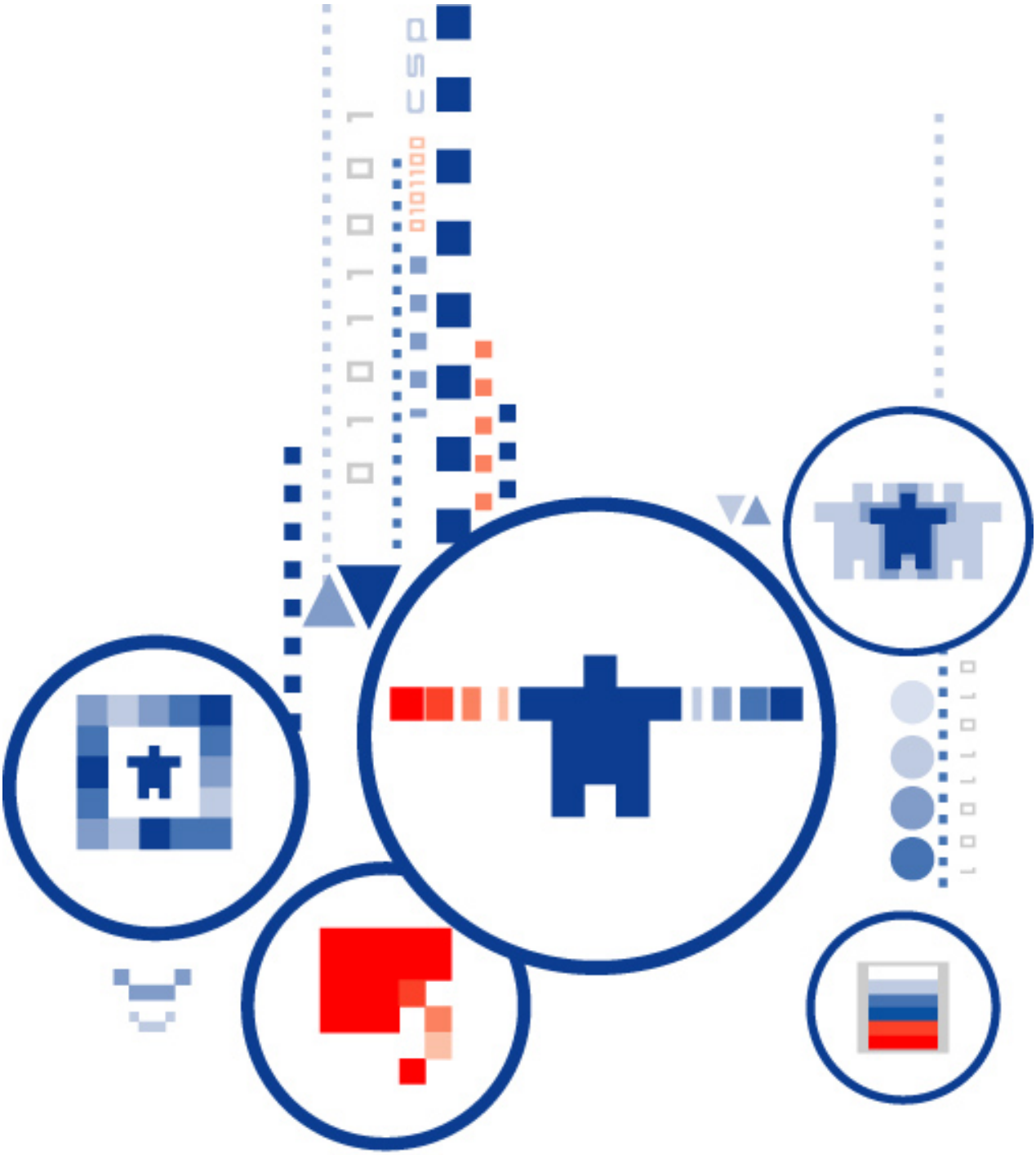
УТВЕРЖДЕН
ЖТЯИ.00035-01 90 02-ЛУ

ЖТЯИ.00035-01 90 02



КриптоПро УЦ

программно–аппаратный комплекс
удостоверяющий центр

Руководство по установке

АННОТАЦИЯ

Настоящий документ содержит описание процесса установки программного комплекса «Удостоверяющий Центр «КриптоПро УЦ» (УЦ).

Настоящий документ предназначен для администраторов как руководство по установке УЦ.

Информация о разработчике ПК «КриптоПро УЦ»:

ООО "Крипто-Про"

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

Телефон: (495) 780 4820

Факс: (495) 780 4820

http://www.CryptoPro.ru

E-mail: info@CryptoPro.ru

СОДЕРЖАНИЕ

1. Архитектура и схема взаимодействия компонентов ПАК «КриптоПро УЦ» 5

1.1. Компоненты ПАК «КриптоПро УЦ» 5

1.2. Схема взаимодействия компонентов ПАК «КриптоПро УЦ» 5

1.3. Режимы работы ПАК «КриптоПро УЦ» 5

2. Общая схема установки 7

2.1. Требования к программным и техническим средствам 7

3. Установка Центра Сертификации 9

3.1. Последовательность установки Центра Сертификации 9

3.2. Установка СКЗИ КриптоПро CSP и КриптоПро TLS 9

3.3. Установка служб Microsoft Internet Information Services и службы очередей сообщений 9

3.4. Формирование и запись в %systemroot% файла политик CAPolicy.inf 10

3.5. Установка службы сертификации 11

3.6. Установка приложений «Утилиты Центра сертификации» 18

3.7. Выпуск и инсталляция сертификата серверной аутентификации Web-сервера ЦС .. 19

3.7.1. Выпуск сертификата WEB-сервера ЦС 19

3.7.2. Инсталляция сертификата серверной аутентификации на Web-сервере ЦС . 24

3.8. Установка программного обеспечения ЦС 25

4. Установка Центра Регистрации 32

4.1. Последовательность установки Центра Регистрации 32

4.2. Установка СКЗИ КриптоПро CSP и КриптоПро TLS 32

4.3. Установка служб Microsoft Internet Information Services и службы очередей сообщений 32

4.4. Установка приложений «Утилиты Центра Регистрации» 32

4.5. Выпуск и инсталляция сертификата серверной аутентификации Web-сервера ЦР... 34

4.5.1. Выпуск сертификата WEB-сервера ЦР 34

4.5.2. Инсталляция сертификата серверной аутентификации на Web-сервере ЦР . 40

4.6. Установка программного обеспечения ЦР 40

4.7. Выпуск и инсталляция клиентского сертификата Центра Регистрации 47

4.8. Настройка и тестирование соединения с Центром Сертификации 55

5. Установка АРМ администратора ЦР 58

5.1. Последовательность установки АРМ администратора ЦР 58

5.2. Установка СКЗИ КриптоПро CSP и КриптоПро TLS 58

5.3. Установка программного обеспечения АРМ администратора ЦР 58

5.4. Подключение привилегированного пользователя 62

6. Установка АРМ разбора конфликтных ситуаций 74

6.1. Последовательность установки АРМ разбора конфликтных ситуаций 74

6.2. Установка СКЗИ КриптоПро CSP 74

6.3. Установка программного обеспечения АРМ разбора конфликтных ситуаций 74

7. Перечень сокращений 77

8. Перечень рисунков 78

1. Архитектура и схема взаимодействия компонентов ПАК «КриптоПро УЦ»

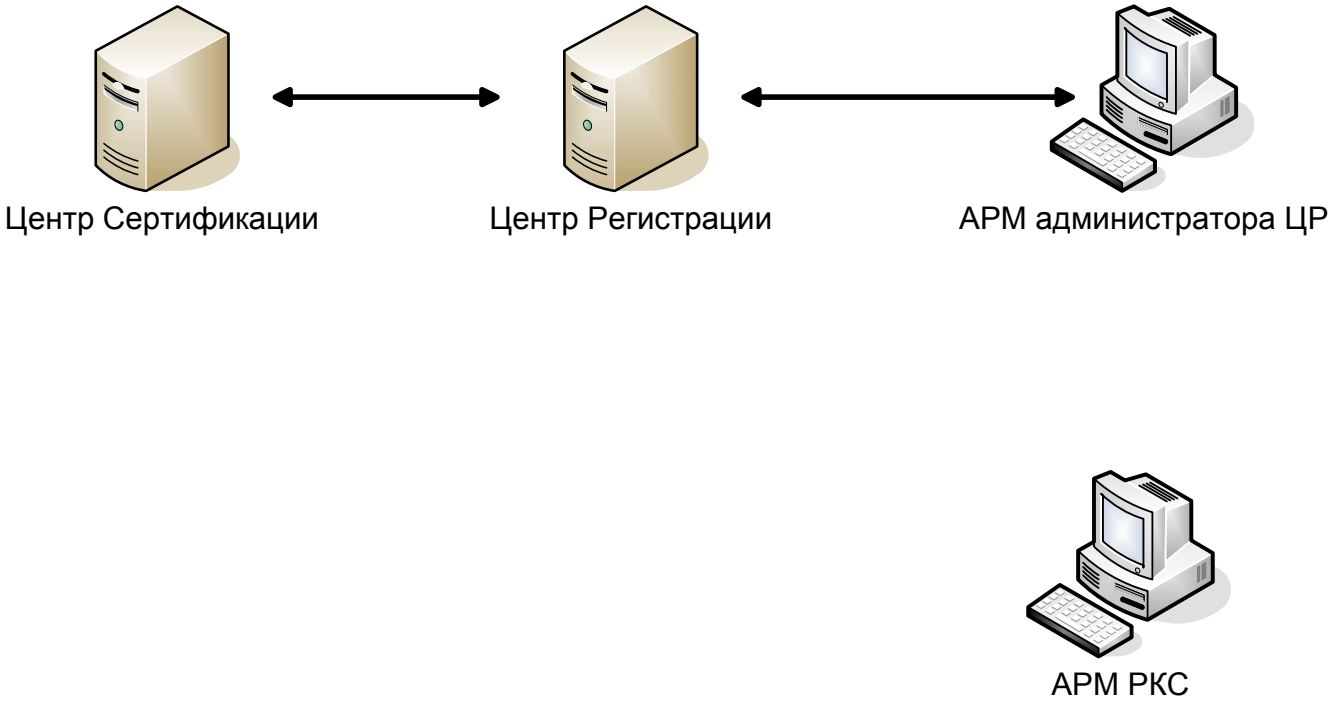
1.1. Компоненты ПАК «КриптоПро УЦ»

В состав ПАК «КриптоПро УЦ» входят следующие программные компоненты, подлежащие установке:

- Центр Сертификации (ЦС)
- Центр Регистрации (ЦР)
- АРМ администратора ЦР
- АРМ разбора конфликтных ситуаций (АРМ РКС)

1.2. Схема взаимодействия компонентов ПАК «КриптоПро УЦ»

Рисунок 1. Схема взаимодействия компонентов ПАК «КриптоПро УЦ»



Как видно из схемы взаимодействия компонентов ПАК «КриптоПро УЦ» (Рисунок 1), Центр Сертификации взаимодействует только с одним или несколькими Центрами Регистрации. АРМ администратора ЦР взаимодействует только с одним или несколькими Центрами Регистрации. АРМ администратора ЦР не вступает во взаимодействие с Центром Сертификации.

Основное взаимодействие между компонентами ПАК «КриптоПро УЦ» осуществляется по протоколам HTTP(S) и, как правило, по порту 443. Используется также протокол HTTP (как правило, порт 80) при передаче файла со списком отозванных сертификатов между компонентами ПАК «КриптоПро УЦ».

АРМ РКС не взаимодействует не с одним из других компонентов ПАК «КриптоПро УЦ» и может работать на изолированном компьютере.

1.3. Режимы работы ПАК «КриптоПро УЦ»

ПАК «КриптоПро УЦ» может работать в двух режимах:

- **Корневой УЦ**
- **Подчиненный УЦ**

Корневой УЦ – это режим, при котором Центр Сертификации ПАК «КриптоПро УЦ», стоит на высшей ступени иерархии Удостоверяющих Центров или используется одиночный Центр Сертификации ПАК «КриптоПро УЦ».

Подчиненный УЦ – это режим, при котором Центр сертификации ПАК «КриптоПро УЦ» получает свой сертификат от вышестоящего в иерархии Удостоверяющих Центров Центра Сертификации.

Выбор режима работы Центра Сертификации ПАК «КриптоПро УЦ» зависит от выбора соответствующего режима при установке службы сертификации ЦС ПАК «КриптоПро УЦ». После установки службы сертификации ЦС ПАК «КриптоПро УЦ» сменить режим работы возможно только путем полной переустановки ПАК «КриптоПро УЦ».

2. Общая схема установки

Установка ПАК «КриптоПро УЦ» выполняется в следующем порядке:

1. Подготовка технических средств компонентов ПАК «КриптоПро УЦ»
2. Установка общесистемного программного обеспечения на технические средства компонентов ПАК «КриптоПро УЦ» (включая обновления Windows)
3. Настройка сетевого взаимодействия общесистемного программного обеспечения компонентов ПАК «КриптоПро УЦ»
4. Установка Центра Сертификации
5. Установка Центра Регистрации
6. Тестирование на Центре Регистрации соединения с Центром Сертификации до получения положительного результата
7. Установка АРМ администратора ЦР
8. Подключение администратора ЦР в качестве привилегированного пользователя с ролью «Оператор»
9. Тестирование соединения АРМ администратора ЦР с Центром Регистрации до получения положительного результата
10. Установка АРМ разбора конфликтных ситуаций.

После завершения установки компонентов ПАК «КриптоПро УЦ» выполняется конфигурирование и настройка компонентов Центр Сертификации и Центр Регистрации в соответствии с требованиями по режиму эксплуатации. Как правило, такие требования определяются Регламентом услуг удостоверяющего центра.

2.1. Требования к программным и техническим средствам

В качестве аппаратной платформы для функционирования Центра Сертификации и Центра Регистрации должен использоваться компьютер (сервер) типа IBM PC с процессором Pentium IV (и выше), частотой процессора от 1 ГГц и с минимальным объемом оперативной памяти – 1 Гбайт.

Специальных требований по защищенности компьютера (сервера) не предъявляется.

Компьютер (сервер) должен быть оснащен:

- устройством защиты от НСД типа электронный замок («Соболь PCI» или «Аккорд»);
- устройством для записи резервных копий на съемный носитель информации (CD-RW, стример и т.д.);
- сетевой картой для обеспечения сетевого взаимодействия.

В качестве программной платформы может использоваться операционная система Microsoft Windows Server 2000 с установленным пакетом обновлений SP4 или Microsoft Windows Server 2003 с установленным пакетом обновлений SP2. Операционные системы могут быть как английской версии, так и русской.

При использовании Microsoft Windows Server 2000 с установленным пакетом обновлений SP4, для обеспечения возможности выпуска сертификата по готовому запросу из файла в случае, когда в запросе имеется атрибут 1.2.840.113549.1.9.14 («Расширения

сертификатов»), а также для обеспечения возможности настройки политик выдачи и политик применения сертификатов обязательно следует установить на серверах ЦС и ЦР 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).

Для обеспечения требований по безопасности эксплуатации не рекомендуется устанавливать Центр Сертификации ПАК «КриптоПро УЦ» на контроллер домена или на сервер, подключенный к домену (Active Directory).

В качестве аппаратной платформы для функционирования АРМ администратора ЦР и АРМ РКС должен использоваться компьютер типа IBM PC с процессором Pentium III (и выше), частой процессора от 700 МГц и с минимальным объемом оперативной памяти – 512 Мбайт.

Специальных требований по защищенности компьютера не предъявляется.

Компьютер должен быть оснащен:

- устройством защиты от НСД типа электронный замок («Соболь PCI» или «Аккорд»);
- сетевой картой для обеспечения сетевого взаимодействия.

В качестве программной платформы может использоваться операционная система Microsoft Windows Server 2000 с установленным пакетом обновлений SP4, Microsoft Windows Professional 2000 с установленным пакетом обновлений SP4, Microsoft Windows Server 2003 с установленным пакетом обновлений SP2, Microsoft Windows XP с установленным пакетом обновлений SP2. Операционные системы могут быть как английской версии, так и русской.

При использовании Microsoft Windows 2000 с установленным пакетом обновлений SP4, для обеспечения возможности выпуска сертификата по готовому запросу из файла в случае, когда в запросе имеется атрибут 1.2.840.113549.1.9.14 («Расширения сертификатов»), обязательно следует установить на компьютере с АРМ администратора ЦР 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).

3. Установка Центра Сертификации

Данный раздел настоящего Руководства определяет последовательность и порядок действий при установке программного обеспечения Центра Сертификации ПК «КриптоПро УЦ» в режиме «с нуля». Данный режим означает, что на сервере была произведена установка операционной системы на отформатированный диск.

Последовательность и порядок действий при установке программного обеспечения Центра Сертификации для обновления ранее установленной версии (релиза) ЦС описываются в документе «Особенности версии» (файл ReleaseNotes.pdf), входящий в состав дистрибутива ПО Центра Сертификации.

3.1. Последовательность установки Центра Сертификации

Установка и конфигурация Центра Сертификации ПАК «КриптоПро УЦ» производится в следующей последовательности:

1. Установка СКЗИ КриптоПро CSP и КриптоПро TLS
2. Установка служб Microsoft Internet Information Services и службы очередей сообщений
3. Формирование и запись в %systemroot% файла политик CAPolicy.inf
4. Установка службы сертификации из состава MS Windows
5. Установка приложений «Утилиты Центра сертификации»
6. Выпуск и инсталляция сертификата серверной аутентификации Web-сервера ЦС
7. Установка программного обеспечения ЦС ПАК «КриптоПро УЦ»

3.2. Установка СКЗИ КриптоПро CSP и КриптоПро TLS

На сервере Центра Сертификации устанавливается СКЗИ «КриптоПро CSP» версии 3.0 (исполнение 6 для класса защиты КС2).

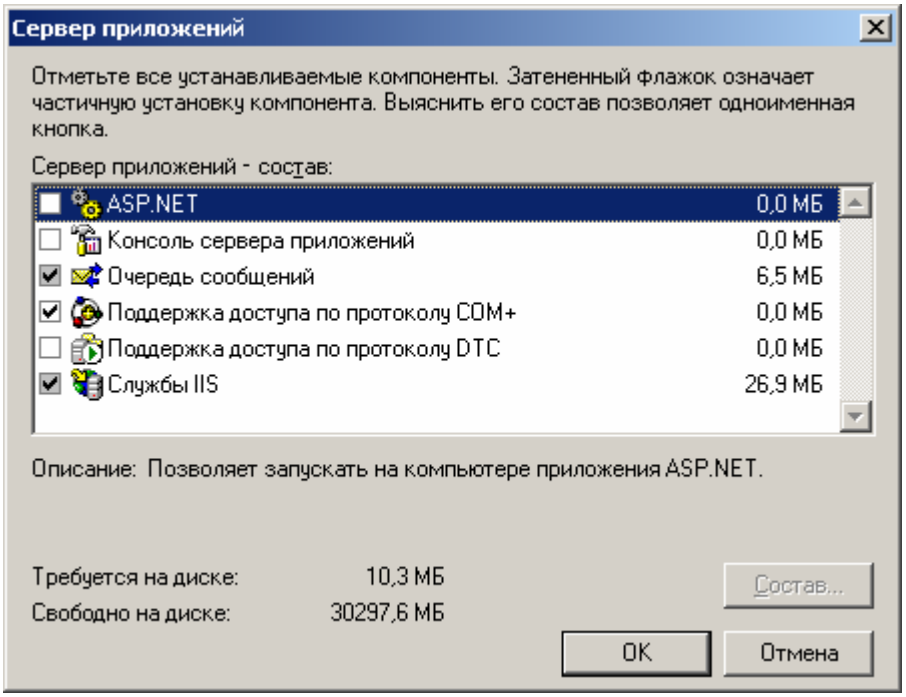
Установка СКЗИ «КриптоПро CSP» осуществляется в соответствии с эксплуатационной документацией. Модуль «КриптоПро TLS» входит в состав дистрибутива и не требует отдельной установки.

После установки программного обеспечения СКЗИ «КриптоПро CSP» и «КриптоПро TLS» необходимо активировать лицензию на продукт из набора лицензий поставки ПАК «КриптоПро УЦ» и включить режим **кеширования** (вкладка **Безопасность** окна свойств КриптоПро CSP).

3.3. Установка служб Microsoft Internet Information Services и службы очередей сообщений

Установка служб осуществляется с использованием Мастера компонентов Windows.

Рисунок 2. Установка служб IIS и службы очередей сообщений



В составе служб IIS рекомендуется оставить следующий набор служб:

- диспетчер служб IIS

- общие файлы

- служба WWW

3.4. Формирование и запись в %systemroot% файла политик CAPolicy.inf

Файл политик CAPolicy.inf используется в «КриптоПро УЦ» в следующих целях:

- Для установки значений дополнения CRL Distribution Point (точка распределения списка отозванных сертификатов, CDP) сертификата открытого ключа уполномоченного лица удостоверяющего центра (сертификата ЦС);
- Для включения в сертификат ЦС политик выдачи сертификатов, издаваемых этим Центром Сертификации.

Для установки значений дополнения CDP сертификата открытого ключа ЦС необходимо **ДО** установки службы сертификации ЦС сформировать файл политик с именем **CAPolicy.inf** и расположить его в системном корневом каталоге **%systemroot%.**

Для корневого Центра Сертификации рекомендуется не включать расширение CDP в состав самоподписанного сертификата ЦС. Для этого необходимо сформировать файл CAPolicy.inf со следующим содержимым:

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

Для включения в сертификаты ЦС политик выдачи сертификатов необходимо сформировать файл политик с именем **CAPolicy.inf** в соответствии со справочным руководством Службы сертификации Windows 2000 (2003) Server и Регламентом УЦ.

Как правило, в большинстве систем политики выдачи сертификатов не используются, и задавать их в файле CAPolicy.inf не нужно. Но исключать расширение CDP из сертификата ЦС настоятельно рекомендуется.

Далее приведены примеры включения политик выдачи сертификатов в сертификат ЦС. Значения OID в этих примерах зарегистрированы ООО «КРИПТО-ПРО» и предназначены для использования только в тестовых целях.

Образец содержимого файла CAPolicy.inf для ЦС Удостоверяющего Центра на Windows 2000 Server, реализующего централизованный режим регистрации пользователей УЦ, и включаемый в дополнение к указанному выше содержимому файла, приведен ниже.

[CAPolicy]

Policies=*CertCPPolicy*

[*CertCPPolicy*]

OID=*1.2.643.2.2.38.1*

URL="http::*//UCWebSite/CAPolicy/default.asp*"

Notice="Класс 1 идентификации субъекта"

Образец содержимого файла CAPolicy.inf для ЦС Удостоверяющего Центра на Windows 2000 Server, реализующего распределенный (сетевой) режим регистрации пользователей УЦ, и включаемый в дополнение к указанному выше содержимому файла, приведен ниже.

[CAPolicy]

Policies=*CertCPPolicy*

[*CertCPPolicy*]

OID=*1.2.643.2.2.38.2*

URL="http::*//UCWebSite/CAPolicy/default.asp*"

Notice="Класс 2 идентификации субъекта"

Для Windows 2003 Server вместо [CAPolicy] нужно использовать [PolicyStatementExtension].

3.5. Установка службы сертификации

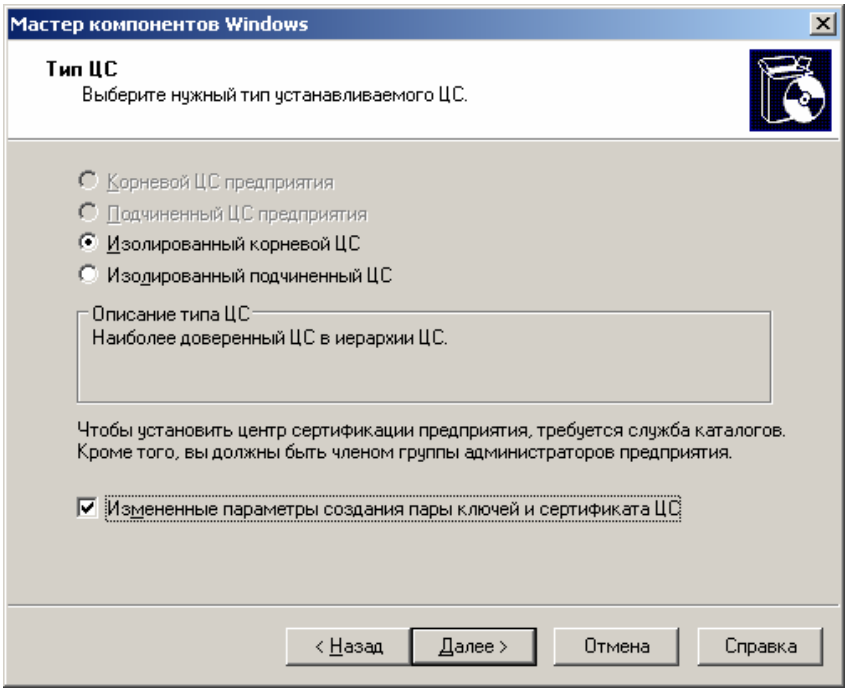
Установка службы сертификации производится с использованием Мастера компонентов Windows в следующей последовательности.

1. Открыть окно **Панели управления**, выполнив команды **Пуск, Настройка, Панель управления**.
2. В окне **Панели управления** выбрать пункт **Установка и удаление программ**.
3. В окне **Установки** выбрать пункт **Добавление и удаление компонентов Windows**.
4. В окне мастера добавления компонентов выбрать **Службы Сертификации** (Certificate Services).
5. Определение режима работы Центра сертификации
   - 5.1. Режим «Корневой Центр сертификации»

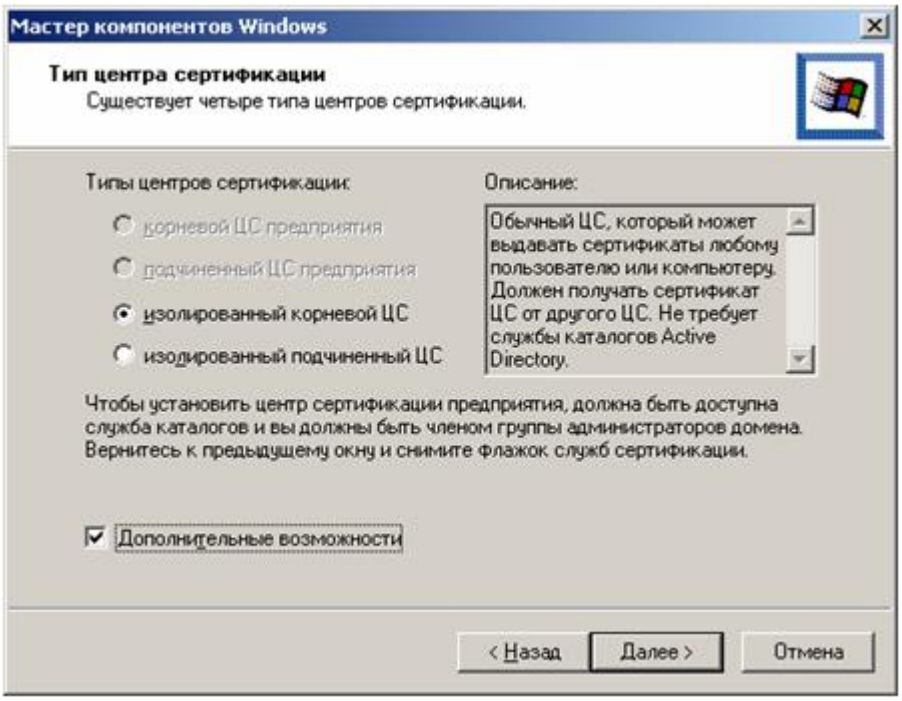
5.1.1. В окне установки **Тип центра сертификации** выбрать **Изолированный корневой ЦС** и установить флаг:

- **Дополнительные возможности** при установке службы сертификации Windows Server 2000. Для Windows Server 2003 данный флаг называется **Измененные параметры создания пары ключей и сертификата ЦС**.

Рисунок 3. Конфигурация ЦС в режиме «Корневой» для Windows Server 2003



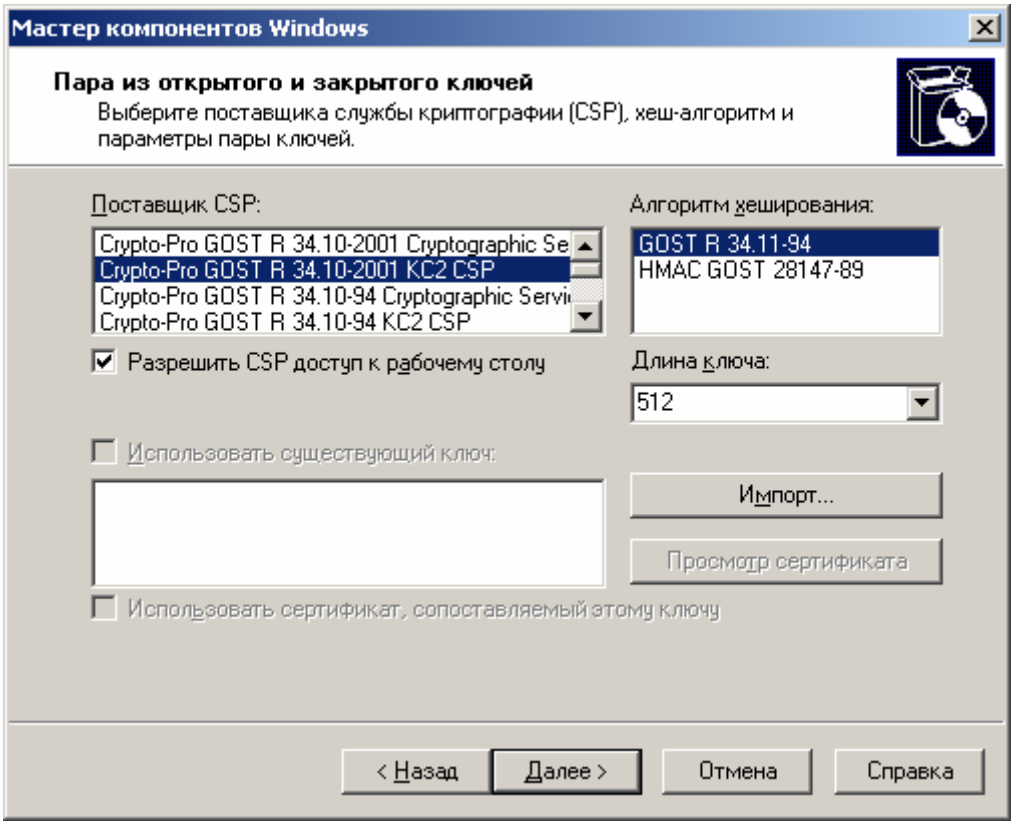
Конфигурация ЦС в режиме «Корневой» для Windows Server 2000



5.1.2. В окне **Пара из открытого и закрытого ключей** выбрать нужный тип провайдера и алгоритм хэширования (см. Рисунок 4). В случае использования существующих ключей, сформированных в соответствии с разделом 3.5 настоящего Руководства, необходимо выбрать (отметить галочкой) опцию **Использовать**

существующий ключ и выбрать из списка наименование соответствующего ключевого контейнера.

Рисунок 4. Выбор параметров генерации ключа ЦС



5.1.3. В окне Сведения о центре сертификации ввести атрибуты ЦС (см. Рисунок 5 и Рисунок 6).

Имя ЦС (общее имя ЦС) может быть введено как кириллицей, так и латиницей. При этом если имя вводится кириллицей, то его длина не должна превышать 12 символов. Если Имя вводится латиницей, то его длина не должна превышать 60 символов. Сведения о ЦС рекомендуется заполнять латиницей.

Рисунок 5. Сведения о центре сертификации в режиме «Корневой» для Windows Server 2000

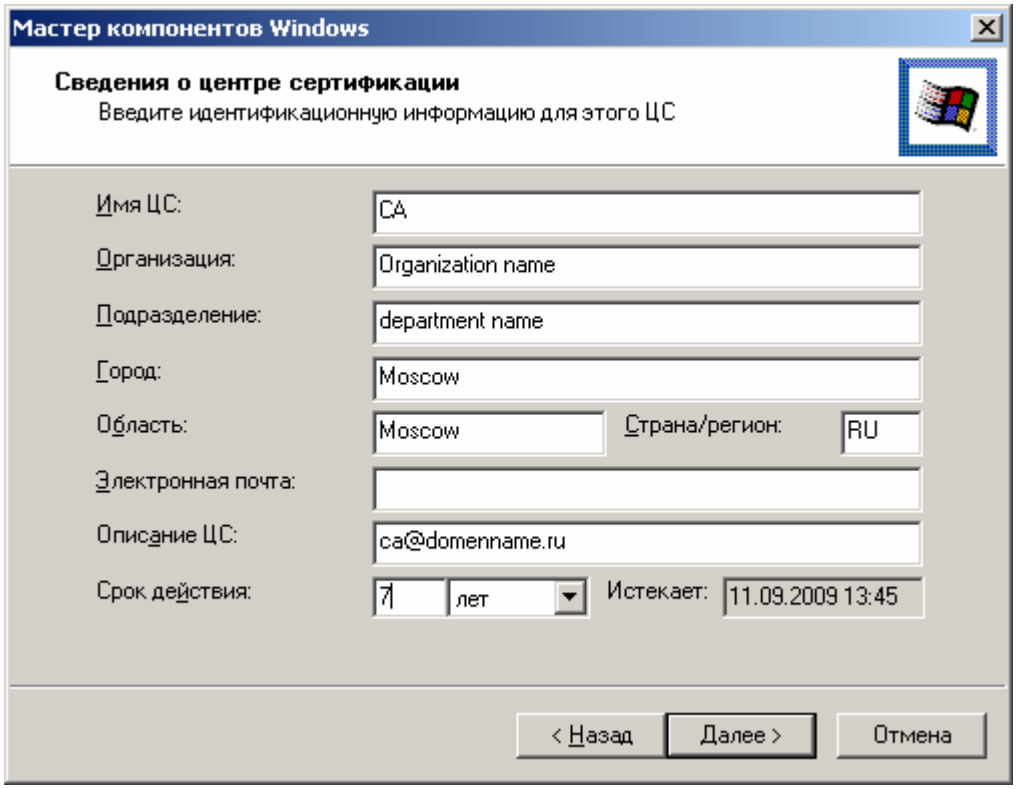
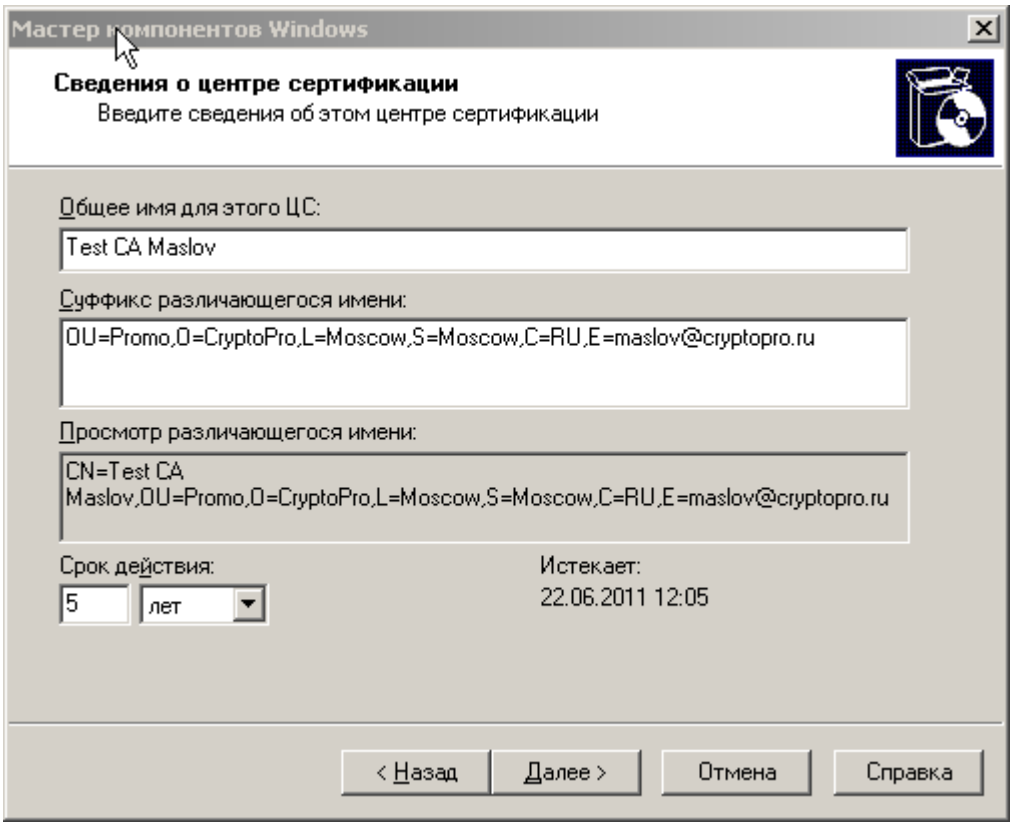
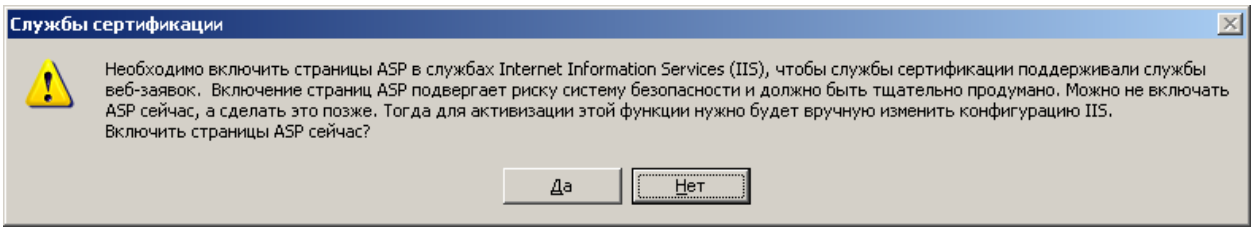


Рисунок 6. Сведения о центре сертификации в режиме «Корневой» для Windows Server 2003



5.1.4. Далее следовать указаниям Мастера установки службы, выбирая предлагаемые значения по умолчанию.

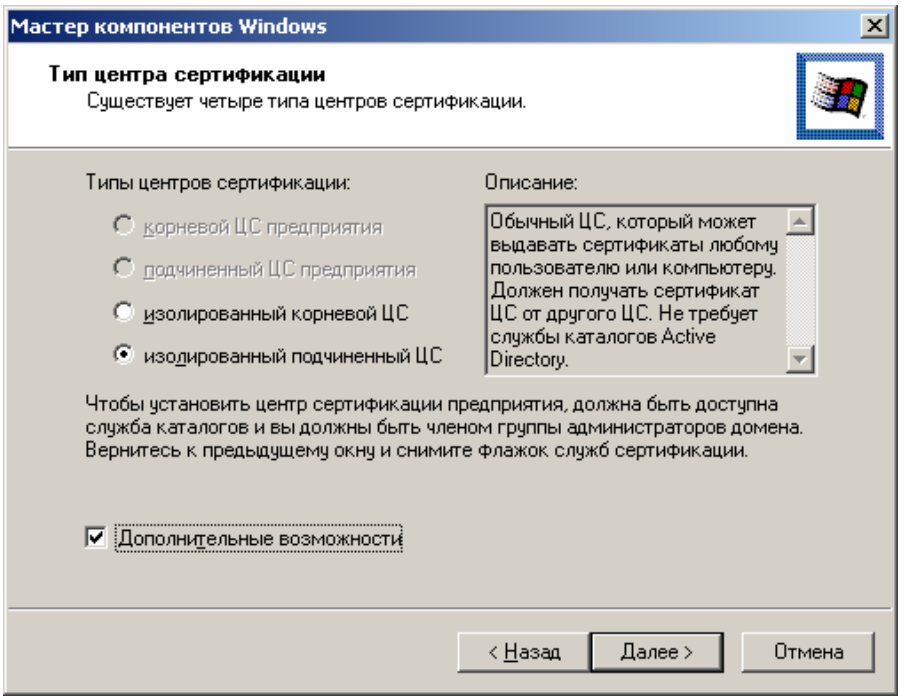
В случае появления (на платформе Windows Server 2003) следующего сообщения, необходимо нажать кнопку **ДА**. При этом разрешается веб-расширение Active Server Pages (ASP). При удалении продуктов запись о разрешении не удаляется. Наличие этой записи необходимо для нормальной работы ПАК «КриптоПро УЦ»



5.2. Режим «Подчиненный Центр сертификации»

5.2.1. В окне установки **Тип центра сертификации** выбрать **Изолированный подчиненный ЦС** (см. Рисунок 7) и установить флаг **Дополнительные возможности** при установке службы сертификации Windows Server 2000. Для Windows Server 2003 данный флаг называется **Измененные параметры создания пары ключей и сертификата ЦС**.

