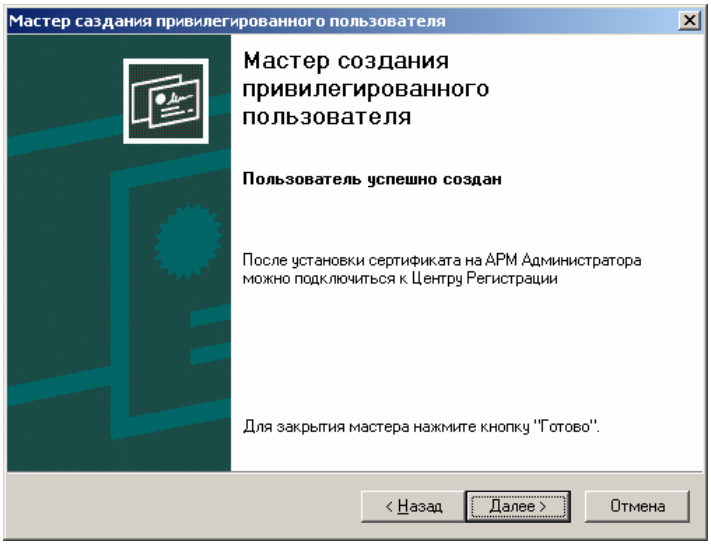
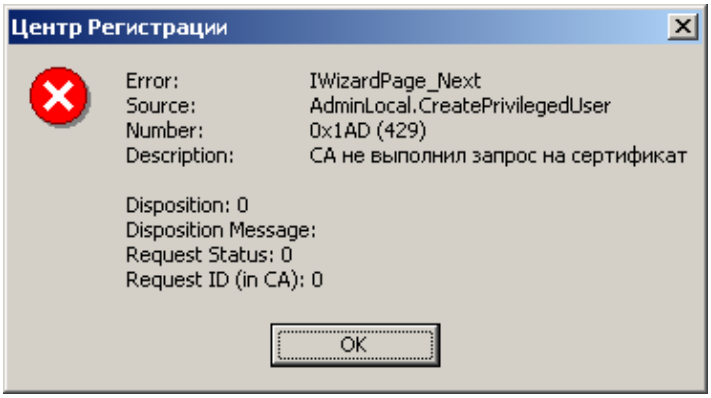


Рисунок 51. Пример сообщения об ошибке Мастера создания привилегированного пользователя



При подключении привилегированного пользователя, запрос на сертификат не подвергается обработке согласно политике обработки подписанных и неподписанных запросов Центра Регистрации.

8. Настройка Центра Регистрации для регистрации и обработки запросов на сертификат ЦС подчиненных УЦ

Для обеспечения возможности регистрации Центров Сертификации подчиненных Удостоверяющих Центров необходимо выполнить следующие настройки Центра Регистрации:

1. В окне свойств модуля доступа Центра Регистрации на вкладке **Политики** (см. Рисунок 24) выберите политику **Обработка неподписанных запросов**;
2. Для соответствующей роли из числа привилегированных пользователей, выполняющих задачу по регистрации подчиненных УЦ (роль **Оператор** в настройках по умолчанию), в список допустимых использований сертификата добавьте идентификатор **Все (область применения отсутствует в запросе)**
3. Для соответствующей роли из числа привилегированных пользователей, выполняющих задачу по выпуску новых сертификатов подчиненных УЦ (роль **Администратор** в настройках по умолчанию), в список допустимых использований сертификата добавьте идентификатор **Все (область применения отсутствует в запросе)**
4. Сохраните настройки.

9. Использование и управление списком отозванных сертификатов на Центре Регистрации

Программное обеспечение Центра Регистрации использует для взаимодействия с внешними приложениями (например, АРМ администратора ЦР) и предоставления пользователям АРМ Web-сервер MS Internet Information Server 5.0 (MS IIS).

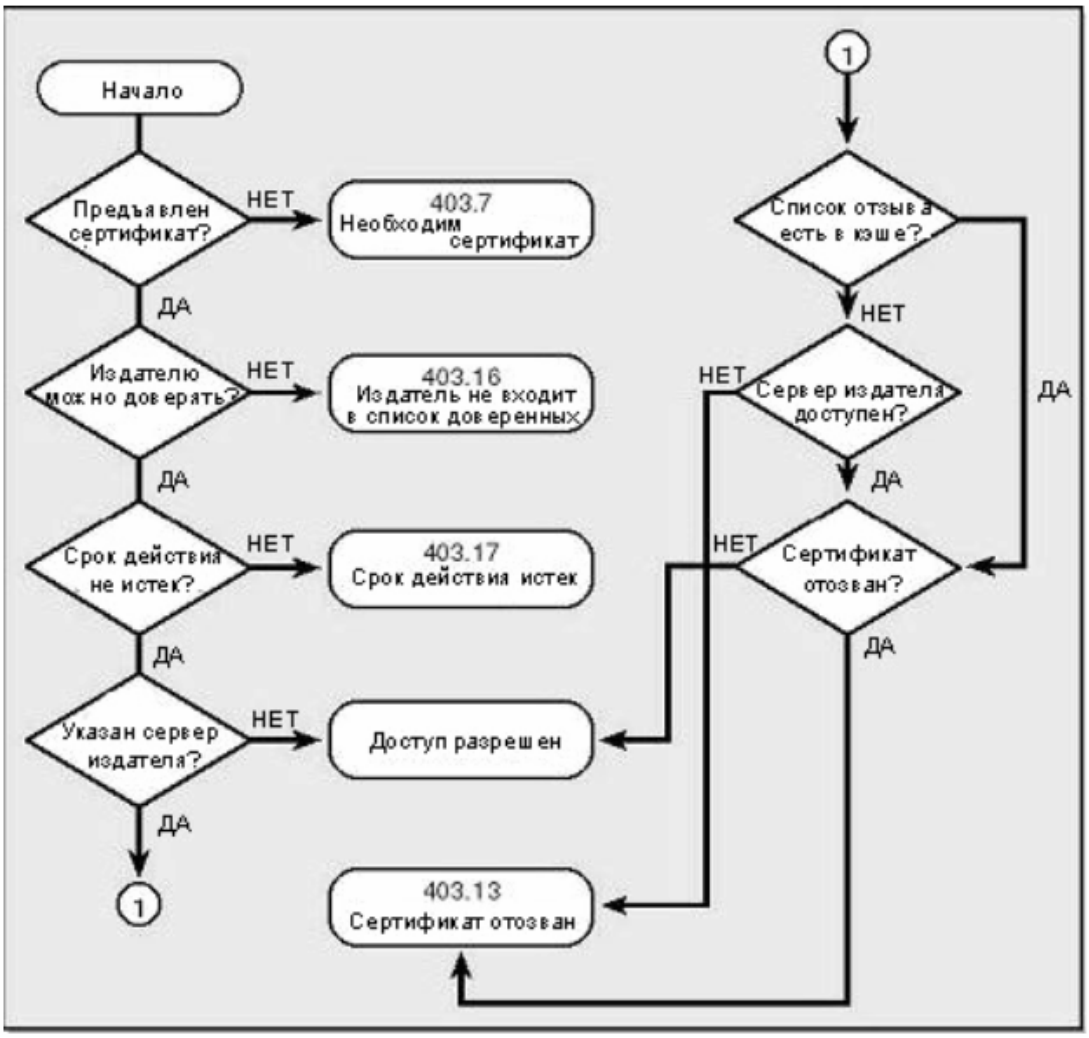
Взаимодействие с внешними приложениями и АРМ осуществляется по защищенным соединениям с использованием транспортных протоколов SSLv3/TLSv1/КриптоПро TLS. При установлении защищенных соединений с использованием режима двухсторонней аутентификации клиент предъявляет свой сертификат открытого ключа и доказывает обладание закрытым ключом, соответствующим открытому ключу. Web-сервер устанавливает доверие к клиентскому сертификату, одним из элементов которого является проверка клиентского сертификата открытого ключа на отсутствие в списке отозванных сертификатов.

Список отозванных сертификатов (CRL) формируется Центром сертификации автоматически по расписанию или по запросу администратора. Каждый CRL снабжается датой его актуальности и планируемой датой формирования следующего CRL. Подробнее о списке отозванных сертификатов, его формате и составе приведено в документе "КриптоПро УЦ. Общее описание".

В случае если Web-серверу MS IIS при выполнении процедуры проверки клиентского сертификата будет недоступен список отозванных сертификатов, то установление соединения блокируется. Поэтому необходимо выполнять регламентные процедуры по актуализации CRL на Центре Регистрации.

Алгоритм работы MS IIS при проверке клиентского сертификата приведен на рисунке 52.

Рисунок 52. Алгоритм проверки клиентского сертификата MS IIS



9.1. Установка нового CRL в связи с истечением его срока действия

Под этой процедурой понимается регулярное обновление списка отозванных сертификатов на Центре Регистрации в связи с предстоящим истечением срока действия ранее установленного CRL на Web-сервере Центра Регистрации.

Данная процедура должна быть выполнена до истечения срока действия ранее установленного («старого») CRL. Временной интервал, когда планируется начало выполнения процедуры установки нового CRL, определяется регламентными документами организации, эксплуатирующей программный комплекс «Удостоверяющий Центр». Рекомендуется данные мероприятия выполнять в день истечения срока «старого» CRL.

1. на АРМ администратора ЦР выполнить последовательно:

   1.1. задачу "Опубликовать CRL". Данная задача обеспечит публикацию (формирование файла с CRL) списка отозванных сертификатов на Центре Сертификации, содержащий актуальный CRL на момент выполнения задачи.

   1.2. задачу "Открыть текущий CRL" с сохранением файла CRL на дискету. Выполнение этой задачи обеспечит загрузку файла опубликованного CRL на рабочее место администратора ЦР.

2. Доставить дискету с файлом CRL на сервер, на котором расположен файл, определенный в точке распространения списка отозванных сертификатов (CDP) сертификатов открытых

ключей пользователей ЦР как точка распространения CRL. Подробнее о составе сертификатов открытых ключей, формируемых Центром Сертификации, смотрите в документе "КриптоПро УЦ. Общее описание".

3. Заменить этот файл на файл с «новым» CRL, расположенным на дискете.

4. В случае если Центр Сертификации настроен на выпуск сертификатов открытых ключей пользователей с пустым CDP, следует на сервере Центра Регистрации установить CRL с дискеты в **хранилище сертификатов локального компьютера** в раздел **Промежуточные центры сертификации**.

9.2. Установка нового CRL в связи с отзывом сертификата до истечения срока действия старого CRL

Под этой процедурой понимается обновление CRL на Центре Регистрации в связи с отзывом сертификата открытого ключа пользователя ЦР с целью обеспечения блокирования доступа пользователя к ресурсам Центра Регистрации на отозванном сертификате открытого ключа.

