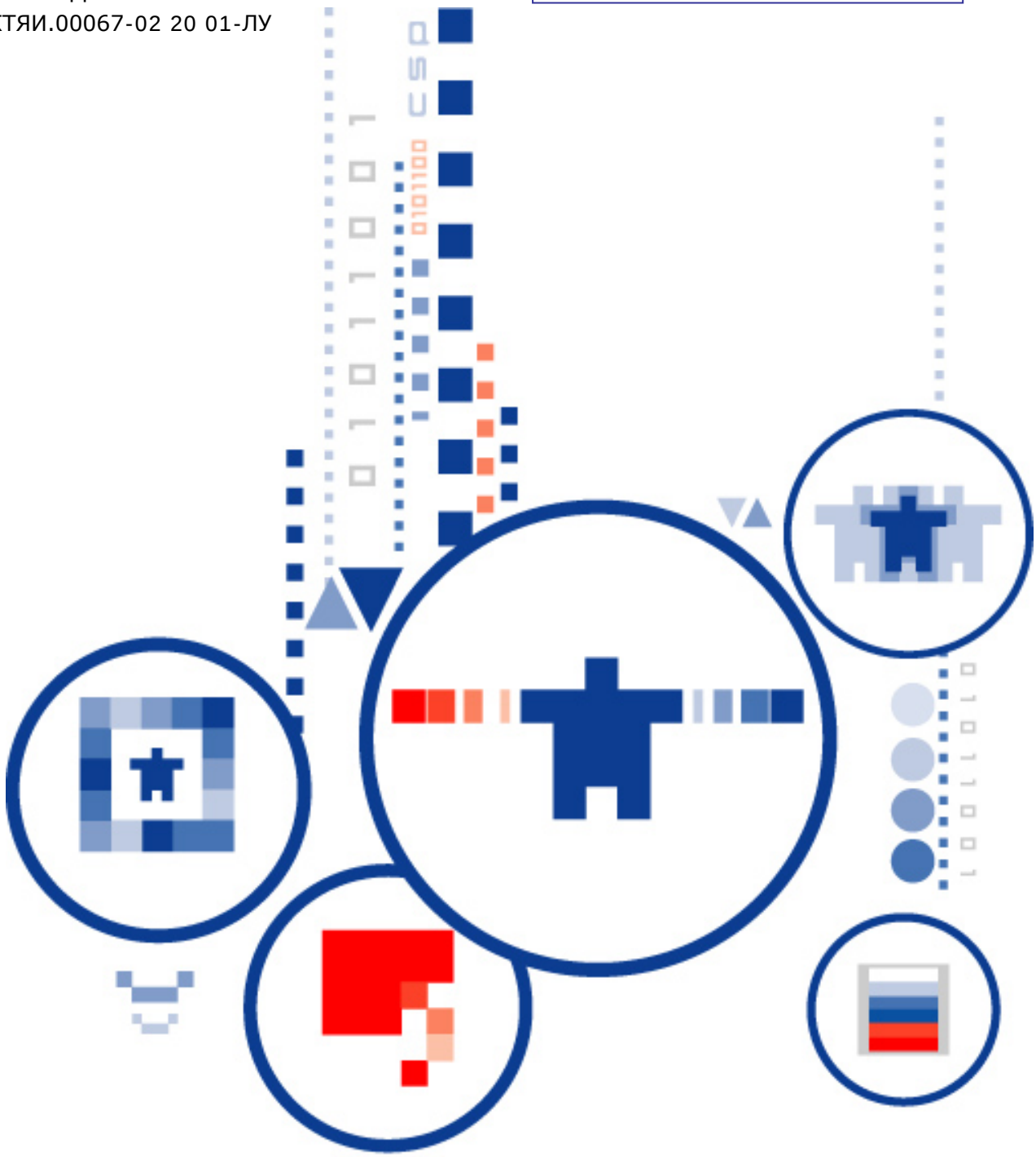
ЖТЯИ.00067-02 90 07

УТВЕРЖДЕН
ЖТЯИ.00067-02 20 01-ЛУ



КриптоПро УЦ

программно–аппаратный комплекс
удостоверяющий центр

Автоматизированное рабочее место администратора Центра Регистрации. Практическая реализация регламентных процедур по регистрации пользователей и управлению сертификатами открытых ключей

АННОТАЦИЯ

Настоящий документ содержит описание выполнения регламентных процедур, осуществляемых привилегированным пользователем Центра Регистрации с использованием программного обеспечения АРМ администратора ЦР.

Данное руководство предназначено для привилегированных пользователей Центра Регистрации, занимающихся регистрацией пользователей, изготовлением и управлением сертификатами открытых ключей пользователей.

Информация о разработчике ПАК «КриптоПро УЦ»:

ООО "Крипто-Про"
127 018, Москва, улица Сущевский вал, 16 строение 5
Телефон: (495) 780 4820
Факс: (495) 780 4820
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

СОДЕРЖАНИЕ

1. Практическая реализация регламентных процедур с использованием АРМ администратора ЦР

1.1. Пользователи и Роли Удостоверяющего Центра

Каждый пользователь, зарегистрированный в Удостоверяющем Центре, ассоциирован с определенной системной ролью. Сопоставление пользователя системной роли осуществляется посредством занесения в сертификат ключа подписи, владельцем которого является пользователь, сведений об указанной роли. Эти сведения заносятся в поле **Extended Key Usage** (**Улучшенный ключ**) сертификата, которое содержит номера объектных идентификаторов (OID'ов) используемых системных ролей.

1.1.1. Применение ролевой модели

Сопоставление каждого пользователя определенной системной роли позволяет осуществить разграничение доступа к объектам Удостоверяющего Центра, наделить пользователей полномочиями по выполнению определенных действий по управлению как личными сертификатами ключей подписи, так и сертификатами других пользователей.

Удостоверяющий Центр обеспечивает реализацию следующих предустановленных ролей:

- **Прошедший проверку;**
- **Временный сертификат;**
- **Пользователь;**
- **Оператор;**
- **Администратор;**
- **Администратор аудита.**

1.1.2. Привилегированные пользователи

Из приведенного в предыдущем пункте списка ролей две роли – **Администратор** и **Оператор** являются привилегированными и предназначены для обеспечения реализации процедур регистрации пользователей в Удостоверяющем Центре и управления изданными сертификатами ключа подписи. Средством обеспечения указанных процедур является программное обеспечение **АРМ администратора Центра Регистрации**.

По умолчанию, роли **Оператор** отводится выполнение функций по регистрации пользователя в Удостоверяющем Центре и изготовления ему первого сертификата ключа подписи. На пользователя, ассоциированного с ролью **Администратор,** возлагаются задачи по осуществлению процедур плановой и внеплановой смены ключей и сертификатов ключей подписи, аннулированию, приостановлению/возобновлению действия сертификатов ключей подписи и иных сервисных функций.

В общем случае, посредством настроек политик безопасности Удостоверяющего Центра, набор действий, разрешенных для пользователей указанных привилегированных ролей, может быть установлен в соответствии с Регламентом Удостоверяющего Центра, а также действующими положением об Удостоверяющем Центре и должностными инструкциями Администратора и Оператора Удостоверяющего Центра.

Администратор аудита осуществляет просмотр, анализ объектов управления Центра регистрации, сохранение и просмотр сохраненного ранее журнала регистрации событий Центра регистрации.

Администратор Аудита обеспечивает выполнение следующих задач:

- просмотр и обработка (анализ) объектов управления Центра регистрации;
- сохранение и подпись журнала регистрации событий Центра регистрации;

- просмотр подписанных журналов регистрации событий Центра регистрации.

В общем случае, посредством настроек политик безопасности Удостоверяющего Центра, набор действий, разрешенных для пользователей указанных привилегированных ролей, может быть установлен в соответствии с Регламентом Удостоверяющего Центра, а также действующими положением об Удостоверяющем центре и должностными инструкциями Администратора, Оператора и Администратора аудита Удостоверяющего Центра.

1.2. Регистрация пользователей

Регистрация пользователей в Удостоверяющем Центре осуществляется **Оператором** (при использовании настроек по умолчанию) и может быть осуществлена в двух режимах: централизованном и распределенном. Выбор режима регистрации определяется владельцем Удостоверяющего Центра и устанавливается Регламентом Удостоверяющего Центра.

Централизованная регистрация пользователя осуществляется при личном прибытии регистрирующегося лица (либо его уполномоченного представителя, действующего на основании соответствующей доверенности) в Удостоверяющий Центр. Распределенная, напротив, позволяет осуществить регистрацию без прибытия в Удостоверяющий Центр, что удобно, например, при значительной территориальной удаленности Удостоверяющего Центра и конечных пользователей.

1.2.1. Регистрация пользователей в централизованном режиме.

Регистрация пользователя в централизованном режиме осуществляется при личном прибытии регистрирующегося лица (либо его уполномоченного представителя) в Удостоверяющий Центр.

Основанием для регистрации пользователя в Удостоверяющем Центре является Заявление на регистрацию, составленное и заверенное установленным Регламентом Удостоверяющего Центра образом и содержащее идентификационные данные регистрирующегося лица.

Процедура регистрации в Удостоверяющем Центре состоит из двух этапов: занесение идентификационной информации регистрирующегося лица в реестр пользователей Удостоверяющего Центра и изготовление первого сертификата ключа подписи.

Изготовление первого сертификата ключа подписи может осуществляться как с генерацией ключей в Удостоверяющем Центре, так и на основании запроса на сертификат, предоставляемого пользователем в Удостоверяющий Центр в виде файла (в последнем случае генерацию ключей осуществляет сам пользователь).

Изготовление первого сертификата ключа подписи должно также осуществляться на основании Заявления – Заявления на изготовление сертификата ключа подписи.

Заявление на изготовление сертификата оформляется установленным Регламентом образом и должно содержать:

- идентификационные данные лица, на чье имя требуется изготовить сертификат;
- набор областей использования ключа и соответствующие этим областям объектные идентификаторы – OID'ы (содержание поля Extended Key Usage сертификата – наименование областей использования);
- В случае изготовления сертификата на основе предоставленного в виде файла запроса на сертификат – установленным образом оформленный бланк запроса на сертификат ключа подписи.

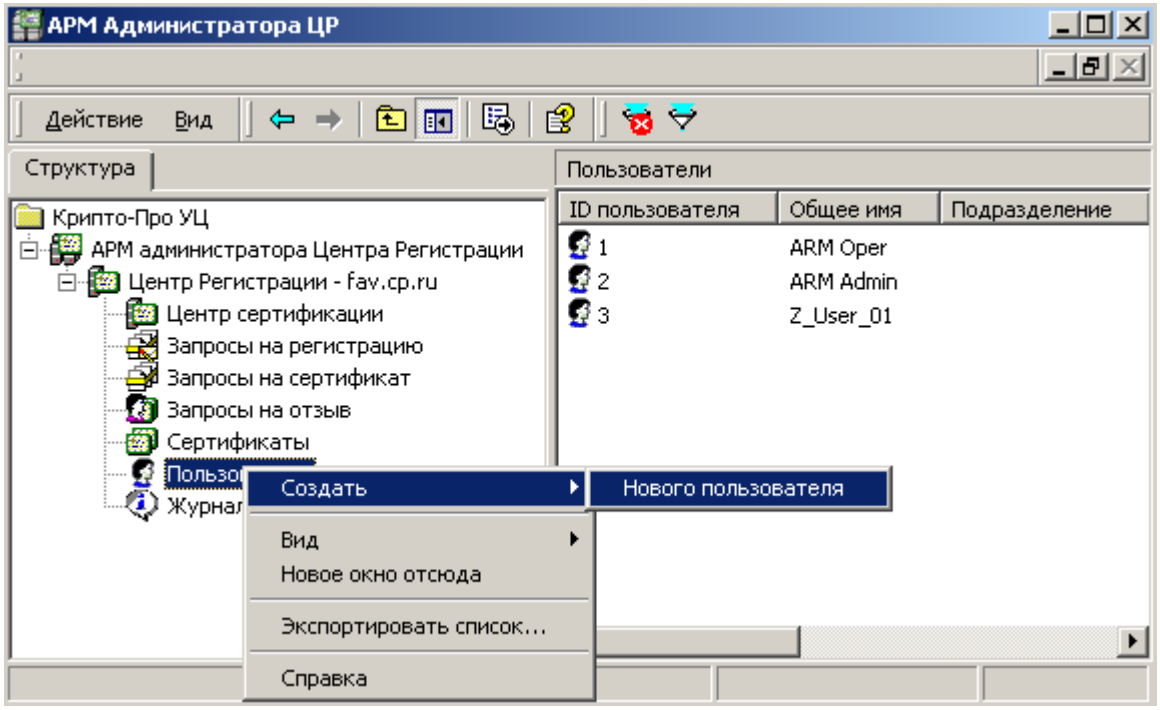
Иногда бывает удобно оформить Заявление на регистрацию и Заявление на изготовление сертификата в виде одного заявления – Заявления на регистрацию пользователя и изготовление сертификата ключа подписи.

1.2.1.1. Регистрация пользователей в централизованном режиме с генерацией ключей в Удостоверяющем Центре

Описание процесса регистрации пользователя в централизованном режиме с генерацией ключей в Удостоверяющем Центре:

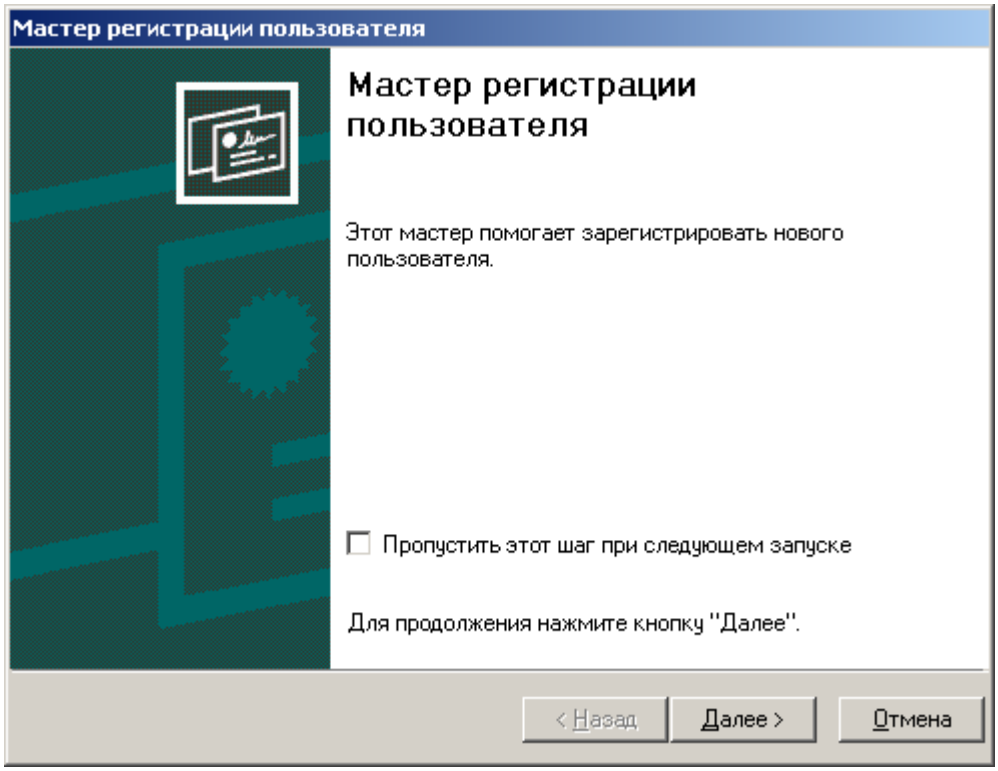
1. В окне **АРМ администратора ЦР** выделите правой кнопкой мыши узел **Пользователи** и в открывшемся контекстном меню нажмите **Создать->Нового пользователя;**

Рисунок 1. Выбор пункта меню создания нового пользователя



Запустится **Мастер регистрации пользователя**. Нажмите кнопку **Далее.**

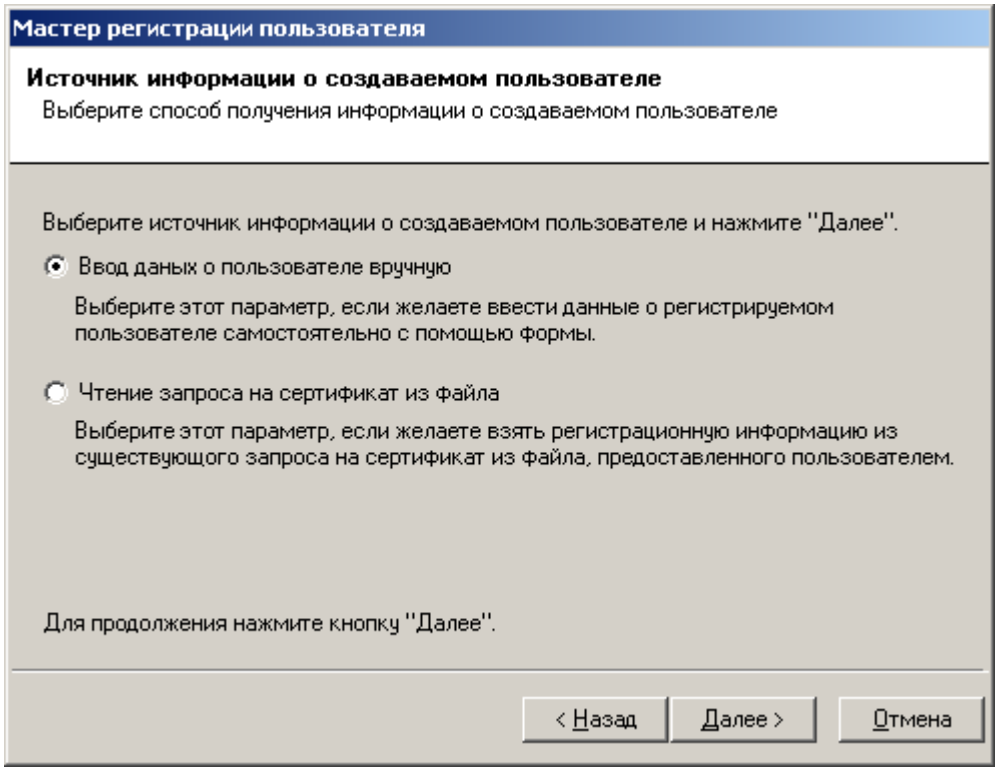
Рисунок 2. Окно первой страницы Мастера регистрации пользователя



Для отключения вывода первого окна **Мастера регистрации пользователя** установите «галку» **Пропустить этот шаг при следующем запуске**

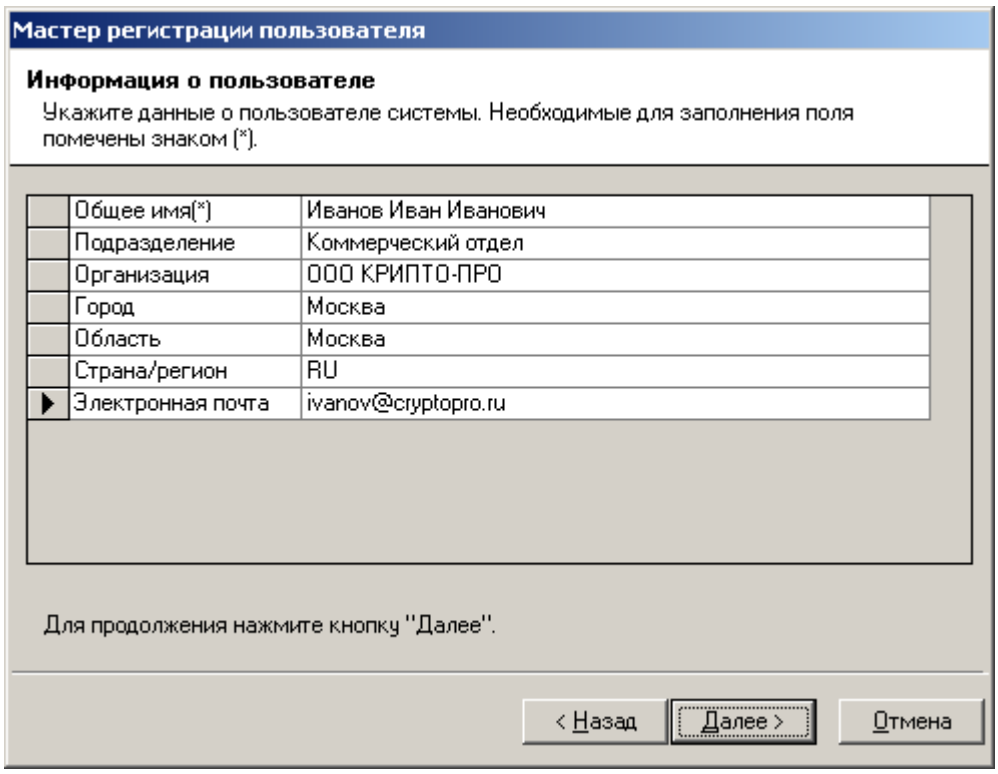
2. В окне **Источник информации о создаваемом пользователе** установите переключатель в положение **Ввод данных о пользователе вручную** и нажмите кнопку **Далее;**

Рисунок 3. Окно источник информации о создаваемом пользователе



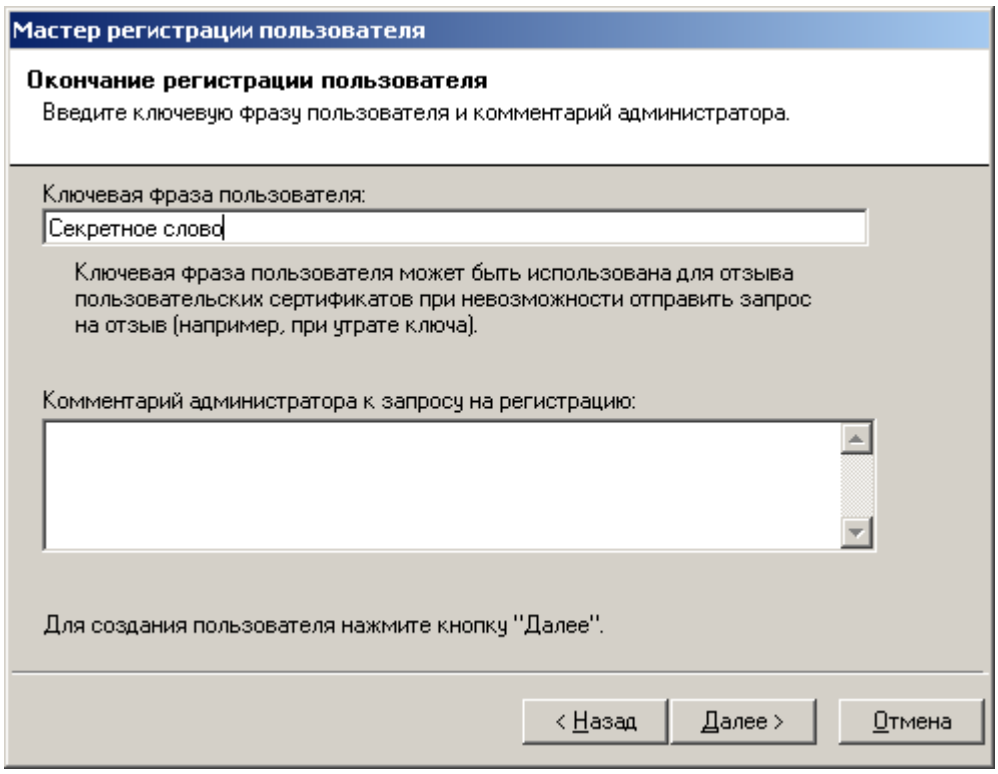
3. В окне **Информация о пользователе** введите идентификационные данные пользователя, указанные в Заявлении на регистрацию. После ввода данных обязательно проверьте идентичность введенных данных и данных, указанных в Заявлении на регистрацию. В случае полного соответствия идентификационной информации нажмите кнопку **Далее;**

Рисунок 4. Окно Информация о пользователе



4. В окне **Окончание регистрации пользователя** введите **Ключевую фразу пользователя**, необходимую для осуществления аутентификации пользователя по телефону в случаях, установленных Регламентом Удостоверяющего Центра (например, для оперативного приостановления действия сертификата ключа подписи при компрометации закрытого ключа). При необходимости введите комментарий к запросу на регистрацию, который носит исключительно информационную нагрузку. По окончании действий по вводу указанных данных нажмите кнопку **Далее;**

Рисунок 5. Окно Окончание регистрации пользователя

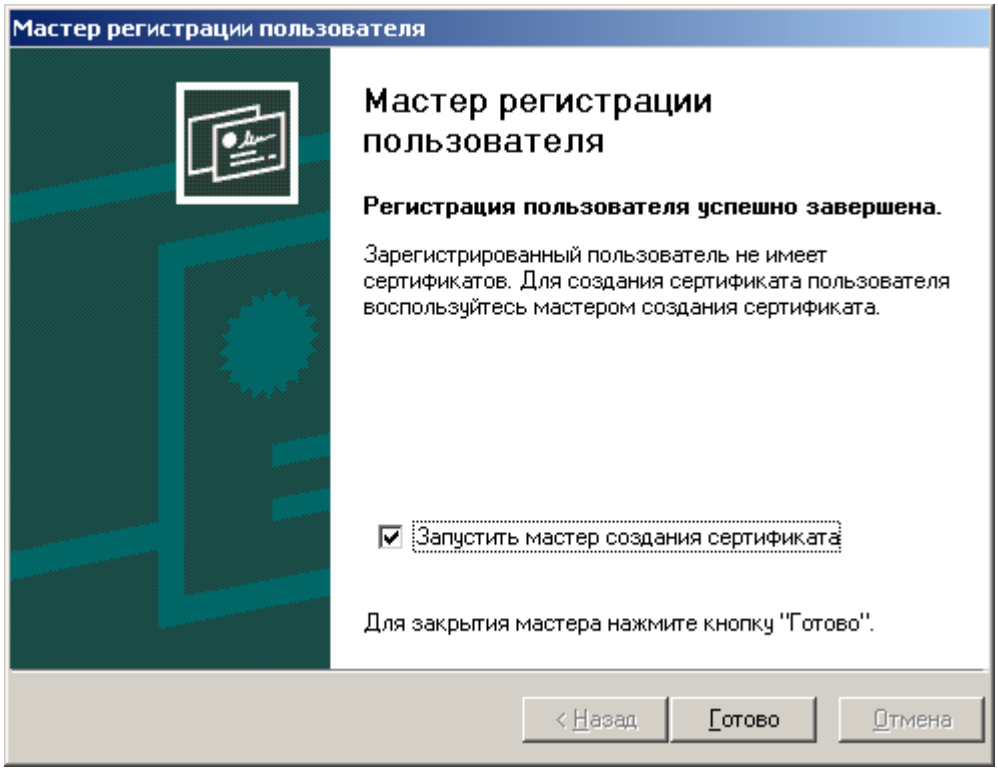


5. Откроется заключительное окно **Мастера регистрации пользователя** информирующее об успешном занесении идентификационных данных пользователя в реестр Удостоверяющего Центра (об успешной регистрации пользователя).