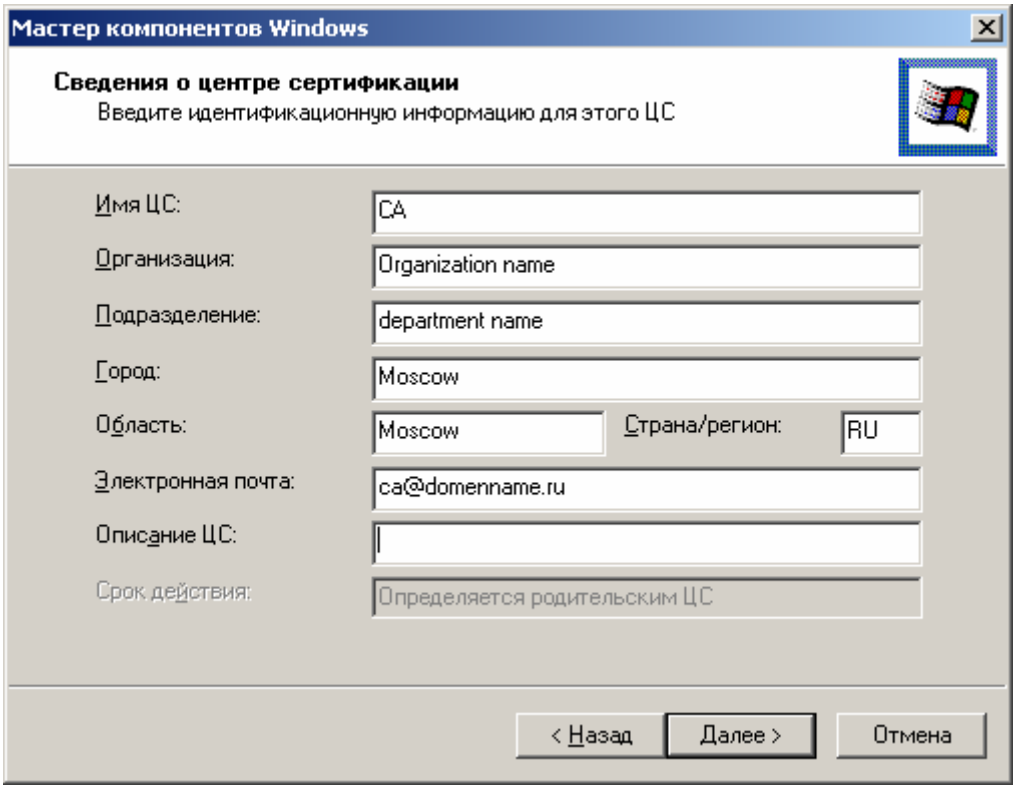
Рисунок 7. Конфигурация ЦС в режиме «Подчиненный» » для Windows Server 2000



5.2.2. В окне **Пара из открытого и закрытого ключей** выбрать нужный тип провайдера и алгоритм хэширования (см.Рисунок 4).

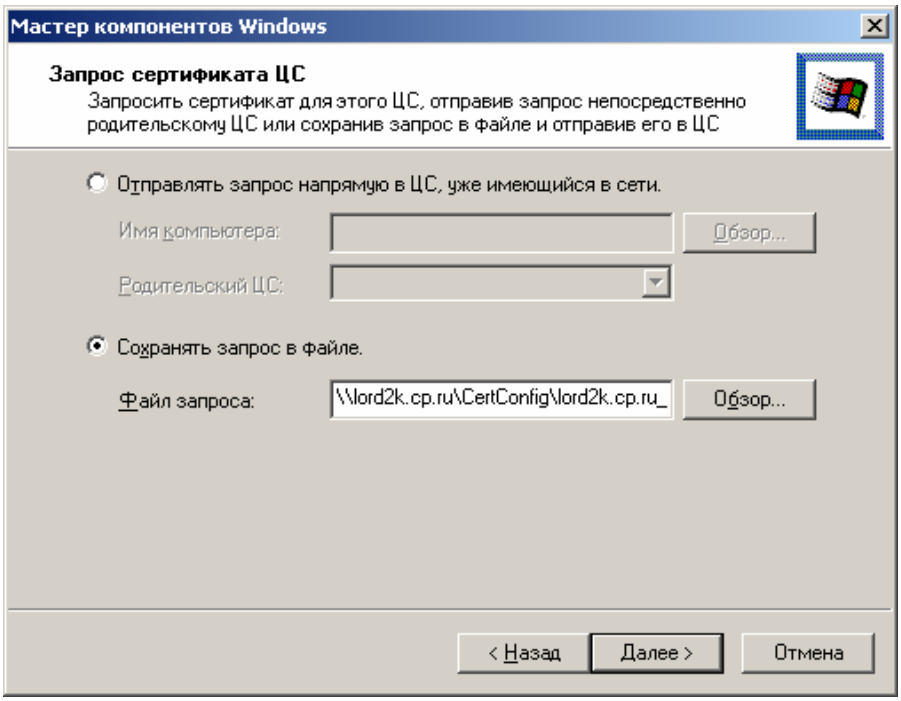
5.2.3. В окне **Сведения о центре сертификации** ввести атрибуты ЦС (см. Рисунок 8). Срок действия сертификат в данном режиме определяется тем Центром сертификации, которому будет подчиняться устанавливаемый ЦС.

Рисунок 8. Сведения о центре сертификации в режиме «Подчиненный»



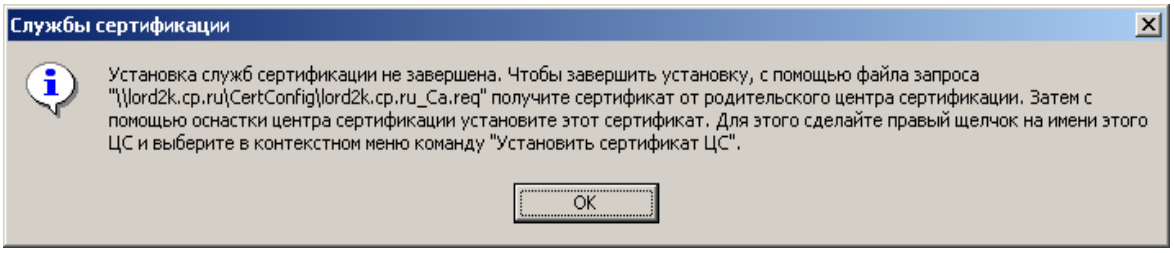
5.2.4. В окне **Запрос сертификата ЦС** выбрать пункт **Запрос в файле** и определить имя и путь размещения файла с запросом на сертификат ЦС (см. Рисунок 9).

Рисунок 9. Запрос на сертификат ЦС



5.2.5. Далее следовать указаниями Мастера до появления сообщения о необходимости продолжения процедуры установки службы сертификации после получения сертификата ЦС (см. Рисунок 10).

Рисунок 10. Сообщение о порядке продолжения установки службы сертификации



5.2.6. Для продолжения процедуры установки ЦС на родительском Центре сертификации получить файлы, содержащие следующую информацию:

- Сертификат устанавливаемого ЦС на основании сформированного запроса;
- Цепочку сертификатов вышестоящих ЦС;
- Списки отозванных сертификатов вышестоящих ЦС.

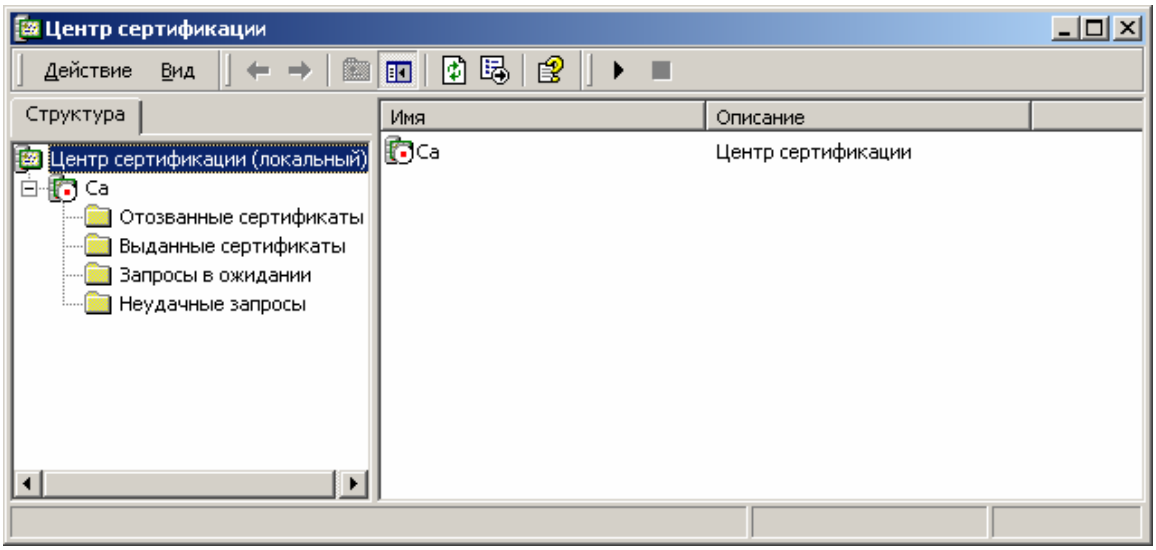
5.2.7. Установить сертификат корневого ЦС в раздел доверенных центров сертификации хранилища сертификатов локального компьютера.

5.2.8. Установить сертификат промежуточных ЦС в раздел промежуточных центров сертификации хранилища сертификатов локального компьютера.

5.2.9. Установить списки отозванных сертификатов вышестоящих ЦС в раздел промежуточных центров сертификации хранилища сертификатов локального компьютера.

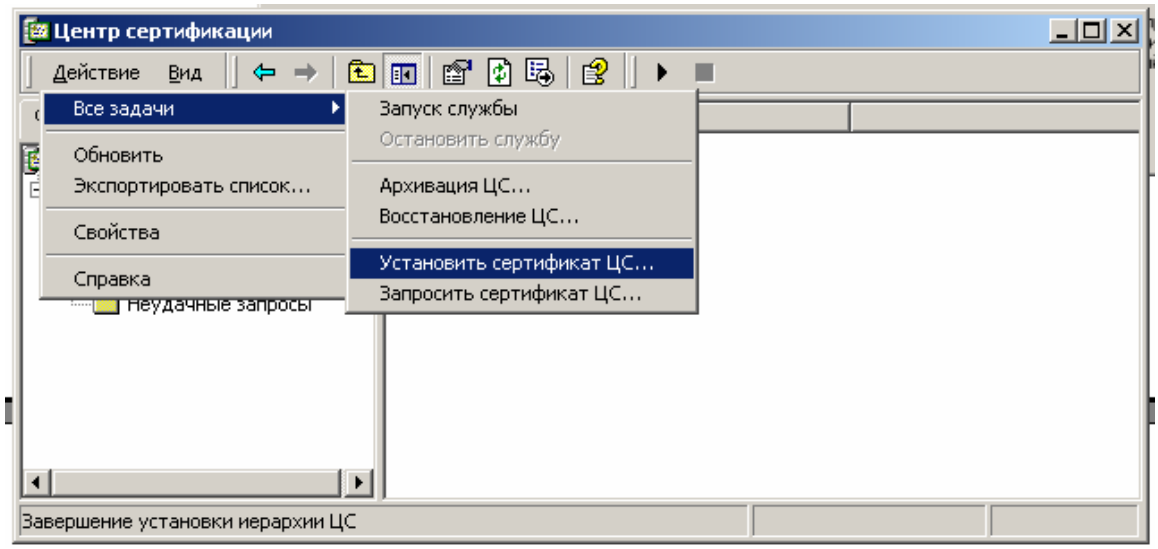
5.2.10. Для продолжения установки службы сертификации открыть консоль управления службы сертификации (см. Рисунок 11)

Рисунок 11. Консоль управления службы сертификации



5.2.11. Нажать кнопку **Действие** и выбрать задачу **Установить сертификат ЦС** (см. Рисунок 12)

Рисунок 12. Запуск задачи установки сертификата ЦС в консоли управления



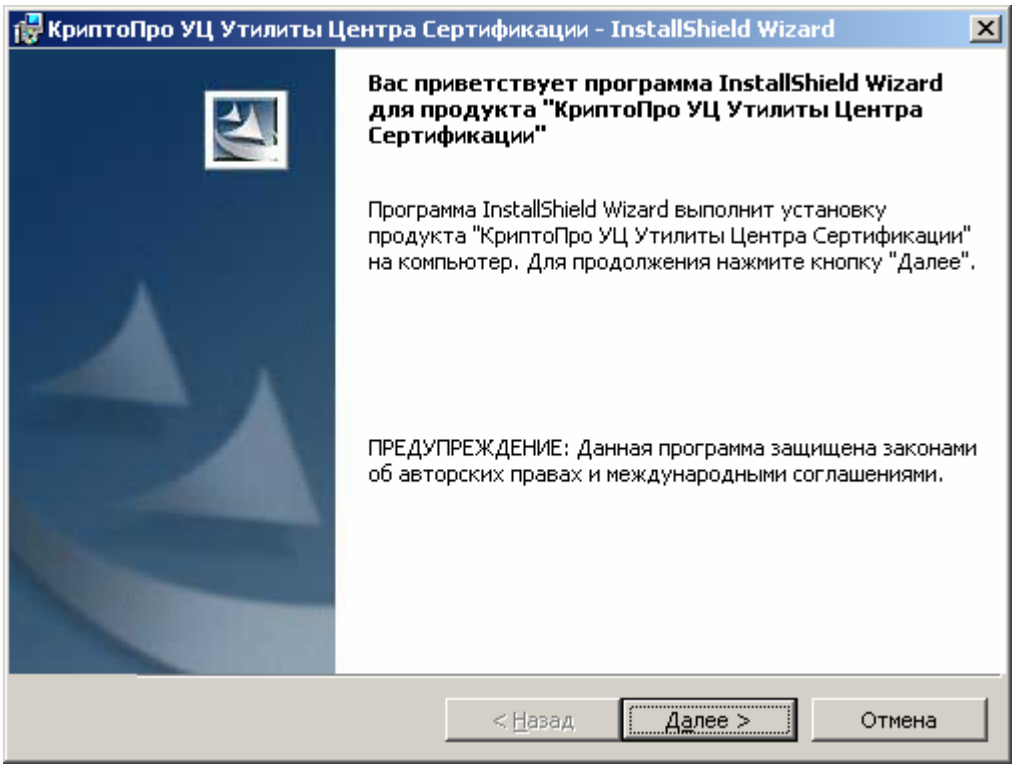
5.2.12. В процессе выполнения задачи установки сертификата выбрать файл с сертификатом устанавливаемого ЦС, полученного на родительском ЦС.

3.6. Установка приложений «Утилиты Центра сертификации»

Для установки приложений Мастеров запустите приложение **SETUP.EXE** из каталога дистрибутива установочного CD.

Инсталляция утилит Центра сертификации производится с помощью Мастера установки (см. Рисунок 13).

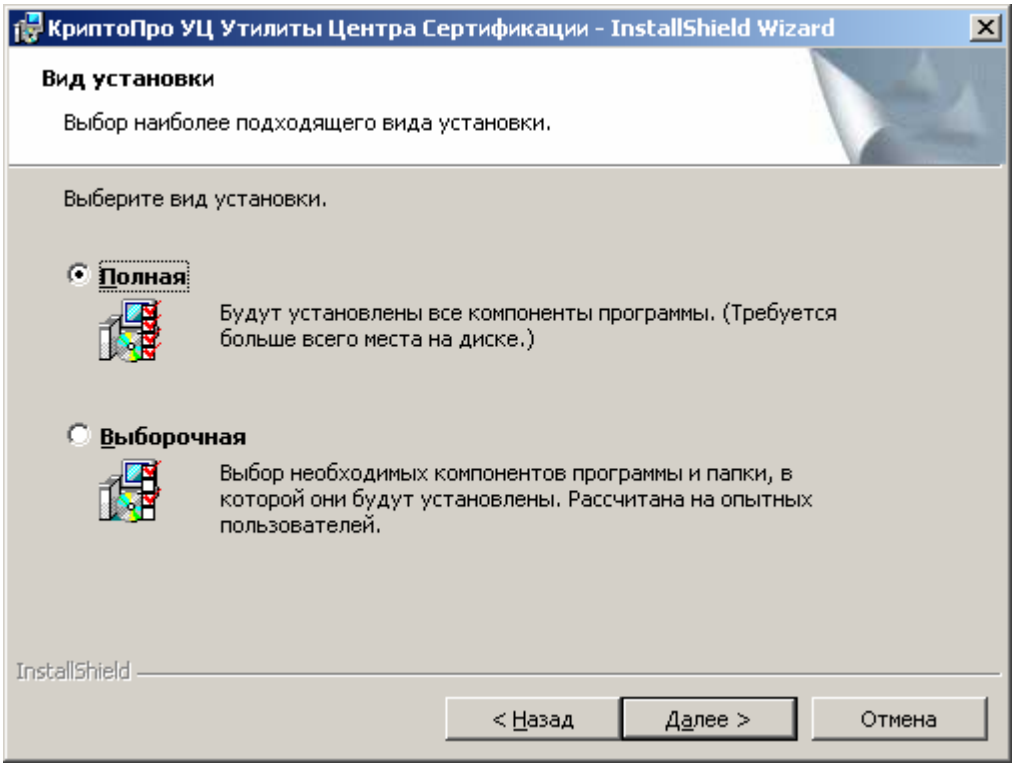
Рисунок 13. Окно Мастера установки утилит Центра сертификации



На все последующие диалоговые сообщения Мастера установки отвечайте выбором значений по умолчанию (кнопка **Далее**).

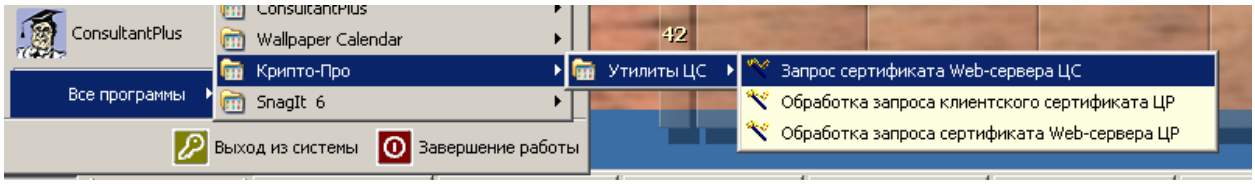
При выборе вида установки (Рисунок 14) следует выбрать **Полная**.

Рисунок 14. Выбор вида установки Утилит Центра Сертификации



После установки, утилиты Центра сертификации (приложения Мастеров) доступны через группу **Крипто-Про** (см. Рисунок 15).

Рисунок 15. Группа "Крипто-Про" меню "Программы"



3.7. Выпуск и инсталляция сертификата серверной аутентификации Web-сервера ЦС

После установки службы сертификации на сервере Центра сертификации необходимо произвести процедуры выпуска, установки и инсталляции на MS IIS сертификата серверной аутентификации Web-сервера Центра Сертификации.

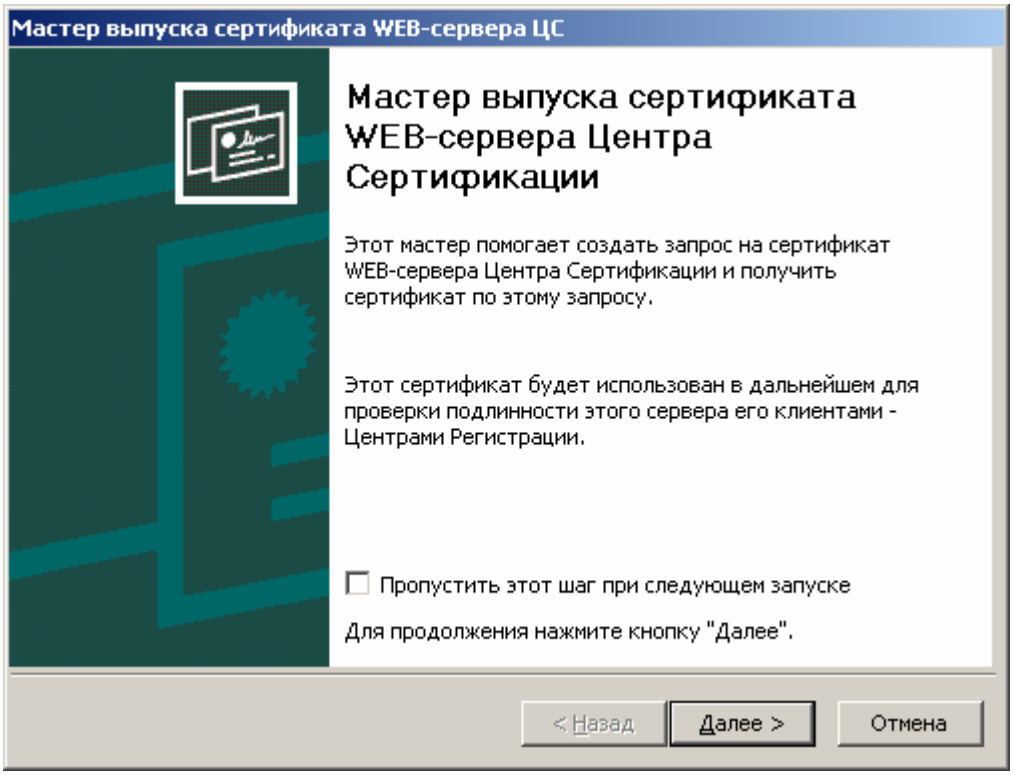
Для этого выполните действия в следующей последовательности

3.7.1. Выпуск сертификата WEB-сервера ЦС

Для обеспечения взаимодействия по HTTPS соединению необходимо сформировать ключи и выпустить сертификат серверной аутентификации WEB-сервера ЦС. Для этого:

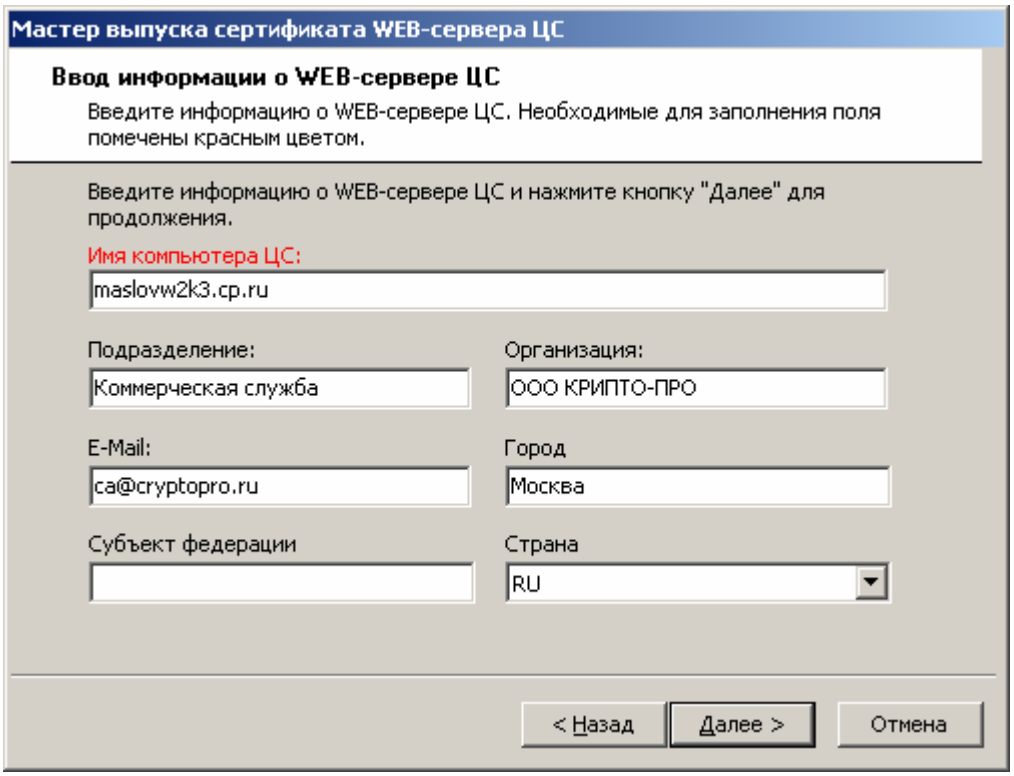
1. Запустите Мастера создания запроса на сертификат WEB-сервера ЦС из группы программ **Крипто-Про** (см. Рисунок 16)

Рисунок 16. Окно Мастера создания запроса на сертификат WEB-сервера ЦС



2. Введите информацию о Web-сервере ЦС (см. Рисунок 17). В разделе **Имя компьютера ЦС** – доменное имя WEB-сервера (например: **lord2k.cp.ru**). Обязательно необходимо, чтобы имя в данном разделе совпадало с доменным именем WEB-сервера Центра Сертификации

Рисунок 17. Окно ввода информации о Web-сервере ЦС Мастера создания запроса на сертификат

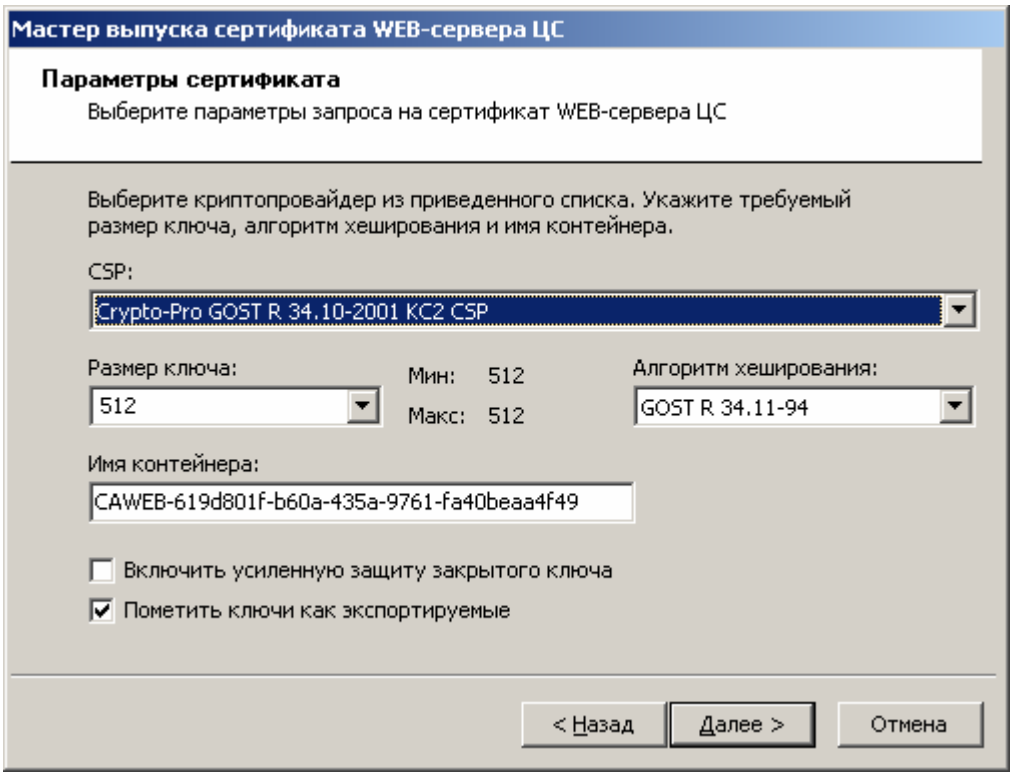


3. При создании запроса на сертификат Web-сервера ЦС необходимо выбрать криптопровайдер (CSP), размер ключа и алгоритм хеширования. Для этого необходимо осуществить определение параметров запроса в диалоговом окне Мастера (см. Рисунок 18).

Не рекомендуется включать усиленную защиту закрытого ключа т.к. это приведет к появлению дополнительных сообщений в процессе работы Центра Сертификации и возможной неработоспособности комплекса в целом.

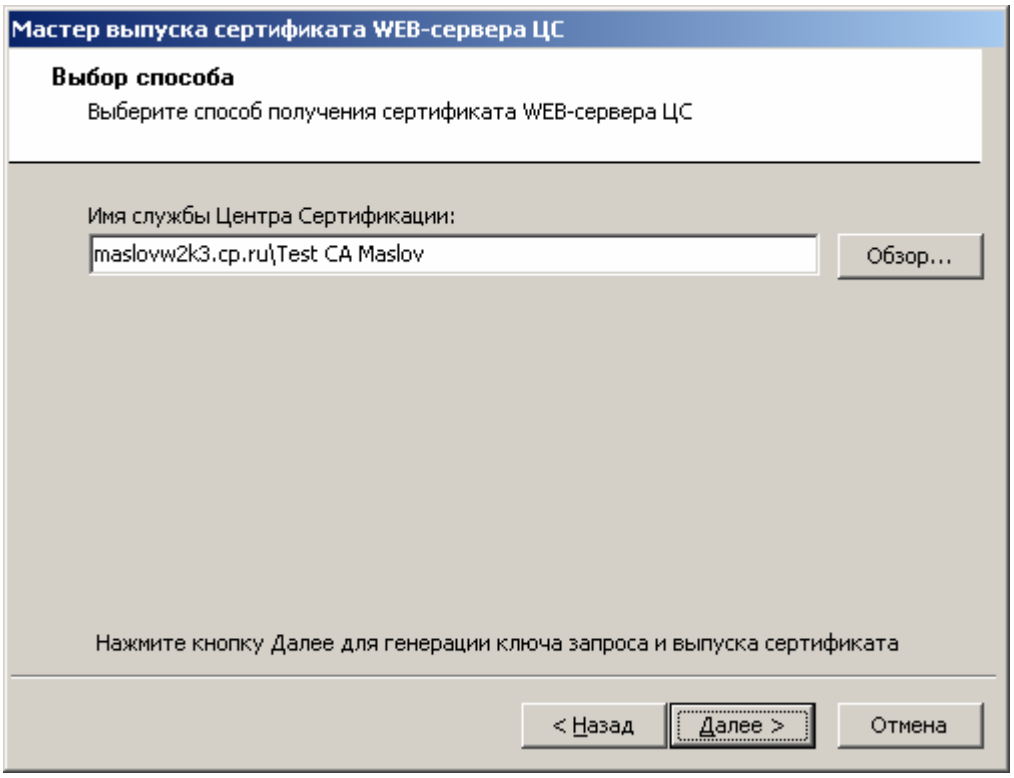
В данном окне Мастера можно задать имя ключевого контейнера или оставить имя по умолчанию.

Рисунок 18. Окно выбора CSP в Мастере создания запроса на сертификат



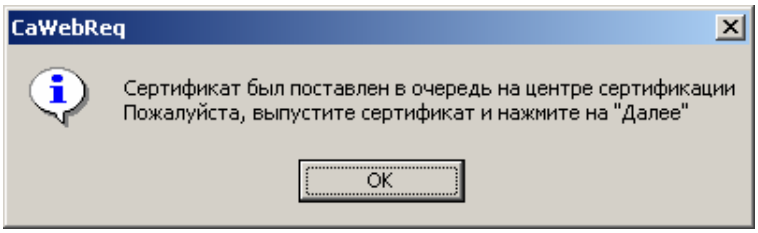
4. В следующем окне (см. Рисунок 19) необходимо выбрать способ получения сертификата Web- сервера Центра сертификации. Для этого нужно выбрать службу сертификации, которая будет обрабатывать запрос (кнопка **Обзор** в верхней строке ввода и выбрать службу из списка). Также необходимо выбрать имя и размещение файла для запроса на сертификат (кнопка **Обзор** в нижней строке ввода). После этого нажмите кнопку **Далее**.

Рисунок 19. Окно выбора способа получения сертификата WEB-сервера ЦС в Мастере



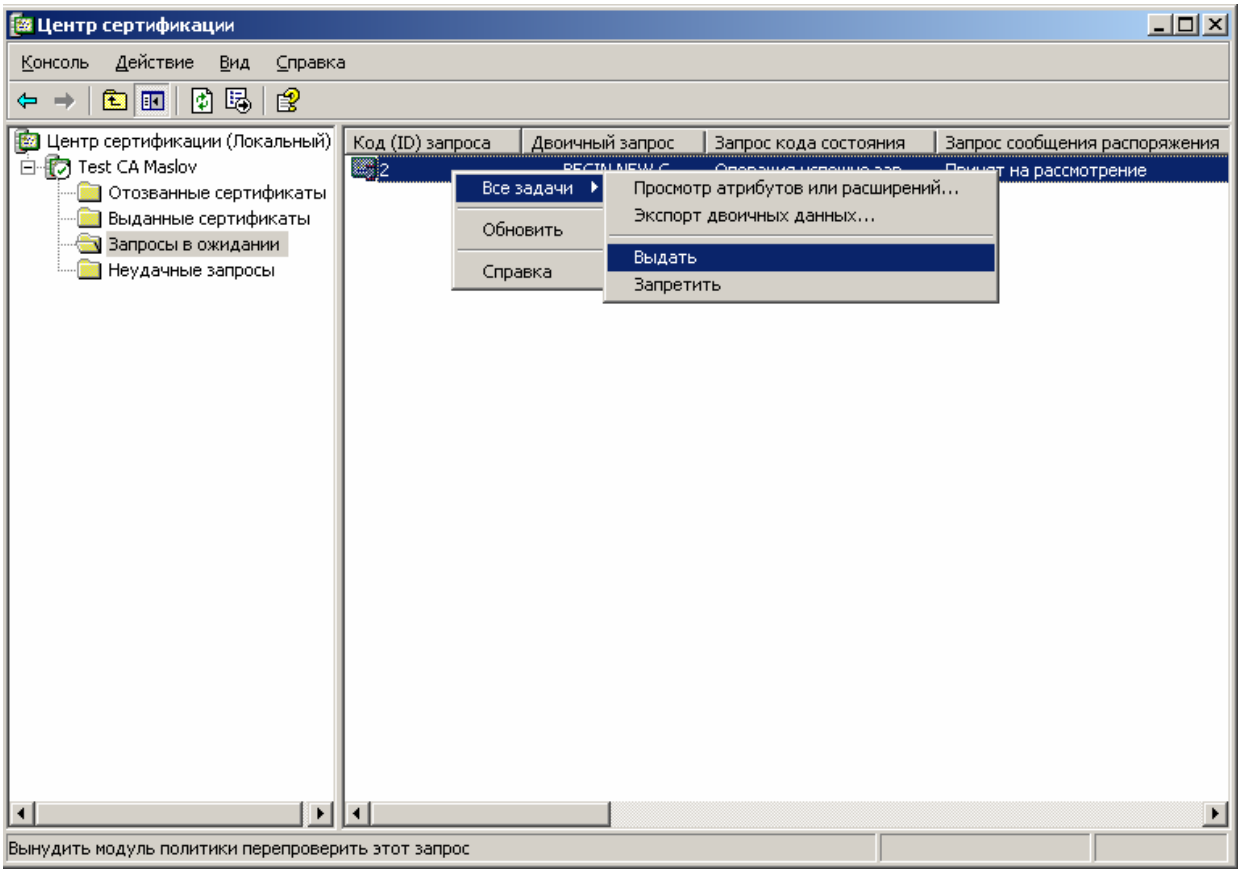
5. В случае если модуль политики службы сертификации не был настроен на автоматический выпуск сертификата по запросу (данный режим включен по умолчанию при установке службы), на экране выводится окно уведомления о необходимости выпуска сертификата по запросу на службе сертификации (см. Рисунок 20)

Рисунок 20. Окно уведомления о необходимости выпуска сертификата по запросу на службе сертификации



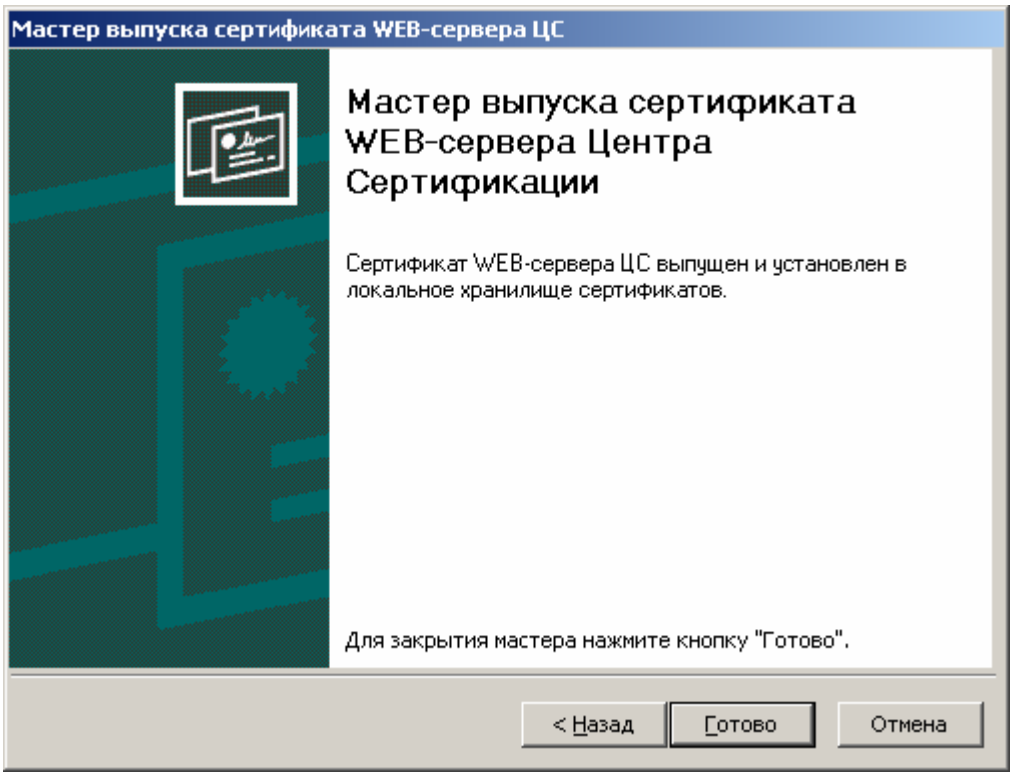
6. Для выпуска сертификата в случае появления данного окна уведомления необходимо открыть оснастку службы сертификации, выбрать список **Запросы в ожидании** и выполнить задачу **Выдать** (см. Рисунок 21).

Рисунок 21. Выдача сертификата по запросу в оснастке службы сертификации



7. Вернитесь в окно выбора способа получения сертификата WEB-сервера ЦС в Мастере (см. Рисунок 19) и нажмите кнопку **Далее**.
8. После генерации ключей, формирования и обработки запроса будет произведен выпуск и установка сертификата Web-сервера Центра сертификации (см. Рисунок 22).