1. выполнить процедуру отзыва сертификата в соответствии с «Руководством администратора»

2. на АРМ администратора ЦР выполнить последовательно:

   2.1. задачу "Опубликовать CRL". Выполнение данной задачи обеспечит формирование CRL, содержащий отозванный сертификат открытого ключа пользователя ЦР.

   2.2. задачу "Открыть текущий CRL" с сохранением файла CRL на дискету

3. Доставить дискету с файлом CRL на сервер, на котором расположен файл, определенный в точке распространения списка отозванных сертификатов (CDP) сертификатов открытых ключей пользователей ЦР как точка распространения CRL. Подробнее о составе сертификатов открытых ключей, формируемых Центром Сертификации, смотрите в документе "КриптоПро УЦ. Общее описание".

4. Заменить этот файл на файл с «новым» CRL, расположенный на дискете.

5. На сервере Центра Регистрации, через MMC консоль ОС Windows 2000 Server, с использованием оснастки "Сертификаты" для локального компьютера удалить CRL из раздела "Промежуточные центры сертификации" (локальный компьютер)

6. С использованием FAR или Проводника найти и удалить закэшированные Web-сервером файлы CRL в подкаталогах каталога кэша IIS. Каталог кэша MS IIS располагается в каталоге \Local Settings\Temporary Internet Files\Content.IE5\ профайла учетной записи компьютера, под которой был осуществлен вход в операционную систему. Наименование закэшированных файлов имеет следующий формат: имя_файла_CRL_как_в_CDP(номер).crl

7. Перезапустить MS IIS с использованием соответствующей задачи в Диспетчере служб Интернета.

9.3. Действия администратора при несоблюдении срока установки нового CRL по истечению срока его действия

После истечения срока действия текущего CRL, Web-сервер Центра Регистрации блокирует доступ к своим ресурсам, на которые требуется доступ по протоколу TLS/SSL с предоставлением клиентского сертификата. В этом случае становится невозможным и соединение приложения «АРМ администратора ЦР» с серверными компонентами Центра Регистрации.

1. На сервере Центра Сертификации через оснастку службы сертификации выполнить задачу публикации CRL

2. Переписать файл с CRL из каталога \winnt\systen32\certsrv\certenroll на дискету

3. Доставить дискету с файлом CRL на сервер, на котором расположен файл, определенный в точке распространения списка отозванных сертификатов (CDP) сертификатов открытых ключей пользователей ЦР как точка распространения CRL. Подробнее о составе сертификатов открытых ключей, формируемых Центром Сертификации, смотрите в документе "КриптоПро УЦ. Общее описание".

4. Заменить этот файл на файл с «новым» CRL, расположенный на дискете.

5. В случае, если Центр Сертификации настроен на выпуск сертификатов открытых ключей пользователей с пустым CDP, следует установить CRL с дискеты в **хранилище сертификатов локального компьютера** в раздел **Промежуточные центры сертификации** на сервере Центра Регистрации.

10. Сроки действия ключей Центра Регистрации и Web-сервера Центра Регистрации

Сроки действия ключей Центра Регистрации и Web-сервера Центра Регистрации устанавливаются на основании Регламента Удостоверяющего Центра организации, эксплуатирующей программный комплекс.

Срок действия сертификата открытого ключа Web-сервера Центра Регистрации рекомендуется устанавливать равным сроку действия соответствующего закрытого ключа Web-сервера Центра Регистрации.

Срок действия сертификата открытого ключа Центра Регистрации рекомендуется устанавливать равным сроку действия соответствующего закрытого ключа Центра Регистрации.

Максимальные сроки действия закрытых ключей и сертификатов Центра Регистрации и Web-сервера Центра Регистрации должны удовлетворять требованиям применяемого СКЗИ.

11. Смена ключей Web-сервера Центра регистрации

Смена ключей Web-сервера Центра Регистрации осуществляется в соответствии с регламентом Удостоверяющего Центра.

Смена ключей Web-сервера Центра Регистрации выполняется в следующем порядке:

1. Генерация новых ключей и создание запроса на сертификат Web-сервера Центра Регистрации;
2. Выпуск и установка нового сертификата Web-сервера Центра Регистрации;
3. Смена сертификата на Web-узле MS IIS;
4. Уничтожение старых ключей на Центре регистрации;

11.1. Генерация новых ключей и создание запроса на сертификат Web-сервера Центра Регистрации

Генерация новых ключей и формирование запроса на сертификат Web-сервера Центра регистрации осуществляется с использованием программы-утилиты **Запрос сертификата Web-сервера ЦР** из состава программного обеспечения Центра регистрации (группа **Крипто-Про**). Описание использования этой программы приведено в разделе **4.5.1 п.1** документа **КриптоПро УЦ Руководство по установке**.

11.2. Выпуск и установка нового сертификата Web-сервера Центра Регистрации

Обработка запроса на сертификат, выпуск сертификата Web-сервера Центра регистрации выполняются на Центре сертификации в соответствии с руководством по эксплуатации Центра сертификации.

Установка выпущенного сертификата, полученного из Центра сертификации в виде файла, осуществляется с использованием Мастера установки сертификата WEB-сервера ЦР из группы **Крипто-Про**. Описание использования этой программы приведено в разделе **4.5.1 п.12** документа **КриптоПро УЦ Руководство по установке**.

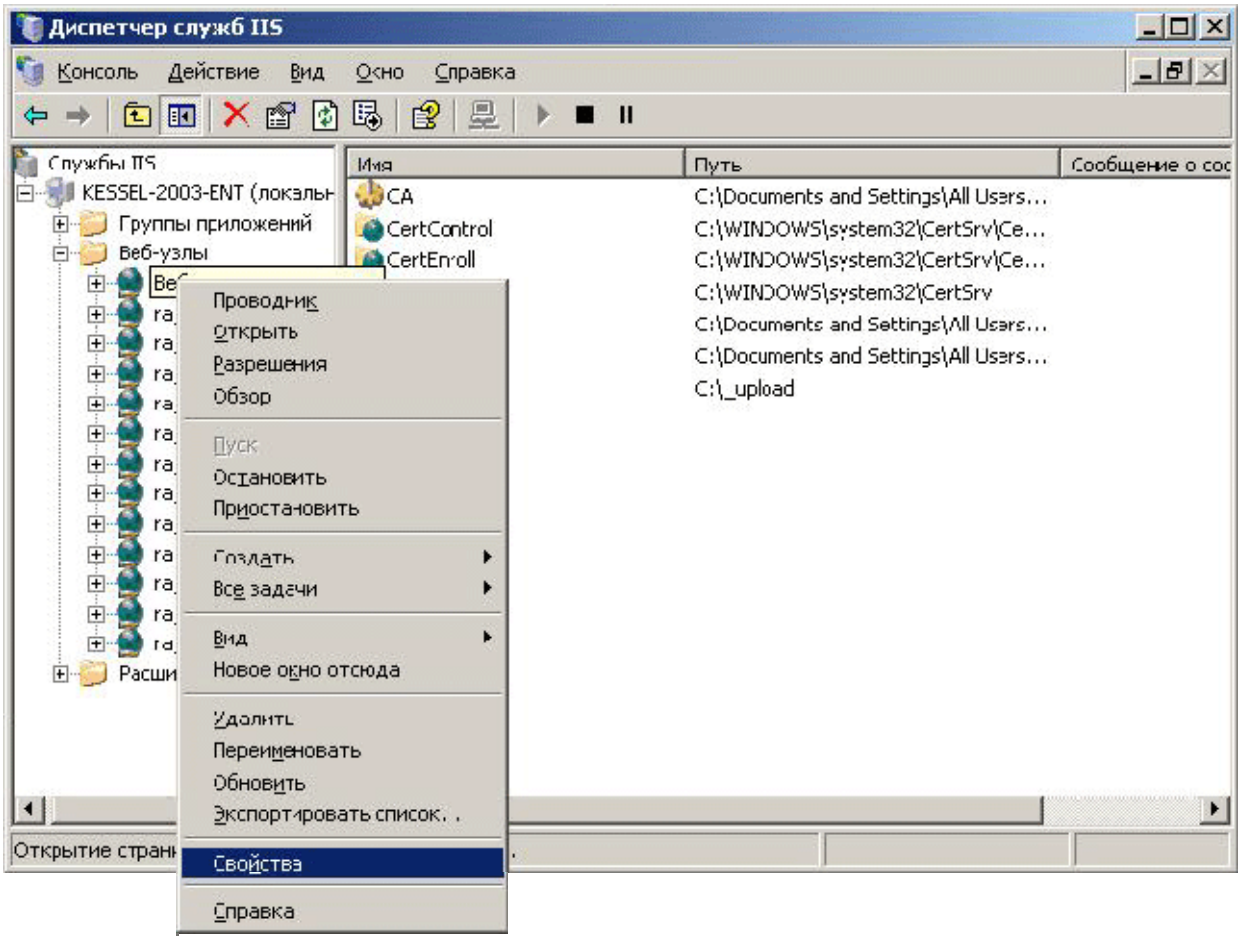
11.3. Смена сертификата на Web-узле MS IIS

После установки выпущенного сертификата Web-сервера Центра регистрации необходимо выполнить процедуру замены сертификата серверной аутентификации на Web-узле Web-сервера MS IIS.

Данное действие выполняется из приложения **Диспетчер служб Интернета** группы **Администрирование**.

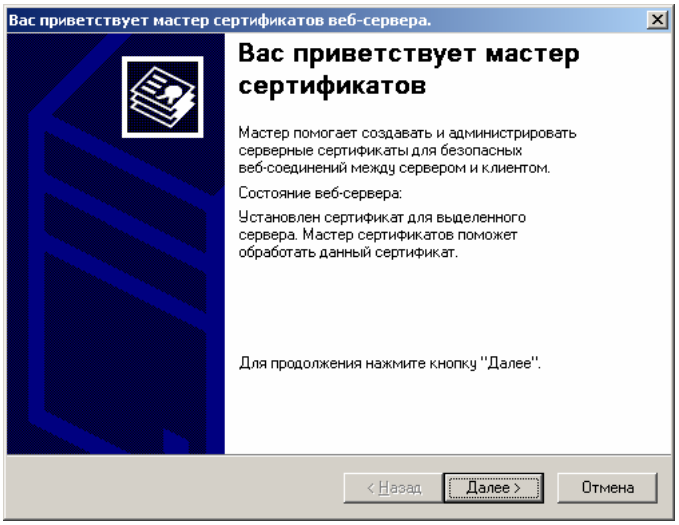
1. Откройте окно свойств Web-узла Web-сервера MS IIS (см. **Рисунок 54**).

