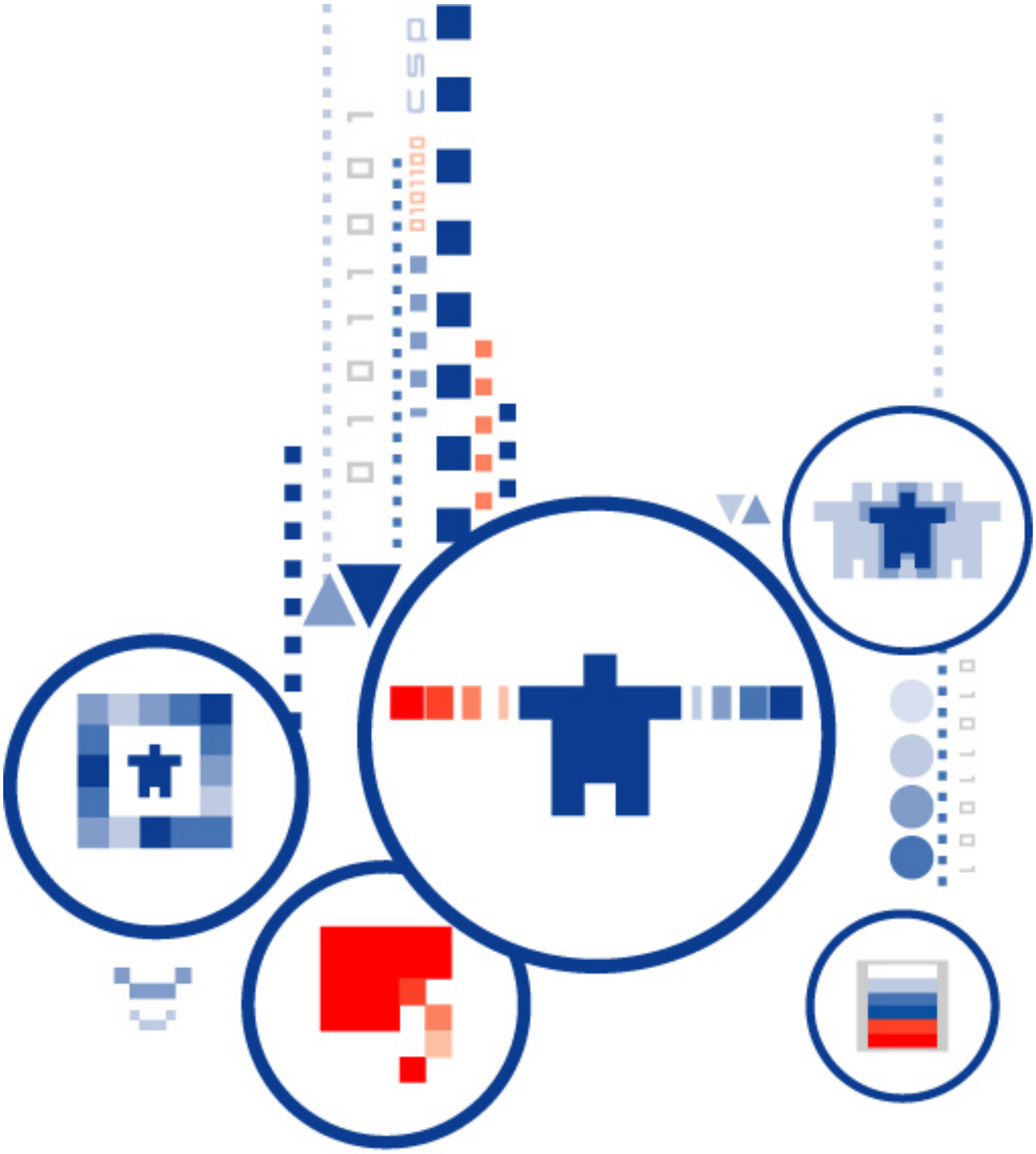
УТВЕРЖДЕН
ЖТЯИ.00035-01 90 12-ЛУ

ЖТЯИ.00035-01 90 12



КриптоПро УЦ

программно-аппаратный комплекс
удостоверяющий центр

Руководство по восстановлению работоспособности компонент

Аннотация

Настоящий документ содержит описание процесса восстановления работоспособности компонент программного комплекса «КриптоПро УЦ» после программно-аппаратных сбоев, повлекших полную или частичную потерю работоспособности и/или данных.

Настоящий документ может использоваться в качестве руководства по осуществлению переноса программных компонент Удостоверяющего центра с одних технических средств на другие (например, при модернизации оборудования).

Документ предназначен для администраторов Удостоверяющих центров.

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. Общие положения 4
2. Восстановление Центра Сертификации ПК «КриптоПро УЦ» 5
2.1. Исходные данные 5
2.2. Установка общесистемного программного обеспечения 5
2.3. Установка СКЗИ «КриптоПро CSP» 5
2.4. Установка сертификата Центра сертификации 6
2.5. Установка службы сертификации Microsoft Certificate Authority 11
2.6. Восстановление из архива базы данных Центра Сертификации 15
2.7. Установка утилит Центра сертификации 18
2.8. Установка сертификата WEB-сервера Центра Сертификации 18
2.9. Установка программного обеспечения Центра сертификации ПК «КриптоПро УЦ» 19
2.10. Настройка программного обеспечения Центра сертификации ПК «КриптоПро УЦ» 19
3. Восстановление Центра Регистрации ПК «КриптоПро УЦ» 20
3.1. Исходные данные 20
3.2. Установка общесистемного программного обеспечения 21
3.3. Установка СКЗИ «КриптоПро CSP» 22
3.4. Установка утилит Центра Регистрации 22
3.5. Установка сертификата Центра Сертификации. 22
3.6. Установка сертификата WEB-сервера Центра Регистрации 22
3.7. Установка программного обеспечения Центра регистрации ПК «КриптоПро УЦ» 22
3.8. Установка сертификата Центра Регистрации 23
3.9. Восстановление Базы данных Центра Регистрации 23
3.10. Настройка программного обеспечения Центра Регистрации ПК «КриптоПро УЦ» 31
4. Восстановление АРМ администратора Центра Регистрации ПК «КриптоПро УЦ» 33
4.1. Исходные данные 33
4.2. Установка общесистемного программного обеспечения и СКЗИ «КриптоПро CSP» 33
4.3. Установка программного обеспечения АРМ администратора Центра регистрации ПК «КриптоПро УЦ» 33
4.4. Установка сертификата Центра сертификации. 33
4.5. Установка сертификата привилегированного пользователя 33

1. Общие положения

Выполнение мероприятий по восстановлению работоспособности компонент программного комплекса «КриптоПро УЦ» обеспечит работу комплекса на восстановленной базе данных.

При этом важно отметить особенности восстановления работоспособности, связанные с настройками параметров работы компонент программного комплекса «КриптоПро УЦ».

Существуют стандартные настройки параметров работы компонент программного комплекса «КриптоПро УЦ», которые устанавливаются при выполнении инсталляции программного обеспечения этих компонент.

Эти стандартные настройки могут быть изменены в ходе конфигурации ПАК «КриптоПро УЦ» после установки программного обеспечения.

Часть настроек, а именно настройки Центра Регистрации, сохраняются в базе данных и восстанавливаются с резервной копии. Остальные настройки ПАК «КриптоПро УЦ» после восстановления с резервной копии необходимо установить вручную.

Настройки Центра Регистрации, сохраняемые в базе данных:

- Настройки на вкладке **Политики**:
    - Дополнительные параметры базы данных;
    - Обработка запросов на отзыв;
    - Обработка неподписанных запросов;
    - Обработка подписанных запросов;
    - Политика имен;
    - Системные роли;
    - Шаблоны писем;
    - Шаблоны сертификатов;
- Настройка действий на вкладке **Безопасность**

2. Восстановление Центра Сертификации ПК «КриптоПро УЦ»

2.1. Исходные данные

Для восстановления Центра Сертификации ПК «КриптоПро УЦ» необходимо иметь, как минимум, следующий набор исходных данных:

- Закрытый ключ уполномоченного лица Удостоверяющего центра (закрытый ключ Центра сертификации), находящийся в контейнере закрытого ключа на внешнем носителе;
- Сертификат уполномоченного лица Удостоверяющего центра (сертификат открытого ключа Центра сертификации) в виде файла на внешнем носителе;
- Сертификаты уполномоченных лиц Удостоверяющих центров (сертификаты Центров сертификации) вышестоящих по иерархии Удостоверяющих центров, включая сертификат уполномоченного лица корневого Удостоверяющего центра в виде файла (файлов) на внешнем носителе (если восстанавливаемый Удостоверяющий центр является подчиненным);
- Архив базы данных Центра сертификации, включающий журнал выданных сертификатов и очередь запросов на сертификат в виде набора файлов на внешнем носителе (подготовленный в соответствии с разделом 2.2 документа ЖТЯИ.00035-01 90 11. «КриптоПро УЦ Руководство администратора баз данных»).

Указанный выше набор исходных данных является минимальным, при котором возможно восстановление работоспособности Центра Сертификации ПК «КриптоПро УЦ». Поэтому лицу, ответственному за эксплуатацию программного обеспечения ПК «КриптоПро УЦ», нужно обеспечить создание, хранение, своевременное обновление (актуализацию) и доступность этих данных.

Рекомендуется также иметь следующие данные:

- Закрытый ключ WEB-сервера Центра сертификации, находящийся в контейнере закрытого ключа на внешнем носителе;
- Сертификат WEB-сервера Центра сертификации в виде файла на внешнем носителе;
- Сертификат Центра регистрации Удостоверяющего центра на внешнем носителе;
- Нормативные документы Удостоверяющего центра (Регламент Удостоверяющего центра, Положение об Удостоверяющем центре), определяющие настройки Центра сертификации.

2.2. Установка общесистемного программного обеспечения

Установка общесистемного программного обеспечения осуществляется в соответствии с требованиями пункта 2.1 «Требования к программным и техническим средствам» документа ЖТЯИ.00035-01 90 02. «КриптоПро УЦ Руководство по установке».

2.3. Установка СКЗИ «КриптоПро CSP»

Установка и настройка СКЗИ «КриптоПро CSP» осуществляется в соответствии с пунктом 3.2 «Установка СКЗИ КриптоПро CSP и КриптоПро TLS» документа ЖТЯИ.00035-01 90 02. «КриптоПро УЦ. Руководство по установке».

2.4. Установка сертификата Центра сертификации

2.4.1. Установка сертификата Центра сертификации в хранилище сертификатов **Локальный компьютер/Доверенные корневые центры сертификации.**

В случае если восстанавливаемый Удостоверяющий центр является корневым, то необходимо установить сертификат Центра сертификации в хранилище сертификатов **Локальный компьютер/Доверенные корневые центры сертификации.**

В случае если восстанавливаемый Удостоверяющий центр является подчиненным, то необходимо установить сертификат Центра сертификации в хранилище сертификатов **Локальный компьютер/Промежуточные центры сертификации.** Дополнительно необходимо установить все сертификаты вышестоящих Центров сертификации, за исключением сертификата корневого Центра сертификации в хранилище сертификатов **Локальный компьютер/Промежуточные центры сертификации.** Сертификат корневого Центра сертификации необходимо установить в хранилище сертификатов **Локальный компьютер/Доверенные корневые центры сертификации.**

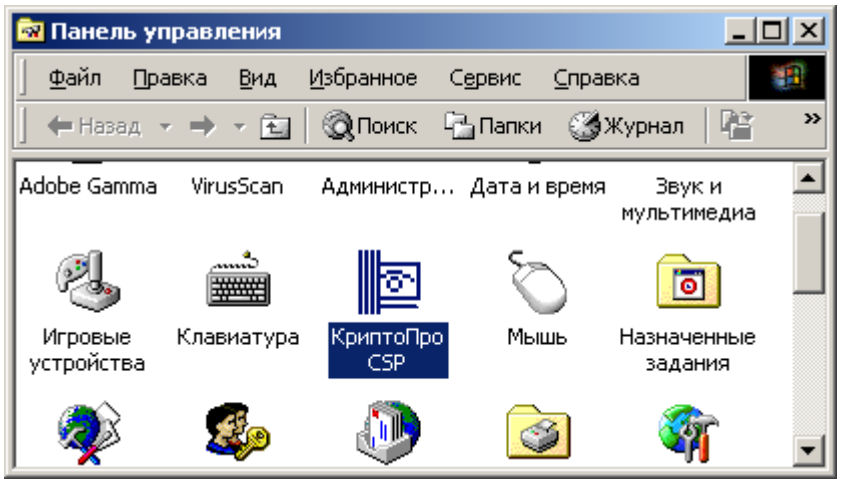
Установка этих сертификатов в хранилище сертификатов **Локального компьютера** осуществляется с помощью стандартного **Мастера импорта сертификатов** ОС Windows (см. раздел **Импорт и экспорт сертификатов** стандартного справочника ОС Windows 2000) с выбором физического хранилища сертификатов.

2.4.2. Установка сертификата Центра сертификации в хранилище сертификатов **Локальный компьютер/Личные**.

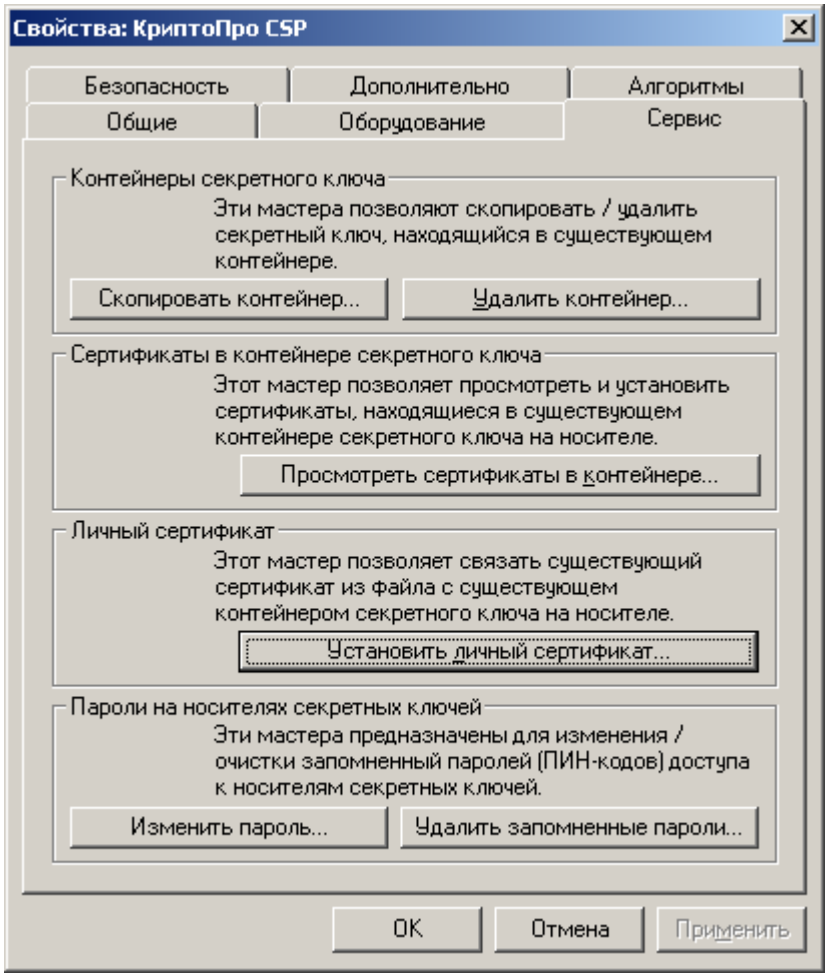
После установки необходимо сертификата Центра сертификации в хранилище сертификатов **Локальный компьютер/Доверенные корневые центры сертификации** установить сертификат Центра сертификации восстанавливаемого Удостоверяющего центра в хранилище **Локальный компьютер/Личные.** Данная установка осуществляется с использованием СКЗИ «КриптоПро CSP».

Последовательность действий по установке сертификата Центра сертификации в хранилище **Локальный компьютер/Личные**:

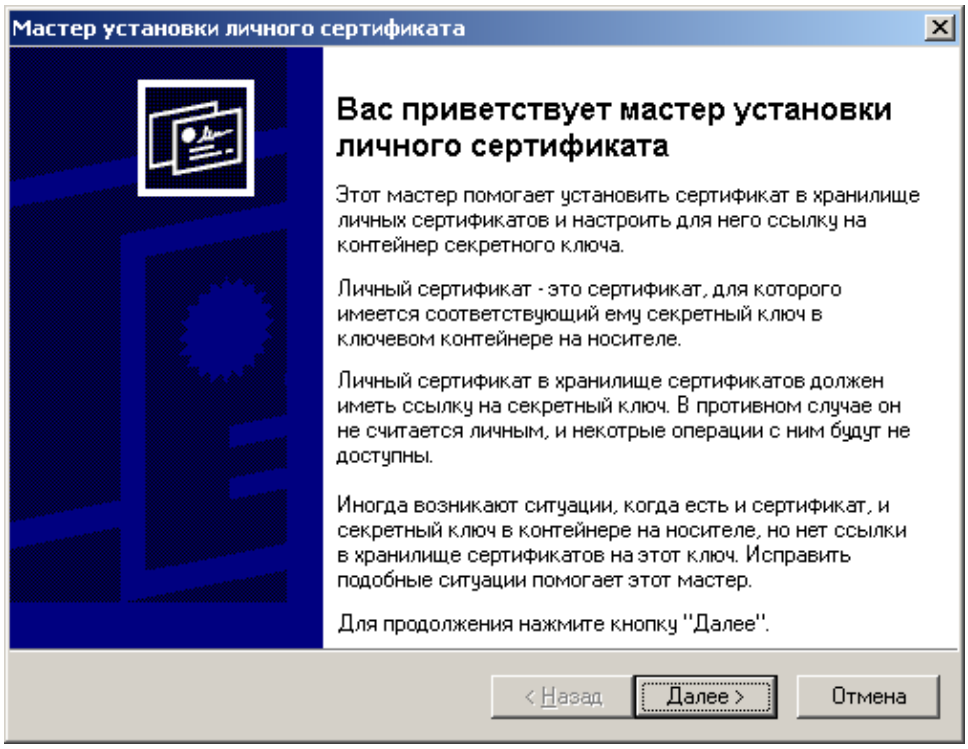
1. Откройте панель управления компьютером, используя пункты меню **Пуск, Настройка, Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**.