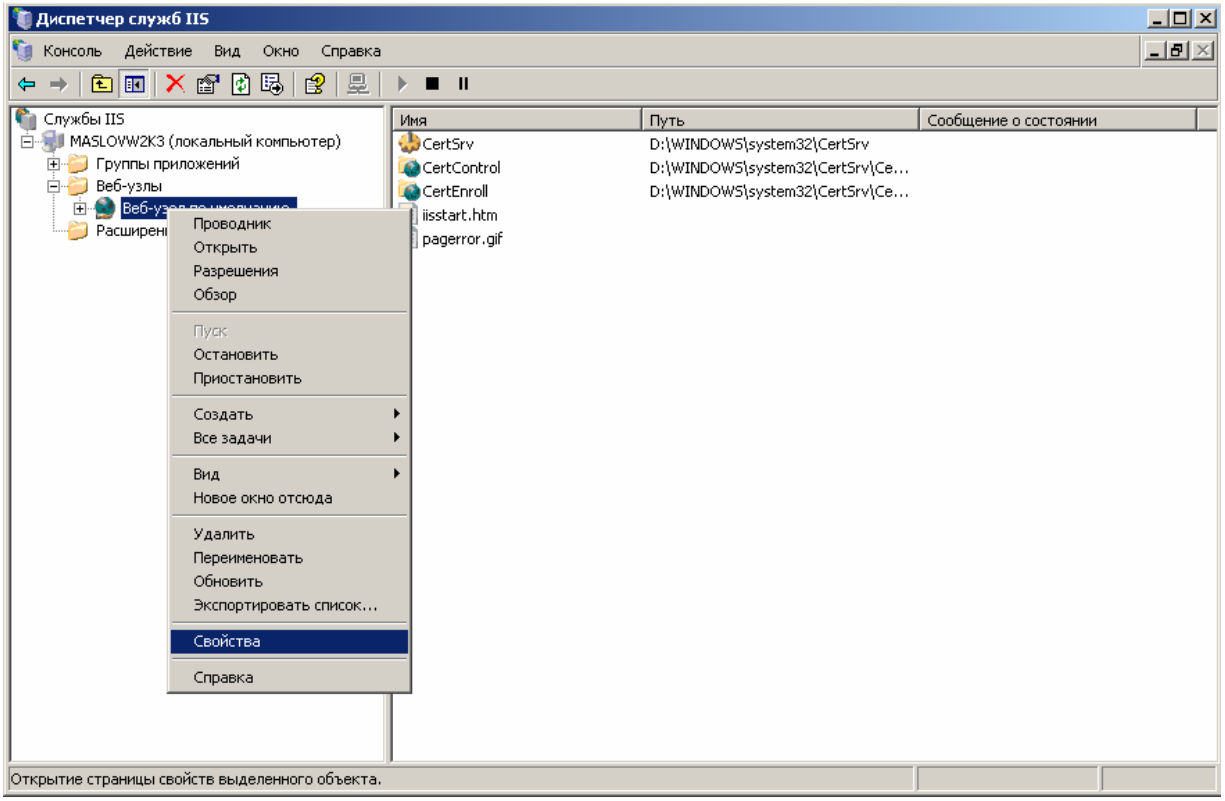
Рисунок 22. Окно завершения работы Мастера выпуска сертификата Web-сервера ЦС



3.7.2. Инсталляция сертификата серверной аутентификации на Web-сервере ЦС

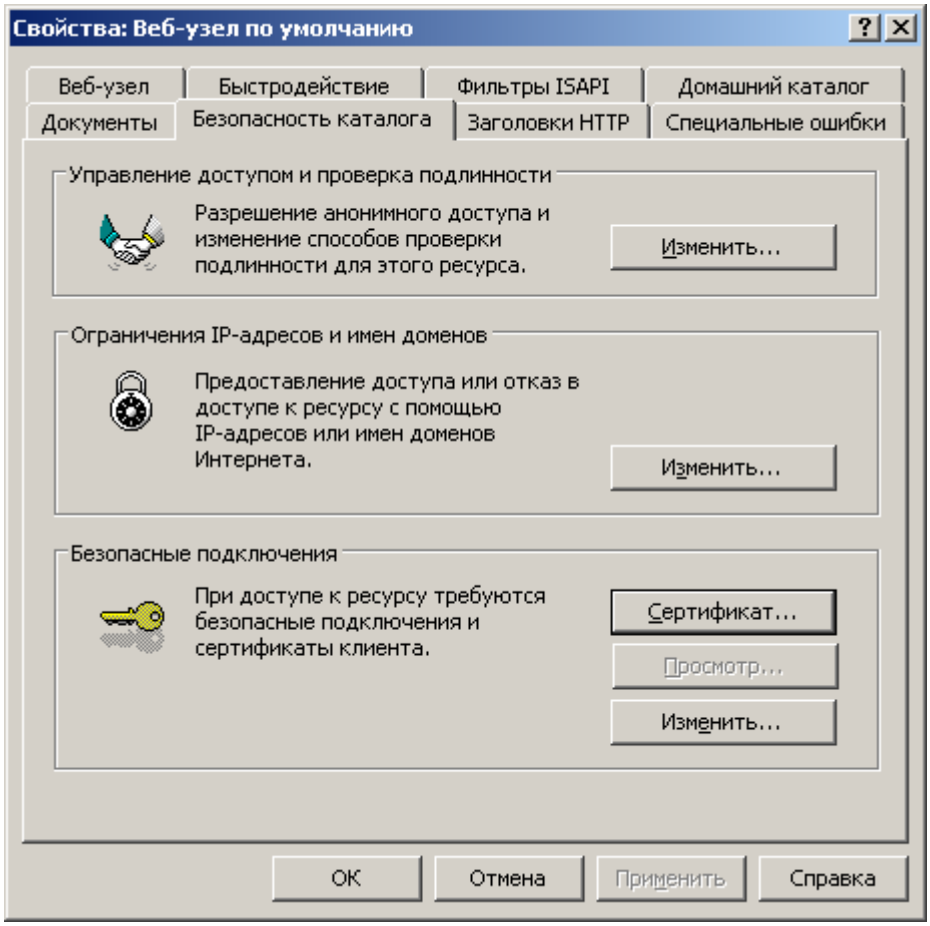
- В разделе "Администрирование" панели программ запустите Диспетчер Служб Интернета;
- Откройте свойства Веб-узла по умолчанию (см. Рисунок 23);

Рисунок 23. Открытие окна свойств Веб-узла по умолчанию MS IIS



- На вкладке «Безопасность каталога», в разделе "Безопасные подключения" выберите сертификат серверной аутентификации WEB-сервера ЦС, который будет использоваться для установления HTTPS соединения (см. Рисунок 24);

Рисунок 24. Вкладка "Безопасность каталога" Web-узла по умолчанию



- В Мастере сертификатов Web-сервера выберите способ "Назначение существующего сертификата";
- Из списка доступных сертификатов выберите сертификат Web-сервера ЦС;
- При установке на платформе Windows Server 2003 будет предложено задать номер SSL порта. Рекомендуется оставить значение по умолчанию (443).
- Нажмите кнопку **Готово** по завершении работы Мастера

3.8. Установка программного обеспечения ЦС

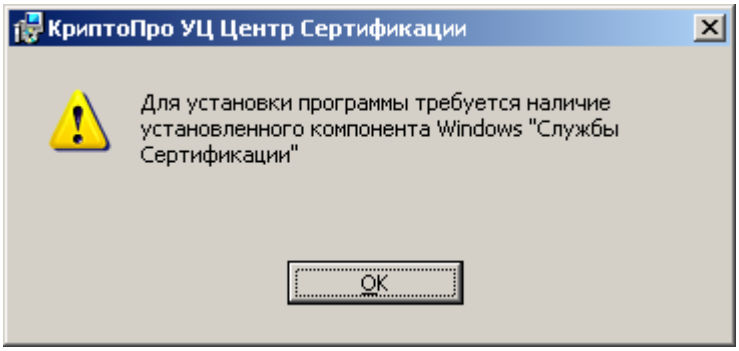
Установка программного обеспечения Центра сертификации осуществляется с CD дистрибутива ПАК «КриптоПро УЦ».

1. Запустите приложение SETUP, расположенное в корневой директории дистрибутива.
2. В начале установки программа осуществит проверку установки необходимых компонентов общесистемного программного обеспечения. К ним относятся:
   a. СКЗИ КриптоПро CSP версии 3.0 и выше.
   b. Служба MS IIS
   c. Служба очередей сообщений
   d. Служба сертификации MS Certificate Authority
   e. Инсталлированный сертификат серверной аутентификации Web-сервера

   Появление диагностических сообщений об отсутствии необходимого компонента говорит о необходимости произвести установку компонента и повторить установку программного обеспечения ЦС.

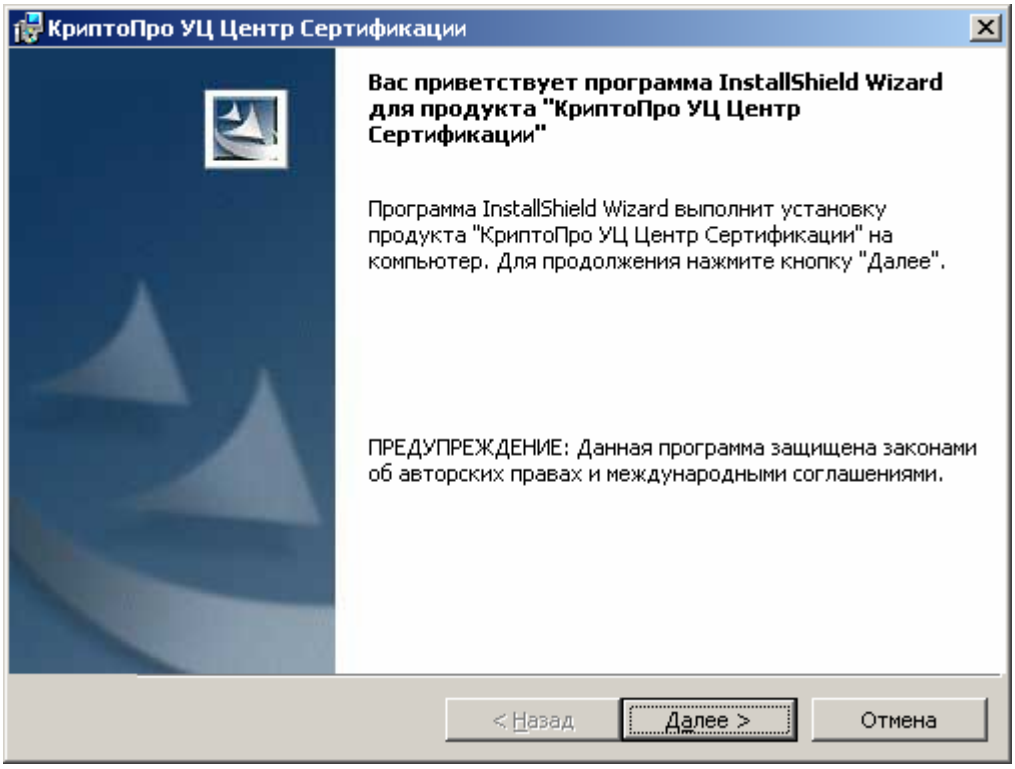
   Пример диагностического сообщения приведен на рисунке ниже.

Рисунок 25. Пример диагностического сообщения ПО дистрибутива ЦС



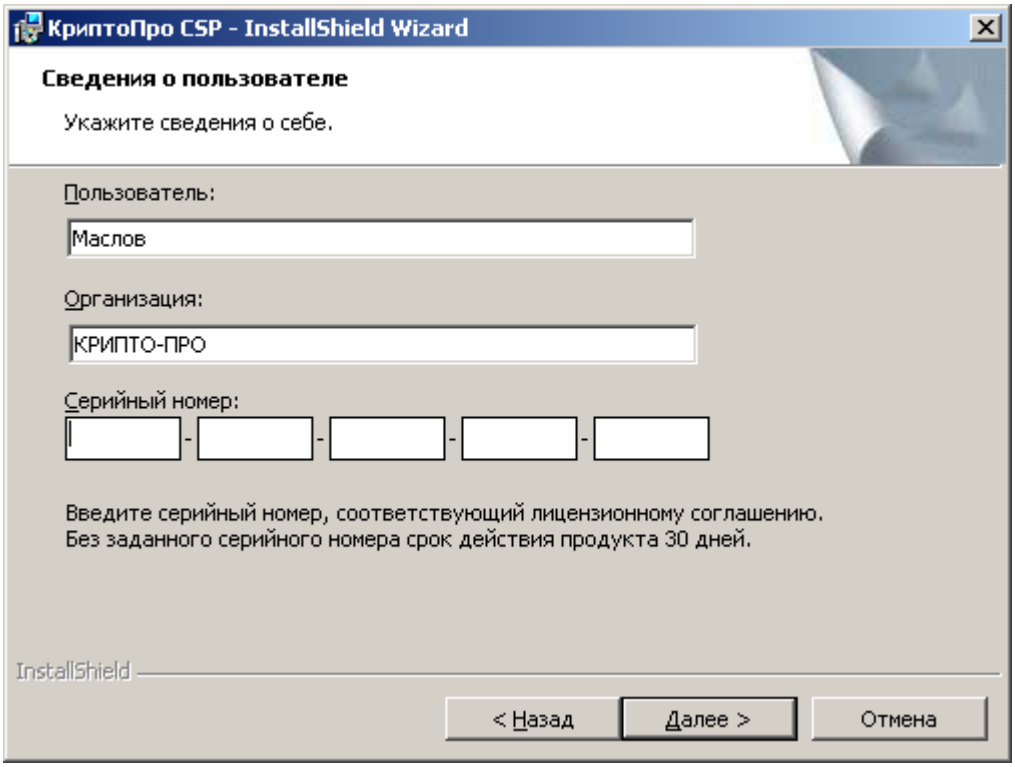
3. После выполнения проверок, в случае положительного результата, программа установки произведет поиск других установленных версий продукта, а также существование учетной записи Центра Сертификации (см. ниже). Если версия ранее установленного на компьютер продукта новее устанавливаемой, то на экране появится сообщение об этом и дальнейшее продолжение установки будет невозможным. Для продолжения нажмите кнопку «Далее», которая станет доступной после окончания описанных действий.

Рисунок 26. Мастер установки ПО Центра сертификации



4. Далее необходимо ввести информацию о пользователе, производящем установку, и серийный номер Лицензии, предоставляющей право на эксплуатацию ЦС. После ввода данных нажмите кнопку **Далее** (см. Рисунок 27). Если все поля для ввода серийного номера оставить пустыми, то программа установки будет использовать серийный номер ознакомительной лицензии, действующей в течение месяца и рассчитанной на 100 пользователей ЦС.

Рисунок 27. Сведения о пользователе ПО ЦС



5. После нажатия кнопки **Далее** программа установки отобразит диалоговое окно (см. Рисунок 28), на котором необходимо выбрать вид установки. Программой установки предлагаются два вида установки: полная и выборочная. Использование вида "выборочная" позволяет сменить папки для установки компонентов (файлов) Центра сертификации. При использовании вида "полная" установка компонентов производится в предопределенные папки:

Компонент	Имя папки по умолчанию	Местоположение папки	Местоположение по умолчанию
Центр Сертификации Крипто-Про УЦ	Crypto Pro\CA	Папка ”Program Files”	C:\Program Files
Удаленный доступ по протоколу SOAP, Виртуальный каталог SOAP доступа на веб-узле 1	CA\Inetpub	Папка ”Crypto Pro” в системной папке ”Application Data” профиля для всех пользователей компьютера	C:\Documents and Settings\All Users\Application Data\Crypto Pro
База данных ЦС	CA\Data		

Рисунок 28. Вид установки ПО ЦС

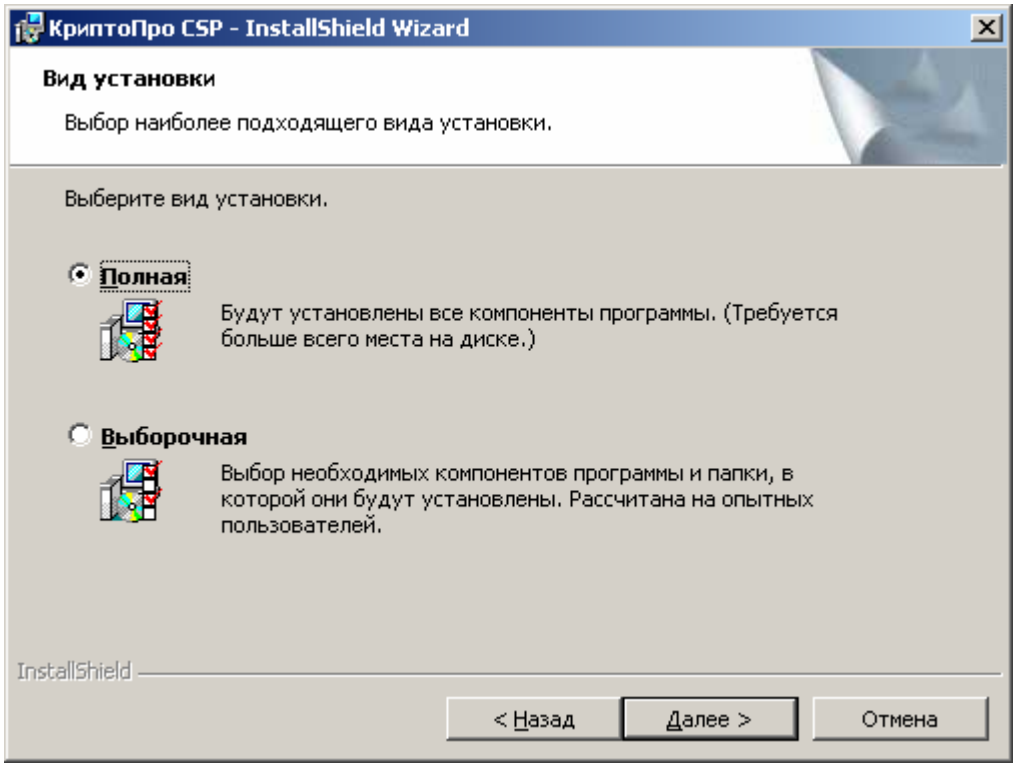
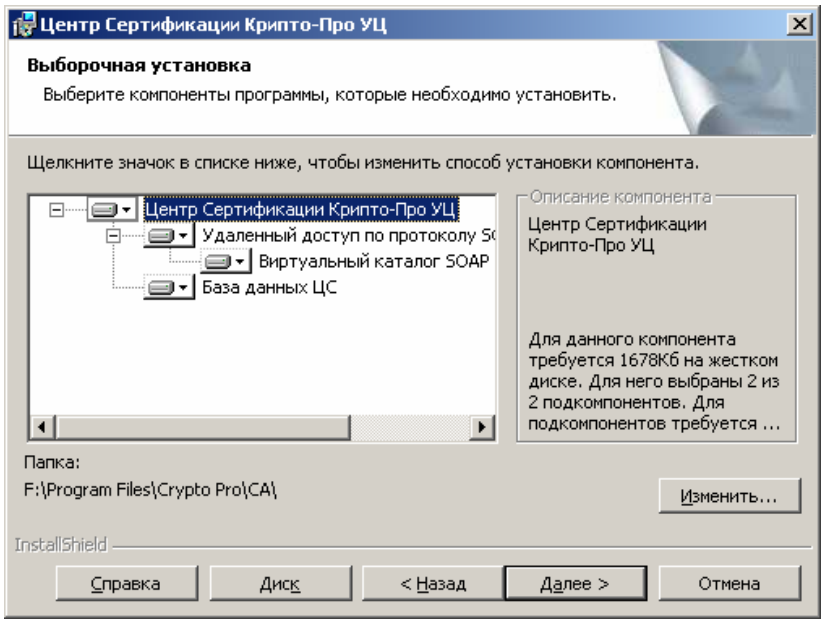


Рисунок 29. Вид установки «Выборочная»



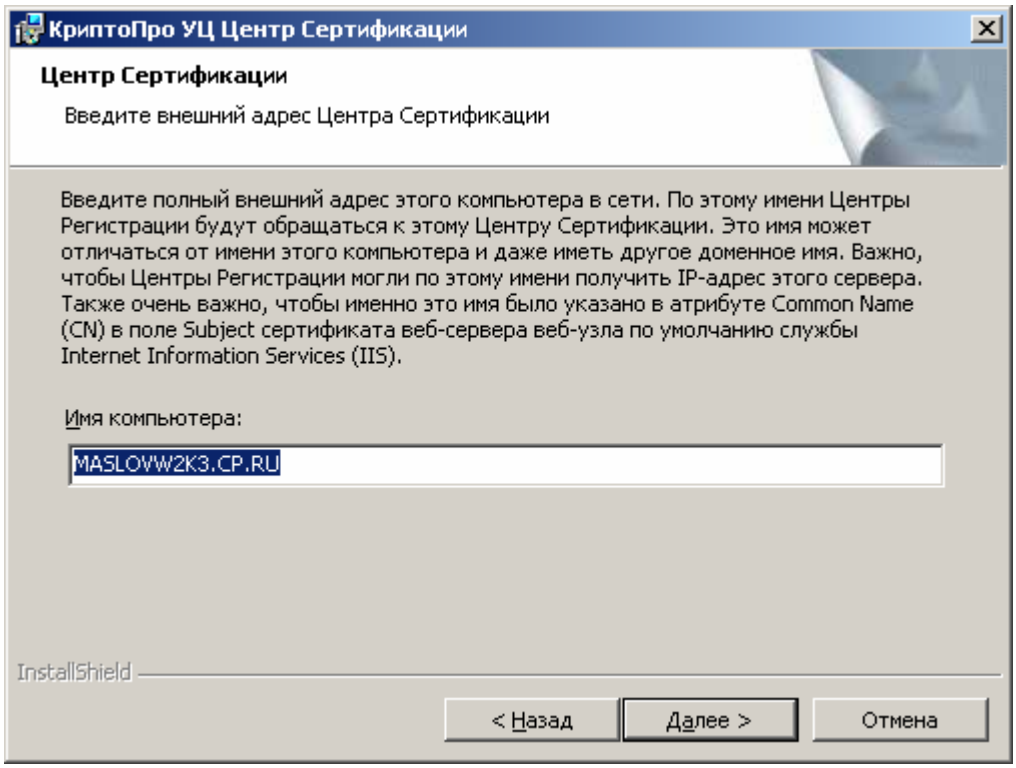
Изменение папок назначения производится следующим образом:

- выберите вид установки **Выборочная** и нажмите кнопку **Далее**
- в появившемся окне (см. Рисунок 28а) выберите компонент, для которого необходимо изменить папку назначения.
- нажмите кнопку **Изменить**, расположенную справа от текстовой строки с именем папки назначения.
- В окне изменения текущей папки назначения выберите нужную папку с использованием элемента окна **Поиск в папке**. В случае если папка не существует, то создайте ее. Для этого нажмите на кнопку с пиктограммой, расположенную в правой части элемента окна **Поиск в папке**.

После выбора папки нажмите кнопку **ОК**. Если необходимо оставить в качестве текущей папки предлагаемую по умолчанию, то нажмите кнопку **Отмена**

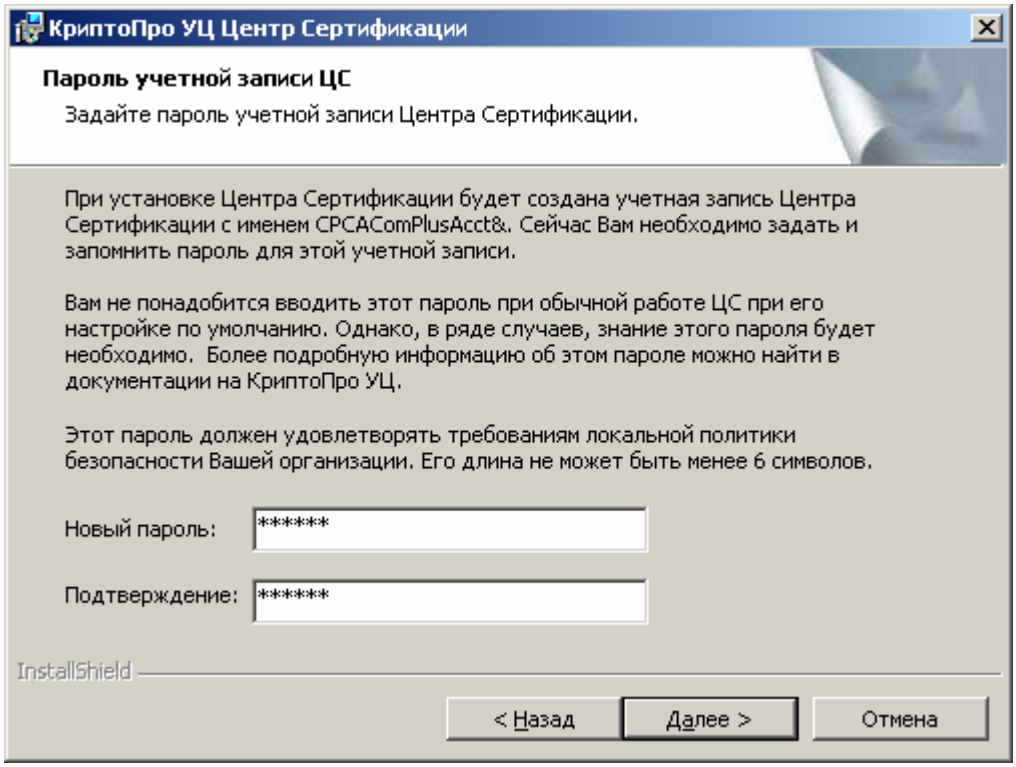
6. После определения вида установки следующим отображается диалоговое окно (см. Рисунок 30), в котором необходимо определить внешний адрес Центра сертификации. По этому адресу ЦС должен быть доступен по протоколу HTTP(S). Данное имя должно обязательно совпадать со значением поля **Имя компьютера ЦС** в сертификате Web-сервера ЦС, изготовленного и использованного ранее (см. Рисунок 17). После ввода данных нажмите кнопку **Далее**.

Рисунок 30. Внешний адрес Центра сертификации



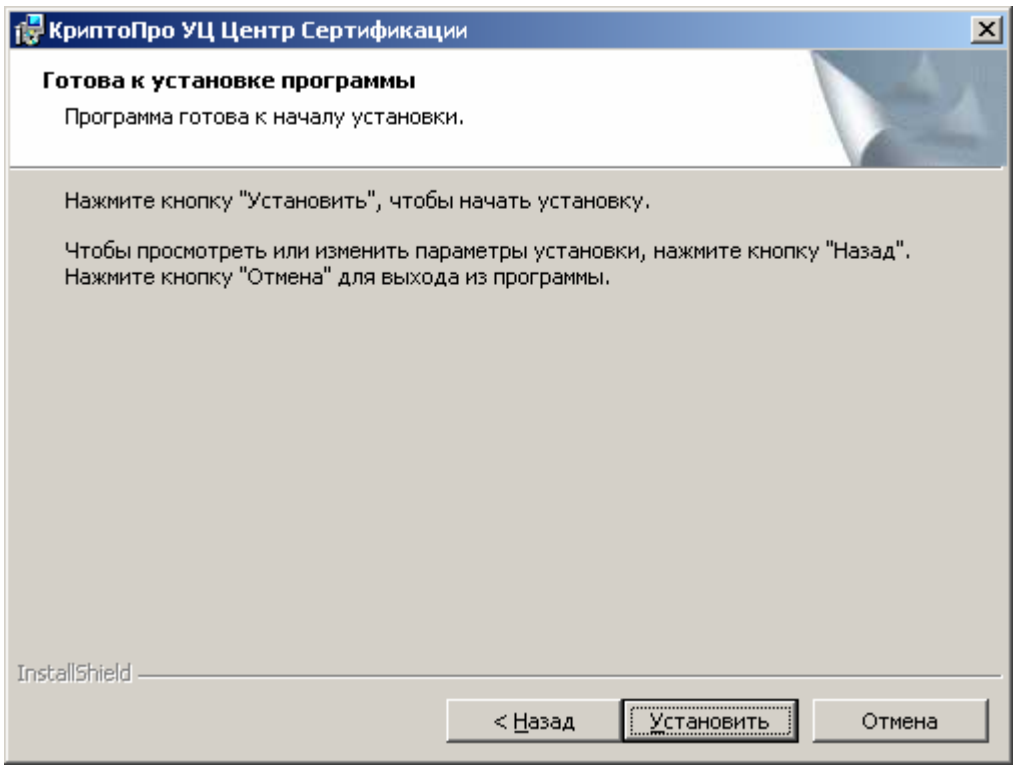
7. В следующем окне Мастера необходимо задать пароль учетной записи Центра Сертификации, на работу от имени которой будут настроены COM+ приложения ЦС, а также задачи планировщика Windows (см. Рисунок 31). Пароль задается при регистрации этой учетной записи. Если учетная запись уже зарегистрирована, то данное диалоговое окно не отображается, а отображается окно для ввода пароля зарегистрированной учетной записи.

Рисунок 31. Пароль учетной записи Центра Сертификации



8. После определения всех необходимых параметров, выполненных на предыдущих шагах, программа установки выведет диалоговое окно (см. Рисунок 32) подтверждения продолжения установки. При необходимости можно вернуться на переопределение параметров установки. Для этого надо нажать кнопку **Назад**. Для подтверждения установки нажмите кнопку **Установить**.

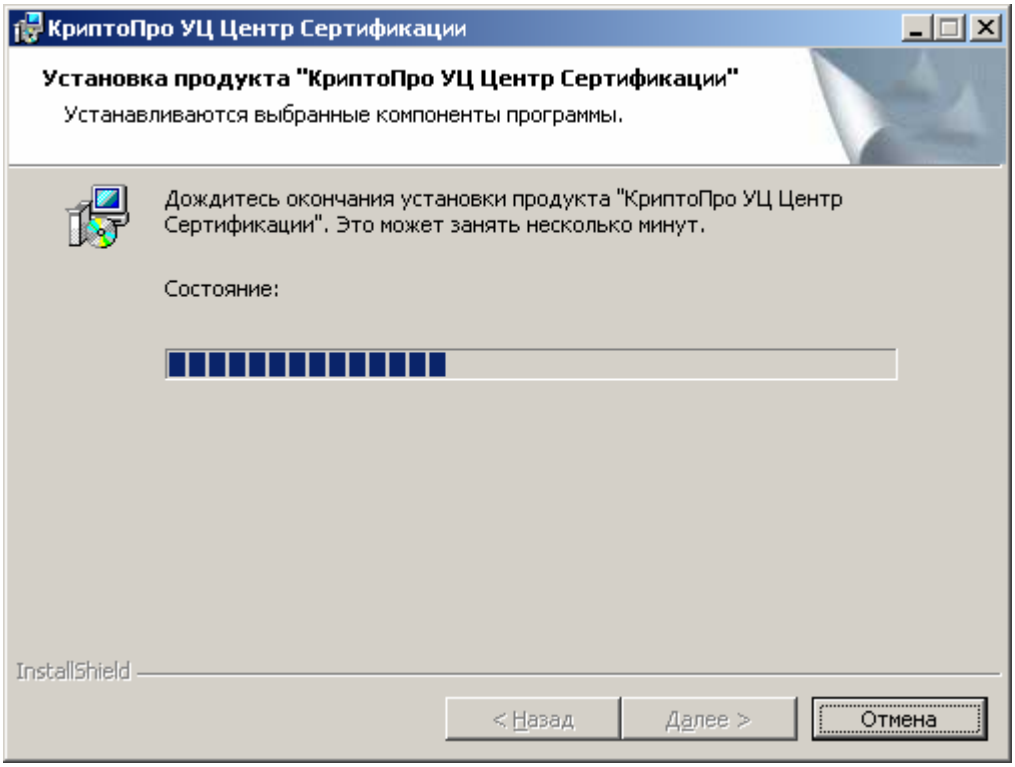
Рисунок 32. Окно подтверждения установки ПО ЦС



9. После нажатия кнопки «Установить», программа производит установку программного обеспечения

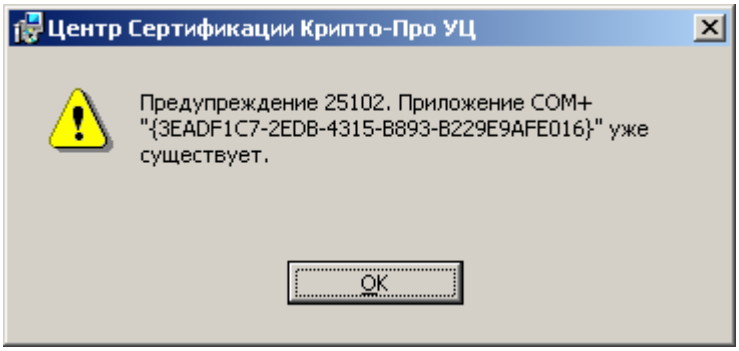
Выполнение действий сопровождается комментариями программы установки, выводимыми в окне состояния. Пример окна смотрите на рисунке ниже.

Рисунок 33. Окно состояния процесса установки ПО ЦС



10. Если на сервере ЦС ранее были установлены предыдущие версии «КриптоПро УЦ» то возможно появление окон предупреждения о наличии в операционной системе зарегистрированных приложений (см. Рисунок 34). В этом случае дополнительных действий оператора не требуется. Для закрытия информационного окна необходимо нажать кнопку **ОК**.

Рисунок 34 . Информационное окно предупреждения мастера установки ЦС



11. После завершения установки программного обеспечения ЦС программа установки выведет диалоговое окно с соответствующим сообщением. Для завершения установки нажмите кнопку **Готово**.

12. Если во время установки в систему были внесены изменения, требующие перезагрузки компьютера, то на экране появится окно с предложением произвести перезагрузку. Для того, чтобы сразу же перезагрузить компьютер, нажмите кнопку **Да**, а для того, чтобы перезагрузить компьютер позже вручную, нажмите **Нет**.

4. Установка Центра Регистрации

Данный раздел настоящего Руководства определяет последовательность и порядок действий при установке программного обеспечения Центра Регистрации ПАК «КриптоПро УЦ» в режиме «с нуля». Данный режим означает, что на сервере была произведена установка операционной системы на отформатированный диск.

Последовательность и порядок действий при установке программного обеспечения Центра Регистрации для обновления ранее установленной версии (релиза) ЦР описываются в документе «Особенности версии» (файл ReleaseNotes.pdf), входящий в состав дистрибутива ПО Центра Регистрации.

4.1. Последовательность установки Центра Регистрации

Установка и конфигурация программного обеспечения Центра Регистрации из состава программного комплекса УЦ производится в следующей последовательности:

1. Установка СКЗИ КриптоПро CSP и КриптоПро TLS
2. Установка служб Microsoft Internet Information Services и службы очереди сообщений
3. Установка приложений «Утилиты Центра регистрации»
4. Выпуск и инсталляция сертификата серверной аутентификации Web-сервера ЦР
5. Установка программного обеспечения ЦР
6. Выпуск и инсталляция клиентского сертификата Центра Регистрации
7. Настройка и тестирование соединения с Центром Сертификации

4.2. Установка СКЗИ КриптоПро CSP и КриптоПро TLS

На сервере Центра Регистрации устанавливается СКЗИ «КриптоПро CSP» версии 3.0 (исполнение 6 для класса защиты КС2).

Установка СКЗИ «КриптоПро CSP» осуществляется в соответствии с эксплуатационной документацией. Модуль «КриптоПро TLS» входит в состав дистрибутива и не требует отдельной установки.

После установки программного обеспечения СКЗИ «КриптоПро CSP» и «КриптоПро TLS» необходимо активировать лицензию на продукт из набора лицензий поставки ПАК «КриптоПро УЦ» и включить режим **кэширования** (вкладка **Безопасность** окна свойств КриптоПро CSP).

4.3. Установка служб Microsoft Internet Information Services и службы очередей сообщений

Установка служб осуществляется с использованием Мастера компонентов Windows (см. Рисунок 2)

В составе служб IIS рекомендуется оставить следующий набор служб:

- диспетчер служб IIS

- общие файлы

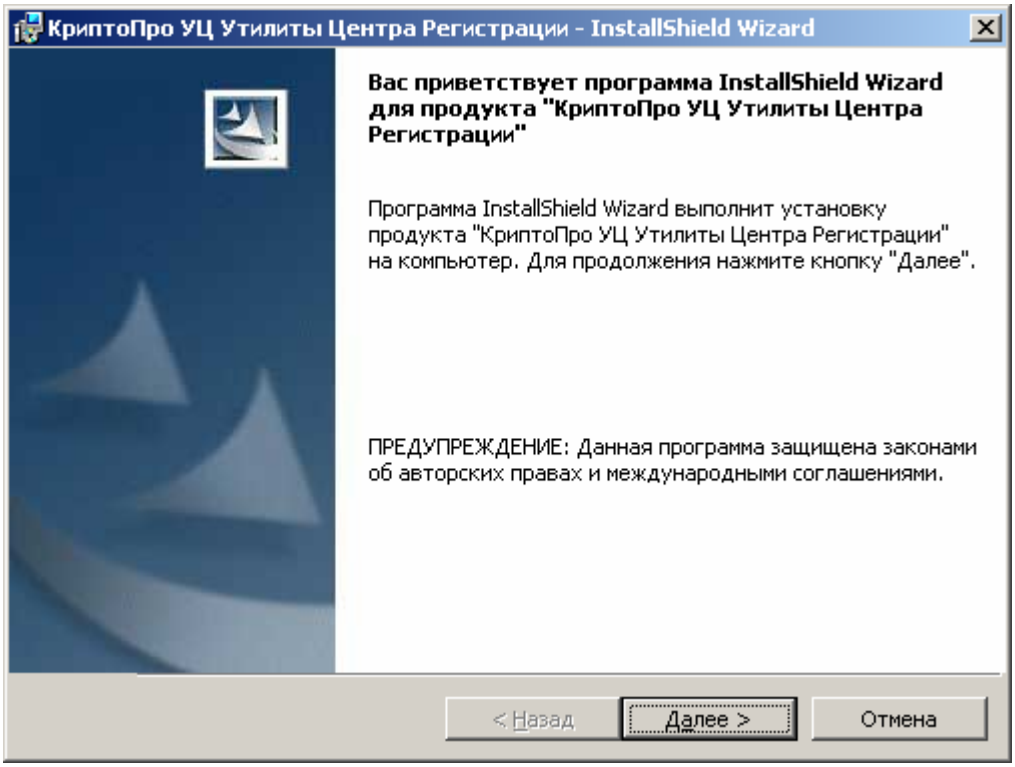
- служба WWW

4.4. Установка приложений «Утилиты Центра Регистрации»

Для установки приложений Мастеров запустите приложение **SETUP.EXE**.

Инсталляция утилит Центра регистрации производится с помощью Мастера установки (см. Рисунок 35).

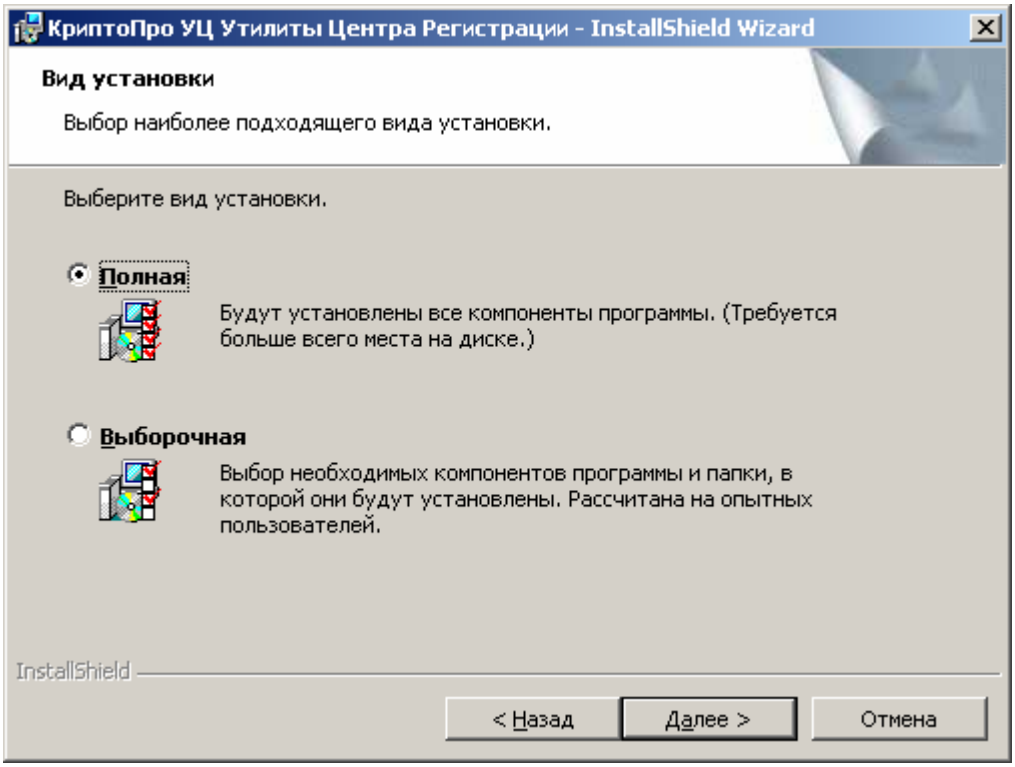
Рисунок 35. Окно Мастера установки утилит Центра Регистрации



На все последующие диалоговые сообщения Мастера установки отвечайте выбором значений по умолчанию (кнопка **Далее**).