Установите в данном окне переключатель **Запустить мастер создания сертификата** для формирования первого сертификата ключа подписи зарегистрированного пользователя и нажмите кнопку **Готово;**

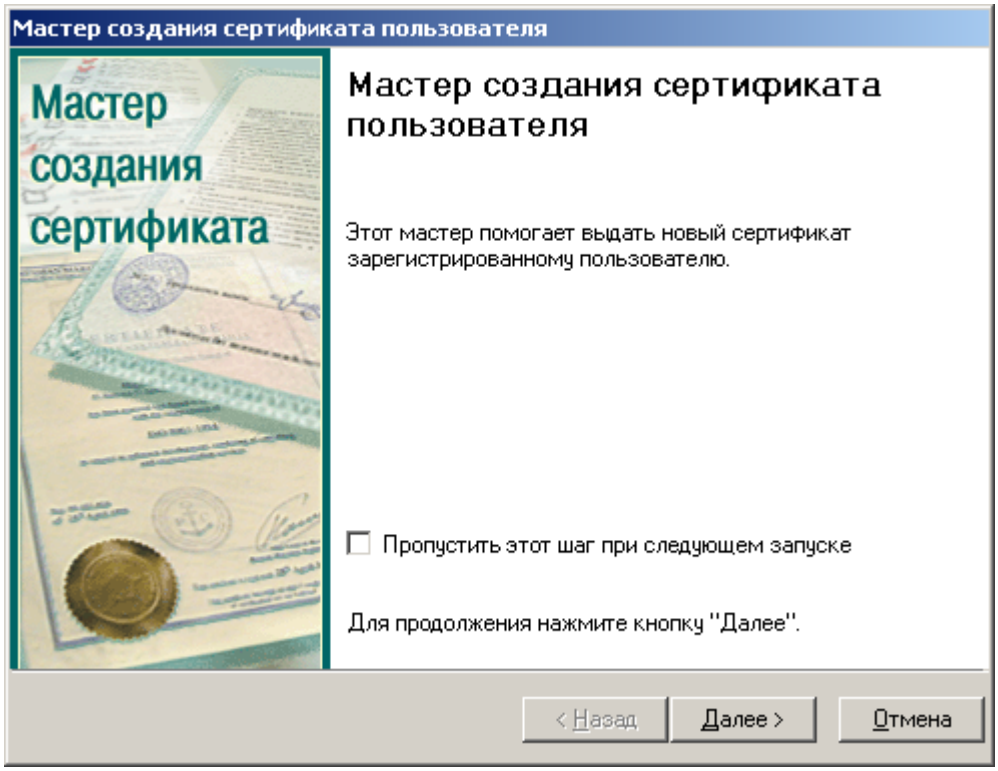

Снятие переключателя **Запустить мастер создания сертификата** заканчивает процедуру регистрации пользователя. В этом случае пользователь не является владельцем ни одного сертификата ключа подписи. Последующее изготовление сертификата осуществляется с помощью задач контекстного меню зарегистрированного пользователя.

Рисунок 6. Заключительное окно Мастера регистрации пользователя



6. Запустится **Мастер создания сертификата.** Нажмите кнопку **Далее;**

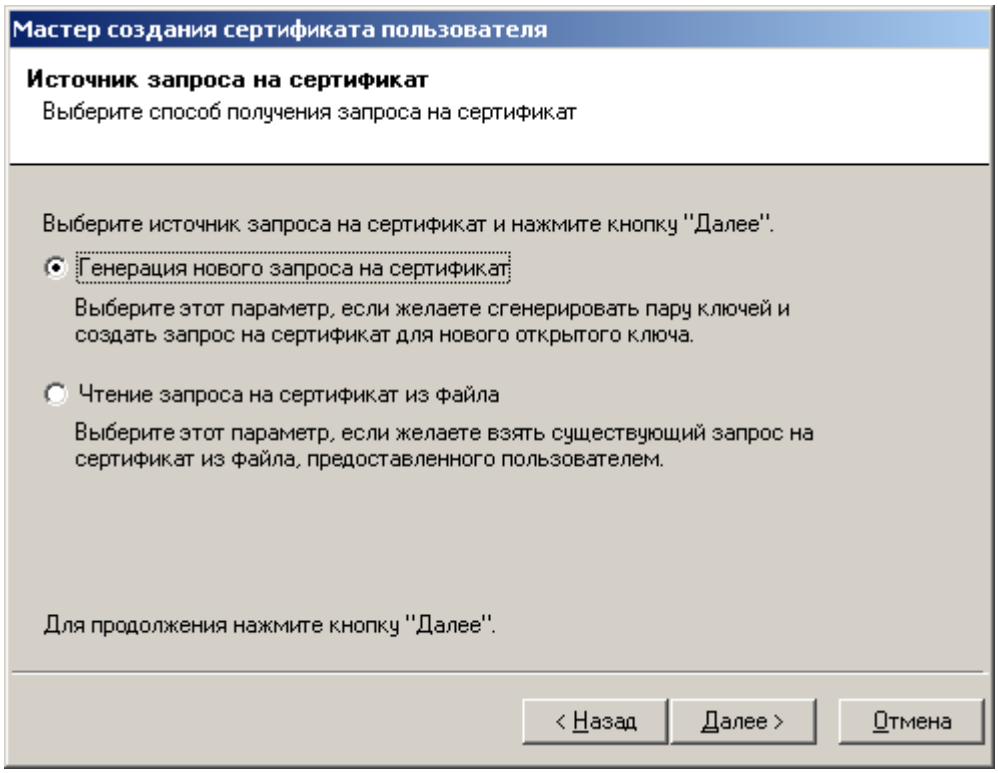
Рисунок 7. Окно первой страницы Мастера создания сертификата пользователя



Для отключения вывода первого окна **Мастера создания сертификата пользователя** установите «галку» **Пропустить этот шаг при следующем запуске.**

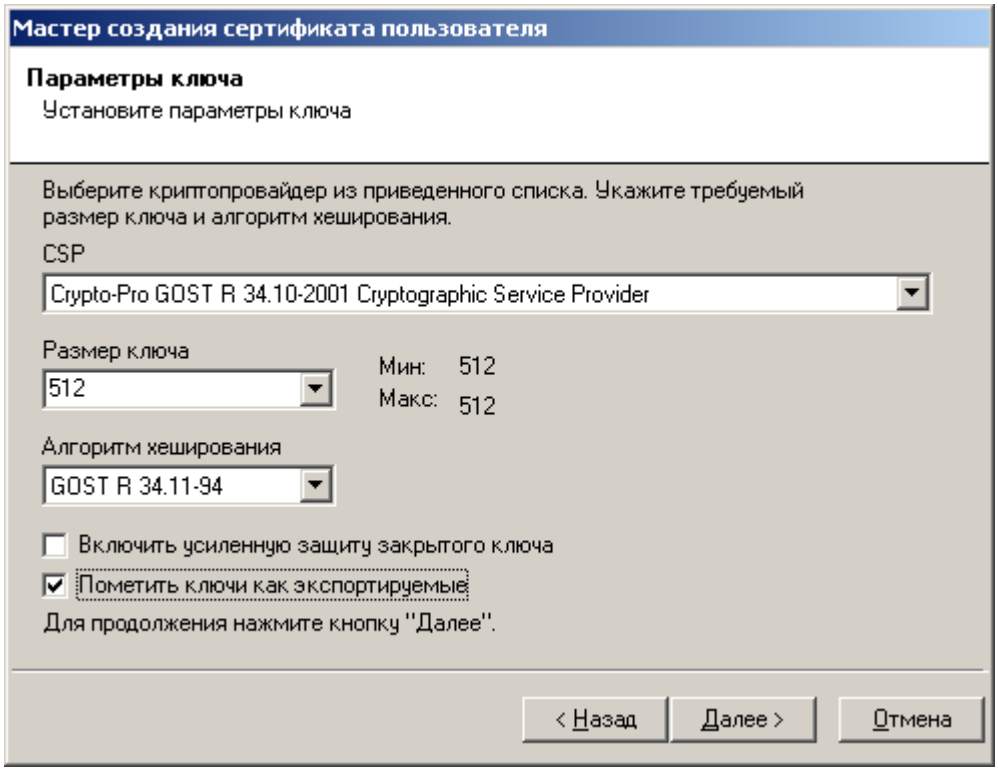
7. В окне **Источник запроса на сертификат** установите переключатель в положение **Генерация нового запроса на сертификат** и нажмите кнопку **Далее;**

Рисунок 8. Окно Источник запроса на сертификат



8. Откроется окно **Параметры ключа**, в котором выберите необходимый криптопровайдер и установите/снимите «галку» **Пометить ключи как экспортируемые**. Нажмите кнопку **Далее;**

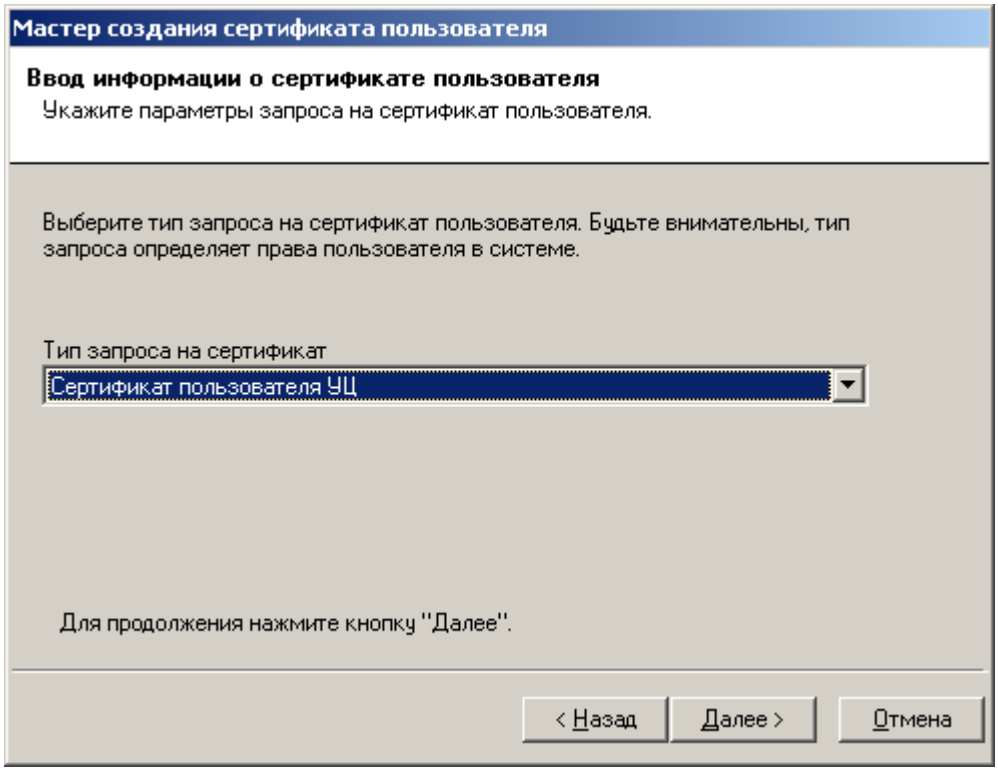
Рисунок 9. Установка параметров генерации ключа



Установка переключателя **Пометить ключи как экспортируемые** позволит в дальнейшем пользователю скопировать закрытый ключ на иной носитель. Снятие этого флага приводит к невозможности копирования ключевого контейнера штатными средствами СКЗИ и операционной системы. Переключатель **Включить усиленную защиту ключа** применяется к закрытым ключам, сформированным предустановленными в системе криптопровайдерами иностранного производства (например, Microsoft Base Cryptographic Provider).

9. В окне **Ввод информации о сертификате пользователя** выберите необходимый шаблон сертификата. Шаблон сертификата содержит области использования ключа, которые требуется занести в сертификат. Выбор указанного шаблона осуществляется в соответствии с положениями Регламента Удостоверяющего Центра и на основании поданного заявления на изготовление сертификата ключа подписи. После выбора необходимого шаблона сертификата нажмите кнопку **Далее;**

Рисунок 10. Выбор шаблона сертификата

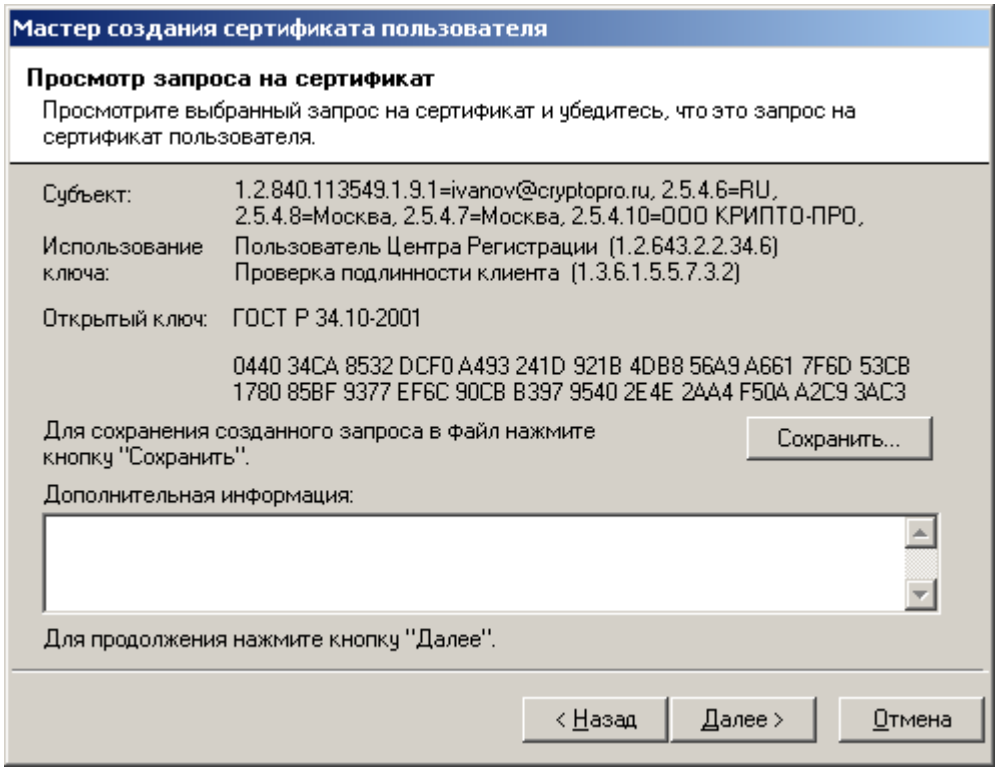


Описанная процедура требует от лица, осуществляющего изготовление сертификата ключа подписи, повышенного внимания, поскольку данные, содержащиеся в шаблоне сертификата определяют отношения, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение, и ошибка, допущенная на данном этапе, может привести к наделению пользователя дополнительными правами и привилегиями (к нелегитимному повышению его статуса).

10. Осуществите генерацию закрытого ключа на используемый ключевой носитель (например, Дискету 3,5” или eToken) и формирование запроса на сертификат ключа подписи. После осуществления указанных действий в окне **Просмотр запроса на сертификат** проверьте правильность указанных идентификационных данных (поле **Субъект**) и областей использования ключа (поле **Использование ключа**). При необходимости введите дополнительную справочную информацию о запросе и нажмите кнопку **Далее;**

Нажатие кнопки **Сохранить** позволяет сохранить сформированный запрос на сертификат в файле формата **PKCS#10.**

Рисунок 11. Просмотр запроса на сертификат



11. Откроется окно **Установка сертификата пользователя**, информирующее об успешном изготовлении сертификата ключа подписи и позволяющее:

- осуществить просмотр изготовленного сертификата, нажатием кнопки **Просмотр...;**
- сохранить изготовленный сертификат в виде файла формата **PKCS#7**, нажатием кнопки **Сохранить...;**
- установить изготовленный сертификат в контейнер секретного ключа (осуществляется установкой соответствующего переключателя);
- установить сертификат в хранилище (осуществляется установкой соответствующего переключателя);
- автоматически подтвердить запрос (осуществляется установкой соответствующего переключателя);

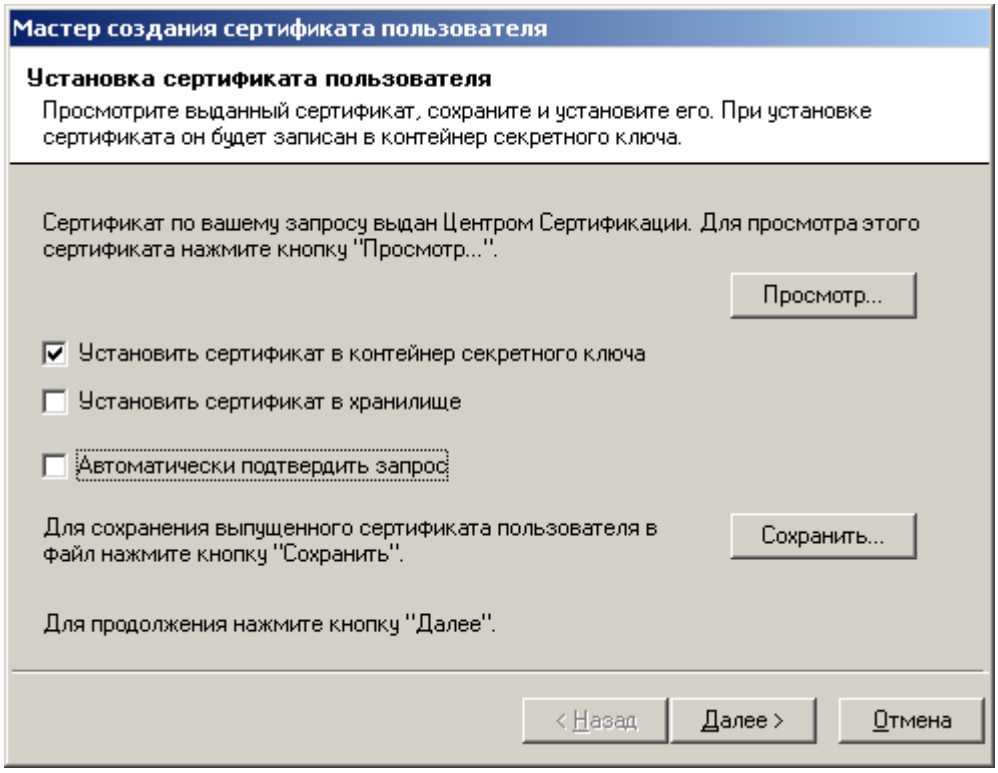
Осуществите установку переключателей, произведите необходимые действия и нажмите кнопку **Далее.**

Конкретная структура ключевого носителя, формируемого при регистрации пользователя, определяется Регламентом Удостоверяющего Центра. Рекомендуется на ключевой носитель помимо собственно контейнера секретного ключа записывать файл изготовленного сертификата ключа подписи (кнопка **Сохранить...**) и дополнительно сохранять сертификат ключа подписи в контейнер секретного ключа (установка флага **Установить сертификат в контейнер секретного ключа**).

Выбор переключателя **Установить сертификат в хранилище** приводит к инсталляции изданного сертификата в хранилище **Сертификаты/Текущий пользователь/Другие пользователи** на ПЭВМ АРМ администратора ЦР. Использование данного переключателя удобно для организации защищенного почтового обмена между привилегированным пользователем и пользователями Удостоверяющего Центра (например, с использованием почтовых клиентов Microsoft Outlook, Microsoft Outlook Express).

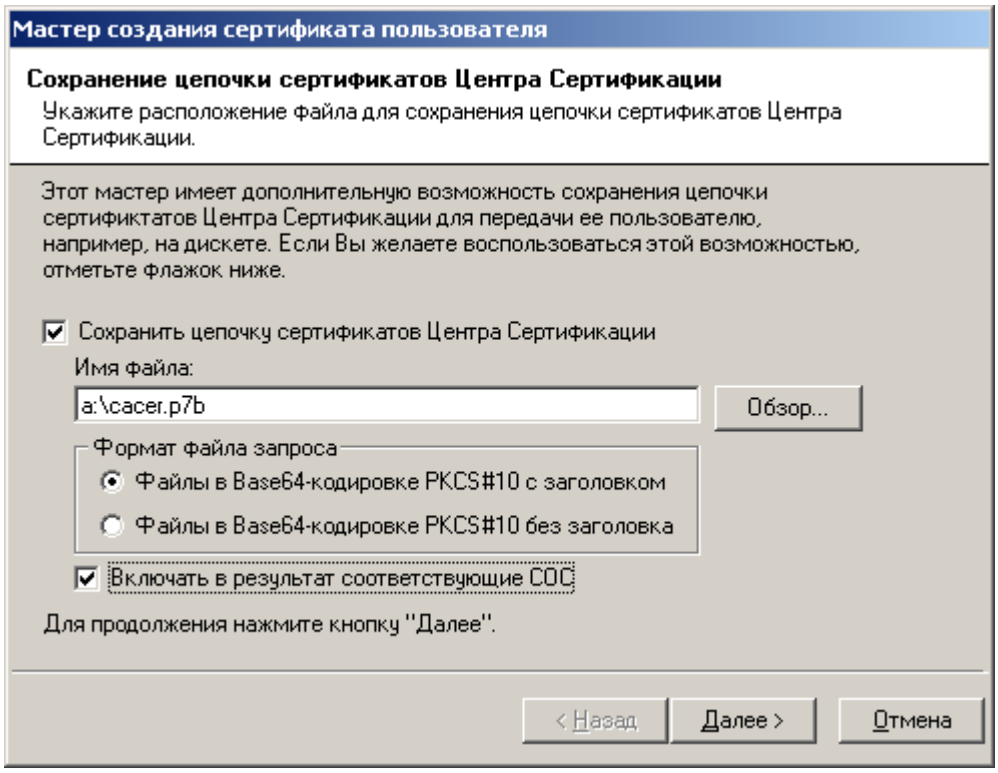
Выбор переключателя **Автоматически подтвердить запрос** устанавливает статус данного запроса в состояние **Завершен** и не требует подтверждения пользователем установки изготовленного сертификата на своей ПЭВМ. Подтверждение пользователем установки осуществляется с использованием **АРМ зарегистрированного пользователя**, являющегося web-приложением Центра Регистрации Удостоверяющего Центра, и требует обязательного сетевого соединения между ПЭВМ пользователя и Центром Регистрации. Рекомендуется использовать указанный переключатель в случае автономного функционирования Удостоверяющего Центра.