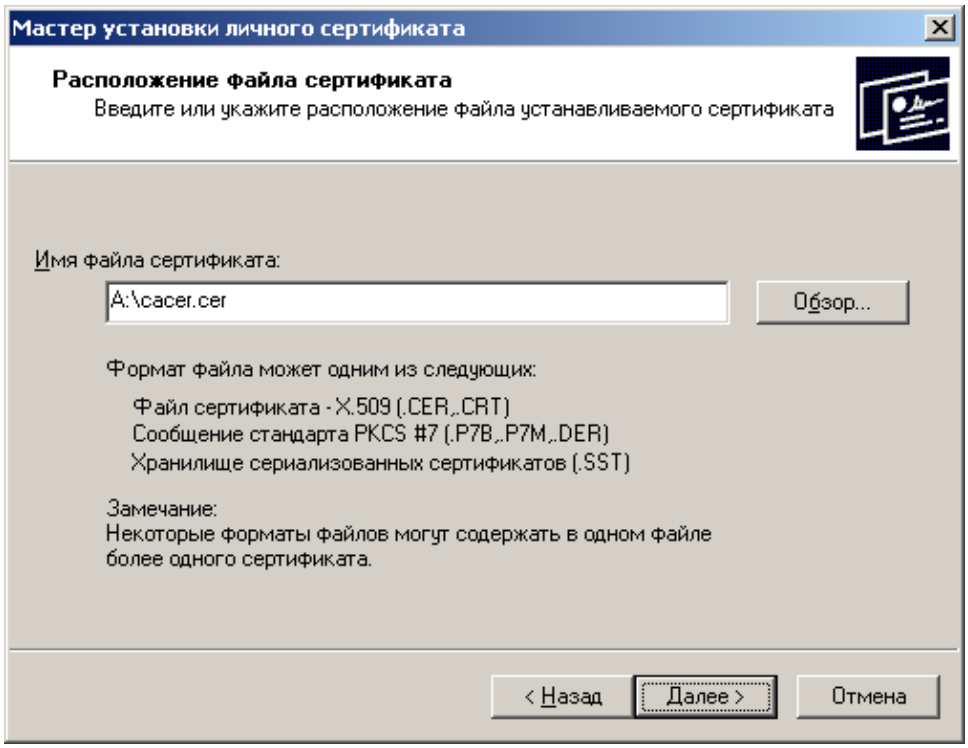
2. В отображаемом окне **Свойства: КриптоПро CSP** выберите закладку **Сервис** и нажмите кнопку **Установить личный сертификат**.



3. В появившемся окне **Мастер установки личного сертификата** ознакомьтесь с текстом и нажмите кнопку **Далее**

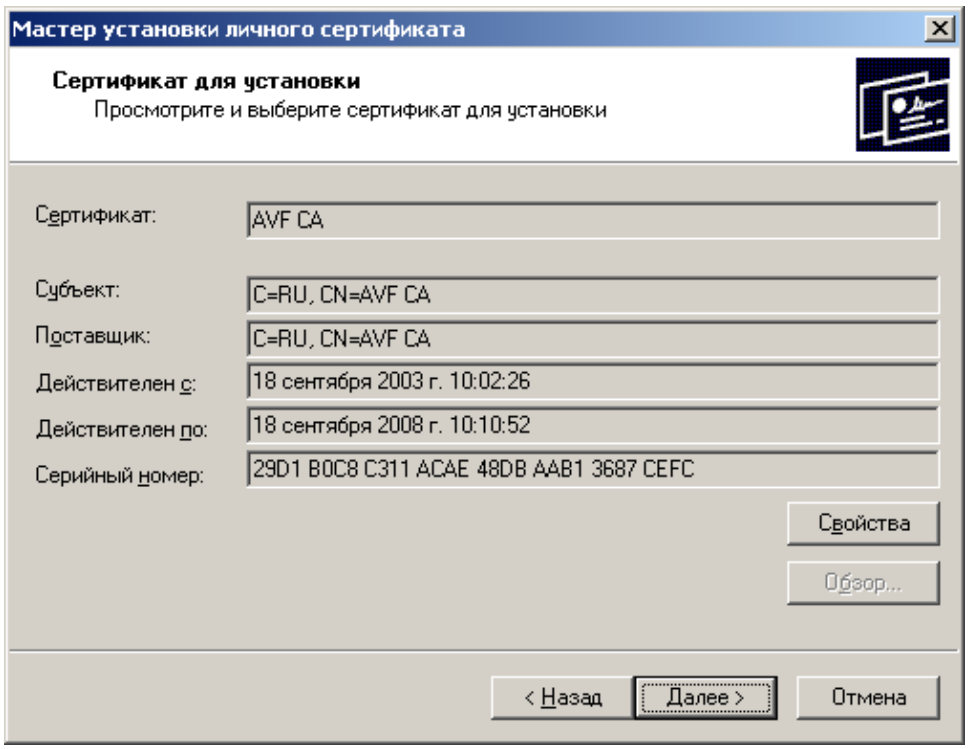


4. Откроется окно **Расположение файла сертификата.** Укажите полный путь к файлу сертификата Центра сертификации на внешнем носителе или выберите его с помощью кнопки **Обзор.** Нажмите кнопку **Далее.**

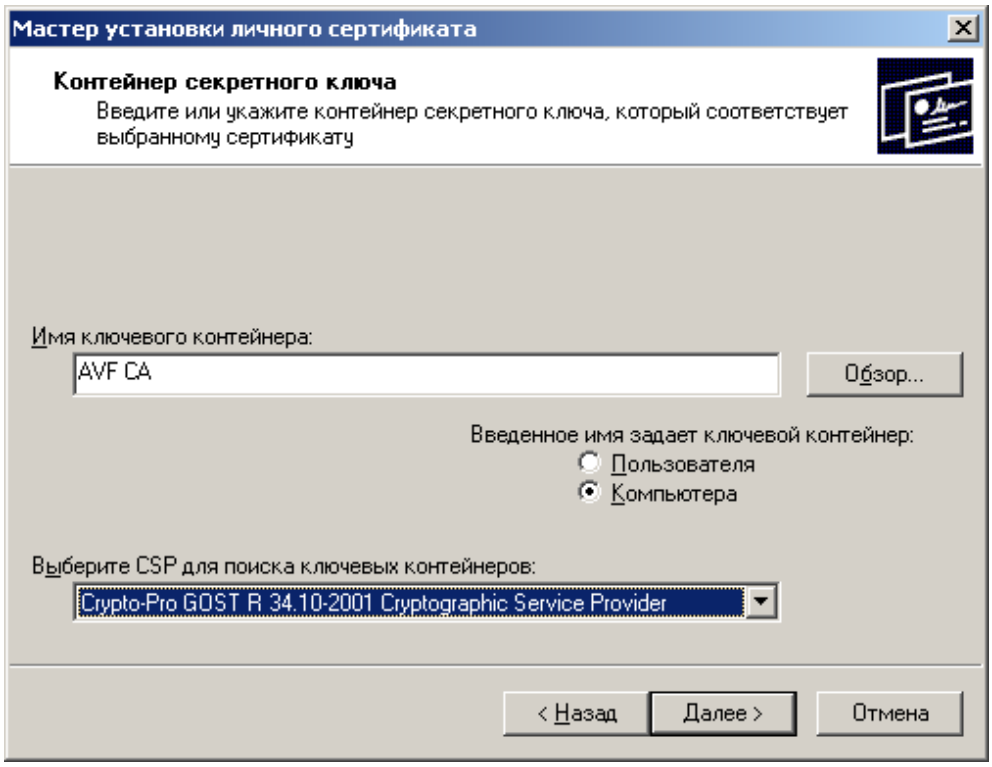


5. В окне **Сертификат для установки** выводится основная информация о сертификате. Нажав на кнопку **Свойства** можно просмотреть

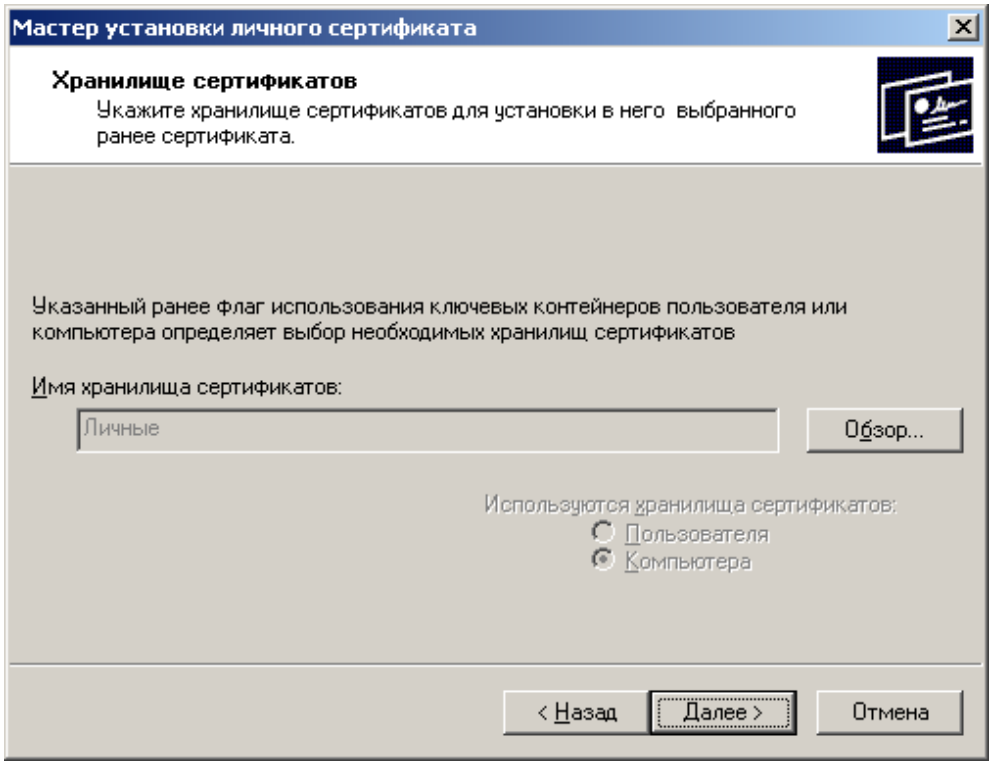
сертификат в стандартном окне просмотра сертификата. Нажмите кнопку **Далее.**



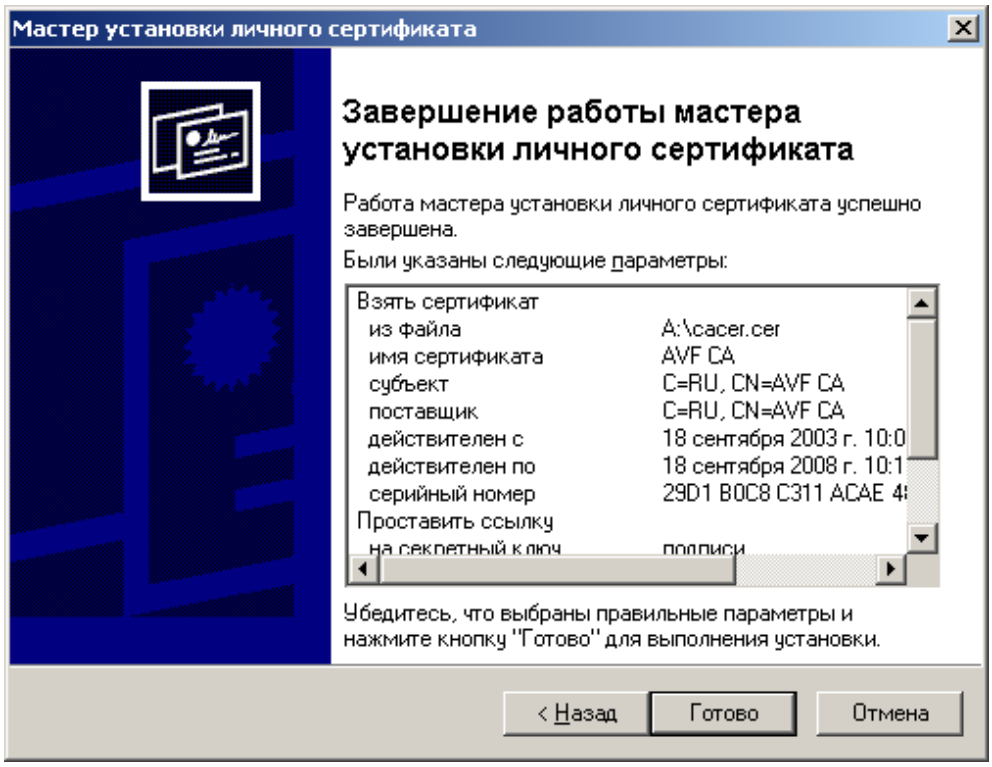
6. В появившемся окне **Контейнер секретного ключа** установите переключатель **Введенное имя задает ключевой контейнер** в положение **Компьютер**, выберите необходимый CSP из предлагаемого списка. С помощью кнопки **Обзор** выберите ключевой контейнер, содержащий закрытый ключ Центра сертификации. Нажмите кнопку **Далее**.



7. Откроется окно **Хранилище сертификатов,** в котором необходимо с помощью кнопки **Обзор** выбрать хранилище сертификатов **Личные**



8. В окне **Завершение работы Мастера установки личного сертификата** убедитесь, что указаны правильные параметры и нажмите кнопку **Готово**.

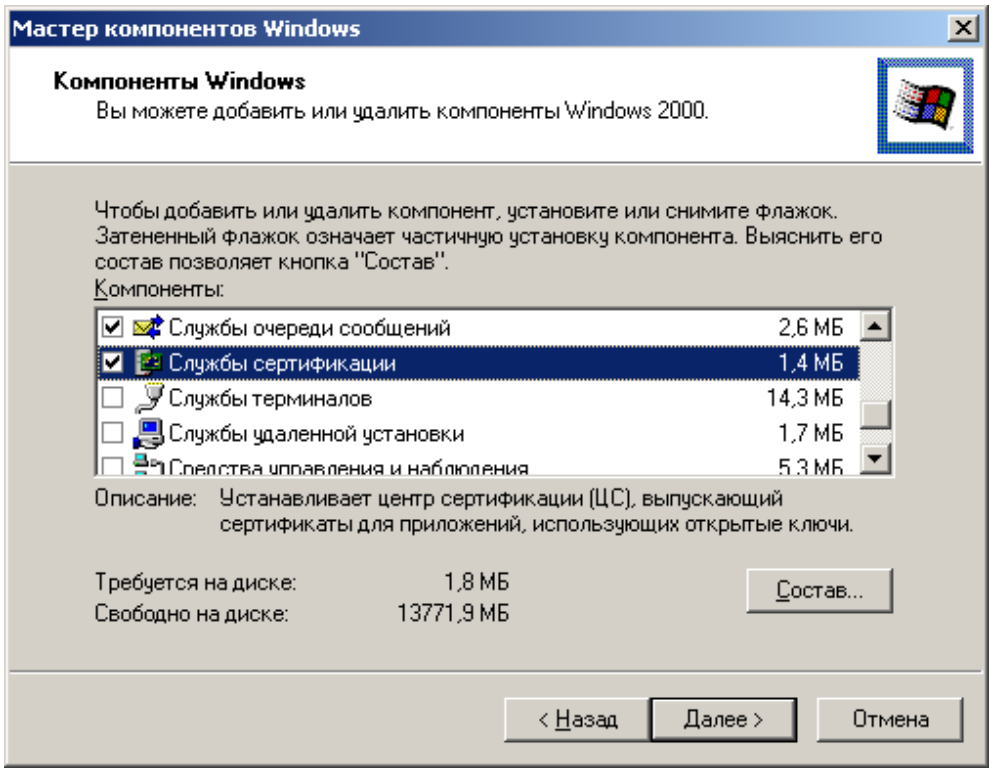


Примечание: Если необходимо изменить тип ключевого носителя закрытого ключа Центра сертификации, то перед установкой сертификата Центра сертификации необходимо скопировать контейнер закрытого ключа Центра сертификации на ключевой носитель нового типа. Данная операция осуществляется с помощью сервисной функции **Скопировать контейнер** СКЗИ «КриптоПро CSP» (окно **Свойства: КриптоПро CSP,** вкладка **Сервис,** кнопка **Скопировать контейнер**). После копирования ключевого контейнера выполните установку сертификата Центра сертификации в хранилище сертификатов **Локальный компьютер/Личные** из нового контейнера.

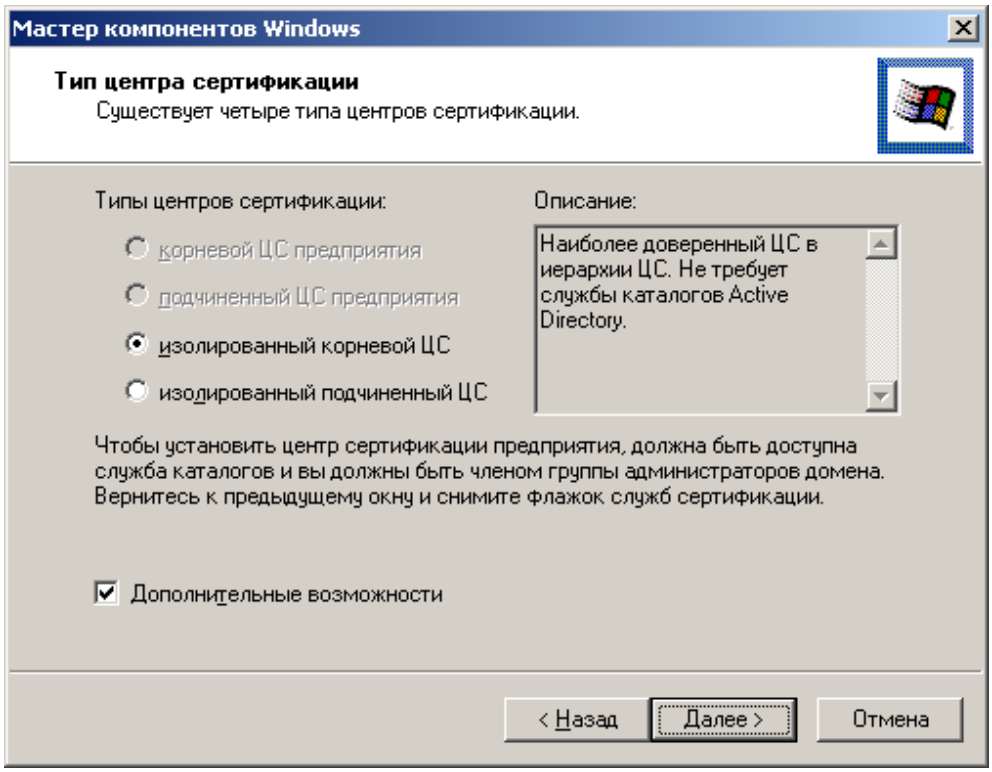
2.5. Установка службы сертификации Microsoft Certificate Authority

Установка службы сертификации Microsoft Certificate Authority осуществляется в следующей последовательности:

1. Откройте окно **Панели управления**, выполнив команды **Пуск**, **Настройка**, **Панель управления**.
2. В окне **Панели управления** выберите пункт **Установка и удаление программ**.
3. В окне **Установки и удаления программ** выберите пункт **Добавление и удаление компонент Windows**.
4. В окне мастера добавления компонент выберите **Службы сертификации**, нажмите кнопку **Далее**.

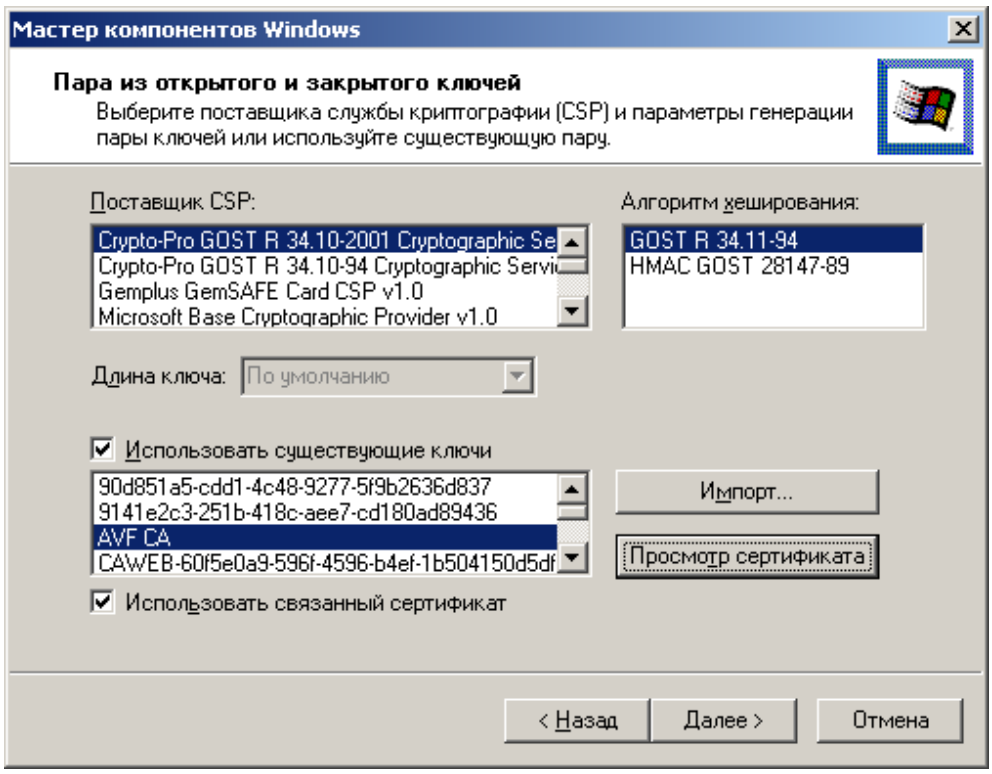


5. В окне **Тип центра сертификации** выберите соответствующий тип Центра сертификации и нажмите кнопку **Далее**.

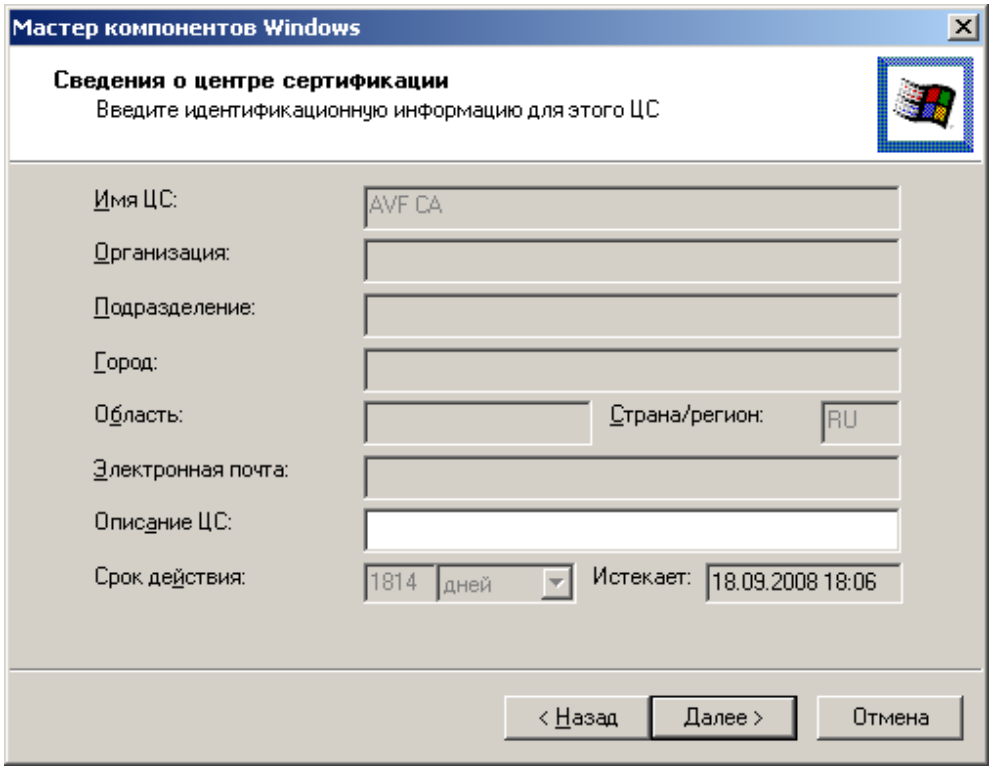


6. Откроется окно **Пара из открытого и закрытого ключей.** Выберите из списка поставщика CSP. Установите флаг **Использовать существующие ключи** и выберите имя контейнера закрытого ключа

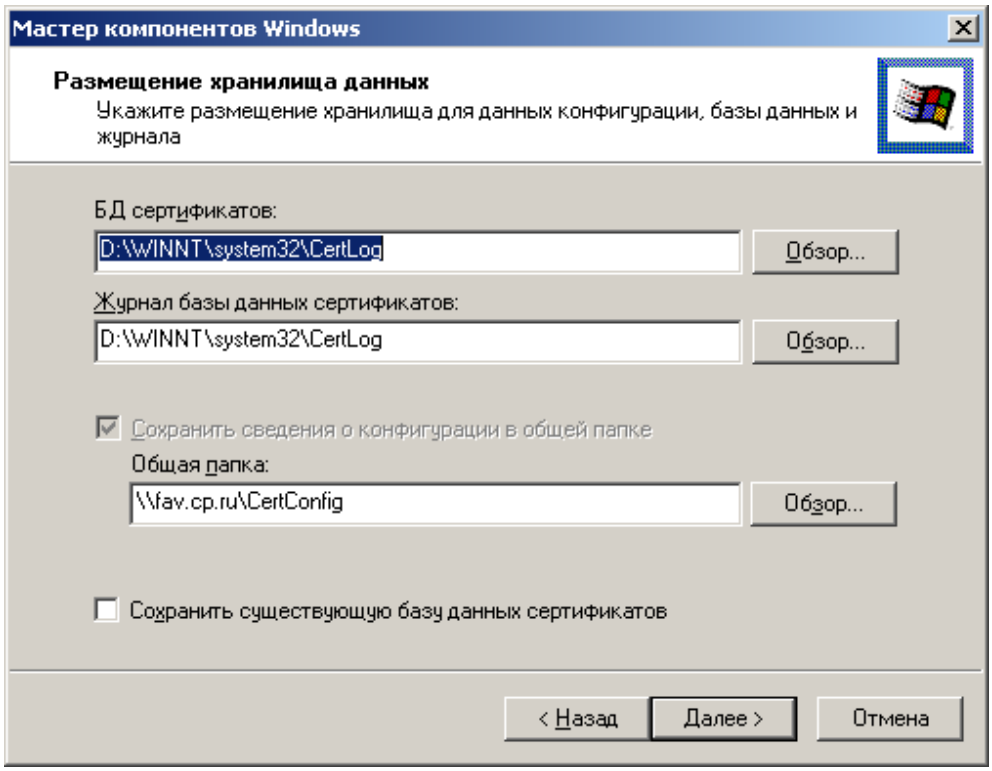
Центра сертификации. Установите флаг **Использовать связанный сертификат** и нажмите кнопку **Далее**.



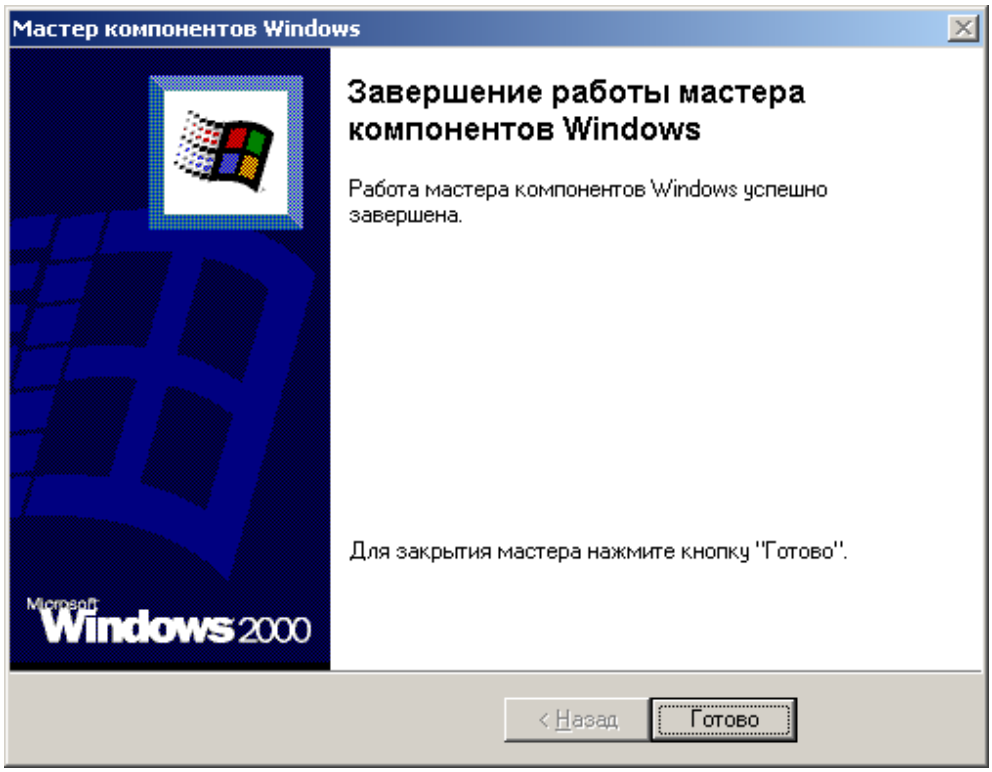
7. В окне сведения о Центре сертификации заполните по необходимости поле **Описание ЦС.** Нажмите кнопку **Далее**.



8. В окне **Размещение хранилища данных** укажите места размещения хранилищ для данных конфигурации, базы данных и журнала. Нажмите кнопку **Далее**.



9. Появится сообщение об останове службы MS IIS и начнется установка службы сертификации на компьютер. После успешной установки службы сертификации появится окно **Завершение работы мастера компонентов Windows.**



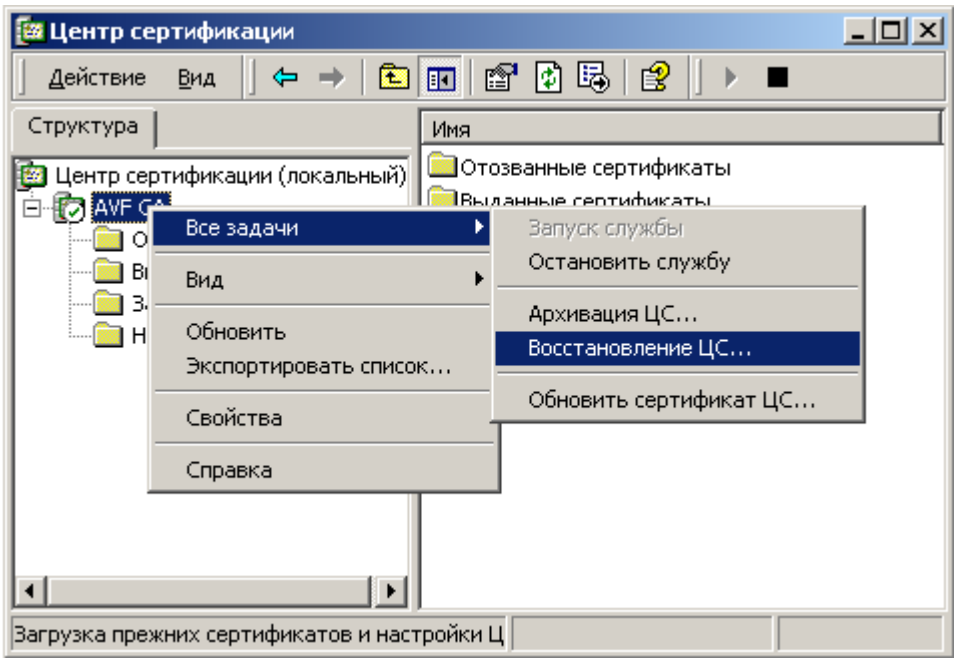
10. Нажмите кнопку **Готово** - служба сертификации успешно установлена.

2.6. Восстановление из архива базы данных Центра Сертификации

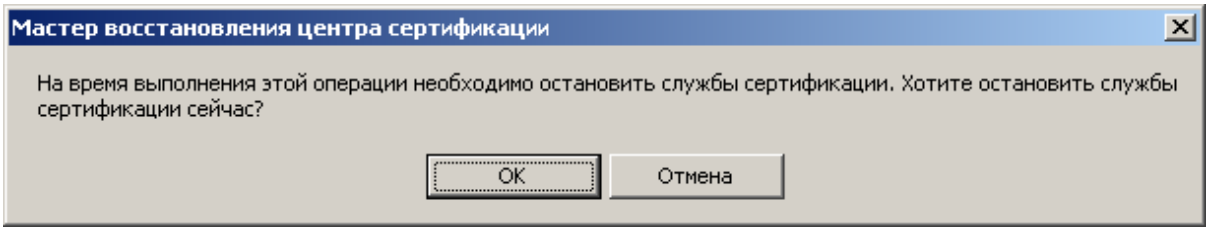
После установки службы сертификации Microsoft Certificate Authority необходимо восстановить данные из архива базы данных Центра Сертификации.

Последовательность действий при восстановлении из архива базы данных Центра Сертификации:

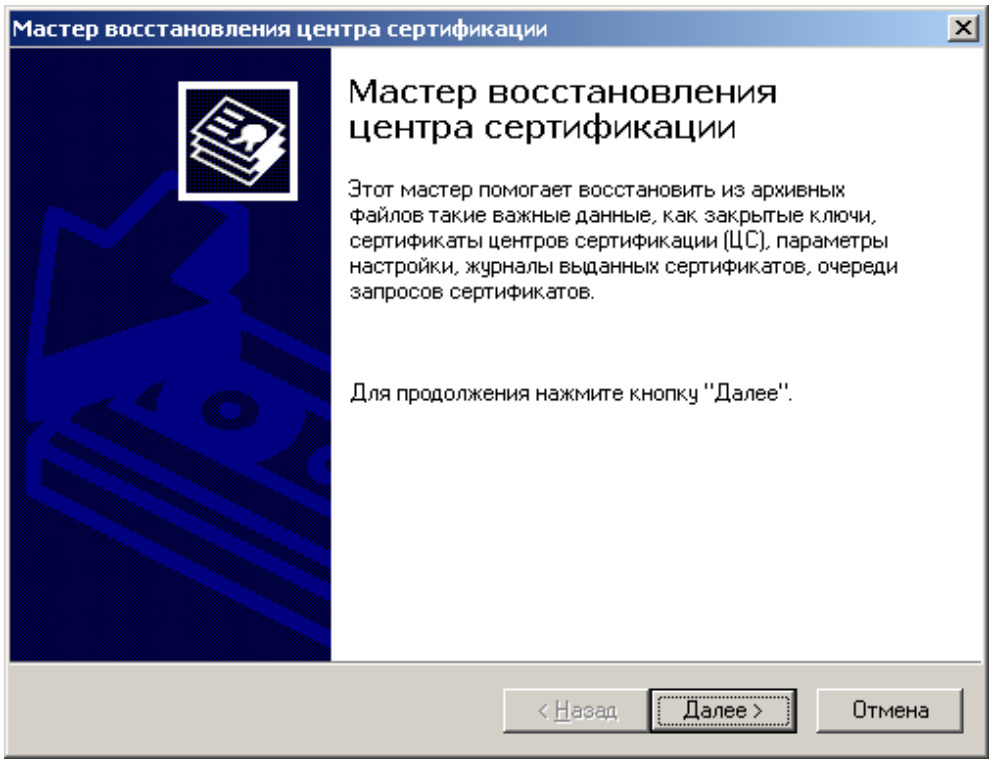
1. Откройте окно **Центра сертификации**, выполнив команды: **Пуск**, **Программы**, **Администрирование**, **Центр сертификации**.
2. Выберите Центр сертификации, нажмите правую кнопку мыши и запустите задачу **Восстановление ЦС.**



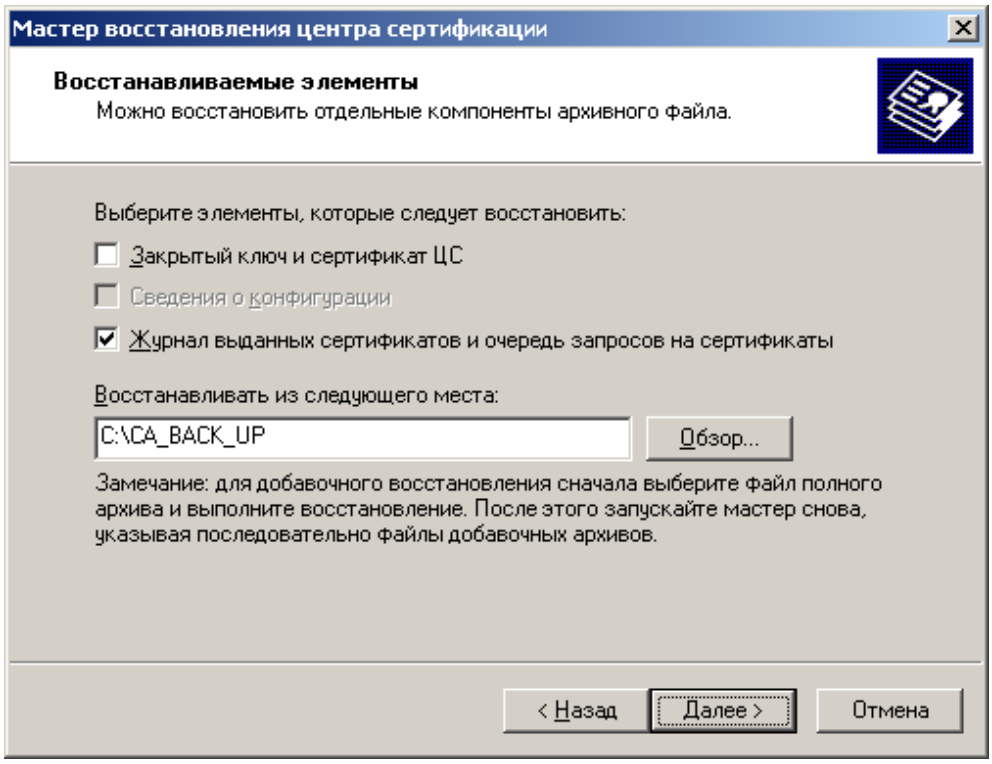
3. Откроется окно, информирующее о необходимости остановки службы сертификации. Нажмите кнопку **OK**.



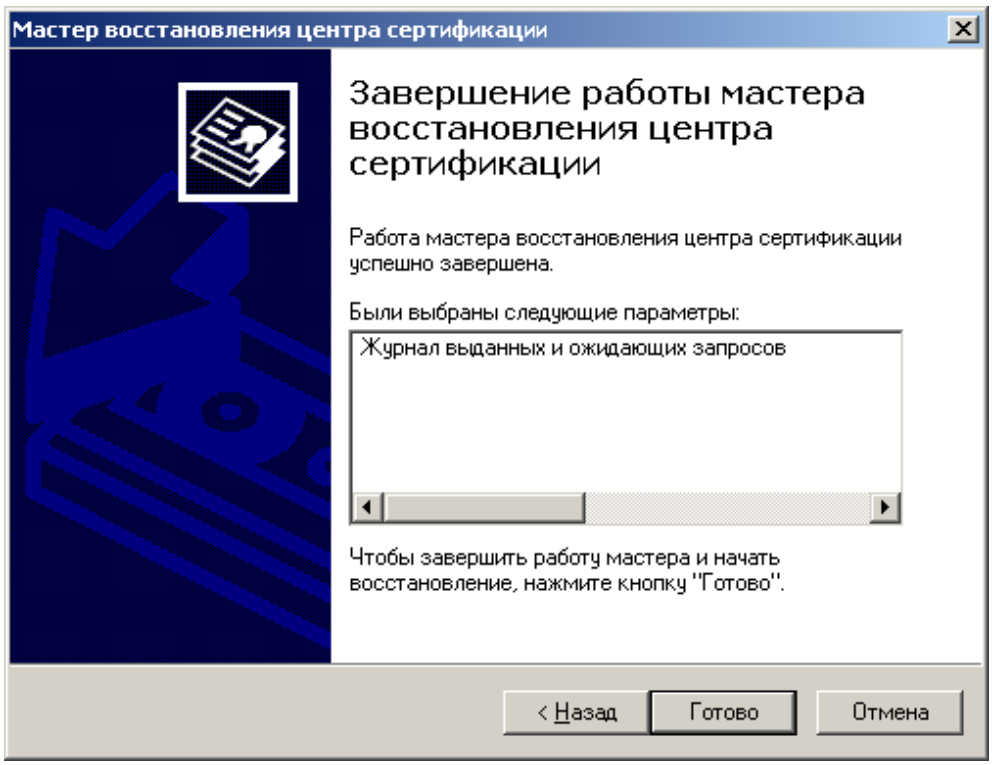
4. Откроется окно **Мастера восстановления центра сертификации**. Нажмите кнопку **Далее**.



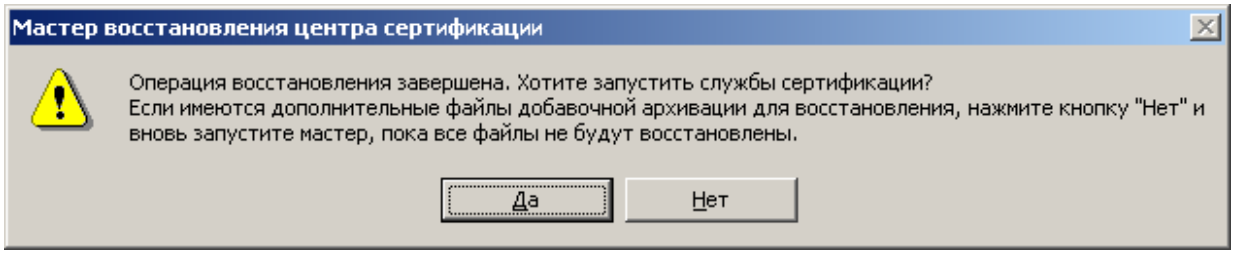
5. В окне **Восстанавливаемые элементы** установите флаг **Журнал выданных сертификатов и очередь запросов на сертификат** и с помощью кнопки **Обзор** укажите место, из которого требуется восстанавливать данные (в случае использования добавочных архивов выполните последовательность действий, описанных в замечании данного окна).



6. Откроется окно **Завершение работы мастера восстановления центра сертификации**. Нажмите кнопку **Готово**.



7. Мастер восстановления центра сертификации произведет выполнение необходимых действий. По окончании работы мастера появится сообщение, информирующее об успешном восстановлении центра сертификации, и предложение запустить службу сертификации (в случае наличия файлов добавочной архивации осуществите действия, описанные в этом окне). Нажмите кнопку **Да**.



8. Запустится служба сертификации – восстановление из архива базы данных Центра Сертификации успешно завершено.

2.7. Установка утилит Центра сертификации

Установка утилит Центра сертификации осуществляется в соответствии с пунктом 3.6 «Установка приложений «Утилиты Центра сертификации»» документа ЖТЯИ.00035-01 90 02. «КриптоПро УЦ. Руководство по установке».

2.8. Установка сертификата WEB-сервера Центра Сертификации

Процедура установки сертификата WEB-сервера Центра сертификации является опциональным шагом и выполняется в случае наличия в исходных данных следующей информации:

- Закрытый ключ WEB-сервера Центра сертификации, находящийся в контейнере закрытого ключа на внешнем носителе;
- Сертификат WEB-сервера Центра сертификации в виде файла на внешнем носителе;

Установка сертификата WEB-сервера Центра сертификации должна быть осуществлена в хранилище сертификатов **Локальный компьютер/Личные** и осуществляется аналогично установке сертификата Центра сертификации в соответствии с п. 2.4.2 данного Руководства.

После успешной установки сертификата WEB-сервера Центра сертификации в хранилище сертификатов необходимо осуществить его инсталляцию на WEB-сервер MS IIS с помощью Мастера сертификатов веб-сервера. Данная операция выполняется в соответствии с пунктом 3.7. «Выпуск и инсталляция сертификата серверной аутентификации Web-сервера ЦС» документа ЖТЯИ.00035-01 90 02. «КриптоПро УЦ. Руководство по установке».

2.9. Установка программного обеспечения Центра сертификации ПК «КриптоПро УЦ»

Установка программного обеспечения Центра сертификации ПК «КриптоПро УЦ» осуществляется в соответствии с пунктом 3.8 «Установка программного обеспечения ЦС» документа ЖТЯИ.00035-01 90 02. «КриптоПро УЦ. Руководство по установке».

2.10. Настройка программного обеспечения Центра сертификации ПК «КриптоПро УЦ»

Настройка программного обеспечения Центра сертификации ПК «КриптоПро УЦ» осуществляется на основании нормативных документов Удостоверяющего центра и в соответствии с документом ЖТЯИ.00035-01 90 04. «КриптоПро УЦ. Центр сертификации. Руководство по эксплуатации на платформе MS Windows 2000 Server» или ЖТЯИ.00035-01 90 03. «КриптоПро УЦ. Центр сертификации. Руководство по эксплуатации на платформе MS Windows 2003 Server»

Примечание: После настройки программного обеспечения Центра сертификации ПК «КриптоПро УЦ» необходимо осуществить выпуск актуального списка отозванных сертификатов (в окне свойств **Модуля выхода КриптоПро** нажать кнопку **Выпустить новый CRL** – пункт 1 «Настройка модуля выхода Крипто-Про УЦ службы сертификации ЦС» документа ЖТЯИ.00035-01 90 04. «КриптоПро УЦ. Центр сертификации. Руководство по эксплуатации на платформе MS Windows 2000 Server» или ЖТЯИ.00035-01 90 03. «КриптоПро УЦ. Центр сертификации. Руководство по эксплуатации на платформе MS Windows 2003 Server»).

3. Восстановление Центра Регистрации ПК «КриптоПро УЦ»

3.1. Исходные данные

Для восстановления Центра Регистрации ПК «КриптоПро УЦ» необходимо иметь, как минимум, файл/файлы архивной копии базы данных Центра регистрации на внешнем носителе.

Также с Центра Сертификации ПК «КриптоПро УЦ» необходимо получить следующие данные:

- Сертификат уполномоченного лица восстанавливаемого Удостоверяющего центра (сертификат Центра сертификации);
- Сертификаты уполномоченных лиц Удостоверяющих центров (сертификаты Центров сертификации) вышестоящих по иерархии Удостоверяющих центров, включая сертификат уполномоченного лица корневого Удостоверяющего центра в виде файла (файлов) на внешнем носителе (если восстанавливаемый Удостоверяющий центр является подчиненным)

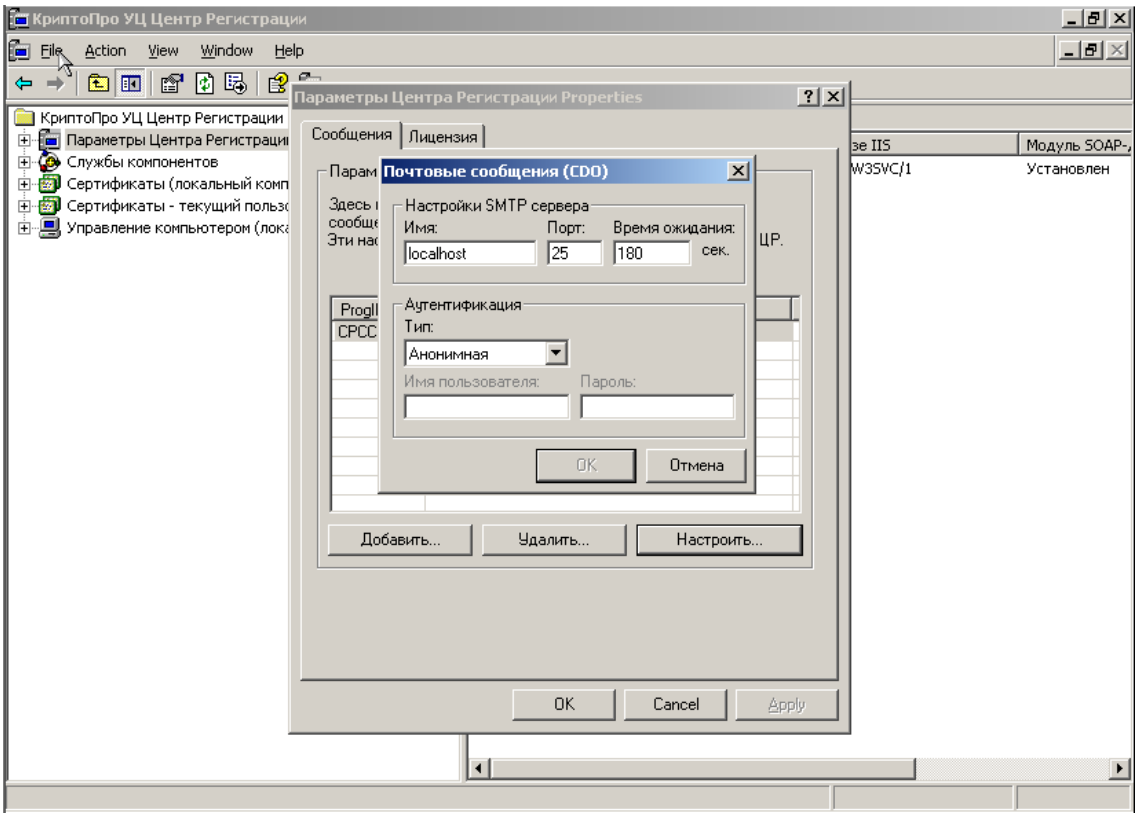
Рекомендуется кроме этого иметь следующие данные:

- Закрытый ключ Центра Регистрации, находящийся в контейнере закрытого ключа на внешнем носителе;
- Сертификат Центра Регистрации в виде файла на внешнем носителе;
- Закрытый ключ WEB-сервера Центра Регистрации, находящийся в контейнере закрытого ключа на внешнем носителе;
- Сертификат WEB-сервера Центра Регистрации в виде файла на внешнем носителе;
- Нормативные документы Удостоверяющего центра (Регламент Удостоверяющего центра, Положение об Удостоверяющем центре), определяющие настройки Центра регистрации.

Для сохранения существовавших настроек, помимо всего перечисленного, необходимо следующее:

- Записать настройки почты старой версии Центра Регистрации.

  Для этого в окне **КриптоПро УЦ Центр Регистрации** в контекстном меню пункта **Параметры Центра Регистрации** выбрать **Свойства**, в появившемся окне параметров отправления почтовых сообщений нажать **«Настроить»** и переписать настройки.



- Для каждого модуля доступа записать настройки подключений к Центру Регистрации и Центру Сертификации.

  (эти настройки можно посмотреть на вкладке «Общие» свойств каждого из модулей доступа)
- Для каждого модуля доступа сохранить следующие файлы:

(Например, если модуль доступа один):

%ALLUSERSPROFILE%\Application Data\CryptoPro\RA\Inetpub\1\RA\web.configuration

%ALLUSERSPROFILE%\Application Data\CryptoPro\RA\Inetpub\1\RA*.job

%ALLUSERSPROFILE%\Application Data\CryptoPro\RA\Inetpub\1\UI\ConstDef.asp

%ALLUSERSPROFILE%\Application Data\CryptoPro\RA\Inetpub\1\UI\Cert.xsl

%ALLUSERSPROFILE%\Application Data\CryptoPro\RA\Inetpub\1\UI\Request.xsl

%windir%\Tasks\RATASK_*.job

3.2. Установка общесистемного программного обеспечения

Установка общесистемного программного обеспечения осуществляется в соответствии с требованиями документа ЖТЯИ.00035-01 90 02. «КриптоПро УЦ Руководство по установке».

3.3. Установка СКЗИ «КриптоПро CSP»

Установка и настройка СКЗИ «КриптоПро CSP» осуществляется в соответствии с пунктом 4.2 «Установка СКЗИ КриптоПро CSP и КриптоПро TLS» документа ЖТЯИ.00035-01 90 02. «КриптоПро УЦ Руководство по установке».

3.4. Установка утилит Центра Регистрации

Установка утилит Центра Регистрации осуществляется в соответствии с пунктом 4.4 «Установка приложений «Утилиты Центра Регистрации»» документа ЖТЯИ.00035-01 90 02. «КриптоПро УЦ Руководство по установке».

3.5. Установка сертификата Центра Сертификации.

Установка сертификата Центра Сертификации (и сертификатов вышестоящих Центров Сертификации, если восстанавливаемый Центр сертификации является подчиненным) Удостоверяющего центра осуществляется аналогично установке, приведенной в пункте 2.4.1 настоящего Руководства.

3.6. Установка сертификата WEB-сервера Центра Регистрации

Процедура установки сертификата WEB-сервера Центра Регистрации является опциональным шагом и выполняется в случае наличия в исходных данных следующей информации:

- Закрытый ключ WEB-сервера Центра Регистрации, находящийся в контейнере закрытого ключа на внешнем носителе;
- Сертификат WEB-сервера Центра Регистрации в виде файла на внешнем носителе;

Установка сертификата WEB-сервера Центра Регистрации должна быть осуществлена в хранилище сертификатов **Локальный компьютер/Личные** и осуществляется аналогично установке сертификата Центра сертификации в соответствии с п. 2.4.2 данного Руководства.

После успешной установки сертификата WEB-сервера Центра регистрации в хранилище сертификатов необходимо осуществить его инсталляцию на WEB-сервер MS IIS с помощью Мастера сертификатов веб-сервера. Данная операция выполняется в соответствии с пунктом 4.5.2 «Инсталляция сертификата серверной аутентификации на Web-сервере ЦР» документа ЖТЯИ.00035-01 90 02. «КриптоПро УЦ Руководство по установке».

3.7. Установка программного обеспечения Центра регистрации ПК «КриптоПро УЦ»

Установка программного обеспечения Центра регистрации ПК «КриптоПро УЦ» осуществляется в соответствии с пунктом 4.6 «Установка программного обеспечения ЦР» документа ЖТЯИ.00035-01 90 02. «КриптоПро УЦ Руководство по установке».

Примечание: Необходимо осуществить установку всех актуальных списков отозванных сертификатов (CRL), изготовленных восстанавливаемым Удостоверяющим центром и всеми вышестоящими по иерархии Удостоверяющими центрами, если восстанавливаемый Удостоверяющий центр является подчиненным. Установка списков отозванных сертификатов должна производиться в хранилище **Локальный компьютер/Промежуточные центры сертификации,** и осуществляется с помощью стандартного **Мастера импорта сертификатов** ОС Windows (см. раздел **Импорт и экспорт сертификатов** стандартного справочника ОС Windows 2000).