При выборе вида установки (Рисунок 36) следует выбрать **Полная**.

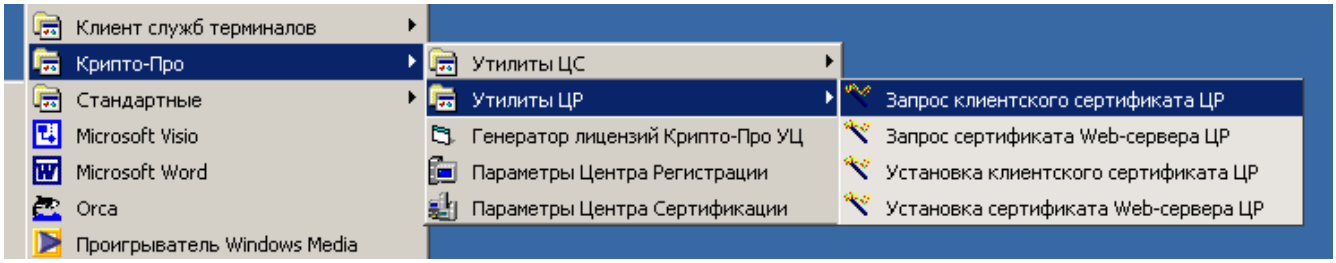
Рисунок 36. Выбор вида установки Утилит Центра Регистрации



На все последующие диалоговые сообщения Мастера установки отвечайте выбором значений по умолчанию (кнопка **Далее**).

После установки, утилиты Центра регистрации (приложения Мастеров) доступны через группу **Крипто-Про** (см. Рисунок 37).

Рисунок 37. Группа "Крипто-Про" меню "Программы"



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

Перед установкой программного обеспечения Центра регистрации необходимо произвести процедуры выпуска, установки и инсталляции на MS IIS сертификата серверной аутентификации Web-сервера Центра регистрации.

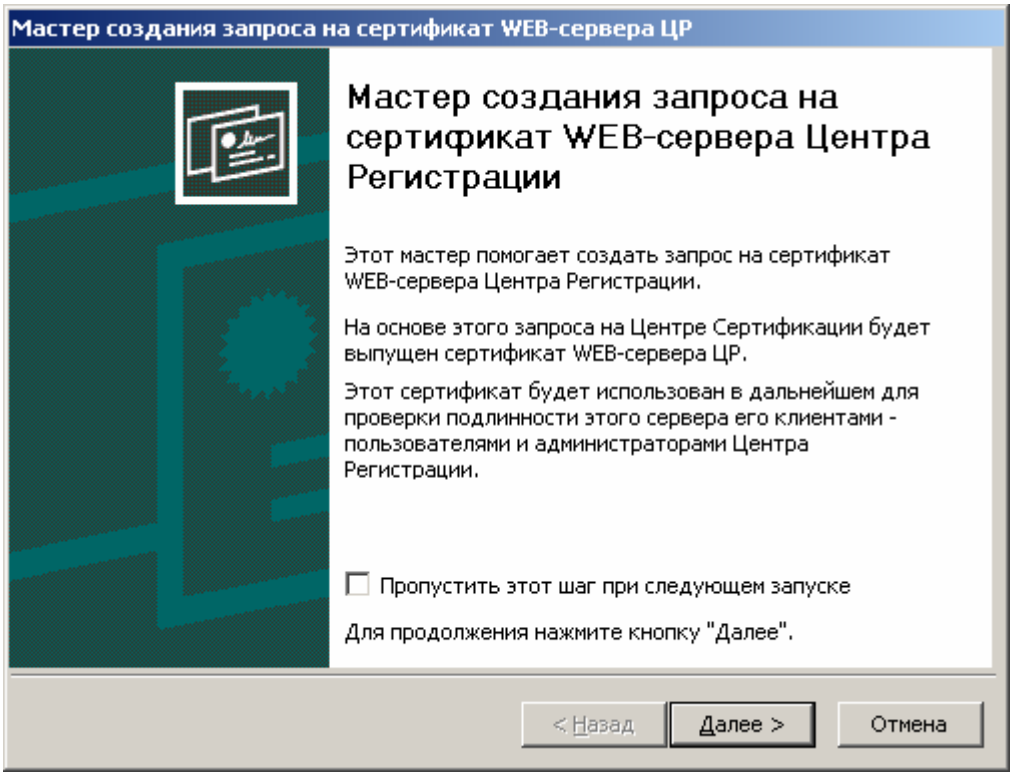
Для этого выполните действия в следующей последовательности

4.5.1. Выпуск сертификата WEB-сервера ЦР

Для обеспечения взаимодействия по HTTPS соединению необходимо сформировать ключи и выпустить сертификат серверной аутентификации WEB-сервера ЦР. Для этого:

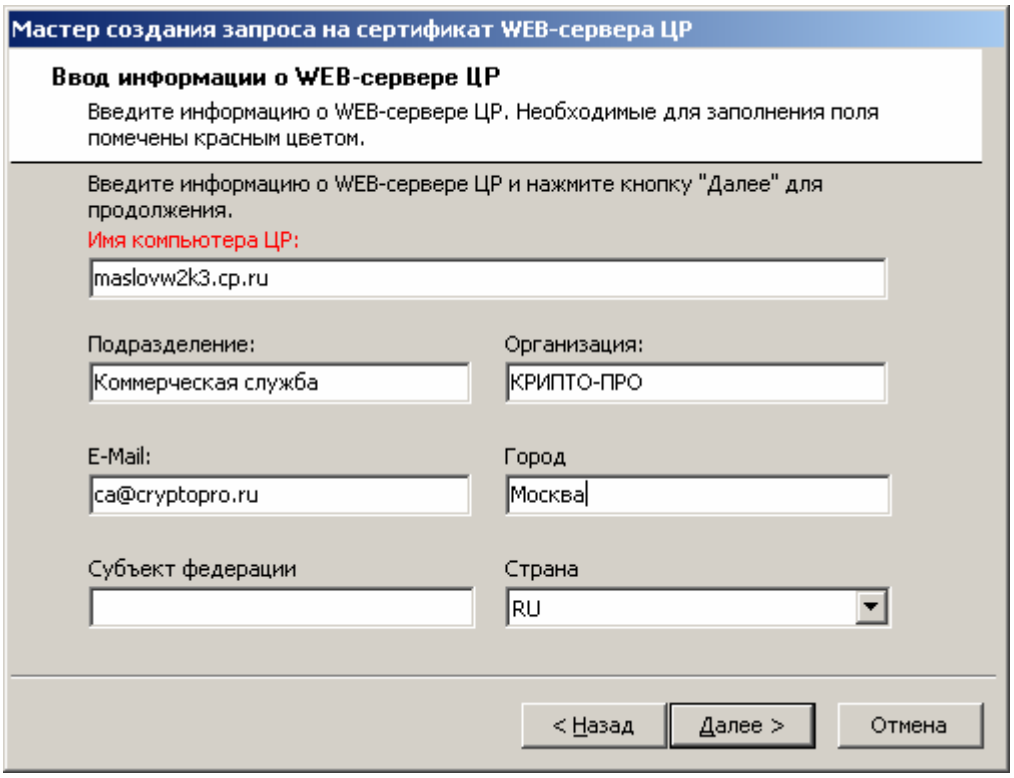
1. Запустите Мастера создания запроса на сертификат WEB-сервера ЦР из группы **Крипто-Про** (см. Рисунок 38)

Рисунок 38. Окно Мастера создания запроса на сертификат WEB-сервера ЦР



2. Введите информацию о Web-сервере ЦР (см. Рисунок 39). В разделе **Имя компьютера ЦР** – доменное имя WEB-сервера (например: **lord2k.cp.ru**).
3. Необходимо, чтобы имя в данном разделе совпадало с доменным именем WEB-сервера Центра Регистрации

Рисунок 39. Окно ввода информации о Web-сервере ЦР Мастера создания запроса на сертификат

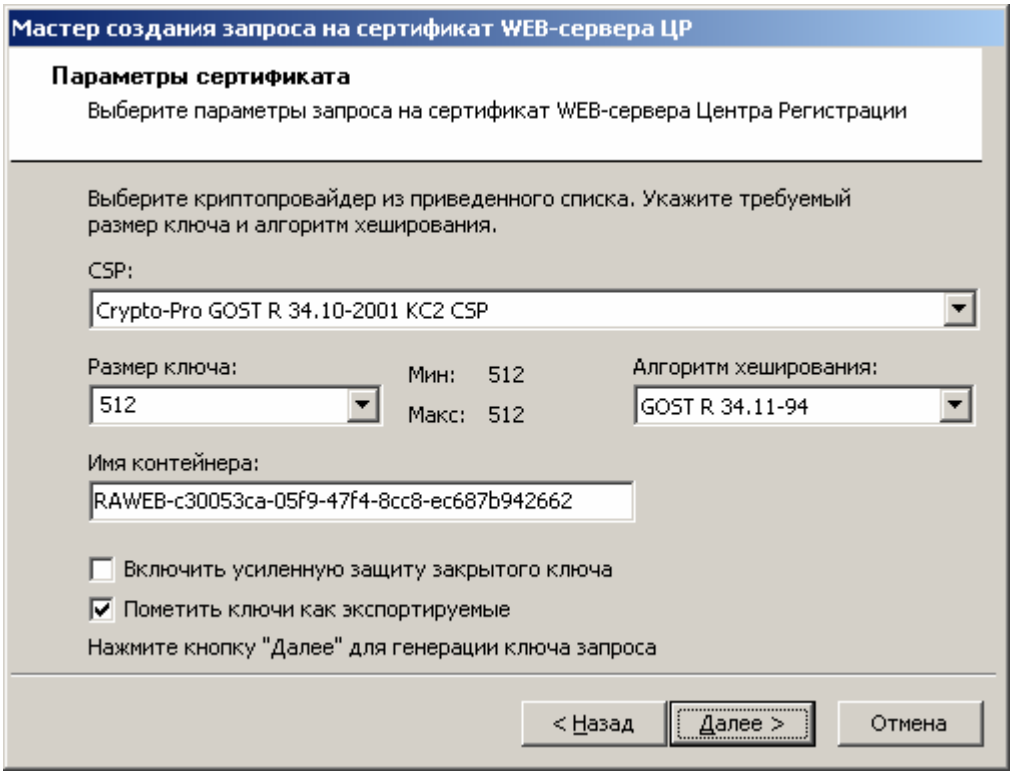


4. В следующем окне необходимо определить используемый криптопровайдер (CSP), размер ключа и алгоритм хеширования (см. Рисунок 40).

Не рекомендуется включать усиленную защиту закрытого ключа т.к. это приведет к появлению дополнительных сообщений в процессе работы Центра Сертификации и возможной неработоспособности комплекса в целом.

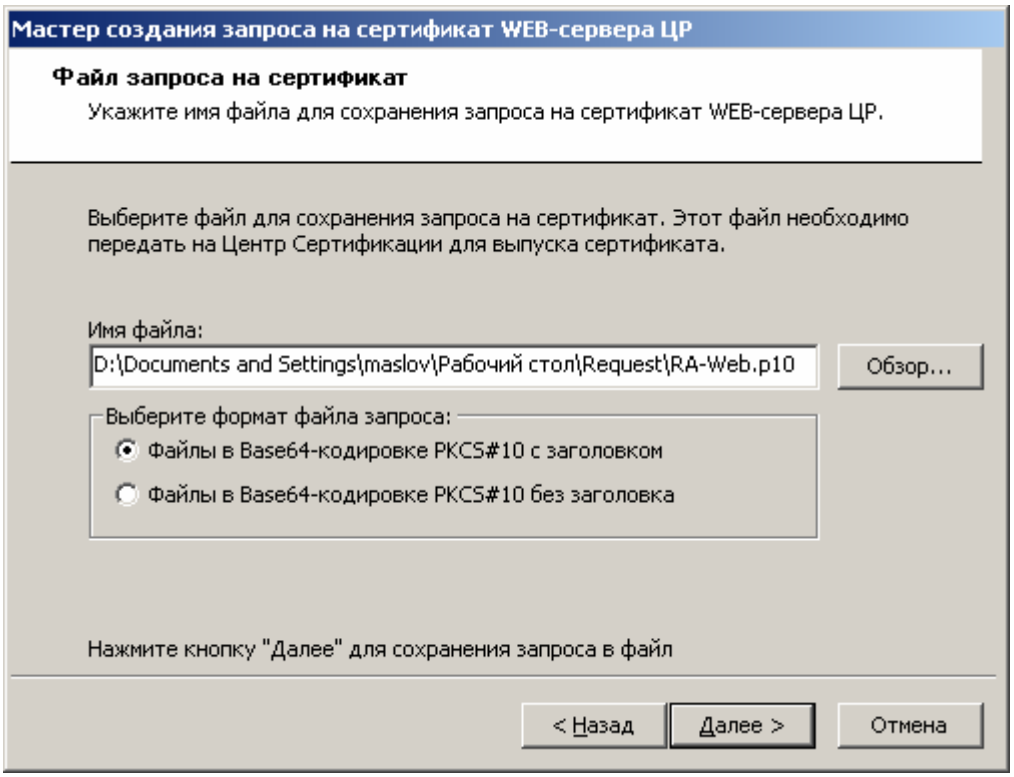
В данном окне Мастера возможно задать имя ключевого контейнера или оставить имя установленное по умолчанию.

Рисунок 40. Окно выбора CSP в Мастере создания запроса на сертификат



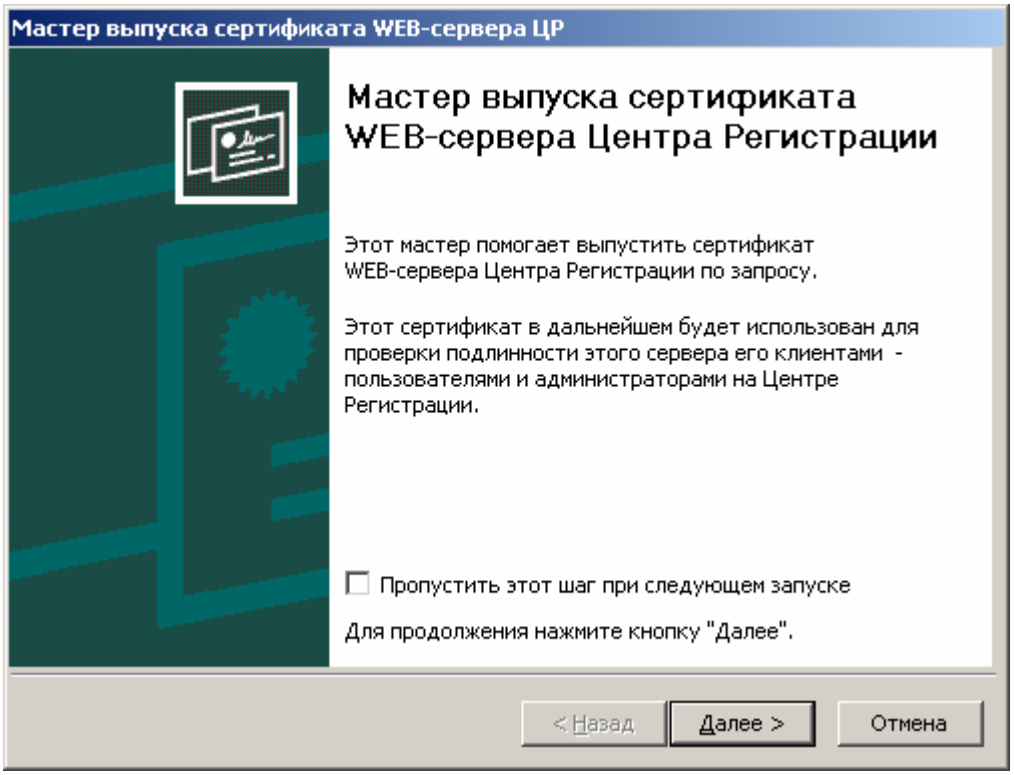
5. После генерации ключей в следующем окне введите имя и размещение файла, в который будет сформирован запрос на сертификат Web-сервера Центра регистрации (см. Рисунок 41).

Рисунок 41. Окно определения файла запроса в Мастере создания запроса на сертификат



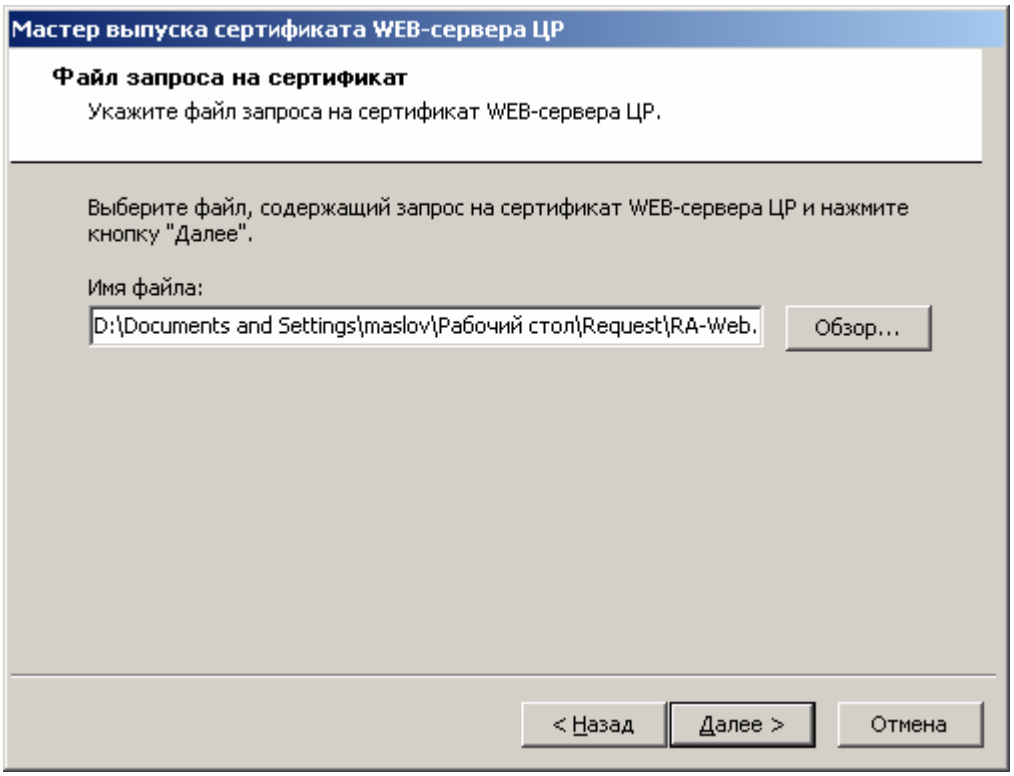
6. В завершающем окне Мастера создания запроса на сертификат кнопку **Готово**.
7. Сформированный файл запроса необходимо доставить на Центр Сертификации ПАК «КриптоПро УЦ» и выпустить там сертификат с использованием Мастера «Обработка запроса сертификата Web-сервера ЦР» из состава «Утилиты ЦС» (см. Рисунок 42)

Рисунок 42. Стартовое окно Мастера выпуска сертификата Web-сервера ЦР



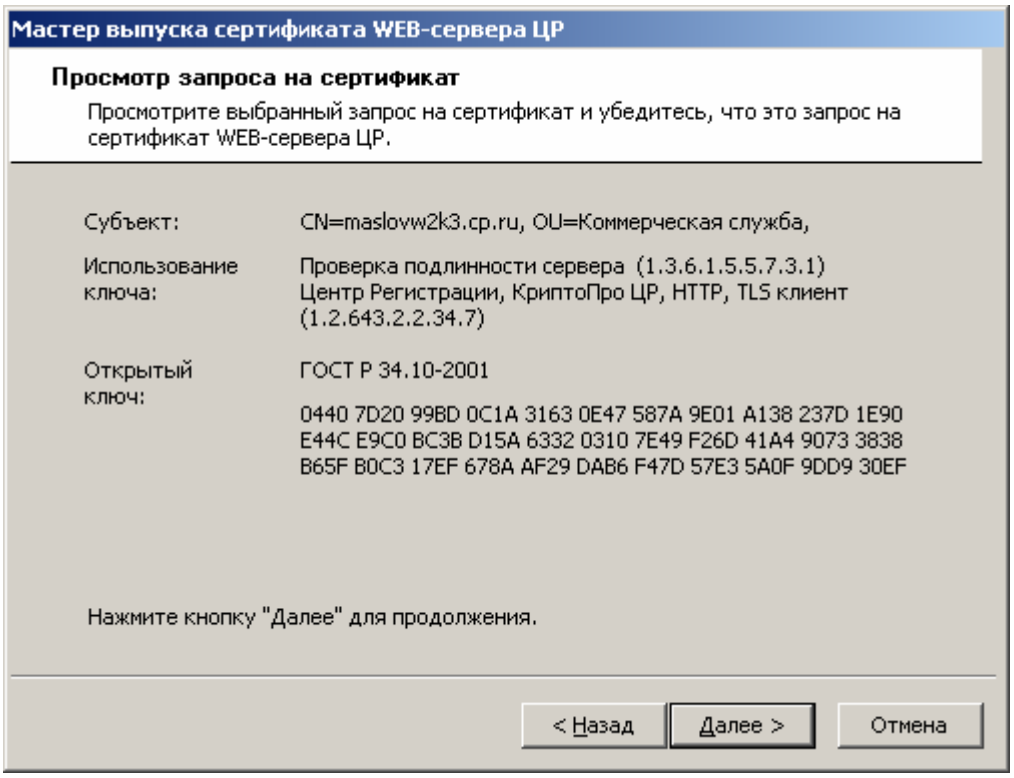
8. В окне выбора файла запроса (см. Рисунок 43) Мастера выпуска сертификата Web-сервера ЦР

Рисунок 43. Окно выбора файла запроса Мастера выпуска сертификата Web-сервера ЦР



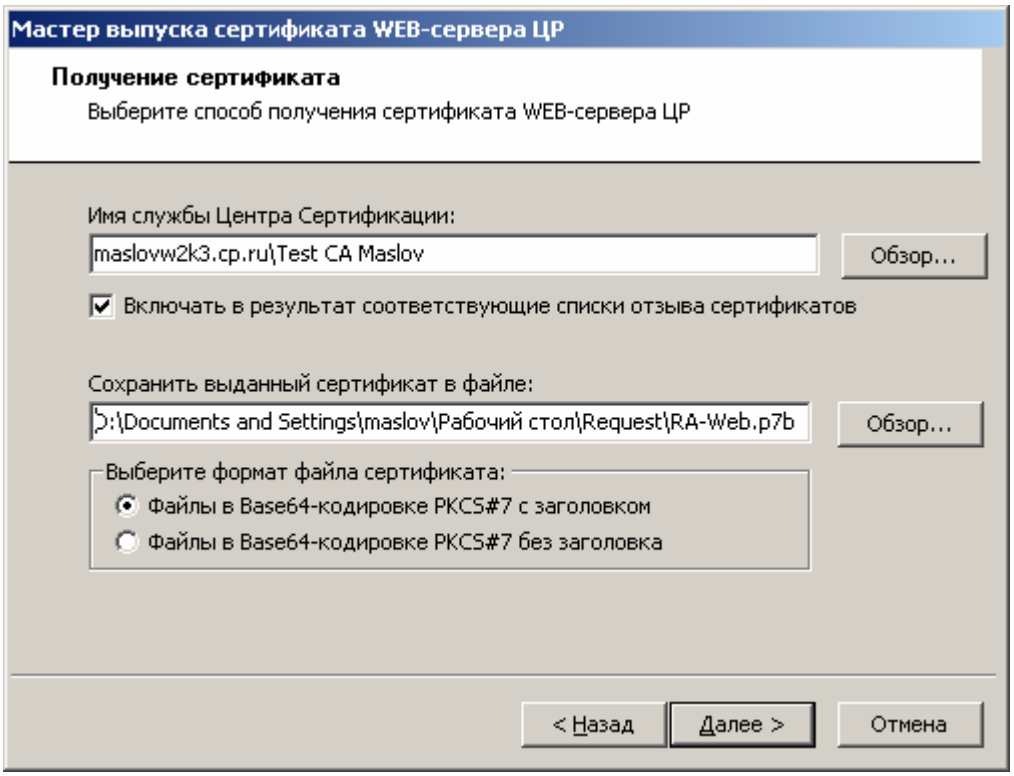
9. В окне просмотра содержимого запроса отображается информация из выбранного файла. Убедитесь в корректности информации, содержащейся в запросе и нажмите кнопку **Далее**.

Рисунок 44. Окно просмотра запроса Мастера выпуска сертификата Web-сервера ЦР



10. В окне получения сертификата (см. Рисунок 45) с помощью кнопки **Обзор** выберите путь и имя файла, куда будет сохранен сертификат. Файл будет содержать цепочку сертификатов, включающую как сам сертификат Веб-сервера ЦР, так и всю цепочку издателей сертификата. Рекомендуется включать в результат соответствующие списки отзыва сертификатов.

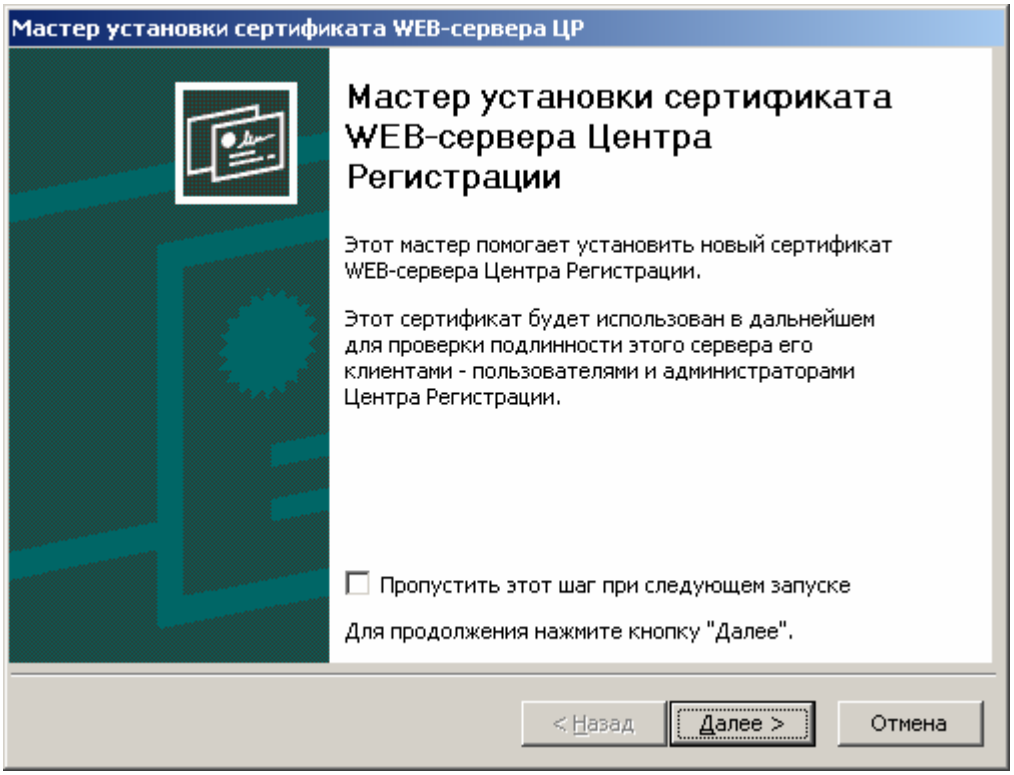
Рисунок 45. Окно получения сертификата Мастера выпуска сертификата Web-сервера ЦР



11. В завершающем окне Мастера выпуска сертификата Web-сервера ЦР нажмите кнопку **Готово**.

12. Выпущенный сертификат, полученный из Центра Сертификации в виде файла и содержащий цепочку сертификатов, необходимо установить на Центре Регистрации с использованием Мастера установки сертификата WEB-сервера ЦР из группы **Крипто-Про** (см. Рисунок 46).

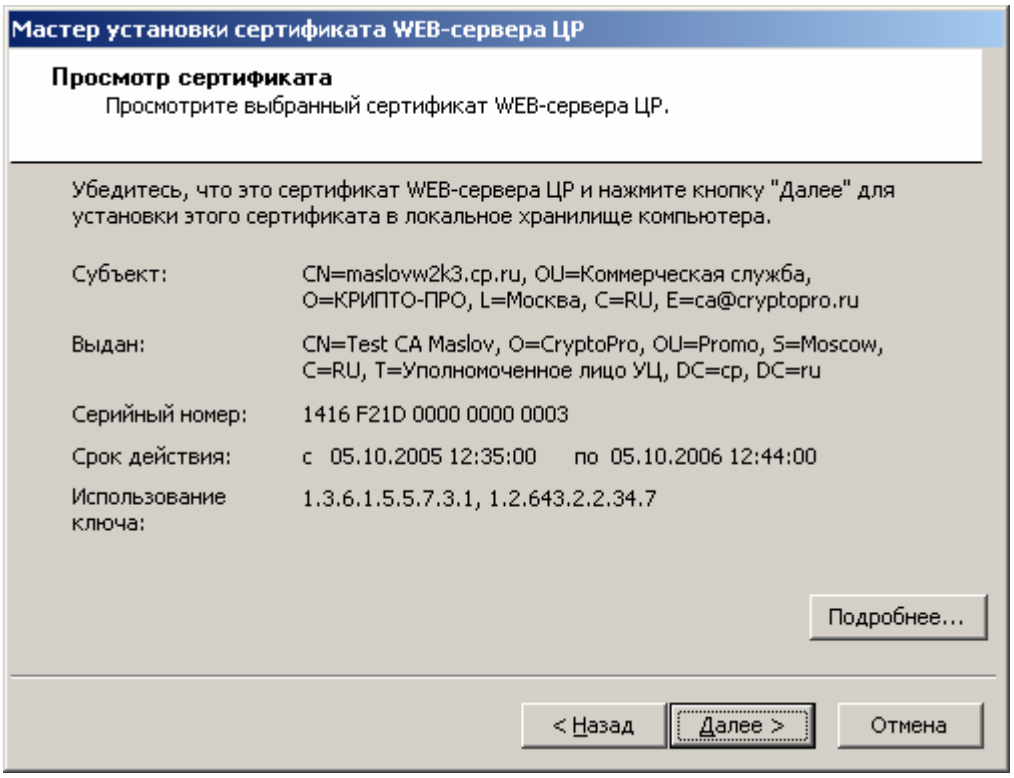
Рисунок 46. Окно Мастера установки сертификата WEB-сервера ЦР



13. В окне выбора файла с сертификатом Web-сервера ЦР выберите файл с цепочкой сертификатов (установив тип расширения файлов *.p7b).

14. В диалоговом окне Мастера убедитесь в том, что выбранный файл содержит необходимый сертификат и нажмите кнопку **Далее** (см. Рисунок 47).

Рисунок 47. Окно отображения информации о сертификате в Мастере установки сертификата WEB-сервера ЦР



15. По окончании установки нажмите кнопку **Готово**.

4.5.2. Инсталляция сертификата серверной аутентификации на Web-сервере ЦР

После выпуска сертификата серверной аутентификации Web-сервера Центра Регистрации и установки на Центре Регистрации необходимо подключить его в MS IIS сервера ЦР.

Для этого выполните следующие действия:

- В разделе «Администрирование» панели программ запустите Диспетчер Служб Интернета;
- Откройте свойства Web-узла по умолчанию (см. Рисунок 23);
- На вкладке «Безопасность каталога» (см. Рисунок 24), в разделе «Безопасные подключения» выберите сертификат серверной аутентификации WEB-сервера ЦР, который будет использоваться для установления HTTPS соединения (в Мастере сертификатов Web-сервера выберите способ «Заменить текущий сертификат»);

4.6. Установка программного обеспечения ЦР

Установка программного обеспечения Центра Регистрации ПАК «КриптоПро УЦ» осуществляется с CD дистрибутива.

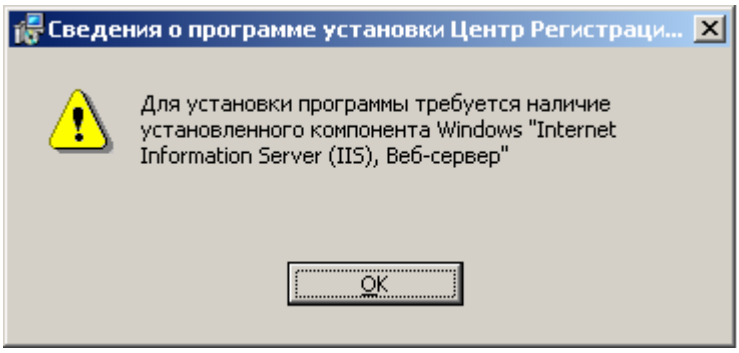
13. Запустите приложение SETUP.EXE, расположенное в корневой директории дистрибутива.
14. Установка осуществляется с использованием программы “InstallShield Wizard для Центра регистрации КриптоПро УЦ”. В начале установки программа осуществит проверку установки необходимых компонентов общесистемного программного обеспечения. К ним относятся:
    a. СКЗИ КриптоПро CSP
    b. Служба MS IIS
    c. Служба очередей сообщений

d. Инсталлированный сертификат серверной аутентификации Web-сервера

Появление диагностических сообщений об отсутствии необходимо компонента говорит о необходимости произвести установку компонента и повторить установку программного обеспечения ЦР.

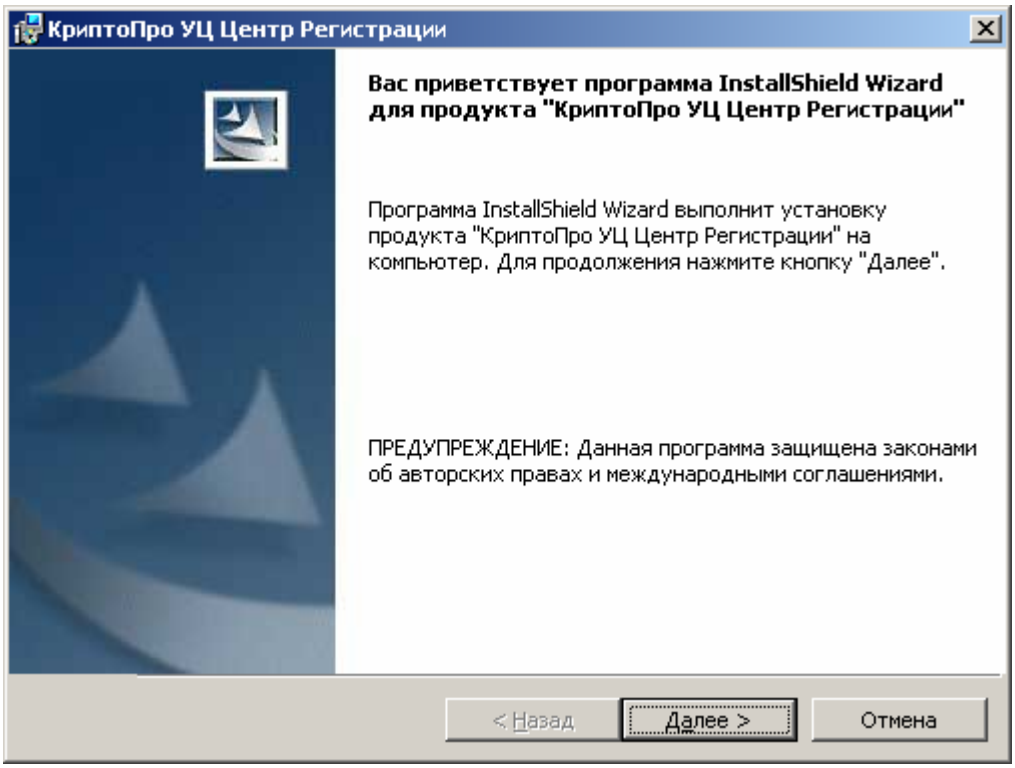
Пример диагностического сообщения приведен на рисунке 48.

Рисунок 48. Пример диагностического сообщения программы установки ЦР



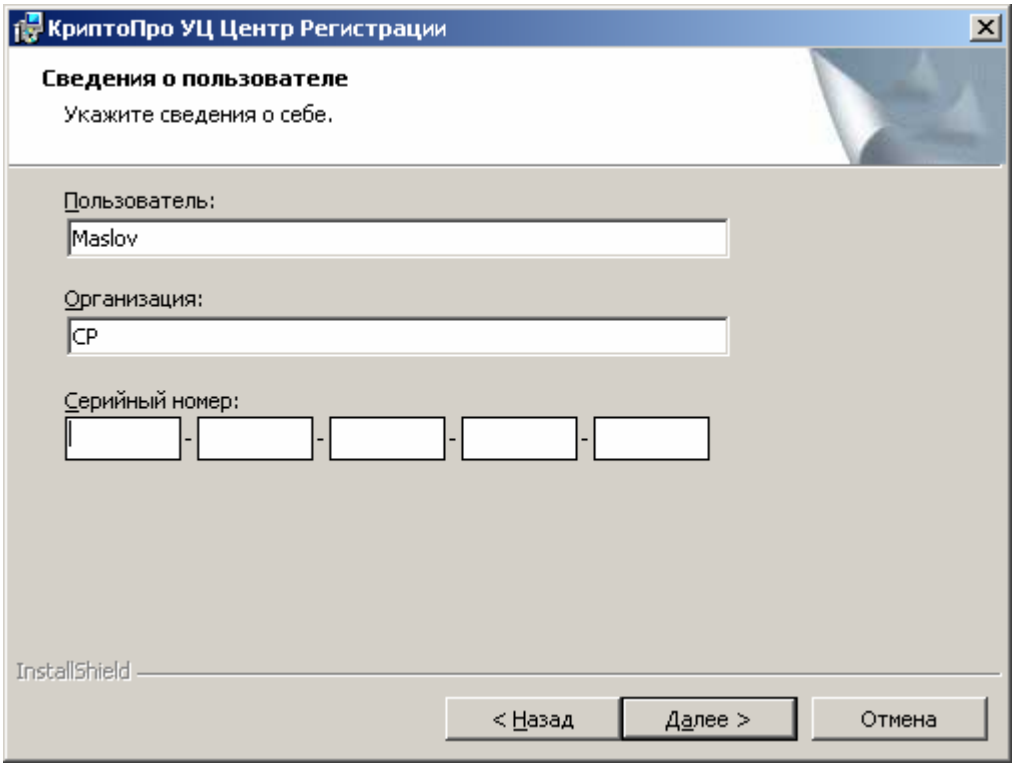
15. После выполнения проверок, в случае положительного результата, программа установки произведет поиск других установленных версий продукта, а также существование учетной записи Центра Регистрации (см. ниже). Если версия ранее установленного на компьютер продукта новее устанавливаемой, то на экране появится сообщение об этом и дальнейшее продолжение установки будет невозможным. Для продолжения нажмите кнопку «Далее»

Рисунок 49. Мастер установки ПО Центра Регистрации



16. Следующим шагом необходимо ввести информацию о пользователе, производящем установку, и серийный номер Лицензии, предоставляющей право на эксплуатацию ЦР. После ввода данных нажмите кнопку **Далее** (см. Рисунок 50). Если все поля для ввода серийного номера оставить пустыми, то программа установки будет использовать серийный номер ознакомительной лицензии, действующей в течение месяца.

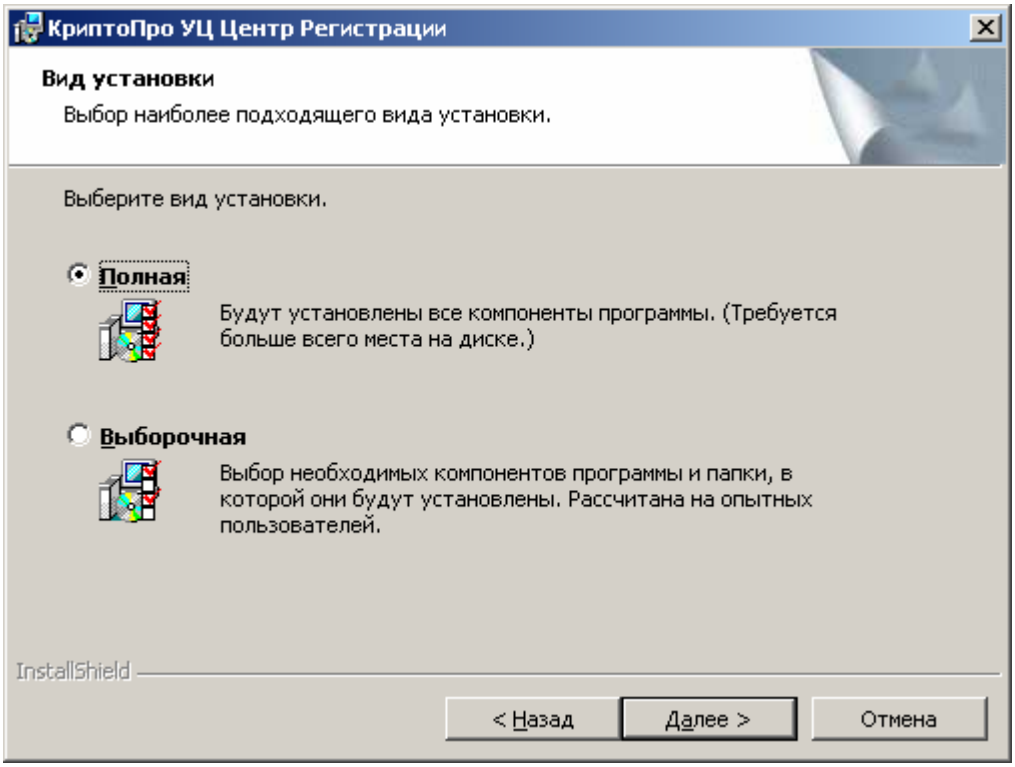
Рисунок 50. Сведения о пользователе ПО ЦР



17. После нажатия кнопки **Далее** программа установки отобразит диалоговое окно (см. Рисунок 17), на котором необходимо выбрать вид установки. Программой установки определены два вида установки: полная и выборочная. Использование вида "выборочная" позволяет сменить папки для установки компонентов (файлов) Центра регистрации, а также определить, какие компоненты нужно устанавливать, а какие нет. При использовании вида "полная" установка компонентов производится в предопределенные папки:

Компонент	Имя папки по умолчанию	Местоположение папки	Местоположение по умолчанию
Центр Регистрации Крипто-Про УЦ	Crypto Pro\RA	Папка ”Program Files”	C:\Program Files
Удаленный доступ по протоколу SOAP, Виртуальный каталог SOAP доступа на веб-узле 1, Веб-интерфейс пользователя по протоколу HTTPS, Виртуальный каталог веб-интерфейса пользователя на веб-узле 1	RA\Inetpub	Папка ”Crypto Pro” в системной папке ”Application Data” профиля для всех пользователей компьютера	C:\Documents and Settings\All Users\Application Data\Crypto Pro
База данных ЦР	RA\Data		

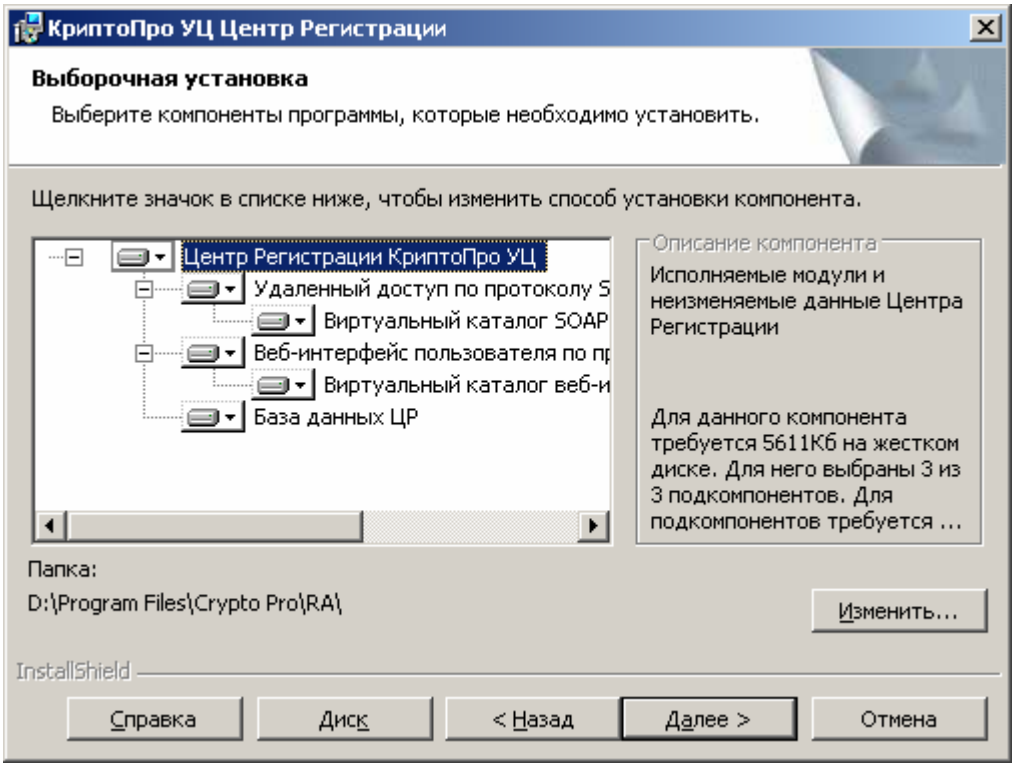
Рисунок 51. Вид установки ПО ЦР



Изменение папок назначения производится следующим образом:

- выберите вид установки **Выборочная** и нажмите кнопку **Далее**
- в появившемся окне (см. Рисунок 52) выберите компонент, для которого необходимо изменить папку назначения.
- нажмите кнопку **Изменить**, расположенную справа от текстовой строки с именем папки назначения.
- В окне изменения текущей папки назначения выберите нужную папку с использованием элемента окна **Поиск в папке**. В случае если папка не существует, то создайте ее. Для этого нажмите на кнопку с пиктограммой, расположенную в правой части элемента окна **Поиск в папке**.

Рисунок 52. Вид установки «Выборочная»



После выбора папки нажмите кнопку **ОК**. Если необходимо оставить в качестве текущей папки предлагаемую по умолчанию, то нажмите кнопку **Отмена**

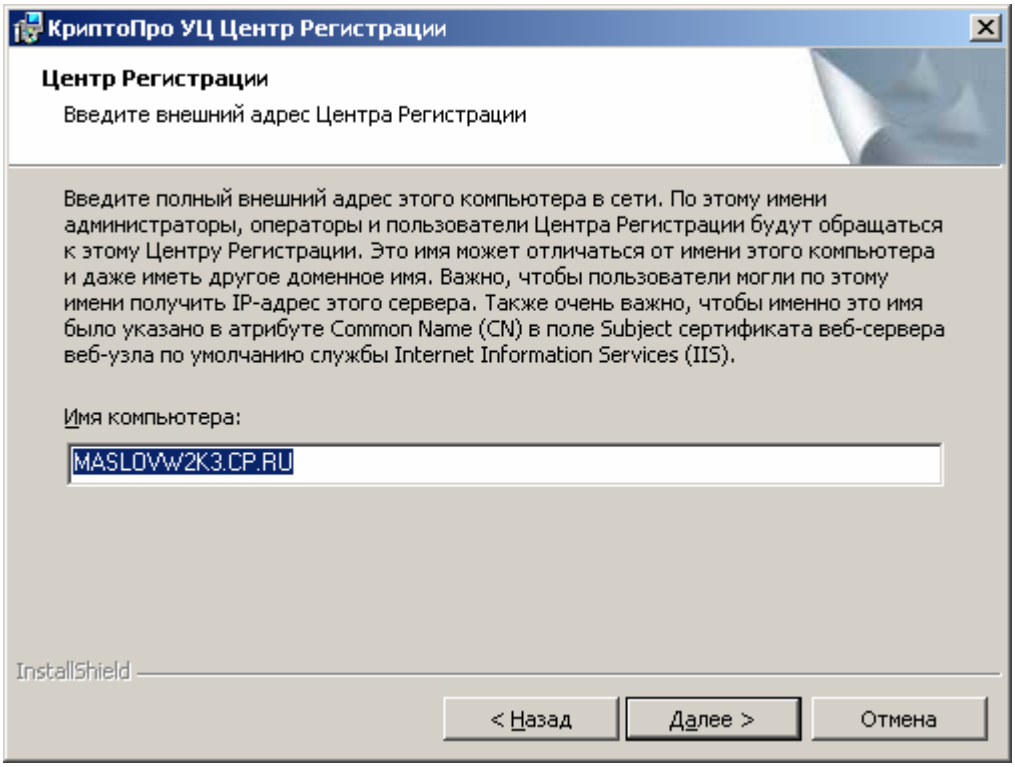
Выбор компонентов для установки производится следующим образом:

- выберите вид установки «выборочная» и нажмите кнопку «далее»
- в появившемся окне (см. Рисунок 17а) выберите компонент и нажмите левую кнопку мыши на прямоугольнике со стрелкой вниз (например:).
- в появившемся меню выберите нужный пункт

Если для какого-либо компонента выбрать «Данный компонент будет недоступен», то этот компонент не устанавливается. При желании его можно будет установить позднее.

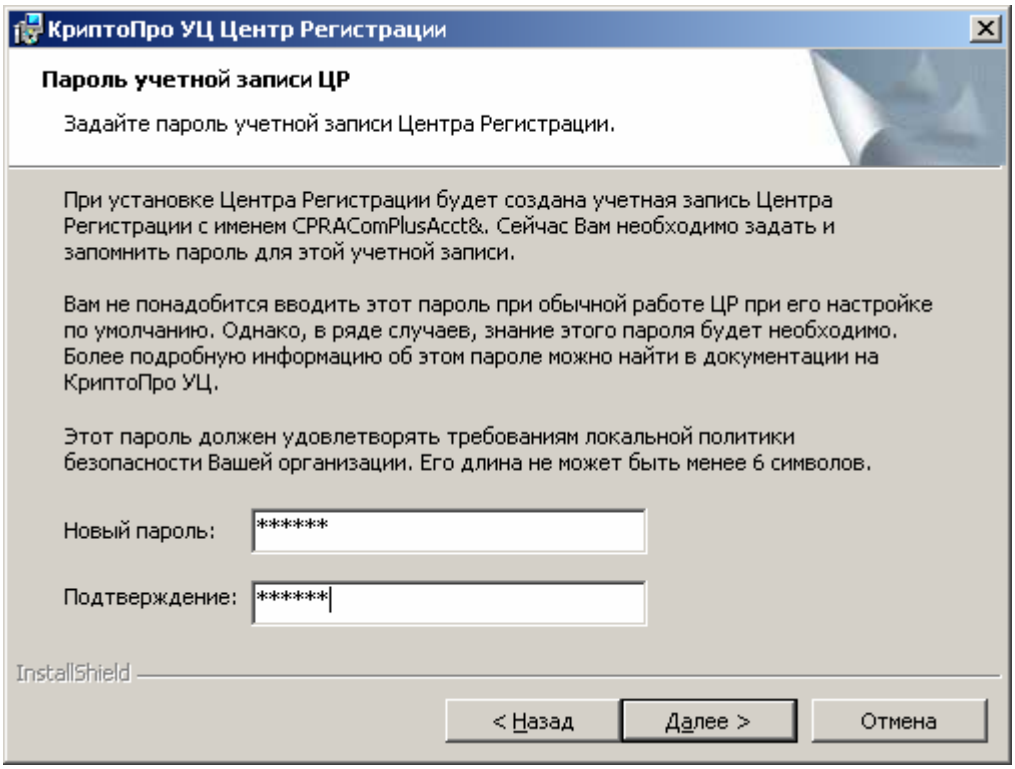
18. После определения вида установки, следующим отображается диалоговое окно (см. Рисунок 53), в котором необходимо определить внешний адрес Центра регистрации. По этому адресу ЦР должен быть доступен по протоколу HTTP(S). После ввода данных нажмите кнопку «Далее».

Рисунок 53. Внешний адрес Центра Регистрации



19. В процессе установки программного обеспечения Центра Регистрации Мастер создает учетную запись на локальном компьютере с именем CPRAComPlusAcct&, с которой будут работать серверные компоненты Центра Регистрации (COM+ приложения). Пароль для этой учетной записи определяется в соответствии с требованиями локальной политики безопасности, но длиной не менее 6 символов. Пароль учетной записи Центра Регистрации задается в окне Мастера установки ПО Центра Регистрации (см. Рисунок 54).

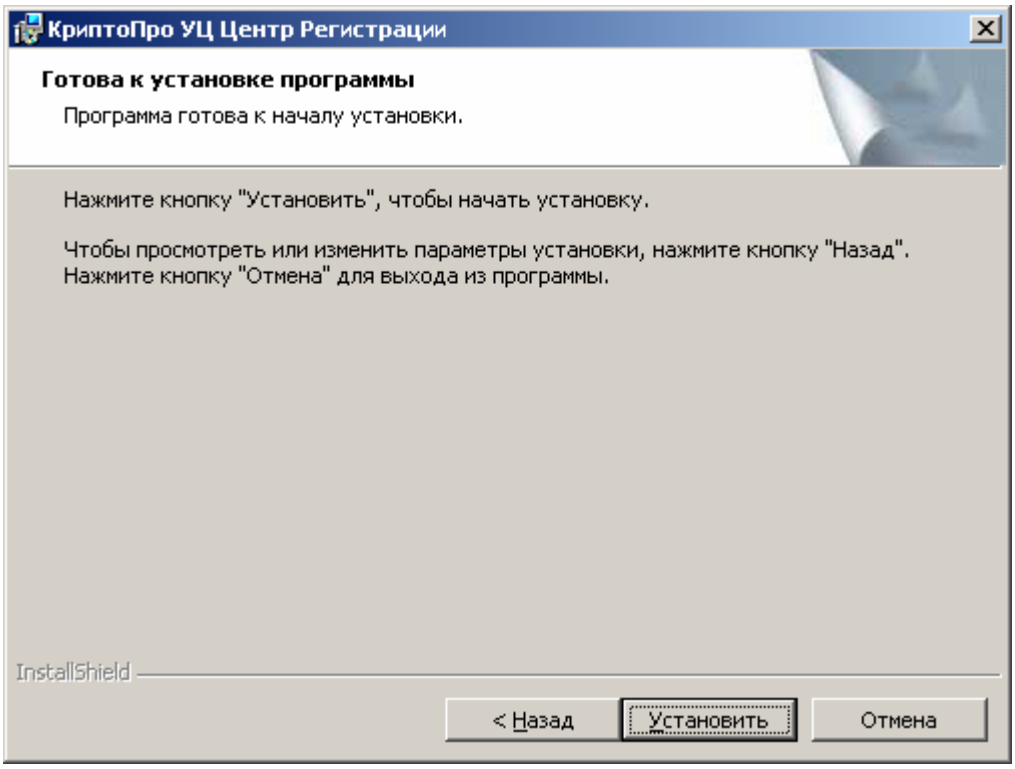
Рисунок 54. Окно определения пароля учетной записи Центра Регистрации Мастера установки ПО ЦР



Введенный пароль учетной записи необходимо запомнить, так как он может понадобиться в процессе эксплуатации ПАК «КриптоПро УЦ».

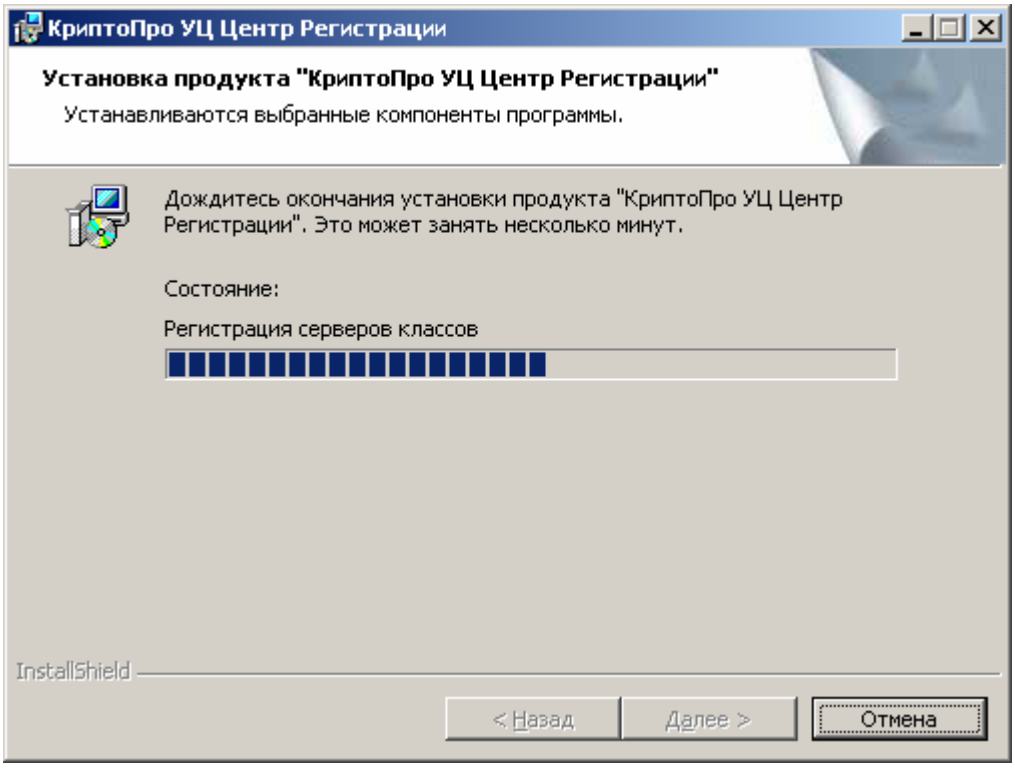
20. После определения всех необходимых параметров, выполненных на предыдущих шагах, программа установки выведет диалоговое окно подтверждения продолжения установки (см. Рисунок 55). При необходимости можно вернуться на переопределение параметров установки. Для этого надо нажать кнопку «Назад». Для подтверждения установки нажмите кнопку «Установить».

Рисунок 55. Окно подтверждения установки ПО ЦР



21. После нажатия кнопки «Установить», программа произведет установку ПО (см. Рисунок 56).

Рисунок 56. Окно состояния процесса установки ПО ЦР



22. После завершения установки и настройки программного обеспечения ЦР программа установки выведет диалоговое окно с соответствующим сообщением. Для завершения установки нажмите кнопку «Готово».

23. Если во время установки в систему были внесены изменения, требующие перезагрузки компьютера, то на экране появится окно с предложением произвести перезагрузку. Для того, чтобы сразу же перезагрузить компьютер, нажмите кнопку **Да**, а для того, чтобы перезагрузить компьютер позже вручную, нажмите **Нет**.

4.7. Выпуск и инсталляция клиентского сертификата Центра Регистрации

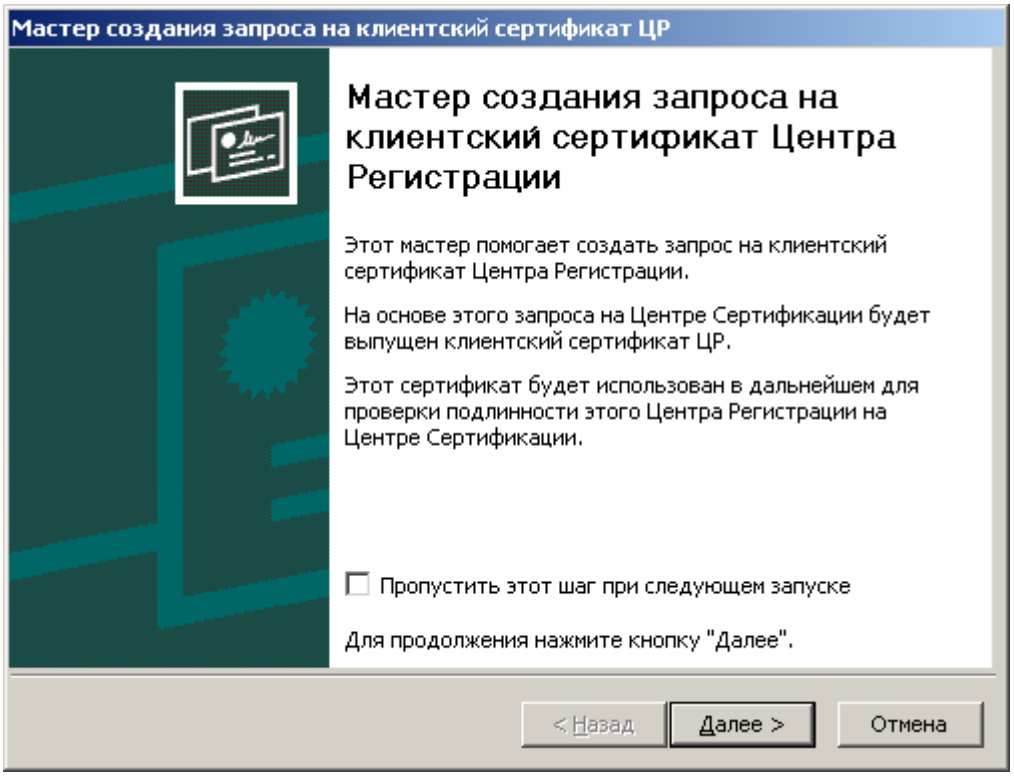
Ключи и клиентский сертификат Центра Регистрации используются для установления соединения и авторизации с Центром Сертификации.

Выпуск и установка клиентского сертификата ЦР выполняется в следующей последовательности:

1. Генерация ключей и формирование запроса на клиентский сертификат.

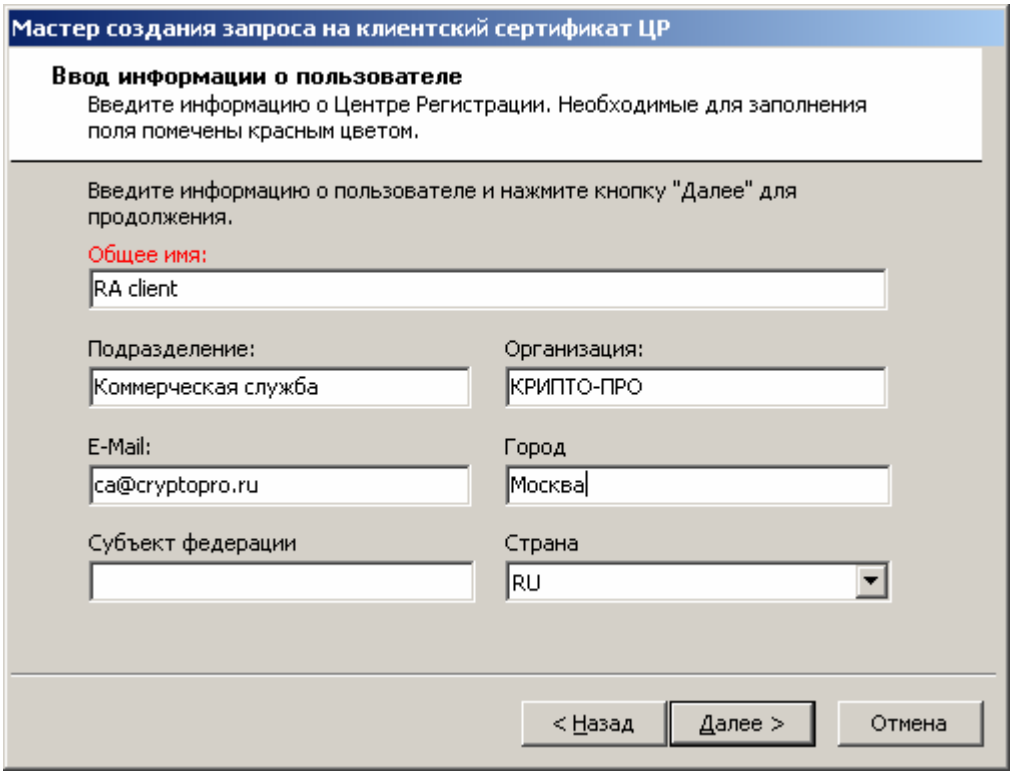
   Для генерации и формирования запроса на сертификат Центра регистрации запустите Мастер «Запрос на клиентский сертификат ЦР» из группы **Крипто-Про** (см. Рисунок 57)

Рисунок 57. Окно Мастера создания запроса на клиентский сертификат ЦР



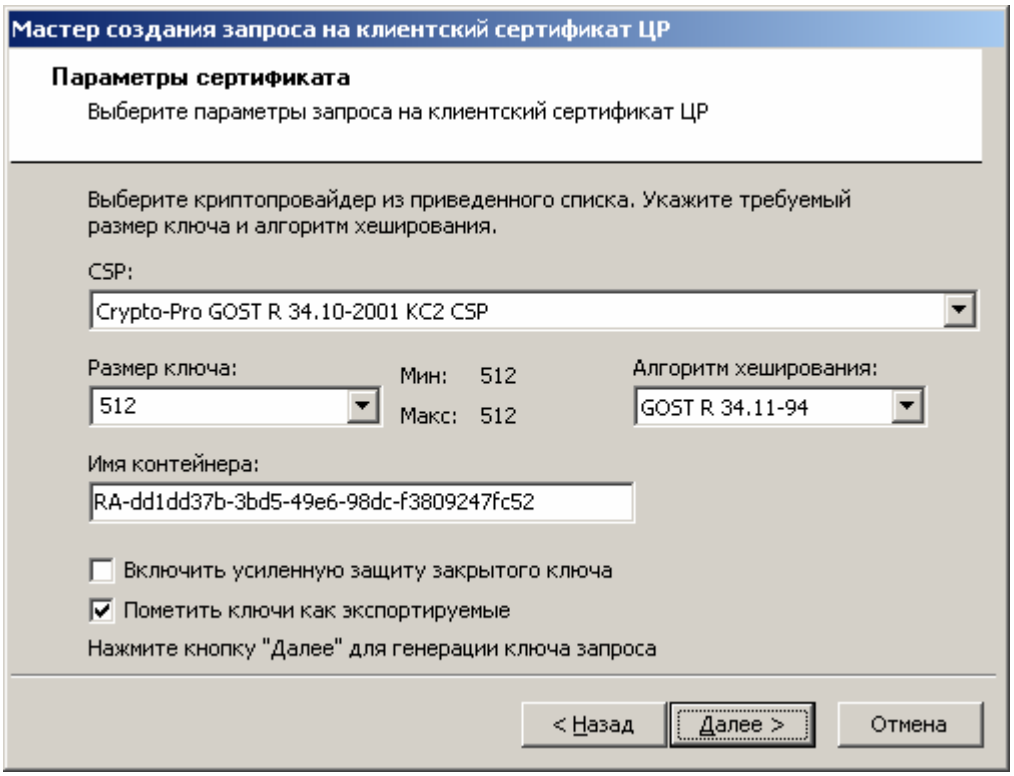
Для подготовки запроса на сертификат Мастер выводит диалоговое окно; в этом окне требуется задать информацию о владельце ключей и сертификата, которые будут использоваться во взаимодействии с Центром сертификации УЦ (см. Рисунок 58).

Рисунок 58. Окно ввода информации о ЦР



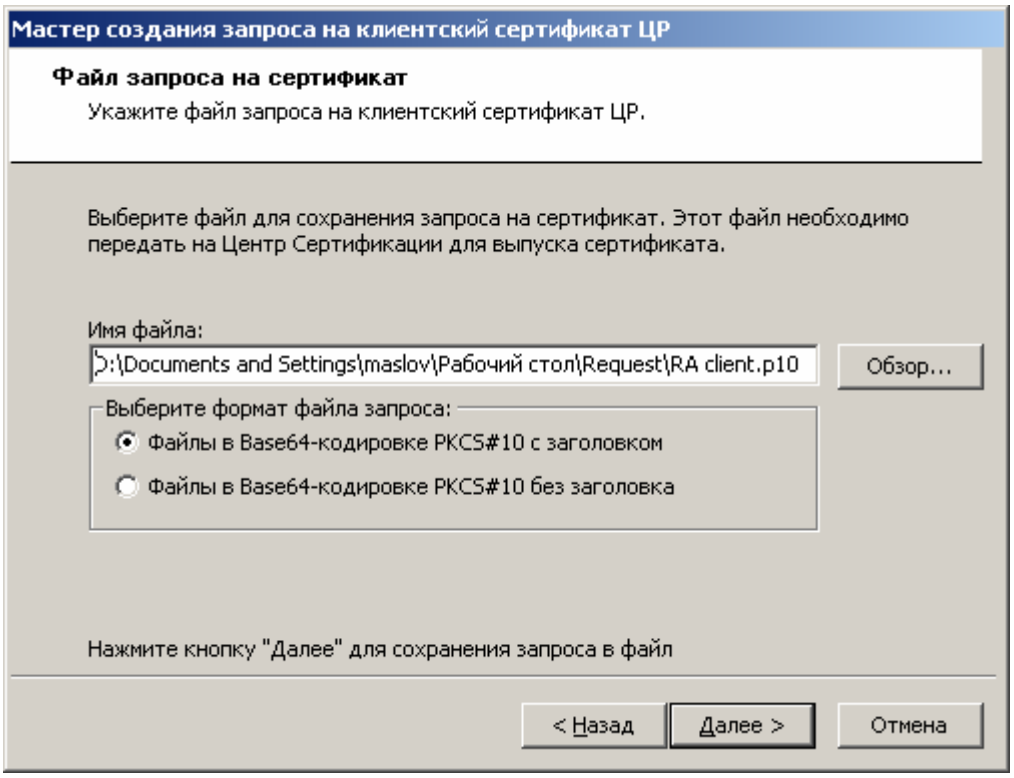
Мастер предоставляет возможность выбора криптопровайдера (CSP), размера ключа и алгоритма хэширования при создании запроса на сертификат. Для этого необходимо осуществить выбор параметров запроса в диалоговом окне Мастера (см. Рисунок 59).

Рисунок 59. Окно выбора CSP в Мастере создания запроса на клиентский сертификат ЦР



После генерации ключей следующим диалоговым окном Мастера будет окно, в котором требуется определить имя и размещение файла, где будет помещен запрос на сертификат Центра регистрации (см. Рисунок 60).

Рисунок 60. Окно выбора файла запроса на сертификат ЦР



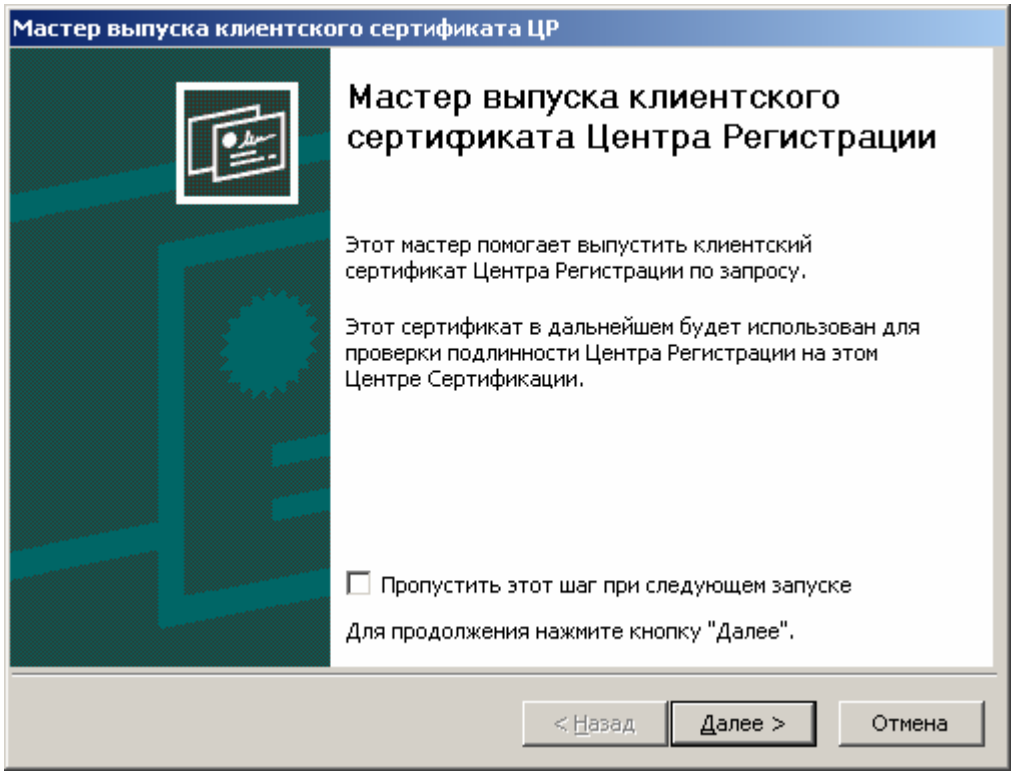
После выбора и ввода необходимой информации происходит формирование файла с запросом на клиентский сертификат Центра Регистрации.

2. Выпуск клиентского сертификата ЦР на Центре Сертификации на основании запроса

Сформированный файл необходимо доставить на Центр Сертификации и выпустить сертификат открытого ключа ЦР.

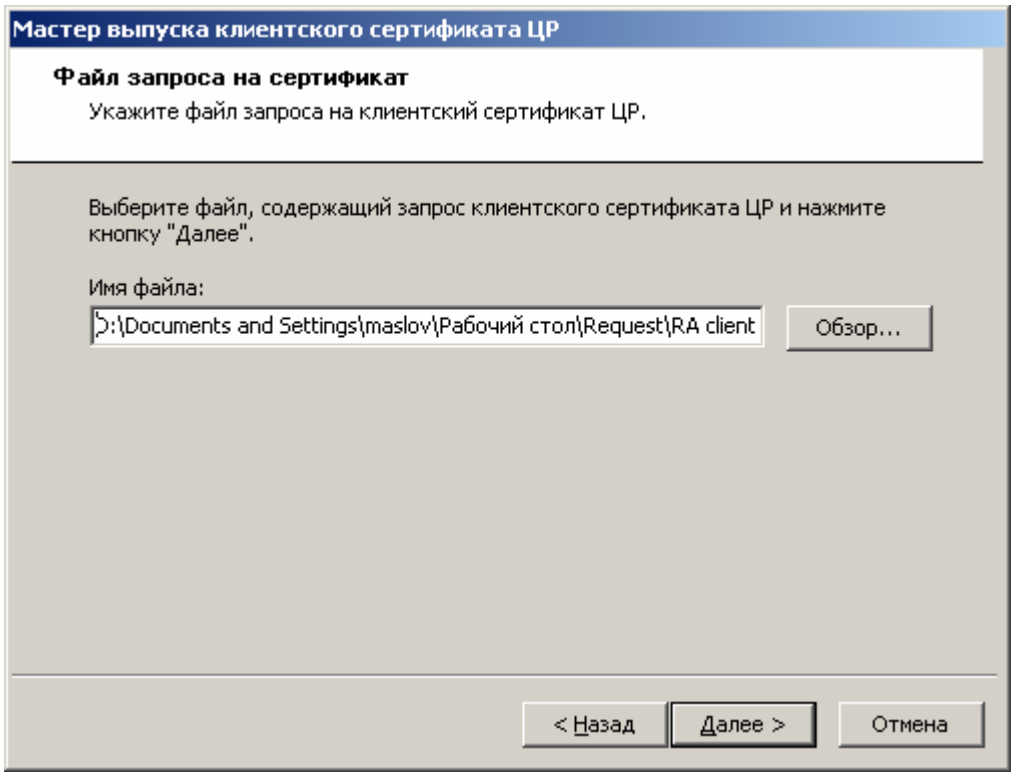
Выпуск клиентского сертификата ЦР производится на Центре Сертификации с помощью утилиты «Обработка запроса клиентского сертификата ЦР» (см. Рисунок 61).

Рисунок 61. Стартовое окно Мастера выпуска клиентского сертификата ЦР



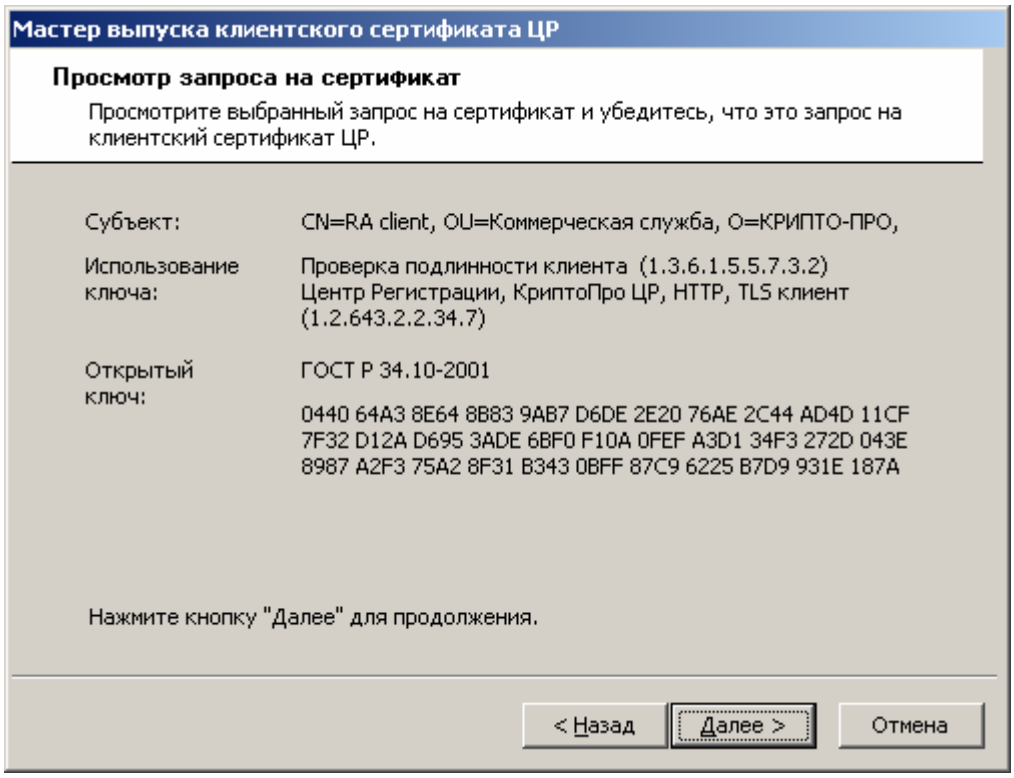
3. В следующем окне Мастера необходимо выбрать файл с запросом на клиентский сертификат ЦР (см. Рисунок 62) и нажать кнопку **Далее**

Рисунок 62. Окно выбора файла запроса Мастера выпуска клиентского сертификата ЦР



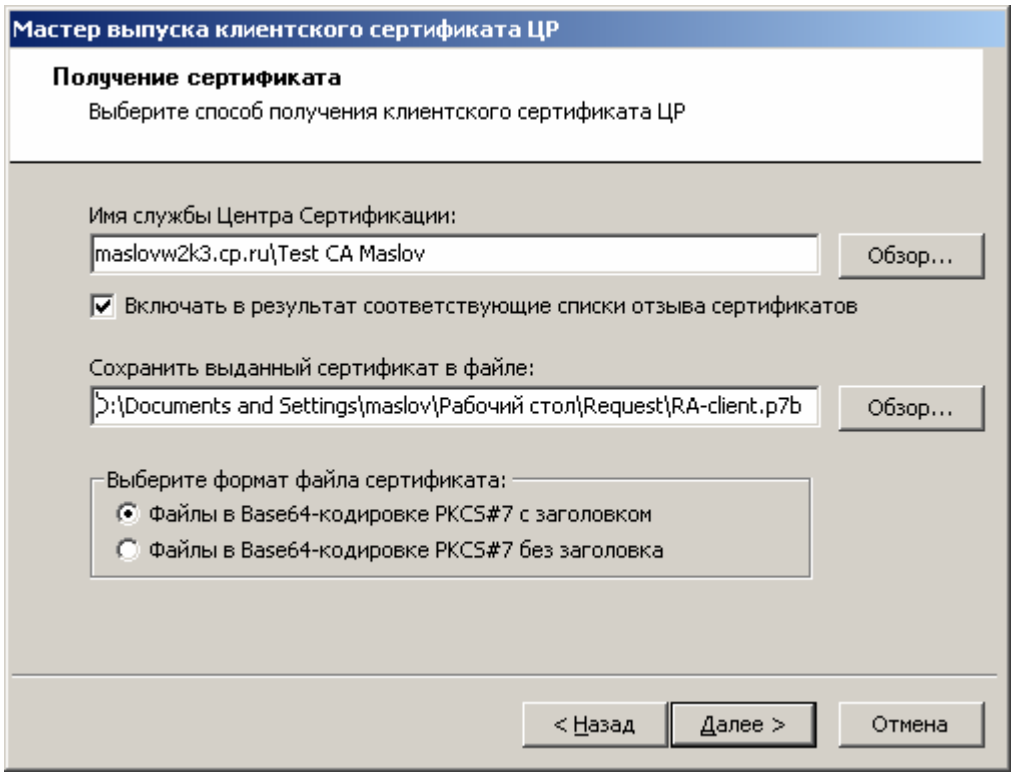
4. В окне просмотра запроса (см.) убедитесь в корректности данных и нажмите кнопку **Далее**

Рисунок 63. Окно просмотра запроса Мастера выпуска клиентского сертификата ЦР



5. В окне получения сертификата (см. Рисунок 64) с помощью кнопки **Обзор** выберите путь и имя файла, куда будет сохранен сертификат и нажмите кнопку **Далее**. Файл результата будет содержать цепочку сертификатов, включающую как сам клиентский сертификат ЦР так и всю цепочку издателей сертификата. Рекомендуется включать в результат соответствующие списки отзыва сертификатов.