Рисунок 12. Окно Установка сертификата пользователя



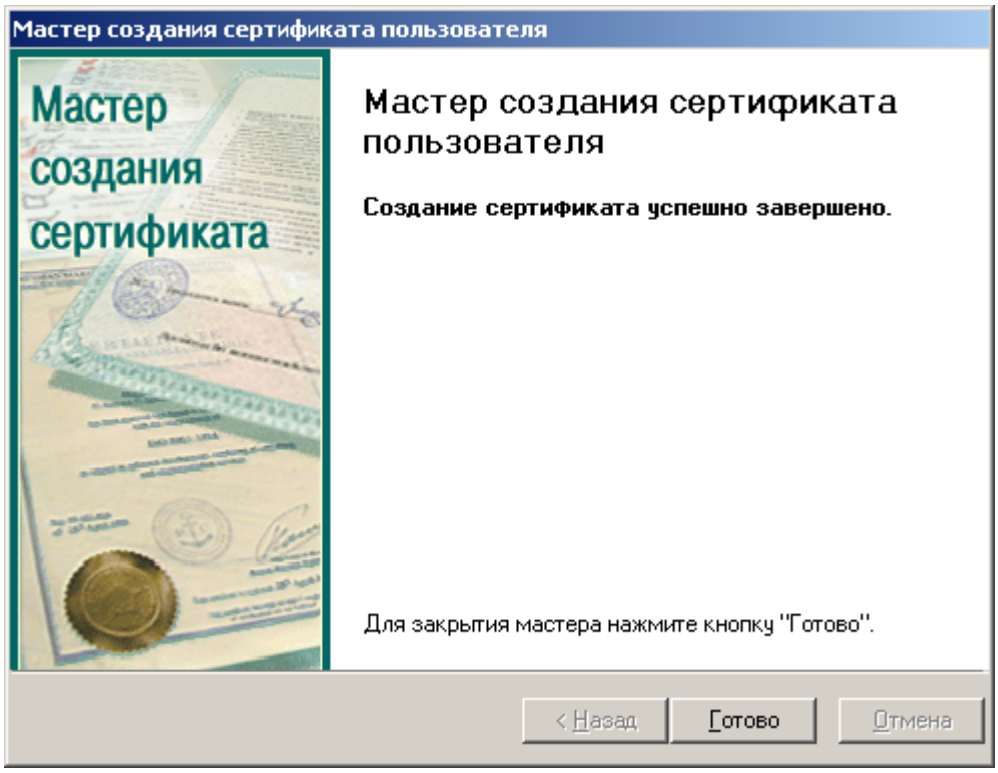
12. Окно **Сохранение цепочки сертификатов центра сертификации** позволяет сохранить все сертификаты издателей и списки отозванных сертификатов, обеспечивающие проверку статуса сертификатов, изданных Удостоверяющим Центром. Установите переключатели **Сохранить цепочку сертификатов Центра Сертификации** и **Включать в результат соответствующие СОС** и введите полный путь для размещения указанных данных. Нажмите кнопку **Далее**;

Рисунок 13. Сохранение цепочки сертификатов и Списка отозванных сертификатов



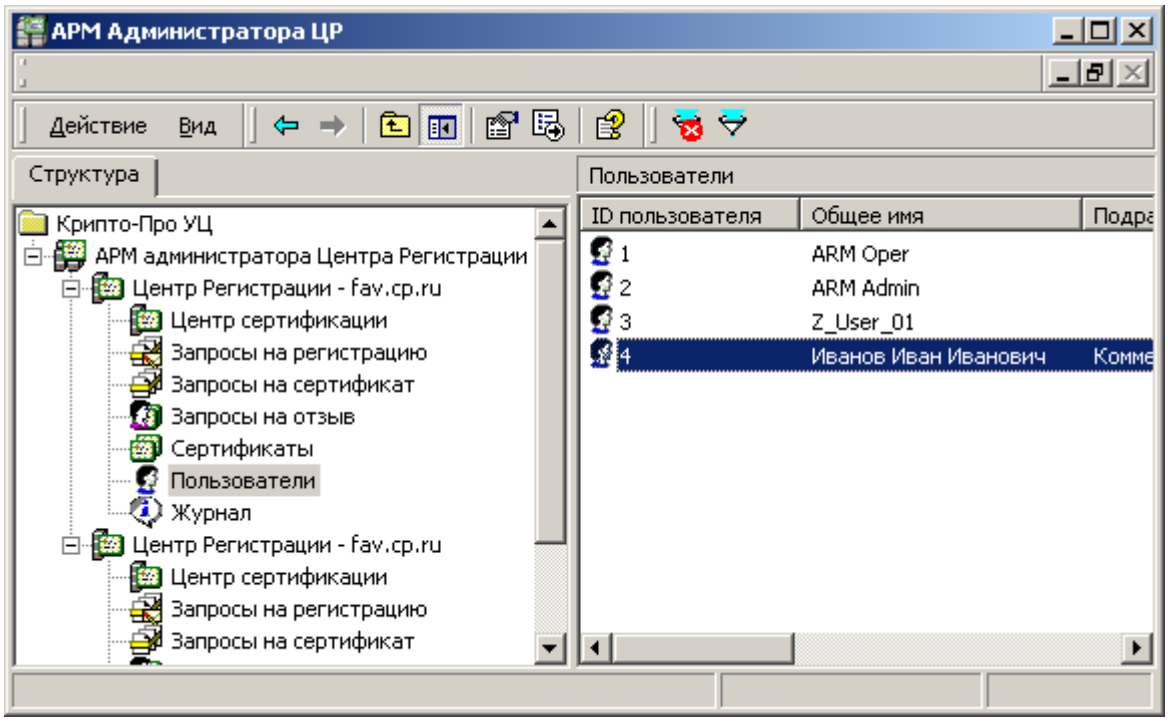
13. После успешного осуществления описанных действий откроется окно, информирующее об успешном изготовлении сертификата. Нажмите кнопку **Готово;**

Рисунок 14. Заключительное окно Мастера создания сертификатов пользователей



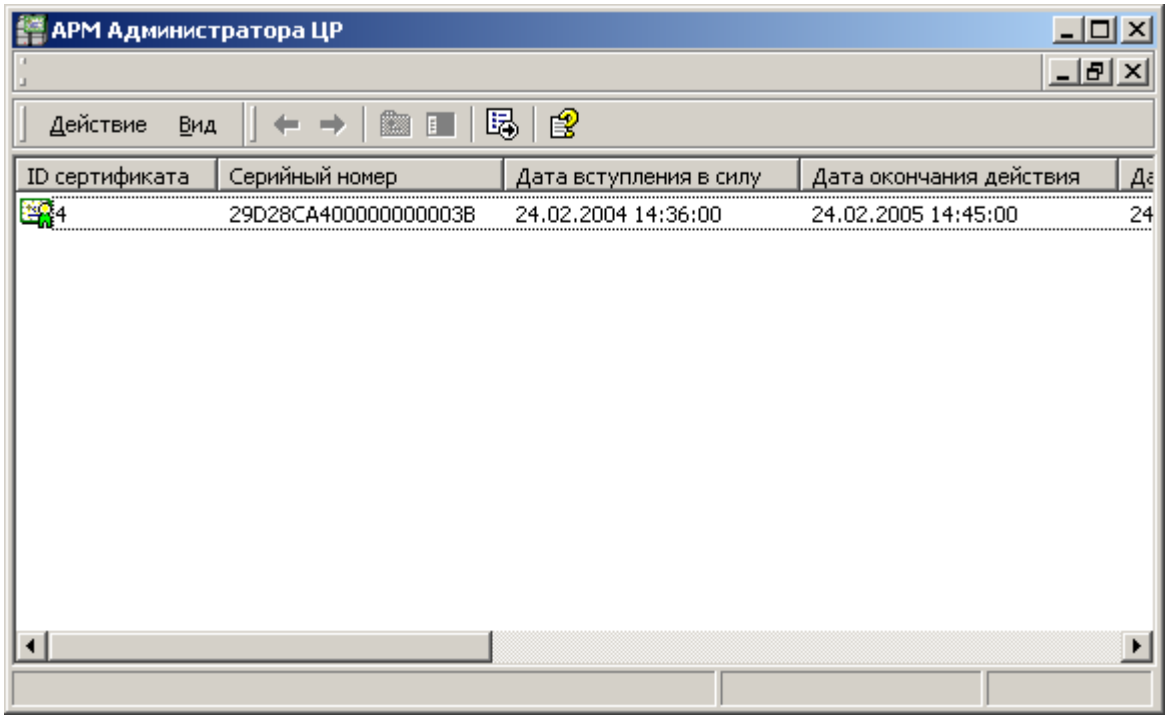
14. В левой части окна **АРМ администратора ЦР** выделите узел **Пользователи** и в правой части окна проверьте наличие учетной записи, соответствующей зарегистрированному пользователю;

Рисунок 15. Выбор учетной записи зарегистрированного пользователя



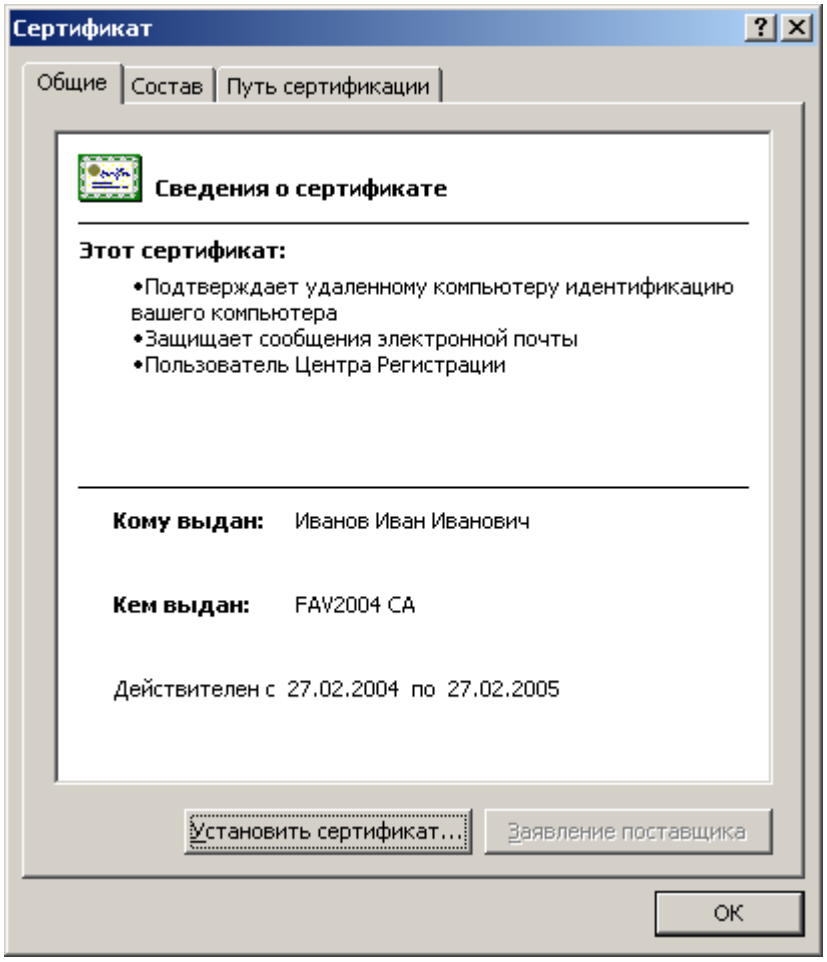
15. Правой кнопкой мыши выделите созданную учетную запись и в контекстном меню выберите **Все задачи->Показать->Сертификаты;**

Рисунок 16. Окно просмотра сертификатов выбранного пользователя



16. Выделите изготовленный сертификат ключа подписи двойным нажатием левой кнопки мыши и просмотрите его в стандартном окне просмотра сертификатов;

Рисунок 17. Стандартное окно просмотра сертификата пользователя



1.2.1.2. Регистрация пользователей в централизованном режиме с генерацией ключей самим пользователем

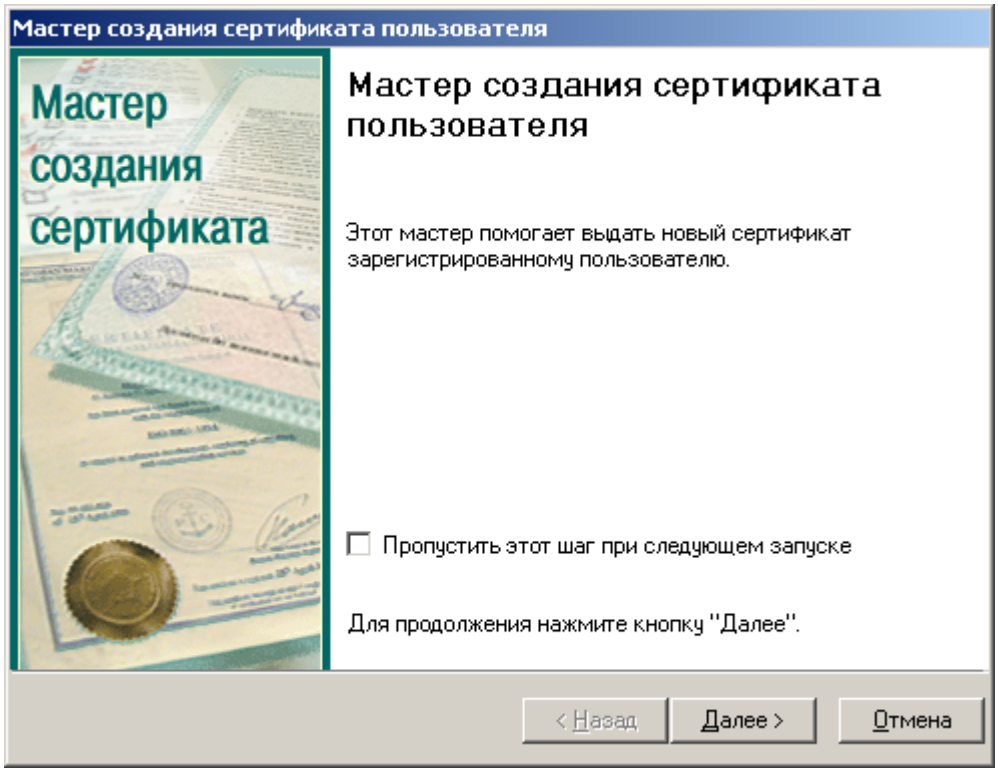
Описание процесса регистрации пользователя в централизованном режиме с генерацией ключей самим пользователем:

1. Формирование пользователем запроса на сертификат осуществляется с использованием специально разрабатываемого программного обеспечения, осуществляющего выполнение следующих функций:
   - Генерация закрытого и открытого ключа подписи;
   - Формирование запроса на сертификат ключа подписи;
   - Формирование бланка запроса на сертификат ключа подписи;
   - Установка изготовленного сертификата ключа подписи

   Для изготовления сертификата ключа подписи пользователь предоставляет файл запроса на сертификат ключа подписи формата PKCS#10 и установленным образом оформленный бланк запроса на сертификат ключа подписи.
2. Занесение идентификационных данных пользователя в Реестр зарегистрированных пользователей Удостоверяющего Центра осуществляется аналогично процедуре, описанной в пунктах 1-5 раздела 17.2.1.1 «Регистрация пользователя в централизованном режиме с генерацией ключей в Удостоверяющем Центре»;

3. После запуска **Мастера создания сертификата** в открывшемся окне нажмите кнопку **Далее;**

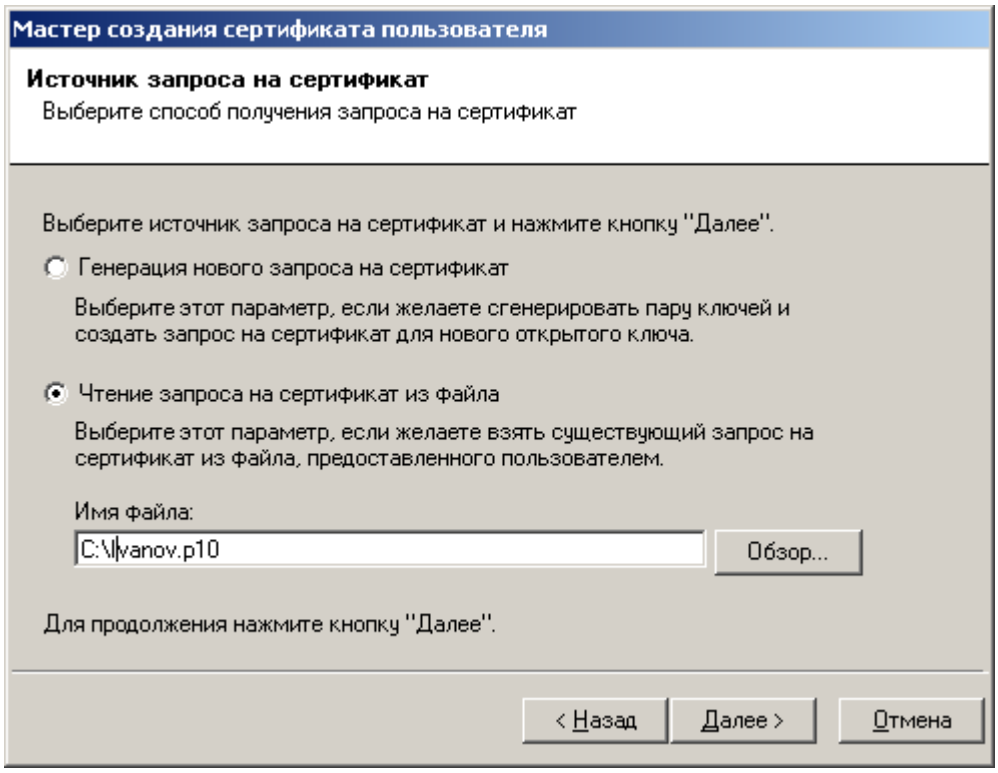
Рисунок 18. Первое окно Мастера создания сертификата пользователя



Для отключения вывода первого окна **Мастера создания сертификата пользователя** установите «галку» **Пропустить этот шаг при следующем запуске.**

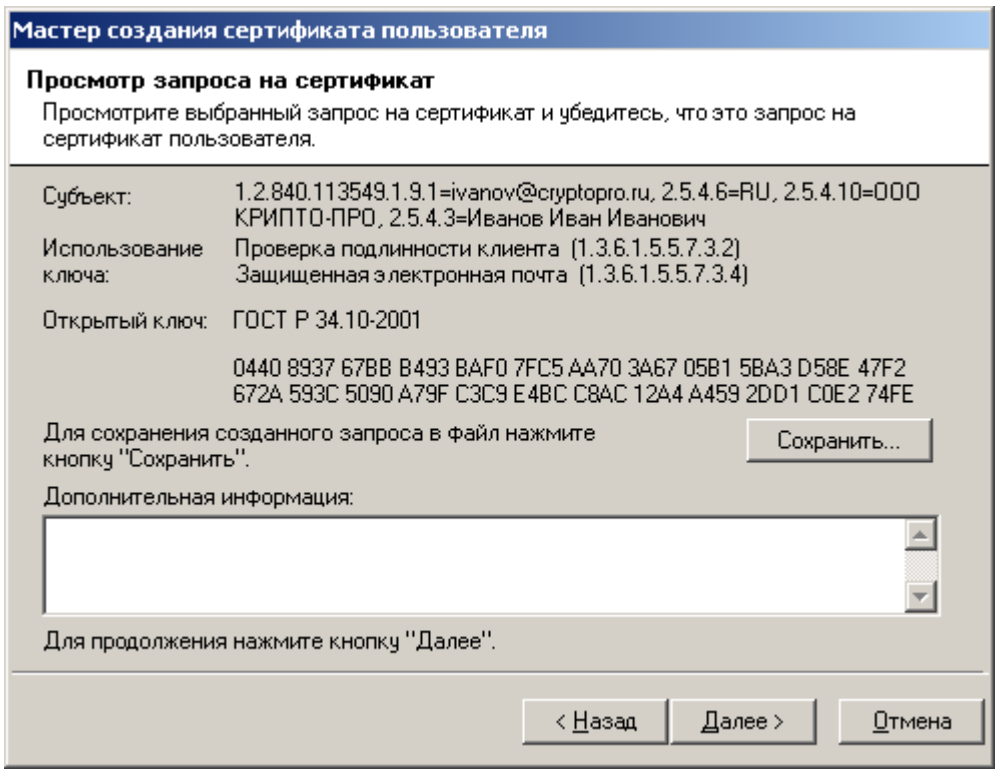
4. В открывшемся окне **Источник запроса на сертификат** выберите переключатель **Чтение запроса на сертификат из файла,** введите имя файла, содержащего запрос на сертификат ключа подписи, и нажмите кнопку **Далее;**

Рисунок 19. Выбор в качестве источника запроса на сертификат файла PKCS#10



5. В окне **Просмотр запроса на сертификат** внимательно проверьте идентичность данных, указанных в полях **Субъект**, **Использование ключа**, **Открытый ключ** данным, содержащимся в предоставленном бланке запроса на сертификат. Только в случае полного совпадения этих данных нажмите кнопку **Далее;**

Рисунок 20. Окно просмотра запроса на сертификат




Описанная процедура требует от лица, осуществляющего изготовление сертификата ключа подписи, повышенного внимания, поскольку данные, содержащиеся в поле **Использование ключа** определяют отношения, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение, и ошибка, допущенная на данном этапе, может привести к наделению пользователя дополнительными правами и привилегиями (к нелегитимному повышению его статуса).

6. Откроется окно **Установка сертификата пользователя**, информирующее об успешном изготовлении сертификата ключа подписи и позволяющее:

- осуществить просмотр изготовленного сертификата, нажатием кнопки **Просмотр...;**
- сохранить изготовленный сертификат в виде файла формата **PKCS#7**, нажатием кнопки **Сохранить...;**
- установить сертификат в хранилище (осуществляется установкой соответствующего переключателя);
- автоматически подтвердить запрос (осуществляется установкой соответствующего переключателя);

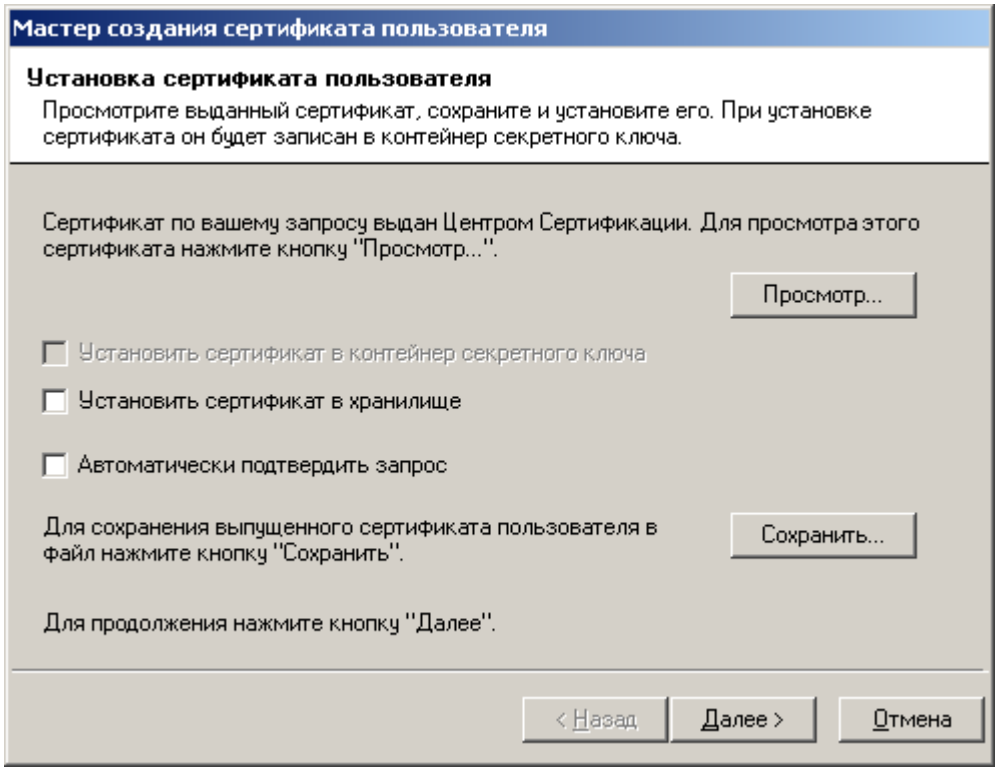
Осуществите установку переключателей, произведите необходимые действия и нажмите кнопку **Далее.**


Порядок предоставления пользователю изготовленного сертификата ключа подписи определяется Регламентом Удостоверяющего Центра. В случае предоставления пользователю сертификата на сменном магнитном носителе удобно воспользоваться кнопкой **Сохранить...** данного окна, и сохранить изданный сертификат на указанный магнитный носитель.

Выбор переключателя **Установить сертификат в хранилище** приводит к инсталляции изданного сертификата в хранилище **Сертификаты/Текущий пользователь/Другие пользователи** на ПЭВМ **АРМ Администратора ЦР**. Использование данного переключателя удобно для организации защищенного почтового обмена между привилегированным пользователем и пользователями Удостоверяющего Центра (например, с использованием почтовых клиентов Microsoft Outlook, Microsoft Outlook Express).