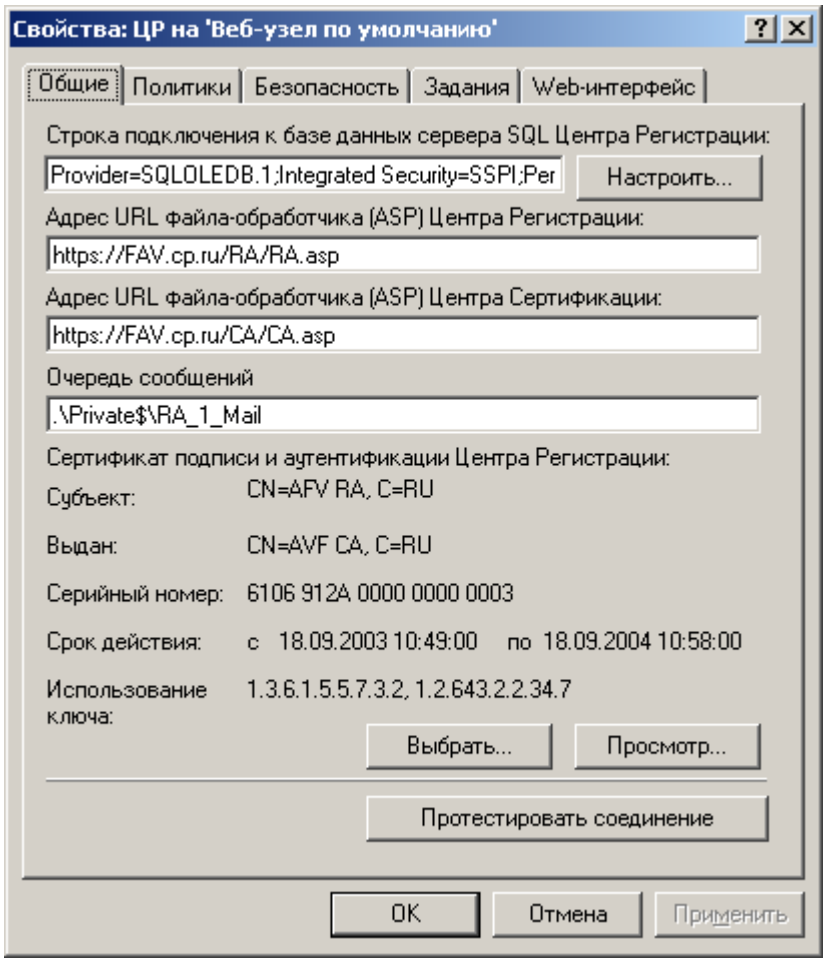
3.8. Установка сертификата Центра Регистрации

Установка сертификата Центра Регистрации должна быть осуществлена в хранилище сертификатов **Локальный компьютер/Личные** и осуществляется аналогично установке сертификата Центра сертификации в соответствии с п. 2.4.2 данного Руководства.

После успешной установки сертификата Центра Регистрации в хранилище сертификатов необходимо осуществить настройку Центра Регистрации на работу с ним.

Для этого откройте окно **Свойства: ЦР на 'Веб – узел по умолчанию'**, нажмите кнопку **Выбрать** и из раскрывшегося списка сертификатов выберите сертификат Центра регистрации.

Не забудьте добавить сертификат Центра Регистрации в список доверенных Центров Регистрации на Центре Сертификации ПК «КриптоПро УЦ» с использованием приложения **Параметры Центра Сертификации**.

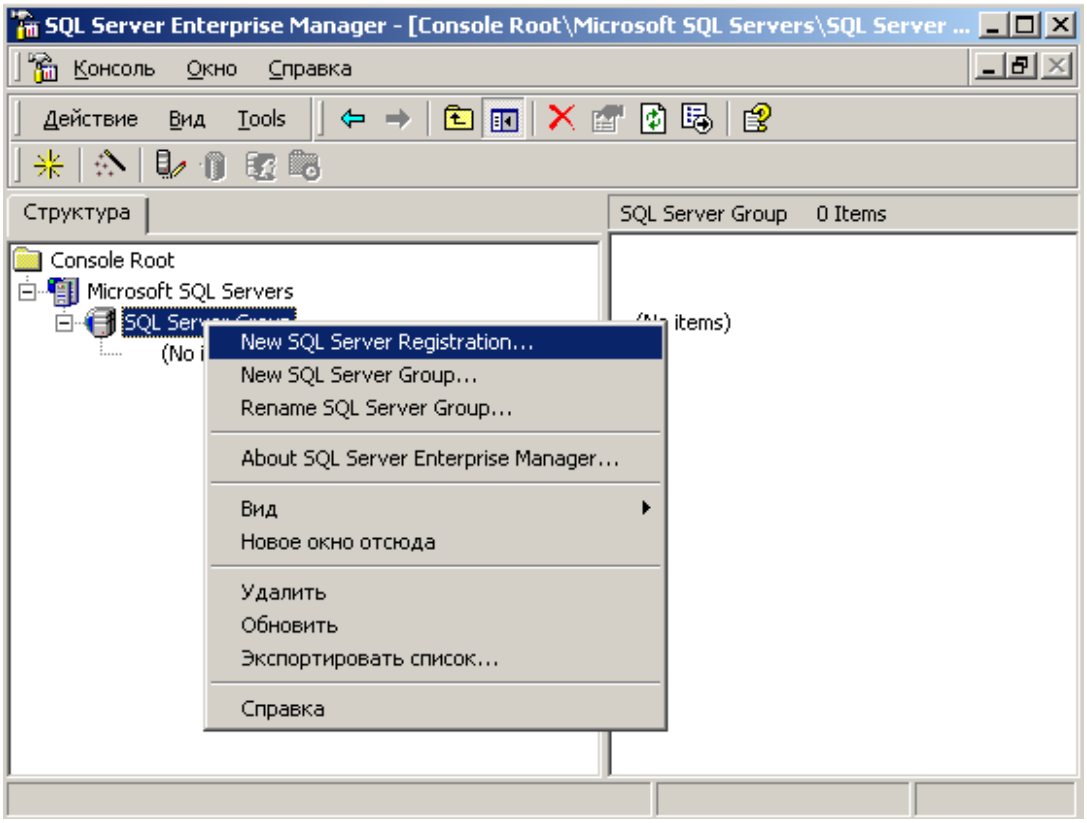


3.9. Восстановление Базы данных Центра Регистрации

Предполагается, что архивная копия Базы данных было сохранена в файл в соответствии с пунктом 3 «База данных Центра регистрации» документа ЖТЯИ.00035-01 90 11 «КриптоПро УЦ. Руководство администратора баз данных»:

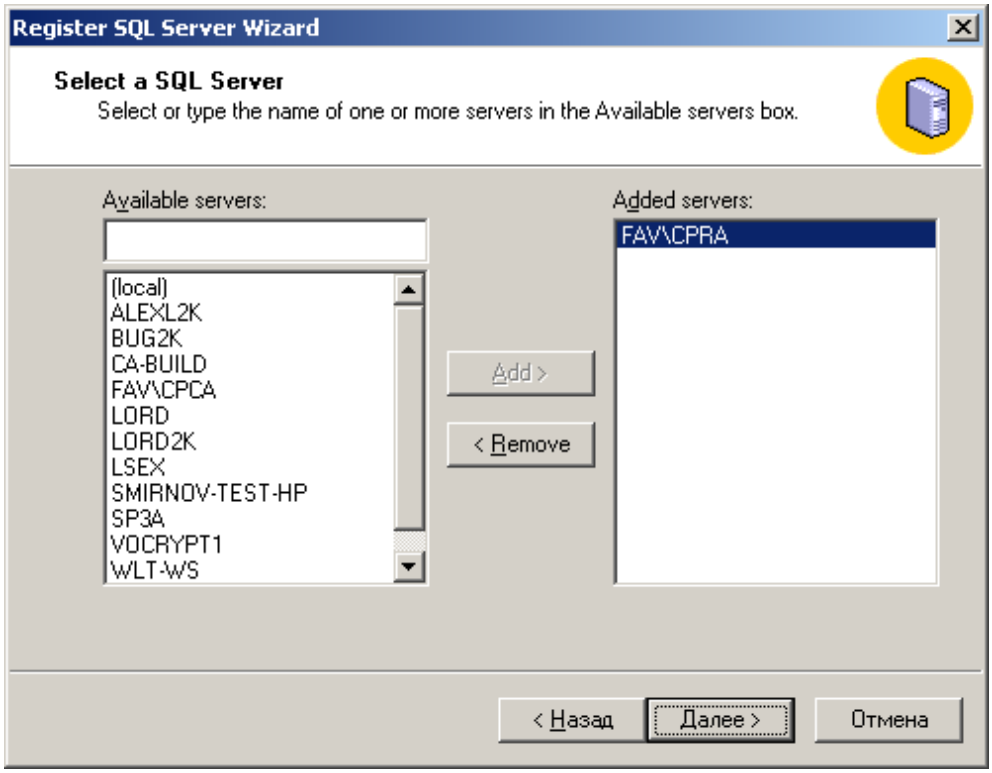
Для восстановления Базы данных Центра Регистрации необходимо на компьютер Центра Регистрации установить приложение SQL Server Enterprise Manager, входящее в состав клиентских средств Microsoft SQL Server 2000 (установка клиентских средств Microsoft SQL Server 2000 Server осуществляется в соответствии со справочной документацией MS SQL 2000 Server).

1. Запустите приложение SQL Server Enterprise Manager из пакета MS SQL Server 2000 Server, выполнив команды **Пуск**, **Программы**, **Microsoft SQL Server**, **Enterprise Manager**
2. Выберите правой кнопкой мыши раздел **SQL Server Group.** В раскрывшемся меню выберите пункт **New SQL Server Registration**



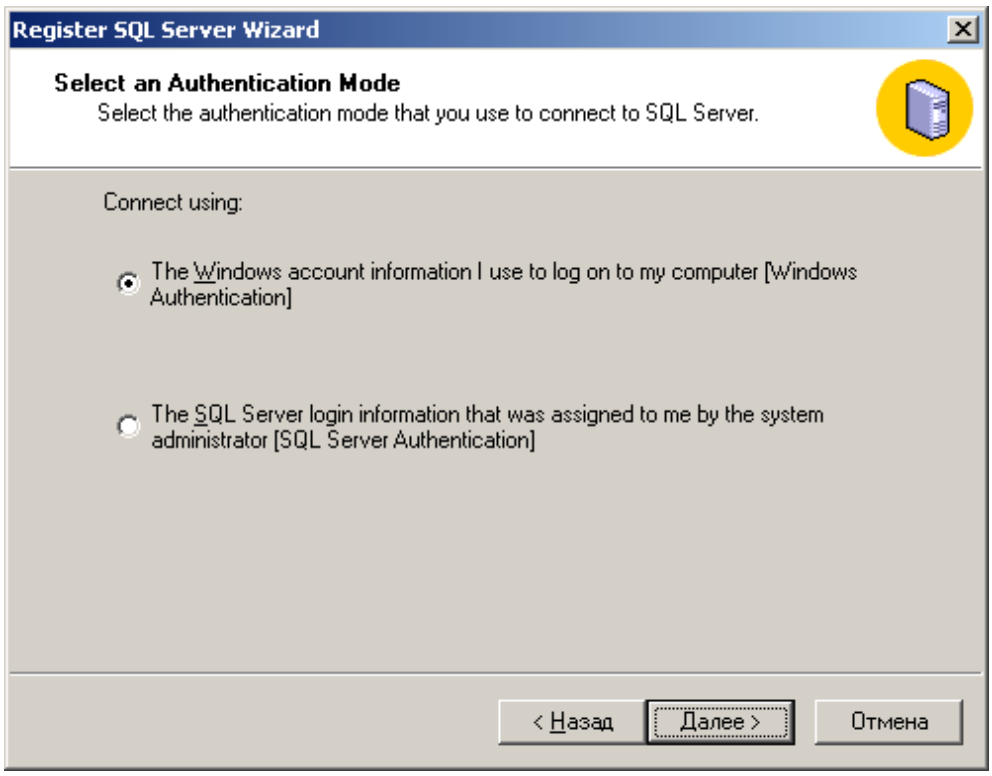
3. Запустится Мастер **Register SQL Server Wizard**, нажмите кнопку **Далее**

4. В окне **Select a SQL Server** в области **Available Servers** выберите **ИмяКомпьютераЦентраРегистрации/CPRA**, нажмите кнопку **Add**. После проделанных операций нажмите кнопку **Далее**

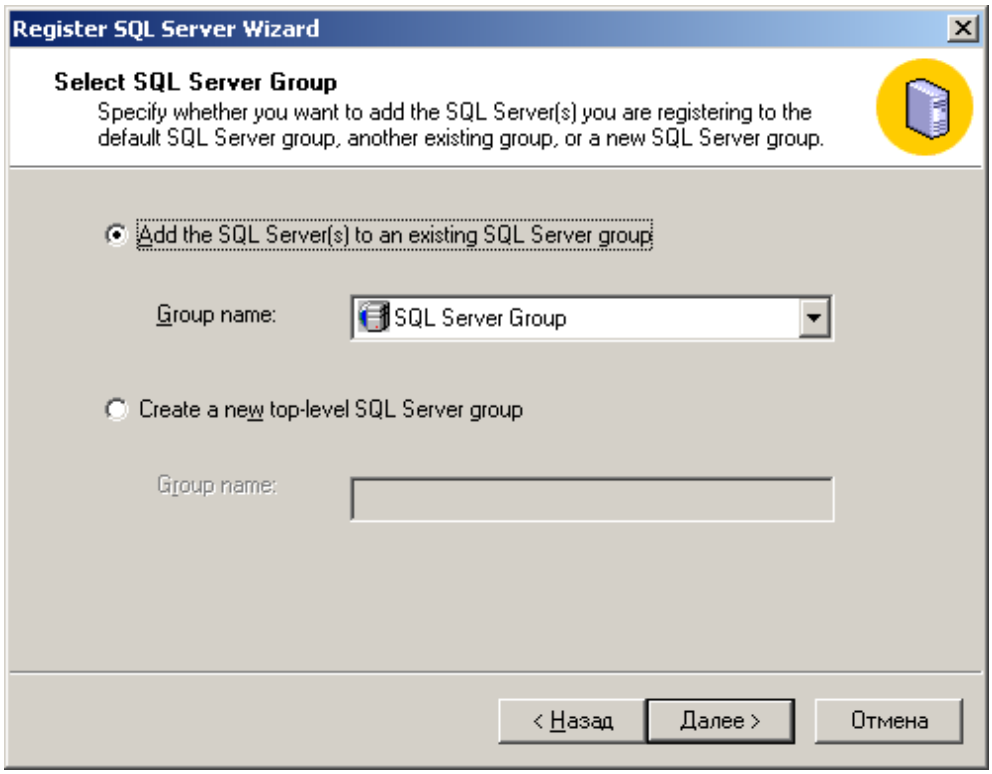


5. В окне **Select an Authentication Mode** установите переключатель **Connect User** в положение **The Windows account information I use**

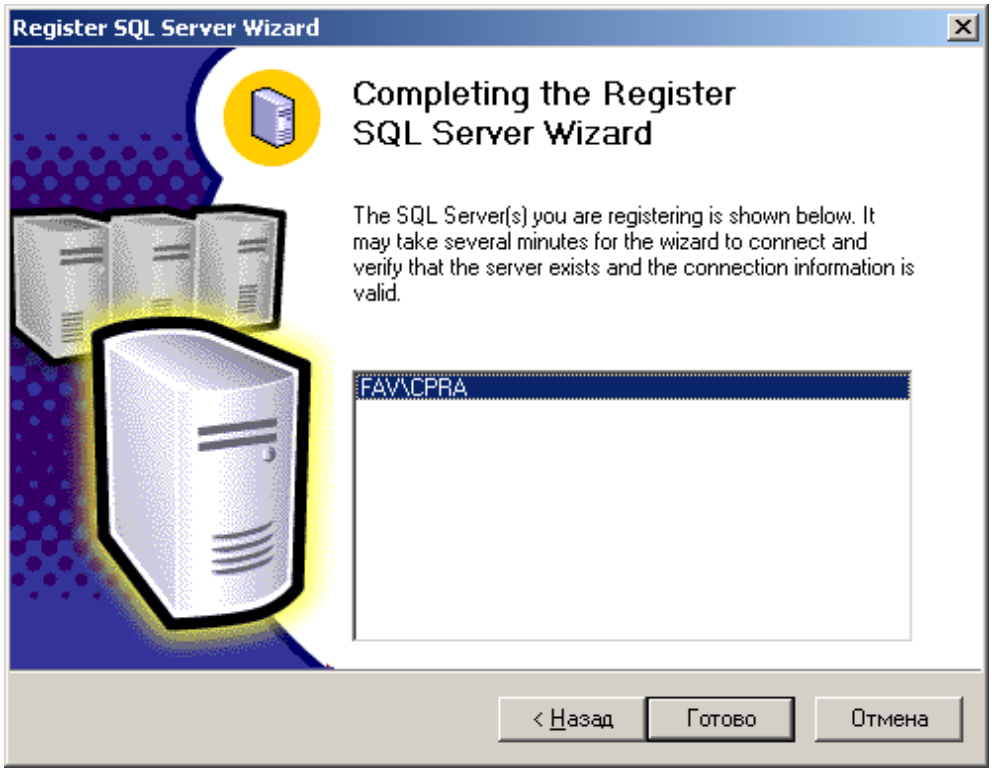
to log on to my Computer [Windows Authentication] и нажмите кнопку **Далее**



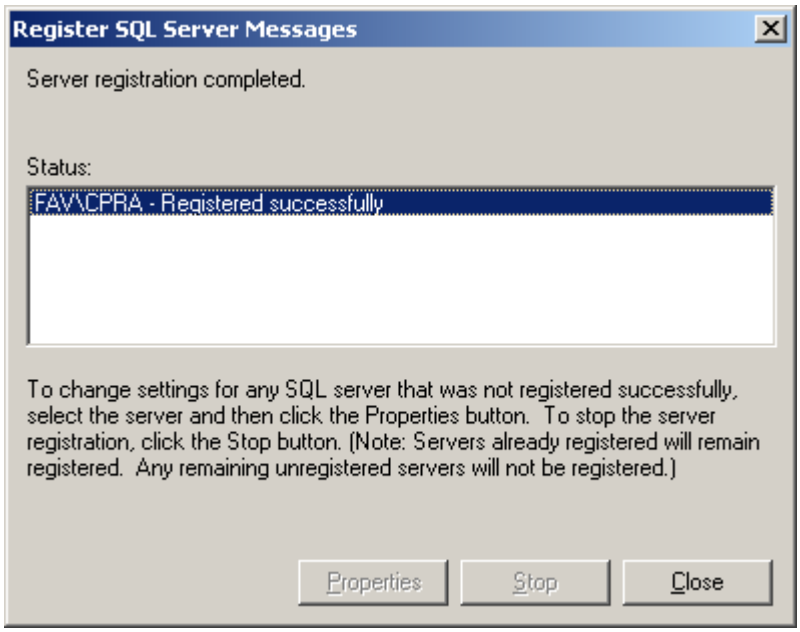
6. В окне **Select SQL Server Group** выберите переключатель **Add the SQL Server(s) to an existing SQL Server group** и в поле **Group name** установите **SQL Server Group**



7. В окне **Completing the Register SQL Server Wizard** нажмите кнопку **Готово**.

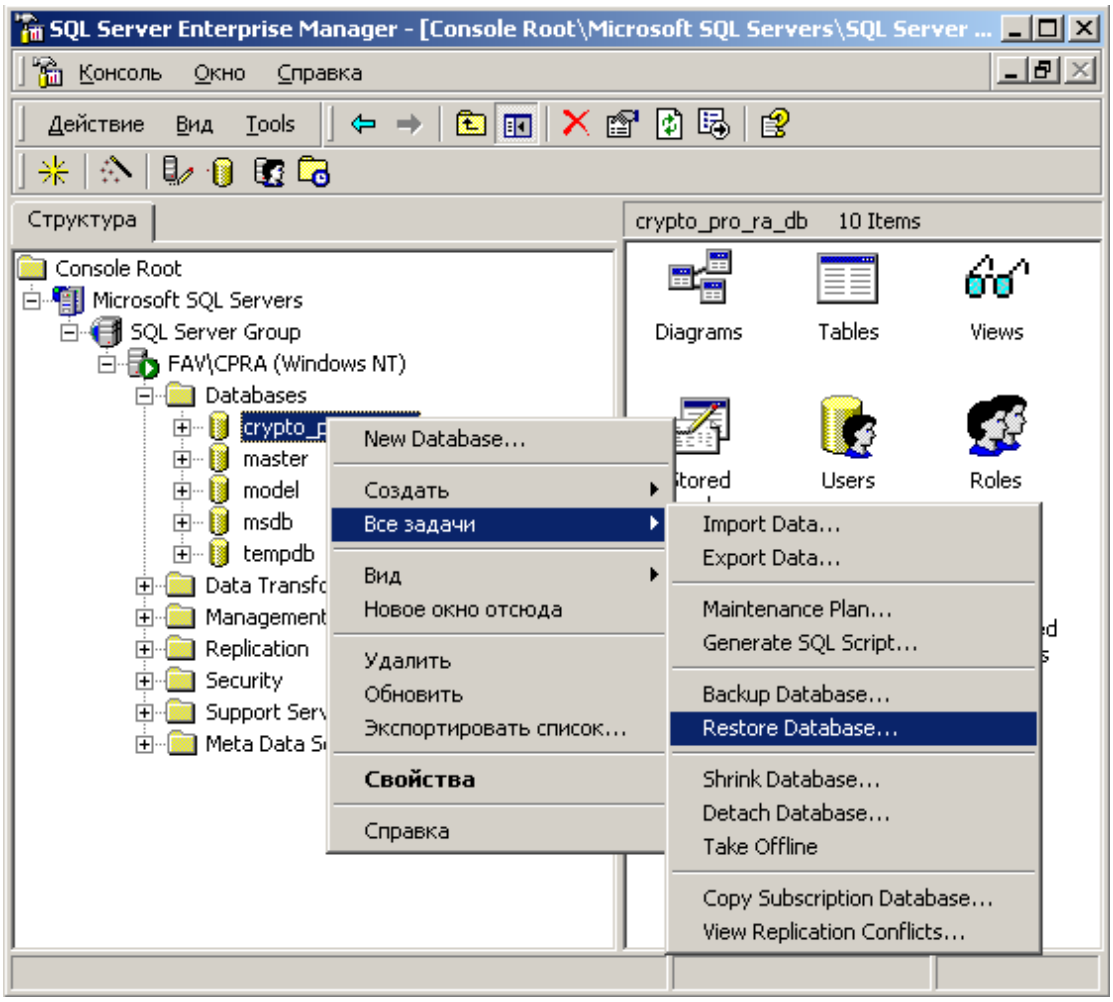


8. Мастер осуществит необходимые действия, сопровождающиеся информационными сообщениями, и выдаст сообщение об успешном окончании работы

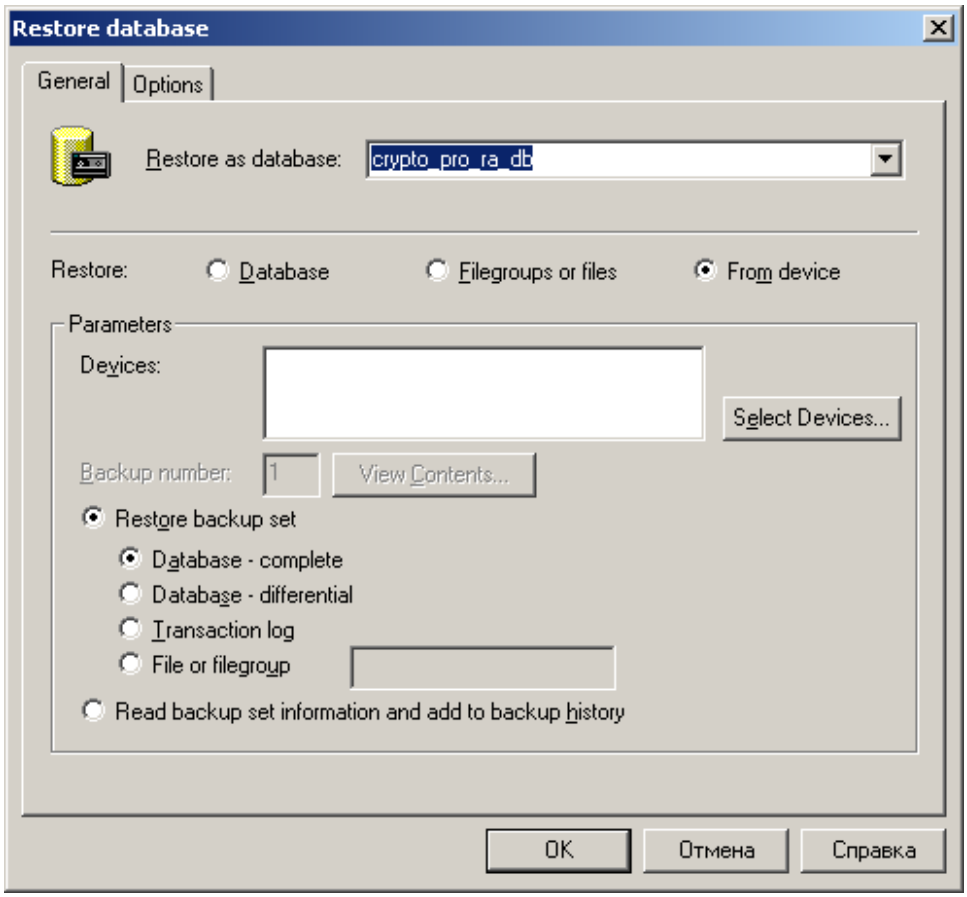


9. Нажмите кнопку **Close**. Работа мастера успешно завершена

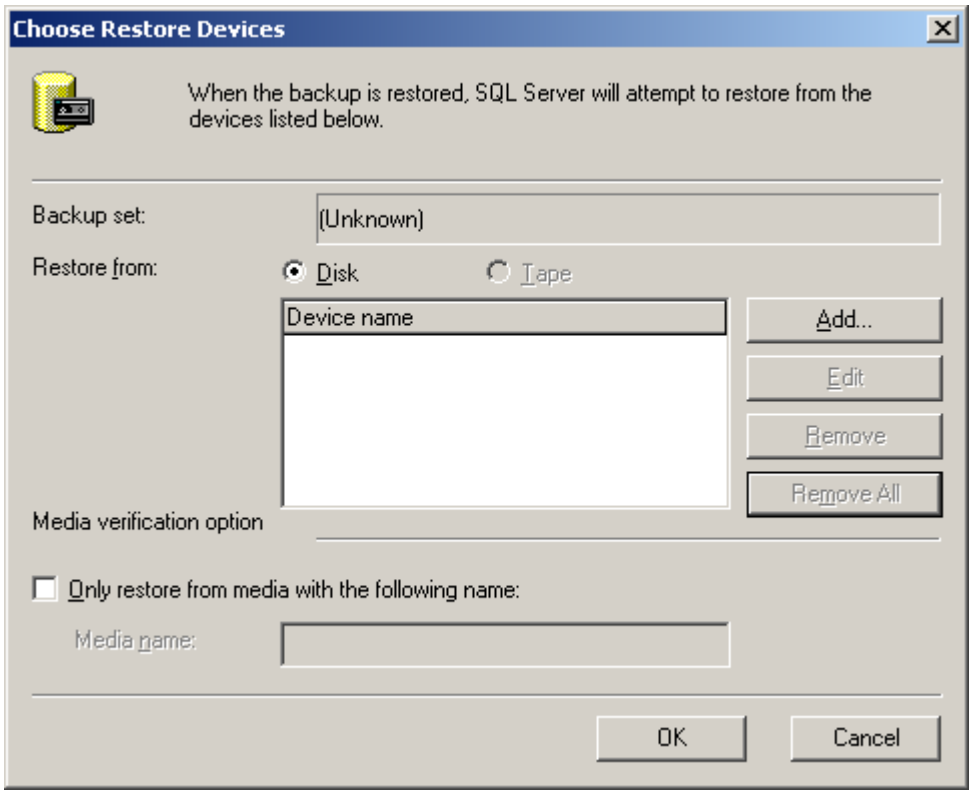
10. В окне приложения **SQL Server Enterprise Manager** выберите правой кнопкой мыши пункт **crypto_pro_ra_db** (**Databases/crypto_pro_ra_db**). В раскрывшемся меню выберите задачу **Restore Database**



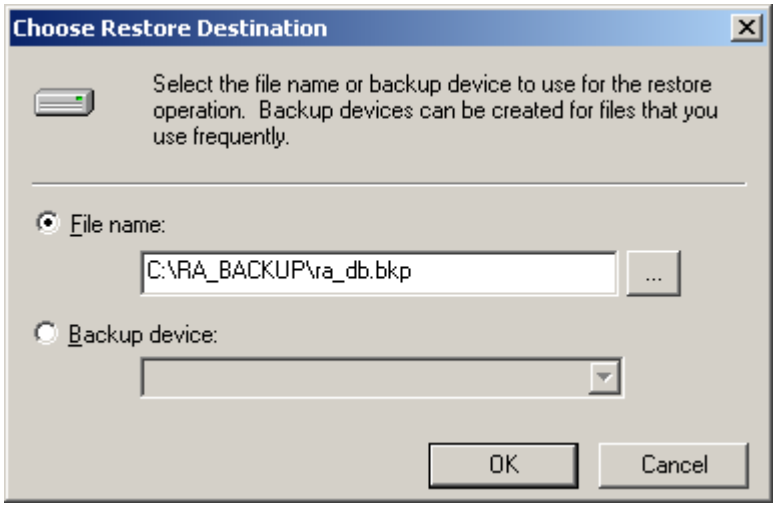
11. В открывшемся окне **Restore Database** проверьте, что поле **Restore as database** содержит **crypto_pro_ra_db**, установите переключатель **Restore** в положение **From device**, в области **Parameters** выберите переключатель **Restore backup set** и установите переключатель **Database – complete**. Для выбора хранилища архивной копии базы данных Центра регистрации нажмите кнопку **Select Devices.**



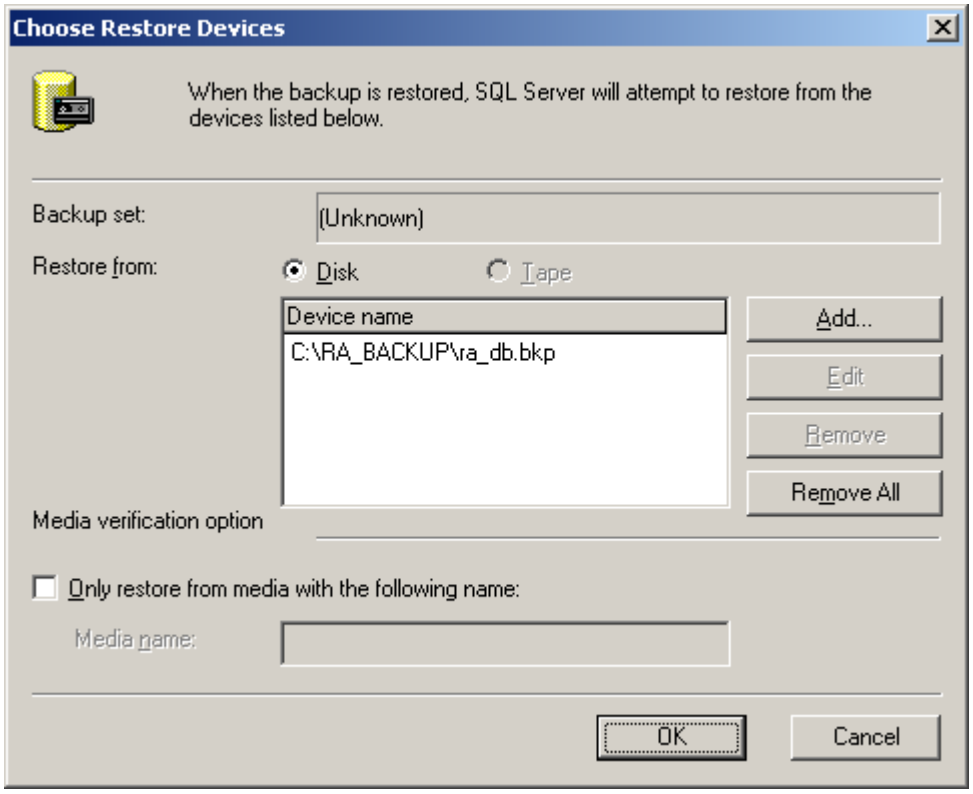
12. В окне **Choose Restore Devices** установите переключатель **Restore from** в положение **Disk** и нажмите кнопку **Add**.



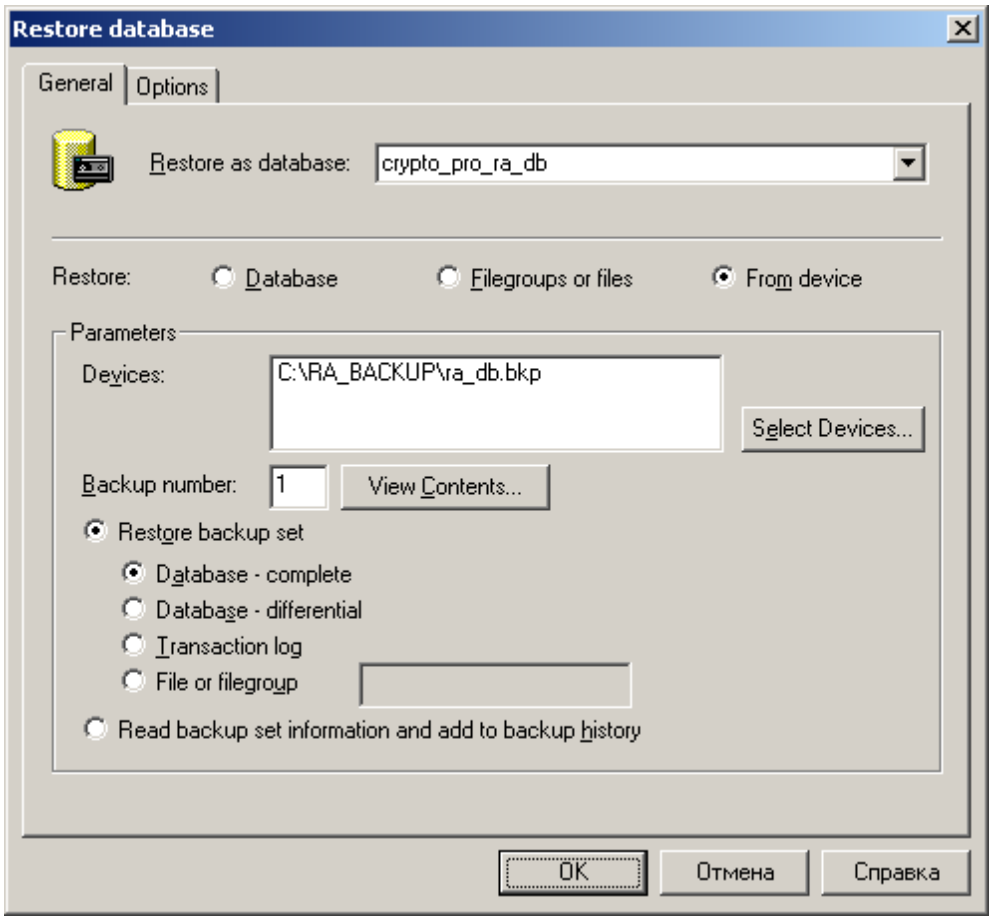
13. В окне **Choose Restore Destination** выберите переключатель **File name** и укажите файл и полный путь к нему, содержащий архивную копию базы данных Центра регистрации. Нажмите кнопку **OK**



14. В окне **Choose Restore Devices** проверьте правильность выбора файла, содержащего архивную копию базы данных Центра регистрации, и нажмите кнопку **OK**



15. В окне **Restore Database** проверьте правильность установленных параметров и нажмите кнопку **OK**



16. Программа осуществит необходимые действия по восстановлению выбранной базы данных, сопровождающиеся информационными сообщениями, и выдаст сообщение об успешном окончании работы

17. Нажмите кнопку **OK** – база данных Центра регистрации успешно восстановлена

3.10. Настройка программного обеспечения Центра Регистрации ПК «КриптоПро УЦ»

Осуществите настройку параметров Центра регистрации, которые не содержались в базе данных Центра регистрации (например, настройку заданий Центра регистрации), на основании нормативных документов Удостоверяющего центра и в соответствии с документом ЖТЯИ.00035-01 90 05. «КриптоПро УЦ Центр регистрации Руководство по эксплуатации».

Восстановите прежние настройки:

- Восстановите настройки почты.

- Для каждого модуля доступа восстановите настройки подключений к Центру Регистрации и Центру Сертификации.
- Для каждого модуля доступа перезапишите сохраненные файлы:

  %ALLUSERSPROFILE%\Application Data\Crypto Pro\RA\Inetpub\<номер модуля>\RA\web.configuration

  %ALLUSERSPROFILE%\Application Data\Crypto Pro\RA\Inetpub\<номер модуля>\RA*.job

  %ALLUSERSPROFILE%\Application Data\Crypto Pro\RA\Inetpub\<номер модуля>\UI\ConstDef.asp

  %ALLUSERSPROFILE%\Application Data\Crypto Pro\RA\Inetpub\<номер модуля>\UI\Cert.xsl

  %ALLUSERSPROFILE%\Application Data\Crypto Pro\RA\Inetpub\<номер модуля>\UI\Request.xsl

  %windir%\Tasks\RATASK_*.job

4. Восстановление АРМ администратора Центра Регистрации ПК «КриптоПро УЦ»

4.1. Исходные данные

Для восстановления АРМ администратора Центра Регистрации ПК «КриптоПро УЦ» должны быть предоставлены следующие данные:

- Закрытый ключ привилегированного пользователя Центра регистрации, находящийся в контейнере закрытого ключа на внешнем носителе;
- Сертификат привилегированного пользователя Центра регистрации в виде файла на внешнем носителе;
- Сертификат уполномоченного лица восстанавливаемого Удостоверяющего центра (сертификат Центра сертификации);
- Сертификаты уполномоченных лиц Удостоверяющих центров (сертификаты Центров сертификации) вышестоящих по иерархии Удостоверяющих центров, включая сертификат уполномоченного лица корневого Удостоверяющего центра в виде файла (файлов) на внешнем носителе (если восстанавливаемый Удостоверяющий центр является подчиненным)

4.2. Установка общесистемного программного обеспечения и СКЗИ «КриптоПро CSP»

Установка общесистемного программного обеспечения и СКЗИ «КриптоПро CSP» осуществляется в соответствии с требованиями документа ЖТЯИ.00035-01 90 02. «КриптоПро УЦ. Руководство по установке».

4.3. Установка программного обеспечения АРМ администратора Центра регистрации ПК «КриптоПро УЦ»

Установка программного обеспечения АРМ администратора центра регистрации ПК «КриптоПро УЦ» осуществляется в соответствии с пунктом 5 «Установка АРМ администратора ЦР» документа ЖТЯИ.00035-01 90 02. «КриптоПро УЦ. Руководство по установке».

4.4. Установка сертификата Центра сертификации.

Установка сертификата Центра сертификации (и сертификатов вышестоящих Центров сертификации, если восстанавливаемый Центр сертификации является подчиненным) Удостоверяющего центра осуществляется аналогично установке, приведенной в пункте 2.4.1 настоящего Руководства.

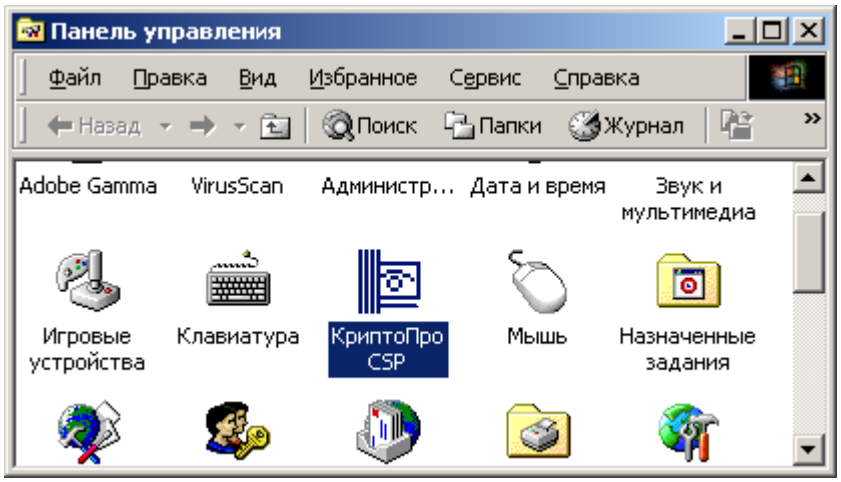
Примечание: Необходимо осуществить установку всех актуальных списков отозванных сертификатов (CRL), изготовленных восстанавливаемым Удостоверяющим центром и всеми вышестоящими по иерархии Удостоверяющими центрами, если восстанавливаемый Удостоверяющий центр является подчиненным. Установка списков отозванных сертификатов должна производиться в хранилище **Локальный компьютер/Промежуточные центры сертификации** и осуществляется с помощью стандартного **Мастера импорта сертификатов** ОС Windows (см. раздел **Импорт и экспорт сертификатов** стандартного справочника ОС Windows 2000).

4.5. Установка сертификата привилегированного пользователя

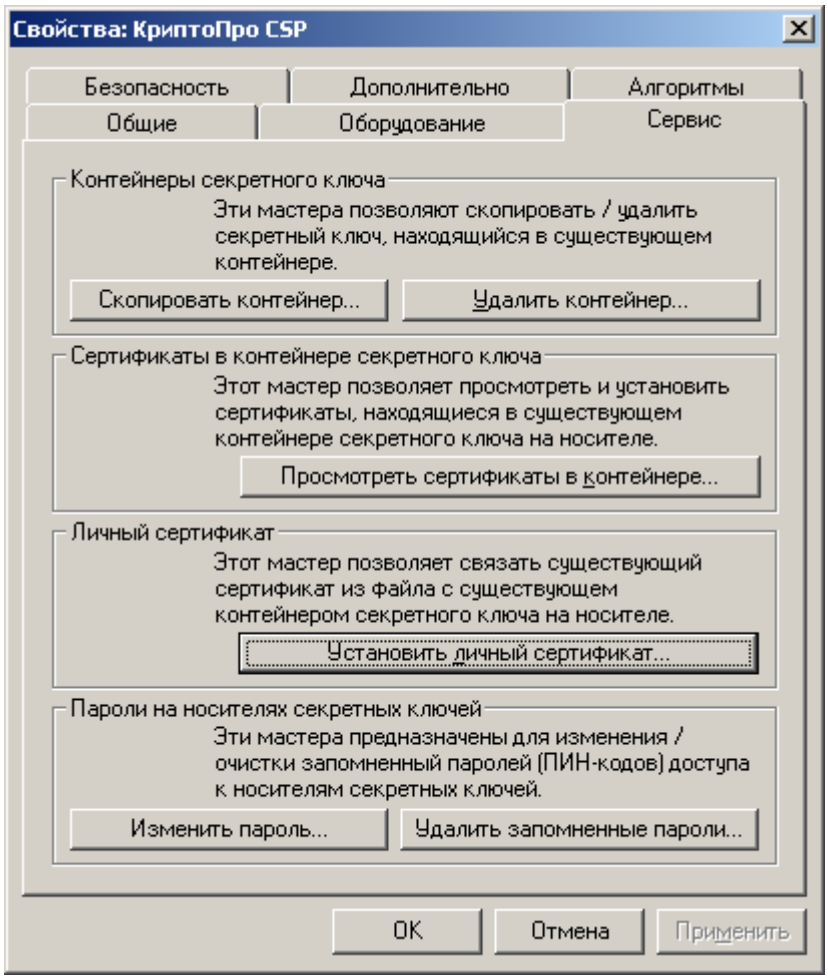
Установка сертификата привилегированного пользователя Центра регистрации должна быть осуществлена в хранилище сертификатов **Текущий пользователь /Личные**.

Последовательность действий по установке сертификата привилегированного пользователя:

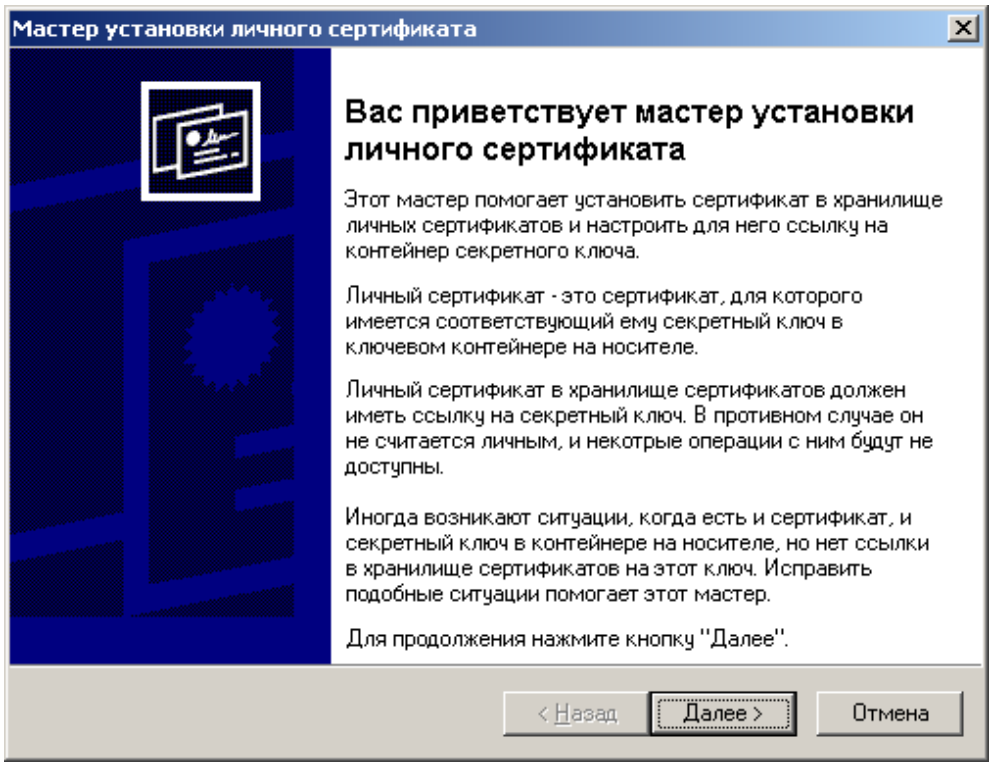
1. Откройте панель управления компьютером, используя пункты меню **Пуск, Настройка, Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**.



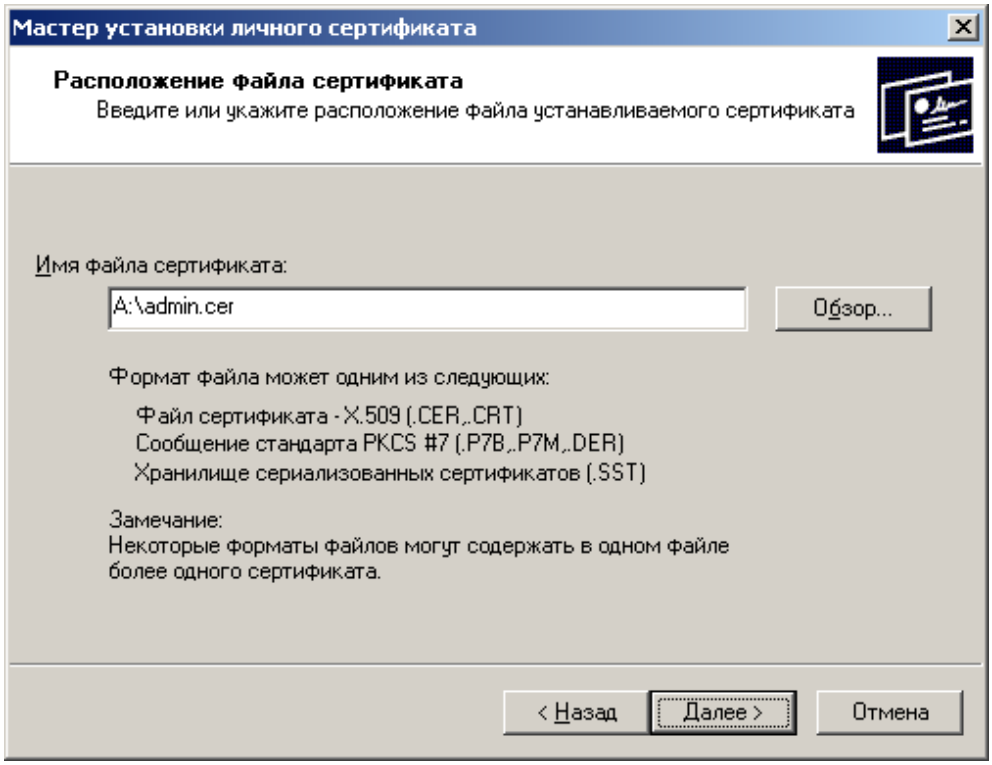
2. В отображаемом окне **Свойства: КриптоПро CSP** выберите закладку **Сервис** и нажмите кнопку **Установить личный сертификат**.



3. В появившемся окне **Мастер установки личного сертификата** ознакомьтесь с текстом и нажмите кнопку **Далее**

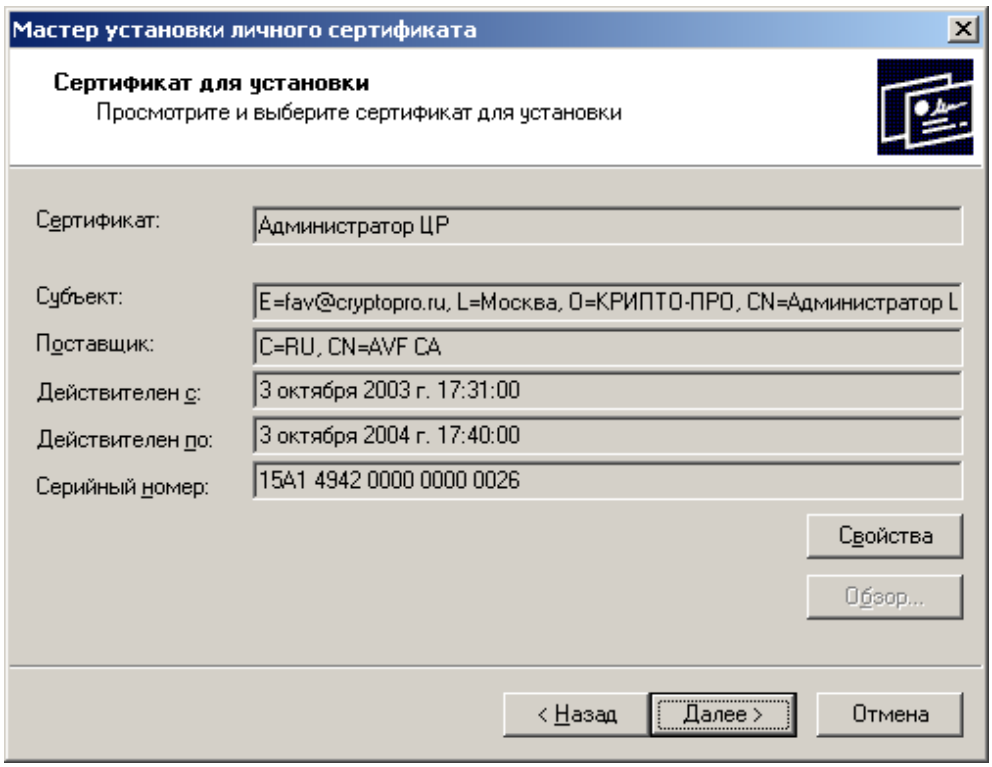


4. Откроется окно **Расположение файла сертификата.** Укажите полный путь к файлу сертификата привилегированного пользователя на внешнем носителе или выберите его с помощью кнопки **Обзор.** Нажмите кнопку **Далее**

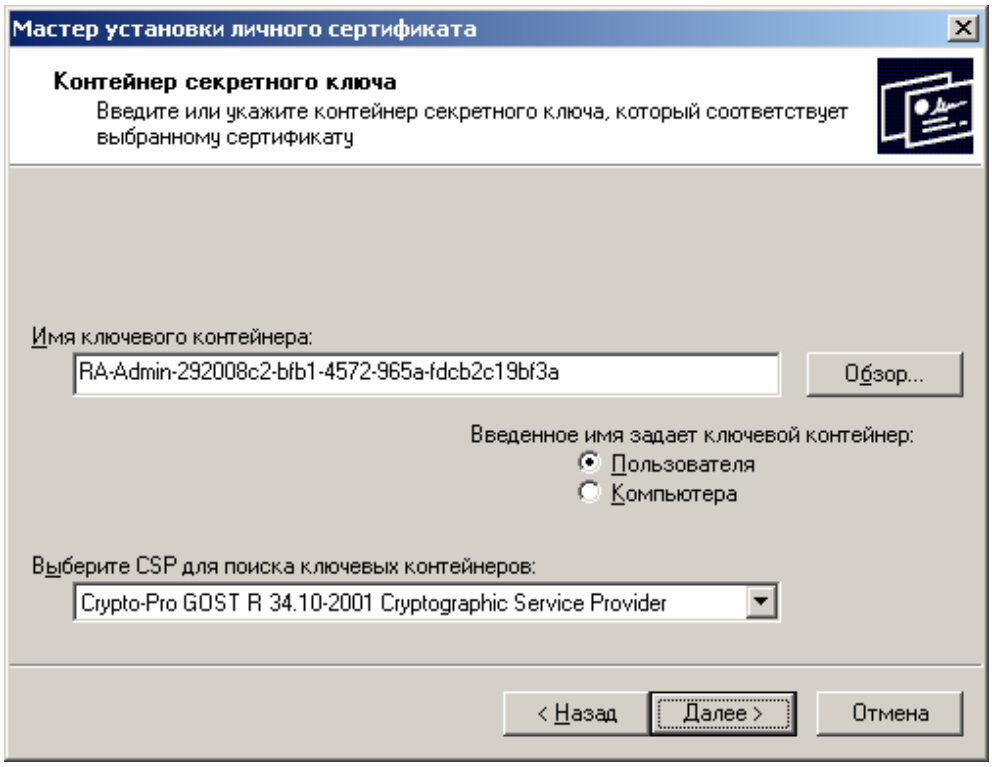


5. В окне **Сертификат для установки** выводится основная информация о сертификате. Нажав на кнопку **Свойства** можно просмотреть

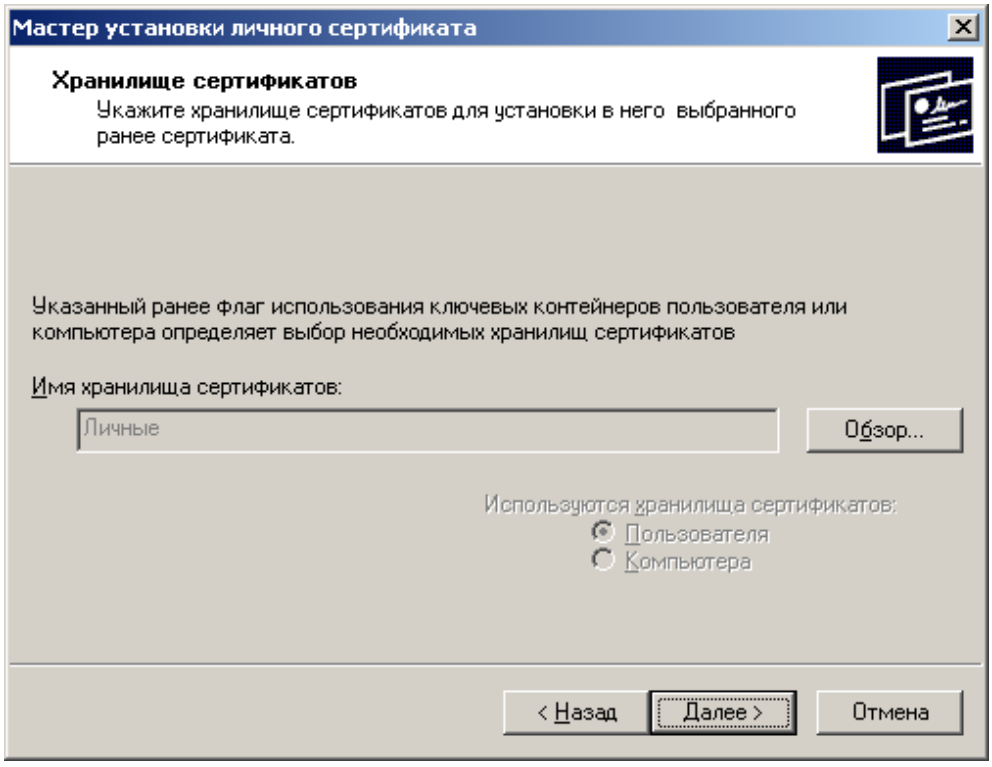
сертификат в стандартном окне просмотра сертификата. Нажмите кнопку **Далее**



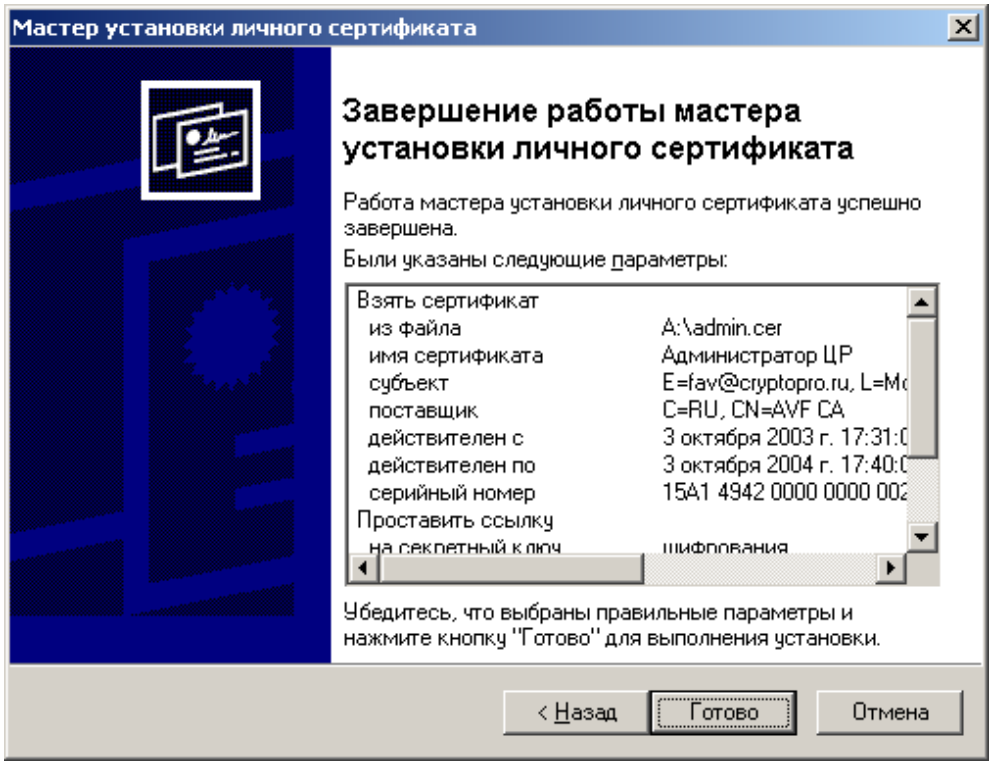
6. В появившемся окне **Контейнер секретного ключа** установите переключатель **Введенное имя задает ключевой контейнер** в положение **Пользователь,** выберите необходимый CSP из предлагаемого списка. С помощью кнопки **Обзор** выберите ключевой контейнер, содержащий закрытый ключ привилегированного пользователя. Нажмите кнопку **Далее**.



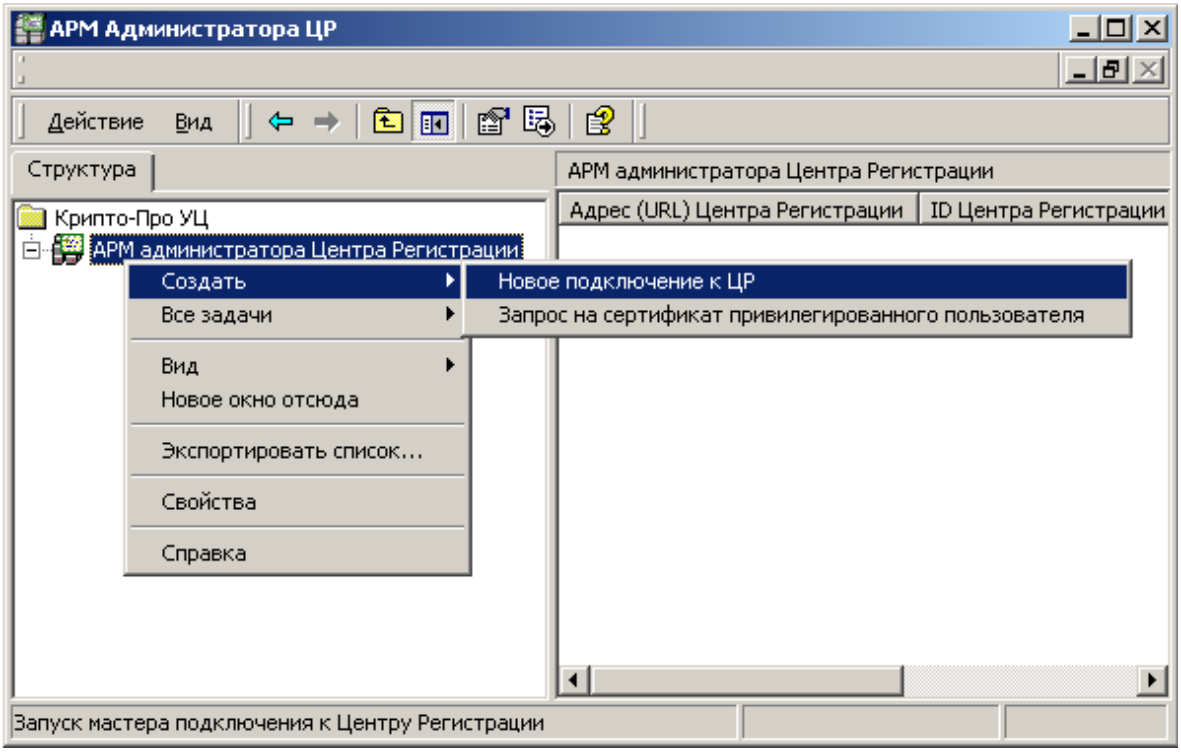
7. Откроется окно **Хранилище сертификатов,** в котором необходимо с помощью кнопки **Обзор** выбрать хранилище сертификатов **Личные**



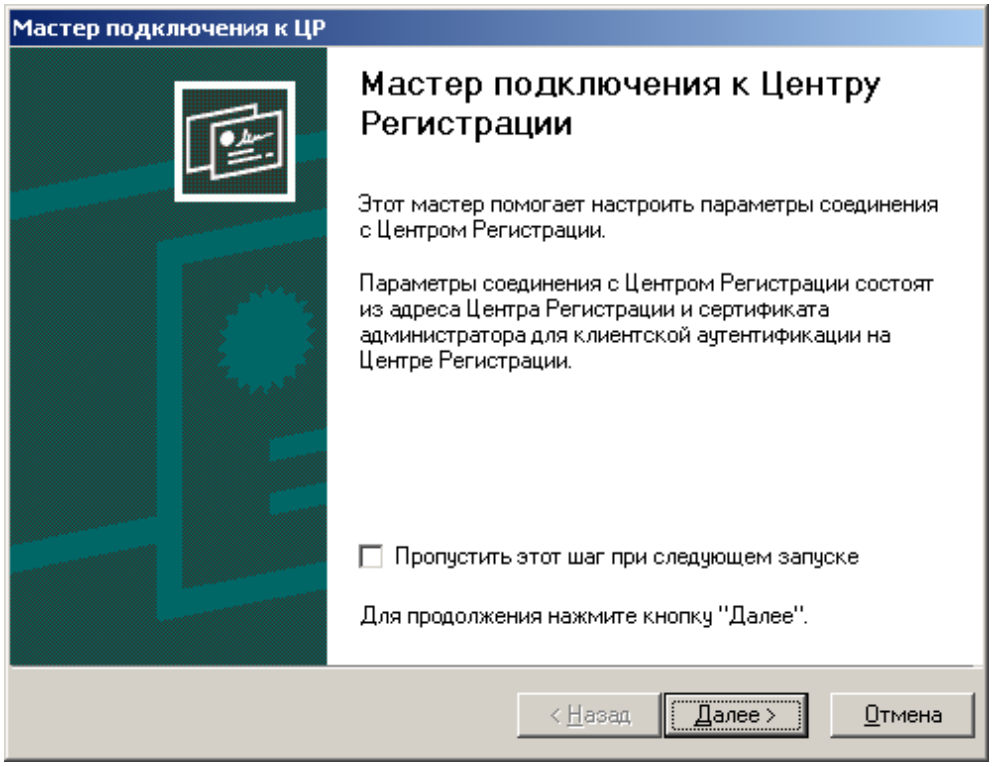
8. В окне **Завершение работы мастера установки личного сертификата** убедитесь, что указаны правильные параметры и нажмите кнопку **Готово**.



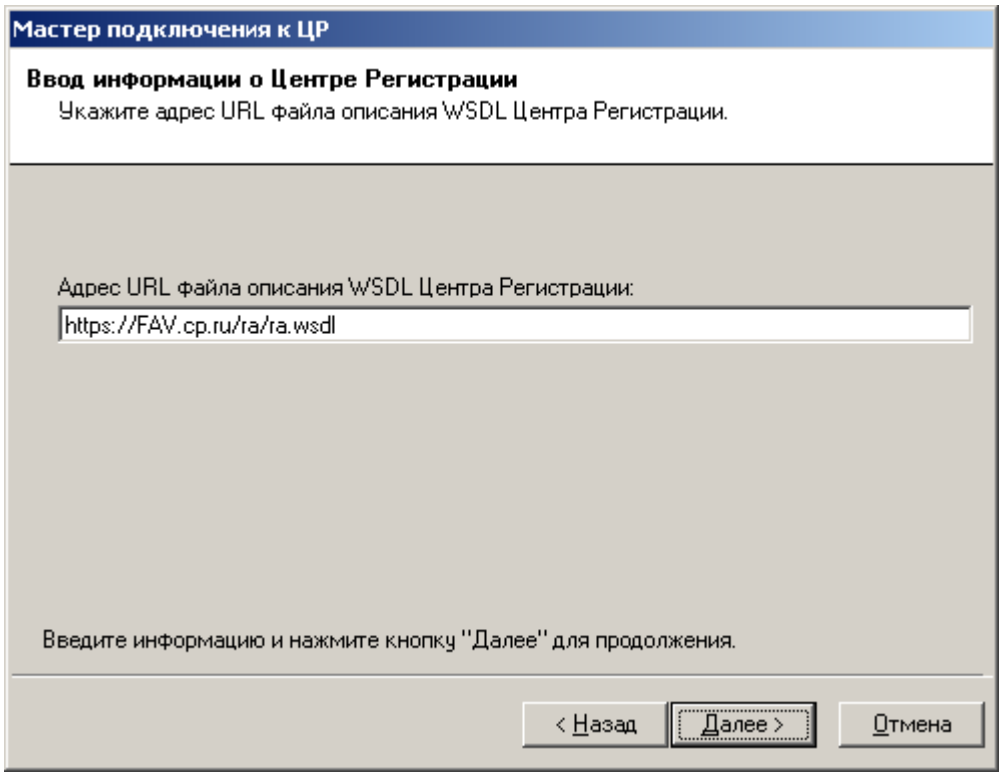
9. Сертификат привилегированного пользователя успешно установлен на компьютер АРМ администратора ЦР.
10. Откройте окно приложения **АРМ администратора ЦР** (**Пуск**, **Программы**, **Крипто-Про**, **АРМ администратора ЦР**), выберите правой кнопкой мыши раздел **АРМ администратора Центра Регистрации**. В открывшемся меню выберите **Создать/Новое подключение к ЦР**



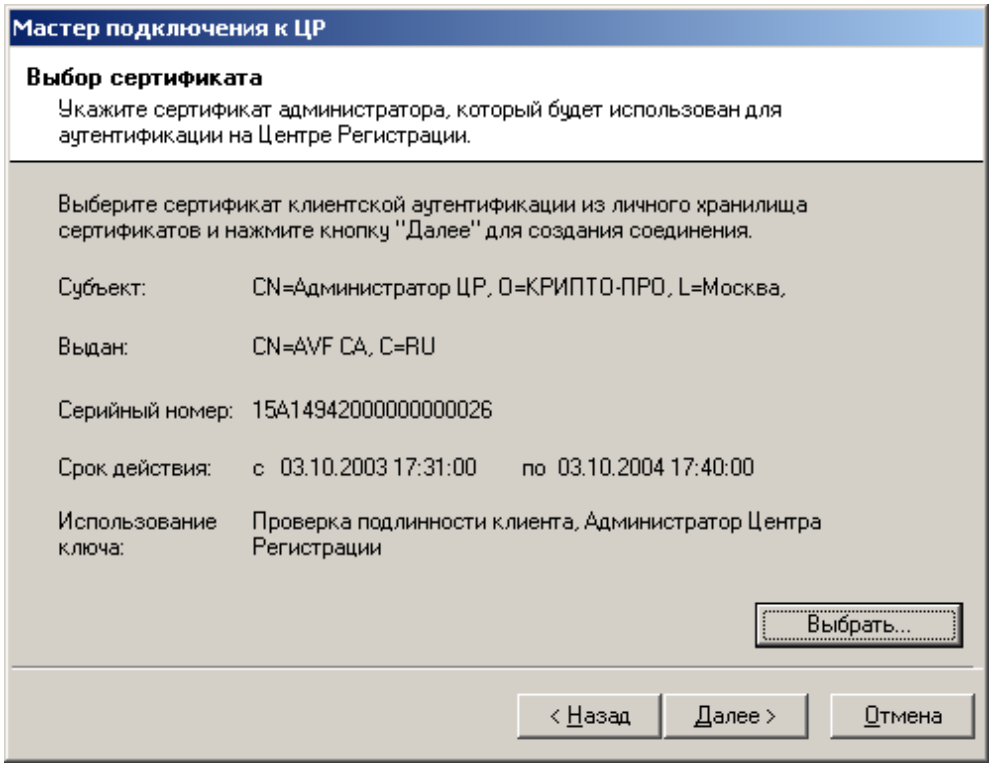
11. Запустится **Мастер подключения к Центру регистрации**. Нажмите кнопку **Далее**



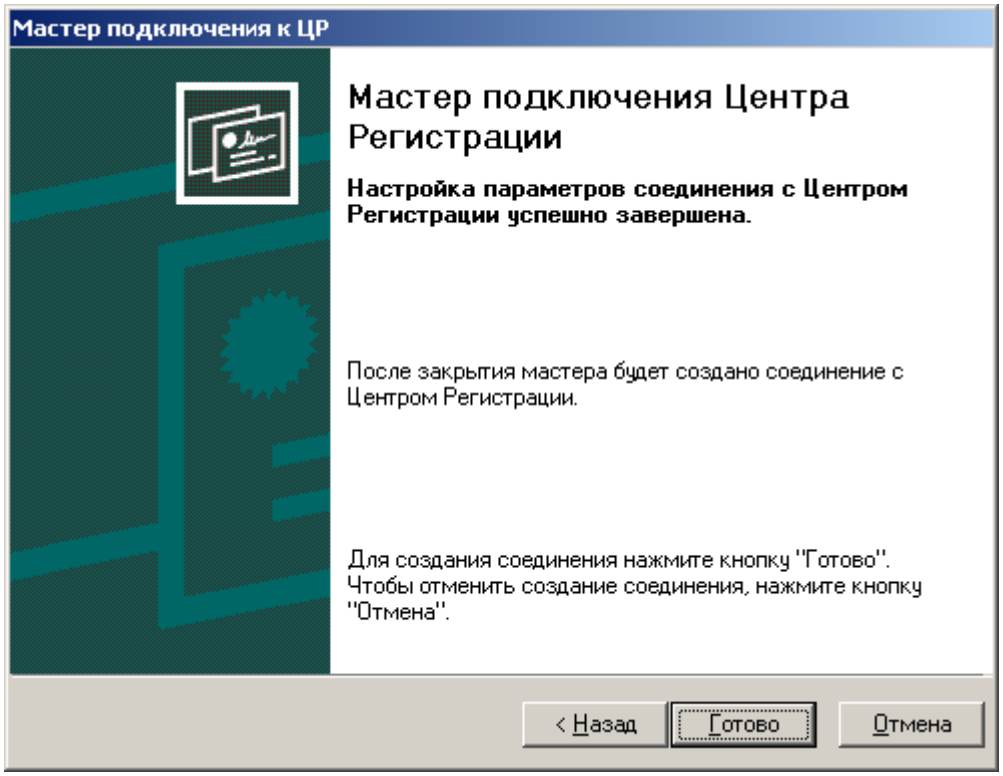
12. В окне **Ввод информации о Центре регистрации** укажите необходимый адрес URL. Нажмите кнопку **Далее**



13. В окне **Выбор сертификата** нажмите кнопку **Выбрать** и из открывшегося списка сертификатов выберите сертификат привилегированного пользователя. Нажмите кнопку **Далее**



14. Откроется окно завершения работы **Мастера подключения Центра регистрации**. Нажмите кнопку **Готово**



15. Приложение осуществит соединение с Центром регистрации