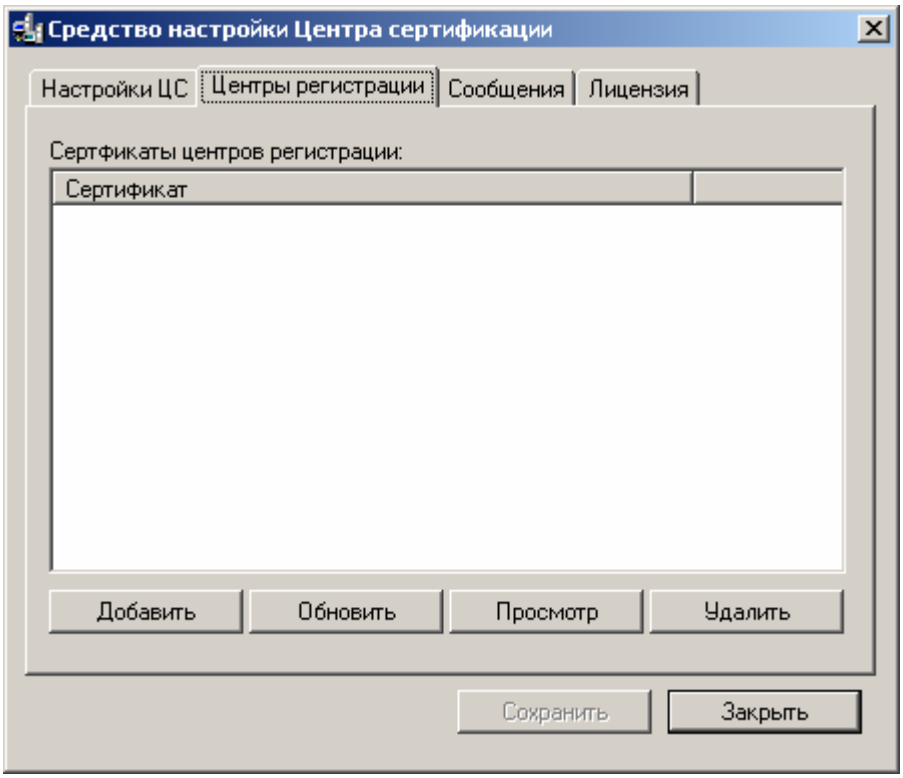
Рисунок 64. Окно получения сертификата Мастера выпуска клиентского сертификата ЦР



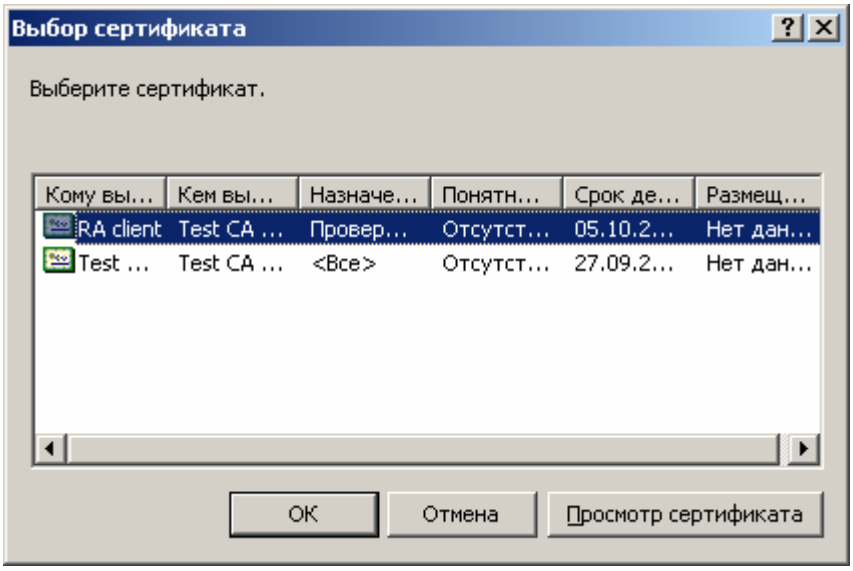
6. В завершающем окне Мастера нажмите кнопку **Готово**
7. Занесение клиентского сертификата ЦР в список доверенных ЦР на Центре Сертификации

Занесение клиентского сертификата ЦР в список доверенных ЦР на Центре Сертификации осуществляется помощью приложения **Параметры Центра Сертификации** (см. Рисунок 65) из группы **Крипто-Про** на вкладке **Центры регистрации**.

Рисунок 65. Вкладка "Центры регистрации" окна настроек приложения "Параметры Центра Сертификации"

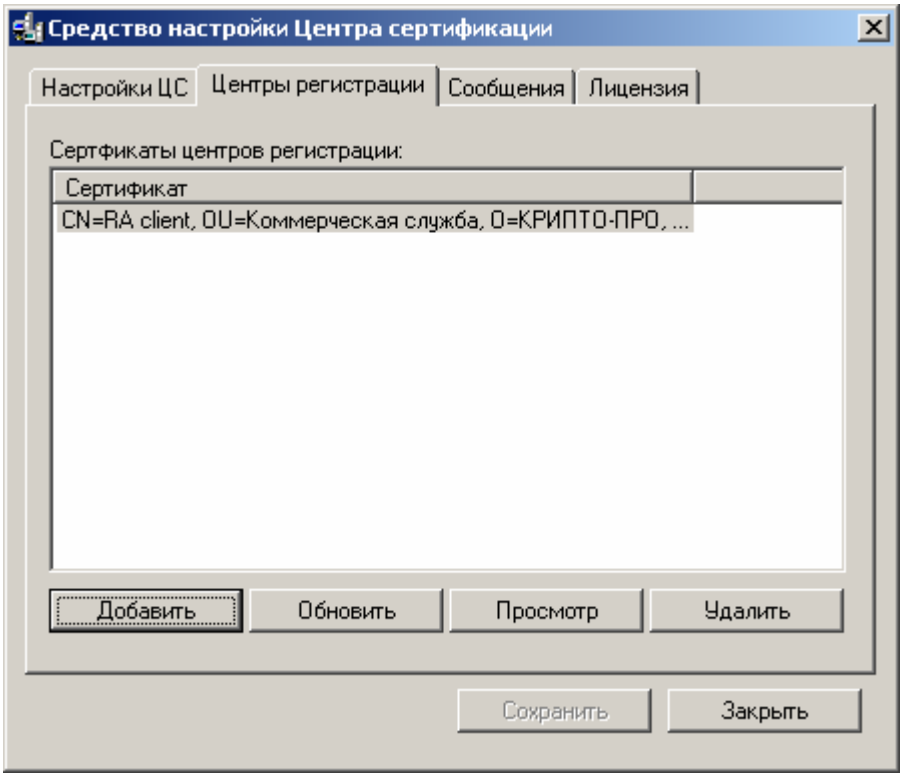


Для добавления клиентского сертификата ЦР в список доверенных ЦР нажмите кнопку **Добавить**, выберите файл с сертификатом клиентского сертификата ЦР, выпущенного ранее на ЦС, в списке сертификатов из цепочки сертификатов выберите клиентский сертификат ЦР и нажмите кнопку **ОК**.



Клиентский сертификат ЦР будет добавлен в список доверенных ЦР (см. Рисунок 66)

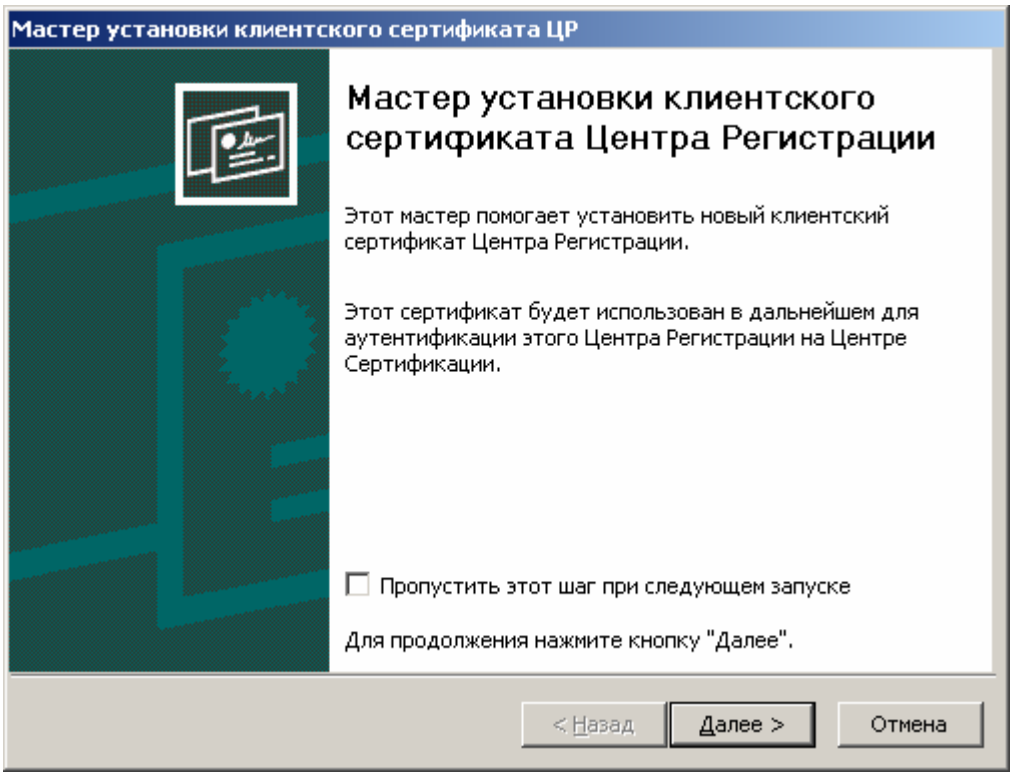
Рисунок 66. Окно доверенных Центров Регистрации



8. Установка клиентского сертификата ЦР на Центре Регистрации

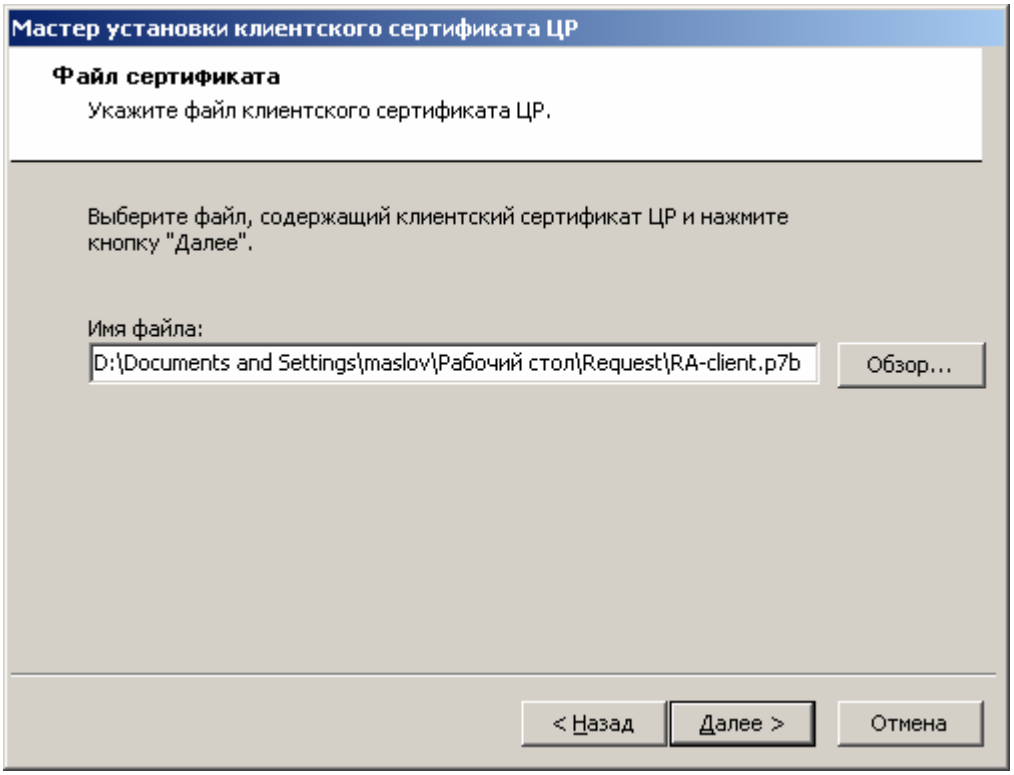
Для установки выпущенного сертификата ЦР на Центре Регистрации необходимо перенести файл и выполнить приложение **Установка клиентского сертификата ЦР** из группы **Крипто-Про** (см. Рисунок 67).

Рисунок 67. Мастер установки клиентского сертификата Центра Регистрации



Данное приложение представляет собой Мастер установки клиентского сертификата Центра регистрации. Мастер установки отобразит диалоговое окно выбора файла сертификата Центра регистрации (см. Рисунок 68).

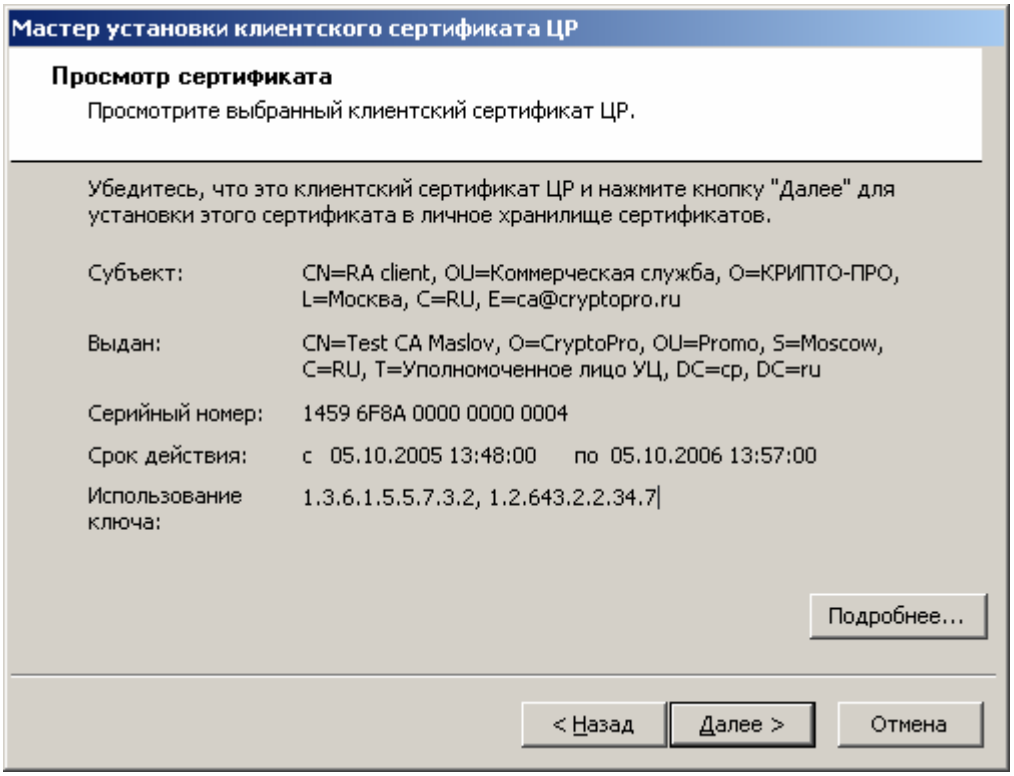
Рисунок 68. Окно выбора сертификата ЦР в Мастере установки



В следующем окне Мастер отобразит информацию по сертификатам из выбранного файла (см. Рисунок 69). В этом окне выводится краткая информация из текущего сертификата в цепочке сертификатов. Для получения более подробной информации о текущем сертификате можно воспользоваться кнопкой **Подробнее**.

Для продолжения работы Мастера нажмите кнопку **Далее**.

Рисунок 69. Окно просмотра выбранного сертификата ЦР в Мастере установки



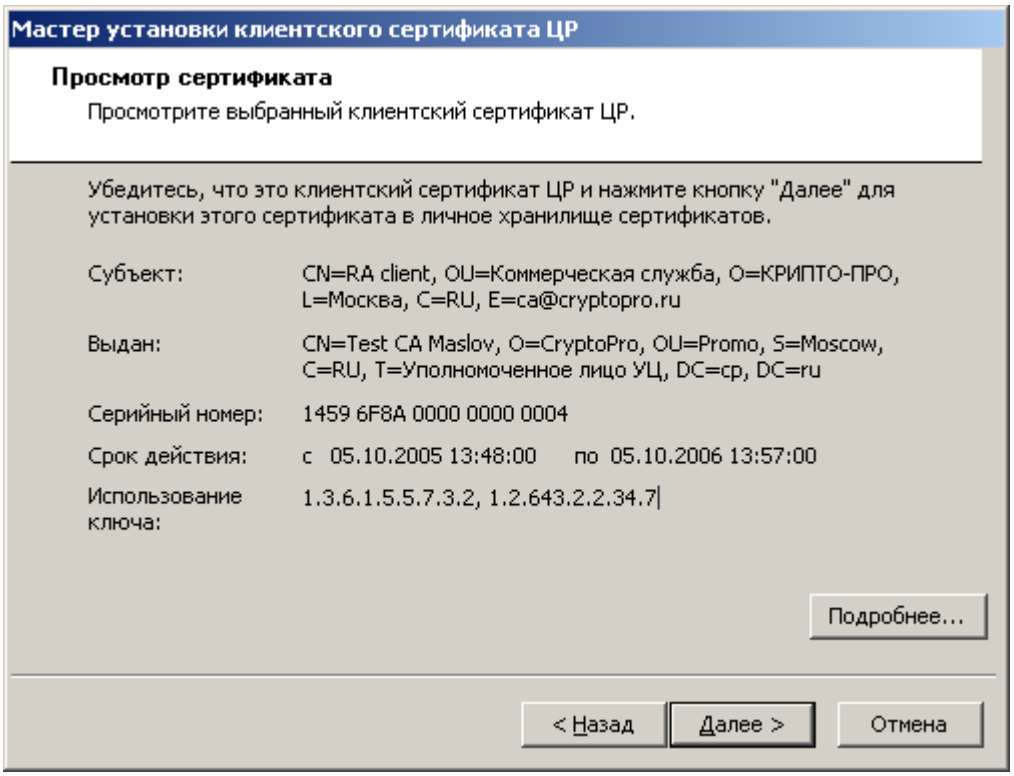
Мастер произведет установку сертификатов из цепочки сертификатов и списков отозванных сертификатов и в случае успешного завершения данной операции будет выведено окно об окончании работы Мастера (см. Рисунок 70).

В случае невозможности успешного завершения работы Мастера отобразится окно, содержащее диагностическое сообщение об ошибке. Типичными причинами ошибки являются:

- отсутствие прав у пользователя на запись в раздел **Личные** хранилища сертификатов локального компьютера;
- в разделе **Личные** хранилища сертификатов локального компьютера уже установлен данный сертификат Центра регистрации.

После завершения работы Мастера с ошибкой и устранения причин возникновения ошибочной ситуации необходимо повторить действия, начиная с задачи формирования запроса на сертификат Центра регистрации.

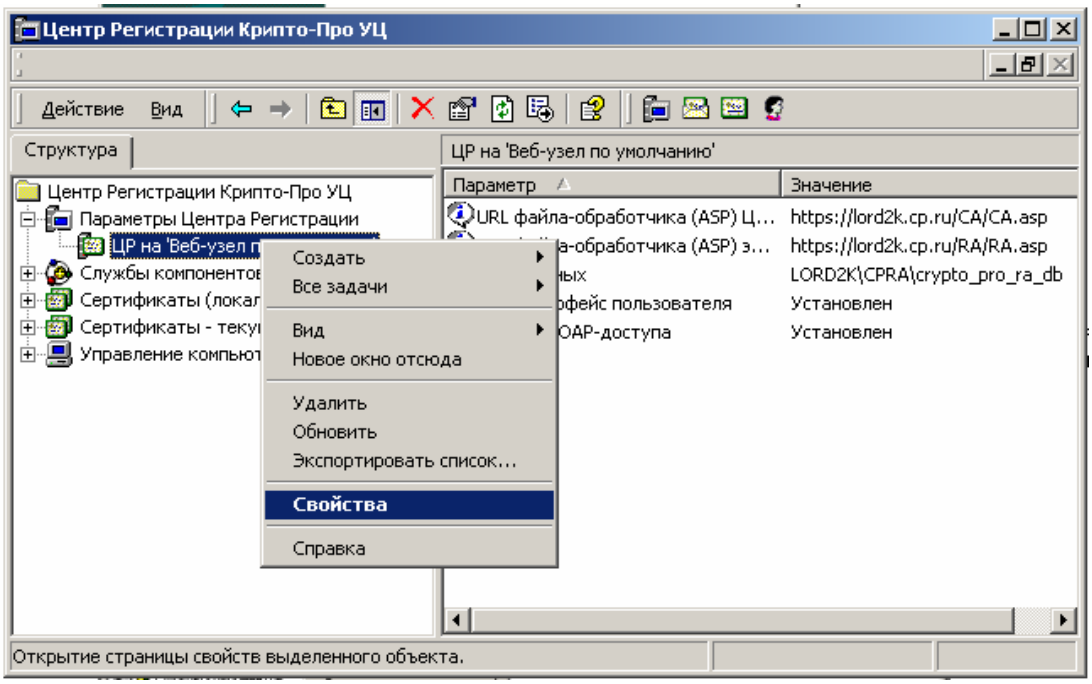
Рисунок 70. Окно успешной установки сертификата ЦР в Мастере установки



4.8. Настройка и тестирование соединения с Центром Сертификации

Настройка соединения Центра Регистрации с Центром Сертификации осуществляется в свойствах узла **Центр Регистрации** приложения **Параметры Центра Регистрации** (см. Рисунок 71).

Рисунок 71. Пункт "Свойства" узла Центра Регистрации



Настройка соединения заключается в установке значения адреса URL файла-обработчика Центра Сертификации и в выборе сертификата подписи и аутентификации Центра Регистрации (клиентского сертификата ЦР).

Адрес URL файла-обработчика Центра Сертификации – параметр, определяющий местоположение и протокол доступа к файлу обработчику программного интерфейса Центра сертификации, с которым будет взаимодействовать установленный Центр регистрации.

Ввод параметра осуществляется на вкладке **Общие** свойств узла Центра регистрации (см. Рисунок 72). Шаблон адреса URL файла-обработчика задан в качестве установленного по умолчанию значения параметра. В этом шаблоне необходимо заменить имя **localhost** на доменное имя Web-сервера Центра сертификации.

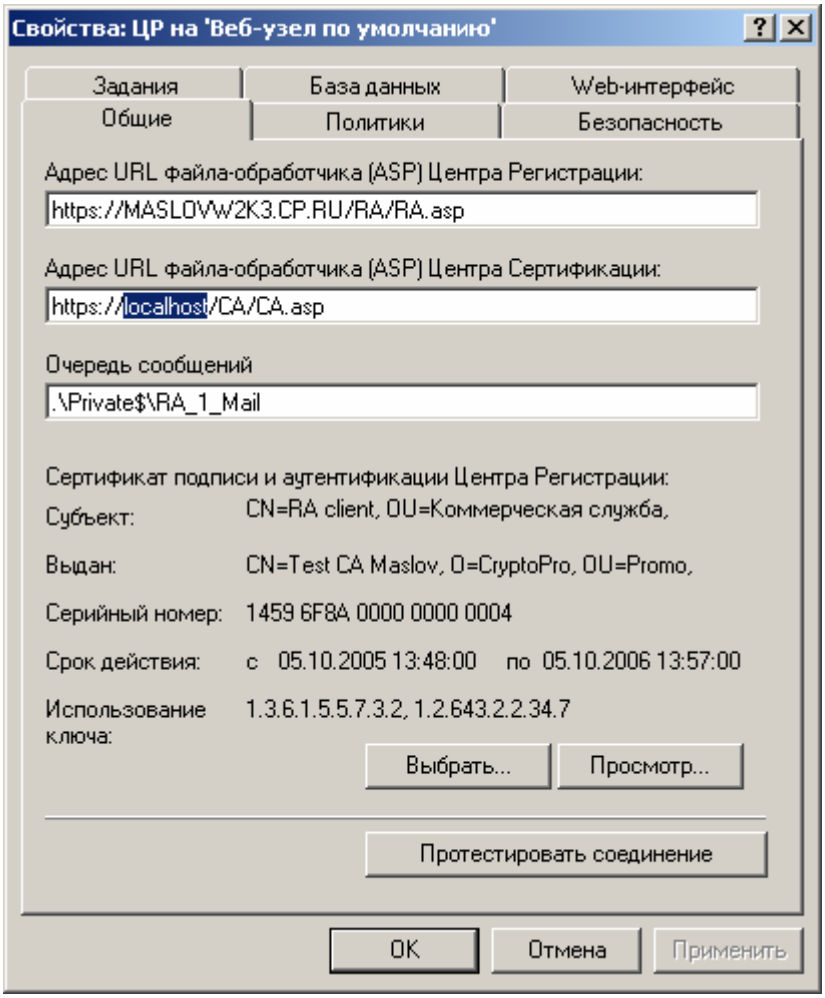
После ввода значения данного параметра необходимо нажать кнопку **Применить**.

Сертификат подписи и аутентификации Центра регистрации – параметр, определяющий информацию по сертификату Центра регистрации, который используется для взаимодействия с Центром Сертификации.

Выбираемый сертификат должен быть включен в список доверенных Центров регистрации на Центре сертификации. Выбор сертификата осуществляется с использованием кнопки **Выбрать**. Подробную информацию о выбранном сертификате можно получить нажатием кнопки **Просмотр**.

Выбор сертификата Центра регистрации осуществляется на вкладке **Общие** свойств узла Центра регистрации (см. Рисунок 72).

Рисунок 72. Вкладка «Общие» окна свойств Центра Регистрации



После выбора сертификата Центра регистрации и определения адреса URL файла-обработчика Центра сертификации можно проверить корректность ввода параметров и протестировать соединение Центра регистрации с Центром сертификации. Для этого нажмите кнопку **Протестировать соединение**. Не забудьте перед тестированием соединения нажать кнопку **Применить**.

Тестирование соединения Центра регистрации с базой данных Центра регистрации, расположенной на SQL сервере осуществляется на вкладке **База данных** путем нажатия кнопки **Протестировать соединение**.

5. Установка АРМ администратора ЦР

5.1. Последовательность установки АРМ администратора ЦР

Установка и конфигурация программного обеспечения АРМ администратора ЦР из состава программного комплекса УЦ производится в следующей последовательности:

1. Установка СКЗИ КриптоПро CSP и КриптоПро TLS
2. Установка программного обеспечения АРМ администратора ЦР
3. Выпуск и инсталляция сертификата привилегированного пользователя
4. Настройка и тестирование соединения с Центром Регистрации

5.2. Установка СКЗИ КриптоПро CSP и КриптоПро TLS

На АРМ администратора ЦР с установленной ОС из следующего перечня: MS Windows 2000 Professional, MS Windows Server 2000 и MS Windows XP, устанавливается СКЗИ КриптоПро CSP (версия 2.0) в составе согласно формуляра ЖТЯИ.00005-02 30 01, вариант исполнения 4 или СКЗИ КриптоПро CSP (версия 3.0) в составе согласно формуляра ЖТЯИ.00015-01 30 01, вариант исполнения 6.

На АРМ администратора ЦР с установленной ОС MS Windows Server 2003 устанавливается СКЗИ КриптоПро CSP (версия 3.0) в составе согласно формуляра ЖТЯИ.00015-01 30 01, вариант исполнения 6.

Установка СКЗИ «КриптоПро CSP» осуществляется в соответствии с эксплуатационной документацией. Для версии 2.0 отдельно ставится модуль «КриптоПро TLS» в соответствии с эксплуатационной документацией. Для версии 3.0 модуль «КриптоПро TLS» не требует отдельной установки.

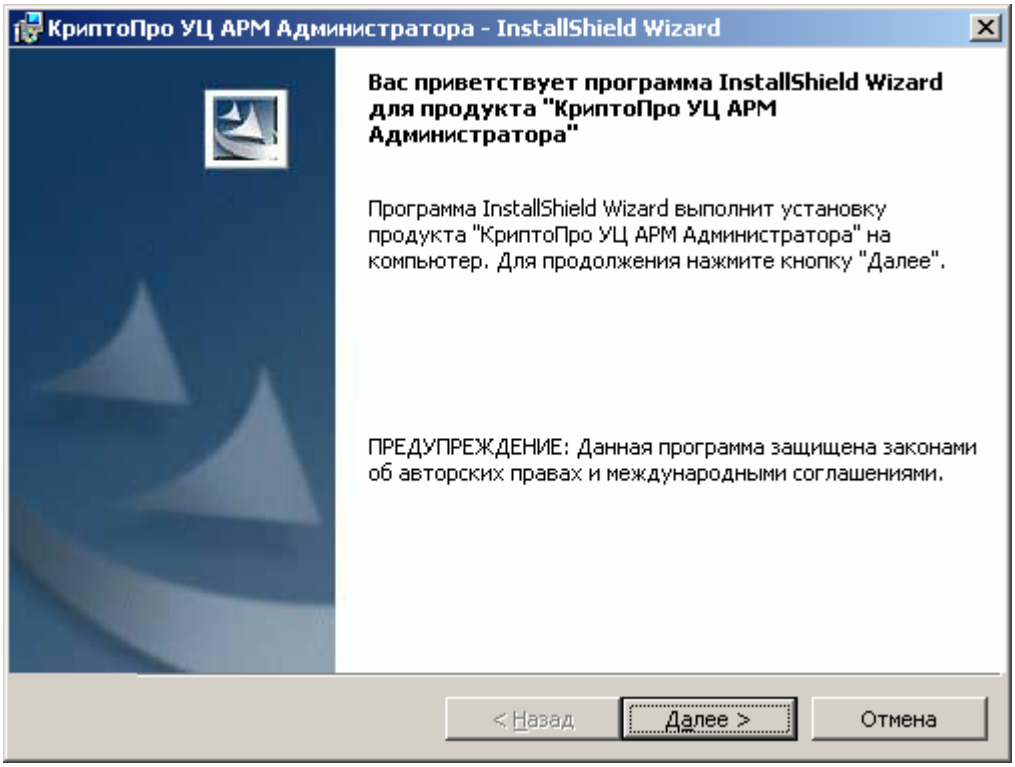
После установки программного обеспечения СКЗИ «КриптоПро CSP» и «КриптоПро TLS» необходимо активировать лицензию на продукт из набора лицензий поставки ПАК «КриптоПро УЦ» и включить режим **кеширования** (вкладка **Безопасность** окна свойств КриптоПро CSP).

5.3. Установка программного обеспечения АРМ администратора ЦР

Для установки ПО АРМ Администратора необходимо запустить программу установки **SETUP.EXE**, расположенную на дистрибутиве ПАК «КриптоПро УЦ».

После запуска программа установки выведет на экран диалоговое окно подтверждения продолжения установки (см. Рисунок 73).

Рисунок 73. Окно Мастера установки ПО АРМ администратора

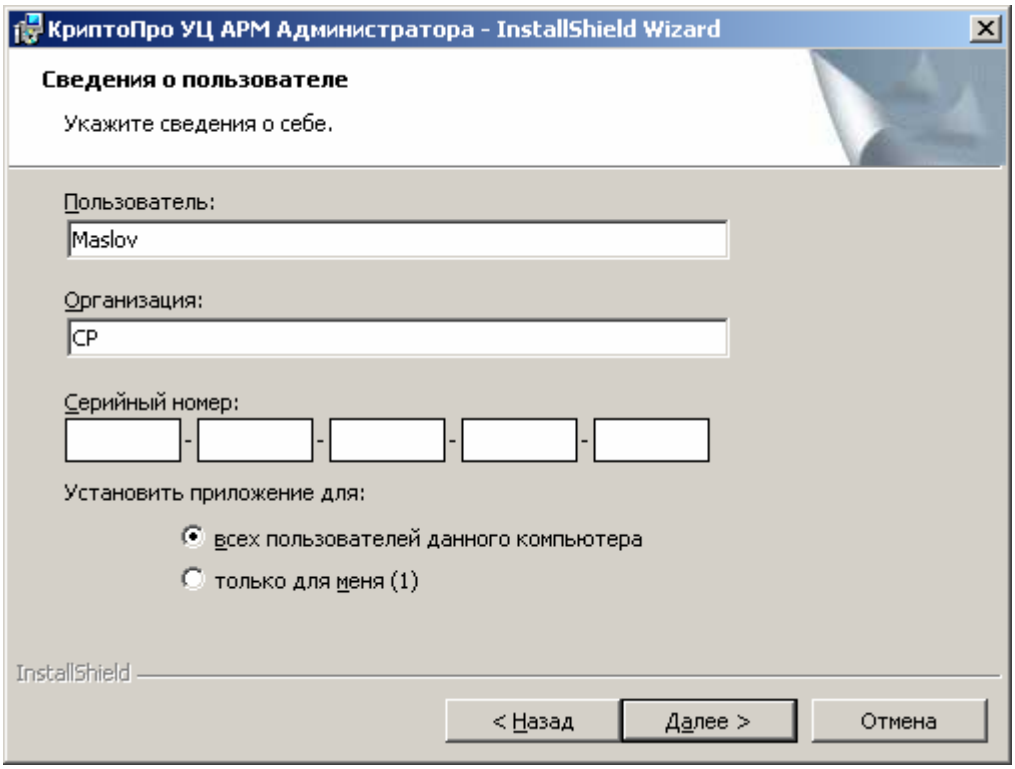


Для продолжения установки ПО АРМ Администратора необходимо нажать кнопку **Далее**. Для отмены установки ПО, нажать кнопку «Отмена».

В следующем окне необходимо ввести информацию о пользователе, производящем установку ПО, наименование организации и серийный номер предоставленной лицензии (см. Рисунок 74) – название организации и серийный номер лицензии должны полностью соответствовать данным, указанным в лицензии.

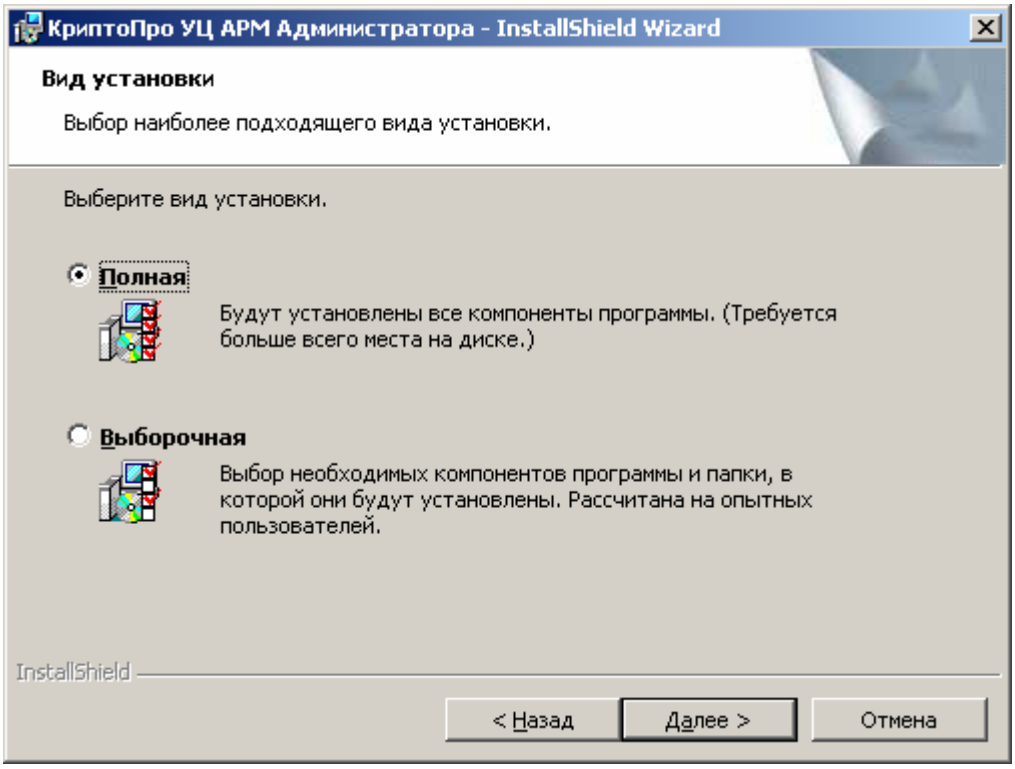
Ввод наименования организации и серийного номера лицензии на этапе установки ПО АРМ Администратора ЦР можно опустить. Последующий ввод указанных данных осуществляется в окне «Свойства: АРМ Администратора Центра Регистрации» (см. раздел 4.2.5. настоящего руководства)

Рисунок 74. Окно ввода информации о пользователе, организации и серийного номера лицензии Мастера установки АРМ администратора



После нажатия кнопки **Далее** на экран будет выведено диалоговое окно, в котором необходимо определить тип установки ПО (см. Рисунок 75).

Рисунок 75. Окно определения типа установки Мастера установки АРМ администратора

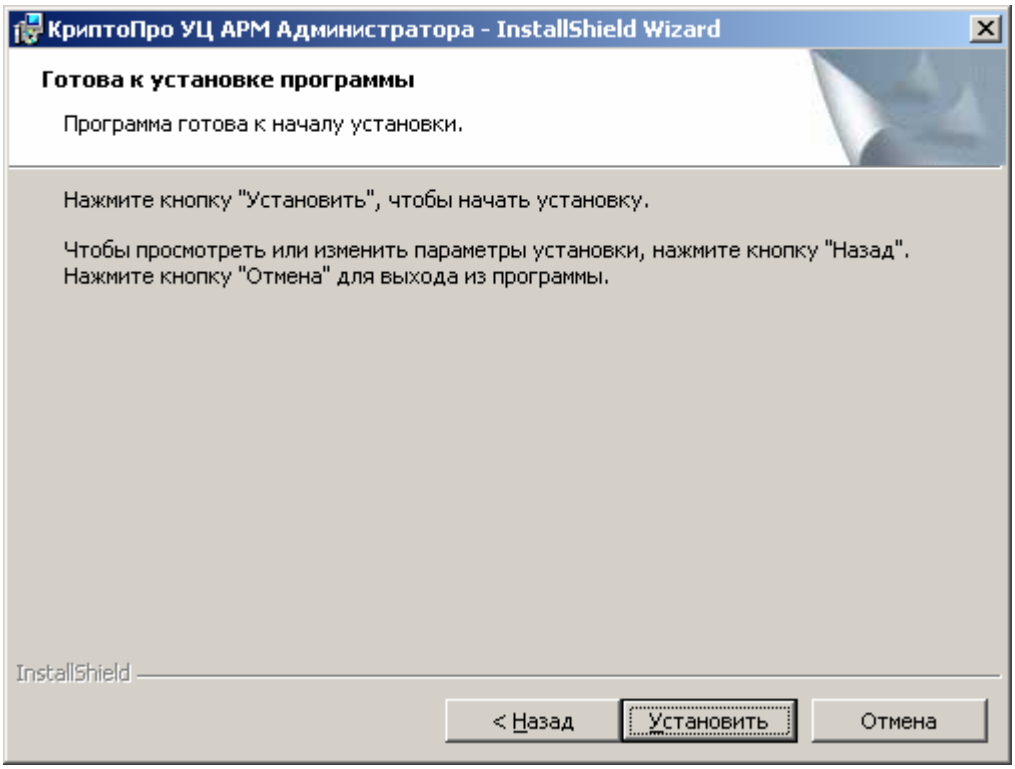


Тип установки **Полная** производит установку программного обеспечения АРМ Администратора в папку назначения, определенную по умолчанию. Таковой папкой является **Program Files\Crypto Pro** системного диска локального компьютера.

Для изменения текущей папки назначения необходимо выбрать тип установки **Выборочная**.

После определения начальных параметров Мастера установки на экран выводится диалоговое окно, в котором инициируется собственно операция установки (см. Рисунок 76).

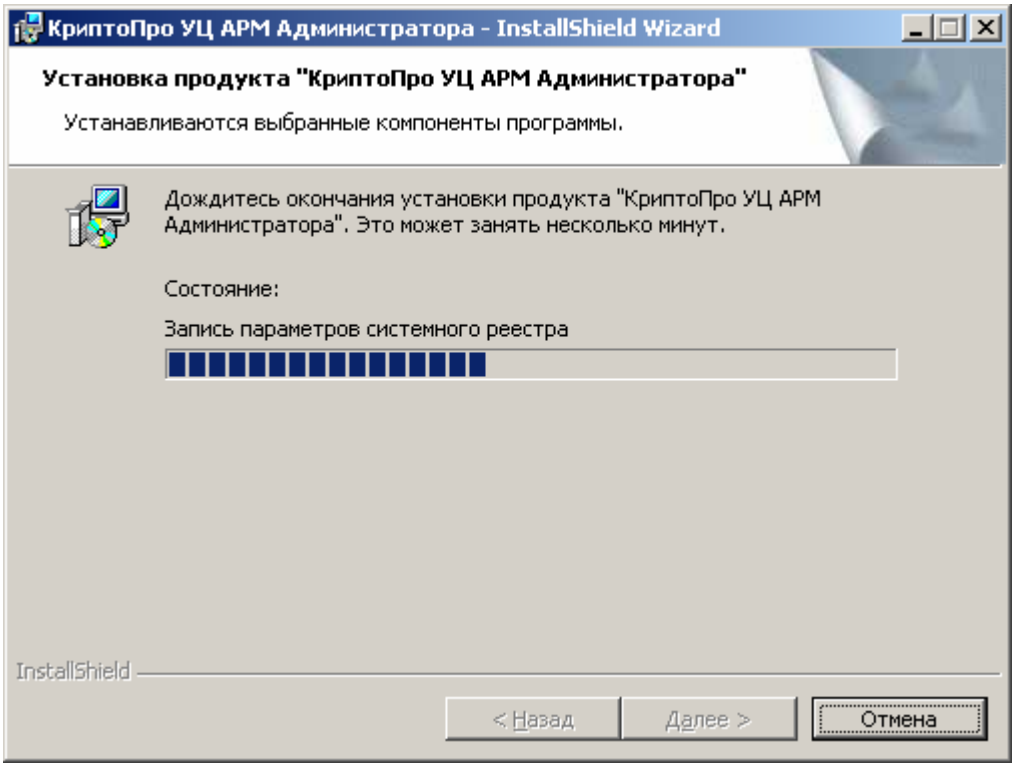
Рисунок 76. Окно подтверждения установки ПО Мастера установки АРМ администратора



Для продолжения установки нажмите кнопку **Установить**. Для изменения ранее введенных параметров установки нажмите кнопку «Назад».

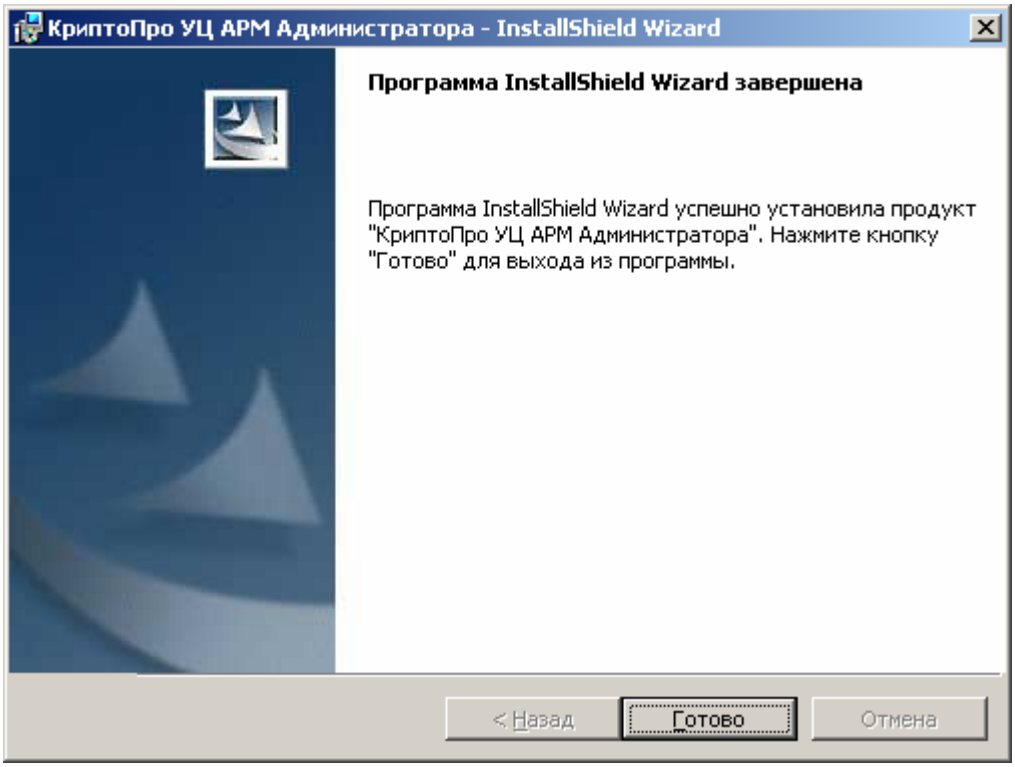
При выполнении операций установки, состояние процесса отображается в окне на экране.

Рисунок 77. Окно состояния установки Мастера установки АРМ администратора



Успешное завершение процесса установки ПО АРМ Администратора должно подтвердиться сообщением Мастера установки (см. Рисунок 78).

Рисунок 78. Окно окончания работы Мастера установки АРМ администратора



В противном случае убедитесь в соответствии общесистемного программного обеспечения требованиям, изложенным в настоящем руководстве. В случае расхождения необходимо привести их в соответствие и повторить процедуру установки заново. Если ошибка повторяется, обратитесь в службу технической поддержки.

В случае появления сообщения о необходимости перезагрузки ОС по завершению установки ПО АРМ Администратора ЦР, выполнить ее.

5.4. Подключение привилегированного пользователя

АРМ администратора ЦР предназначено для работы привилегированных пользователей Удостоверяющего центра – Администратора и/или Оператора.

Тип привилегированных пользователей Удостоверяющего центра определяется соответствующей ролью («Оператор Центра Регистрации» или «Администратор Центра Регистрации») в области применения (EKU) сертификата открытого ключа привилегированного пользователя.

Действия по подключению привилегированного пользователя совпадают как для Администратора, так и для Оператора, поэтому дальнейшее описание будет осуществляться применительно к Администратору.

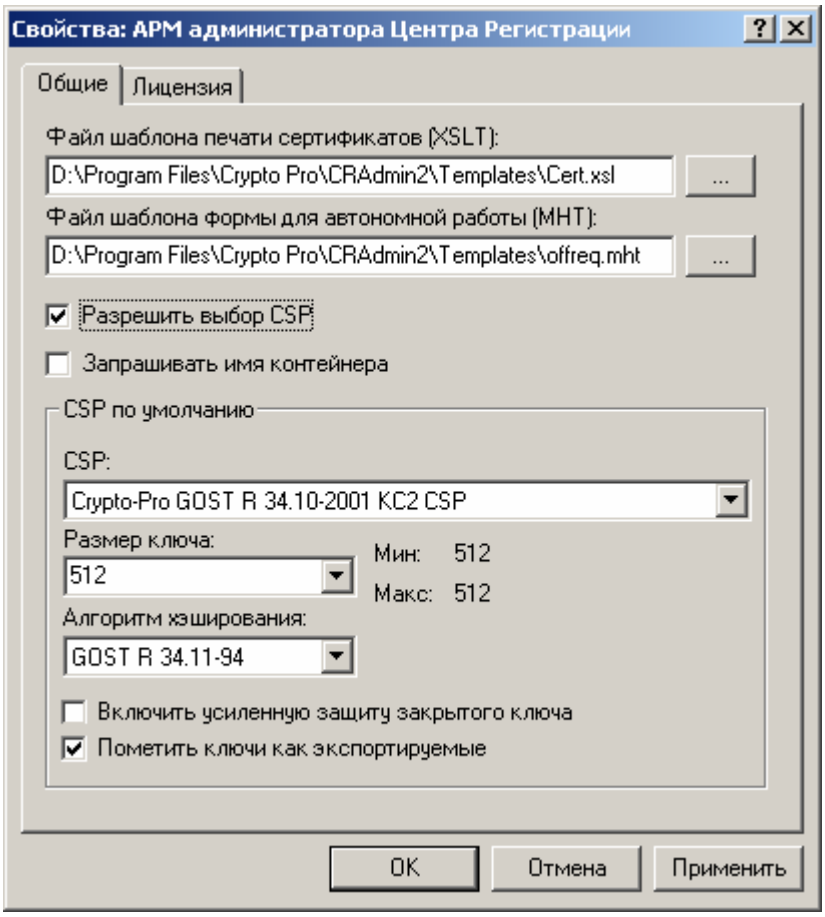
При первом запуске **АРМ администратора ЦР,** если у администратора не существует личного сертификата открытого ключа, необходимо выполнить следующие регламентные процедуры:

- создать запрос на сертификат администратора ЦР. Данное действие производится на рабочем месте администратора ЦР с использованием программного обеспечения АРМ.
- выпустить сертификат администратора ЦР. Данное действие производится на Центре Регистрации.
- установить сертификат администратора ЦР. Установка сертификата выполняется на рабочем месте администратора ЦР с использованием программного обеспечения АРМ.
- создать подключение к ЦР. Создание подключения к ЦР выполняется на рабочем месте администратора ЦР с использованием программного обеспечения АРМ.

После установки программного обеспечения АРМ администратора ЦР оно настроено для работы с СКЗИ «КриптоПро CSP» по алгоритму ГОСТ Р 34.10-2001.

Если необходимо разрешить выбор криптопровайдера (CSP) при генерации ключей привилегированного пользователя и пользователей ЦР в дальнейшем, то необходимо выбрать пункт Разрешить выбор CSP в окне свойств АРМ администратора (см. Рисунок 79)

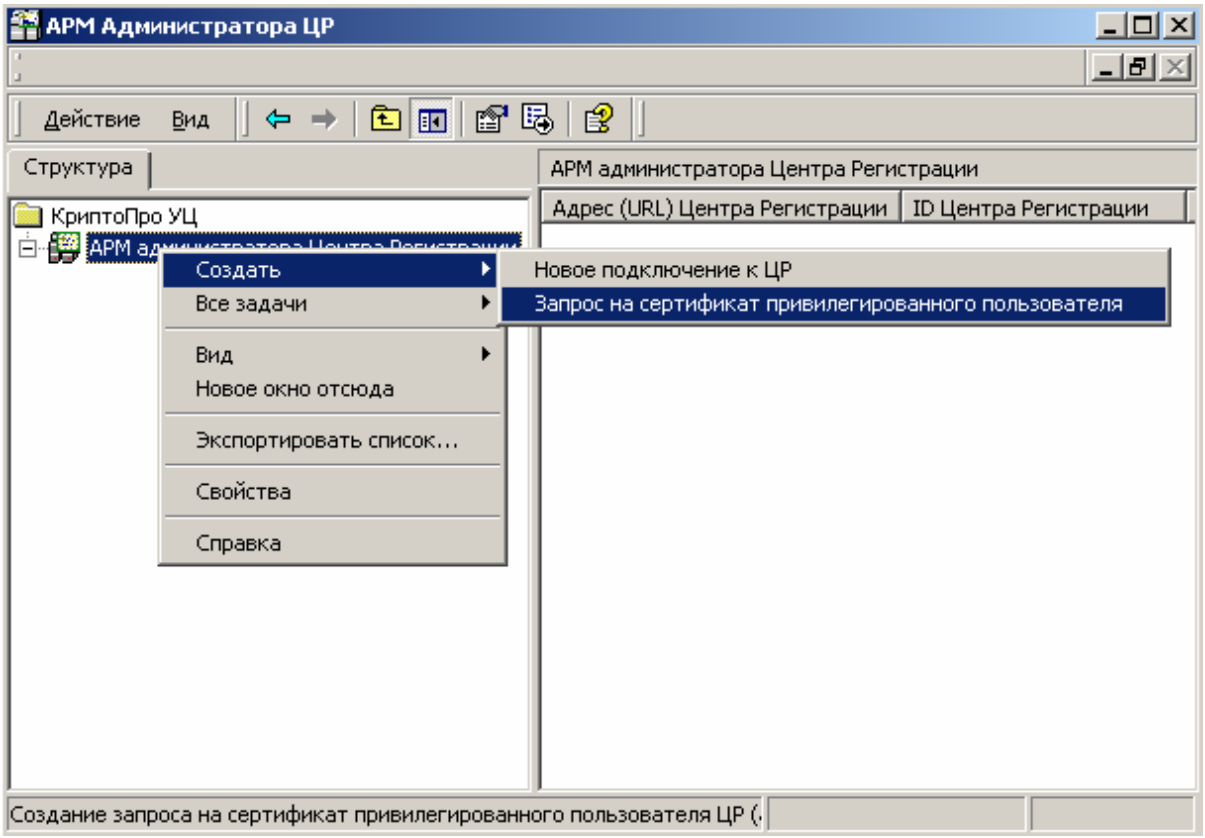
Рисунок 79. Окно свойств АРМ администратора ЦР



Для создания запроса на сертификат администратора ЦР запустите приложение **АРМ администратора ЦР** путем нажатия кнопки **Пуск** и выбора в меню **Программы** пункта **Крипто Про\АРМ Администратора ЦР**.

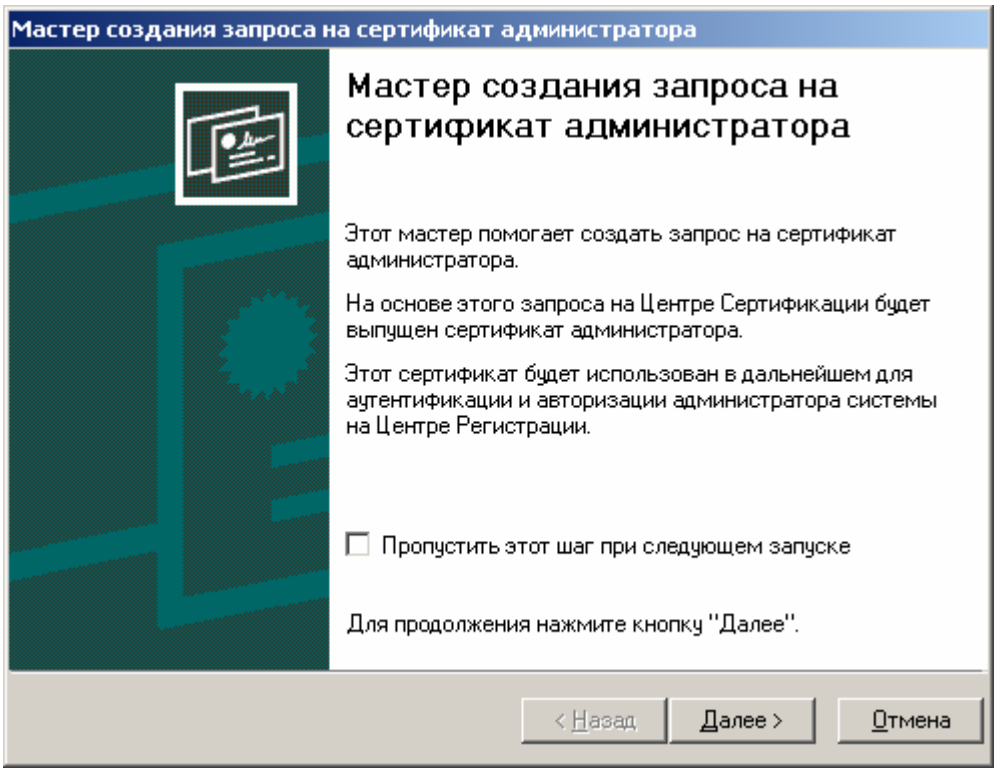
Выполните задачу **Создать -> Запрос на сертификат привилегированного пользователя** (см. Рисунок 80).

Рисунок 80. Запуск задачи создания запроса на сертификат администратора



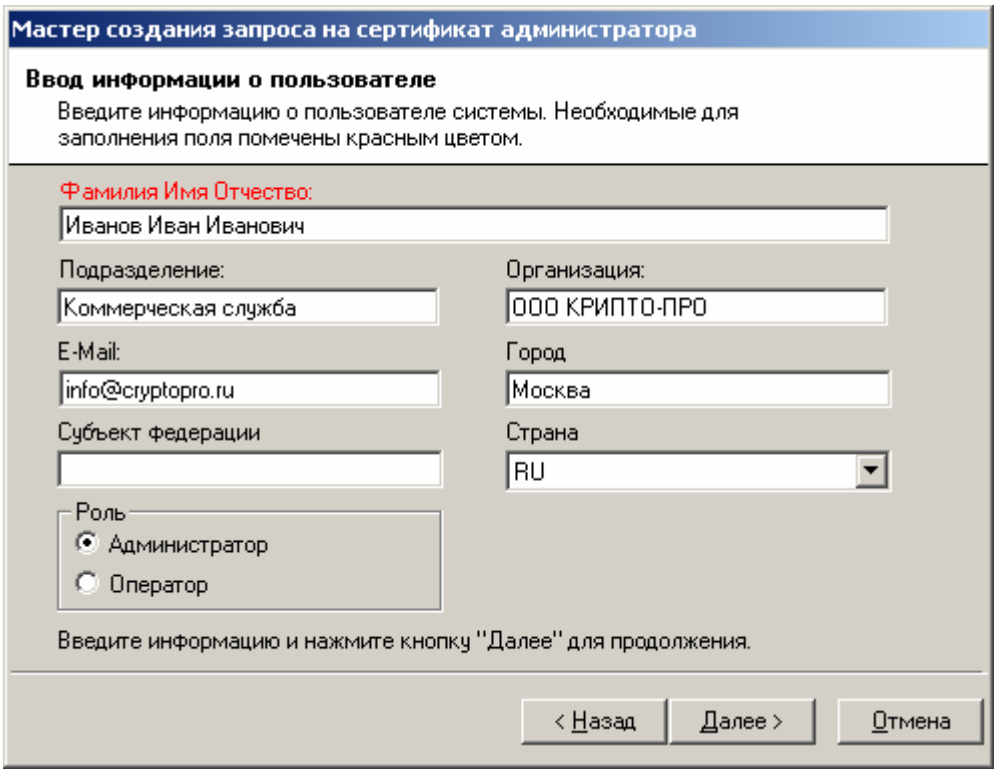
В стартовом окне (см. Рисунок 81) Мастера создания запроса на сертификат администратора нажмите кнопку **Далее**

Рисунок 81. Стартовое окно Мастера создания запроса на сертификат администратора



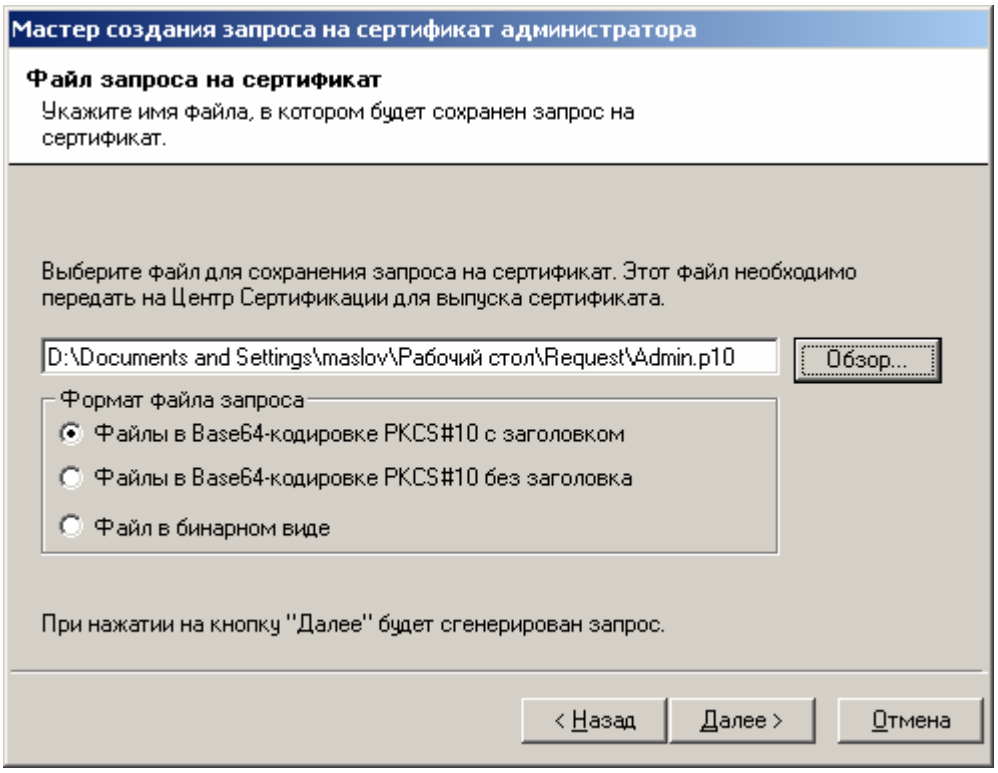
В окне ввода информации о администраторе (см. Рисунок 82) Мастера создания запроса на сертификат администратора необходимо ввести идентификационные данные и выбрать роль привилегированного пользователя (левый нижний угол окна ввода) и нажать кнопку **Далее**.

Рисунок 82. Окно ввода информации о пользователе Мастера создания запроса на сертификат администратора



В окне определения файла запроса на сертификат (см. рис. 83) Мастера создания запроса на сертификат администратора необходимо ввести путь к файлу, в котором будет сохранен запрос на сертификат.

Рисунок 83. Окно выбора файла сохранения запроса Мастера создания запроса на сертификат администратора

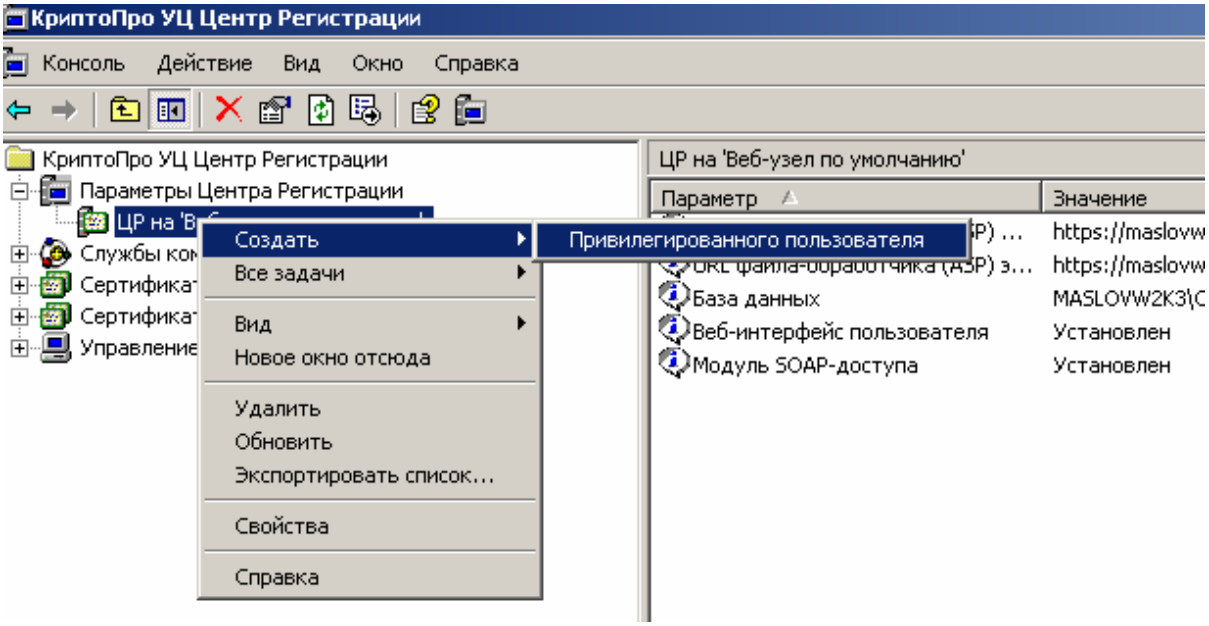


После генерации ключей закройте Мастер нажатием кнопки **Готово**

Сформированный файл запроса на сертификат администратора необходимо передать на Центр Регистрации

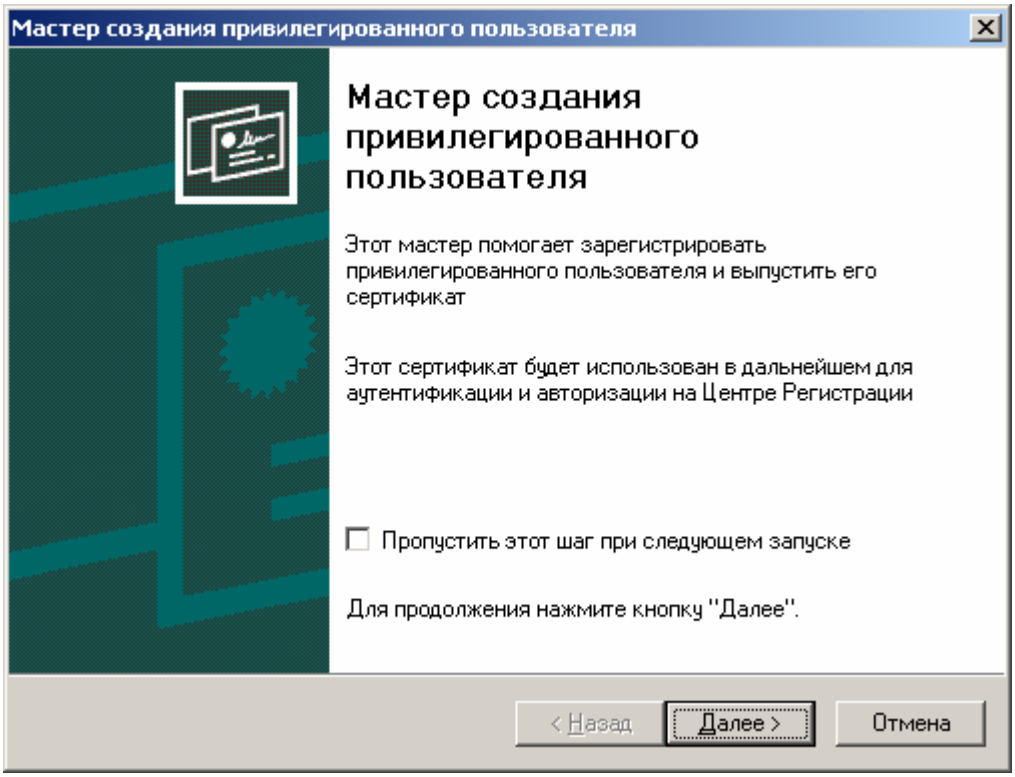
На Центре Регистрации необходимо выполнить задачу **Создать/Привилегированного пользователя** для модуля доступа **ЦР на «Веб-узле по умолчанию»** (см. Рисунок 84)

Рисунок 84. Выполнение задачи создания привилегированного пользователя



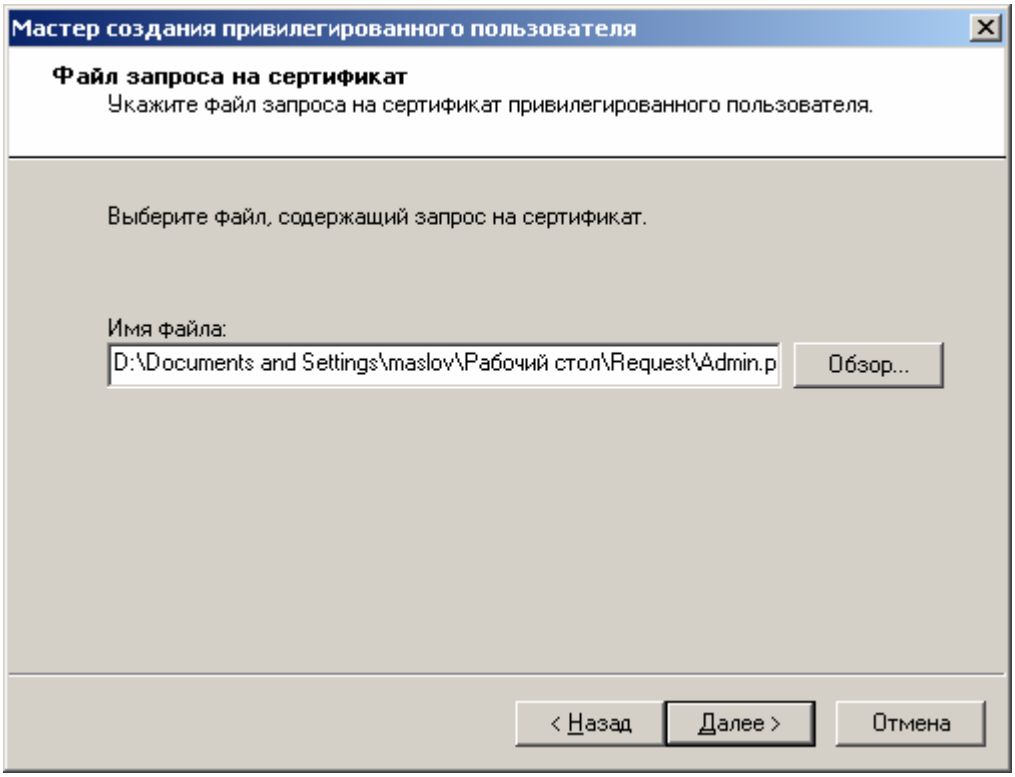
При выполнении указанной задачи будет запущен Мастер создания привилегированного пользователя (см. Рисунок 85)

Рисунок 85. Стартовое окно Мастера создания привилегированного пользователя



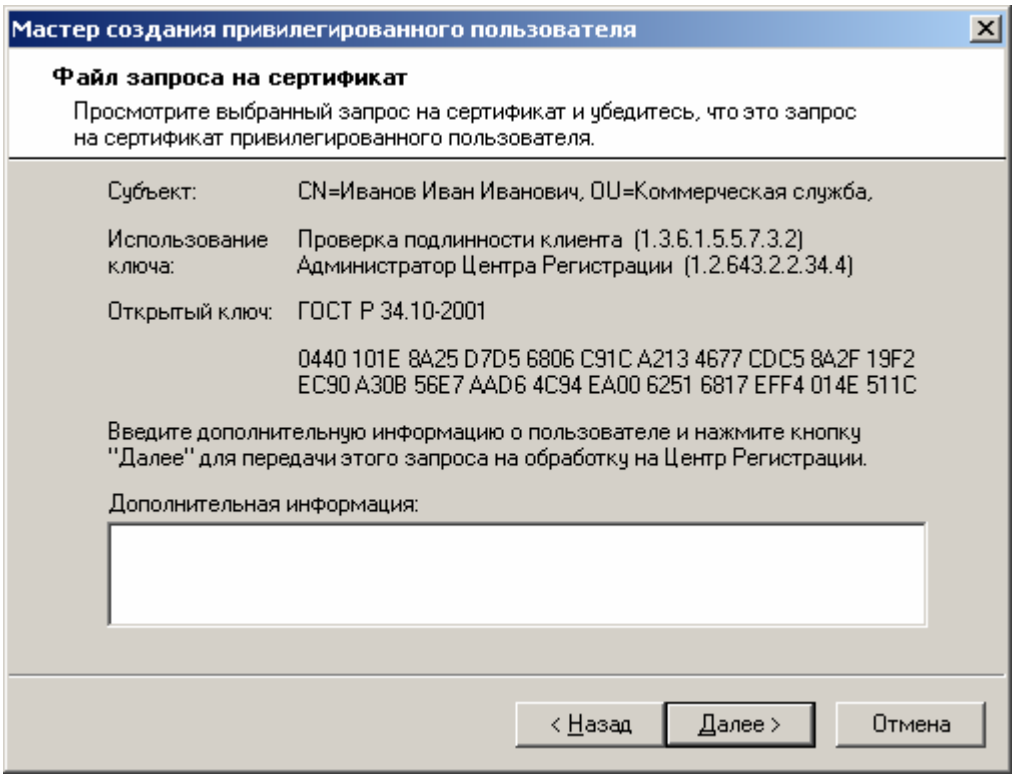
В следующем окне Мастера выберите файл с запросом на сертификат администратора, доставленный на Центр Регистрации (см. Рисунок 86), и нажмите кнопку **Далее**

Рисунок 86. Окно выбора файла запроса Мастера создания привилегированного пользователя



Будет отображено окно (см. Рисунок 87) с содержимым запроса. Необходимо убедиться в корректности информации, находящейся в запросе, при необходимости ввести дополнительную информацию к запросу (она будет занесена в базу данных Центра Регистрации как комментарий к запросу на регистрацию) и нажать кнопку **Далее**

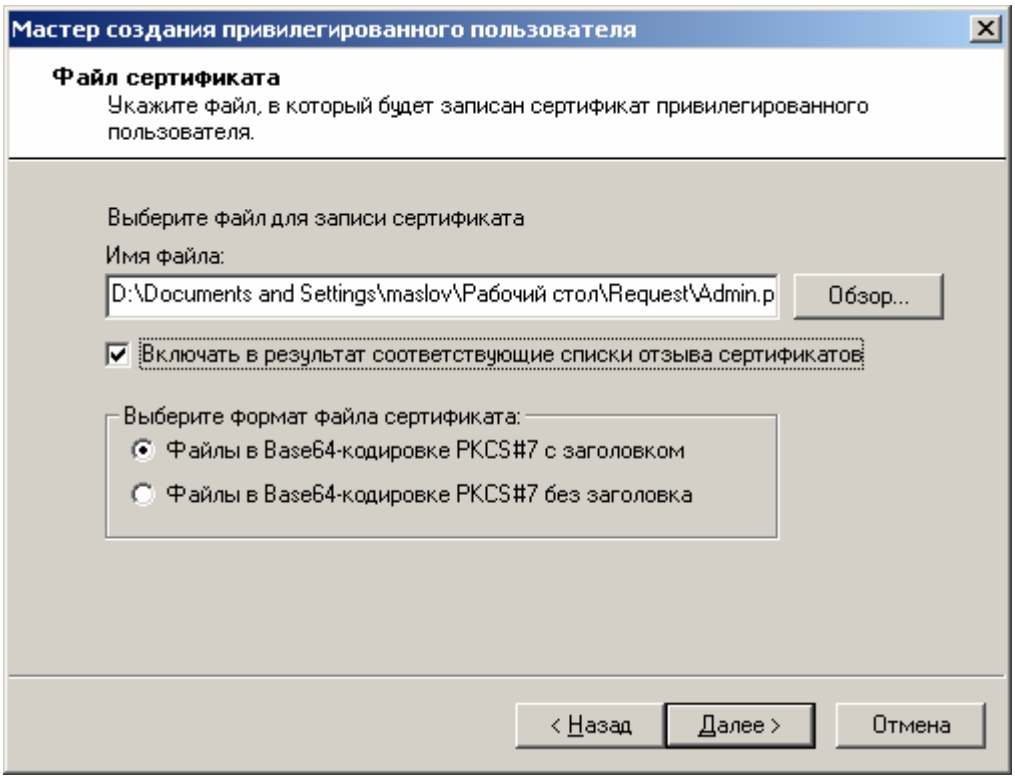
Рисунок 87. Окно информации о запросе Мастера создания привилегированного пользователя



После этого в следующем окне (см. Рисунок 88) необходимо выбрать путь и имя файла, куда будет записан результат в виде цепочки сертификатов и нажать кнопку **Далее**.

Рекомендуется включать в результат списки отзыва сертификатов, путем отметки соответствующего пункта в окне.

Рисунок 88. Окно выбора файла для записи сертификата Мастера создания привилегированного пользователя



В результирующем окне нажмите кнопку **Готово.**

Изготовленный файл необходимо перенести на компьютер АРМ администратора ЦР.

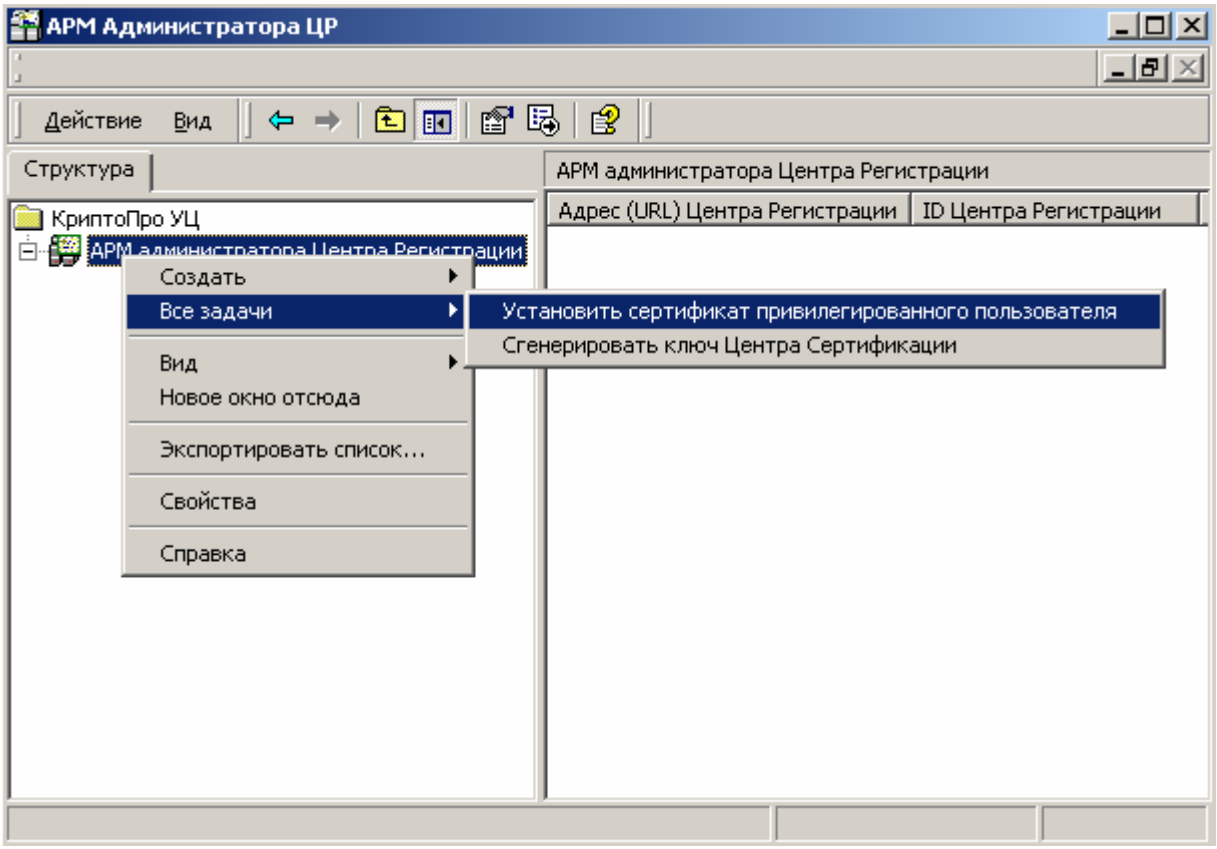
Перед установкой сертификата администратора на рабочем месте необходимо выполнить следующие действия на локальном компьютере с АРМ администратора:

- Установить в список доверенных ЦС хранилища сертификатов текущего пользователя полученный сертификат Центра Сертификации.
- Установить список отозванных сертификатов в хранилище сертификатов текущего пользователя.

В том случае, если изготовленный сертификат администратора, сертификат центра Сертификации и список отозванных сертификатов предоставляются Центром Регистрации в виде одного файла с расширением .p7b, программное обеспечение АРМ администратора автоматически произведет их установку на ПЭВМ.

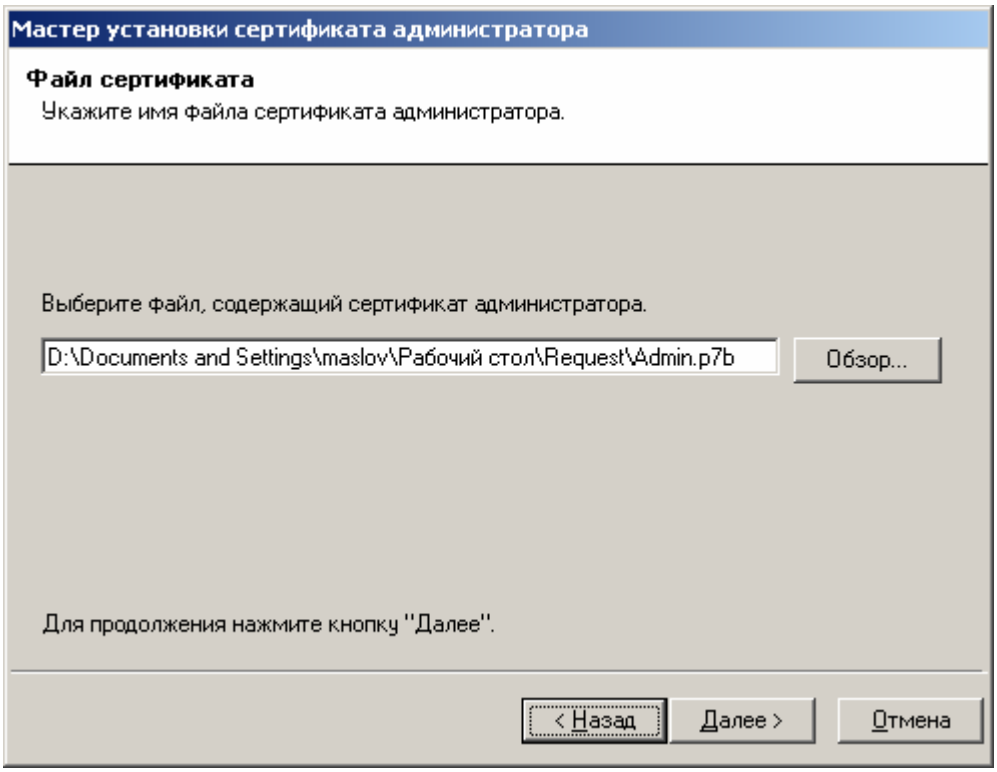
Для установки выпущенного сертификата на рабочем месте Администратора ЦР выполните задачу **Установить сертификат привилегированного пользователя** (см. Рисунок 89).

Рисунок 89. Запуск задачи установки сертификата администратора



В процессе установки укажите файл, полученный с Центра Регистрации и содержащий сертификат администратора (см. Рисунок 90).

Рисунок 90. Окно выбора файла с сертификатом Мастера установки сертификата администратора

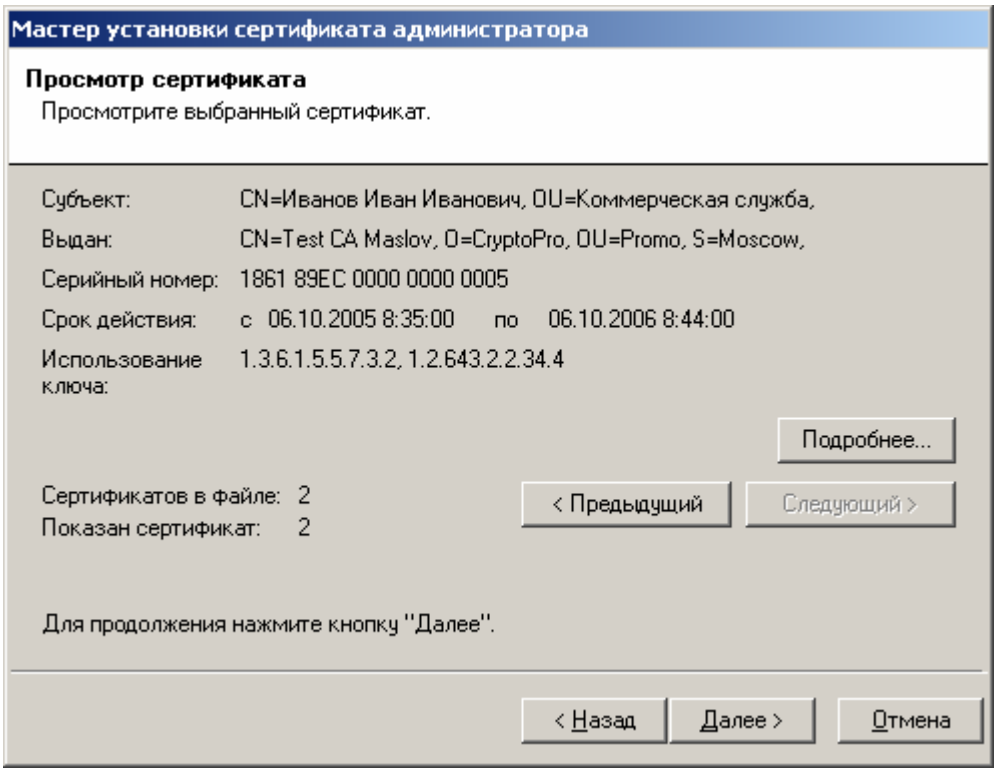


В следующем окне Мастера установки сертификата администратора убедитесь в том, что устанавливается сертификат, соответствующий запросу (см. Рисунок 91) Для просмотра сертификата(ов) издателя(ей) (сертификата(ов) Центра Сертификации) используются кнопки

Следующий> и **<Предыдущий**, а также кнопка **Подробнее** для детализации информации о текущем сертификате в цепочке сертификатов.

Отсутствие других сертификатов в цепочке, кроме сертификата администратора (**сертификатов в файле: 1**), говорит о том, что с Центра Регистрации поступил файл не с цепочкой сертификатов, а файл только с сертификатом администратора. Тем не менее это не препятствует установке сертификата администратора с помощью Мастера.

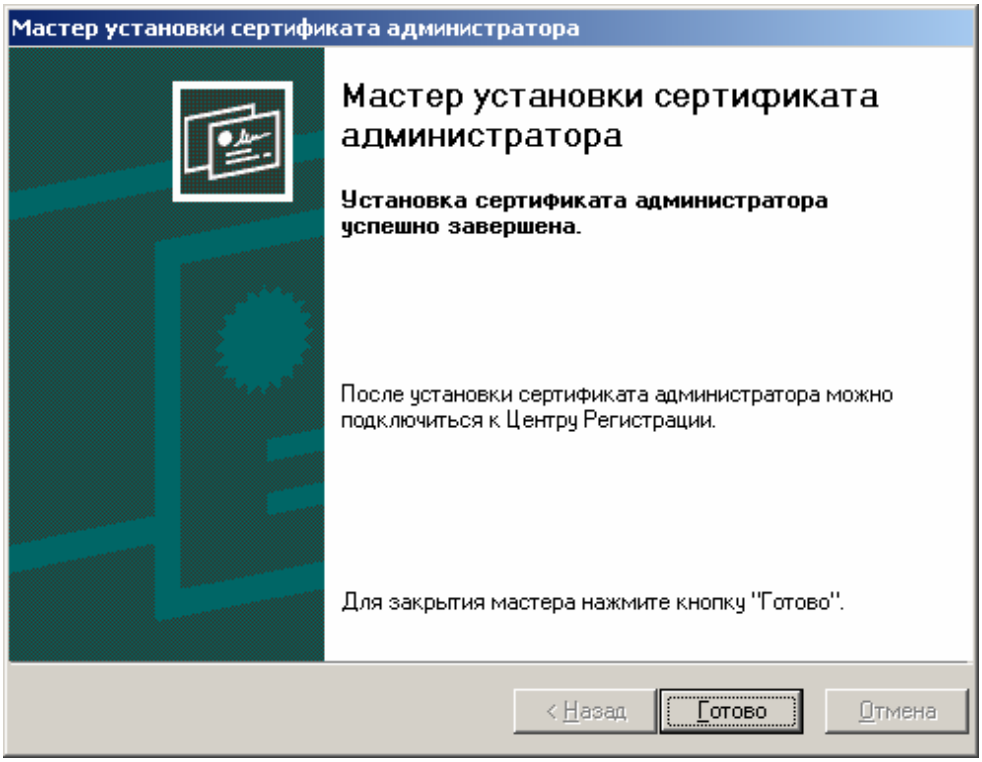
Рисунок 91. Окно просмотра сертификата Мастера установки сертификата администратора



После нажатия кнопки **Далее** выполняется установка сертификата администратора в раздел Личные хранилища сертификатов текущего пользователя для последующего использования в АРМ администратора при создании подключения к Центру Регистрации.

Об успешном завершении записи сертификата на рабочее место свидетельствует появление окна Мастера (см. Рисунок 92).

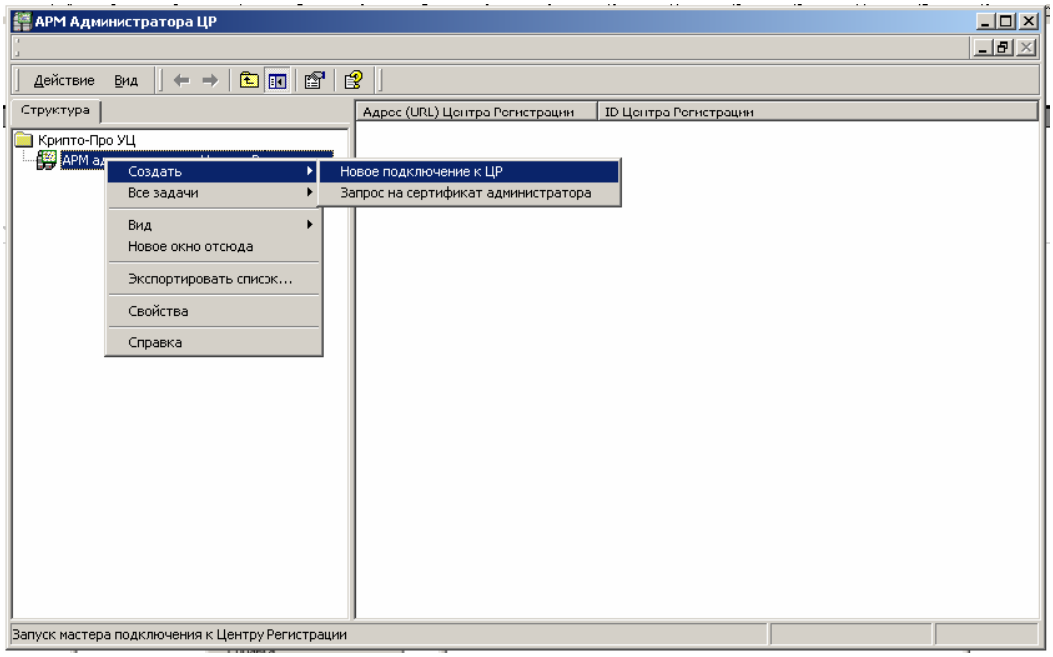
Рисунок 92. Окно завершения установки сертификата администратора



В противном случае будет выдано соответствующее диагностическое окно Мастера с сообщением об ошибке.

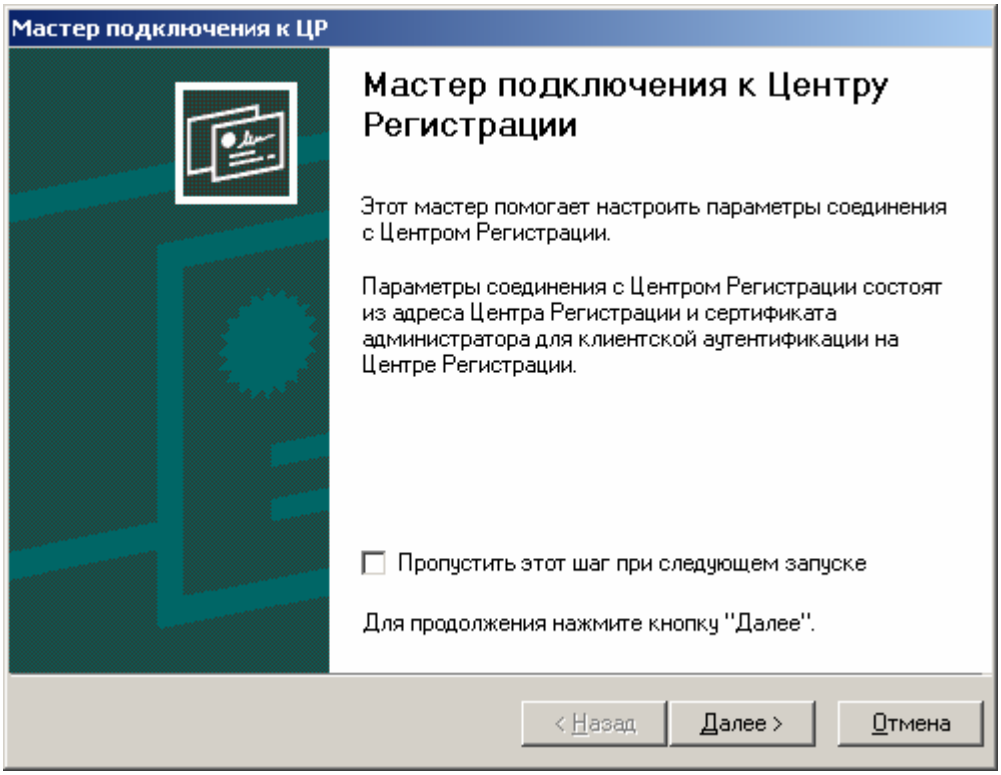
После выполнения установки сертификата необходимо перейти к созданию подключения к ЦР. Для этого требуется запустить на выполнение задачу **Новое подключение к ЦР** (см. Рисунок 93).

Рисунок 93. Запуск задачи создания подключения к ЦР



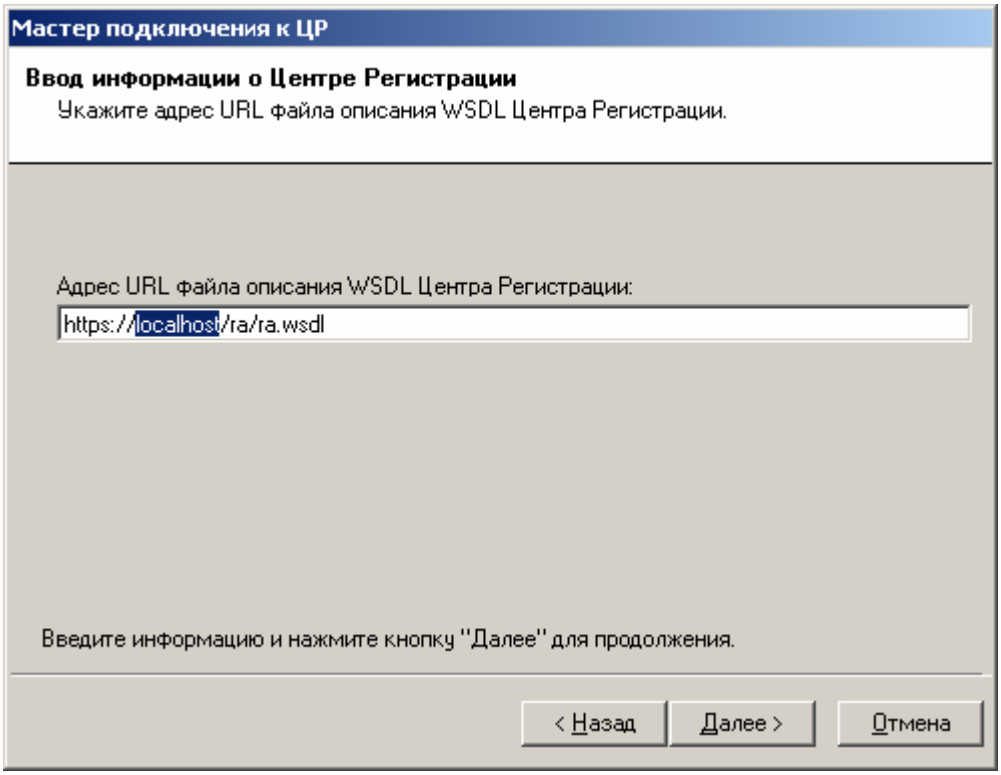
Создание подключения осуществляется с помощью Мастера подключения к ЦР (см. Рисунок 94).

Рисунок 94. Мастер подключения к ЦР



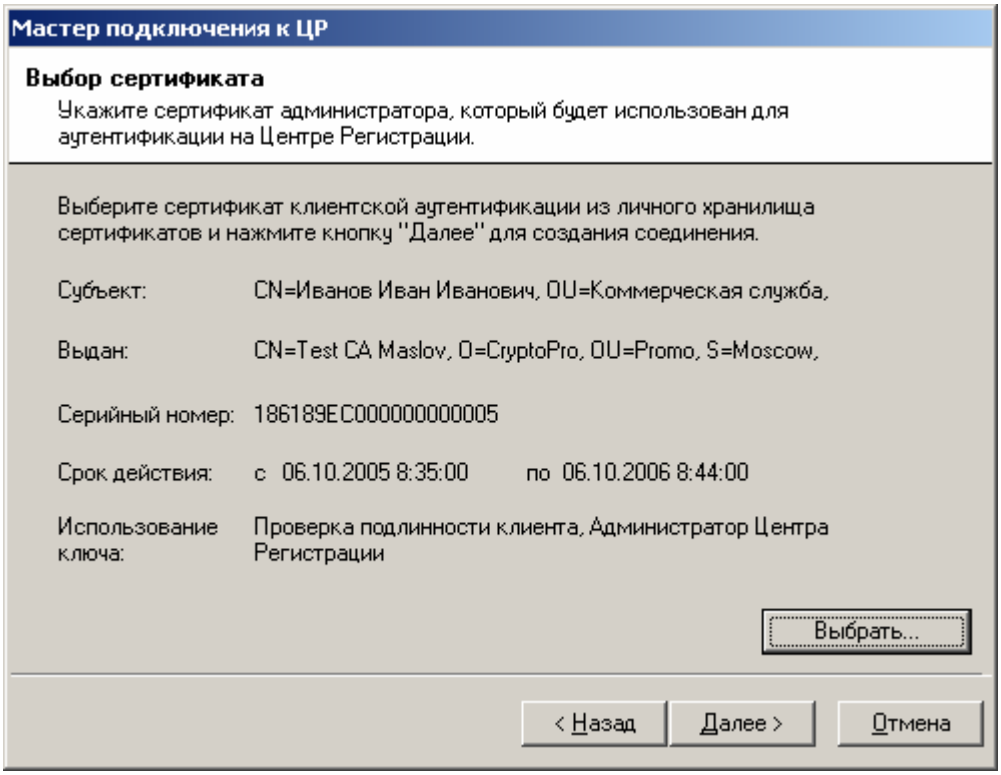
В ходе подключения необходимо ввести URL Web-сервиса Центра регистрации (файла RA.WSDL), с которым будет работать АРМ (см. Рисунок 95).

Рисунок 95. Задание адреса ЦР в Мастере подключения к ЦР



В следующем окне Мастера необходимо выбрать сертификат администратора (см. Рисунок 96). Для выбора сертификата администратора нажмите кнопку **Выбрать**.

Рисунок 96. Выбор сертификата администратора в Мастере подключения к ЦР



ПО АРМ администратора Центра Регистрации не ограничивает в количестве подключений к одному или нескольким ЦР. Прочие подключения к ЦР создаются в описанном выше порядке. Но активным может быть только одно из созданных подключений.

6. Установка АРМ разбора конфликтных ситуаций

6.1. Последовательность установки АРМ разбора конфликтных ситуаций

Установка и конфигурация программного обеспечения АРМ разбора конфликтных ситуаций из состава программного комплекса УЦ производится в следующей последовательности:

1. Установка СКЗИ КриптоПро CSP
2. Установка программного обеспечения АРМ разбора конфликтных ситуаций

6.2. Установка СКЗИ КриптоПро CSP

На АРМ разбора конфликтных ситуаций с установленной ОС из следующего перечня: MS Windows 2000 Professional, MS Windows Server 2000 и MS Windows XP, устанавливается СКЗИ КриптоПро CSP (версия 2.0) в составе согласно формуляра ЖТЯИ.00005-02 30 01, вариант исполнения 4 или СКЗИ КриптоПро CSP (версия 3.0) в составе согласно формуляра ЖТЯИ.00015-01 30 01, вариант исполнения 6.

На АРМ разбора конфликтных ситуаций с установленной ОС MS Windows Server 2003 устанавливается СКЗИ КриптоПро CSP (версия 3.0) в составе согласно формуляра ЖТЯИ.00015-01 30 01, вариант исполнения 6.

Установка СКЗИ «КриптоПро CSP» осуществляется в соответствии с эксплуатационной документацией.

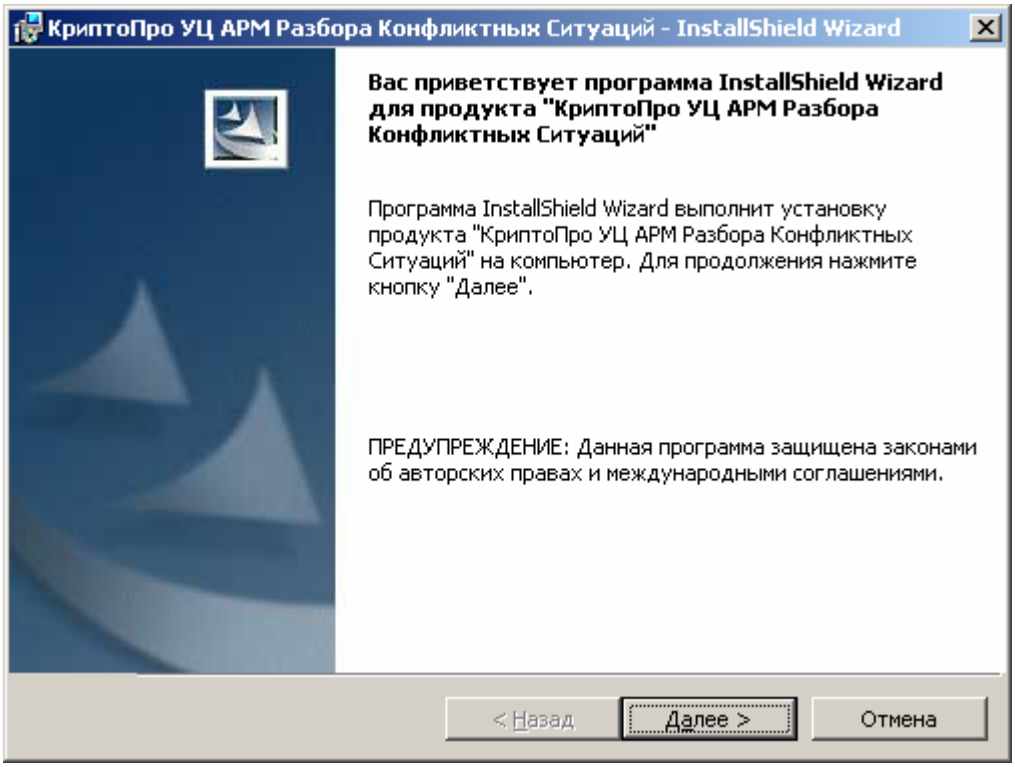
После установки программного обеспечения СКЗИ «КриптоПро CSP» необходимо активировать лицензию на продукт из набора лицензий поставки ПАК «КриптоПро УЦ» и включить режим **кеширования** (вкладка **Безопасность** окна свойств КриптоПро CSP).

6.3. Установка программного обеспечения АРМ разбора конфликтных ситуаций

Для установки ПО АРМ разбора конфликтных ситуаций необходимо выполнить программу установки **SETUP.EXE**, расположенную на CD дистрибутива.

После запуска программа установки выведет на экран диалоговое окно подтверждения продолжения установки (см. Рисунок 97).

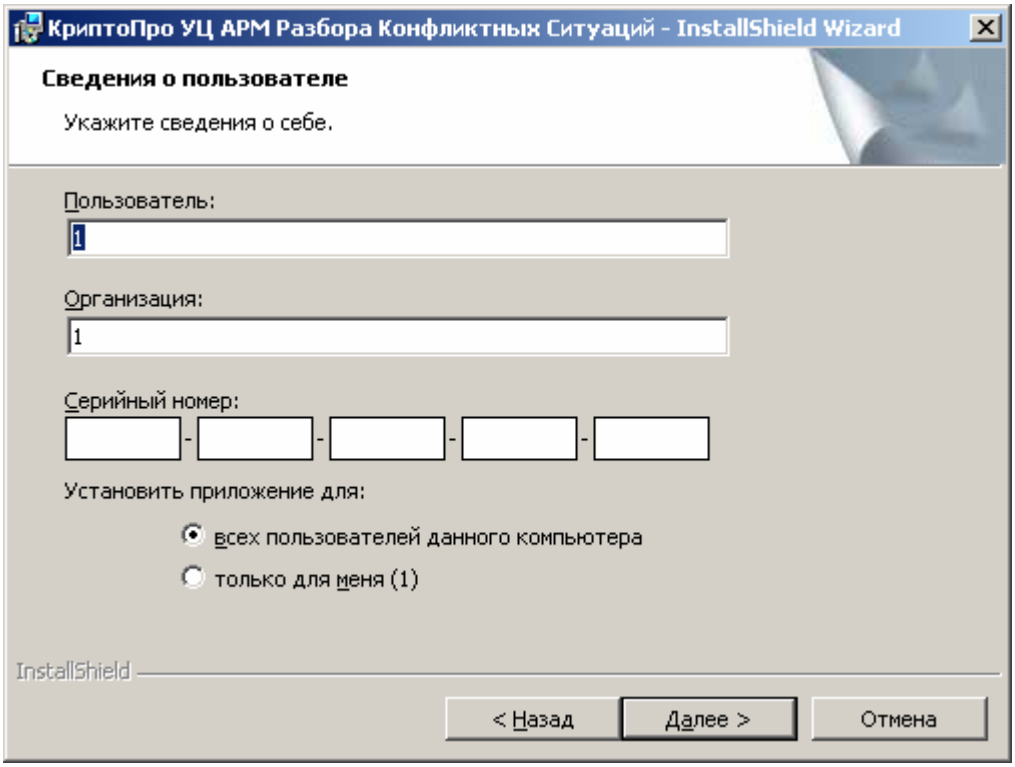
Рисунок 97. Окно Мастера установки ПО АРМ разбора конфликтных ситуаций



Для продолжения установки ПО АРМ разбора конфликтных ситуаций необходимо нажать кнопку **Далее**.

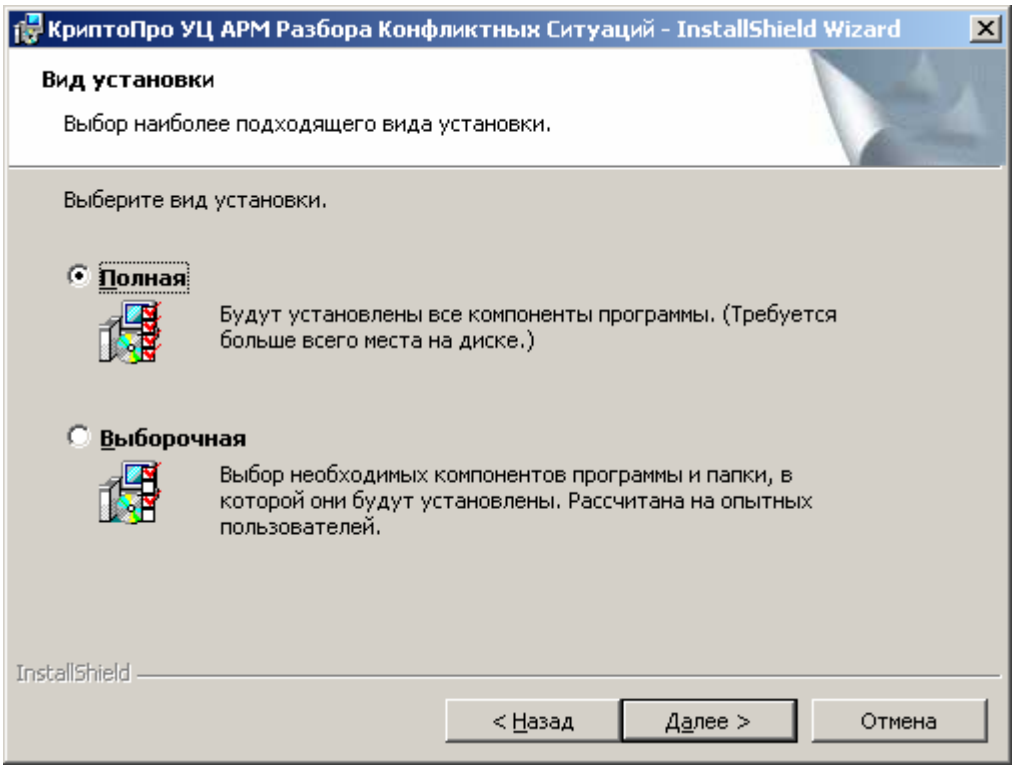
В следующем окне необходимо ввести информацию о пользователе, производящем установку ПО, наименование организации и номер лицензии (см. Рисунок 98).

Рисунок 98. Окно сведений о пользователе Мастера установки АРМ разбора конфликтных ситуаций



После нажатия кнопки **Далее** на экран будет выведено диалоговое окно, в котором необходимо определить тип установки ПО (см. Рисунок 99).

Рисунок 99. Окно определения типа установки Мастера установки АРМ разбора конфликтных ситуаций



Вид установки **Полная** производит установку программного обеспечения АРМ разбора конфликтных ситуаций в папку назначения, определенную по умолчанию. Таковой папкой является **Program Files\Crypto Pro** системного диска локального компьютера.

Для изменения текущей папки назначения необходимо выбрать вид установки **Выборочная**.

После определения начальных параметров Мастера установки на экран выводится диалоговое окно, в котором инициируется собственно операция установки.

Для продолжения установки нажмите кнопку **Установить**. Для изменения ранее введенных параметров установки нажмите кнопку **Назад**.

При выполнении операций установки, состояние процесса отображается в окне на экране.

Успешное завершение процесса установки ПО АРМ разбора конфликтных ситуаций должно подтвердится сообщением Мастера установки.

7. 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

8. Перечень рисунков

Рисунок 1. Схема взаимодействия компонентов ПАК «КриптоПро УЦ»....5
Рисунок 2. Установка служб IIS и службы очередей сообщений 10
Рисунок 3. Конфигурация ЦС в режиме «Корневой» для Windows Server 2003....12
Рисунок 4. Выбор параметров генерации ключа ЦС....13
Рисунок 5. Сведения о центре сертификации в режиме «Корневой» для Windows Server 2000 . 14
Рисунок 6. Сведения о центре сертификации в режиме «Корневой» для Windows Server 2003 . 14
Рисунок 7. Конфигурация ЦС в режиме «Подчиненный» » для Windows Server 2000 15
Рисунок 8. Сведения о центре сертификации в режиме «Подчиненный» 16
Рисунок 9. Запрос на сертификат ЦС 16
Рисунок 10. Сообщение о порядке продолжения установки службы сертификации 17
Рисунок 11. Консоль управления службы сертификации....17
Рисунок 12. Запуск задачи установки сертификата ЦС в консоли управления 18
Рисунок 13. Окно Мастера установки утилит Центра сертификации....18
Рисунок 14. Выбор вида установки Утилит Центра Сертификации 19
Рисунок 15. Группа "Крипто-Про" меню "Программы"....19
Рисунок 16. Окно Мастера создания запроса на сертификат WEB-сервера ЦС 20
Рисунок 17. Окно ввода информации о Web-сервере ЦС Мастера создания запроса на сертификат....20
Рисунок 18. Окно выбора CSP в Мастере создания запроса на сертификат....21
Рисунок 19. Окно выбора способа получения сертификата WEB-сервера ЦС в Мастере....22
Рисунок 20. Окно уведомления о необходимости выпуска сертификата по запросу на службе сертификации....22
Рисунок 21. Выдача сертификата по запросу в оснастке службы сертификации 23
Рисунок 22. Окно завершения работы Мастера выпуска сертификата Web-сервера ЦС 23
Рисунок 23. Открытие окна свойств Веб-узла по умолчанию MS IIS....24
Рисунок 24. Вкладка "Безопасность каталога" Web-узла по умолчанию 25
Рисунок 25. Пример диагностического сообщения ПО дистрибутива ЦС 26
Рисунок 26. Мастер установки ПО Центра сертификации....26
Рисунок 27. Сведения о пользователе ПО ЦС....27
Рисунок 28. Вид установки ПО ЦС 28
Рисунок 29. Вид установки «Выборочная» 28
Рисунок 30. Внешний адрес Центра сертификации....29
Рисунок 31. Пароль учетной записи Центра Сертификации....30
Рисунок 32. Окно подтверждения установки ПО ЦС 30
Рисунок 33. Окно состояния процесса установки ПО ЦС 31
Рисунок 34 . Информационное окно предупреждения мастера установки ЦС....31
Рисунок 35. Окно Мастера установки утилит Центра Регистрации....33
Рисунок 36. Выбор вида установки Утилит Центра Регистрации....33

Рисунок 37. Группа "Крипто-Про" меню "Программы" 34
Рисунок 38. Окно Мастера создания запроса на сертификат WEB-сервера ЦР 34
Рисунок 39. Окно ввода информации о Web-сервере ЦР Мастера создания запроса на сертификат 35
Рисунок 40. Окно выбора CSP в Мастере создания запроса на сертификат 36
Рисунок 41. Окно определения файла запроса в Мастере создания запроса на сертификат 36
Рисунок 42. Стартовое окно Мастера выпуска сертификата Web-сервера ЦР 37
Рисунок 43. Окно выбора файла запроса Мастера выпуска сертификата Web-сервера ЦР 37
Рисунок 44. Окно просмотра запроса Мастера выпуска сертификата Web-сервера ЦР 38
Рисунок 45. Окно получения сертификата Мастера выпуска сертификата Web-сервера ЦР 38
Рисунок 46. Окно Мастера установки сертификата WEB-сервера ЦР 39
Рисунок 47. Окно отображения информации о сертификате в Мастере установки сертификата WEB-сервера ЦР 40
Рисунок 48. Пример диагностического сообщения программы установки ЦР 41
Рисунок 49. Мастер установки ПО Центра Регистрации 41
Рисунок 50. Сведения о пользователе ПО ЦР 42
Рисунок 51. Вид установки ПО ЦР 43
Рисунок 52. Вид установки «Выборочная» 44
Рисунок 53. Внешний адрес Центра Регистрации 45
Рисунок 54. Окно определения пароля учетной записи Центра Регистрации Мастера установки ПО ЦР 45
Рисунок 55. Окно подтверждения установки ПО ЦР 46
Рисунок 56. Окно состояния процесса установки ПО ЦР 46
Рисунок 57. Окно Мастера создания запроса на клиентский сертификат ЦР 47
Рисунок 58. Окно ввода информации о ЦР 48
Рисунок 59. Окно выбора CSP в Мастере создания запроса на клиентский сертификат ЦР 48
Рисунок 60. Окно выбора файла запроса на сертификат ЦР 49
Рисунок 61. Стартовое окно Мастера выпуска клиентского сертификата ЦР 50
Рисунок 62. Окно выбора файла запроса Мастера выпуска клиентского сертификата ЦР 50
Рисунок 63. Окно просмотра запроса Мастера выпуска клиентского сертификата ЦР 51
Рисунок 64. Окно получения сертификата Мастера выпуска клиентского сертификата ЦР 51
Рисунок 65. Вкладка "Центры регистрации" окна настроек приложения "Параметры Центра Сертификации" 52
Рисунок 66. Окно доверенных Центров Регистрации 53
Рисунок 67. Мастер установки клиентского сертификата Центра Регистрации 53
Рисунок 68. Окно выбора сертификата ЦР в Мастере установки 54
Рисунок 69. Окно просмотра выбранного сертификата ЦР в Мастере установки 54
Рисунок 70. Окно успешной установки сертификата ЦР в Мастере установки 55
Рисунок 71. Пункт "Свойства" узла Центра Регистрации 56
Рисунок 72. Вкладка «Общие» окна свойств Центра Регистрации 57
Рисунок 73. Окно Мастера установки ПО АРМ администратора 59

Рисунок 74. Окно ввода информации о пользователе, организации и серийного номера лицензии Мастера установки АРМ администратора 60

Рисунок 75. Окно определения типа установки Мастера установки АРМ администратора 60

Рисунок 76. Окно подтверждения установки ПО Мастера установки АРМ администратора 61

Рисунок 77. Окно состояния установки Мастера установки АРМ администратора 61

Рисунок 78. Окно окончания работы Мастера установки АРМ администратора 62

Рисунок 79. Окно свойств АРМ администратора ЦР 63

Рисунок 80. Запуск задачи создания запроса на сертификат администратора 64

Рисунок 81. Стартовое окно Мастера создания запроса на сертификат администратора 64

Рисунок 82. Окно ввода информации о пользователе Мастера создания запроса на сертификат администратора 65

Рисунок 83. Окно выбора файла сохранения запроса Мастера создания запроса на сертификат администратора 65

Рисунок 84. Выполнение задачи создания привилегированного пользователя 66

Рисунок 85. Стартовое окно Мастера создания привилегированного пользователя 66

Рисунок 86. Окно выбора файла запроса Мастера создания привилегированного пользователя 67

Рисунок 87. Окно информации о запросе Мастера создания привилегированного пользователя 67

Рисунок 88. Окно выбора файла для записи сертификата Мастера создания привилегированного пользователя 68

Рисунок 89. Запуск задачи установки сертификата администратора 69

Рисунок 90. Окно выбора файла с сертификатом Мастера установки сертификата администратора 69

Рисунок 91. Окно просмотра сертификата Мастера установки сертификата администратора 70

Рисунок 92. Окно завершения установки сертификата администратора 71

Рисунок 93. Запуск задачи создания подключения к ЦР 71

Рисунок 94. Мастер подключения к ЦР 72

Рисунок 95. Задание адреса ЦР в Мастере подключения к ЦР 72

Рисунок 96. Выбор сертификата администратора в Мастере подключения к ЦР 73

Рисунок 97. Окно Мастера установки ПО АРМ разбора конфликтных ситуаций 75

Рисунок 98. Окно сведений о пользователе Мастера установки АРМ разбора конфликтных ситуаций 75

Рисунок 99. Окно определения типа установки Мастера установки АРМ разбора конфликтных ситуаций 76