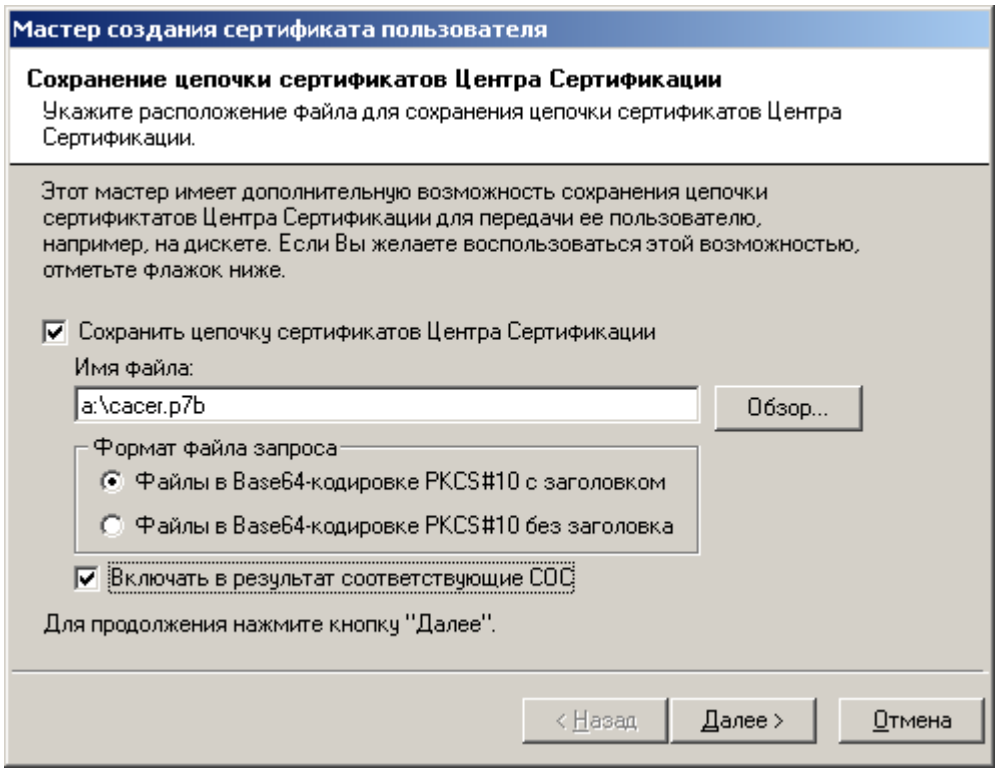
Выбор переключателя **Автоматически подтвердить запрос** устанавливает статус данного запроса в состояние **Завершен** и не требует подтверждения пользователем установки изготовленного сертификата на своей ПЭВМ. Подтверждение пользователем установки осуществляется с использованием АРМ зарегистрированного пользователя, являющегося web-приложением Центра Регистрации Удостоверяющего Центра, и требует обязательного сетевого соединения между ПЭВМ пользователя и Центром Регистрации. Рекомендуется использовать указанный переключатель в случае автономного функционирования Удостоверяющего Центра.

Рисунок 21. Окно Установки сертификата пользователя



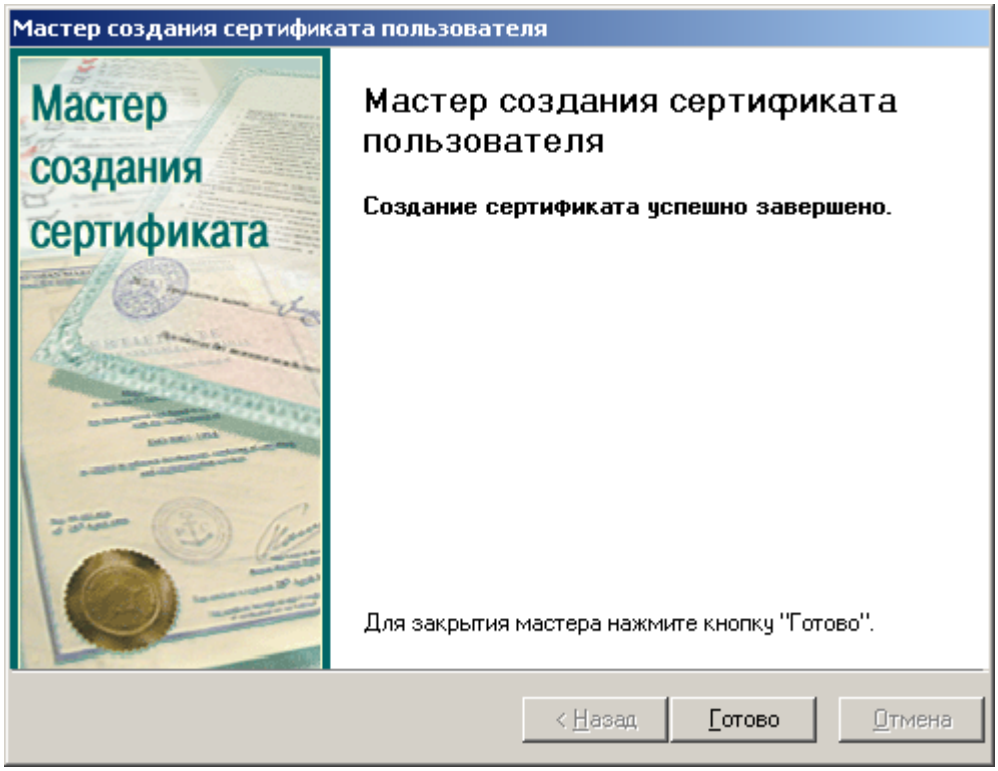
7. Окно **Сохранение цепочки сертификатов центра сертификации** позволяет сохранить все сертификаты издателей и списки отозванных сертификатов, обеспечивающие проверку статуса сертификатов, изданных Удостоверяющим Центром. Установите переключатели **Сохранить цепочку сертификатов Центра Сертификации** и **Включать в результат соответствующие СОС** и введите полный путь для размещения указанных данных. Нажмите кнопку **Далее**;

Рисунок 22. Окно сохранения цепочки сертификатов и Списка отозванных сертификатов



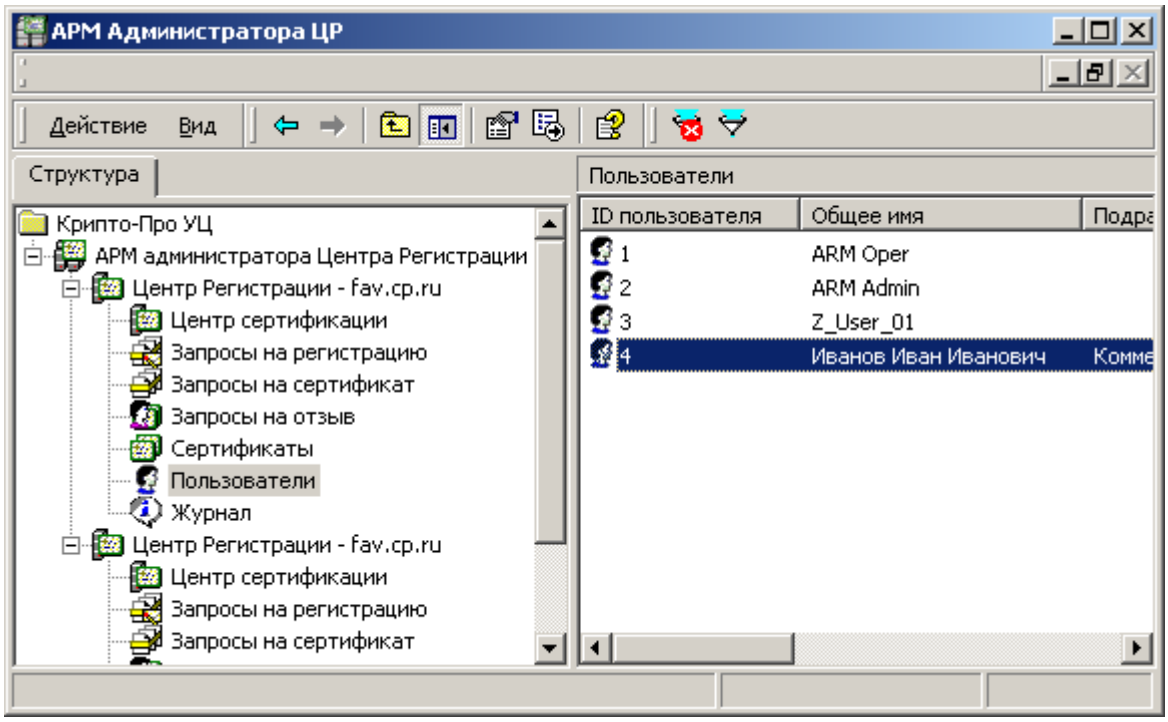
8. После успешного осуществления описанных действий откроется окно, информирующее об успешном изготовлении сертификата. Нажмите кнопку **Готово;**

Рисунок 23. Заключительное окно Мастера создания сертификата



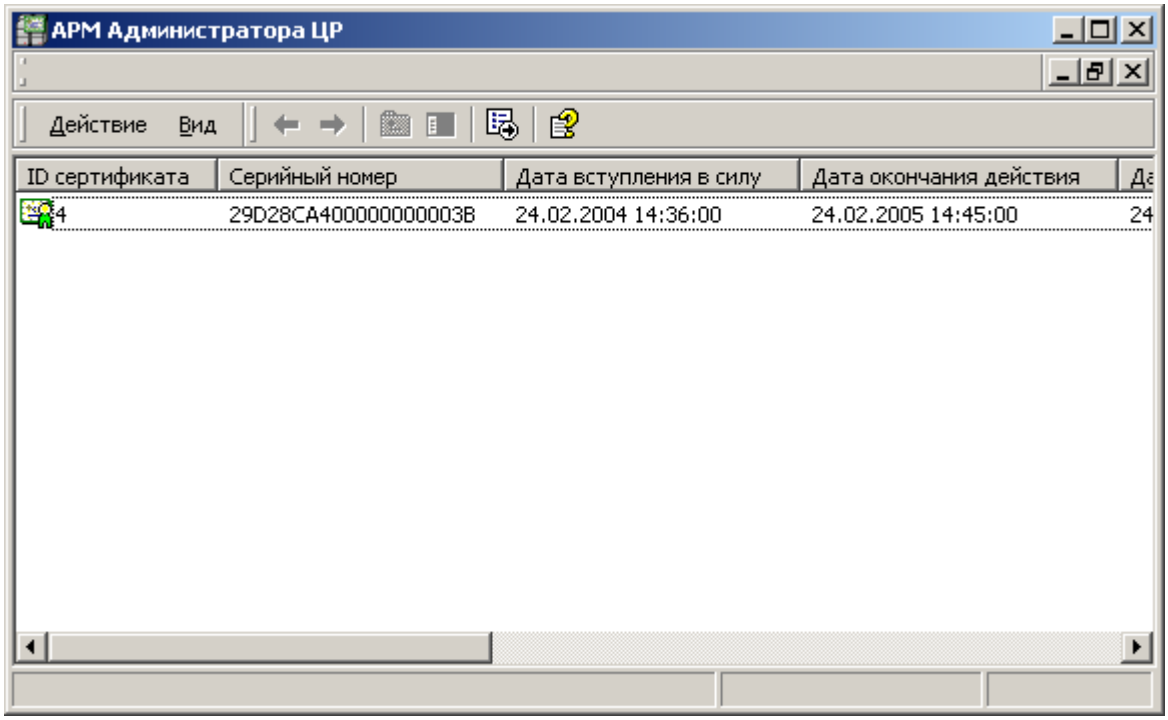
9. В левой части окна **АРМ администратора ЦР** выделите узел **Пользователи** и в правой части окна проверьте наличие учетной записи, соответствующей зарегистрированному пользователю;

Рисунок 24. Выбор учетной записи зарегистрированного пользователя



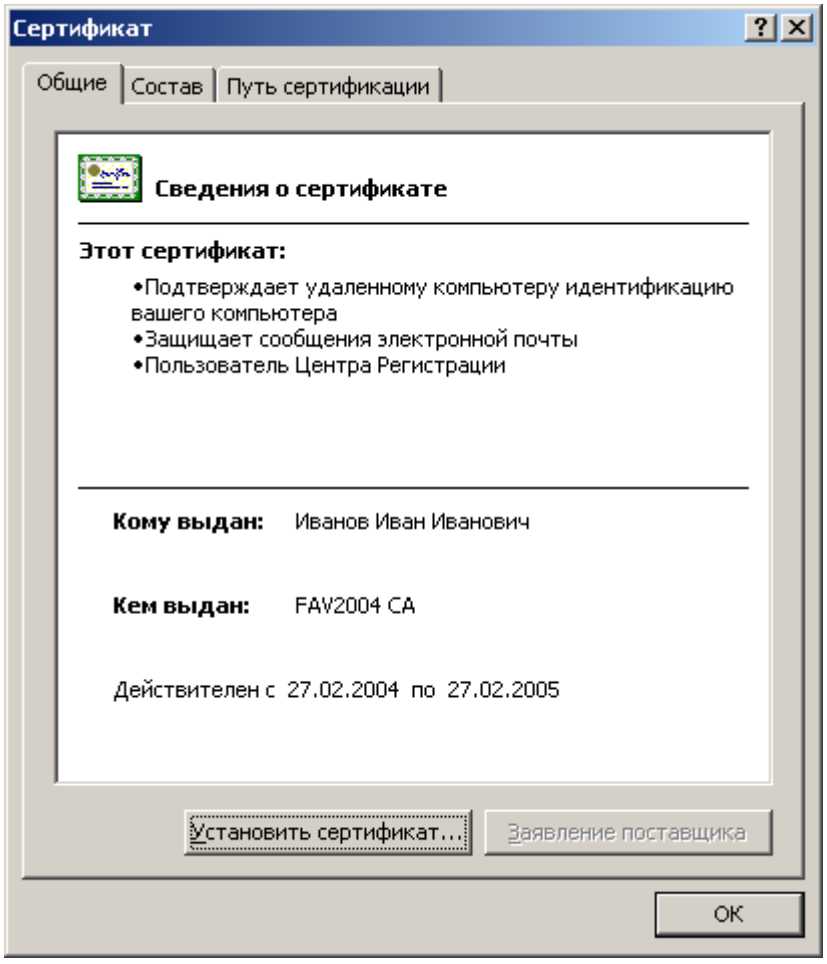
10. Правой кнопкой мыши выделите созданную учетную запись и в контекстном меню выберите **Все задачи->Показать->Сертификаты;**

Рисунок 25. Окно просмотра изданных сертификатов зарегистрированного пользователя



11. Выделите изготовленный сертификат ключа подписи двойным нажатием левой кнопки мыши и просмотрите его в стандартном окне просмотра сертификатов.

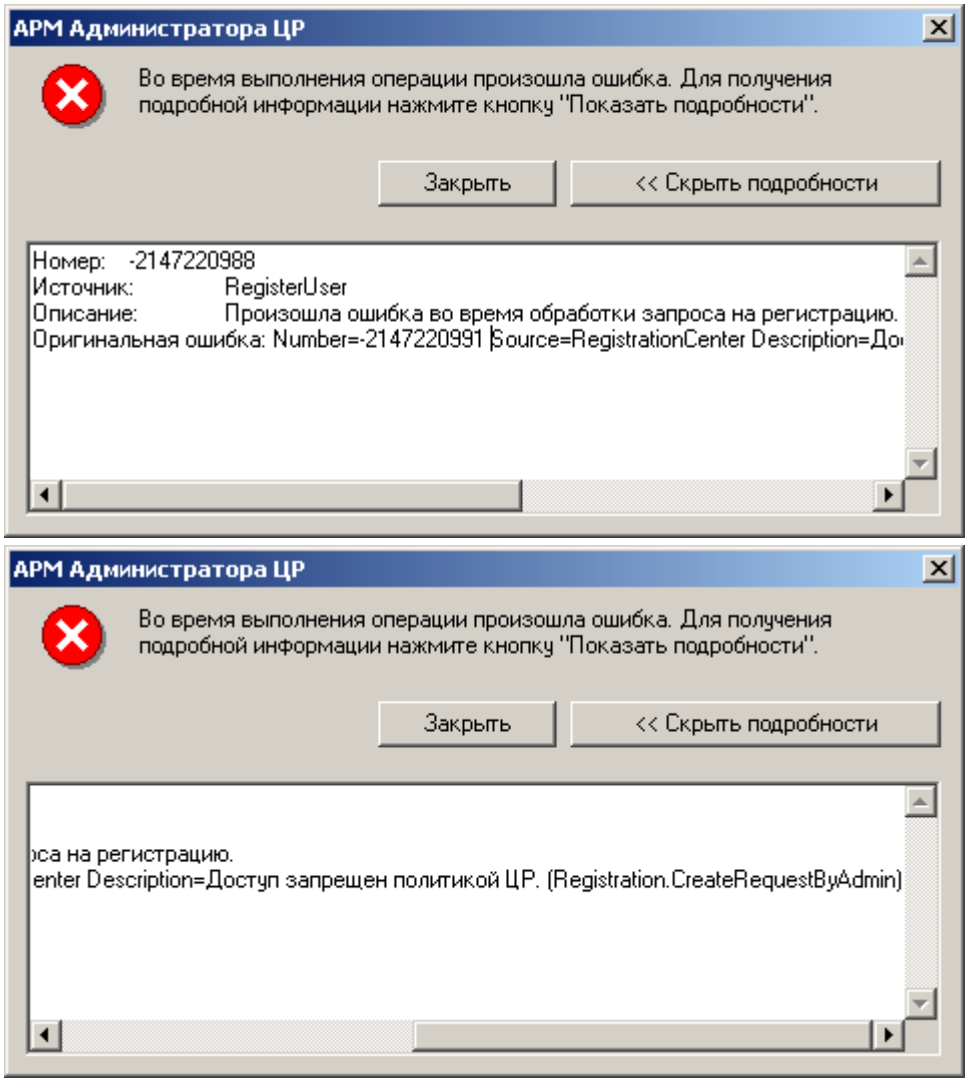
Рисунок 26. Стандартное окно просмотра сертификата пользователя



1.2.1.3. Наиболее часто встречающиеся ошибки, возникающие при регистрации пользователя в централизованном режиме:

1. После нажатия на кнопку **Далее** в окне **Окончание регистрации пользователя** появляется сообщение:

Рисунок 27. Ошибка при выполнении метода Regisration.CreateRequestByAdmin

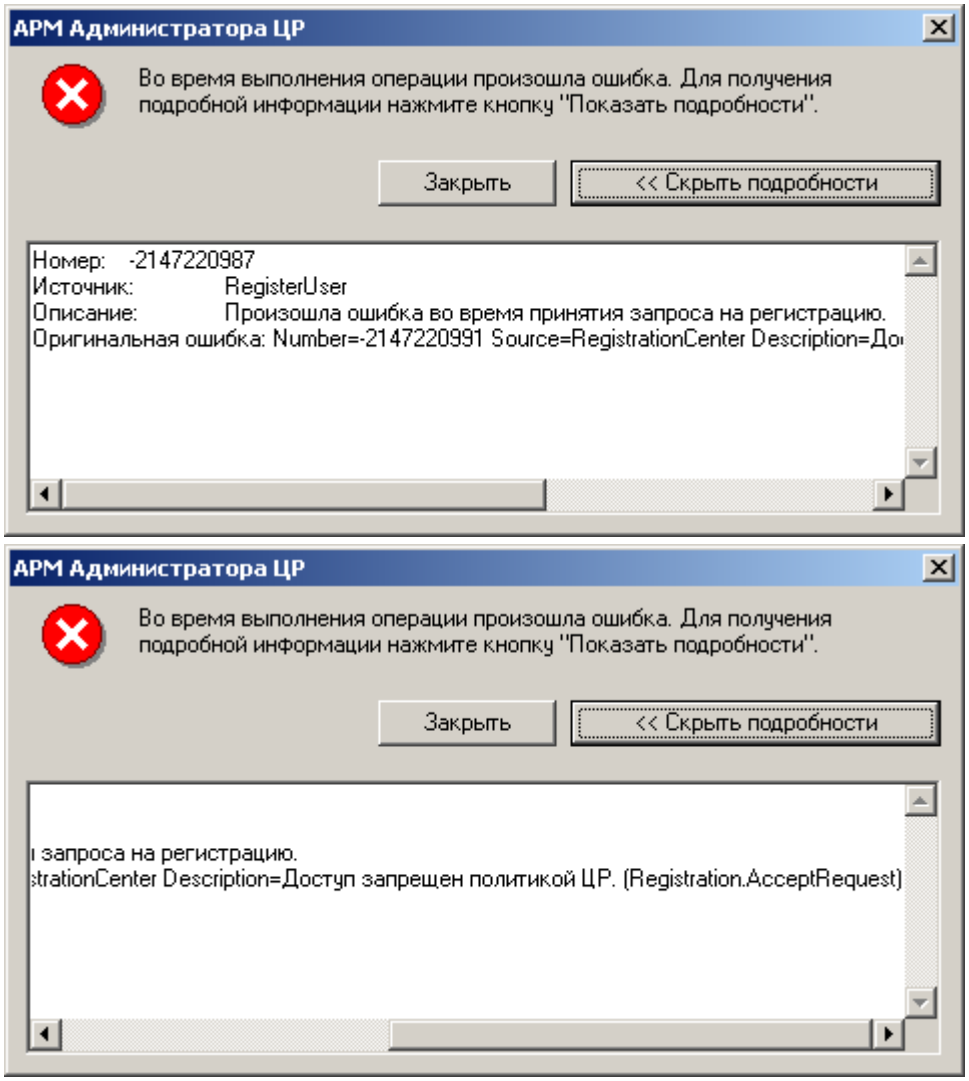


У привилегированного пользователя (**Оператора** или **Администратора**), производящего регистрацию пользователя в Удостоверяющем Центре, недостаточно прав на выполнение метода **Registration.CreateRequestByAdmin**.

На Центре Регистрации необходимо осуществить настройку политики безопасности, позволяющую осуществлять выполнение указанного метода.

2. После нажатия на кнопку **Далее** в окне **Окончание регистрации пользователя** появляется сообщение:

Рисунок 28. Ошибка при выполнении метода Registration.AcceptRequest

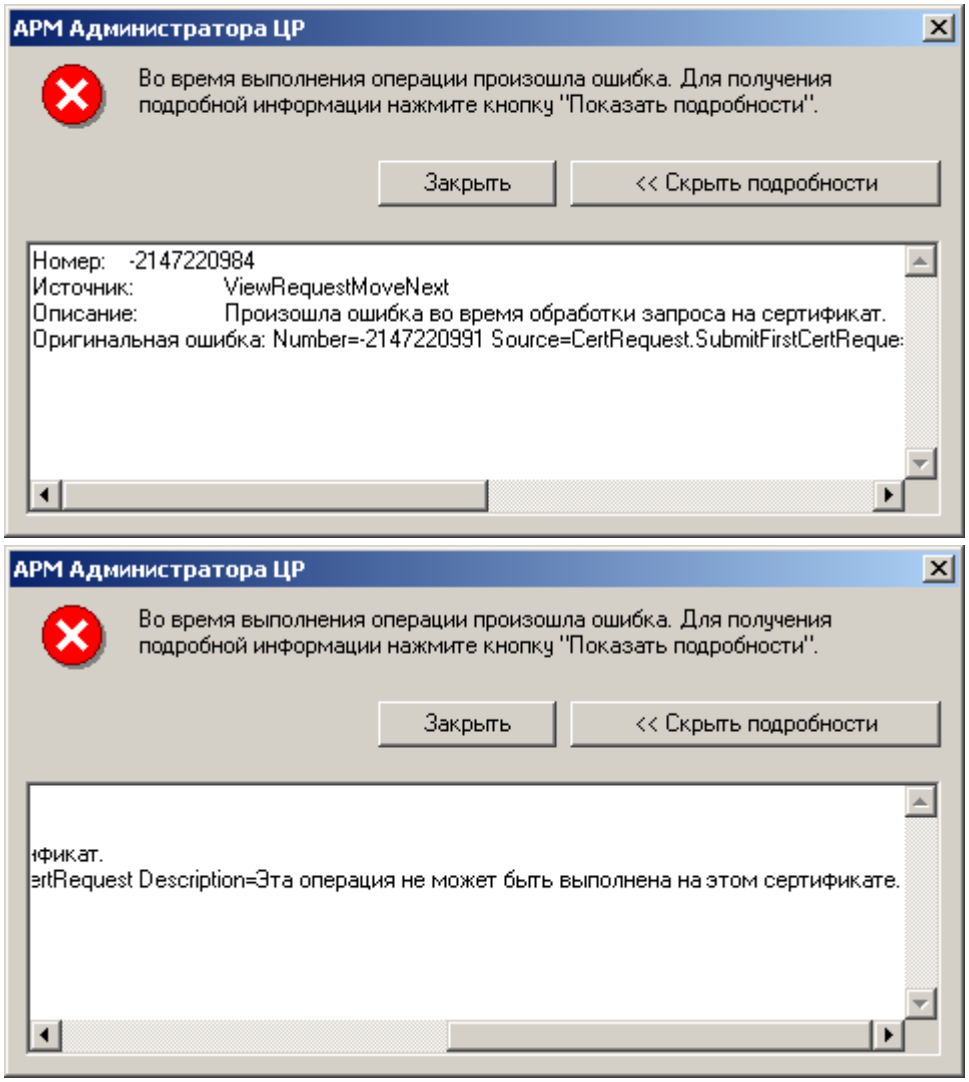


У привилегированного пользователя (**Оператора** или **Администратора**), производящего регистрацию пользователя в Удостоверяющем Центре, недостаточно прав на выполнение метода **Registration.AcceptRequest**.

На Центре Регистрации необходимо осуществить настройку политики безопасности, позволяющую осуществлять выполнение указанного метода.

3. После нажатия на кнопку **Далее** в окне **Просмотр запроса на сертификат** появляется сообщение:

Рисунок 29. Ошибка при выполнении метода CertRequest.SubmitFirstCertRequest

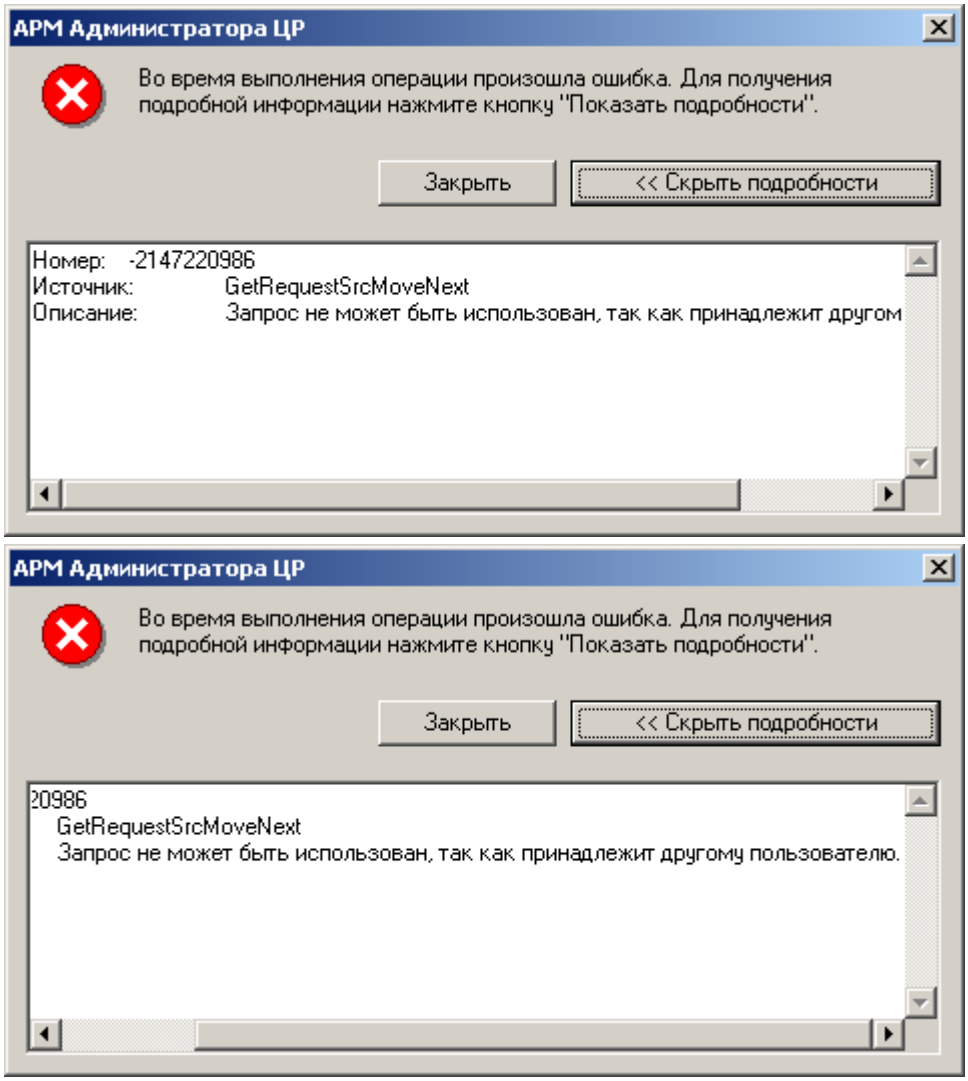


Привилегированный пользователь (**Оператор** или **Администратор**), производящий регистрацию пользователя в Удостоверяющем Центре, не имеет прав на изготовление сертификата, содержащего области использования, указанные в шаблоне на сертификат.

На Центре Регистрации осуществите настройку Политики обработки неподписанных запросов и добавьте необходимые области использования сертификата.

4. После нажатия кнопку **Далее** в окне **Источник запроса на сертификат**, в случае выбора переключателя **Чтение запроса на сертификат из файла** появляется сообщение:

Рисунок 30. Ошибка - Запрос принадлежит другому пользователю



Идентификационные данные пользователя, содержащиеся в запросе на сертификат отличны от идентификационных данных зарегистрированного пользователя, на имя которого требуется изготовить сертификат (например, выбран файл, содержащий запрос на сертификат другого пользователя), либо при формировании файла запроса была допущена ошибка (например, нарушен установленный порядок следования компонент имени субъекта).

При появлении сообщения об ошибке в системный журнал приложений (**Пуск/Программы/Администрирование/ПросмотрСобытий/Журнал Приложений**) заносится подробная информация о возникшей ситуации, анализ которой позволит точно определить причину ошибки.

Рисунок 31. Окно просмотра Журнала приложений

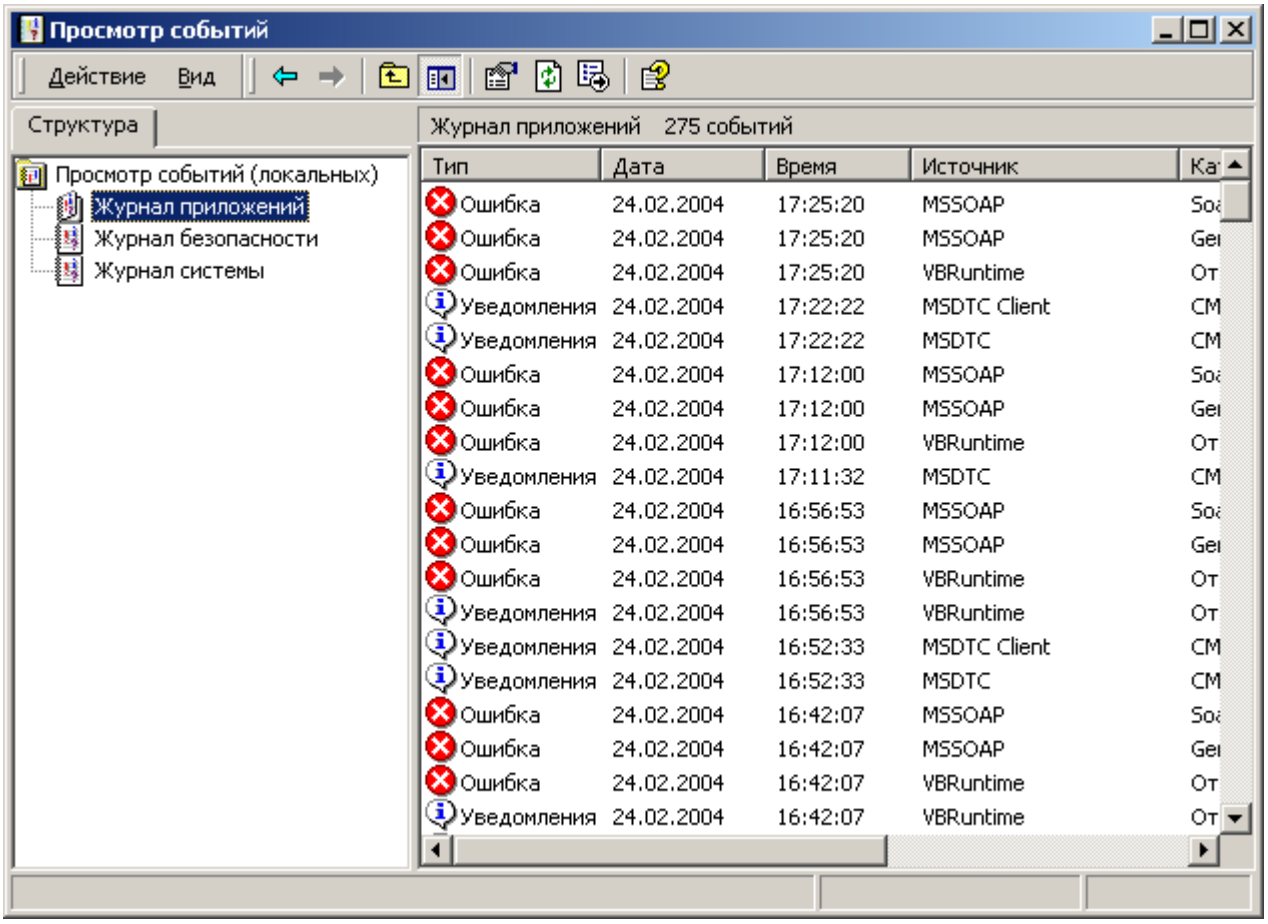
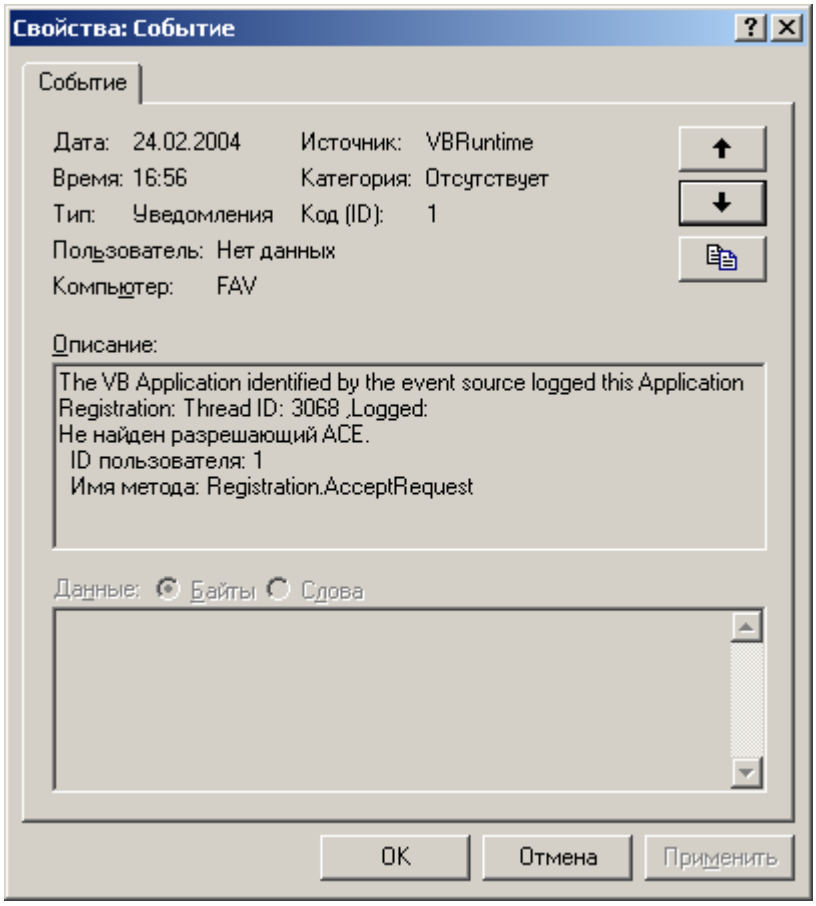


Рисунок 32. Окно просмотра описания произошедшего события



1.2.2. Регистрация пользователя в распределенном режиме

Регистрация пользователя в распределенном режиме осуществляется без обязательного прибытия регистрирующегося лица (или его уполномоченного представителя) в Удостоверяющий Центр, и удобна в случае отдаленного расположения пользователей от Удостоверяющего Центра (например, в разных субъектах Российской федерации).

Регистрация пользователей в распределенном режиме может осуществляться:

- посредством **АРМ регистрации пользователя**, предоставляемого Удостоверяющим Центром и требующего непосредственной связи пользователя с Центром Регистрации (например, с использованием сети общего пользования Internet);
- на основе запроса на сертификат ключа подписи в виде файла, в случае автономного функционирования Удостоверяющего Центра или при отсутствии линий связи пользователей с Центром Регистрации.

Процедура регистрации в Удостоверяющем Центре состоит из двух этапов: занесение идентификационной информации регистрирующегося лица в реестр пользователей Удостоверяющего Центра и изготовление первого сертификата ключа подписи.

Регистрация пользователя осуществляется на основе запроса на регистрацию, переданного в электронном виде (либо при помощи **АРМ регистрации пользователя**, либо на основе файла запроса на сертификат ключа подписи, предоставленного средствами почтовой или курьерской связи). Подтверждение данных, содержащихся в запросе на регистрацию, осуществляется обязательным направлением в

Удостоверяющий Центр Заявления на регистрацию, оформленного в соответствии с положениями Регламента Удостоверяющего Центра.

Изготовление первого сертификата ключа подписи пользователя осуществляется на основе запроса на сертификат, переданного в электронном виде (либо при помощи **АРМ регистрации пользователя**, либо на основе файла запроса на сертификат ключа подписи, предоставленного средствами почтовой или курьерской связи). Подтверждение данных, содержащихся в запросе на сертификат, осуществляется обязательным направлением в Удостоверяющий Центр Заявления на изготовление сертификата.

Заявление на изготовление сертификата ключа подписи, оформляется установленным Регламентом образом, и должно содержать:

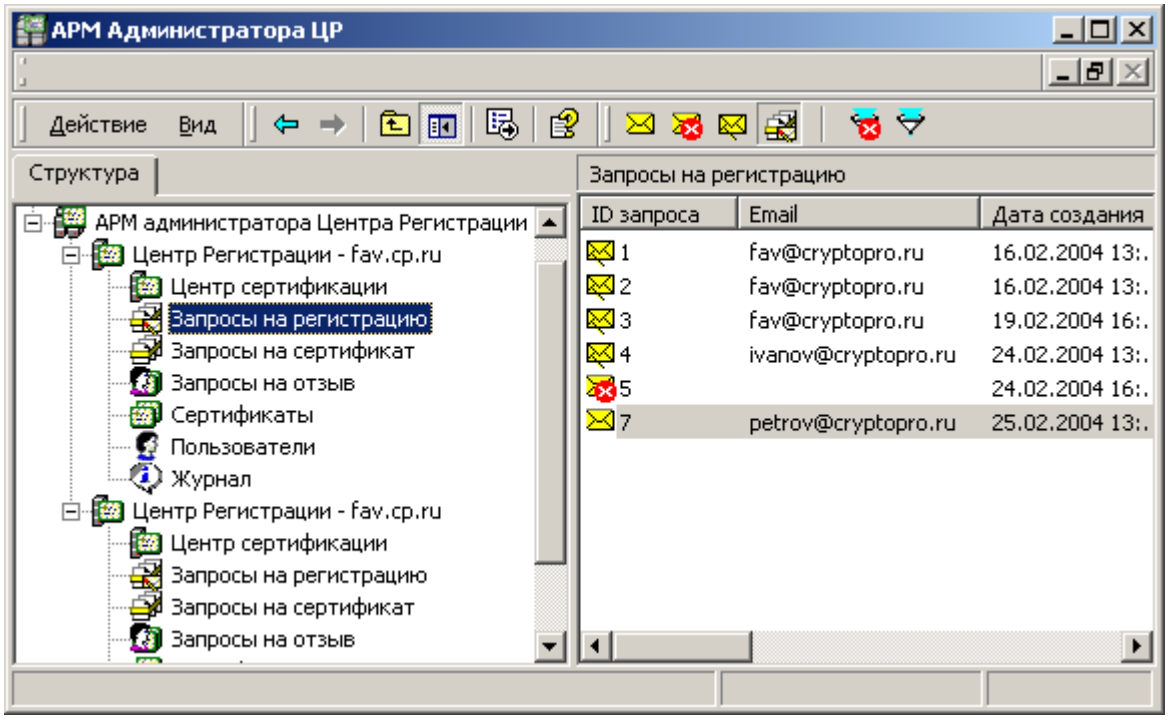
- идентификационные данные лица, на чье имя требуется изготовить сертификат;
- набор областей использования ключа и соответствующие этим областям объектные идентификаторы – OID'ы (содержание поля Extended Key Usage сертификата – наименование областей использования);
- В случае изготовления сертификата на основе предоставленного в виде файла запроса на сертификат – установленным образом оформленный бланк запроса на сертификат ключа подписи.

1.2.2.1. Регистрация пользователя в распределенном режиме с использованием **АРМ регистрации пользователя**

Описание процесса регистрации пользователя в распределенном режиме с использованием **АРМ регистрации пользователя:**

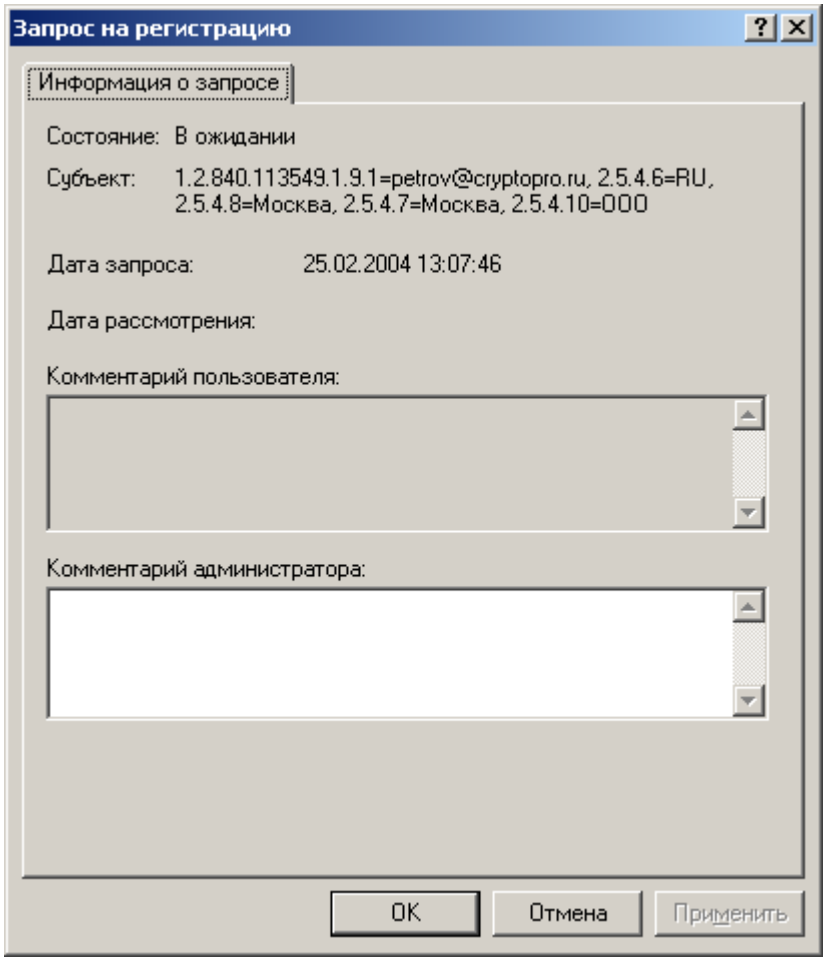
1. После получения Заявления на регистрацию Удостоверяющий Центр направляет доверенным каналом передачи данных (например, с использованием фельдъегерской почтовой или курьерской связи) в адрес регистрирующегося лица сертификат уполномоченного лица Удостоверяющего Центра и актуальный список отозванных сертификатов в электронном виде на магнитном носителе;
2. Пользователь устанавливает на своем рабочем месте сертификат уполномоченного лица Удостоверяющего Центра, список отозванных сертификатов и с помощью **АРМ регистрации пользователя** формирует и направляет в Удостоверяющий Центр запрос на регистрацию;
3. После отправки запроса регистрирующимся лицом в окне **АРМ администратора ЦР** в папке **Запросы на регистрацию** появляется новый запрос, ожидающий обработки;

Рисунок 33. Окно просмотра запросов на регистрацию пользователей



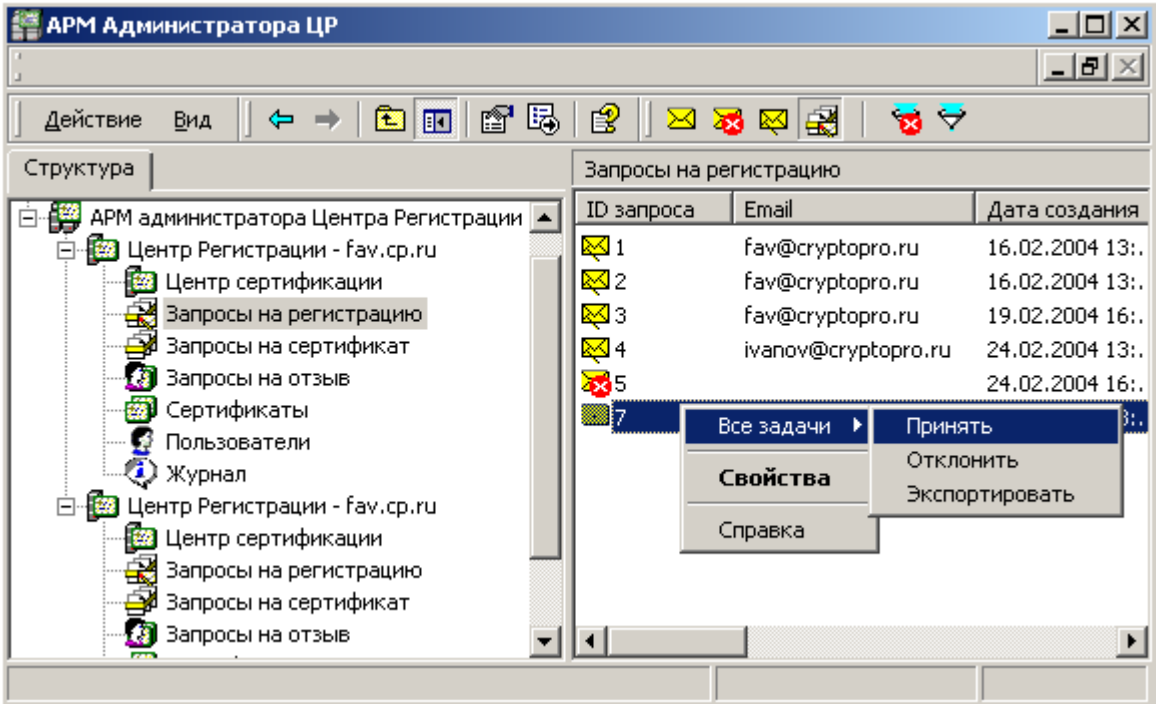
4. Выделите правой кнопкой мыши поступивший запрос на регистрацию и в открывшемся контекстном меню выберите пункт **Свойства.** Откроется окно свойств запроса на регистрацию;

Рисунок 34. Окно просмотра свойств запроса на регистрацию



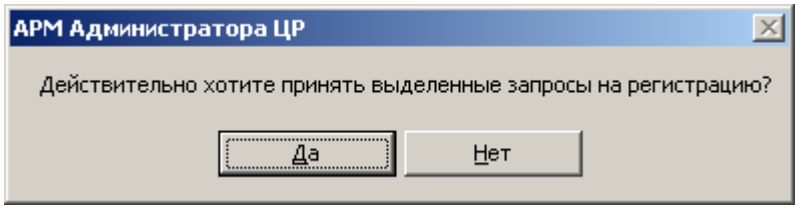
5. Внимательно проверьте идентичность идентификационных данных, содержащихся в поле **Субъект** данным, указанным в Заявлении на регистрацию, направленном ранее в Удостоверяющий Центр в бумажном виде. В случае полного соответствия данных в окне свойств запроса на регистрацию нажмите кнопку **ОК**, затем в окне **АРМ Администратора ЦР** выделите правой кнопкой мыши данный запрос на регистрацию и в открывшемся контекстном меню выберите **Принять;**

Рисунок 35. Принятие запроса на регистрацию



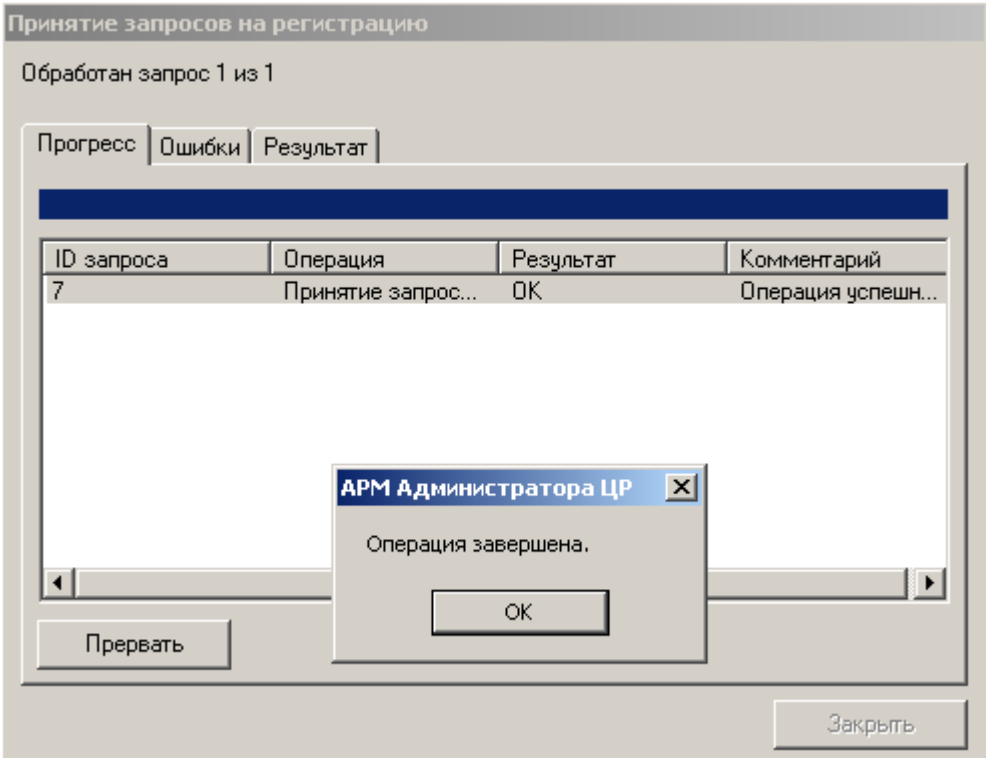
6. При принятии запроса на регистрацию откроется предупреждающее окно, требующее подтверждения выбранных действий. Нажмите кнопку **Да;**

Рисунок 36. Подтверждение действий по принятию запроса на регистрацию



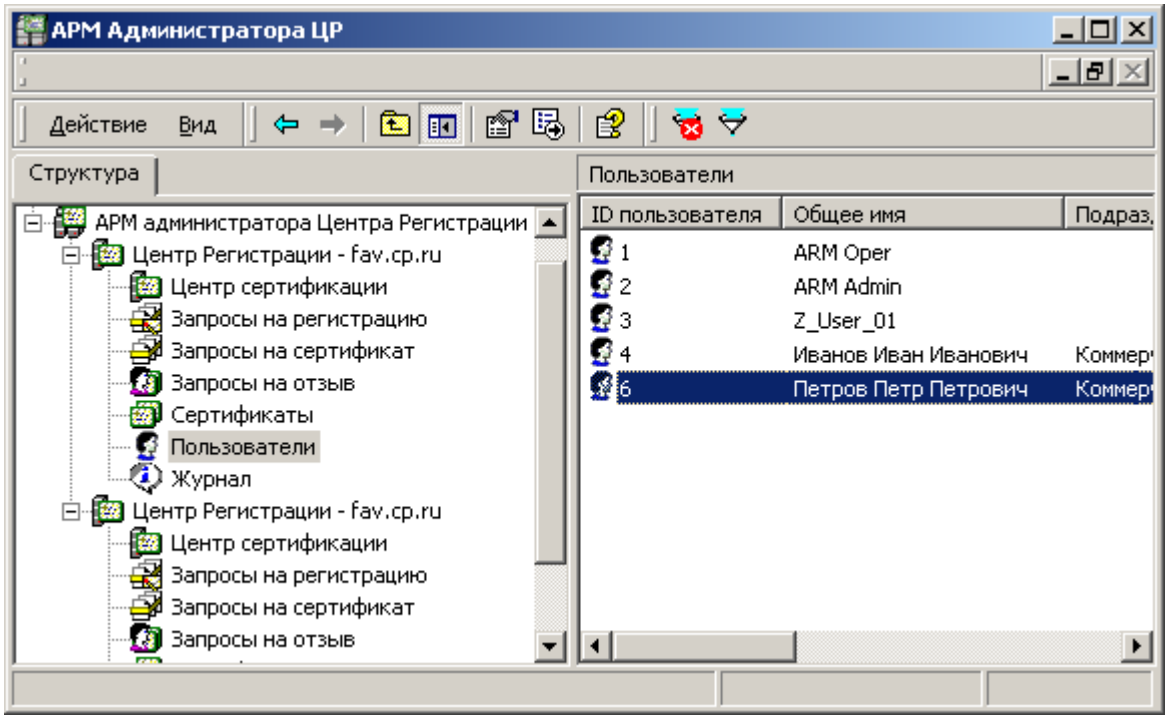
7. По окончании выполнения действий по занесению регистрационной информации в Реестр Удостоверяющего Центра появится сообщение, информирующее об окончании указанных операций, и их результат;

Рисунок 37. Окно просмотра результата регистрации пользователя



8. В окне **АРМ Администратора ЦР** выделите левой кнопкой мыши узел **Пользователи** и проверьте наличие учетной записи, соответствующей зарегистрированному пользователю;

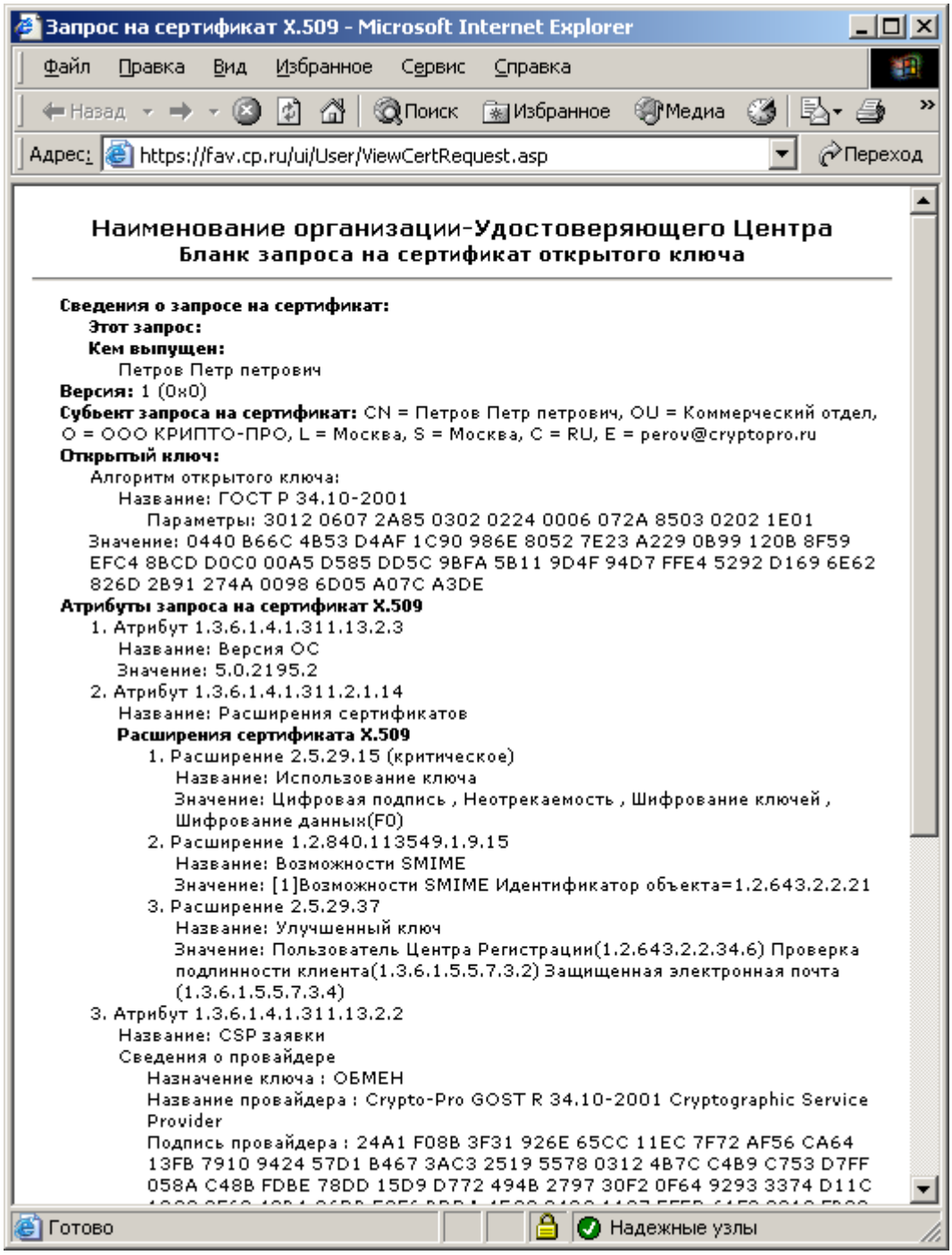
Рисунок 38. Окно просмотра зарегистрированных пользователей



По окончании осуществления действий, по созданию учетной записи зарегистрированного пользователя в Реестре Удостоверяющего Центра, целесообразно оповестить регистрирующееся лицо об этом. Для этого на Центре Регистрации необходимо настроить соответствующие задачи автоматического формирования и отправки почтовых сообщений (посредством электронной почты) в адрес регистрирующегося лица.

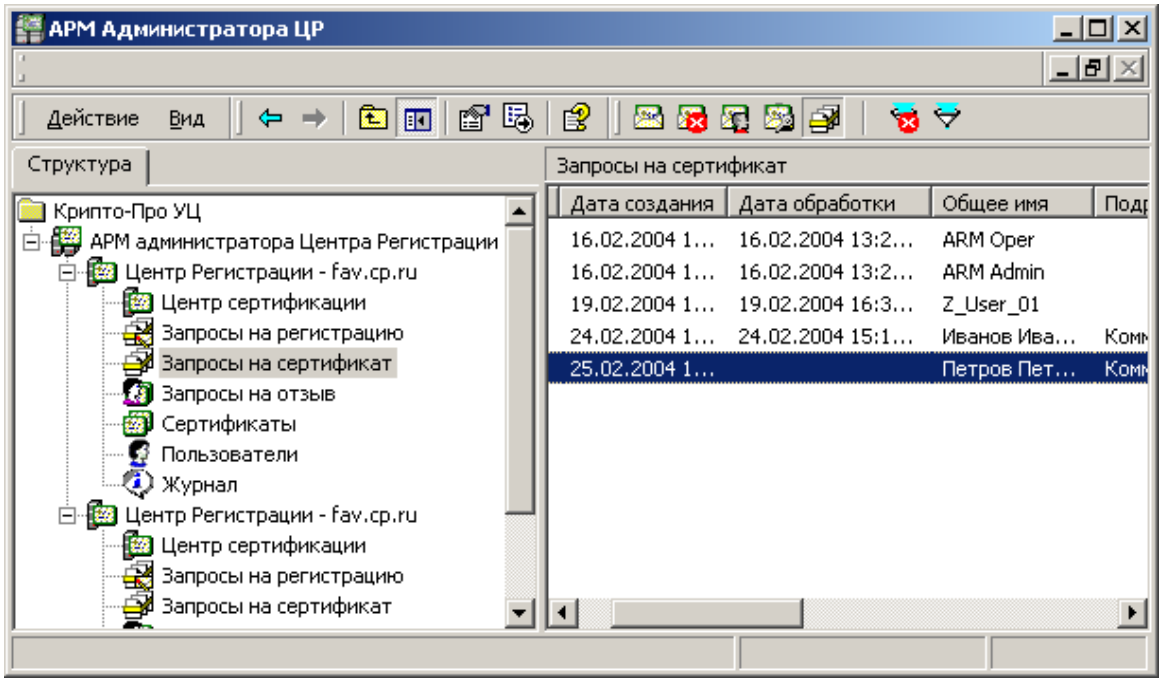
9. После получения уведомления об успешном занесении идентификационных данных в Реестр Удостоверяющего Центра регистрирующийся пользователь с помощью **АРМ пользователя, обладающего маркером временного доступа,** осуществляет на своем рабочем месте генерацию ключей, формирование запроса на сертификат ключа подписи и направляет его в Удостоверяющий Центр. Дополнительно регистрирующийся пользователь распечатывает бланк запроса на сертификат ключа подписи на бумажном носителе и в соответствии с Регламентом Удостоверяющего Центра направляет Заявление на изготовление сертификата ключа подписи (бланк запроса на сертификат является частью Заявления);

Рисунок 39. Шаблон бланка сертификата ключа подписи



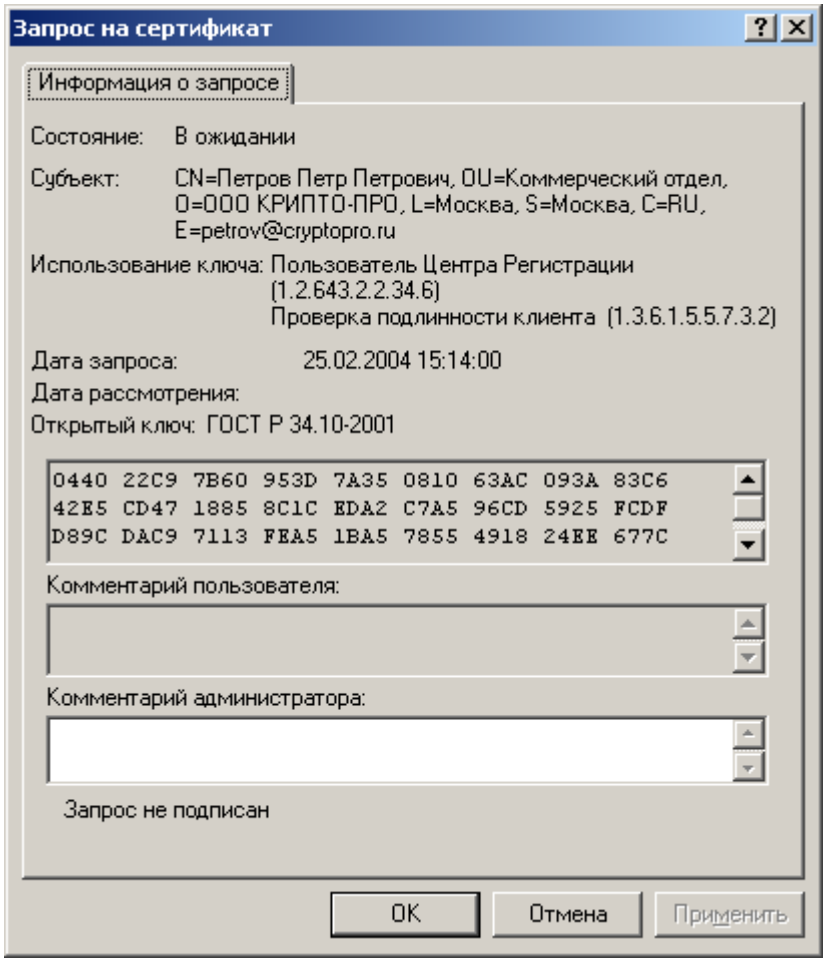
10. После отправки запроса на изготовление сертификата в окне **АРМ администратора ЦР** в папке **Запросы на сертификат** появляется новый запрос, ожидающий обработки;

Рисунок 40. Окно просмотра запросов на сертификат ключа подписи



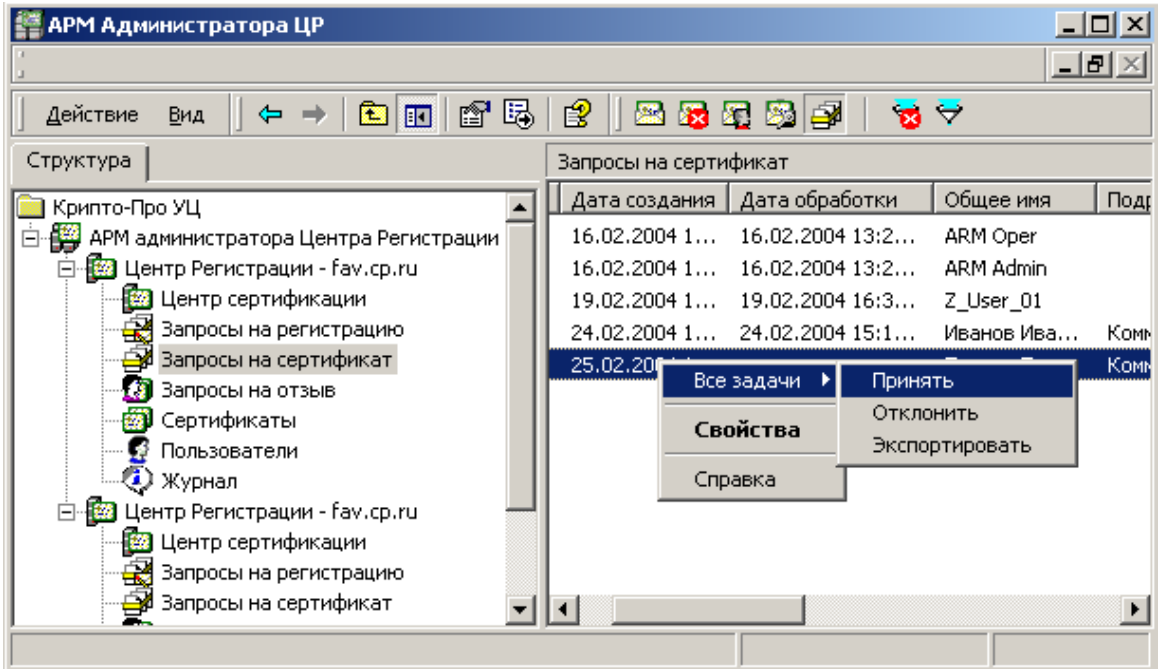
11. Выделите правой кнопкой мыши поступивший запрос на сертификат и в открывшемся контекстном меню выберите пункт **Свойства.** Откроется окно свойств запроса на сертификат;

Рисунок 41. Окно просмотра свойств запроса на сертификат



12. Внимательно проверьте идентичность данных, содержащихся в поле **Субъект**, **Использование ключа** и **Открытый ключ** данным, указанным в Заявлении на изготовление сертификата, направленном в Удостоверяющий Центр в бумажном виде. В случае полного соответствия данных в окне свойств запроса на сертификат нажмите кнопку **ОК**, затем в окне **АРМ Администратора ЦР** выделите правой кнопкой мыши данный запрос на сертификат и в открывшемся контекстном меню выберите **Принять;**

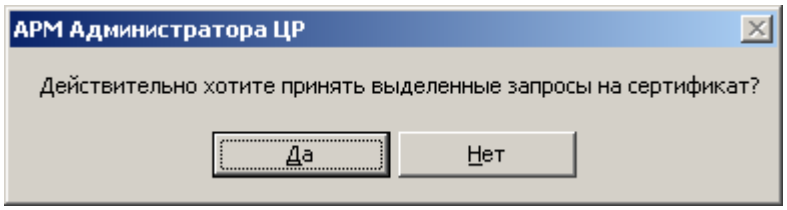
Рисунок 42. Принятие поступившего запроса на сертификат



Описанная процедура требует от лица, осуществляющего изготовление сертификата ключа подписи, повышенного внимания, поскольку данные, содержащиеся в поле **Использование ключа** определяют отношения, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение, и ошибка, допущенная на данном этапе, может привести к наделению пользователя дополнительными правами и привилегиями (к нелегитимному повышению его статуса).

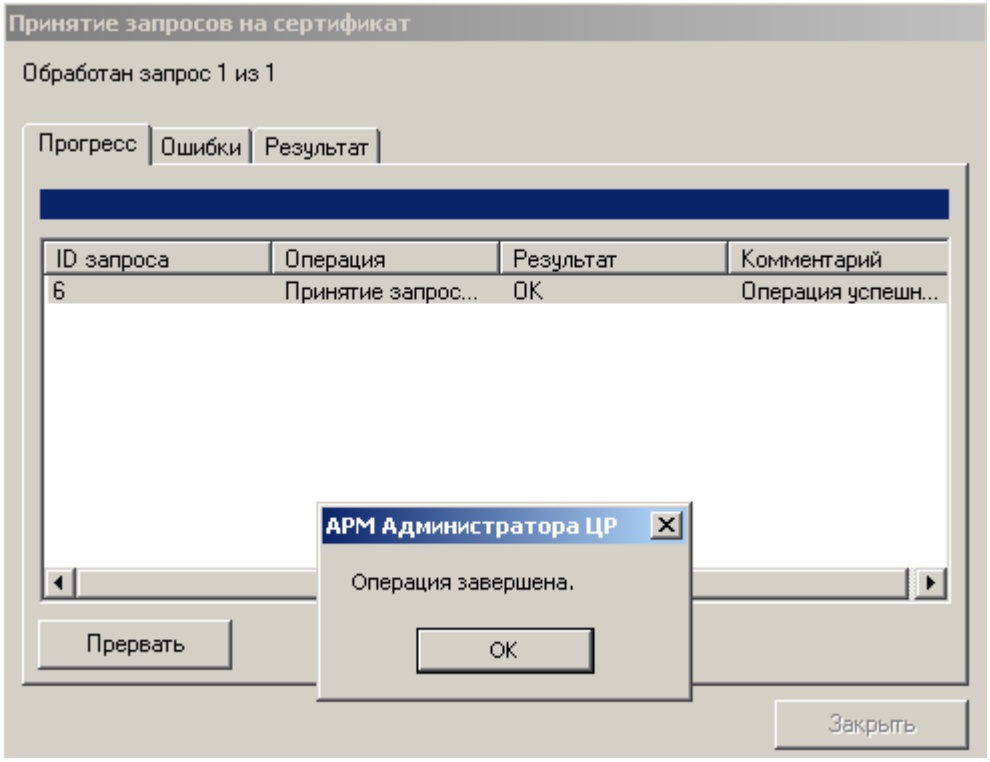
13. При принятии запроса на сертификат откроется предупреждающее окно, требующее подтверждения выбранных действий. Нажмите кнопку **Да**;

Рисунок 43. Окно подтверждения действий по принятию запроса на сертификат



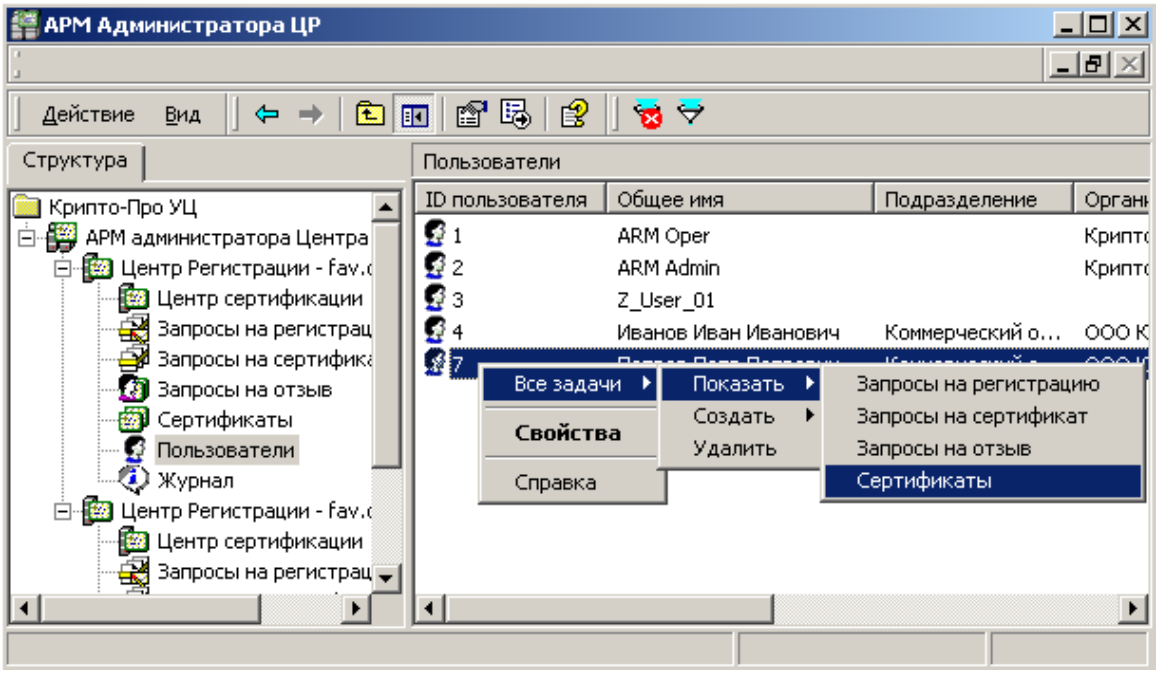
14. По окончании выполнения действий по изготовлению сертификата ключа подписи появится сообщение, информирующее об окончании указанных операций, и их результат;

Рисунок 44. Окно просмотра результата принятия запроса на сертификат



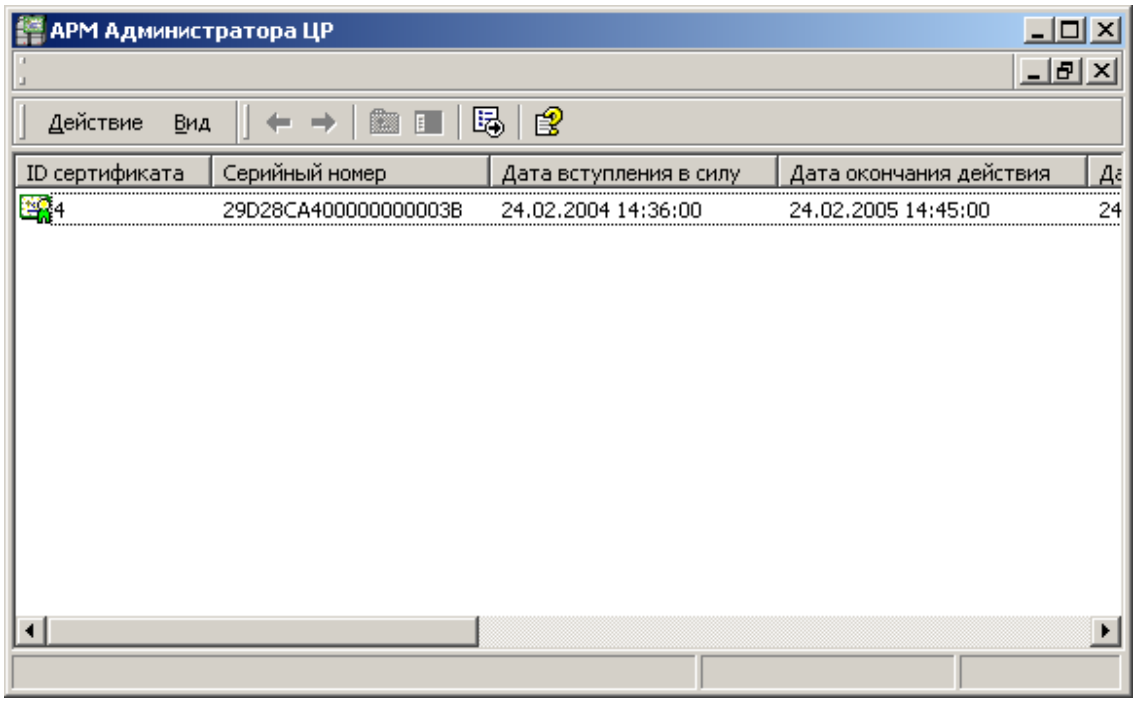
15. В правой области окна **АРМ Администратора ЦР** выделите левой кнопкой мыши узел **Пользователи**, затем в правой части окна выделите правой кнопкой мыши учетную запись зарегистрировавшегося пользователя и в открывшемся контекстном меню выберите пункт **Все задачи -> Показать -> Сертификаты;**

Рисунок 45. Выбор просмотра сертификатов зарегистрированного пользователя



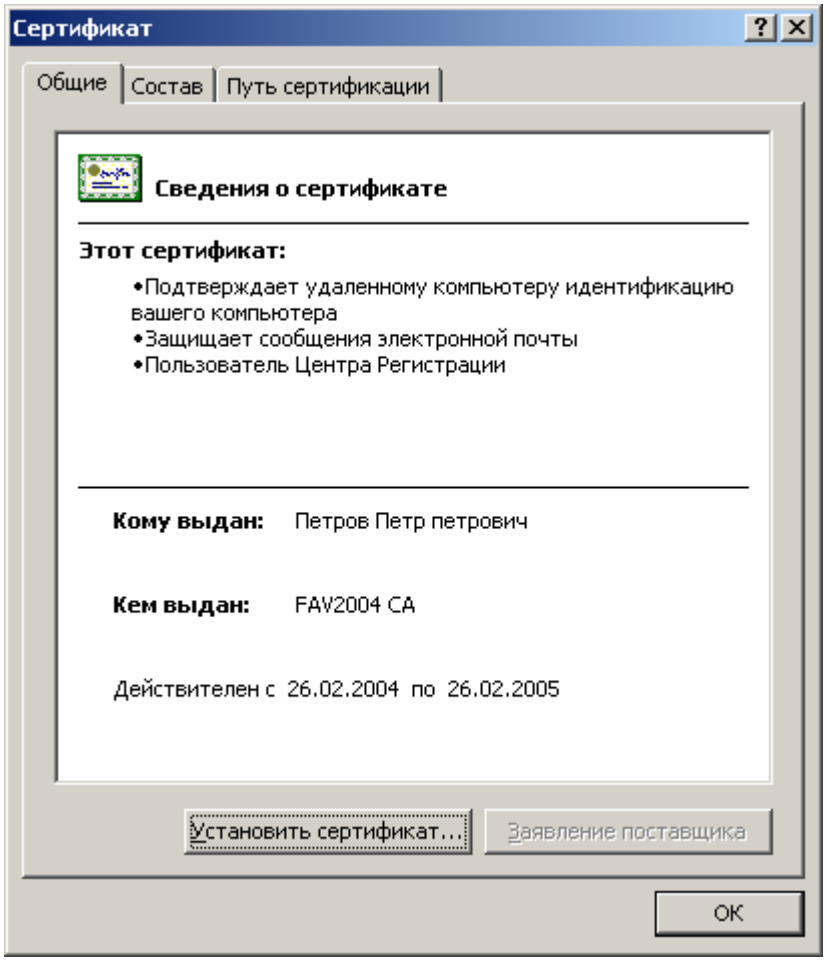
16. Откроется окно просмотра изданных сертификатов зарегистрировавшегося пользователя;

Рисунок 46. Окно просмотра изданных сертификатов пользователя



17. Выделите изготовленный сертификат ключа подписи двойным нажатием левой кнопки мыши и просмотрите его в стандартном окне просмотра сертификатов.

Рисунок 47. Стандартное окно просмотра сертификата ключа подписи



По окончании осуществления действий по изготовлению сертификата ключа подписи, целесообразно оповестить владельца изготовленного сертификата об этом. Для этого на Центре Регистрации необходимо настроить соответствующие задачи автоматического формирования и отправки почтовых сообщений (посредством электронной почты) в адрес владельца сертификата ключа подписи.

1.2.2.2. Регистрация пользователя в распределенном режиме на основе запроса на сертификат в виде файла

Данный метод регистрации пользователя используется в том случае, когда генерация ключей пользователя должна осуществляться только на его рабочем месте, а функционирование Удостоверяющего Центра осуществляется автономно или конечный пользователь не имеет линий связи с Центром Регистрации Удостоверяющего Центра.

Формирование пользователем запроса на сертификат осуществляется с использованием специально разрабатываемого программного обеспечения, осуществляющего выполнение следующих функций:

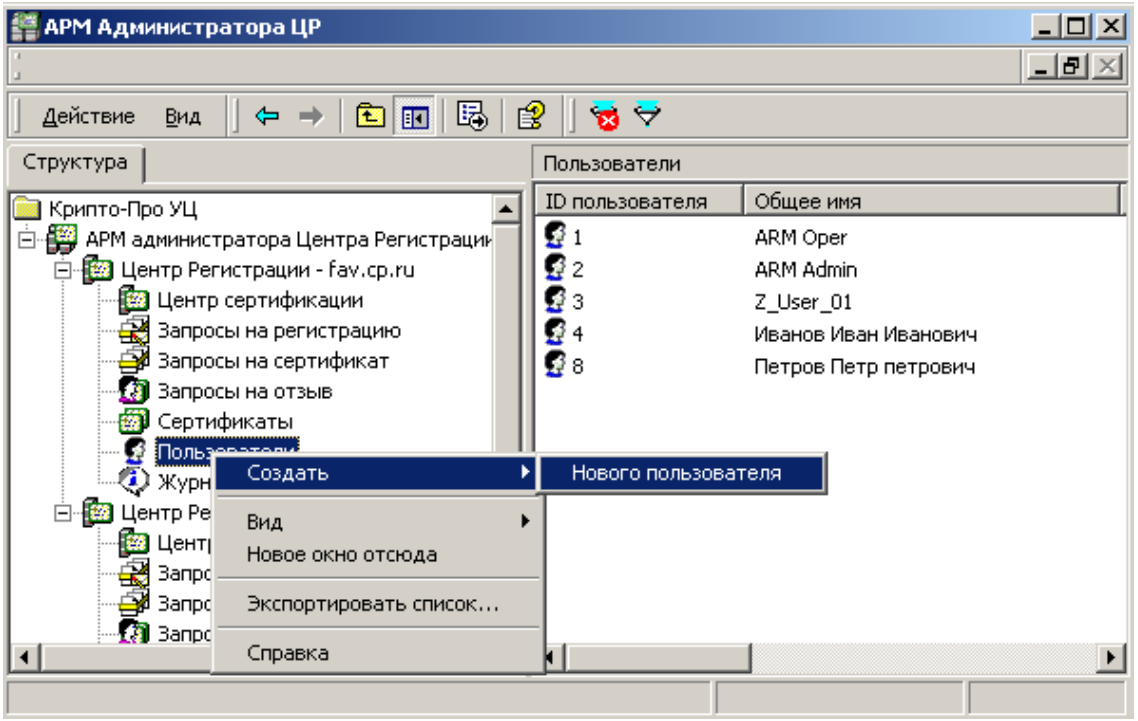
- Генерация закрытого и открытого ключа подписи;
- Формирование запроса на сертификат ключа подписи;
- Формирование бланка запроса на сертификат ключа подписи;
- Установка изготовленного сертификата ключа подписи

Описание процесса регистрации пользователя в распределенном режиме на основе запроса на сертификат в виде файла:

1. Регистрирующееся лицо на своем рабочем месте генерирует закрытый и открытый ключ, формирует запрос на сертификат ключа подписи в виде файла, распечатывает и оформляет бланк запроса на сертификат ключа подписи и доверенным каналом связи предоставляет указанные данные в Удостоверяющий Центр;

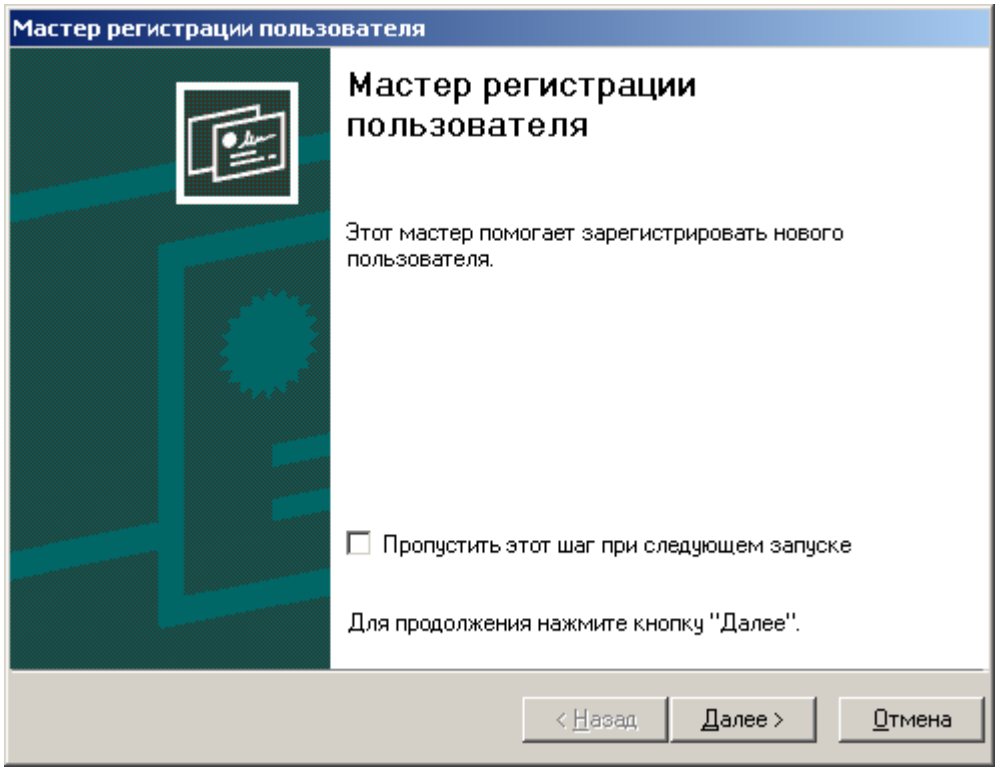
2. После предоставления пользователем необходимых данных в окне **АРМ администратора ЦР** правой кнопкой мыши выделите узел **Пользователи** и в открывшемся контекстном меню выберите **Создать -> Нового пользователя;**

Рисунок 48. Выбор пункта меню создания нового пользователя



3. Запустится **Мастер регистрации пользователя**, нажмите кнопку **Далее;**

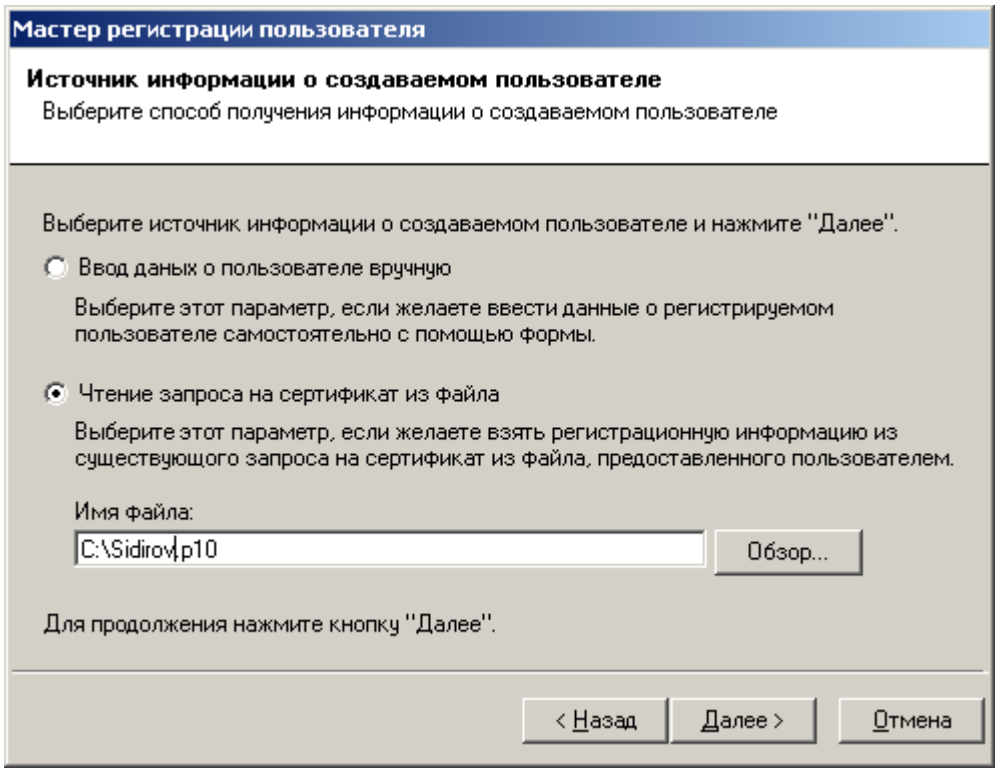
Рисунок 49. Первое окно Мастера регистрации пользователя



Для отключения вывода первого окна **Мастера регистрации пользователя** установите «галку» **Пропустить этот шаг при следующем запуске.**

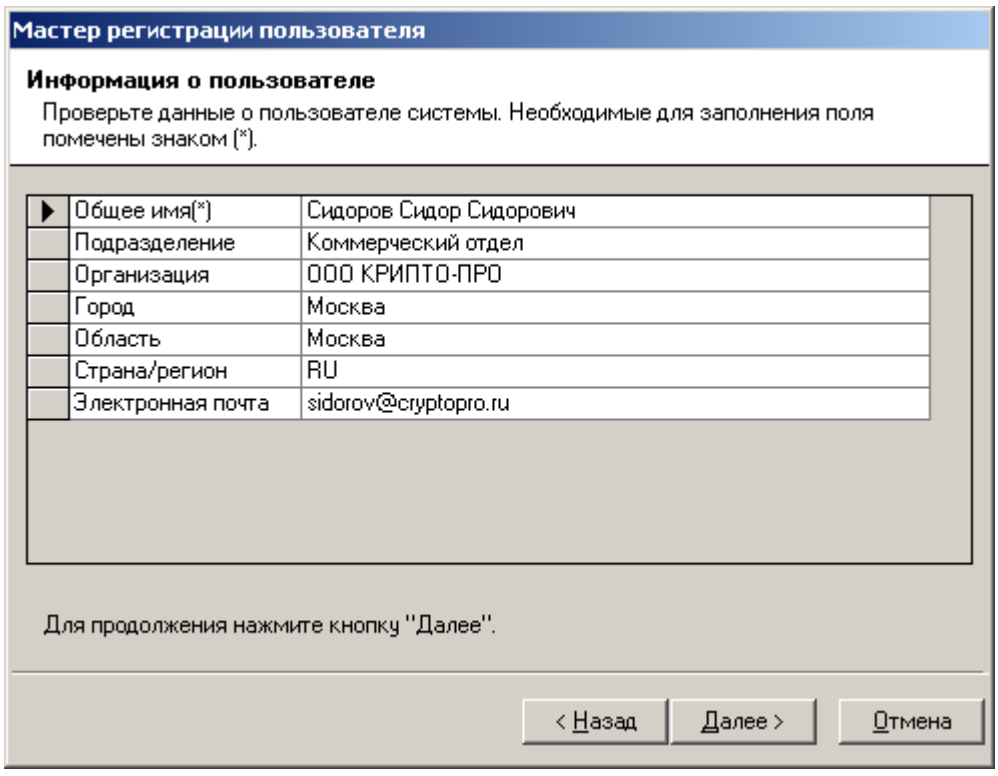
4. Откроется окно **Источник информации о создаваемом пользователе**, в котором выберите переключатель **Чтение запроса на сертификат из файла** и с помощью кнопки **Обзор** укажите имя файла, содержащего запрос на сертификат ключа подписи формата PKCS#10. Нажмите кнопку **Далее;**

Рисунок 50. Выбор способа получения информации о пользователе с использованием запроса на сертификат



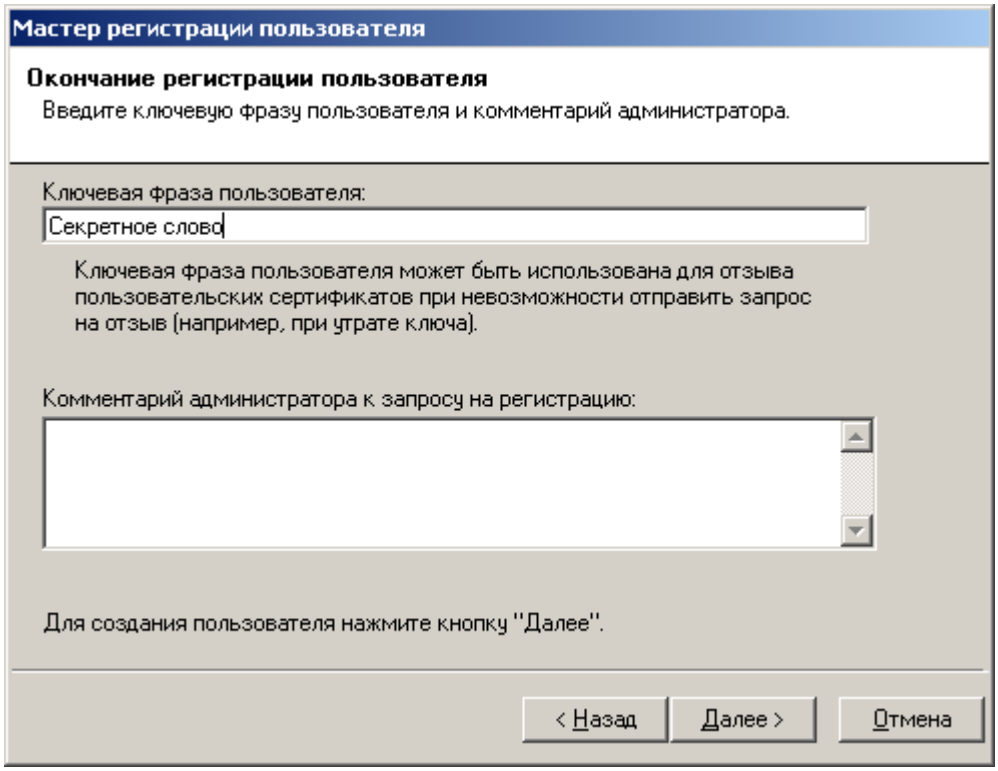
5. В открывшемся окне **Информация о пользователе** внимательно сравните указанные идентификационные данные с идентификационными данными, содержащимися в Заявлении на регистрацию, и в случае идентичности этих данных нажмите кнопку **Далее;**

Рисунок 51. Окно информации о пользователе



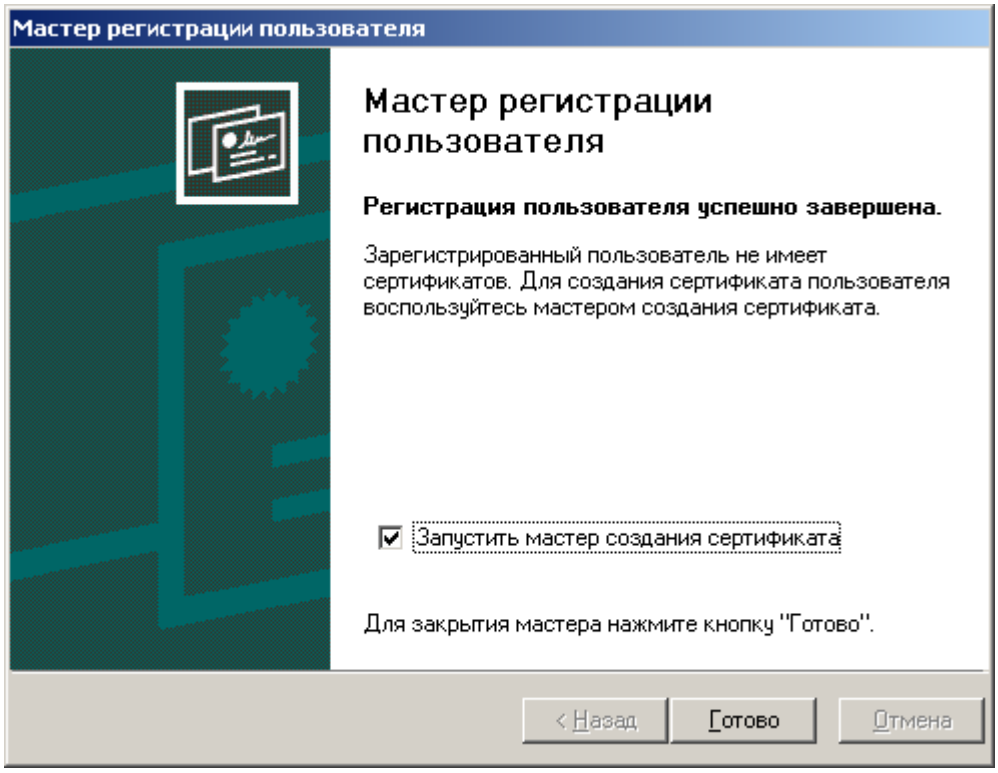
6. В окне **Окончание регистрации пользователя** введите **Ключевую фразу пользователя**, при необходимости напишите комментарий и нажмите кнопку **Далее;**

Рисунок 52. Ввод ключевой фразы пользователя и комментария администратора



7. В завершающем окне **Мастера регистрации пользователя** установите «галку» **Запустить мастер создания сертификата** и нажмите кнопку **Готово;**

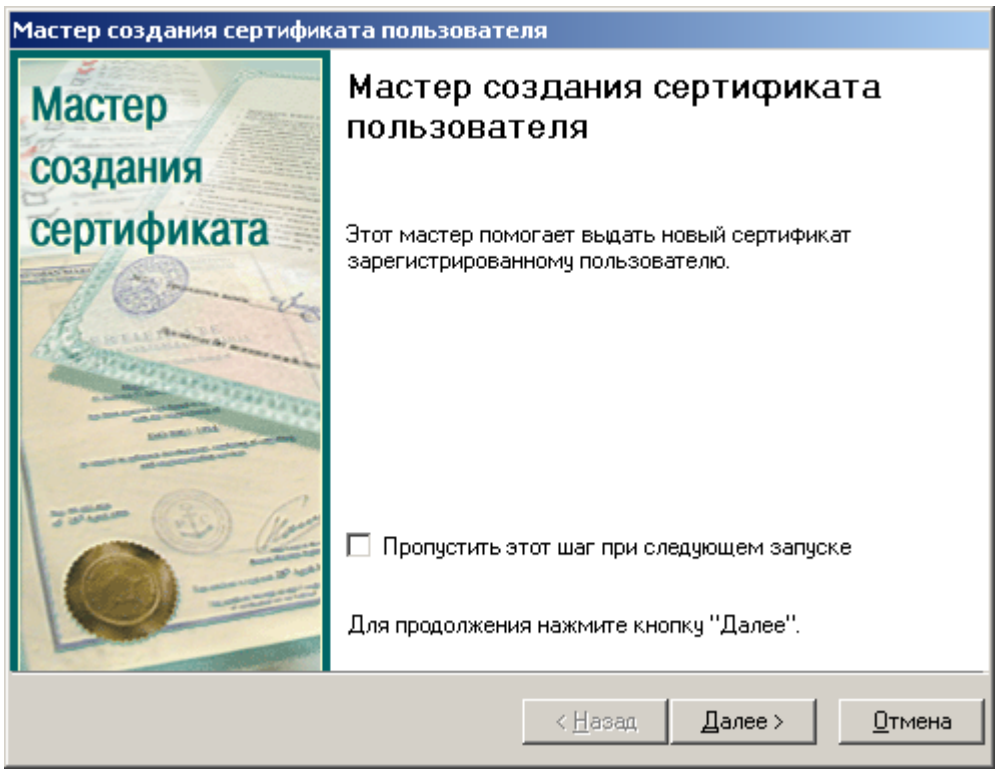
Рисунок 53. Завершающее окно Мастера регистрации пользователя



Снятие переключателя **Запустить мастер создания сертификата** заканчивает процедуру регистрации пользователя. В этом случае пользователь не является владельцем ни одного сертификата ключа подписи. Последующее изготовление сертификата осуществляется с помощью задач контекстного меню зарегистрированного пользователя.

8. Запустится **Мастер создания сертификата пользователя**, нажмите кнопку **Далее;**

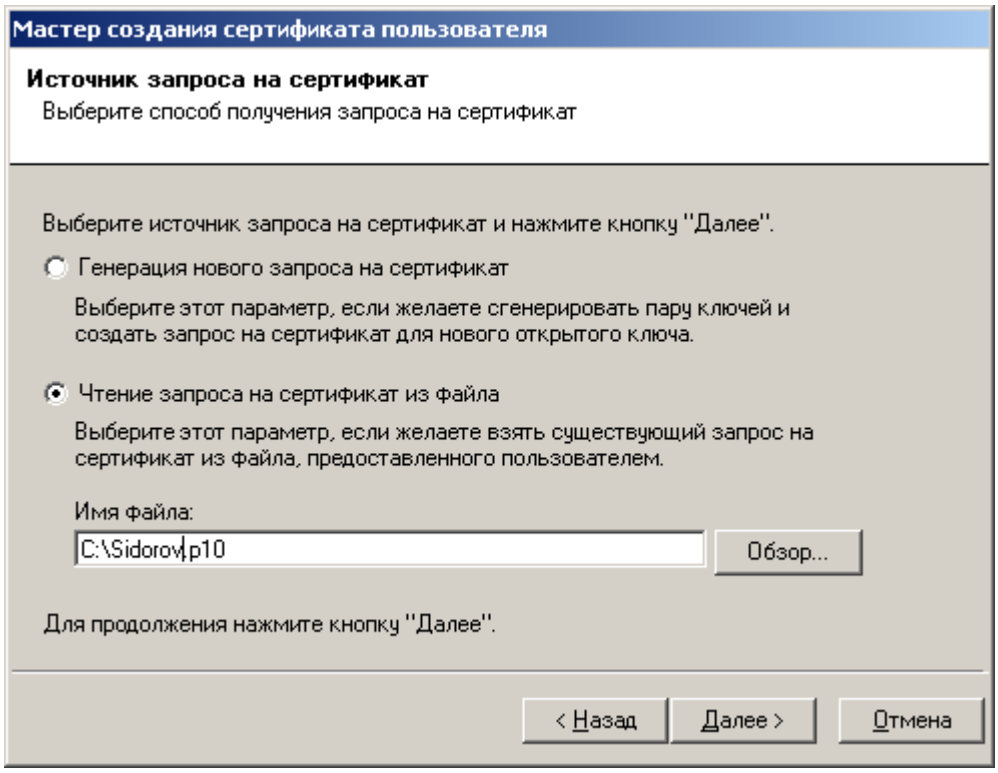
Рисунок 54. Первое окно Мастера создания сертификата пользователя



Для отключения вывода первого окна **Мастера создания сертификата пользователя** установите «галку» **Пропустить этот шаг при следующем запуске.**

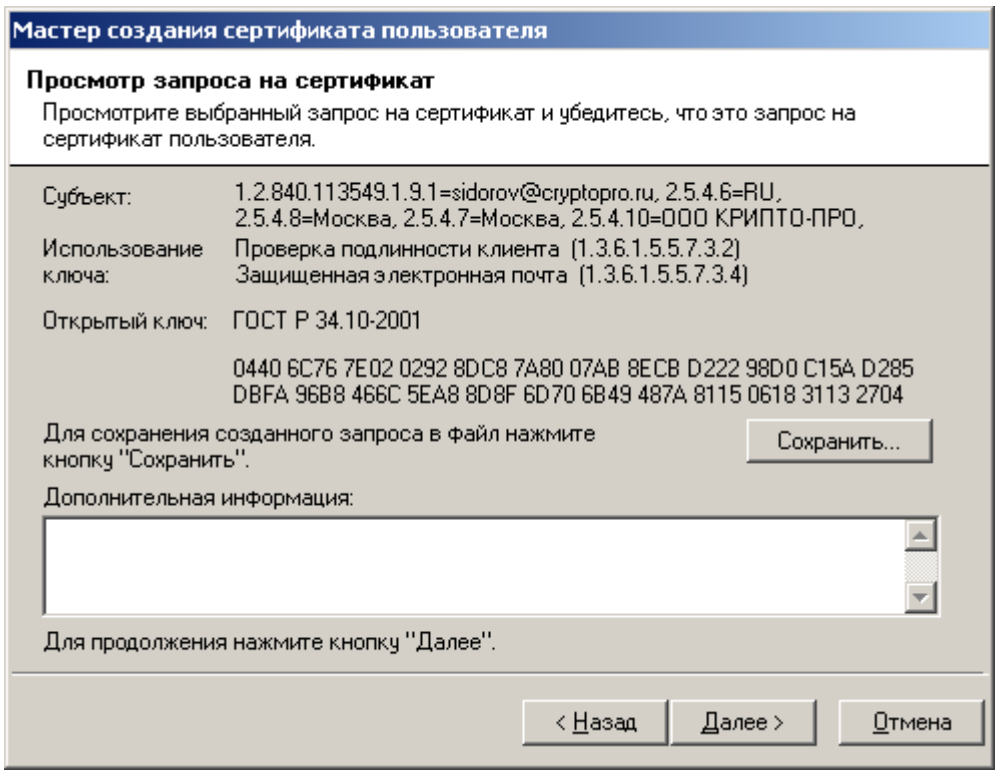
9. В открывшемся окне **Источник запроса на сертификат** выберите переключатель **Чтение запроса на сертификат из файла** и введите имя файла, использовавшееся при регистрации пользователя (с помощью **Мастера регистрации пользователя**), и нажмите кнопку **Далее;**

Рисунок 55. Выбор способа получения запроса на сертификат из существующего файла



10. В окне **Просмотр запроса на сертификат** внимательно проверьте идентичность данных, указанных в полях **Субъект**, **Использование ключа**, **Открытый ключ** данным, содержащимся в Заявлении на сертификат (бланке запроса на сертификат). Только в случае полного совпадения этих данных нажмите кнопку **Далее;**

Рисунок 56. Окно просмотра запроса на сертификат




Описанная процедура требует от лица, осуществляющего изготовление сертификата ключа подписи, повышенного внимания, поскольку данные, содержащиеся в поле **Использование ключа** определяют отношения, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение, и ошибка, допущенная на данном этапе, может привести к наделению пользователя дополнительными правами и привилегиями (к нелегитимному повышению его статуса).

11. Откроется окно **Установка сертификата пользователя**, информирующее об успешном изготовлении сертификата ключа подписи и позволяющее:

- осуществить просмотр изготовленного сертификата, нажатием кнопки **Просмотр...;**
- сохранить изготовленный сертификат в виде файла формата **PKCS#7**, нажатием кнопки **Сохранить...;**
- установить сертификат в хранилище (осуществляется установкой соответствующего переключателя);
- автоматически подтвердить запрос (осуществляется установкой соответствующего переключателя);

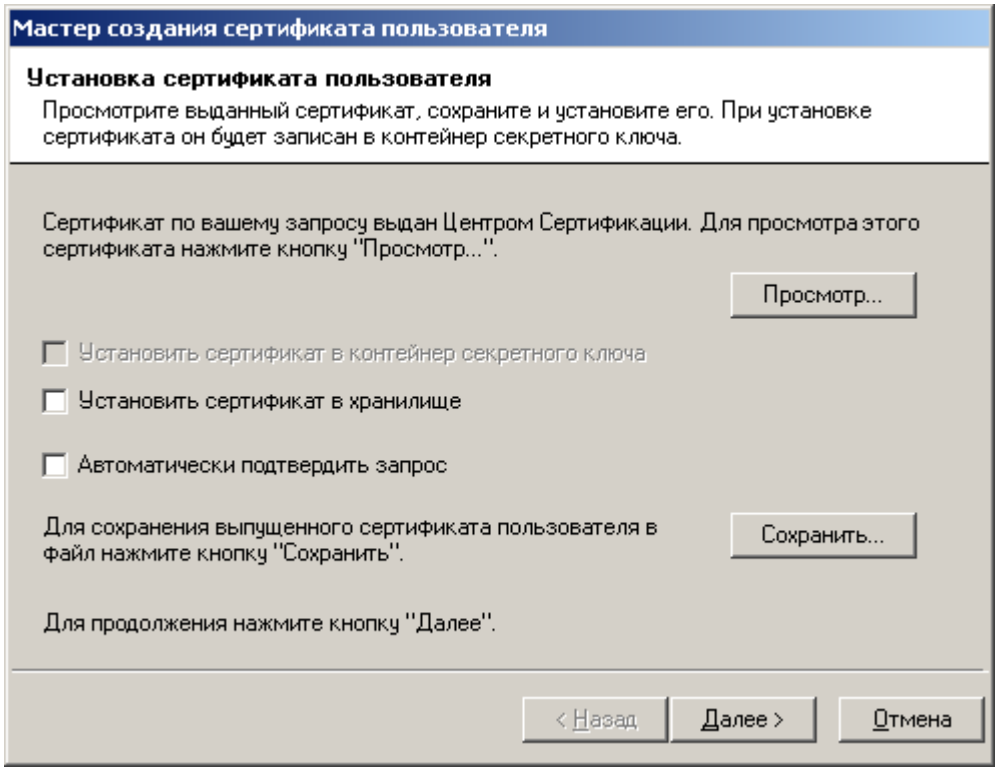
Осуществите установку переключателей, произведите необходимые действия и нажмите кнопку **Далее;**


Порядок предоставления пользователю изготовленного сертификата ключа подписи определяется Регламентом Удостоверяющего Центра. В случае предоставления пользователю сертификата на сменном магнитном носителе (например, посредством почтовой связи) удобно воспользоваться кнопкой **Сохранить...** данного окна.

Выбор переключателя **Установить сертификат в хранилище** приводит к инсталляции изданного сертификата в хранилище **Сертификаты/Текущий пользователь/Другие пользователи** на ПЭВМ **АРМ Администратора ЦР**. Использование данного переключателя удобно для организации защищенного почтового обмена между привилегированным пользователем и пользователями Удостоверяющего Центра (например, с использованием почтовых клиентов Microsoft Outlook, Microsoft Outlook Express).

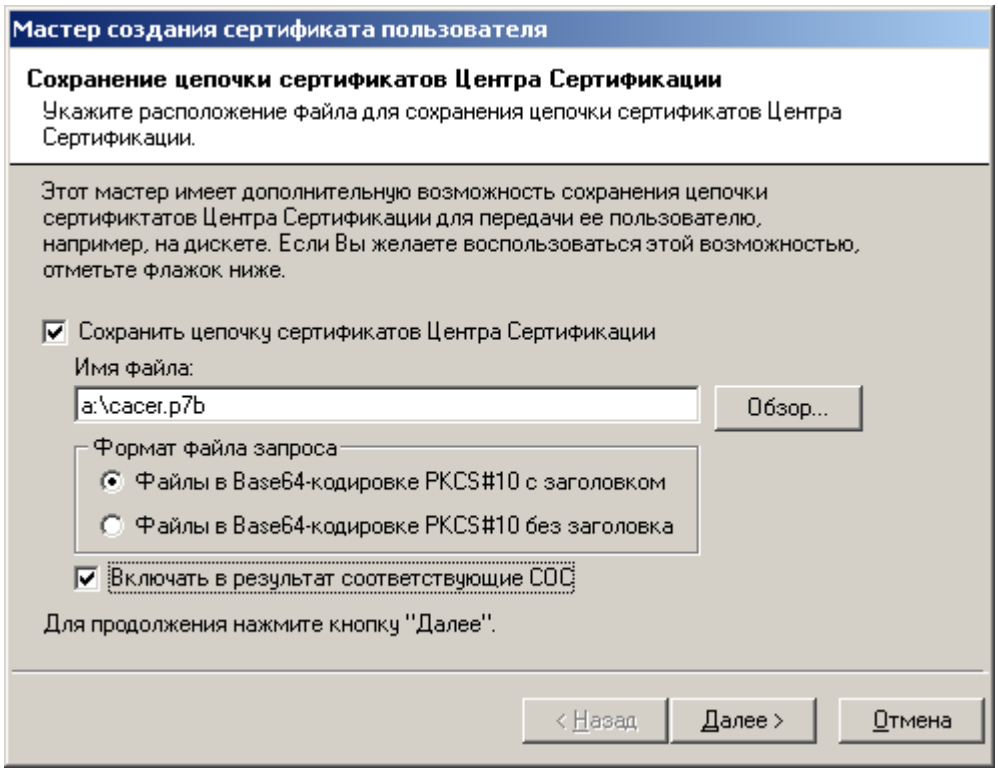
Выбор переключателя **Автоматически подтвердить запрос** устанавливает статус данного запроса в состояние **Завершен** и не требует подтверждения пользователем установки изготовленного сертификата на своей ПЭВМ. Подтверждение пользователем установки осуществляется с использованием АРМ зарегистрированного пользователя, являющегося web-приложением Центра Регистрации Удостоверяющего Центра, и требует обязательного сетевого соединения между ПЭВМ пользователя и Центром Регистрации. Рекомендуется использовать указанный переключатель в случае автономного функционирования Удостоверяющего Центра.

Рисунок 57. Окно установки сертификата пользователя



12. Окно **Сохранение цепочки сертификатов Центра Сертификации** позволяет сохранить все сертификаты издателей и списки отозванных сертификатов, обеспечивающие проверку статуса сертификатов, изданных Удостоверяющим Центром. При необходимости, установите переключатели **Сохранить цепочку сертификатов Центра Сертификации** и **Включать в результат соответствующие СОС** и введите полный путь для размещения указанных данных. Нажмите кнопку **Далее**.

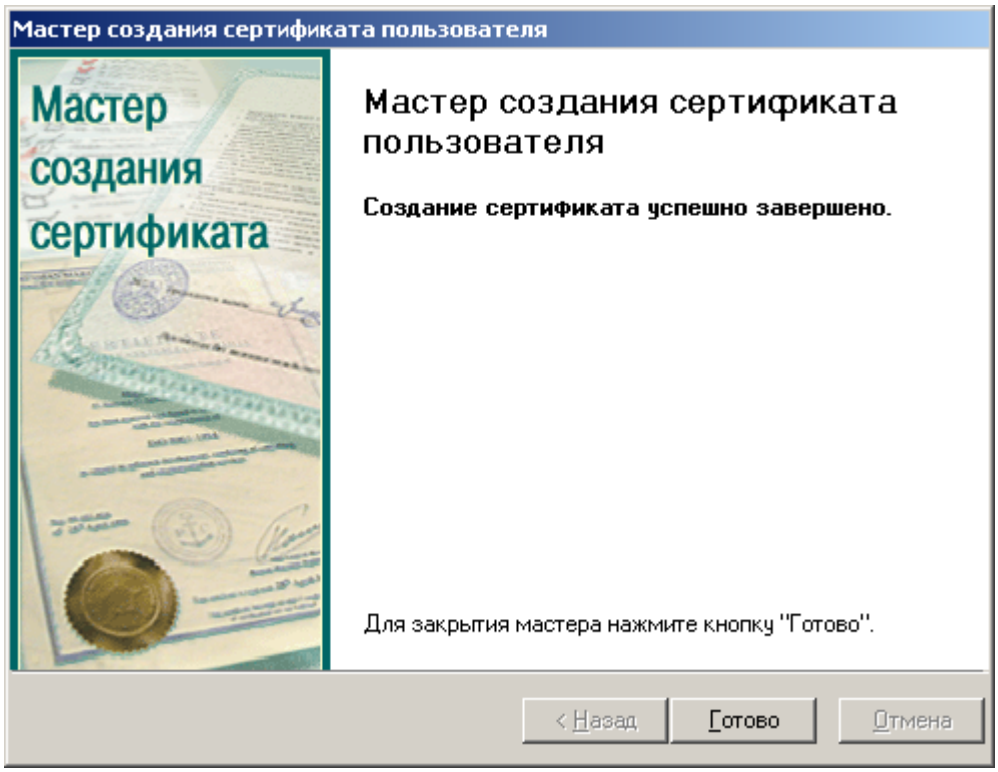
Рисунок 58. Окно сохранения цепочки сертификатов и списков отозванных сертификатов



В случае предоставления пользователю изготовленного сертификата ключа подписи на сменном магнитном носителе (например, посредством почтовой связи) целесообразно записать на этот же носитель и актуальный список отозванных сертификатов.

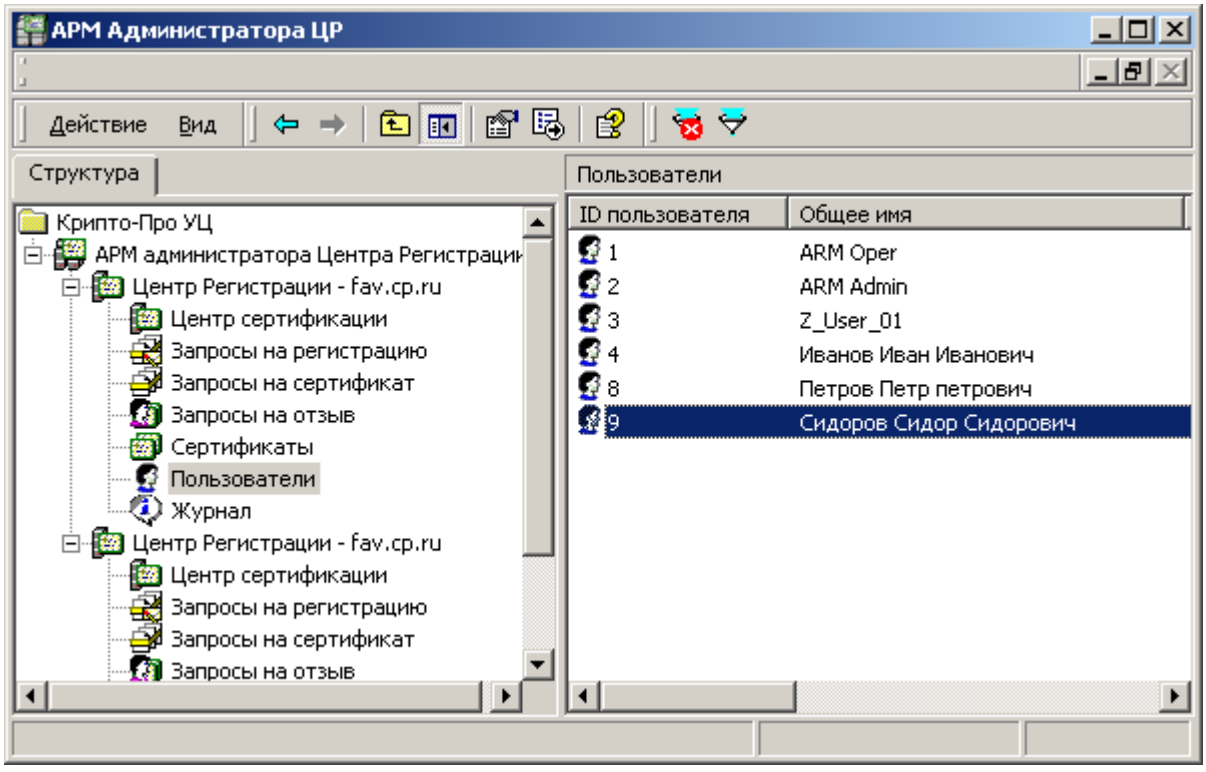
13. После успешного осуществления описанных действий откроется окно, информирующее об успешном изготовлении сертификата. Нажмите кнопку **Готово;**

Рисунок 59. Заключительное окно Мастера создания сертификата пользователя



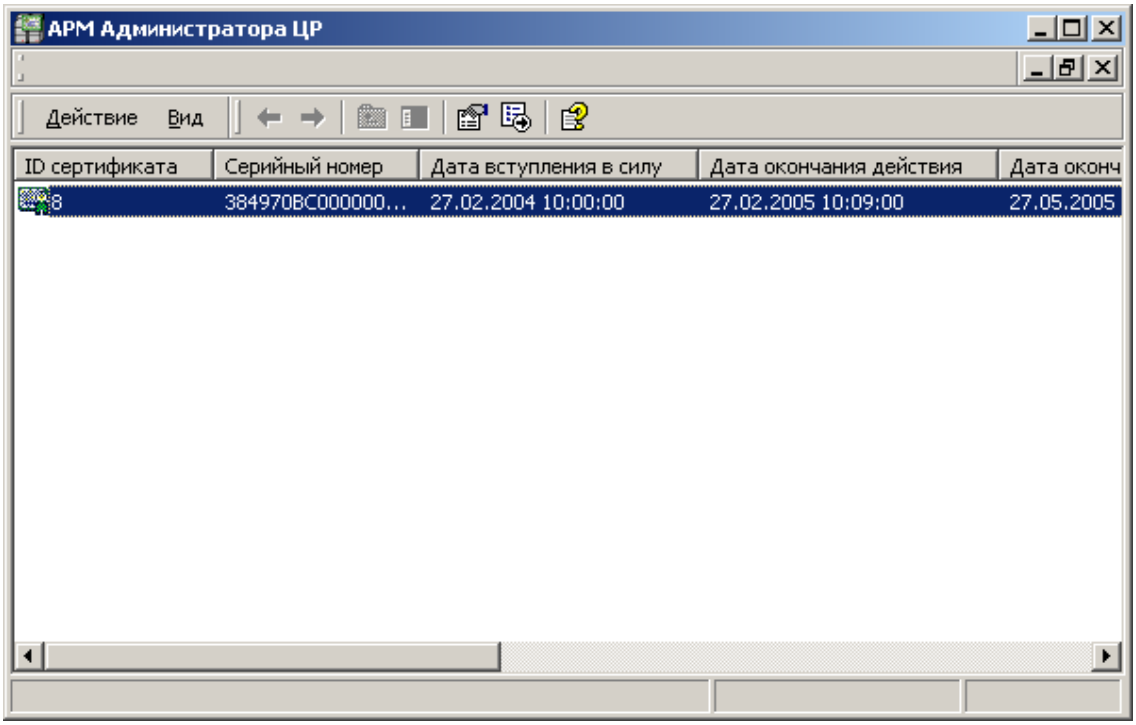
14. В левой части окна **АРМ администратора ЦР** выделите узел **Пользователи** и в правой части окна проверьте наличие учетной записи, соответствующей зарегистрированному пользователю;

Рисунок 60. Просмотр учетных записей зарегистрированных пользователей



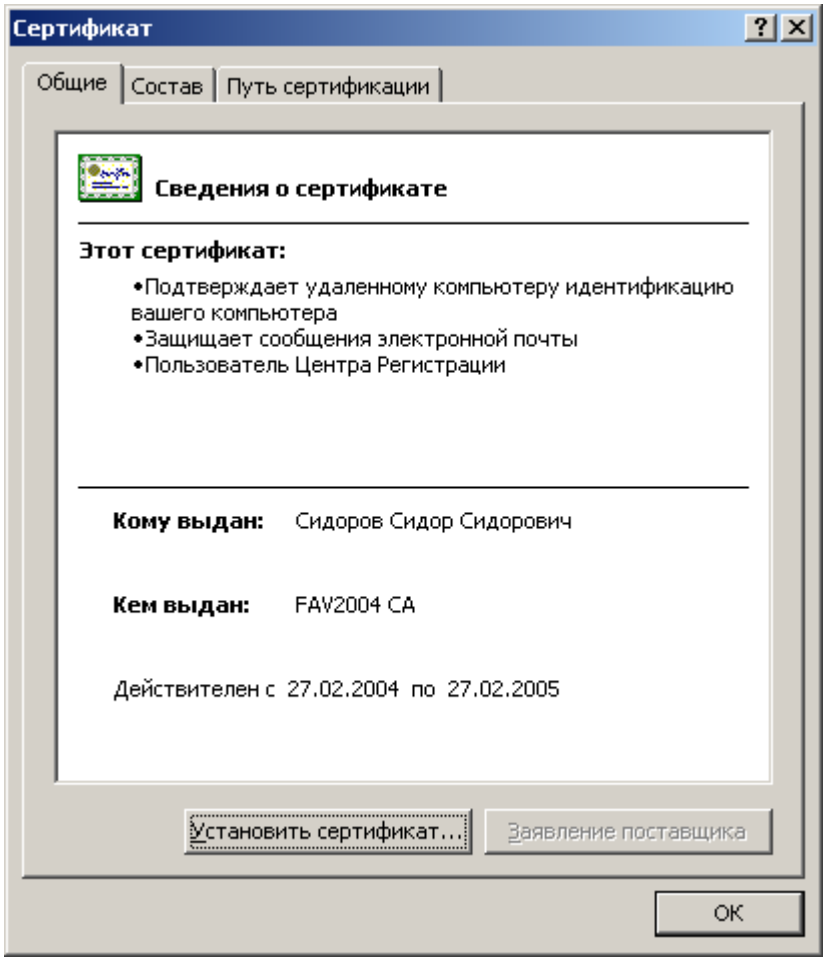
15. Правой кнопкой мыши выделите созданную учетную запись и в контекстном меню выберите **Все задачи->Показать->Сертификаты;**

Рисунок 61. Просмотр изданных сертификатов зарегистрированного пользователя



16. