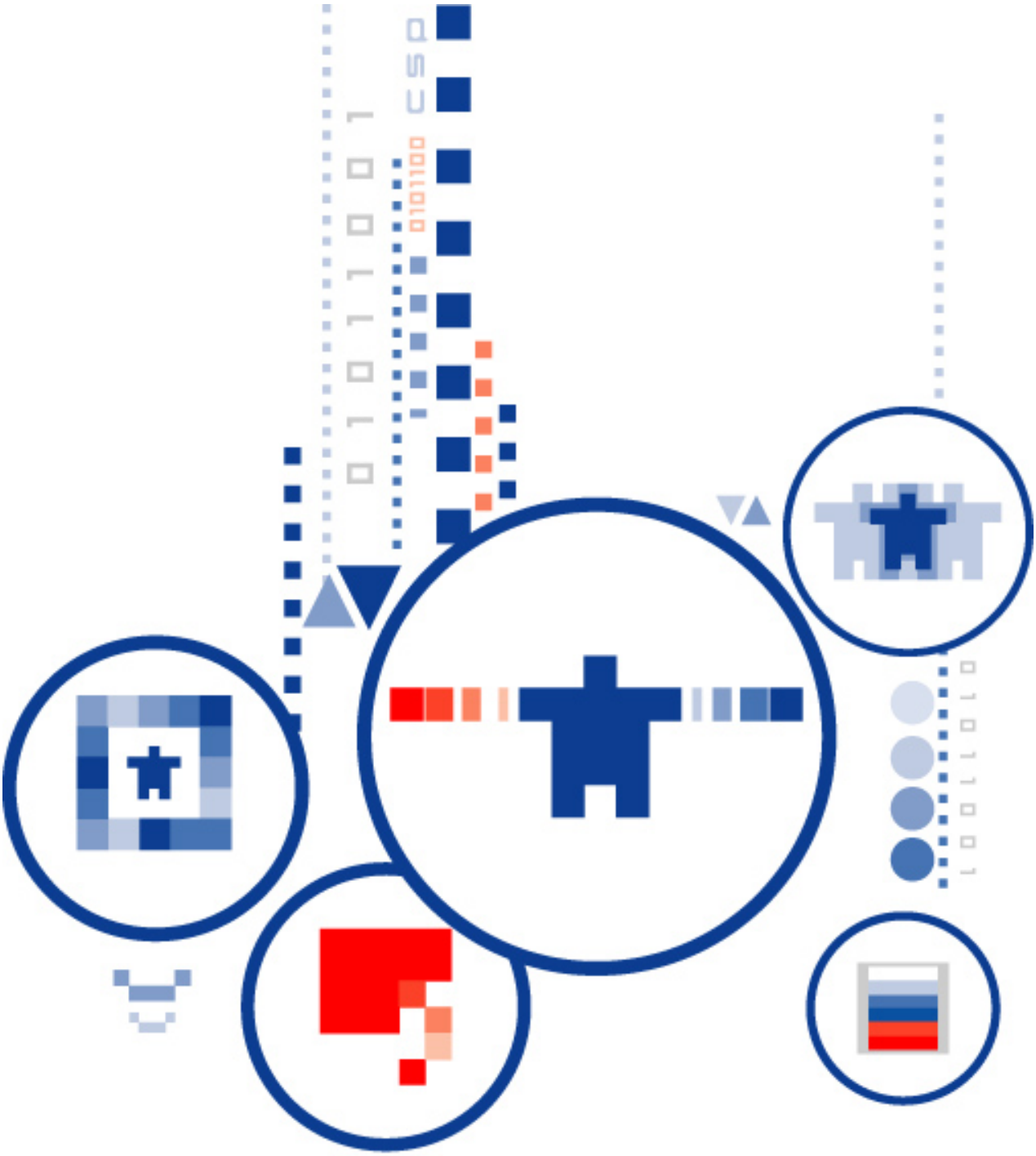
УТВЕРЖДЕН
ЖТЯИ.00035-01 90 04-ЛУ

ЖТЯИ.00035-01 90 04



КриптоПро УЦ

программно–аппаратный комплекс
удостоверяющий центр

Центр Сертификации. Руководство по эксплуатации на платформе Microsoft Windows 2000 Server

АННОТАЦИЯ

Настоящий документ содержит описание настройки и конфигурации программного компонента Центр Сертификации, входящего в состав программно-аппаратного комплекса «Удостоверяющий Центр «КриптоПро УЦ» (ПАК «КриптоПро УЦ»), и установленного на компьютере с операционной системой Microsoft Windows 2000 Server.

Конфигурация программного обеспечения ЦС выполняется в следующих случаях:

- после установки программного обеспечения ЦС;
- при подключении Центра (или Центров) регистрации в процессе установки программного обеспечения «Удостоверяющий центр»;
- при подключении следующих Центров регистрации при изменении конфигурации или масштабировании в процессе эксплуатации УЦ;
- при изменении параметров политики ЦС по выпуску сертификатов открытых ключей в процессе эксплуатации УЦ;
- при изменении параметров публикации списков отозванных сертификатов (CRL);
- при выполнении мероприятий по смене ключей аутентификации программного компонента Центра регистрации.

Конфигурация программного обеспечения ЦС заключается в настройке параметров работы следующих компонентов:

- Модуль выхода КриптоПро УЦ службы сертификации ЦС
- Модуль политики КриптоПро УЦ службы сертификации ЦС
- Приложение «Параметры Центра Сертификации»

Настоящий документ предназначен для администраторов как руководство по настройки и конфигурации Центр Сертификации.

Информация о разработчике ПАК «КриптоПро УЦ»:

ООО "Крипто-Про"

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

Телефон: (495) 780 4820

Факс: (495) 780 4820

http://www.CryptoPro.ru

E-mail: info@CryptoPro.ru

СОДЕРЖАНИЕ

1. Настройка модуля выхода КриптоПро УЦ службы сертификации ЦС 5

1.1. Пример настройки расписания СОС при организации работы удостоверяющего центра 9

2. Настройка модуля политики КриптоПро УЦ службы сертификации ЦС 11

2.1. Политика имен субъектов сертификата открытого ключа 13

2.2. Расширения сертификатов X.509 13

2.3. Использование ключа, политики выдачи и политики применения сертификатов 14

2.4. Точки распространения списка отозванных сертификатов (CDP) и точки распространения Authority Information Access (AIA) 16

2.5. Размещение файла журнала ЦС 18

3. Настройка приложения «Параметры Центра Сертификации» 20

4. Генерация ключей Центра Сертификации 25

5. Обработка запросов на сертификат Web-сервера Центра регистрации 26

6. Подключение Центров Регистрации в составе УЦ 29

6.1. Обработка запроса и выпуск сертификата открытого ключа Центра регистрации 29

6.1.1. Получение файла с запросом на сертификат открытого ключа Центра регистрации 29

6.1.2. Выпуск и сохранение сертификата открытого ключа Центра регистрации 29

6.1.3. Передача выходных данных в Центр регистрации 31

6.2. Добавление сертификата Центра регистрации в список доверенных ЦР на Центре сертификации 31

7. Публикация списка отозванных сертификатов 33

7.1. Режимы публикации списка отозванных сертификатов 33

7.2. Периодичность публикации списка отозванных сертификатов 33

7.3. Публикация списков отозванных сертификатов для доставки в подчиненные УЦ 33

7.3.1. Настройка публикации СОС в режиме корневого изолированного ЦС 34

7.3.2. Настройка публикации СОС в режиме подчиненного изолированного ЦС 34

8. Настройка Центра Сертификации для выпуска сертификатов подчиненных ЦС 37

9. Формирование запроса на кросс-сертификат Центра Сертификации 39

9.1. Запуск утилиты 39

9.2. Структура файла с дополнительными параметрами 40

10. Сроки действия ключей 42

10.1. Сроки действия ключей Центра Сертификации 42

10.2. Сроки действия ключей пользователей и Web-сервера ЦС 42

11. Смена ключей Web-сервера Центра Сертификации 43

11.1. Генерация новых ключей, выпуск и установка нового сертификата Web-сервера Центра сертификации 43

11.2. Смена сертификата на Web-узле MS IIS 43

11.3. Уничтожение старых ключей на Центре регистрации 45

12. Смена ключей Центра Сертификации 47

12.1. Смена ключей Центра Сертификации в режиме **Корневой Центр Сертификации** 47

12.2. Смена ключей Центра Сертификации в режиме **Подчиненный Центр Сертификации** 48

13. Форматы серийных номеров сертификатов открытых ключей и алгоритмы их формирования 50

14. Обеспечение целостности программных средств Центра Сертификации 51

15. Удаление программного обеспечения Центра сертификации 52

16. Перечень сокращений 54

17. Перечень рисунков 55

1. Настройка модуля выхода КриптоПро УЦ службы сертификации ЦС

Модуль выхода КриптоПро УЦ службы сертификации обеспечивает настройку следующих параметров работы Центра Сертификации:

- Настройка параметров равномерного автоматического выпуска СОС;
- Настройка параметров автоматического выпуска СОС по специальному расписанию;
- Установление режима публикации СОС в папку CDP с целью его последующего переноса на Центр Регистрации;
- Установление режима записи файла СОС в архив (архивирование СОС).

Модуль выхода КриптоПро УЦ не вмешивается в расписание публикации СОС службой сертификации, но он перехватывает все события публикации СОС. При этом возможны перерывы в работе службы сертификации и внеплановые выпуски СОС.

Если отключено специальное расписание публикаций, то все изданные службой СОС немедленно попадают в папку для публикации.

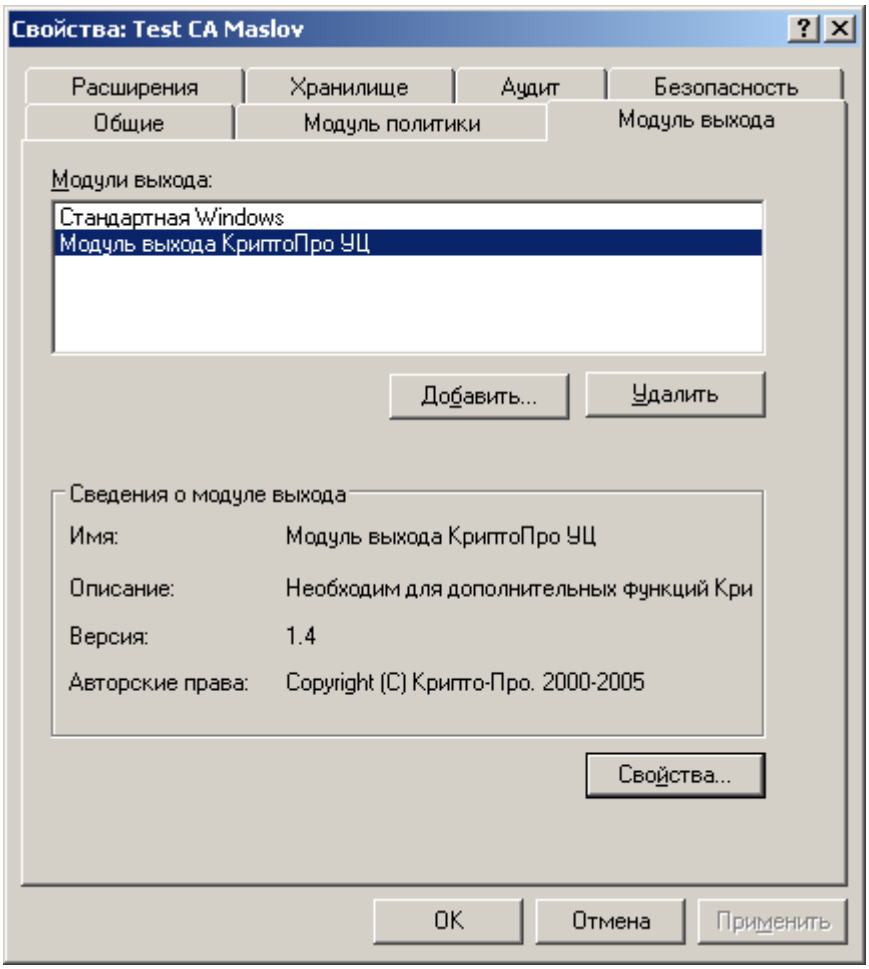
При включении специального расписания публикаций модуль выхода КриптоПро УЦ, прежде чем обновить файл СОС в папке для публикации, осуществляет сравнение времён действия (nextUpdate) только что выпущенного списка, и уже опубликованного. Если опубликованный список имеет время действия большее, либо равное времени действия только что выпущенного списка, то файл СОС не обновляется, иначе – обновляется, т.е. осуществляется публикация нового СОС. Кроме этого, если время издания СОС службой сертификации попадает на нерабочий период, то такой СОС может быть продлён до начала следующего рабочего периода и опубликован в изменённом виде. Продление осуществляется в том случае, если ещё не был опубликован продлённый СОС для данного нерабочего периода, т.е. всегда продлевается только первый СОС, изданный в данный нерабочий период.

Если включено специальное расписание публикации, то в архив попадают не все СОС, изданные службой сертификации, а только те, которые попадают в папку для публикации согласно описанному выше алгоритму.

Настройка модуля выхода службы сертификации производится путем выполнения следующих действий:

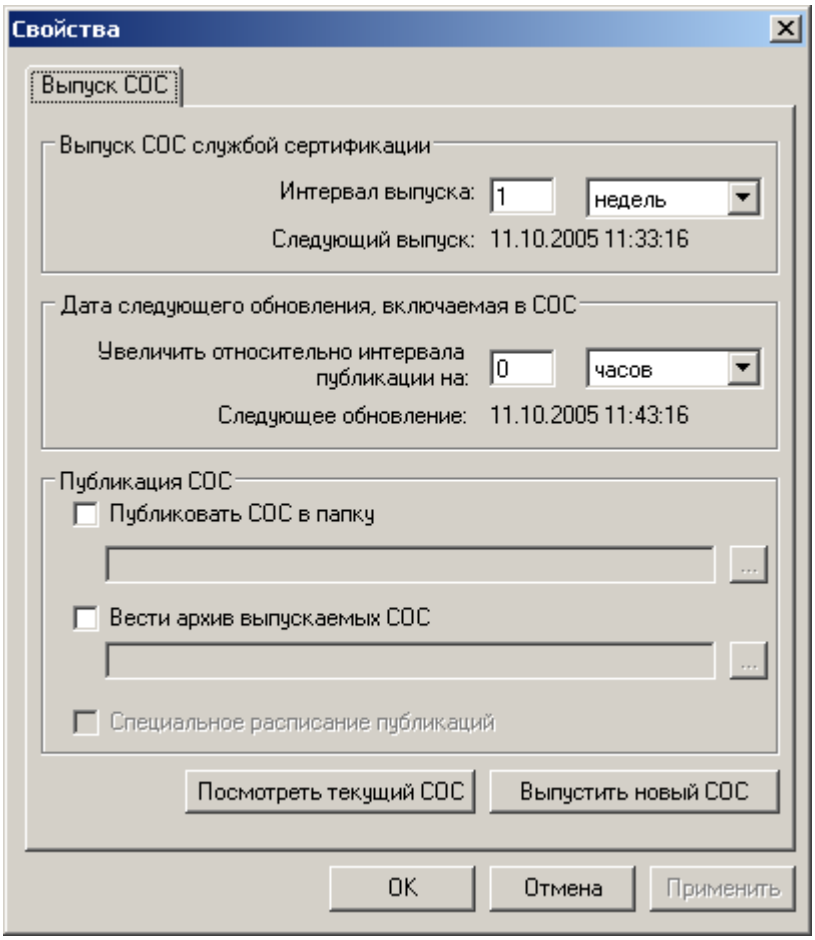
- Запустите административную консоль управления службы сертификации.
- С использованием интерфейса консоли, откройте диалог свойств центра сертификации.
- Выберите закладку **Модуль выхода**
- В списке модулей выхода выберите модуль выхода КриптоПро УЦ и нажмите кнопку **Свойства** (см. Рисунок 1).

Рисунок 1. Вкладка "Модуль выхода" службы сертификации



В появившемся окне (см. Рисунок 2) выполните настройку параметров модуля выхода КриптоПро УЦ.

Рисунок 2. Окно свойств модуля выхода КриптоПро УЦ



Параметрами настройки являются:

- интервал выпуска СОС службой сертификации;
- значение приращения интервала публикации СОС;
- параметры публикации СОС в папку;
- параметры записи архива СОС;
- параметры специального расписания публикации СОС.

Интервал выпуска СОС – это значение и единица измерения этого значения, определяющего через какой промежуток времени будет выполнена в автоматическом режиме задача по выпуску (формированию в файл) нового СОС.

Значение приращения интервала публикации СОС – это значение и единица измерения этого значения, определяющего приращение к интервалу публикации СОС. Сумма значений интервала публикации и значения его приращения определяют период действия, заносимый в СОС и определяемый в нём датами **Действителен до** и **Следующее обновление**.

Задание этого приращения необходимо для обеспечения интервала времени, в течении которого будет осуществлена рассылка потребителям нового СОС и обеспечения действия в этом промежутке времени старого СОС.