Рисунок 53. Окно свойств Web-узла Web-сервера MS IIS



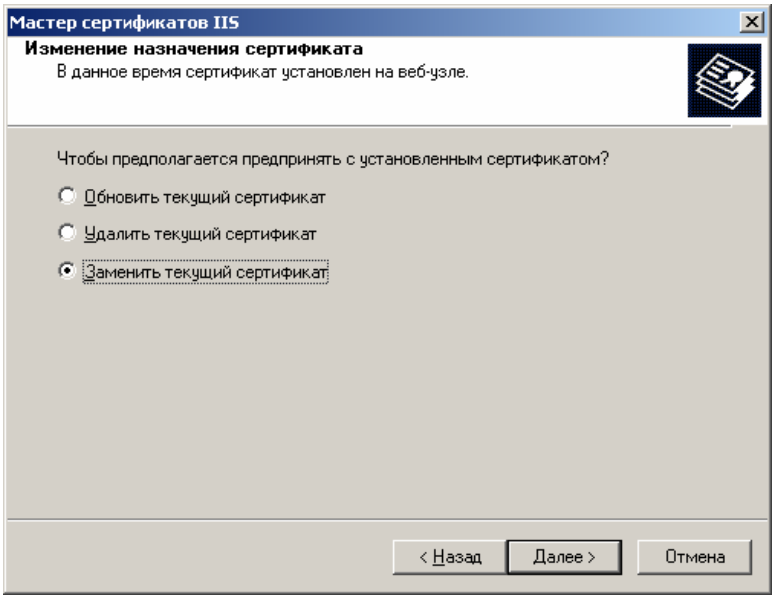
2. Выберите вкладку **Безопасность каталога**.
3. На данной вкладке нажмите кнопку **Сертификат** в группе **Безопасные подключения**.
4. Запустится Мастер сертификатов Web-сервера (см. Рисунок 54).

Рисунок 54. Окно Мастера сертификатов Web-сервера



5. Нажмите кнопку **Далее** и в следующем окне выберите **Заменить текущий сертификат** (см. Рисунок 55) и нажмите кнопку **Далее**.

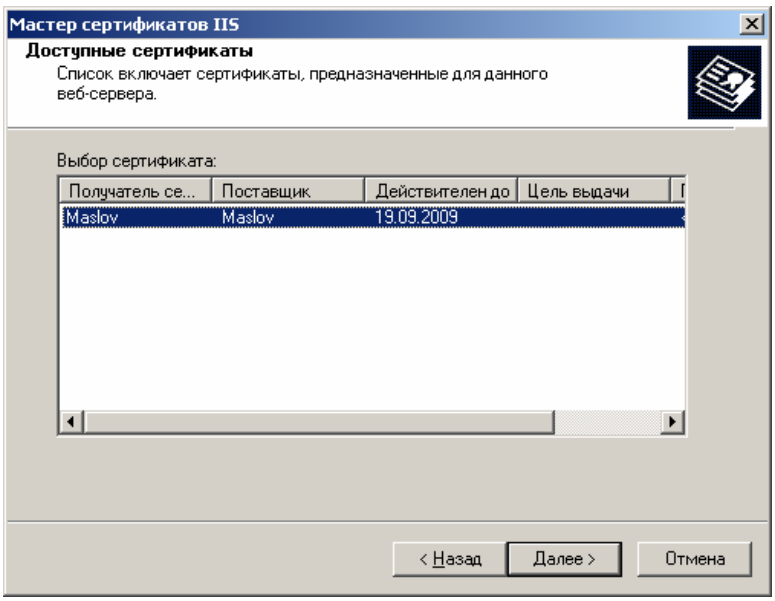
Рисунок 55. Окно изменения назначения сертификата Мастера сертификатов Web-сервера



Обязательно нужно выбирать опцию **Заменить текущий сертификат**. Если выполнить опцию **Удалить текущий сертификат**, то это приведет к снятию всех SSL/TLS настроек к файлам и виртуальным каталогам веб-узла Центра Регистрации, что в свою очередь приведет к полной неработоспособности Центра Регистрации.

6. В появившемся окне выберите новый установленный сертификат и нажмите кнопку **Далее** (см. Рисунок 56).

Рисунок 56. Окно выбора сертификата для замены существующего в Мастере сертификатов Web-сервера



Таким образом, будет произведена смена сертификата Web-сервера Центра регистрации в MS IIS.

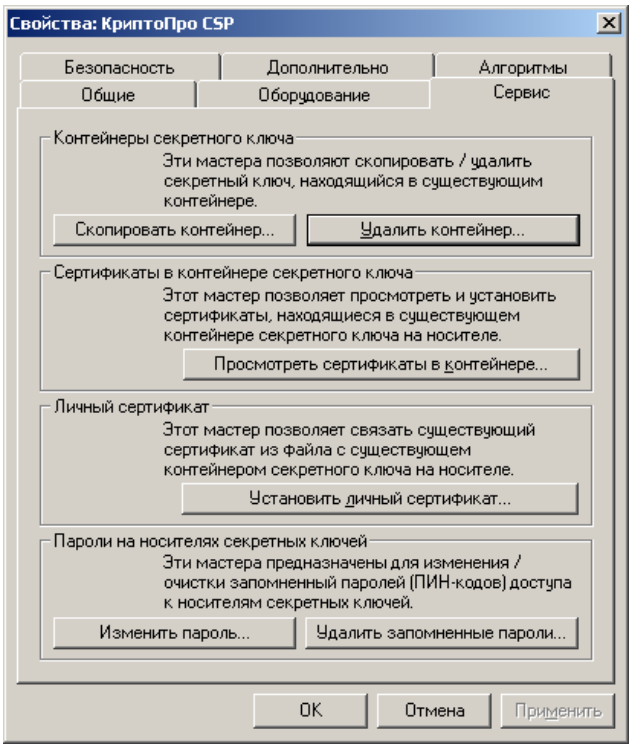
11.4. Уничтожение старых ключей на Центре регистрации

Уничтожение старых ключей Web-сервера Центра регистрации на ключевом носителе выполняется с использованием программного обеспечения СКЗИ КриптоПро CSP.

Для этого запустите приложение КриптоПро CSP из панели управления (Control Panel) и выберите вкладку **Сервис**.

На указанной вкладке нажмите кнопку **Удалить контейнер** (см. Рисунок 57).

Рисунок 57. Вкладка "Сервис" приложения КриптоПро CSP



12. Смена ключей Центра регистрации

Смена ключей Центра Регистрации осуществляется в соответствии с регламентом Удостоверяющего Центра.

Смена ключей Центра Регистрации выполняется в следующем порядке:

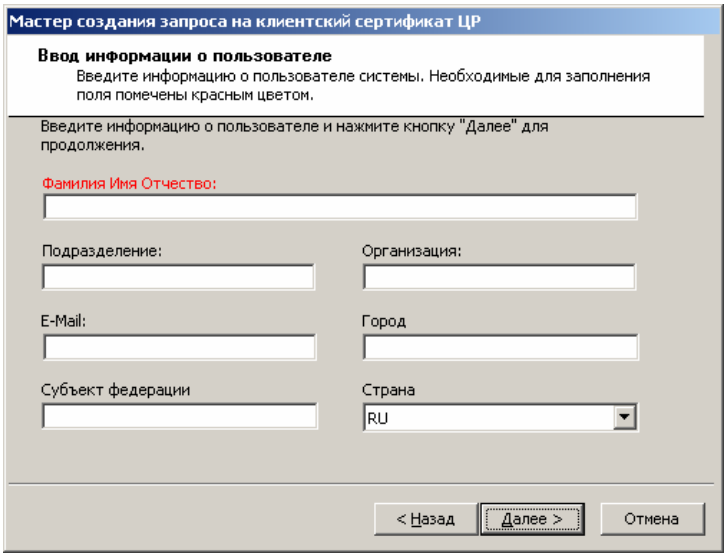
1. Генерация новых ключей и создание запроса на сертификат Центра Регистрации;
2. Выпуск нового сертификата Центра Регистрации;
3. Добавление нового сертификата в список доверенных ЦР на Центре сертификации;
4. Удаление старого сертификата из списка доверенных ЦР на Центре сертификации;
5. Установка нового сертификата Центра Регистрации;
6. Изменение параметра настройки Центра регистрации;
7. Уничтожение старых ключей на Центре регистрации;

12.1. Генерация новых ключей и создание запроса на сертификат Центра Регистрации

Генерация новых ключей и формирование запроса на сертификат Центра регистрации (сертификат с клиентской аутентификацией) осуществляется с использованием программы-утилиты **Запрос клиентского сертификата ЦР** из состава программного обеспечения Центра регистрации (группа **Крипто-Про**). Данное приложение представляет собой Мастер, который обеспечит выполнение всех необходимых действий. Действия выполняются в следующем порядке:

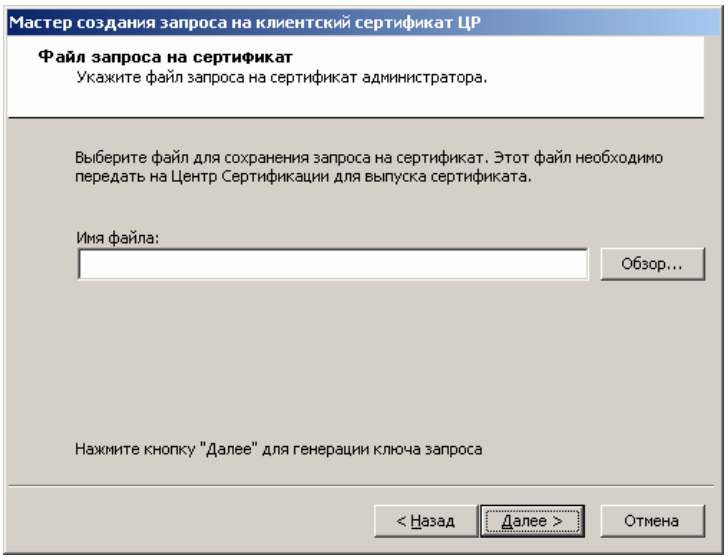
1. В окне ввода информации о пользователе введите информацию о владельце ключей и сертификата, которые будут использоваться во взаимодействии с Центром сертификации УЦ (см. Рисунок 58).

Рисунок 58. Окно ввода информации о пользователей Мастера клиентского сертификата ЦР



2. Следующим диалоговым окном Мастера является окно, в котором требуется определить имя и размещения файла, где будет сохранен запрос на сертификат Центра регистрации (см. Рисунок 59).

Рисунок 59. Окно определения файла запроса Мастера клиентского сертификата ЦР



3. Для генерации ключей и формирования файла нажмите кнопку **Далее**.

12.2. Выпуск нового сертификата Центра Регистрации

Выпуск сертификата Центра регистрации осуществляется на Центре сертификации в соответствии с руководством по эксплуатации Центра сертификации.

12.3. Добавление нового сертификата в список доверенных ЦР на Центре сертификации

Добавление сертификата Центра регистрации в список доверенных ЦР осуществляется на Центре сертификации в соответствии с руководством по эксплуатации Центра сертификации.

12.4. Удаление старого сертификата из списка доверенных ЦР на Центре сертификации

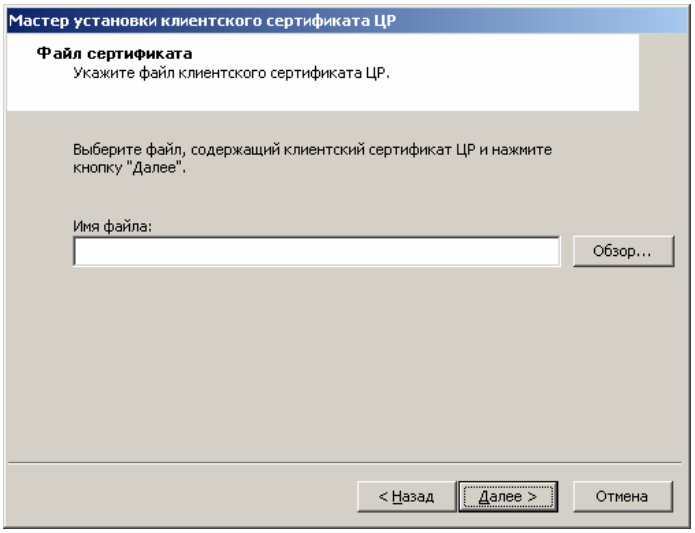
Удаление старого сертификата Центра регистрации из списка доверенных ЦР осуществляется на Центре сертификации в соответствии с руководством по эксплуатации Центра сертификации.

12.5. Установка нового сертификата Центра Регистрации

Установка выпущенного сертификата, полученного из Центра сертификации в виде файла, осуществляется с использованием Мастера установки клиентского сертификата ЦР из группы **Крипто-Про**.

В диалоговом окне Мастера определите имя файла, полученного в Центре сертификации и содержащего выпущенный сертификат Центра регистрации (см. Рисунок 60).

Рисунок 60. Окно выбора файла в Мастере установки клиентского сертификата ЦР



В следующем окне отобразится информация о сертификате, содержащемся в выбранном файле. Убедитесь в правильности выбора файла и сертификата и нажмите кнопку **Далее**.

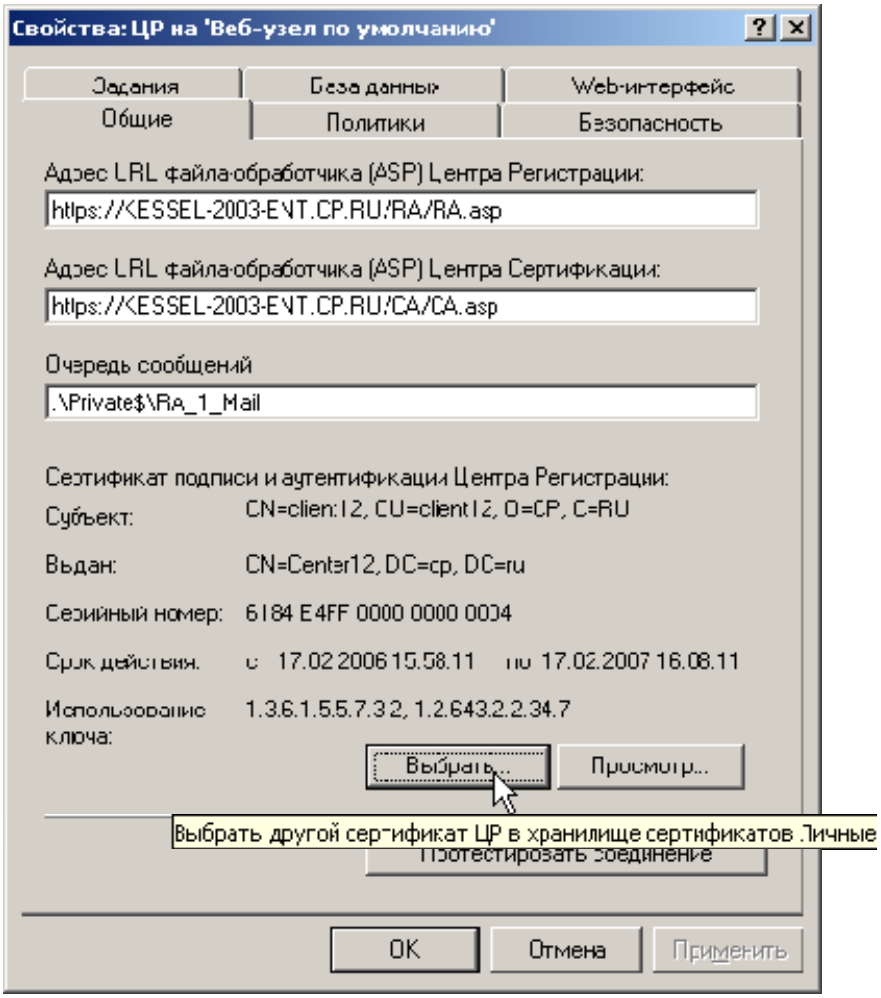
После этих действий будет произведена установка сертификата в раздел **Личные** хранилища сертификатов локального компьютера.

12.6. Изменение параметра настройки Центра регистрации

Изменение настройки Центра регистрации выполняется для смены значения параметра, определяющего сертификат, используемый для установления соединения с Центром сертификации.

Выбор сертификата Центра регистрации осуществляется на вкладке **Общие** свойств узла Центра регистрации (см. Рисунок 61). Для выбора нового сертификата Центра регистрации нажмите кнопку **Выбрать**.

Рисунок 61. Выбор нового сертификата Центра регистрации на вкладке Общие свойств узла Центра регистрации



После смены сертификата Центра регистрации нажмите кнопку **Применить** и протестируйте соединение с использование кнопки **Протестировать соединение**.

12.7. Уничтожение старых ключей на Центре регистрации

Уничтожение старых ключей Центра регистрации на ключевом носителе выполняется с использованием программного обеспечения СКЗИ КриптоПро CSP.

Для этого запустите приложение КриптоПро CSP из панели управления (Control Panel) и выберите вкладку **Сервис**.

На указанной вкладке нажмите кнопку **Удалить контейнер** (см. Рисунок 57).

13. Обеспечение целостности программных средств Центра Регистрации

Система контроля целостности программных компонентов Центра Регистрации основывается на аппаратном контроле целостности программных модулей Центра Регистрации и общесистемного программного обеспечения до загрузки операционной системы.

Данная система контроля целостности обеспечивается использованием сертифицированного устройства типа электронный замок.

Периодичность контроля целостности программных компонентов Центра Регистрации – ежесуточно. Выполняется путем перезапуска операционной системы компьютера Центра Регистрации.

В состав программных модулей Центра Сертификации, подвергающихся контролю целостности входят:

Наименование модуля	**Расположение (по умолчанию)**
RAConfig.msc	..:\Program Files\Crypto Pro\RA\bin
Все файлы *.dll каталога	..:\Program Files\Crypto Pro\RA\bin
Все файлы *.exe каталога	..:\Program Files\Crypto Pro\RA\bin
Все файлы *.dll каталога	..:\Program Files\Common Files\Crypto Pro\Shared
Все файлы *.exe каталога	..:\Program Files\Common Files\Crypto Pro\Shared
Все файлы каталога без подкаталогов	..:\Documents and Settings\All Users\Application Data\Crypto Pro\RA\Inetpub\1\RA
Все файлы каталога и подкаталогов	..:\Documents and Settings\All Users\Application Data\Crypto Pro\RA\Inetpub\1\UI
Все файлы каталога без подкаталогов	..:\Documents and Settings\All Users\Application Data\Crypto Pro\RA\Inetpub\<идентификатор веб-узла>\RA
Все файлы каталога и подкаталогов	..:\Documents and Settings\All Users\Application Data\Crypto Pro\RA\Inetpub\<идентификатор веб-узла>\UI

Идентификатор веб-узла – это целое число, которое IIS присваивает при создании веб-узла. Для «веб-узла по умолчанию» значение идентификатора равно 1. Контроль целостности осуществляется для тех значений идентификаторов веб-узлов, на которые ставились компоненты дополнительных модулей доступа ЦР.

Контроль целостности программных компонентов средств СКЗИ, используемых в Центре Регистрации, осуществляется средствами самого СКЗИ.

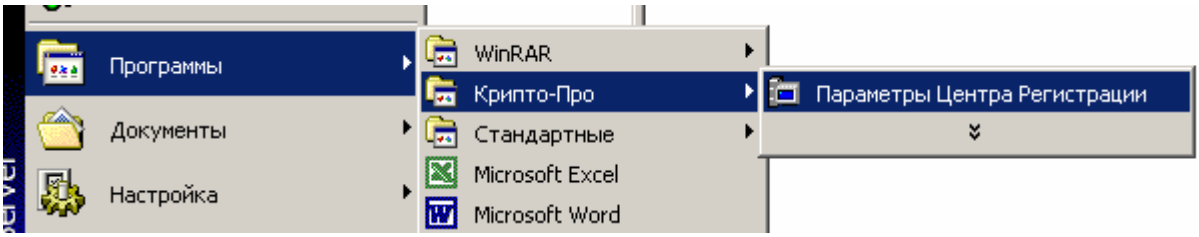
14. Приложение «Параметры Центра Регистрации»

Приложение «Параметры Центра Регистрации» является основным средством настройки ПО Центра Регистрации и управления его работой. Ряд задач, выполняемых с использованием данного приложения, описывается в предыдущих разделах настоящего Руководства.

14.1. Запуск приложения

Запуск приложения «Параметры Центра Регистрации» осуществляется из группы **Крипто-Про** пункта меню **Программы** кнопки **Пуск** (см. рисунок ниже).

Рисунок 62. Запуск приложения "Параметры Центра Регистрации"

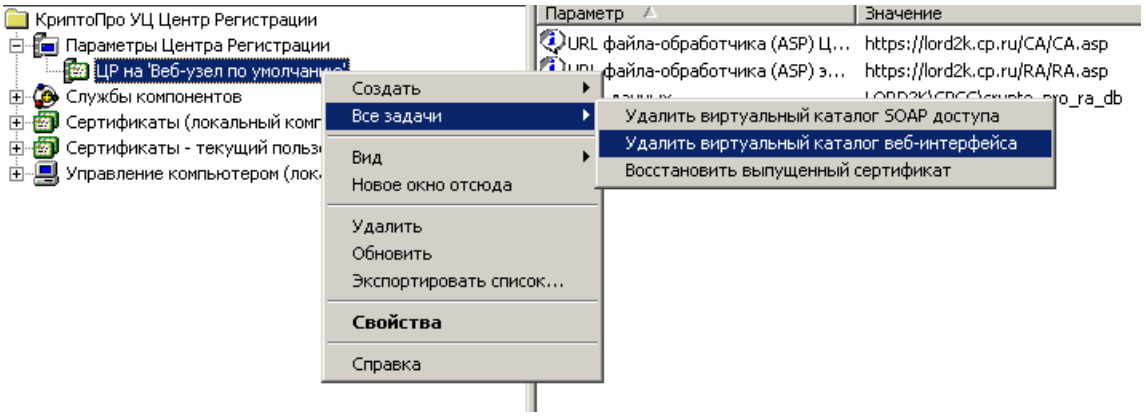


14.2. Удаление виртуального каталога веб-интерфейса

Удаление виртуального каталога веб-интерфейса выполняется в случае, когда предоставление услуг удостоверяющего центра осуществляется без предоставления пользователям доступа к ПО Центра Регистрации посредством использования приложений АРМ пользователя. Т.е. когда не используется распределенный режим регистрации пользователей и распределенный режим управления ключами и сертификатами. В этом случае рекомендуется удалить виртуальный каталог, содержащий приложения, реализующие АРМы пользователя, с сервера Центра Регистрации.

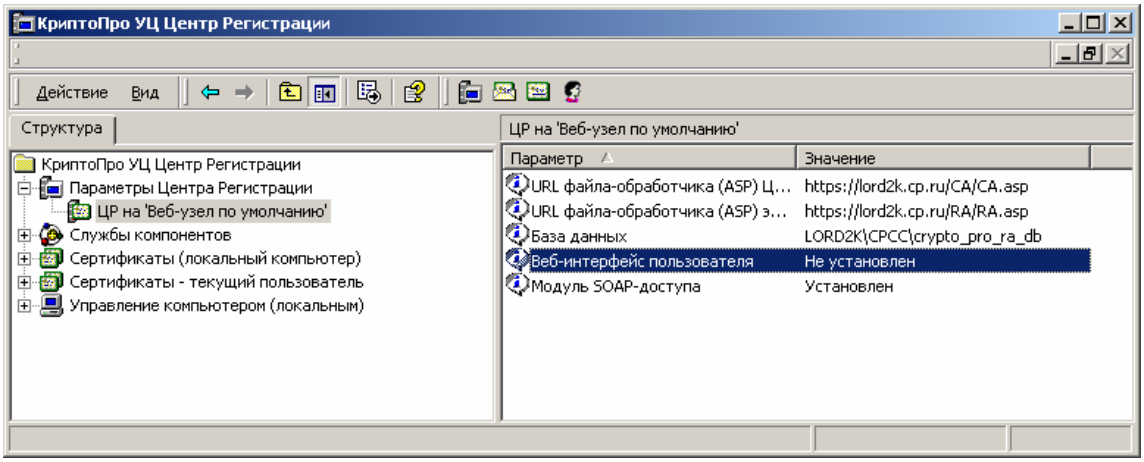
Для запуска задачи удаления виртуального каталога указателем манипулятора типа «мышь» выберите соответствующий модуль доступа, нажмите правую кнопку мыши и в группе **Все задачи** контекстного меню запустите задачу **Удалить виртуальный каталог веб-интерфейса**.

Рисунок 63. Запуск задачи удаление виртуального каталога веб-интерфейса



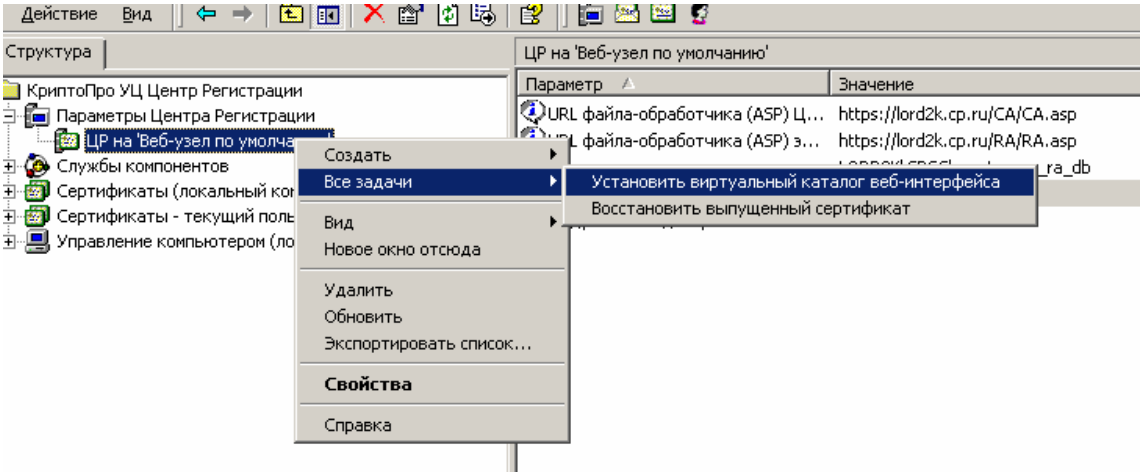
Выполнение данной задачи осуществляется в неинтерактивном режиме с выводом окна, отображающим ход выполнения задачи.

По завершении задачи, состояние параметра **Веб-интерфейс пользователя** будет установлено в значение **Не установлен**.



В случае необходимости восстановления возможности доступа пользователей к ресурсам Центра Регистрации посредством приложений АРМ пользователя, требуется выполнить задачу **Установить виртуальный каталог веб-интерфейса**.

Рисунок 64. Запуск задачи установки виртуального каталога веб-интерфейса



При выполнении этой задачи будет затребован ввод пароля для учетной записи **CPRAComPlusAcct**.

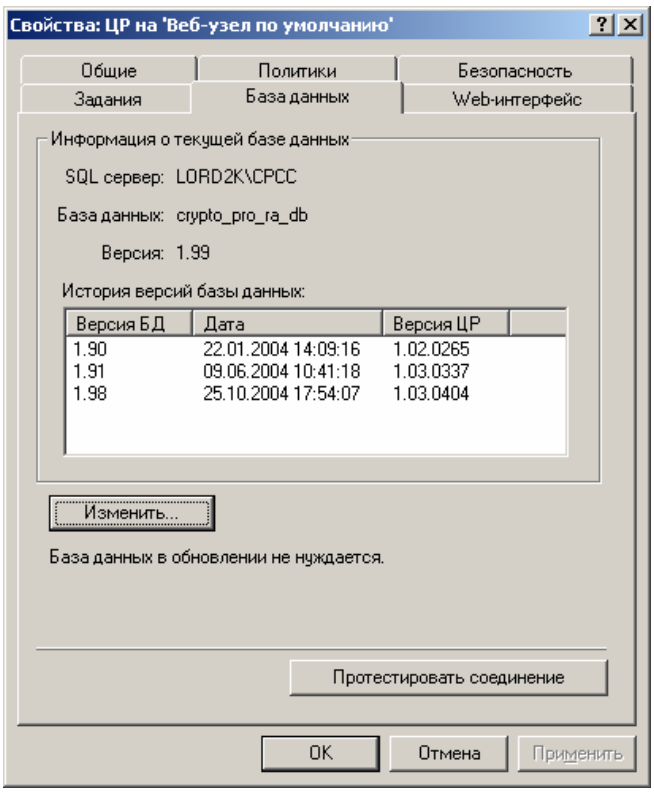
Важно отметить, что если при установке ПО Центра Регистрации был выбран вид установки **Выборочная** и при этом виртуальный каталог веб-интерфейса не был отмечен к установке, то установить виртуальный каталог веб-интерфейса представляется возможным только путем переустановки ПО Центра Регистрации полностью. Поэтому рекомендуется при установке ПО Центра Регистрации не отключать установку виртуального каталога веб-интерфейса, а потом (если он не нужен) удалять его.

14.3. Создание новой (пустой) базы данных Центра Регистрации

Функционал создания приложения «Параметры Центра Регистрации» позволяет создание новой базы данных Центра Регистрации. Под новой базой Центра Регистрации понимается база данных на экземпляре MSDE либо MS SQL Server 2000, с созданной структурой и занесенными служебными записями. Причины, требующие создания новой базы, могут быть разнообразны. Это опциональная возможность.

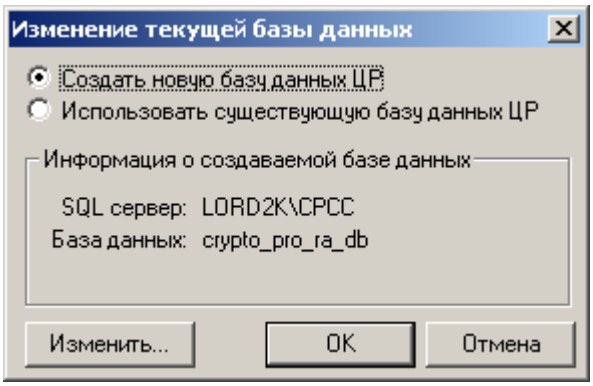
14.3.1. Создание новой базы данных в экземпляре CPCC для MSDE

Откройте окно свойств соответствующего модуля доступа приложения «Параметры Центра Регистрации» и перейдите на вкладку **База данных**.



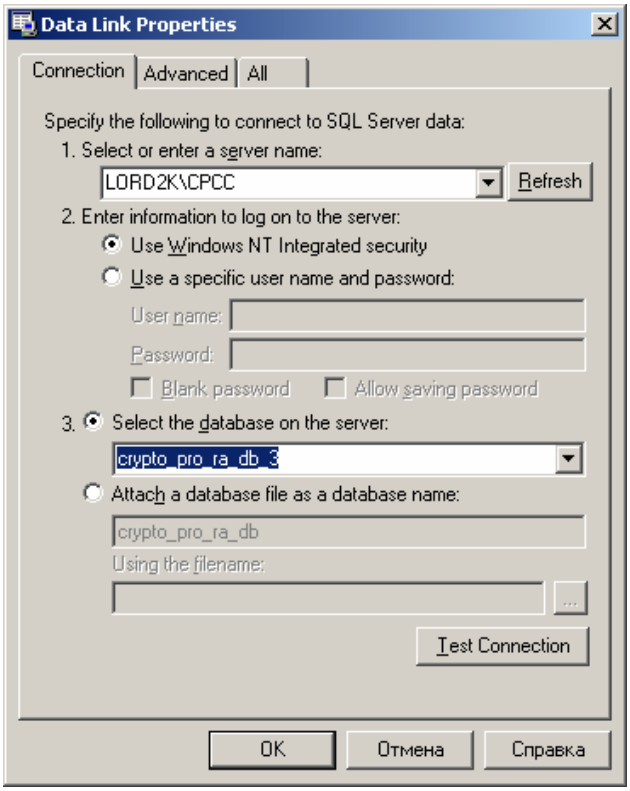
Нажмите кнопку **Изменить** и появившемся окне, выбрав опцию **Создать новую базу данных ЦР**, нажмите кнопку **Изменить**.

Рисунок 65. Окно изменения текущей базы данных с опцией «Создать новую базу данных ЦР»



В окне свойств соединения с базой данных (см. Рисунок 66) введите имя новой базы данных и нажмите кнопку **ОК**.

Рисунок 66. Окно свойств соединения с базой данных (Связь с данными)



В окне **Изменение текущей базы данных** нажмите также кнопку **ОК**. Выполниться задача создания новой базы данных.

14.3.2. Создание новой базы данных в экземпляре MS SQL Server 2000

Создание новой базы данных Центра Регистрации в экземпляре MS SQL Server 2000 практически не отличается от создания БД в экземпляре MSDE, описанной в предыдущем пункте, за исключением того, что пустая база данных должна быть предварительно создана на SQL Server штатным способом. Имя этой новой базы вводится на окне свойств соединения базы данных (см. Рисунок 66).

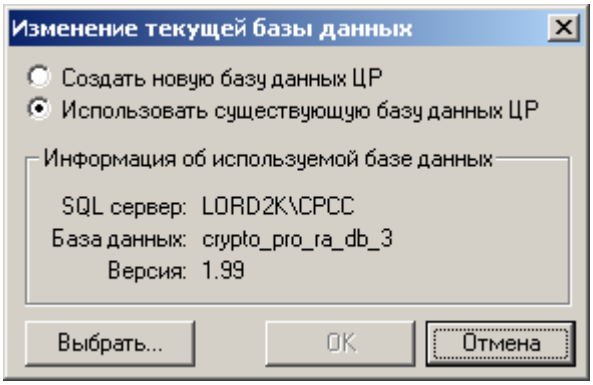
14.4. Изменение базы данных

Изменение текущей базы данных Центра Регистрации («перенаправление» ее на другую базу данных, предварительно созданную) осуществляется следующим способом.

Откройте окно свойств соответствующего модуля доступа приложения «Параметры Центра Регистрации» и перейдите на вкладку **База данных**.

Нажмите кнопку **Изменить** в появившемся окне (см. Рисунок 67), выбрав опцию **Использовать существующую базу данных ЦР**, нажмите кнопку **Выбрать**.

Рисунок 67. Окно изменения текущей базы данных с опцией «Изменить существующую базу данных ЦР»



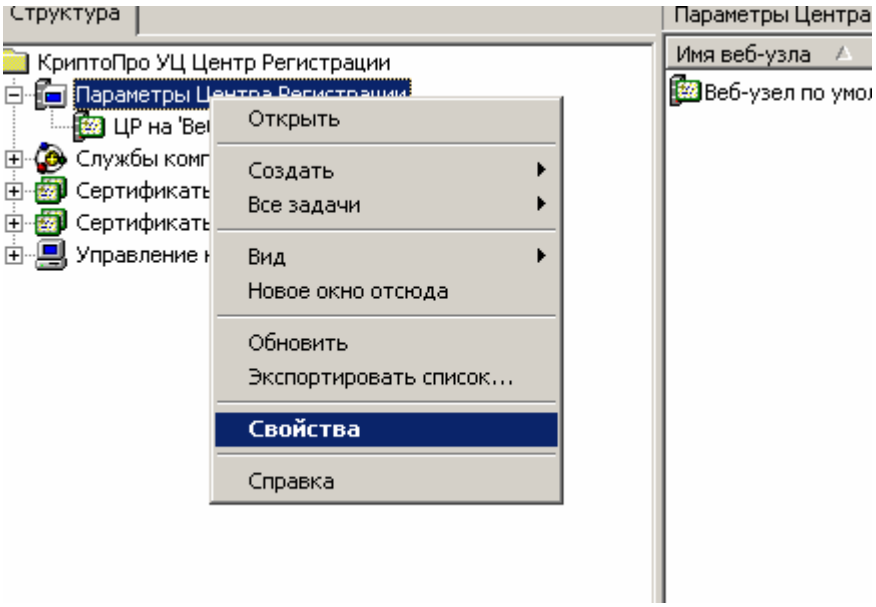
В следующем окне установки свойств соединения выберите нужную базу данных и нажмите кнопку **ОК**. В окне изменения текущей базы данных также нажмите кнопку **ОК**. Выполнится задача создания новой базы данных

14.5. Установка (ввод параметров) лицензии

Установка (ввод параметров) лицензии на право пользования компонентами Центра Регистрации осуществляется тогда, когда не был осуществлен ввод наименования организации и серийного номера лицензии при установке ПО Центра Регистрации или производится изменение лицензионных данных (изменение лицензии).

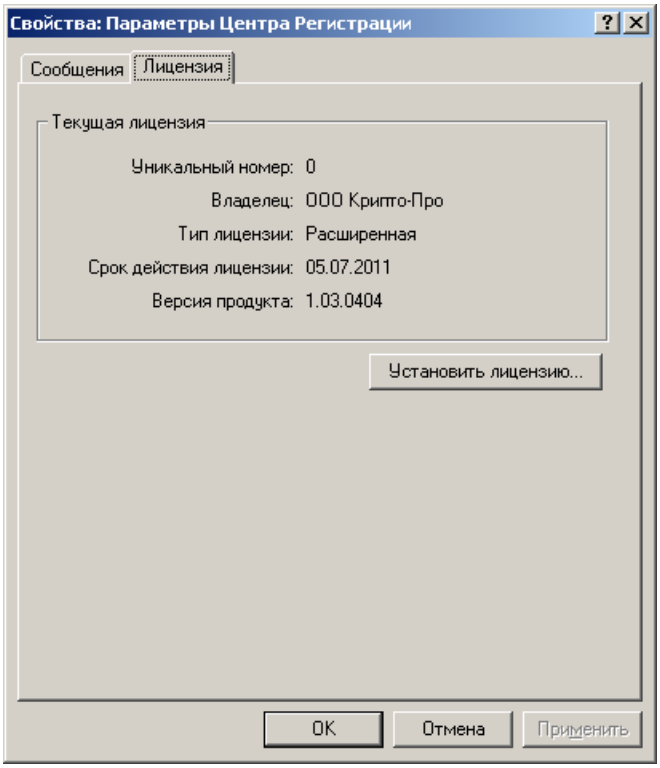
Для выполнения этой процедуры выполните следующие действия:

В приложении «Параметры Центра Регистрации» откройте окно свойств приложения (см. рисунки ниже).

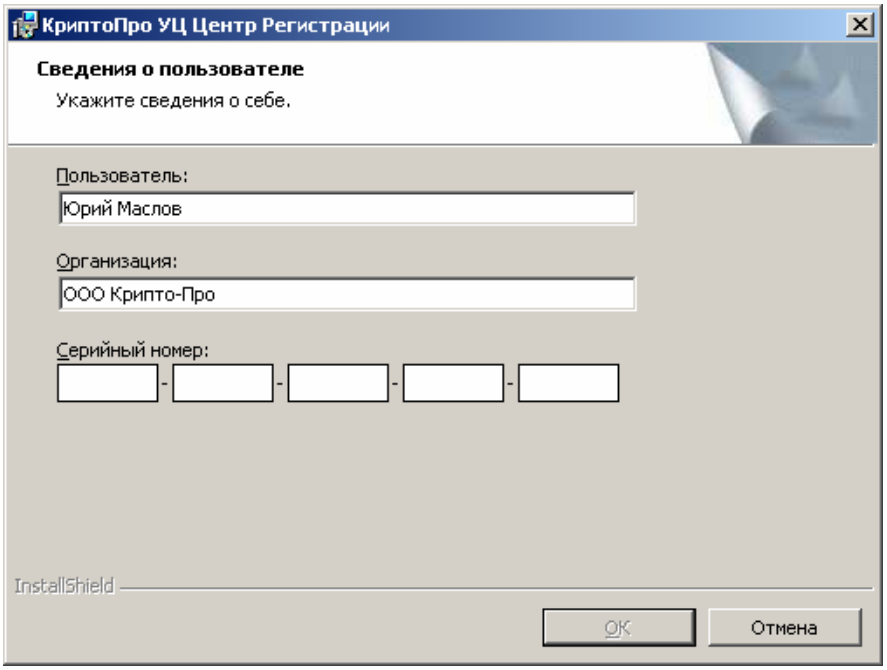


Перейдите на вкладку **Лицензия** окна свойств приложения «Параметры Центра Регистрации» и нажмите кнопку **Установить лицензию**.

Рисунок 68. Вкладка "Лицензия" окна свойств приложения "Параметры Центра Регистрации"



В окне ввода сведений о пользователе введите наименование организации и серийный номер из лицензии и нажмите кнопку **ОК**.



15. Настройка репликации базы данных Центра Регистрации КриптоПро УЦ

Репликация позволяет осуществлять резервное копирование базы данных Центра Регистрации КриптоПро УЦ в реальном времени. Центр Регистрации может продолжить работу с резервной копией в случае отказа основной базы (например, по причине аппаратного сбоя на сервере баз данных). Поддерживается транзакционная модель репликации. В репликации принимают участие две стороны: издатель и подписчик. Издателем является сервер, на котором расположена основная база данных Центра Регистрации. Подписчиком является сервер, на котором располагается резервная копия базы данных Центра Регистрации.

Основная база данных Центра Регистрации (которая располагается на издателе) должна находиться под управлением MS SQL Server Standard Edition или MS SQL Server Enterprise Edition (это ограничение связано с тем, что MS SQL Server Desktop Edition не поддерживает транзакционную репликацию).

На подписчике должен быть установлен SQL Server любой редакции (включая MSDE).

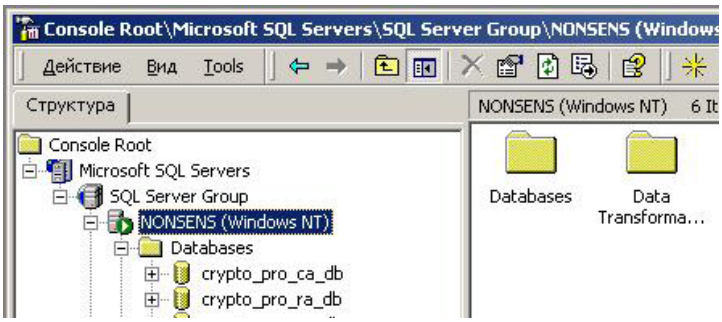
15.1. Предварительное конфигурирование издателя

15.1.1. Настройка публикации и распространения

Запустите SQL Server Enterprise Manager (**Пуск – Программы - Microsoft SQL Server - Entrprise Manager**).

Выберите в дереве SQL Server, на котором планируется настраивать параметры публикации и распространения.

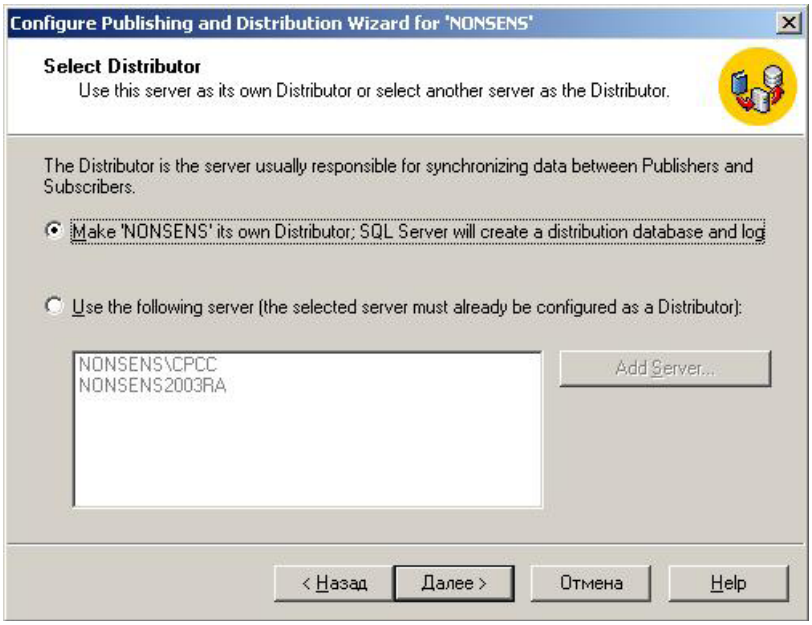
Рисунок 69. Выбор сервера



В меню Tools выберите Replication - Configure Publishing, Subscribers and Distribution. Появится главное окно мастера настройки публикации, подписчиков и распространения. Пропустите начальную страницу, щелкнув Далее.

Выберите переключатель Make '<имя вашего сервера>' its own Distributor; SQL Server will create a distribution database and log, если хотите, чтобы сервер Центра Регистрации был своим собственным распространителем. В противном случае выберите другой переключатель (см. Рисунок 70). Щелкните Далее.

Рисунок 70. Выбор распространителя



Укажите папку, в которой будут храниться снимки данных (см. Рисунок 71). Можно оставить папку по умолчанию, не обращая внимания на предупреждение, которое в этом случае может быть выдано. Нажмите Далее.

Рисунок 71. Папка для снимков данных

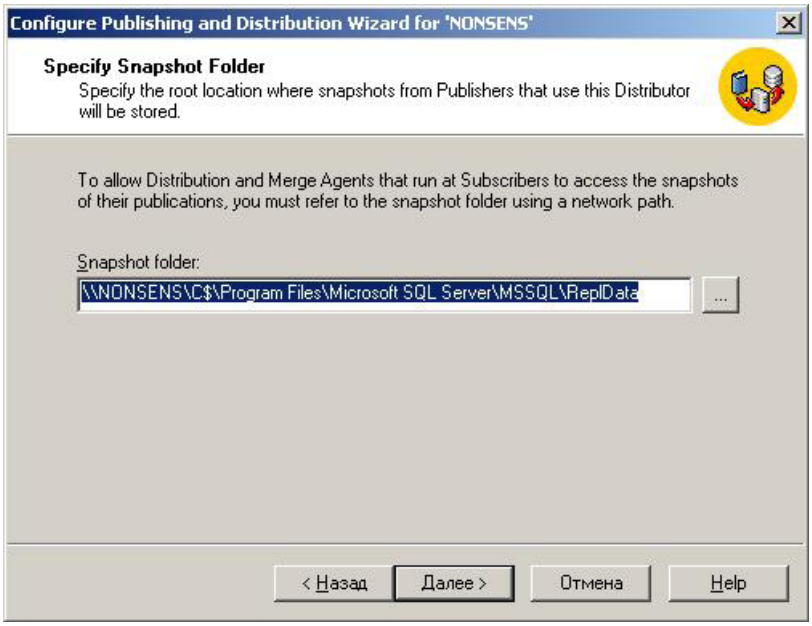
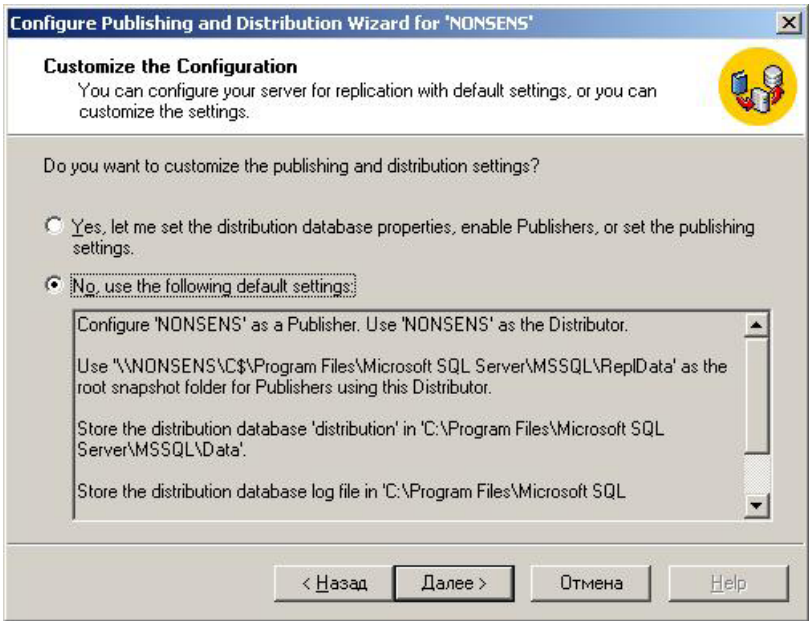


Рисунок 72. Окно настроек публикации и распространения



Выберите переключатель No, use the following parameters, чтобы оставить остальным параметрам значения по умолчанию, в противном случае выберите другой переключатель (см. Рисунок 72). Щелкните Далее

На завершающей странице мастера щелкните кнопку **Finish**

15.1.2. Настройка учетной записи службы SQL Server Agent

Назначьте службе SQL Server Agent учетную запись, которая имеет достаточно полномочий для входа на компьютер подписчика и подключения к SQL Server. Она должна быть членом роли db_owner базы данных подписчика. Если компьютеры издателя и подписчика находятся в одном домене, целесообразно запускать SQL Server Agent от имени специально созданной доменной учетной записи. Если компьютеры находятся в разных доменах (или вовсе не в доменах), то необходимо завести на каждом из них учетные записи с совпадающими именами и паролями и наделить их соответствующими полномочиями.

15.2. Предварительное конфигурирование подписчика

Создайте пустую базу данных. Эта база будет приемником. Рекомендуется, чтобы ее имя совпадало с именем основной базы данных Центра Регистрации (по умолчанию — crypto_pro_ra_db). Позаботьтесь о том, чтобы учетная запись, от имени которой работает SQL Server Agent издателя была членом группы db_owner (см. п. 15.1.2).

15.3. Настройка репликации

Для автоматизации настройки репликации базы данных Центра Регистрации используется сценарий RA_ConfigureReplication.vbs и соответствующий файл RA_PatchSubscriber*.sql (см. Таблица 7). Файлы расположены в папке **\Program Files\Crypto Pro\RA\scripts**. Сценарий запускается при помощи интерпретатора cscript. Запускать сценарий необходимо на издателе. Сценарий принимает следующие параметры:

- имя экземпляра SQL Server, на котором находится основная БД Центра регистрации (издатель);
- имя базы данных Центра регистрации;
- имя экземпляра SQL Server подписчика;
- имя базы данных подписчика;

- имя учетной записи для подключения к SQL Server подписчика*;
- пароль учетной записи для подключения к SQL Server подписчика*.

* Звездочкой помечены необязательные параметры. Они нужны только в случае, если учетная запись, от имени которой запускается сценарий, не имеет доступа к SQL Server подписчика. В этом случае указывайте встроенную учетную запись sa и ее пароль.

Таблица 7. Перечень файлов для настройки репликации

Имя файла	Комментарии
RA_ConfigureReplication.vbs	Настраивает транзакционную репликацию базы данных Центра регистрации
RA_PatchSubscriber.sql	Необходим для работы RA_ConfigureReplication.vbs. Приводит базу данных подписчика в надлежащее состояние. Должен находиться в одном каталоге с RA_ConfigureReplication.vbs.
RA_PatchSubscriber_108.sql	Для базы данных от версии 108 и старше.

Примеры:

cscript RA_ConfigureReplication.vbs PRODUCTION_SRV crypto_pro_ra_db BACKUP_SRV crypto_pro_ra_db

cscript RA_ConfigureReplication.vbs PRODUCTION_SRV crypto_pro_ra_db BACKUP_SRV crypto_pro_ra_db sa qwerTYUI

16. Удаление программного обеспечения Центра регистрации

Удаление программного обеспечения Центра регистрации осуществляется в следующем порядке:

1. Удаление компоненты «КриптоПро УЦ - Центр регистрации»;
2. Удаление приложений «Утилиты Центра регистрации»;
3. Удаление служб Microsoft Internet Information Services и службы очереди сообщений;
4. Удаление сертификата Веб-сервера Центра регистрации и клиентского сертификата Центра регистрации из хранилища сертификатов локального компьютера и уничтожение соответствующих этим сертификатам закрытых ключей - выполняется в том случае, если в дальнейшем нет необходимости их применения, либо срок действия данных закрытых ключей истек.
5. Удаление сертификата Центра сертификации (уполномоченного лица удостоверяющего центра) из соответствующего хранилища доверенных сертификатов центров сертификации - выполняется в том случае, если в дальнейшем нет необходимости применения данного сертификата для построения цепочки сертификатов пользователей удостоверяющего центра на компьютере Центра регистрации.
6. Удаление СКЗИ КриптоПро CSP (КриптоПро TLS) - выполняется в том случае, если в дальнейшем на компьютере Центра регистрации отсутствует необходимость использования СКЗИ.

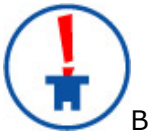
Удаление компоненты «КриптоПро УЦ – Центр регистрации», «Утилиты Центра регистрации» и СКЗИ «КриптоПро CSP» осуществляется с использованием сервиса **Установка и удаления программ**, запускающегося из **Панели управления компьютера**. Для удаления необходимой компоненты, выделите ее левой кнопкой мыши и нажмите на кнопку **Удалить**.

Удаление служб Microsoft Internet Information Services и службы очереди сообщений осуществляется с использованием сервиса **Удаление компонент Windows**, путем снятия соответствующих флагов, определяющих наличие данного компонента в системе.

Удаление сертификата Веб-сервера Центра регистрации и клиентского сертификата Центра регистрации из хранилища сертификатов **Локальный компьютер/Личные** осуществляется с использованием интерфейса консоли **mmc** и изолированной оснастки **Сертификаты**. Удаление закрытых ключей, соответствующих данным сертификатам, осуществляется штатными средствами используемого СКЗИ.

Удаление сертификата Центра сертификации (уполномоченного лица удостоверяющего центра) из хранилища сертификатов **Локальный компьютер/Доверенные корневые центры сертификации** (если удостоверяющий центр – корневой), либо **Локальный компьютер/Промежуточные центры сертификации** (если удостоверяющий центр – подчиненный) осуществляется с использованием интерфейса консоли **mmc** и изолированной оснастки **Сертификаты**.

При удалении программного обеспечения Центра регистрации База данных Центра регистрации и средства управления базами данных (Microsoft SQL Server или MSDE) не удаляются. База данных остается в том самом месте расположения на жестком диске, где она была создана при первой установке программного обеспечения Центра регистрации. Файлы Базы данных Центра регистрации не удаляются автоматически и при удалении средства управления базами данных (Microsoft SQL Server или MSDE). Создание новой Базы данных (пустой) или подключение другой осуществляется в порядке, определенном соответствующими разделами настоящего документа.



В случае повторной инсталляции программного обеспечения на данный компьютер (компьютер, на котором ранее было установлено программное обеспечение Центра регистрации), в том случае если место расположения на жестком диске Базы данных Центра регистрации не изменялось, программа установки обнаружит существующую Базу данных и автоматически ее подключит в качестве актуальной Базы данных Центра регистрации.

В данном случае пользователи удостоверяющего центра, при условии наличия на Центре регистрации установленного сертификата Центра сертификации и актуального списка отозванных сертификатов, смогут получить доступ к своей персональной странице посредством **АРМ пользователя** и указанием ссылки **Вход для зарегистрированных пользователей**.

При этом если программное обеспечение Центра сертификации также было удалено (либо удалено и восстановлено, но с созданием новой Базы данных Центра сертификации), то пользователи, а также любой привилегированный пользователь, не смогут аннулировать (отозвать) и приостановить действие сертификатов, содержащихся в Базе данных Центра регистрации.

17. Перечень сокращений

CRL	Список отозванных сертификатов (Certificate Revocation List)
DN	Отличительное имя (Distinguished Name)
ITU-T	Международный комитет по телекоммуникациям (International Telecommunication Union)
IETF	Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol.
	Упрощенный протокол доступа к справочнику
TM	Устройство хранения информации на таблетке touch-memory
PKI	Public Key Infrastructure. Аналог ИОК.
RDN	Относительное отличительное имя (Relative Distinguished Name)
URI	Единый идентификатор ресурса (Uniform Resource Identifier)
URL	Единый локатор ресурса (Uniform Resource Locator)
АС	Автоматизированная система
АРМ	Автоматизированное рабочее место
ДСЧ	Датчик случайных чисел
ИОК	Инфраструктура Открытых Ключей
КП	Конечный пользователь
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СОС	Список отозванных сертификатов (Certificate Revocation List)
СС	Справочник сертификатов открытых ключей. Сетевой справочник
ЦР	Центр Регистрации
ЦС	Центр Сертификации
ЭЦП	Электронная цифровая подпись
УЦ	Удостоверяющий Центр

18. Перечень рисунков

Рисунок 1. Схема взаимодействия компонентов Центра регистрации 5
Рисунок 2. Пункт "Свойства" узла Центра Регистрации 7
Рисунок 3. Вкладка "Безопасность" свойств узла Центра регистрации 18
Рисунок 4. Вкладка "Задания" свойств узла Центра регистрации 19
Рисунок 5. Вкладка "База данных" свойств узла Центра Регистрации 20
Рисунок 6. Вкладка "Web-интерфейс" свойств узла Центра Регистрации 22
Рисунок 7. Пункт "Свойства" Параметры Центра Регистрации 23
Рисунок 8. Окно компонент рассылки сообщений 24
Рисунок 9. Окно настройки параметров компоненты CDO 24
Рисунок 10. Окно Мастера создания Web-узлов 25
Рисунок 11. Пример установки TCP-порта и порта SSL для Web-узла 26
Рисунок 12. Окно свойств безопасных подключений Web-узла модуля доступа ЦР 27
Рисунок 13. Запуск задачи создания модуля доступа ЦР 27
Рисунок 14. Окно выбора Web-узла Мастера создания нового модуля доступа 28
Рисунок 15. Окно ввода пароля учетной записи Центра Регистрации Мастера создания нового модуля доступа к ЦР 28
Рисунок 16. Окно определения параметров в Мастере создания нового модуля доступа к ЦР ... 29
Рисунок 17. Окно завершения работы Мастера создания нового модуля доступа к ЦР 29
Рисунок 18. Запуск задачи удаления модуля доступа Центра Регистрации 30
Рисунок 19. Окно подтверждения удаления модуля доступа ЦР 30
Рисунок 20. Окно программы установки Центра Регистрации Крипто-Про УЦ при удалении модуля доступа 30
Рисунок 21. Окно Мастера установки Центра Регистрации Крипто-Про УЦ при завершении удаления модуля доступа 31
Рисунок 22. Окно свойств компонента Связь с данными 32
Рисунок 23. Окно свойств компонента Связь с данными 33
Рисунок 24. Вкладка "Политики" свойств узла Центра Регистрации 34
Рисунок 25. Окно элемента разрешений для действия Центра регистрации 43
Рисунок 26. Окно выбора роли при создании элемента разрешений 43
Рисунок 27. Окно свойств элемента разрешений 43
Рисунок 28. Окно свойств расписания регламентного задания Центра Регистрации 48
Рисунок 29. Идентификатор области использования ключа подчиненных УЦ 49
Рисунок 30. Схема взаимодействия заданий публикации COC на ЦС и ЦР 50
Рисунок 31. Окно свойств заданий публикации COC 52
Рисунок 32. Окно настройки задания публикации COC 53
Рисунок 33. Окно свойств задания рассылки сообщения из пакета задания публикации COC .. 53
Рисунок 34. Окно MMC консоли "Active Directory Users and Computers" 55
Рисунок 35. Вызов окна настройки модуля экспорта сертификатов 55

Рисунок 36. Окно настройки модуля экспорта сертификатов 56
Рисунок 37. Запуск Мастера регистрации SQL сервера в консоли Enterprise Manager 58
Рисунок 38. Создание нового пакета Meta Data Services 58
Рисунок 39. Запуск задания Transfer Database Task 59
Рисунок 40. Вкладка Source свойств задания Transfer Database Task 59
Рисунок 41. Вкладка Destination свойств задания Transfer Database Task 60
Рисунок 42. Вкладка Databases свойств задания Transfer Database Task 60
Рисунок 43. Запуск исполнения задания переноса базы данных 61
Рисунок 44. Окно свойств приложения Параметры Центра Регистрации 62
Рисунок 45. Окно параметров отправки почтовых сообщений (CDO) 63
Рисунок 46. Задача Создать Привилегированного пользователя 64
Рисунок 47. Окно выбора файла с запросом в Мастере создания привилегированного пользователя 65
Рисунок 48. Окно просмотра файла с запросом на сертификат привилегированного пользователя 65
Рисунок 49. Окно выбора файла записи сертификата Мастера создания привилегированного пользователя 66
Рисунок 50. Окно сообщения о создании привилегированного пользователя 66
Рисунок 51. Пример сообщения об ошибке Мастера создания привилегированного пользователя 67
Рисунок 52. Алгоритм проверки клиентского сертификата MS IIS 70
Рисунок 53. Окно свойств Web-узла Web-сервера MS IIS 75
Рисунок 54. Окно Мастера сертификатов Web-сервера 75
Рисунок 55. Окно изменения назначения сертификата Мастера сертификатов Web-сервера 76
Рисунок 56. Окно выбора сертификата для замены существующего в Мастере сертификатов Web-сервера 76
Рисунок 57. Вкладка "Сервис" приложения КриптоПро CSP 77
Рисунок 58. Окно ввода информации о пользователей Мастера клиентского сертификата ЦР 78
Рисунок 59. Окно определения файла запроса Мастера клиентского сертификата ЦР 79
Рисунок 60. Окно выбора файла в Мастере установки клиентского сертификата ЦР 80
Рисунок 61. Выбор нового сертификата Центра регистрации на вкладке Общие свойств узла Центра регистрации 81
Рисунок 62. Запуск приложения "Параметры Центра Регистрации" 83
Рисунок 63. Запуск задачи удаление виртуального каталога веб-интерфейса 83
Рисунок 64. Запуск задачи установки виртуального каталога веб-интерфейса 84
Рисунок 65. Окно изменения текущей базы данных с опцией «Создать новую базу данных ЦР» 85
Рисунок 66. Окно свойств соединения с базой данных (Связь с данными) 86
Рисунок 67. Окно изменения текущей базы данных с опцией «Изменить существующую базу данных ЦР» 87
Рисунок 68. Вкладка "Лицензия" окна свойств приложения "Параметры Центра Регистрации" 88
Рисунок 69. Выбор сервера 89
Рисунок 70. Выбор распространителя 90

Рисунок 71. Папка для снимков данных 90
Рисунок 72. Окно настроек публикации и распространения 91

19. Перечень таблиц

Таблица 1. Таблица допустимых действий Центра Регистрации 37
Таблица 2. Таблица прав доступа для роли Администратор 39
Таблица 3. Таблица прав доступа для роли Оператор 40
Таблица 4. Таблица прав доступа для роли Пользователь Центра Регистрации 42
Таблица 5. Таблица соответствия наименований заданий и файлов настройки 48
Таблица 6. Таблица соответствия наименований заданий публикации COC и файлов настройки 54
Таблица 7. Перечень файлов для настройки репликации 92

20. Перечень ссылочных документов

Удостоверяющий центр	Общее описание
Удостоверяющий центр	Руководство администратора
[SOAP]	Simple Object Access Protocol (SOAP) 1.1. World Wide Web Consortium. 08.05.2000
[X.509]	ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework, June 1997.
[RFC 2459]	RFC 2459. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", January 1999.

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопроводи-тельного документа и дата	Подпись	Дата
Изм.	изменен-ных	Заменен-ных	новых	аннули-рованных					