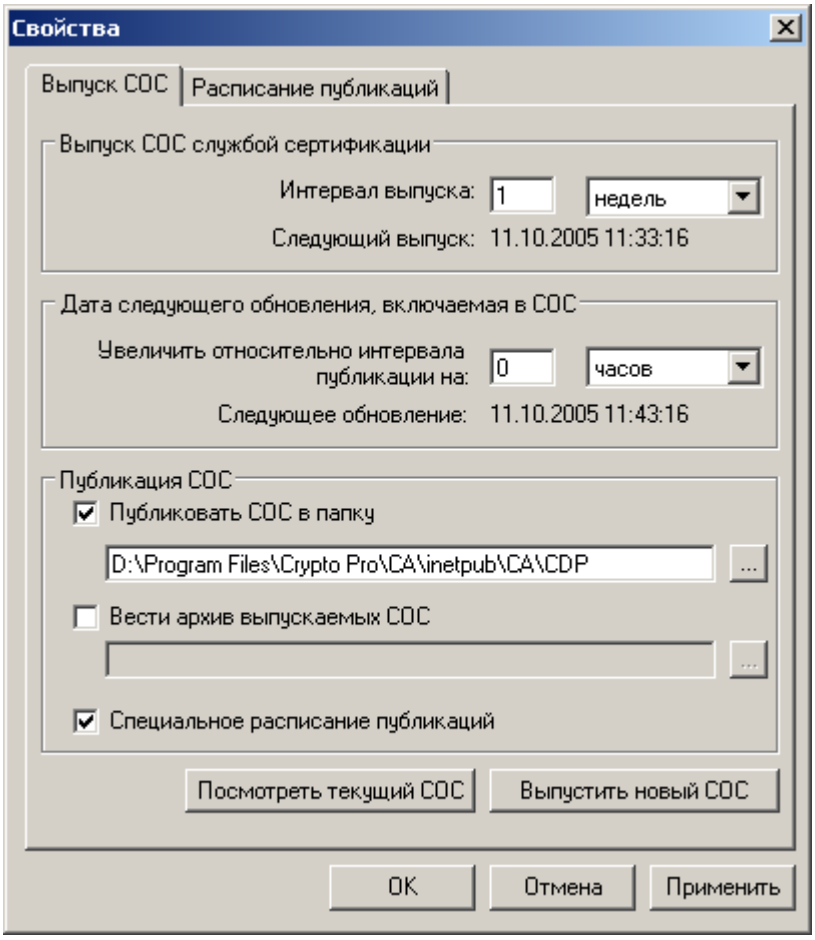
Параметры публикации СОС в папку – включают или выключают режим публикации (запись файла) СОС в папку, из которой файл будет доступен с Центра Регистрации для получения соответствующими задачами Центра Регистрации (например, с целью автоматической рассылки СОС с помощью Центра Регистрации в подчиненные УЦ). Данная папка должна являться домашним каталогом папки CDP виртуального каталога CA Web-узла Центра Сертификации. Более подробно о публикации СОС можно ознакомиться в разделе 7 настоящего Руководства.

Параметры записи архива СОС – эти параметры определяют путь к каталогу с файловым архивом файлов СОС.

Параметры специального расписания публикации СОС – эти параметры определяют задание на выпуск СОС по произвольно настраиваемому расписанию.

Для настройки параметров специального расписания публикации СОС выберите пункт **Специальное расписание публикаций** в окне свойств модуля выхода КриптоПро УЦ. Выбор данного пункта возможен только при выбранном пункте **Публиковать СОС в папку**. После выбора пункта **Специальное расписание публикаций** в окне свойств модуля выхода КриптоПро УЦ появляется дополнительная вкладка **Расписание публикаций** (см. Рисунок 3), выбрав которую можно настраивать параметры специального расписания публикации СОС.

Рисунок 3. Окно свойств модуля выхода КриптоПро УЦ с вкладкой "Расписание публикаций"

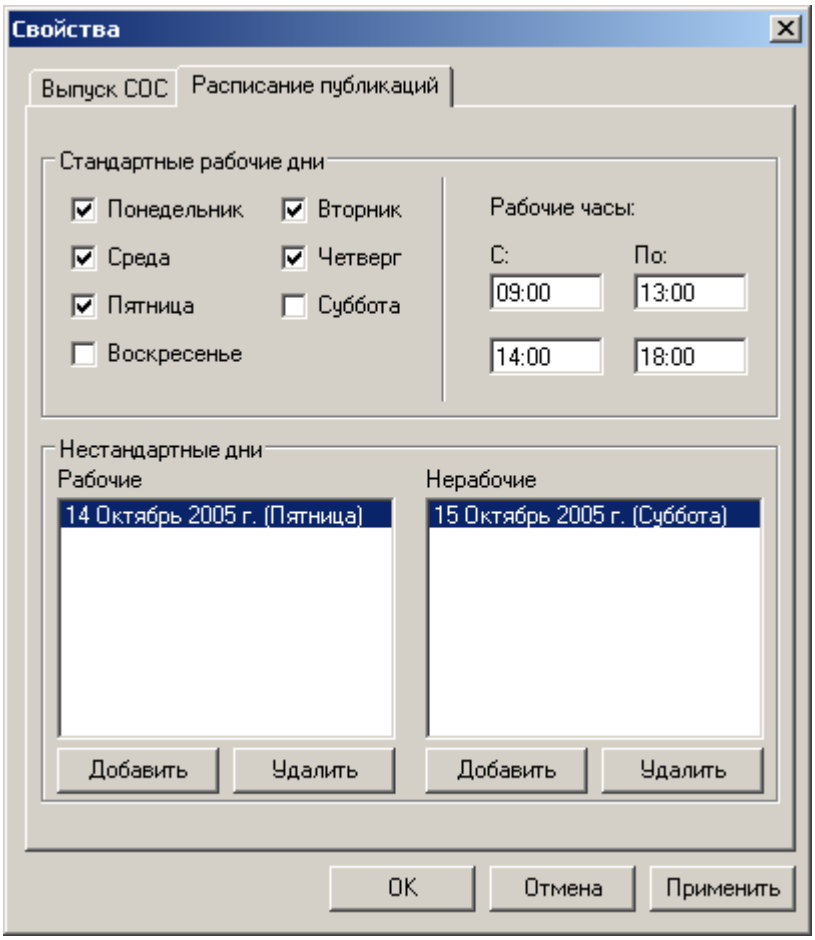


В окне свойства расписания публикаций СОС (Рисунок 4) настраивается расписание по рабочим и нерабочим дням работы удостоверяющего центра.

На этой вкладке настраивается требуемое расписание рабочих и выходных дней и часов. В верхней части вкладки настраивается обычное рабочее расписание – какие дни недели и какие часы в эти дни считаются рабочими, при этом в рабочий день может быть задан один перерыв. В нижней части можно выделить обозначить некоторые дни нестандартными рабочими или выходными днями.

В группе **Стандартные рабочие дни**, дни недели, отмеченные галочками, становятся обычными рабочими днями, расписание рабочих часов которых определяется согласно параметрам, заданных в группе **Рабочие часы**. Можно задать два интервала рабочего времени в рабочий день. Обычно до обеда и после обеда. Если удостоверяющий центр работает без обеда, то требуется задать один интервал рабочего времени. Время задается в формате ЧЧ:ММ.

Рисунок 4. Окно настройки расписания публикаций СОС



Если на рабочие дни удостоверяющего центра (дни недели, отмеченные галочками) приходятся выходные или праздничные дни, то такие дни надо добавить в список **Нерабочие** группы **Нестандартные дни**.

Если какие-то или праздничные дни удостоверяющего центра (дни недели, НЕ отмеченные галочками) объявлены рабочими, то такие дни надо добавить в список **Рабочие** группы **Нестандартные дни**.

1.1. Пример настройки расписания СОС при организации работы удостоверяющего центра

Использование специального расписания публикации СОС позволяет выполнять обязательства УЦ перед клиентами по периодичности издания СОС в рабочее время, тогда как в выходные часы проводить техническое обслуживание аппаратного и программного обеспечения УЦ, в том числе с отключением электропитания или компьютерной сети.

Возможна следующая схема организации настроек УЦ и рабочего времени администратора УЦ. Зададим следующие начальные условия:

- УЦ несёт обязательства перед клиентами по отзыву сертификатов в рабочее время: с понедельника по пятницу с 9:00 до 18:00 с перерывом с 13:00 до 14:00.
- УЦ несёт обязательства перед клиентами, что информация об отзыве публикуется не позднее 1 часа (To) с момента обращения клиента, с учётом рабочего времени.
- Максимальное время перекладывания выпущенного СОС из папки для публикации в точку CDP, доступную клиентам, составляет 15 минут.
- Максимальное время расхождения часов УЦ с часами клиентов составляет 10 минут (s).

Для работы по такой схеме необходимо сделать следующие настройки в модуле выхода:

- Период публикации СОС устанавливается в 25 минут (T). Расчёт данного времени приведён ниже.
- Интервал перекрытия СОС настраивается в 15 минут (o) – максимальное время перекладывания СОС в точку CDP.
- Настраивается специальное расписание публикации в соответствии с рабочим временем.

Покажем, что период публикации СОС в 25 минут удовлетворяет условиям. Предположим, что в 10:00 по часам УЦ был опубликован СОС в соответствии с описанными настройками, тогда в нём будут проставлены следующие времена: thisUpdate – 9:50, nextUpdate – 10:50 (10:00 + период + интервал перекрытия + расхождение часов). Теперь, допустим, клиент обращается в 9:51 по его часам в УЦ с просьбой отозвать сертификат. В этом случае, он рассчитывает, что не позднее 10:51 по его часам, в CDP будет находиться СОС, в котором будет зафиксирован факт аннулирования его сертификата. Все другие клиенты, часы которых могут отличаться от УЦ на 10 минут, получат этот СОС также не позднее 10:51 по их часам. Тогда УЦ необходимо, не позднее 10:41 по его часам, положить СОС в CDP, то есть опубликовать его на ЦС необходимо не позднее 10:26. Этот предельный случай и достигается путём установки периода в 25 минут.

Аналогичные аргументы можно применить для расчёта других временных интервалов. Формула для расчёта периода публикации: T = To - o - 2s.

Алгоритм продления срока действия СОС в выходное время учитывает настроенную периодичность публикации СОС службой сертификации с целью обеспечить публикацию нового списка не позднее заданного интервала с начала рабочего времени (для выполнения обязательств УЦ), а также не публиковать в CDP СОС, выпущенные ранее необходимого срока для минимизации накладных расходов.

Выпущенный в нерабочее время СОС продлевается до момента времени, рассчитываемого по следующей формуле: Tк = t + T + o + 2s, где t – момент начала рабочего времени. Покажем на примере, что такой СОС достигает указанной цели. В нашем случае СОС, продлённый с вечера понедельника до утра вторника, будет иметь время nextUpdate 10:00. Теперь пусть клиент обращается в 9:01 по часам УЦ с просьбой отозвать сертификат. В таком случае, для достижения поставленной цели необходимо и достаточно, чтобы СОС, выпущенный в 9:02 по часам УЦ попал в CDP, а СОС, выпущенный в 9:00 не попал туда. Выпущенный в 9:00 СОС имеет время nextUpdate 10:00. Таким образом, согласно алгоритму работы модуля выхода, он не будет опубликован, поскольку продлённый СОС со временем nextUpdate 10:00 уже был опубликован. Аналогично, СОС, выпущенный в 9:02 будет иметь время nextUpdate 10:02 и будет опубликован, что и требовалось доказать.

Для своевременной фиксации факта отзыва сертификата в БД УЦ необходимо, чтобы все компьютеры УЦ и служба сертификации на ЦС были запущены к началу рабочего времени.

Модуль выхода продлевает первый СОС, выпущенный в нерабочее время с учётом возможного расхождения часов УЦ с часами клиента. Для того чтобы провести техническое обслуживание УЦ в нерабочее время, администратору необходимо дождаться публикации продлённого СОС, после чего можно отключать УЦ. Также можно не дожидаясь очередной плановой публикации СОС службой осуществить публикацию вручную сразу после начала нерабочего времени, т.е. в 18:10 по нашему примеру.

2. Настройка модуля политики КриптоПро УЦ службы сертификации ЦС

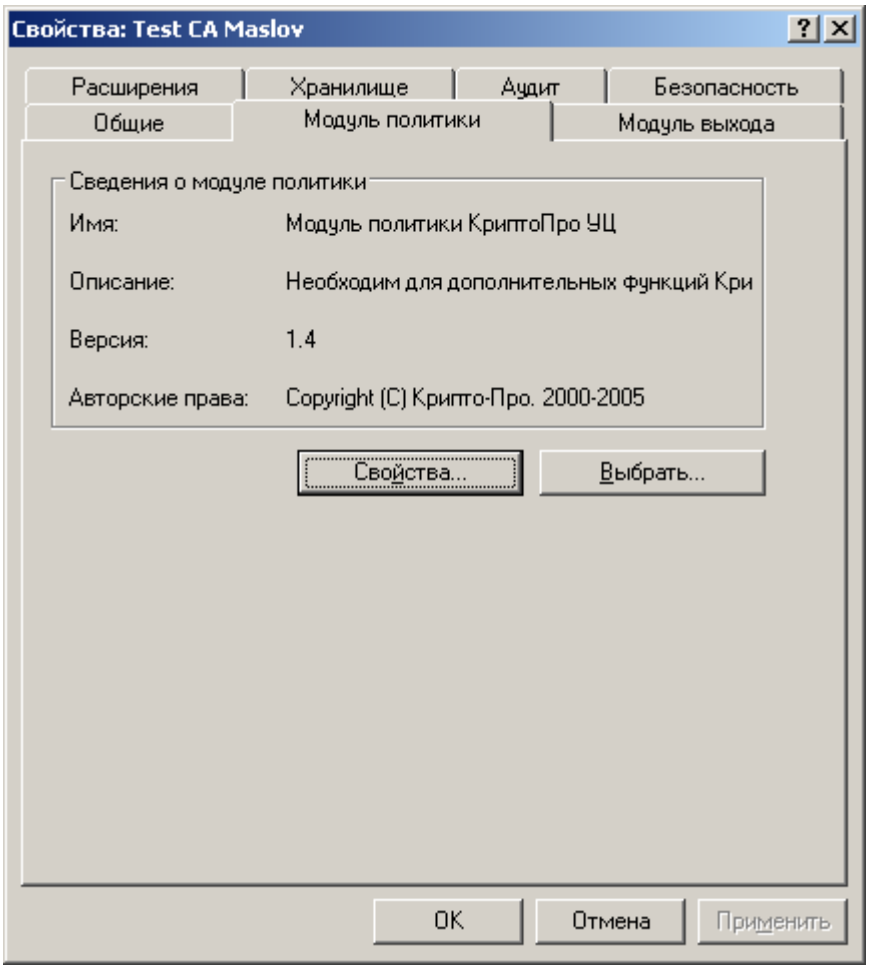
Модуль политики Крипто-Про УЦ службы сертификации обеспечивает настройку следующих основных параметров работы Центра Сертификации:

- Установления политики имен (ограничений) на имена субъектов (владельцев) издаваемых сертификатов;
- Установление допустимых расширений из запроса на сертификаты, включаемых в издаваемые сертификаты;
- Установление информации о точках распространения списка отозванных сертификатов (CDP) и точек распространения Authority Information Access (AIA) (например, расширения CDP -точки распространения списка отозванных сертификатов), включаемых в издаваемые сертификаты;
- Определение списка допустимых областей использования ключа (EKU), политик выдачи, политик применения сертификатов и параметров вычисления срока действия для издаваемых сертификатов;
- Определение месторасположения журнала аудита ЦС.

Настройка модуля политики службы сертификации производится путем выполнения следующих действий:

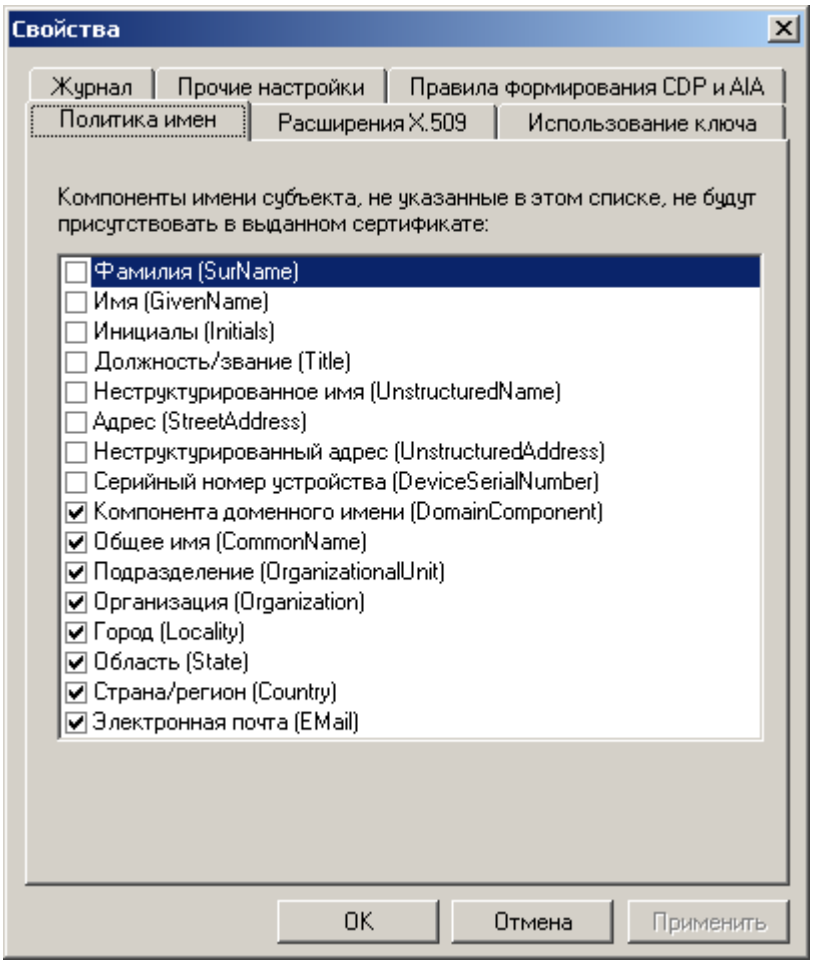
- Запустите административную консоль управления (оснастку) службы сертификации.
- С использованием интерфейса консоли, откройте диалог свойств центра сертификации.
- Выберите закладку **Модуль политики** и нажмите кнопку **Настроить** (см. Рисунок 5).

Рисунок 5. Вкладка "Модуль политики" службы сертификации



- В появившемся окне свойств установите параметры работы модуля политики службы сертификации ЦС.

Рисунок 6. Окно свойств модуля политики КриптоПро УЦ



2.1. Политика имен субъектов сертификата открытого ключа

Имя субъекта сертификата открытого ключа (SubjectDN) – это набор идентификаторов (компонентов), помещаемых в сертификат открытого ключа и описывающих субъекта (владельца) сертификата открытого ключа.

Компоненты имени субъекта сертификата и их значения переносятся из запроса на сертификат открытого ключа.

Данный параметр модуля политики службы сертификации ЦС определяет список тех компонентов имени субъекта, которые будут переносится без изменений из запроса в сертификат открытого ключа. В случае, если в запросе на сертификат в имени субъекта содержатся идентификаторы которые не отмечены в качестве разрешенных в списке, данный запрос будет отвергнут модулем политики.

Управление списком допустимых компонентов имени субъекта сертификата осуществляется на вкладке Политика имен окна свойств модуля политики ЦС (см. Рисунок 6).

2.2. Расширения сертификатов X.509

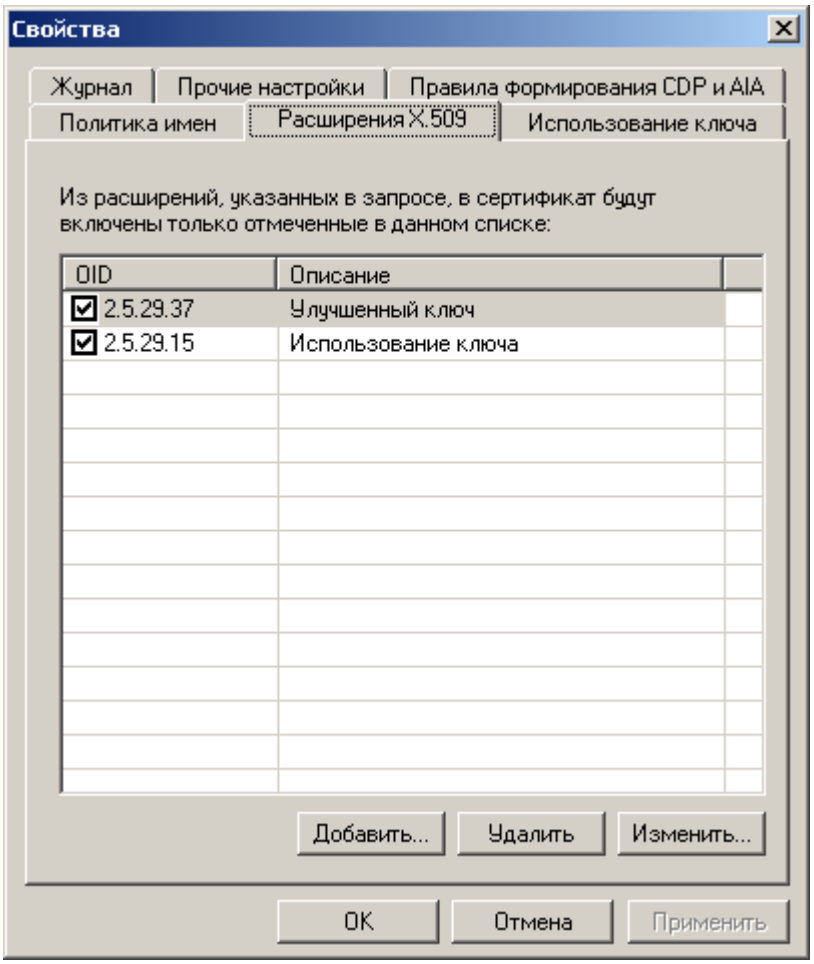
Расширения сертификатов открытых ключей – это идентификаторы (OIDs), определяющие пользовательские расширения сертификата открытого ключа.

При обработке запроса на сертификат модулем политики ЦС, расширения, содержащиеся в запросе на сертификат и находящиеся в списке допустимых расширений сертификатов, будут перенесены в выпускаемый сертификат открытого ключа без изменений. В

противном случае, расширения из запроса не будут перенесены в выпускаемый сертификат открытого ключа.

Управление списком допустимых расширений сертификатов осуществляется на вкладке Расширения X.509 окна свойств модуля политики ЦС (см. Рисунок 7).

Рисунок 7. Вкладка "Расширения X.509" свойств модуля политики ЦС



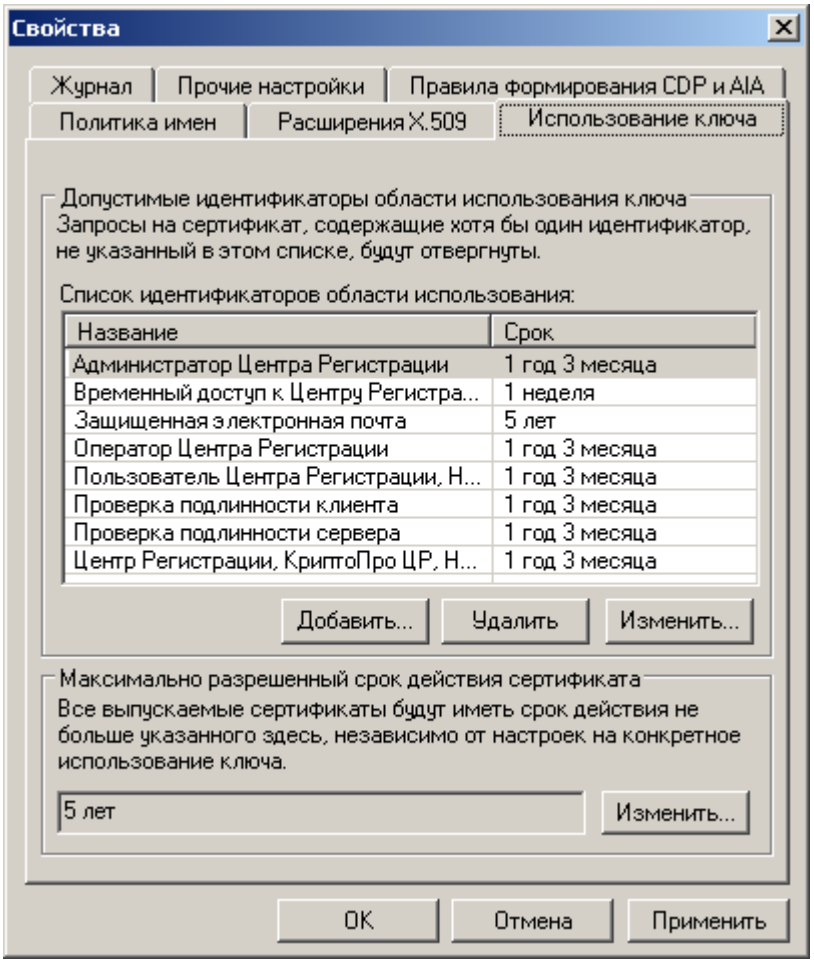
2.3. Использование ключа, политики выдачи и политики применения сертификатов

Допустимые области использования (применения) ключа – это расширение сертификата открытого ключа (EKU), определяющее области применения сертификата открытого ключа и соответствующего закрытого ключа.

Каждая область применения определяется идентификатором, включающимся в расширение EKU. Таких идентификаторов в расширении может быть несколько.

Данные идентификаторы содержатся в запросе на сертификат открытого ключа и заносятся в выпускаемый сертификат в случае, если все они присутствуют в списке допустимых областей применения (см. Рисунок 8). В противном случае, если хотя бы один идентификатор (одна область применения) из запроса на сертификат не содержится в списке, данный запрос будет отвергнут.

Рисунок 8. Вкладка "Использование ключа" свойств модуля политики КриптоПро УЦ



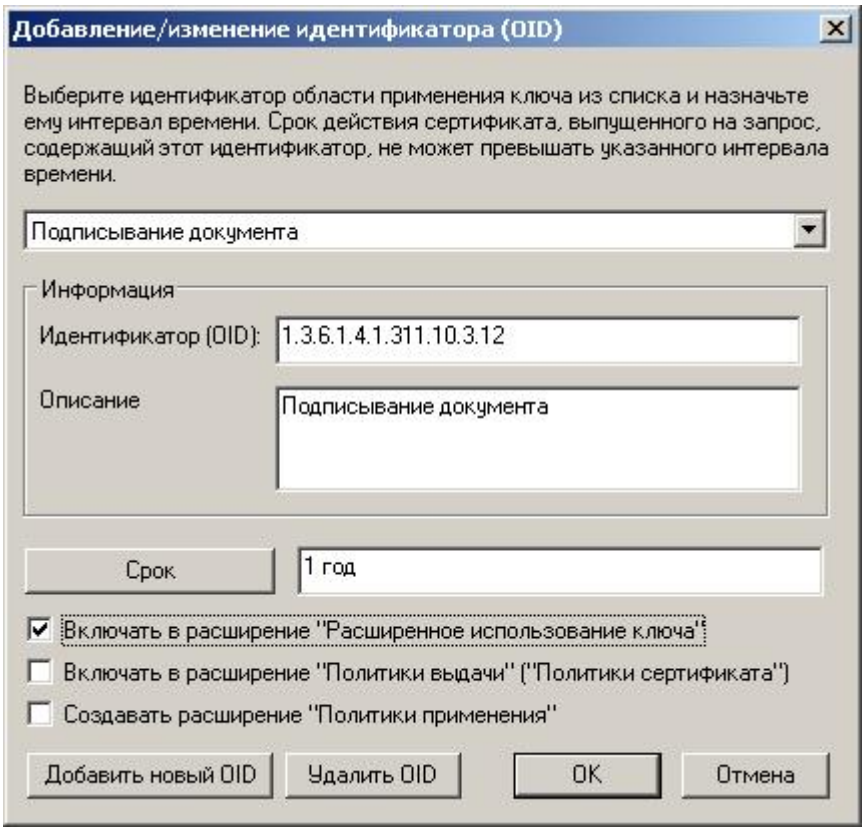
Каждый идентификатор области применения ключа определяет значение срока действия ключа, используемого в данной области применения. Срок действия ключа настраивается для каждой области применения отдельно при добавлении новой области применения или при нажатии кнопки «Изменить» для существующей области применения (см. Рисунок 9).

Максимальное значение срока действия сертификатов открытого ключа

Максимальное значение срока действия сертификатов открытого ключа – это параметр модуля политики, определяющий ограничение на срок действия сертификата открытого ключа.

Управление значением максимального срока действия сертификатов открытого ключа осуществляется на вкладке Использование ключа окна свойств модуля политики ЦС (см. Рисунок 8).

Рисунок 9. Настройка параметров использования ключа



Каждый идентификатор области использования ключа (EKU) из запроса на сертификат может быть помещён в выдаваемый сертификат в одном из трёх вариантов:

А) как идентификатор EKU (по умолчанию)

Б) как идентификатор политики выдачи сертификатов

В) как идентификатор политики применения сертификатов и как идентификатор EKU.

Если хотя бы для одного идентификатора EKU из конкретного запроса на сертификат включена опция **Создавать расширение "Политики применения"**, то расширение "Политики применения" будет создано и в него будут включены все остальные идентификаторы EKU из этого запроса на сертификат, которые были настроены как идентификаторы расширенного использования ключа.

Способ добавления идентификатора настраивается при добавлении новой области применения или при нажатии кнопки «Изменить» для существующей области применения (см. Рисунок 9).

Управление списком допустимых расширений сертификатов, политиками выдачи и политиками применения сертификатов и значениями сроков действия ключей осуществляется на вкладке Использование ключа окна свойств модуля политики ЦС (см. Рисунок 8).

2.4. Точки распространения списка отозванных сертификатов (CDP) и точки распространения Authority Information Access (AIA)

К точкам распространения Authority Information Access (AIA) относятся:

- Точки получения сертификата ЦС;
- Точки получения актуального статуса сертификата (OCSP).

Точки получения сертификата ЦС – это местоположения сертификата ЦС, издавшего сертификат открытого ключа. Местоположение определяет путь к файлу с сертификатом ЦС и протокол доступа.

Точка получения сертификата ЦС представляет собой строку, содержащую местоположение файла CRL.

Таких точек может быть указано несколько. В этом случае каждая точка получения сертификата ЦС будет определять один из протоколов, по которому возможен доступ к файлу.

Допустимы следующие префиксы, определяющие протокол доступа:

ldap, http, ftp, file

Точки получения сертификата ЦС заносятся в выпускаемые Центром сертификации сертификаты открытых ключей.

Точки получения актуального статуса сертификата – это местоположение (URL) службы OCSP, предоставляющей информацию о действующем статусе сертификата открытого ключа.

Допустим только один префикс, определяющий протокол доступа: **http**

Определение и задание точек получения актуального статуса сертификата аналогично определению и заданию точек получения сертификата ЦС.

Управление точками получения актуального статуса сертификата осуществляется на вкладке **Информация о ЦС** окна свойств модуля политики ЦС (см. Рисунок 10).

Точки распространения списка отозванных сертификатов – это местоположения списка отозванных сертификатов (CRL), издаваемых ЦС. Местоположение определяет путь к файлу CRL и протокол доступа.

Точка распространения списка отозванных сертификатов представляет собой строку, содержащую местоположение файла CRL.

Таких точек может быть указано несколько. В этом случае каждая точка распространения списка отозванных сертификатов будет определять один из протоколов, по которому возможен доступ к файлу.

Например, Точка

http://sectestca1.rte.microsoft.com/CertEnroll/SecTestCA1.crl определяет местоположение (URL) списка отозванных сертификатов по протоколу HTTP. Допустимы следующие префиксы, определяющие протокол доступа:

ldap, http, ftp, file

Точки распространения списка отозванных сертификатов заносятся в выпускаемые Центром сертификации сертификаты открытых ключей (расширение CDP).

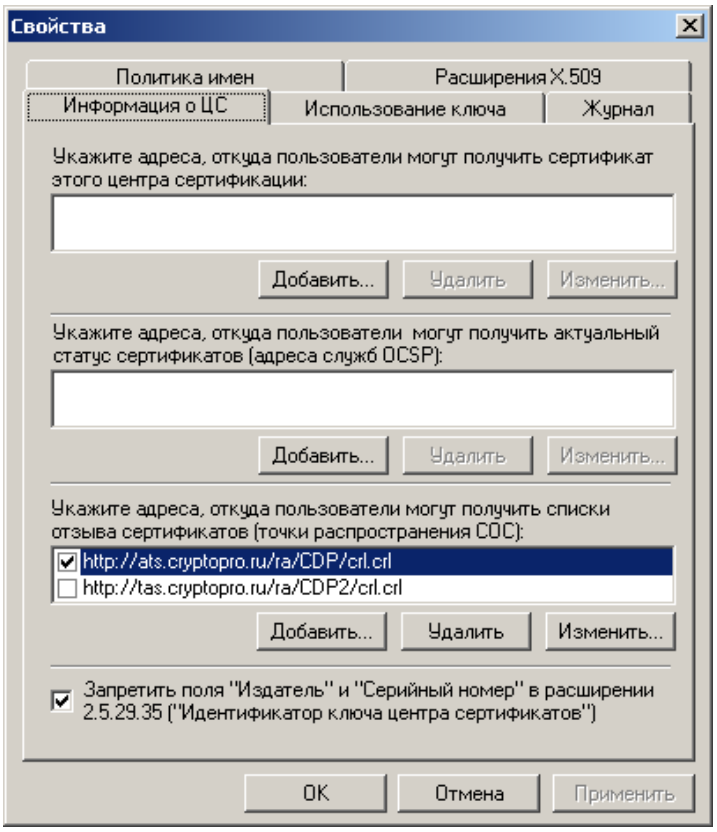
Политика кросс-сертификации – это параметр, определяющий запрет на включение в издаваемые сертификаты полей «Издатель» и «Серийный номер» расширения «Идентификатор ключа центра сертификации».

Включенный запрет обеспечит необходимые условия для построения цепочек сертификатов, включающих кросс-сертификаты, на платформе Windows.

Параметр задается на вкладке **Информация о ЦС** окна свойств модуля политики ЦС (см. Рисунок 10).

При включении этого параметра, политика кросс-сертификации не распространяется на ранее изданные сертификаты.

Рисунок 10. Вкладка "Информация о ЦС" свойств модуля политики ЦС



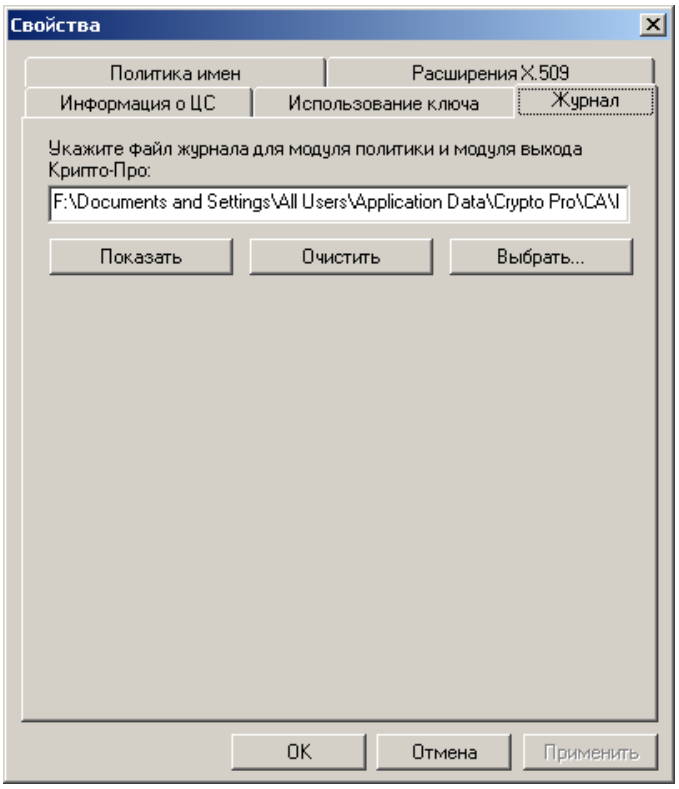
2.5. Размещение файла журнала ЦС

Журнал протоколирования работы ЦС представляет собой файл в текстовом формате, размещаемый на локальном диске ЦС.

Место размещения файла журнала указывается на вкладке **Журнал** окна свойств модуля политики ЦС (см. Рисунок 11).

Формат записей журнала протоколирования работы ЦС описан в «Руководстве по безопасности» из состава эксплуатационной документации ПАК «КриптоПро УЦ».

Рисунок 11. Вкладка "Журнал" свойств модуля политики ЦС



После установки значений нажмите кнопку «OK» и произведите перезапуск службы сертификации для приведения изменений в действие.

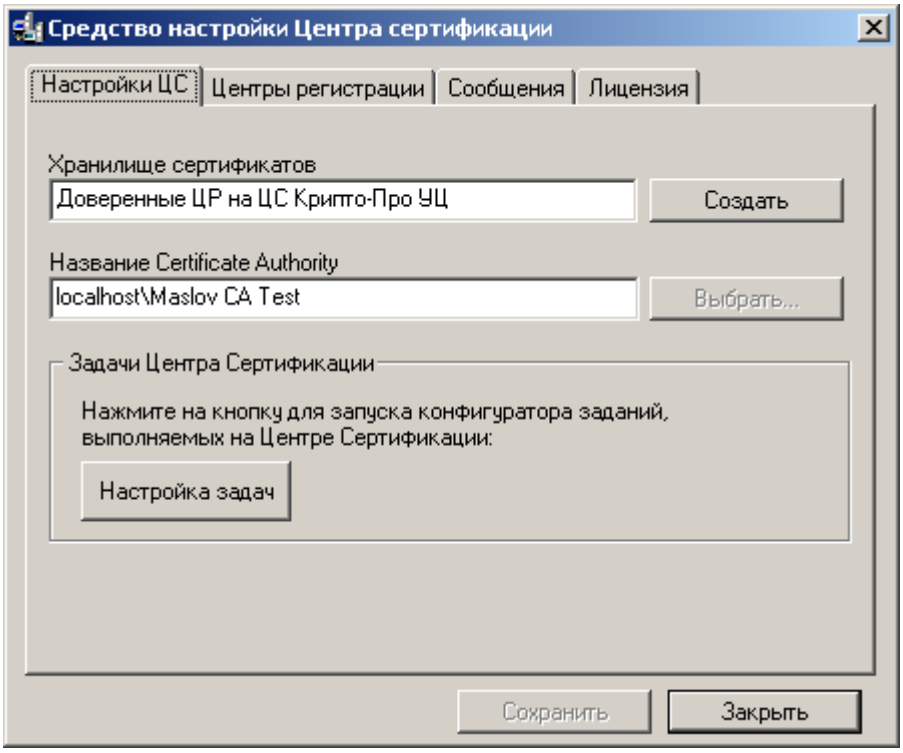
3. Настройка приложения «Параметры Центра Сертификации»

Приложение «Параметры Центра Сертификации» обеспечивает настройку следующих основных параметров работы Центра Сертификации:

- Наименование и создание раздела хранилища сертификатов локального компьютера, который будет содержать список сертификатов доверенных Центров Регистрации;
- Управление списком сертификатов доверенных Центров Регистрации (просмотр, добавление, удаление);
- Установление значений параметров компоненты отправки почтовых сообщений (параметры подключения к почтовому серверу: имя сервера, порт, тип аутентификации и т.д.);
- Ввод параметров лицензии на Центр Сертификации «КриптоПро УЦ» (наименовании организации, серийный номер);
- Настройка задания переноса файлов СОС (CRL) в каталог CDP для дальнейшего их переноса на Центр Регистрации.

Настройка модуля взаимодействия с Центрами регистрации осуществляется с использованием приложения **Параметры Центра Сертификации** из группы «Крипто-Про» (см. Рисунок 12).

Рисунок 12. Приложение "Параметры Центра сертификации"



Параметрами настройки и конфигурации модуля взаимодействия с Центрами регистрации являются:

- **Хранилище сертификатов Центров регистрации**

  Хранилище сертификатов Центров Регистрации – это раздел хранилища сертификатов локального компьютера, используемого для хранения сертификатов Центров регистрации.

Центры регистрации, сертификаты которых лежат в хранилище сертификатов Центров Регистрации считаются "подключенными" к Центру сертификации и могут передавать запросы на Центр сертификации с целью их обработки.

При установке ПО ЦС автоматически создается хранилище сертификатов Центров регистрации с наименованием по умолчанию "Доверенные ЦР на ЦС Крипто-Про УЦ".

Приложение настройки позволяет сменить раздел хранилища. Для этого необходимо на вкладке **Настройки ЦС** ввести в поле ввода новое наименование хранилища (см. Рисунок 12) и нажать кнопку **Создать**.

- **Название службы сертификации ЦС**

Название службы сертификации ЦС – это наименование службы Certificates Authority, расположенной на локальном компьютере ЦС.

Поле **Название Certificate Authority** на вкладке **Настройки ЦС** (см. Рисунок 12) на вкладке содержит DNS имя сервера и имя Центра сертификации, разделенные символом «\» (обратный слеш). Выбор службы сертификации осуществляется с помощью кнопки **Выбрать**.

- **Параметры задания доставки СОС**

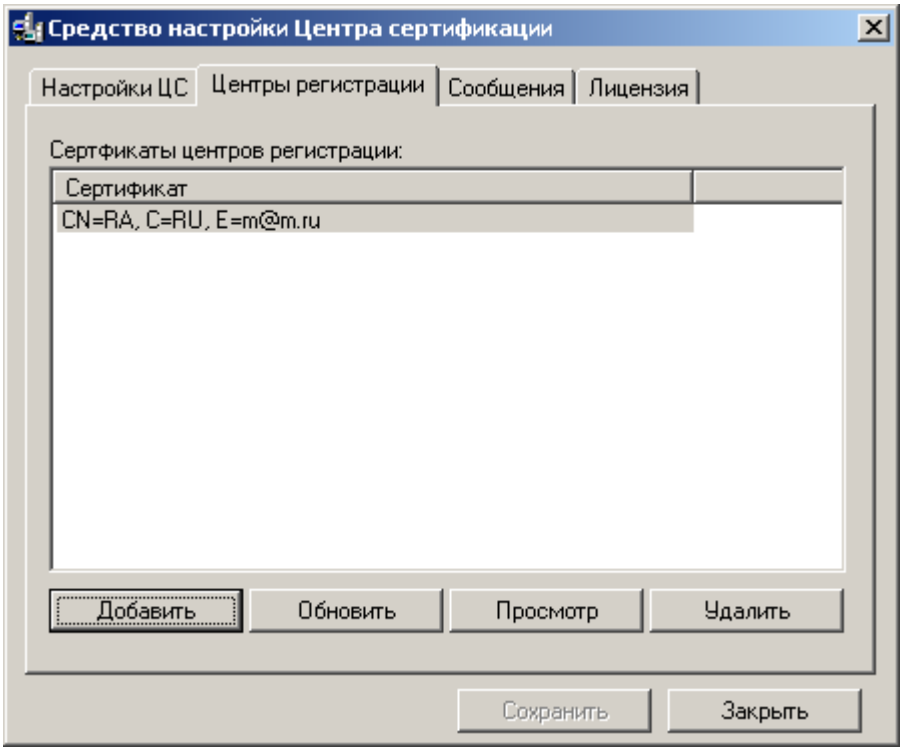
Параметры задания доставки СОС – это параметры, определяющие режимы распространения списков отозванных сертификатов (СОС, CRL) из вышестоящих по иерархии УЦ в подчиненные УЦ. Более подробно о доставке CRL можно ознакомиться в разделе 7 настоящего Руководства.

- **Список сертификатов Центров регистрации**

Список сертификатов Центров регистрации – это набор сертификатов открытых ключей, обеспечивающих аутентификацию в качестве клиента при взаимодействии Центра регистрации с Центром сертификации. Данный набор сертификатов Центров регистрации размещается в хранилище сертификатов Центров регистрации, местоположение которого, определяется параметром настройки **Хранилище сертификатов**.

Управление списком осуществляется на вкладке **Центры регистрации** (см. Рисунок 13).

Рисунок 13. Вкладка "Центры регистрации" средства настройки Центра сертификации



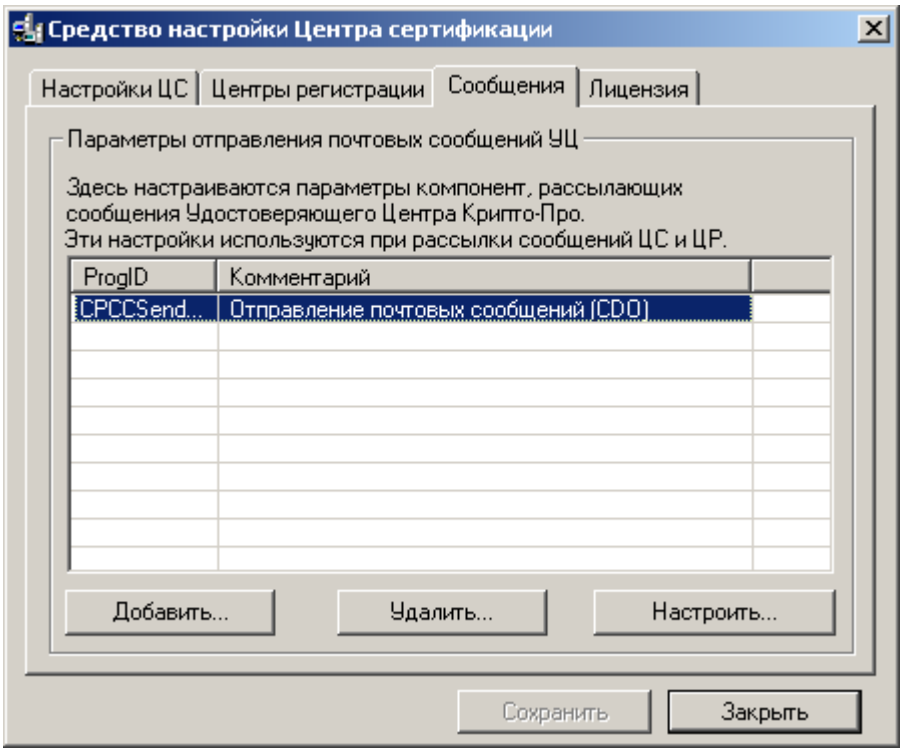
- **Параметры отправления почтовых сообщений УЦ**

Параметры отправления почтовых сообщений УЦ – это параметры программных модулей (компонент), рассылающих почтовые сообщения, формируемые программным обеспечением Центра Сертификации (модулем политики, модулем выхода и т.д.).

Управление Параметры отправления почтовых сообщений ЦС осуществляется на вкладке **Сообщения** (см. Рисунок 14).

Для настройки компоненты требуется выбрать компоненту из списка и нажать кнопку **Настроить**.

Рисунок 14. Вкладка "Сообщения" средства настройки Центра сертификации



- **Параметры Лицензии на право эксплуатации программного обеспечения Центра Сертификации**

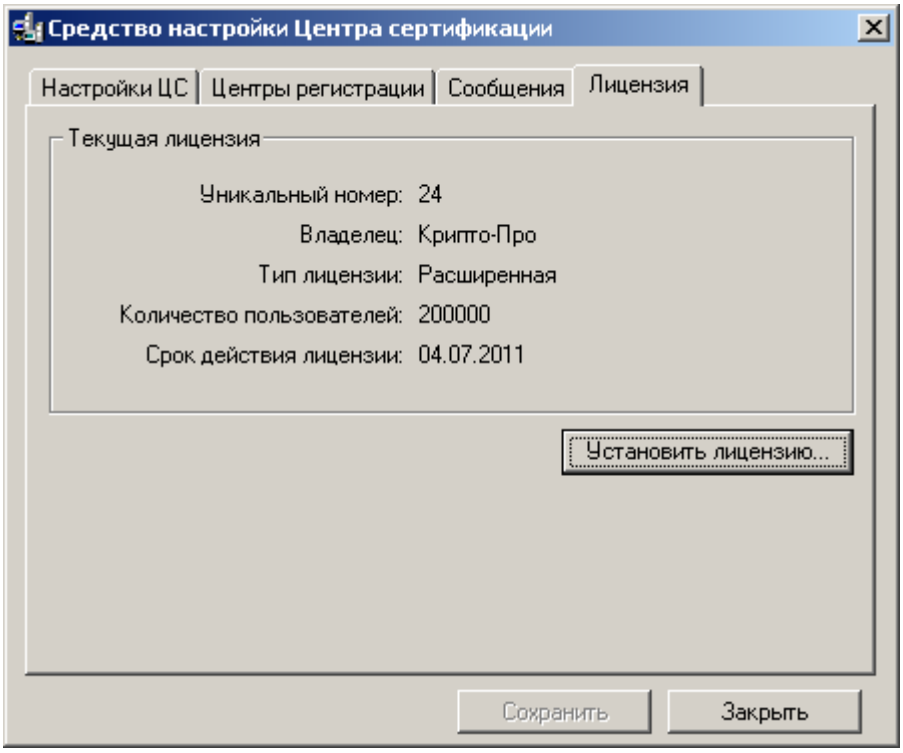
  Параметры Лицензии на право эксплуатации программного обеспечения Центра Сертификации – это права, предоставленные поставщиком программного обеспечения УЦ, выраженные в Лицензии.

  К правам относятся:

  - срок действия лицензии;
  - количество пользователей (владельцев сертификатов открытых ключей), которое может обслуживать Центр Сертификации УЦ.

  Для установки серийного номера Лицензии нажмите кнопку **Установить лицензию** на вкладке **Лицензия** окна свойств модуля политики (см. Рисунок 15).

Рисунок 15. Вкладка "Лицензия" средства настройки Центра сертификации



4. Генерация ключей Центра Сертификации

Ключами Центра Сертификации является ключевая пара, состоящего из закрытого и открытого ключа уполномоченного лица Удостоверяющего Центра в терминах действующего законодательства.

Ключи Центра Сертификации могут быть сформированы (сгенерированны) либо в процессе установки службы сертификации Центра Сертификации, либо с использованием программного обеспечения АРМ администратора ЦР, реализующего функцию генерации ключей Центра Сертификации.

Для целей генерации ключей ЦС АРМ администратора предоставляет задачу "Сгенерировать ключ Центра Сертификации". Подробнее о задаче смотрите в Руководстве администратора Центра Регистрации.

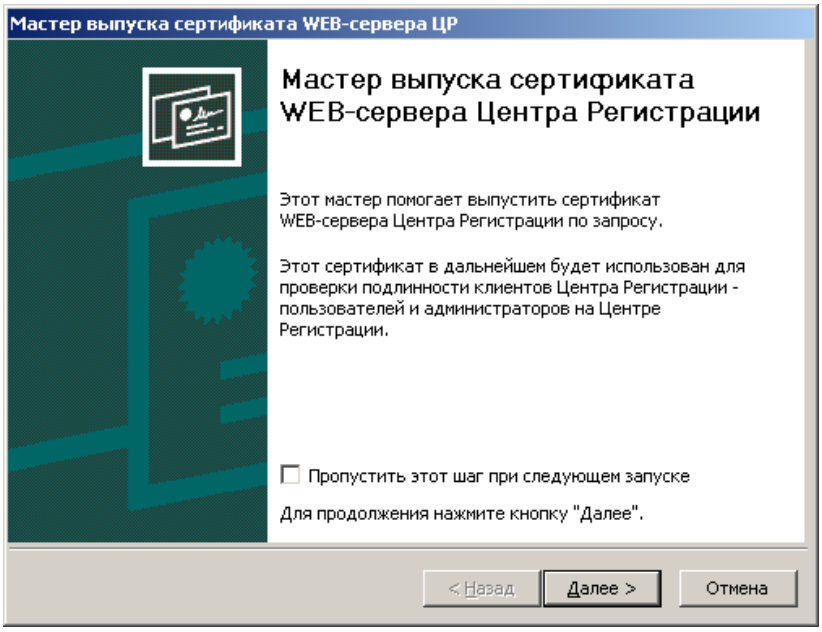
5. Обработка запросов на сертификат Web-сервера Центра регистрации

Обработка запросов на сертификат Web-сервера Центра регистрации заключается в выпуске сертификата открытого ключа Web-сервера Центра регистрации на основании запроса на сертификат, поступившего из Центра регистрации в виде файла.

Выпущенный сертификат (или цепочка сертификатов) Web-сервера Центра регистрации возвращаются в адрес запросившего также в виде файла.

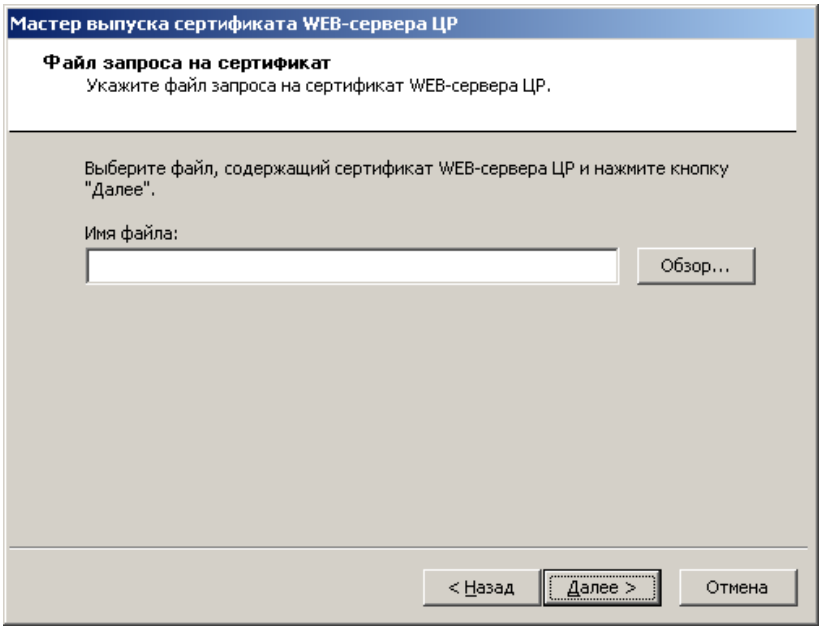
Обработка запроса выполняется с помощью программы-утилиты **Обработка запроса на сертификат WEB-сервера ЦС** из группы **Крипто-Про** (см. Рисунок 16). Эта программа представляет собой Мастер выпуска сертификата WEB-сервера Центра регистрации.

Рисунок 16. Мастер выпуска сертификата WEB-сервера Центра Регистрации



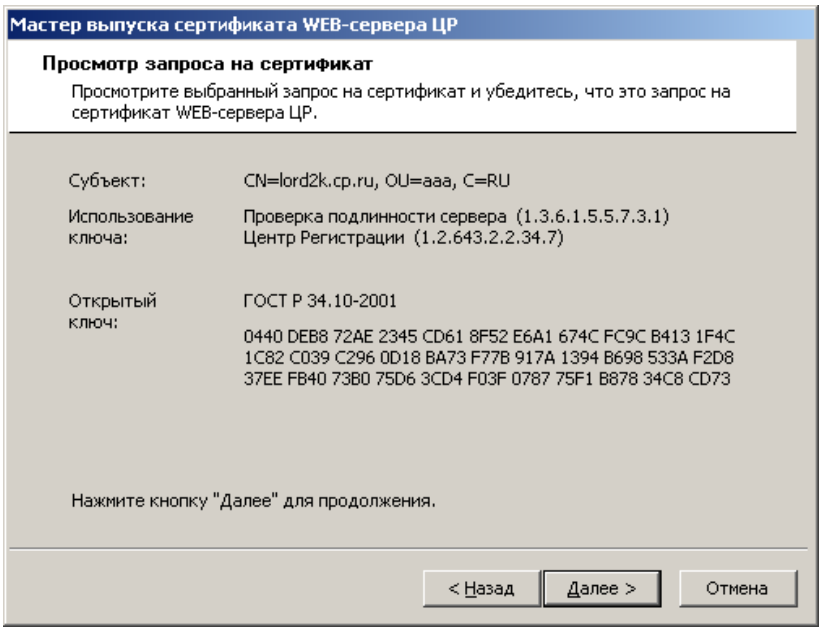
После запуска Мастера в диалоговом окне (см. Рисунок 17) необходимо выбрать файл, содержащий запрос на сертификат Web-сервера Центра регистрации.

Рисунок 17. Окно выбора файла с запросом в Мастере выпуска сертификата WEB-сервера ЦР



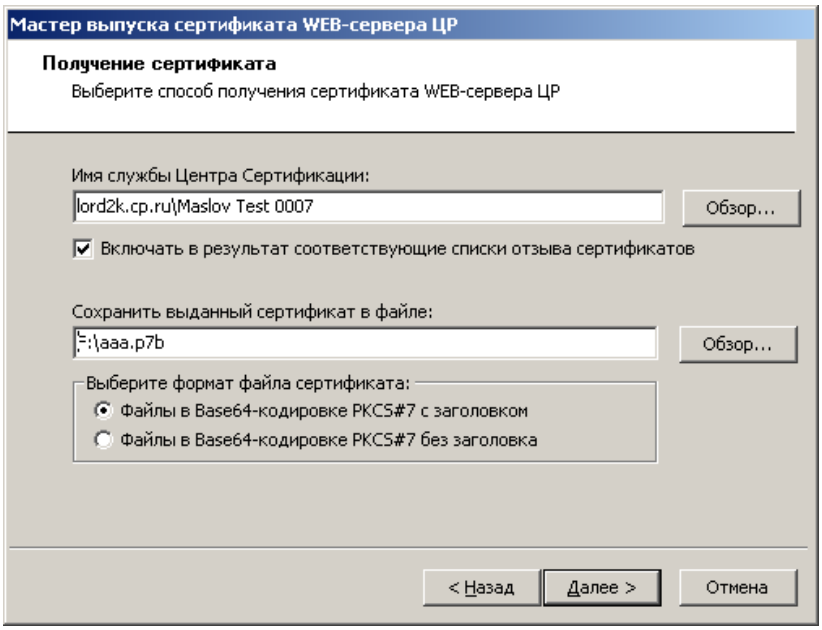
После выбора файла с запросом на сертификат отобразится диалоговое окно (см. Рисунок 18) с информацией о запросе, содержащимся в файле. Убедитесь в корректности информации о Web-сервере Центра регистрации и нажмите кнопку **Далее**.

Рисунок 18. Окно с информацией о запросе Мастера выпуска сертификата Web-сервера ЦР



В следующем окне (см. Рисунок 19) необходимо выбрать службу сертификации ЦС, которая обработает запрос; определить имя, и размещение файла, в который будет записан выпущенный сертификат в виде цепочки сертификатов (расширение *.p7b).

Рисунок 19. Окно определения способа получения сертификата в Мастере выпуска сертификата Web-сервера ЦР



Важным моментом является включение в результат обработки запроса на сертификат Web-сервера ЦР списков отзыва сертификатов для всей цепочки сертификатов. Установка опции **Включить...** обеспечивает автоматическую их установку в соответствующий раздел хранилища сертификатов на Центре Регистрации при установке выпущенного сертификата Web-сервера ЦР. Рекомендуется включать данную опцию с целью уменьшения ручных операций и исключения ошибок установки, связанных с ними.

После обработки запроса, будет сформирован файл, в указанном месте расположения и с указанным именем, содержащий цепочку сертификатов.

6. Подключение Центров Регистрации в составе УЦ

Подключение Центров регистрации, входящих в состав Удостоверяющих центров, осуществляется путем выполнения следующих регламентных процедур:

1. Обработка запроса и выпуск сертификата открытого ключа Центра регистрации;
2. Добавление сертификата Центра регистрации в список доверенных ЦР на Центре сертификации.

6.1. Обработка запроса и выпуск сертификата открытого ключа Центра регистрации

Под сертификатом открытого ключа Центра регистрации понимается сертификат открытого ключа (сертификат клиентской аутентификации), с использованием которого осуществляется взаимодействие программного обеспечения Центра регистрации с Центром сертификации.

Обработка запроса и выпуск сертификата открытого ключа Центра регистрации выполняется в следующей последовательности:

1. Получение файла с запросом на сертификат открытого ключа Центра регистрации;
2. Выпуск и сохранение сертификата открытого ключа Центра регистрации;
3. Передача выходных данных в Центр регистрации

6.1.1. Получение файла с запросом на сертификат открытого ключа Центра регистрации

Файл с запросом на сертификат открытого ключа Центра регистрации формируется непосредственно на подключаемом Центре регистрации с использованием приложения **Запрос клиентского сертификата ЦР** из состава приложений Мастеров Центра регистрации. Данный файл содержит запрос на сертификат открытого ключа в формате PKCS#10 в кодировке Base-64.

Вследствие того, что запрос подписан электронно-цифровой подписью на ключе Центра Регистрации, он может быть передан по открытым каналам связи. Необходимо обеспечить достоверную идентификацию отправителя запроса с помощью организационно-технических мероприятий.

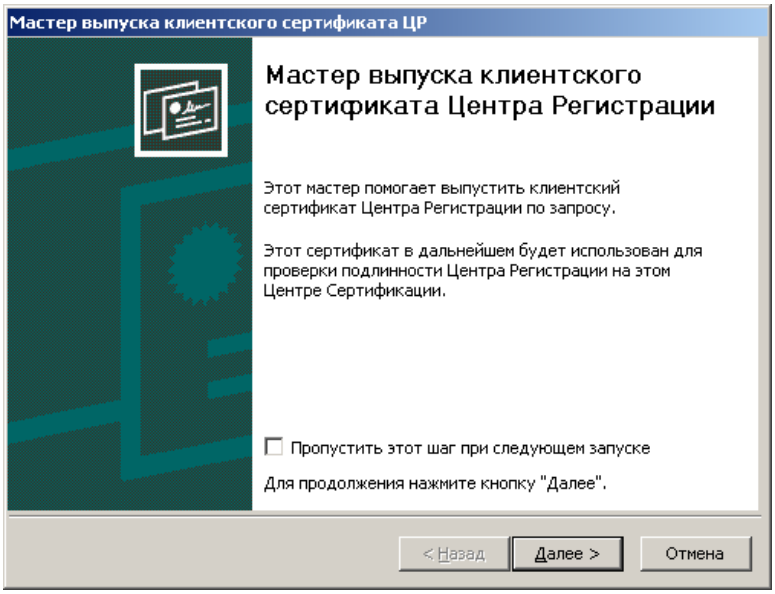
Файл с запросом на сертификат открытого ключа Центра регистрации скопируйте на локальный диск сервера Центра сертификации.

6.1.2. Выпуск и сохранение сертификата открытого ключа Центра регистрации

Выпуск сертификата открытого ключа Центра регистрации осуществляется на основании полученного запроса на сертификат с помощью приложения **Обработка запроса клиентского сертификата ЦР** из состава приложений Мастеров Центра сертификации.

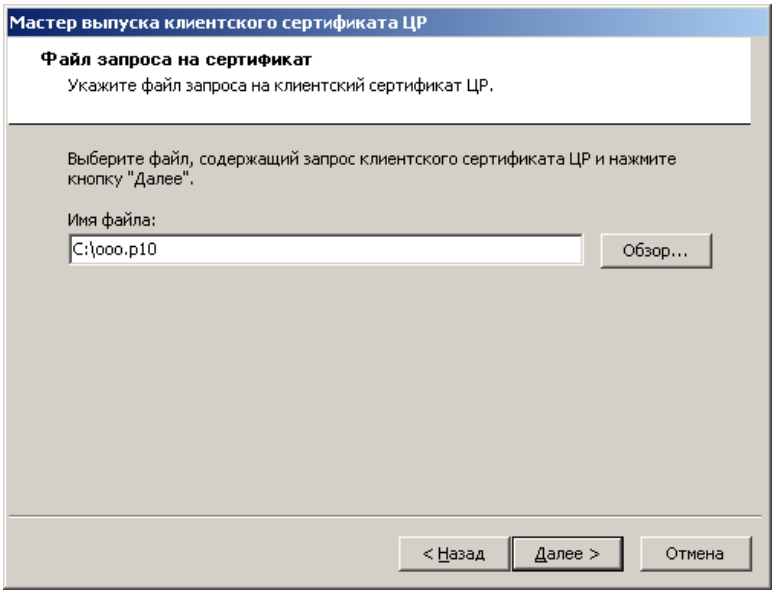
1. Запустить приложение **Обработка запроса клиентского сертификата ЦР** из состава приложений Мастеров Центра сертификации (см. Рисунок 20).

Рисунок 20. Окно Мастера выпуска клиентского сертификата Центра Регистрации



2. В следующем окне с помощью кнопки **Обзор** выберите файл, содержащий запрос на сертификат открытого ключа Центра регистрации (см. Рисунок 21).

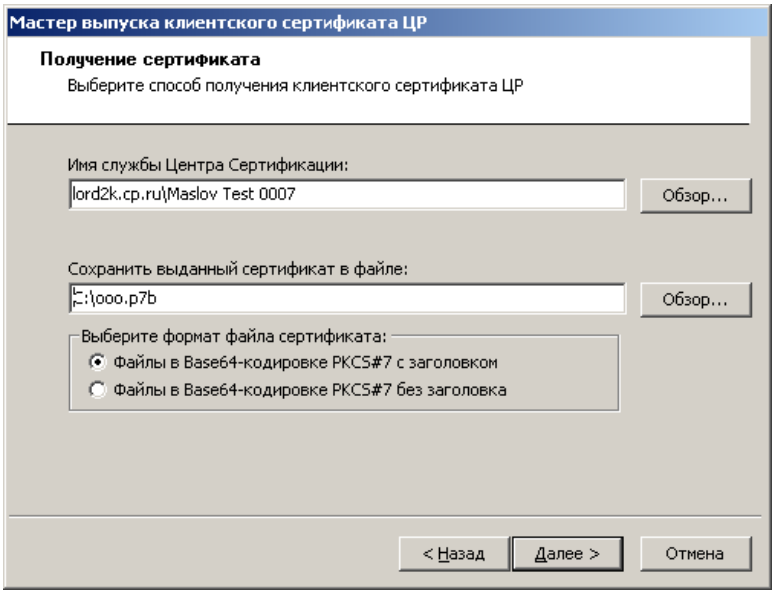
Рисунок 21. Окно выбора файла с запросом Мастера выпуска клиентского сертификата ЦР



3. В информационном окне Мастера убедитесь в корректности информации, содержащейся в запросе на сертификат Центра регистрации. При положительном решении о корректности нажмите кнопку **Далее**.

4. В окне получения сертификата выберите службу Центра сертификации, имя и размещения файла, в котором будет сохранен выпущенный сертификат (см. Рисунок 22). Сохранение сертификата будет осуществлено в формате PKCS#7 в кодировке Base-64, т.е. в виде цепочки сертификатов.

Рисунок 22. Окно получения сертификата Мастера выпуска клиентского сертификата ЦР



5. По завершению работы Мастера нажмите кнопку **Готово**.

6.1.3. Передача выходных данных в Центр регистрации

По завершению выпуска сертификата открытого ключа Центра регистрации, необходимо передать в подключаемый Центр регистрации следующие выходные данные:

- файл с цепочкой сертификатов, сохраненный Мастером выпуска клиентского сертификата ЦР (см. Рисунок 22);
- файл со списком отозванных сертификатов Центра Сертификации, расположенный в каталоге :\WINNT\system32\CertSrv\CertEnroll с расширением *.**crl** .

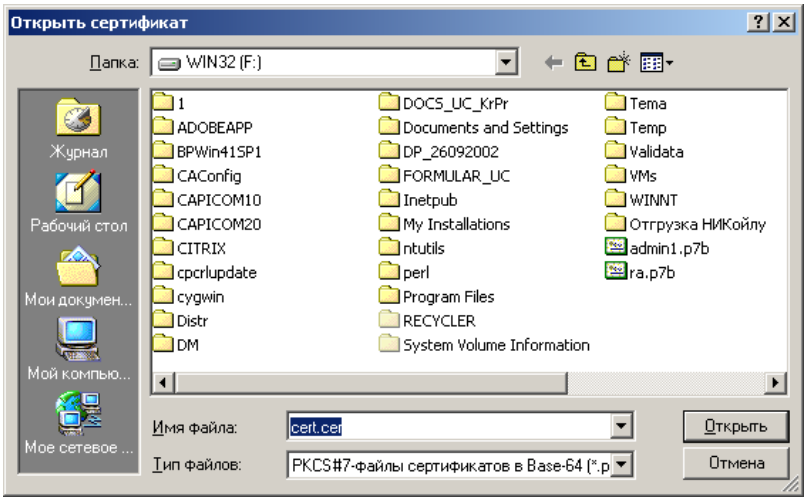
6.2. Добавление сертификата Центра регистрации в список доверенных ЦР на Центре сертификации

Добавление сертификата Центра регистрации в список доверенных ЦР на Центре сертификации осуществляется с использованием приложения **Параметры Центра Сертификации** из группы «Крипто-Про» (см. Рисунок 12).

Для добавления в список выполните следующие действия:

1. На вкладке **Центры регистрации** (см. Рисунок 13) нажмите кнопку **Добавить**.
2. В появившемся окне с использованием кнопки **Обзор** (см. Рисунок 23) выберите файл с сертификатом открытого ключа Центра регистрации, созданного в процессе обработки запроса и выпуска сертификата Центра регистрации.

Рисунок 23. Окно выбора сертификата Центра регистрации при подключении в список доверенных



3. После выбора файла нажмите кнопку **Открыть**.
4. В случае успешного добавления сведения о сертификате появятся в списке доверенных. В противном случае отобразится окно с диагностикой ошибки.

7. Публикация списка отозванных сертификатов

Под публикацией СОС понимается процедура формирования файла СОС и его размещение в установленном каталоге.

Список отозванных (аннулированных) сертификатов (СОС) открытых ключей пользователей и подчиненных Центров сертификации формируется службой сертификации Центра Сертификации и размещается в виде файла в каталоге ..:\WINNT\system32\CertSrv\CertEnroll загрузочного диска.

Имя файла со списком отозванных сертификатов совпадает с именем службы сертификации Центра Сертификации и имеет расширение **.crl**.

7.1. Режимы публикации списка отозванных сертификатов

Публикация списка отозванных сертификатов может осуществляться в трех режимах:

- в автоматическом, с заданной периодичностью;
- в ручном, по запросу администратора Центра Регистрации, имеющего соответствующие права на ЦР;
- в смешанном, с периодичной публикацией СОС по расписанию и внеочередной публикацией СОС по запросу администратора Центра Регистрации, имеющего соответствующие права на ЦР.

Режим и периодичность публикации СОС определяется Регламентом Удостоверяющего Центра.

7.2. Периодичность публикации списка отозванных сертификатов

Задание периодичности публикации СОС осуществляется в окне свойств модуля выхода Крипто-Про УЦ службы сертификации Центра Сертификации (см. Рисунок 2).

При этом, важным для понимания являются две составляющие: интервал публикации и дата следующего обновления, включаемого в CRL.

Под **интервалом публикации** понимается промежуток времени, через который будет выполняться задача службы сертификации ЦС по публикации CRL в виде файла. Таким образом, каждая последующая публикация будет выполняться через интервал публикации, считая от даты предыдущей публикации.

Дата следующего обновления, включаемая в CRL, формируется путем сложения интервала публикации и значения приращения интервала публикации CRL и прибавления полученного временного интервала к дате предыдущей публикации.

В ручном режиме публикации списка отозванных сертификатов, при выполнении запроса, полученного от ЦР, на ЦС будет сформирован файл CRL, значение параметра **Действителен до** будет равно дате выполнения запроса, а значение параметра **Следующее обновление** будет равно дате, получаемой путем прибавления к дате выполнения запроса интервала публикации и значения приращения интервала публикации.

7.3. Публикация списков отозванных сертификатов для доставки в подчиненные УЦ

Удостоверяющий Центр может быть включен в Инфраструктуру Удостоверяющих Центров, построенную по иерархической модели. В этом случае Центр Сертификации УЦ может работать либо в режиме корневого изолированного ЦС, либо в режиме подчиненного изолированного ЦС. Режим определяется режимом установки службы сертификации ЦС (см. раздел **1.3** документа **КриптоПро УЦ Руководство по установке**).

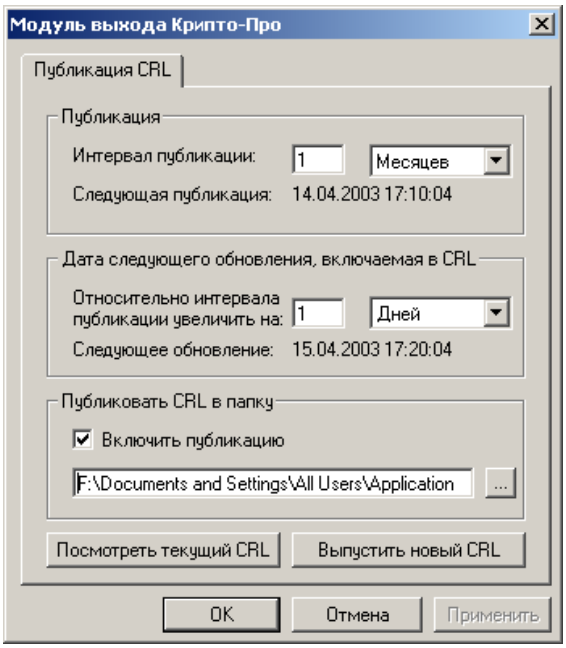
7.3.1. Настройка публикации СОС в режиме корневого изолированного ЦС

В данном режиме под публикацией СОС понимается процедура публикации (формирования файла) CRL, формируемого службой сертификации ЦС, в папку CDP виртуального каталога CA Web-узла ЦС.

Для технического обеспечения публикации СОС в режиме корневого изолированного ЦС необходимо выполнить следующие действия:

1. В окне настройки параметров модуля выхода Крипто-Про УЦ включить публикацию CRL в папку (см. Рисунок 24)

Рисунок 24. Окно параметров модуля выхода с включенной публикацией CRL в папку



2. Перезапустить службу сертификации ЦС

В результате данных настроек при каждом формировании файла CRL службой сертификации ЦС, сформированный файл будет записываться помимо каталога ..:\WINNT\system32\CertSrv\CertEnroll загрузочного диска, также в каталог ..:\Documents and Settings\All Users\Application Data\Crypto Pro\CA\Inetpub\1\CA\CDP\, являющийся домашним каталогом папки CDP виртуального каталога CA Web-узла ЦС (по умолчанию). Имя файла, записываемого в папку CDP, будет совпадать со значением расширения **идентификатор ключа субъекта** сертификата открытого ключа ЦС.

7.3.2. Настройка публикации СОС в режиме подчиненного изолированного ЦС

В данном режиме под публикацией СОС понимается композиция следующих процедур:

- процедура публикации (формирования файла) CRL, формируемого службой сертификации ЦС, в папку CDP виртуального каталога CA Web-узла ЦС;
- процедура репликации файлов CRL, поступивших в папку incoming виртуального каталога CA Web-узла ЦС из вышестоящих УЦ, в папку CDP виртуального каталога CA Web-узла ЦС.

Для технического обеспечения публикации СОС в режиме подчиненного изолированного ЦС необходимо выполнить следующие действия:

1. Включить публикацию CRL в папку в модуле выхода Крипто-Про УЦ (см. Рисунок 24)
2. Перезапустить службу сертификации ЦС
3. Запустить приложение **Задачи Центра сертификации** из группы **Крипто-Про**

4. В списке заданий выберите задание **Перенос СОС** и нажмите кнопку **Свойства**

5. Из пакета заданий выберите первое задание и нажмите кнопку **Свойства**.

В появившемся окне (см. Рисунок 25) необходимо настроить параметры задания. К ним относятся:

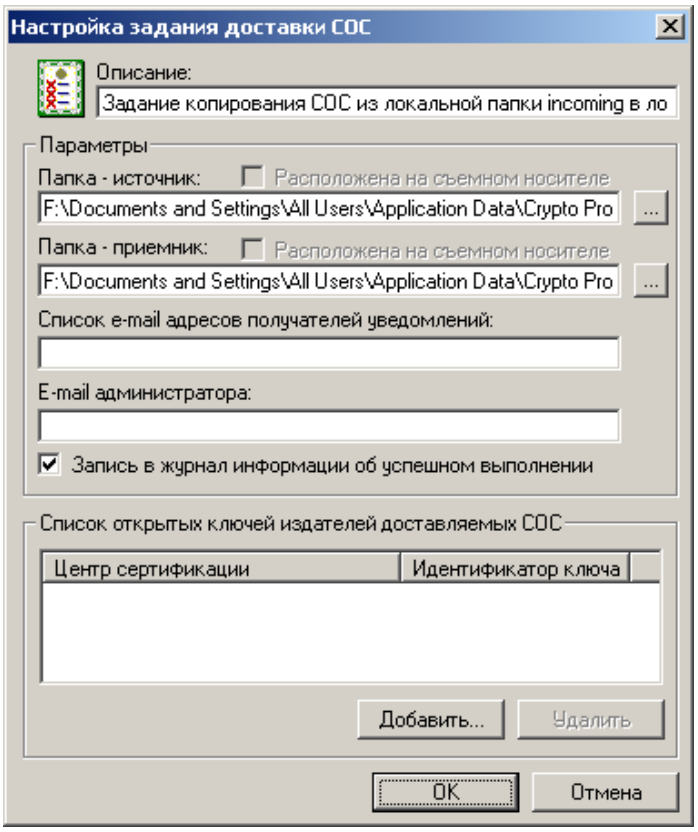
Папка-источник – определяет домашний каталог папки incoming виртуального каталога CA Web-узла ЦС, содержащий файлы с CRL, поступившие от вышестоящих УЦ.

Папка-приемник – определяет домашний каталог папки CDP виртуального каталога CA Web-узла ЦС, 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 будут 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 окна (см. Рисунок 56).

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

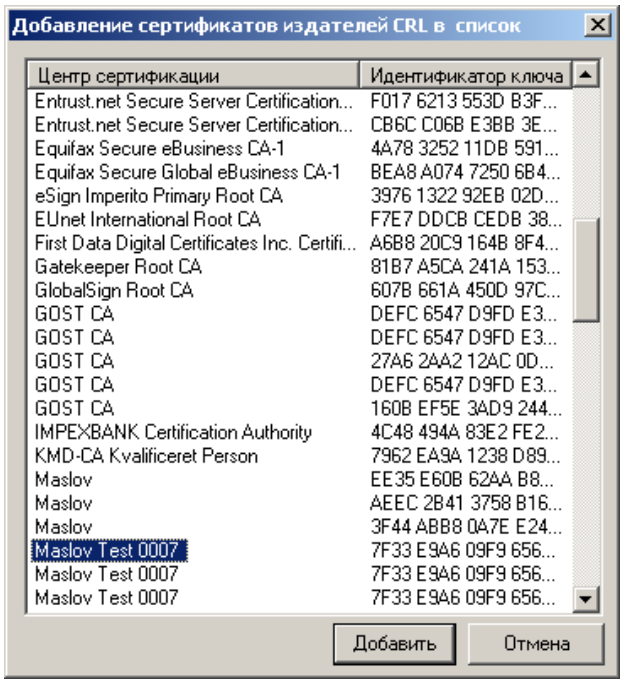
Рисунок 25. Окно свойств настройки задания доставки СОС



Для управления списком открытых ключей издателей доставляемых СОС используются кнопки **Добавить** и **Удалить**.

Для добавления в список издателя необходимо нажать кнопку **Добавить** и в появившемся списке сертификатов доверенных ЦС локального компьютера (информация берется из системного реестра) (см. Рисунок 26) выберите соответствующую строку и нажмите кнопку **Добавить**.

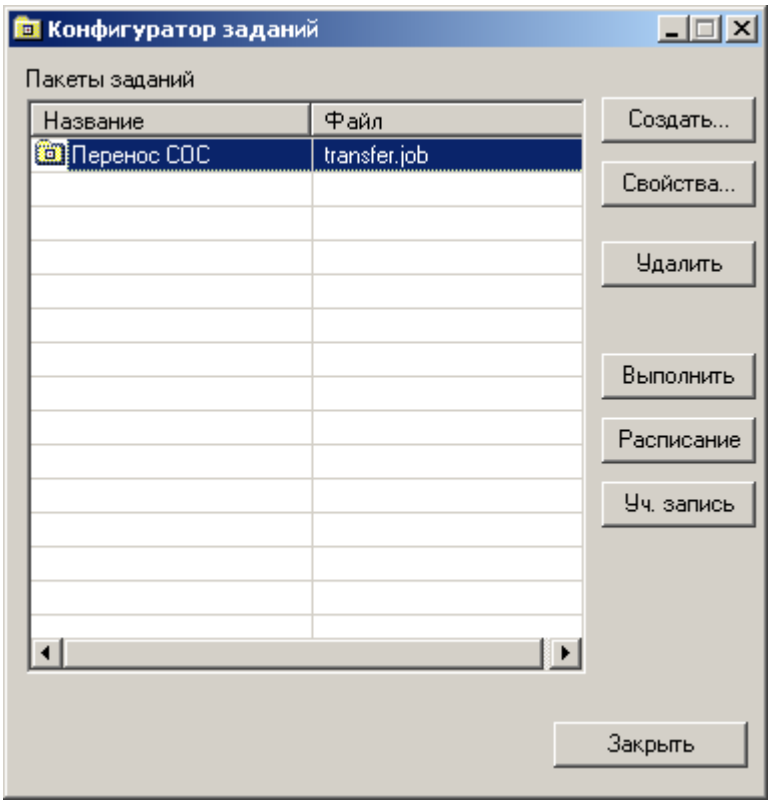
Рисунок 26. Окно добавления издателей СОС в список



В случае если задание настраивается с режимом отправки уведомлений о ходе его работы, необходимо произвести настройку задания отправки сообщений из пакета задания переноса СОС.

6. Запустите приложение **Задачи Центра сертификации** из группы **Крипто-Про**
7. В появившемся окне (см. Рисунок 27) настройте параметры работы задания.

Рисунок 27. Окно конфигурации заданий Центра Сертификации



8. Настройка Центра Сертификации для выпуска сертификатов подчиненных ЦС

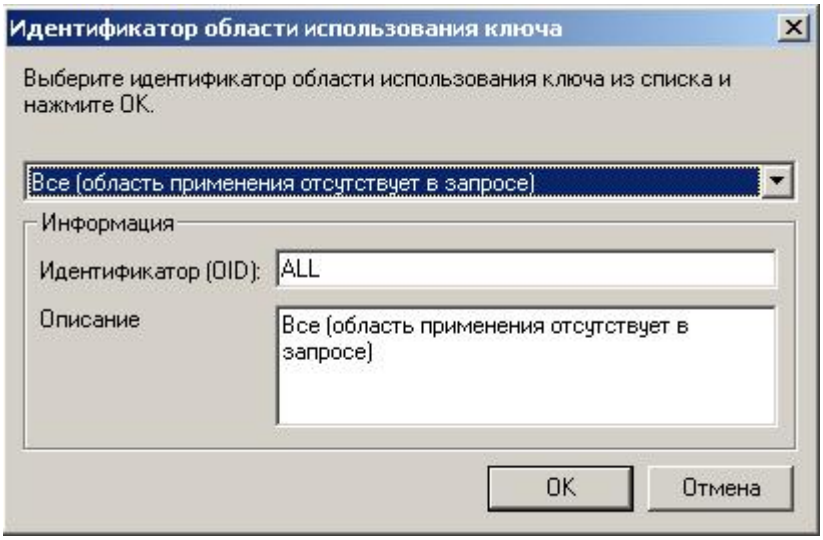
Для обеспечения возможности выпуска сертификата подчиненного Центра Сертификации по запросу на сертификат, выпущенному на Windows 2003 Server, обязательно следует установить на сервере ЦС с ОС Windows 2000 Server обновление KB835732 (http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx) или содержащий его "Накопительный пакет обновлений 1 для Windows 2000 с пакетом обновлений 4" (http://www.microsoft.com/downloads/details.aspx?displaylang=ru&FamilyID=B54730CF-8850-4531-B52B-BF28B324C662).

Настройки модуля политики Центра Сертификации УЦ КриптоПро, устанавливаемые по умолчанию, не позволяют осуществить обработку запроса и выпуск сертификата подчиненного Центра Сертификации.

Для обеспечения этой возможности необходимо выполнить следующие действия:

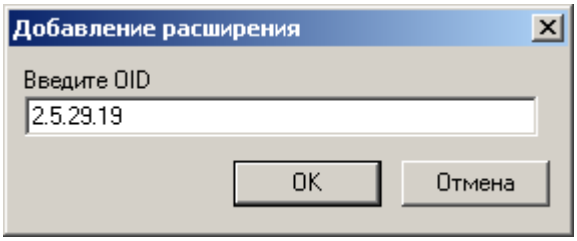
- Запустите административную консоль управления службы сертификации.
- С использованием интерфейса консоли, откройте диалог свойств центра сертификации.
- Выберите закладку **Модуль политики** и нажмите **Настроить** (см. Рисунок 5).
- На вкладке **Использование ключа** добавьте в список идентификаторов области применения идентификатор **Все (область применения отсутствует в запросе)** (см. Рисунок 28).

Рисунок 28. Окно выбора идентификатора сертификатов подчиненных Центров Сертификации при добавлении в список допустимых



- На вкладке **Расширения X.509** добавьте в список допустимых расширений X.509 сертификатов идентификаторы с номерами **2.5.29.19** (см. Рисунок 29), **1.3.6.1.4.1.311.21.1** и **1.3.6.1.4.1.311.20.2**.

Рисунок 29. Окно добавления расширения в список допустимых расширений сертификатов



- Перезапустите службу сертификации.

Рекомендация! Если Центр Сертификации выпускает сертификаты не только подчиненных ЦС, но и обычных пользователей то такую настройку модуля политики Центра Сертификации рекомендуется выполнять перед каждой обработкой запроса на сертификат подчиненного ЦС и убирать изменения после обработки.

9. Формирование запроса на кросс-сертификат Центра Сертификации

Запрос на сертификат Центра Сертификации представляет собой запрос в формате PKCS#10 на изготовление кросс-сертификата Центра Сертификации.

Формирование запроса производится с помощью утилиты **cacertreq.exe** из дистрибутива программного обеспечения Центра Сертификации ПАК «КриптоПро УЦ».

После установки ПО Центра Сертификации указанная утилита располагается по следующему пути **"Program Files\Crypto Pro\CA\bin\cacertreq.exe"**.

Данная утилита разработана по аналогии с утилитой из состава Windows 2003 Server.

Запускается утилита из командной строки.

9.1. Запуск утилиты

CaCertReq.exe -policy [-config CAMachineName\CAName] [-binary] [CACertFileIn [PolicyFileIn [CAPKCS10RequestFileOut]]]

Параметры утилиты:

- -policy: Обязательный аргумент, присутствует по аналогии с утилитой из Windows 2003 Server
- -config: [MachineName\CANoname]. Необязательный аргумент, служит для выбора центра из нескольких установленных либо, при единственном установленном центре, для дополнительной проверки.
- -binary: Необязательный параметр, определяет вид выходных данных. При отсутствии данные выдаются в виде base64 с заголовком --NEW CERTIFICATE REQUEST--, иначе – в DER.
- CaCertFileIn: Необязательный параметр, определяющий имя файла с сертификатом, для которого будет создаваться запрос на кросс-сертификацию. При отсутствии данного параметра запрос будет создан для первого сертификата CA в списке.
- PolicyFileIn: Необязательный параметр, определяет имя файла, содержащего дополнительные параметры запроса на сертификат. Присутствует, только если присутствует параметр CaCertFileIn.
- CAPKCS10RequestFileOut: Необязательный параметр, определяет имя выходного файла, в который будет записан сгенерированный запрос на кросс-сертификат. При отсутствии этого параметра запрос будет выдан на стандартное устройство вывода, это возможно только при отсутствии параметра –binary, иначе возникнет ошибка. Этот параметр присутствует, только если присутствуют параметры CaCertFileIn и CAPKCS10RequestFileOut

В случае, если не задан параметр CAPKCS10RequestFileOut для сохранения запроса в файл можно использовать стандартный механизм перенаправления вывода, т.е. в конце командной строки поставить знак > и задать имя файла. После создания запроса в полученном файле необходимо удалить все символы до начала заголовка запроса, т.е. до строки

-----BEGIN NEW CERTIFICATE REQUEST-----

9.2. Структура файла с дополнительными параметрами

Файл с дополнительными параметрами может состоять из одного или нескольких разделов. Возможные разделы – [Version], [EnhancedKeyUsage], [BasicConstraintsExtension], [CaCertReq] и [SKID].

- [Version] : обязательный раздел. Должен содержать строку Signature="$Windows NT$".
- [EnhancedKeyUsage] : необязательный раздел. Содержит дополнительные значения расширения «Улучшенный ключ» сертификата. Имеет вид OID = value, где value – OID использований ключа, который будет добавлен в запрос. Используется по следующему принципу :
    - Если раздел отсутствует или не содержит ни одного OID, то эти использования ключа будут взяты из сертификата центра (если там есть это расширение)
    - При наличии хотя бы одного OID использования ключа соответствующее расширение сертификата цента будет проигнорировано.

  Также содержит значение Critical, определяющее, является ли это расширение критическим. Если это значение отсутствует, то расширение будет критическим.
- [BasicConstraintsExtension]: необязательный раздел. Содержит дополнительные значения поля «Основные ограничения» сертификата. Если этот раздел отсутствует, то значения берутся из исходного сертификата ЦС. Возможные значения:
    - PathLength – определяет максимально допустимое количество сертификатов промежуточных Центров сертификации (расположенных в иерархии ниже данного сертификата ЦС) при построении цепочки сертификатов.
    - Critical – определяет, является ли это расширение критическим.

  Кроме того, в запрос всегда автоматически заносится поле «Тип субъекта» со значением «ЦС».
- [CaCertReq]: необязательный раздел. Определяет алгоритм хеширования, который будет использован при подписи запроса. Имеет вид hashalg = value, где value может быть или OID алгоритма, или одно из значений: gr3411, sha1 или md5. Если не существует алгоритма подписи для открытого ключа и указанного алгоритма хеширования, то программа завершится с ошибкой. Если этот раздел отсутствует, то перебором будет выбран первый подходящий алгоритм.
- [SKID]: необязательный раздел. Определяет создание расширения SubjectKeyIdentifier. Имеет вид type = value, где value может принимать значение 1 или 2. В зависимости от этого значение SubjectKeyIdentifier генерируется первым или вторым методом, как описано в RFC 3280.
    - Первый метод: значение является 160 битовым хэшем значения BIT STRING открытого ключа (исключая тэг, длину и количество неиспользованных бит)
    - Второй метод: значение состоит из 4х битового поля со значением 0100, сопровождаемым наименее значимыми шестидесятью битами хэша значения BIT STRING открытого ключа (исключая тэг, длину и количество неиспользованных бит)

  Также этот раздел определяет, является ли это расширение критическим или нет (critical = true или critical = false).

  Используется следующим образом:
    - Если в сертификате центра есть расширение SubjectKeyIdentifier, то оно целиком переносится в запрос и этот раздел игнорируется.
    - Если в сертификате нет этого расширения, то используется этот раздел. Если отсутствует какой-либо из параметров или раздел целиком, то по умолчанию применяется первый метод генерации значения SubjectKeyIdentifer и расширение является некритическим.

Также файл может содержать комментарии – строчки, начинающиеся с символа «;».

Пример файла настроек:

```
[Version]
Signature="$Windows NT$"

;Необязательным разделом файла CApolicy.inf является [EnhancedKeyUsage], ;который используется для задания расширения EnhancedKeyUsage OID.

;Можно использовать несколько OID.
 [EnhancedKeyUsage]
OID=1.2.3.4.5
OID=1.2.3.4.6
Critical = False

;Необязательным разделом файла CApolicy.inf является ;[BasicConstraintsExtension], который используется для задания расширения ;Basic Constraints

[BasicConstraintsExtension]
; Subject Type is not supported always set to CA
; maximum subordinate CA path length
PathLength = 3
Critical = False

[CaCertReq]
; алгоритм хеширования
; HashAlg = 1.2.643.2.2.9
HashAlg = gr3411

[SKID]
; генерация расширения SubjectKeyIdentifier
Type = 1
Critical = false
```

10. Сроки действия ключей

10.1. Сроки действия ключей Центра Сертификации

Сроки действия ключей Центра Сертификации определяются Регламентом Удостоверяющего Центра организации, эксплуатирующей программный комплекс. При этом должны выполняться требования:

- Центр Сертификации эксплуатируется в контролируемой зоне.
- Отчуждаемые ключевые носители хранятся в охраняемом помещении и не покидают контролируемой зоны.

Максимальные сроки действия закрытого ключа Центра Сертификации и сертификата Центра Сертификации должны удовлетворять требованиям применяемого СКЗИ.

Максимальный срок действия закрытого ключа Центра Сертификации при использовании СКЗИ «КриптоПро CSP» – 1 год 3 месяца.

Максимальный срок действия сертификата Центра Сертификации при использовании СКЗИ «КриптоПро CSP» – 30 лет.

При использовании СКЗИ «КриптоПро CSP» максимальный срок действия закрытого ключа Центра Сертификации может быть увеличен до 3-х лет при условии обеспечения одной из следующих организационных мер:

- Удостоверяющий Центр функционирует в автономном режиме без подключения к сети организации или публичной сети. Обмен информацией между УЦ и пользователями УЦ осуществляется посредством переноса данных на отчуждаемых носителях (магнитных дискетах и т.д.);
- Для формирования сертификатов открытых ключей пользователей закрытый ключ Центра Сертификации применяется в течение максимального срока действия закрытых ключей используемого СКЗИ, в остальное время исключительно для формирования списка отозванных сертификатов.

Срок действия сертификата открытого ключа корневого Центра Сертификации задается (вводится) при установке службы сертификации Центра Сертификации.

Срок действия сертификата открытого ключа подчиненного Центра Сертификации определяется политиками вышестоящего Центра Сертификации, который производит обработку запроса и выпуск сертификата открытого ключа подчиненного Центра Сертификации.

10.2. Сроки действия ключей пользователей и Web-сервера ЦС

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

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

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

11. Смена ключей Web-сервера Центра Сертификации

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

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

1. Генерация новых ключей, выпуск и установка нового сертификата Web-сервера Центра сертификации;
2. Смена сертификата на Web-узле MS IIS;
3. Уничтожение старых ключей на Центре сертификации;

11.1. Генерация новых ключей, выпуск и установка нового сертификата Web-сервера Центра сертификации

Генерация новых ключей, выпуск и установка нового сертификата Web-сервера Центра сертификации осуществляется с использованием программы-утилиты **Запрос сертификата Web-сервера ЦС** из состава программного обеспечения Центра сертификации (группа **Крипто-Про**). Описание использования этой программы приведено в разделе **4.5.1 п.1** документа **КриптоПро УЦ Руководство по установке.**

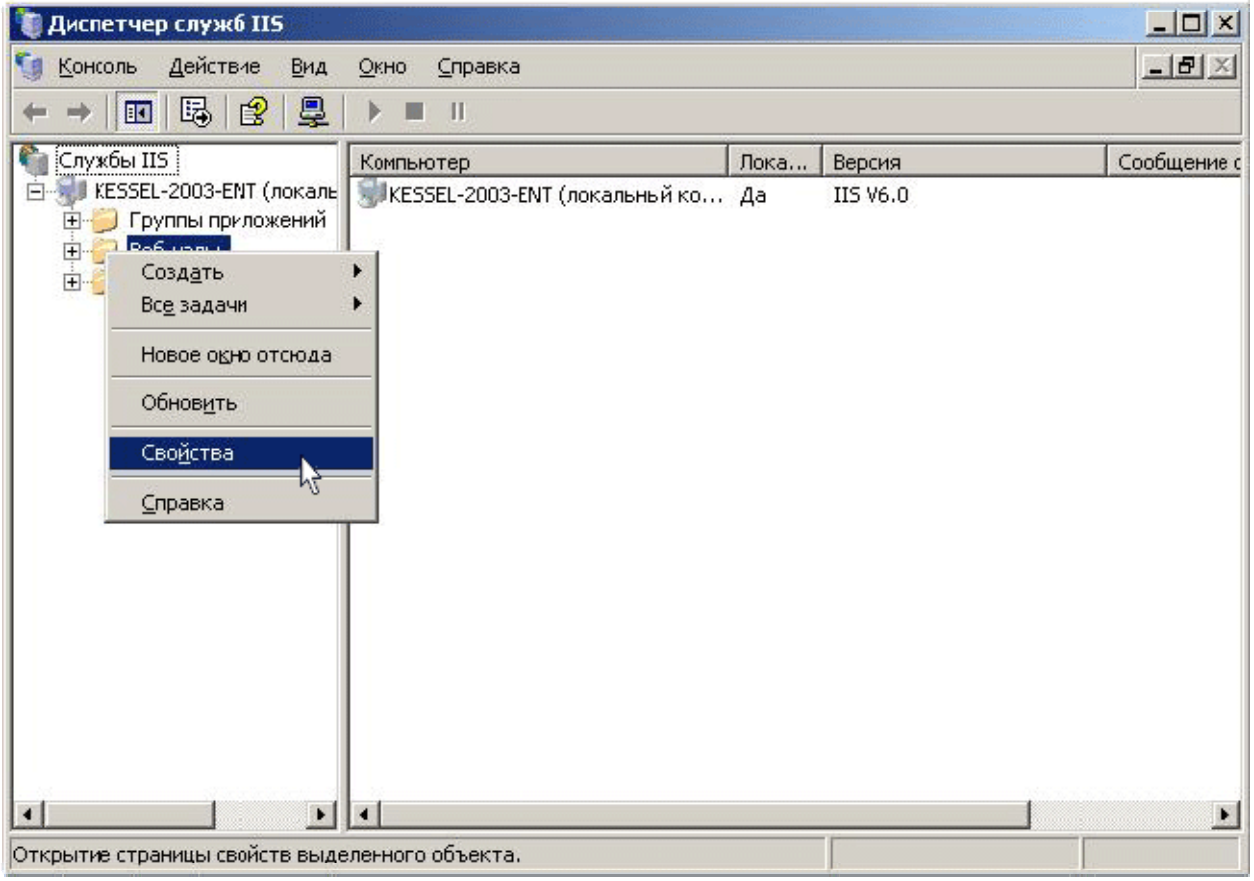
11.2. Смена сертификата на Web-узле MS IIS

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

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

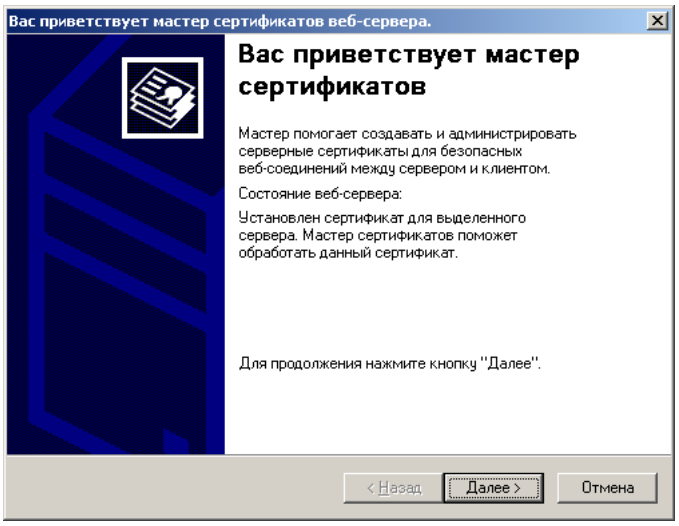
1. Откройте окно свойств Web-узла Web-сервера MS IIS (см. Рисунок 30).

Рисунок 30. Окно свойств Web-узла Web-сервера MS IIS



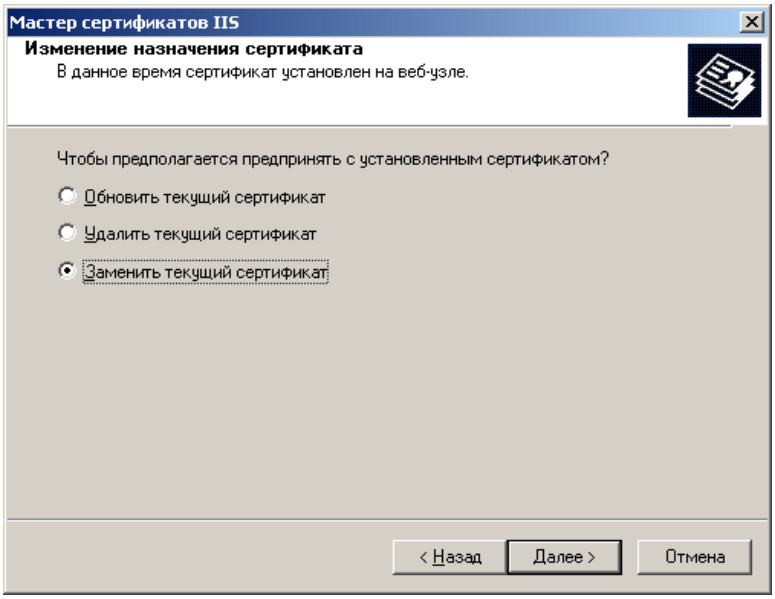
2. Выберите вкладку **Безопасность каталога**.
3. На данной вкладке нажмите кнопку **Сертификат** в группе **Безопасные подключения**.
4. Запустится Мастер сертификатов Web-сервера (см. Рисунок 31).

Рисунок 31. Окно Мастера сертификатов Web-сервера



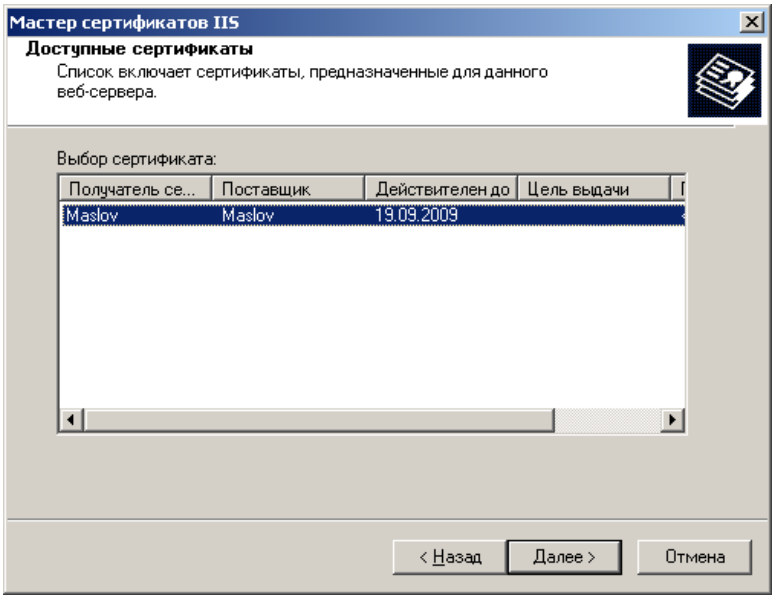
5. Нажмите кнопку **Далее** и в следующем окне выберите **Заменить текущий сертификат** (см. Рисунок 32) и нажмите кнопку **Далее**.

Рисунок 32. Окно изменения назначения сертификата Мастера сертификатов Web-сервера



6. В появившемся окне выберите новый установленный сертификат и нажмите кнопку **Далее** (см. Рисунок 33).

Рисунок 33. Окно выбора сертификата для замены существующего в Мастере сертификатов Web-сервера



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

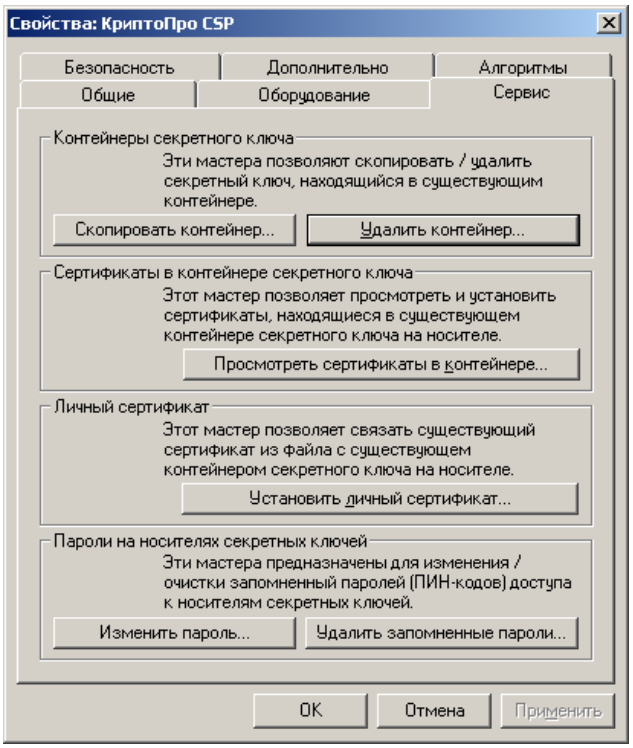
11.3. Уничтожение старых ключей на Центре регистрации

Уничтожение старых ключей Web-сервера Центра сертификации 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 34).

Рисунок 34. Вкладка "Сервис" приложения КриптоПро CSP



12. Смена ключей Центра Сертификации

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

Схема процедуры смены ключей Центра сертификации зависит от режима работы Центра сертификации.

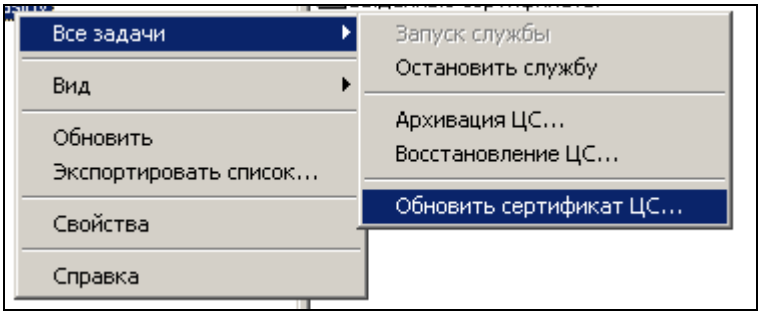
12.1. Смена ключей Центра Сертификации в режиме **Корневой Центр Сертификации**

Смена ключей Центра Сертификации в режиме **Корневой Центр Сертификации** выполняется в следующем порядке:

Остановите службу сертификации Центра сертификации.

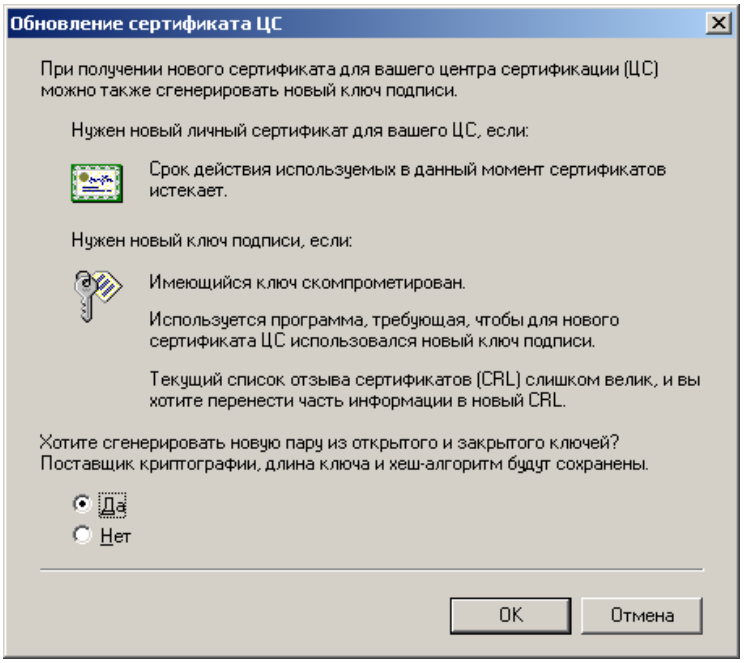
Из списка задач службы сертификации Центра сертификации запустите задачу **Обновить сертификат ЦС**.

Рисунок 35. Задача "Обновить сертификат" службы сертификации ЦС



В окне обновления сертификата ЦС выберите режим создания новых ключей подписи ЦС (отметьте **Да**) и нажмите **ОК**.

Рисунок 36. Окно выбора режима выполнения задачи обновления сертификата службы сертификации ЦС



Выполнится генерация новых ключей Центра сертификации и будет сформирован самоподписанный сертификат Центра сертификации.

После этого запустите службу сертификации Центра сертификации.

12.2. Смена ключей Центра Сертификации в режиме **Подчиненный Центр Сертификации**

Смена ключей Центра Сертификации в режиме **Подчиненный Центр Сертификации** выполняется в следующем порядке:

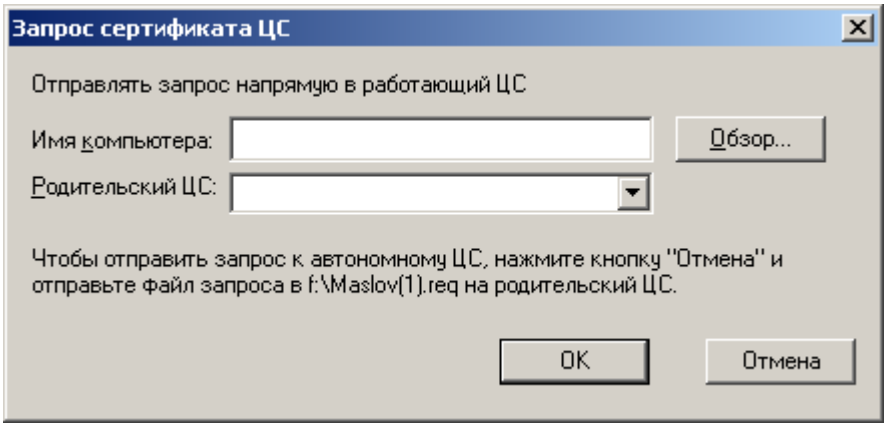
Остановите службу сертификации Центра сертификации.

Из списка задач службы сертификации Центра сертификации (см. Рисунок 35) запустите задачу **Обновить сертификат ЦС**.

В окне обновления сертификата (см. Рисунок 36) ЦС выберите режим создания новых ключей подписи ЦС (отметьте **Да**) и нажмите **ОК**.

Выполнится генерация новых ключей Центра сертификации и будет выведено диалоговое окно (см. Рисунок 37) способа отправки запроса на сертификат ЦС.

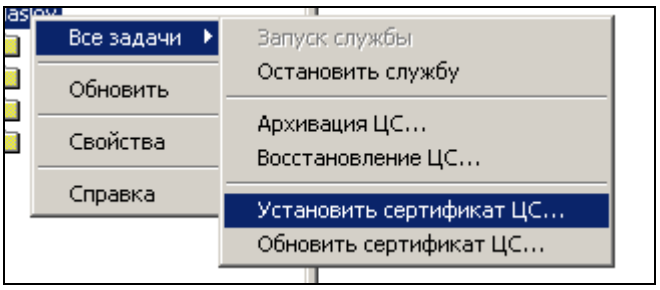
Рисунок 37. Окно назначения обработки запроса в задаче "Обновить сертификат ЦС" подчиненного ЦС



Для обработки запроса на Центре сертификации вышестоящего уровня через файл, нажмите кнопку **Отмена**. На диске будет сформирован файл с именем и размещением, указанным в окне Рисунок 37.

После обработки запроса на сертификат ЦС в вышестоящем Центре сертификации выполните задачу **Установить сертификат ЦС** из списка задач службы сертификации ЦС (см.). Предварительно остановите службу сертификации ЦС.

Рисунок 38. Задача "Установить сертификат" службы сертификации ЦС

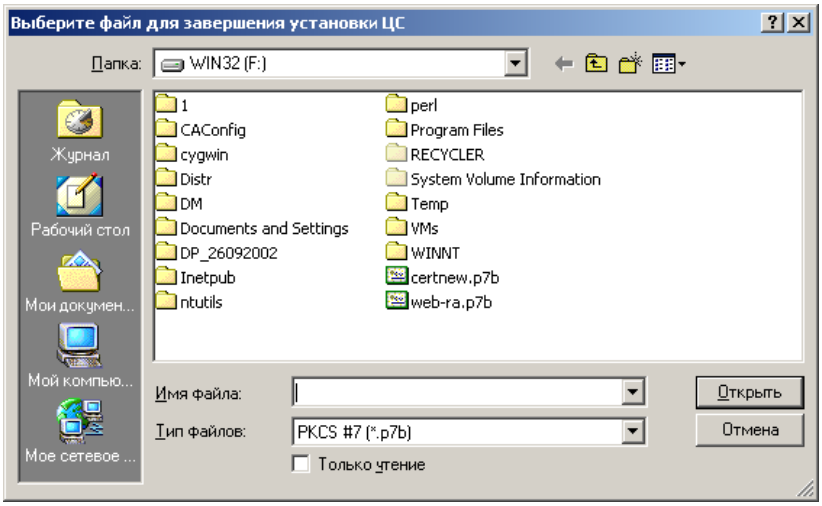


После запуска задачи **Установить сертификат ЦС** на экран будет выведено окно, в котором нужно выбрать файл с выпущенным сертификатом Центра сертификации (см. Рисунок 39).

Выбрав файл с сертификатом ЦС, выполнится установка данного сертификата в службу сертификации ЦС.

После этого запустите службу сертификации Центра сертификации.

Рисунок 39. Окно выбора файла с сертификатом ЦС в задаче "Установить сертификат ЦС" подчиненного ЦС



13. Форматы серийных номеров сертификатов открытых ключей и алгоритмы их формирования

В Центре Сертификации ПК "КриптоПро УЦ" поддерживается два типа (метода) генерации серийных номеров, определяемые настройками Службы сертификации Windows 2000 Server:

1. Тип серийных номеров по умолчанию.
2. Альтернативный тип серийных номеров.

Тип серийных номеров по умолчанию определяется следующим форматом: DWORD от значения GetTickCount() + USHORT индекса службы CA (изменяется от 0 для первого ключа и сертификата Центра Сертификации и увеличивается на 1 при обновлении сертификата Центра Сертификации) + DWORD идентификатора запроса на сертификат (RequestId).

Общая длина 10 байт или 20 шестнадцатеричных цифр.

Альтернативный тип серийных номеров определяется следующим форматом: 1 байт, с фиксированным значением, получаемый из реестра + DWORD идентификатора запроса на сертификат (RequestId) + 8 байт как результат вызова функции CryptGenRandom() + USHORT индекса службы CA (изменяется от 0 для первого ключа и сертификата Центра Сертификации и увеличивается на 1 при обновлении сертификата Центра Сертификации) + DWORD идентификатора запроса на сертификат (RequestId).

Общая длина 19 байт или 38 шестнадцатеричных цифр.

Переход на альтернативный тип серийных номеров и установление фиксированного значения байта в реестре осуществляется выполнением следующей команды на ЦС (пример в части установления значения байта в 0x33): certutil -setreg ca\HighSerial 0x33

При формировании серийного номера сертификата вызов системных функций (GetTickCount, CryptGenRandom) осуществляется при изготовлении КАЖДОГО сертификата. При этом лидирующие нули серийного номера обрезаются.

Таким образом, длина серийного номера при типе серийных номеров по умолчанию является величиной переменной. При альтернативном типе серийных номеров длина серийного номера является величиной постоянной.

14. Обеспечение целостности программных средств Центра Сертификации

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

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

Периодичность контроля целостности программных компонент Центра сертификации – ежесуточно. Выполняется путем перезапуска операционной системы компьютера Центра Сертификации.

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

Наименование модуля	**Расположение (по умолчанию)**
Все файлы *.dll каталога	..:\Program Files\Crypto Pro\CA\bin
Все файлы *.exe каталога	..:\Program Files\Crypto Pro\CA\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\CA\Inetpub\1\CA\

Контроль целостности программных компонент средств СКЗИ, используемых в Центре Сертификации, осуществляется средствами самого СКЗИ.

15. Удаление программного обеспечения Центра сертификации

Удаление программного обеспечения Центра сертификации осуществляется в следующем порядке:

1. Удаление компоненты «КриптоПро УЦ - Центр сертификации»;
2. Удаление приложений «Утилиты Центра сертификации»;
3. Удаление служб Microsoft Certificate Authority, Microsoft Internet Information Services и службы очереди сообщений;
4. Удаление сертификата Центра сертификации (уполномоченного лица Удостоверяющего центра) и Веб-сервера Центра сертификации 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 сертификации.
6. Удаление СКЗИ КриптоПро CSP (КриптоПро TLS) – выполняется в том случае, если в дальнейшем на компьютере Центра сертификации отсутствует необходимость использования СКЗИ.

В том случае, если удаление программного обеспечения Центра сертификации вызвано прекращением деятельности удостоверяющего центра и сертификаты открытых ключей пользователей должны быть отозваны, то необходимо с использованием **АРМ администратора Центра регистрации** или непосредственно из консоли управления Microsoft Certificate Authority отозвать данные сертификаты и изготовить список отозванных сертификатов на срок, соответствующий окончанию срока действия сертификата Центра сертификации (уполномоченного лица Удостоверяющего центра).

Если отзывать сертификаты не требуется, то необходимо без отзыва данных сертификатов изготовить список отозванных сертификатов на срок, соответствующий окончанию срока действия сертификата Центра сертификации (уполномоченного лица Удостоверяющего центра). В данном случае, после удаления программного обеспечения Центра сертификации, в список отозванных сертификатов не удастся занести дополнительную информацию о сертификате (его серийный номер), который потребуется отозвать. Информирование пользователей об отзыве такого сертификата должно реализовываться организационными мерами.

Удаление компоненты «КриптоПро УЦ – Центр сертификации», «Утилиты Центра сертификации» 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 Certificate Authority, 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 Центра сертификации (уполномоченного лица удостоверяющего центра) и сертификата Веб-сервера Центра сертификации 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 сертификации База данных службы Microsoft Certificate Authority не удаляется. База данных остается в том самом месте расположения на жестком диске, где она была создана при первой установке программного обеспечения Microsoft Certificate Authority.

В случае повторной инсталляции службы сертификации Microsoft Certificate Authority на данный компьютер (компьютер, на котором ранее было установлено программное обеспечение Центра сертификации), а также в том случае если при установке используется закрытый ключ и сертификат Центра сертификации, применявшиеся на компьютере Центра сертификации ранее, администратору предоставляется возможность выбора – использовать старую базу данных изданных сертификатов или создать новую.

16. 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

17. Перечень рисунков

Рисунок 1. Вкладка "Модуль выхода" службы сертификации....6
Рисунок 2. Окно свойств модуля выхода КриптоПро УЦ....7
Рисунок 3. Окно свойств модуля выхода КриптоПро УЦ с вкладкой "Расписание публикаций"....8
Рисунок 4. Окно настройки расписания публикаций СОС....9
Рисунок 5. Вкладка "Модуль политики" службы сертификации....12
Рисунок 6. Окно свойств модуля политики КриптоПро УЦ....13
Рисунок 7. Вкладка "Расширения X.509" свойств модуля политики ЦС....14
Рисунок 8. Вкладка "Использование ключа" свойств модуля политики КриптоПро УЦ....15
Рисунок 9. Настройка параметров использования ключа....16
Рисунок 10. Вкладка "Информация о ЦС" свойств модуля политики ЦС....18
Рисунок 11. Вкладка "Журнал" свойств модуля политики ЦС....19
Рисунок 12. Приложение "Параметры Центра сертификации"....20
Рисунок 13. Вкладка "Центры регистрации" средства настройки Центра сертификации....22
Рисунок 14. Вкладка "Сообщения" средства настройки Центра сертификации....23
Рисунок 15. Вкладка "Лицензия" средства настройки Центра сертификации....24
Рисунок 16. Мастер выпуска сертификата WEB-сервера Центра Регистрации....26
Рисунок 17. Окно выбора файла с запросом в Мастере выпуска сертификата WEB-сервера ЦР 26
Рисунок 18. Окно с информацией о запросе Мастера выпуска сертификата Web-сервера ЦР ...27
Рисунок 19. Окно определения способа получения сертификата в Мастере выпуска сертификата Web-сервера ЦР....27
Рисунок 20. Окно Мастера выпуска клиентского сертификата Центра Регистрации....30
Рисунок 21. Окно выбора файла с запросом Мастера выпуска клиентского сертификата ЦР....30
Рисунок 22. Окно получения сертификата Мастера выпуска клиентского сертификата ЦР....31
Рисунок 23. Окно выбора сертификата Центра регистрации при подключении в список доверенных....32
Рисунок 24. Окно параметров модуля выхода с включенной публикацией CRL в папку....34
Рисунок 25. Окно свойств настройки задания доставки СОС....35
Рисунок 26. Окно добавления издателей СОС в список....36
Рисунок 27. Окно конфигурации заданий Центра Сертификации....36
Рисунок 28. Окно выбора идентификатора сертификатов подчиненных Центров Сертификации при добавлении в список допустимых....37
Рисунок 29. Окно добавления расширения в список допустимых расширений сертификатов ...38
Рисунок 30. Окно свойств Web-узла Web-сервера MS IIS....44
Рисунок 31. Окно Мастера сертификатов Web-сервера....44
Рисунок 32. Окно изменения назначения сертификата Мастера сертификатов Web-сервера....45
Рисунок 33. Окно выбора сертификата для замены существующего в Мастере сертификатов Web-сервера....45
Рисунок 34. Вкладка "Сервис" приложения КриптоПро CSP....46
Рисунок 35. Задача "Обновить сертификат" службы сертификации ЦС....47

Рисунок 36. Окно выбора режима выполнения задачи обновления сертификата службы сертификации ЦС 47

Рисунок 37. Окно назначения обработки запроса в задаче "Обновить сертификат ЦС" подчиненного ЦС 48

Рисунок 38. Задача "Установить сертификат" службы сертификации ЦС 48

Рисунок 39. Окно выбора файла с сертификатом ЦС в задаче "Установить сертификат ЦС" подчиненного ЦС 49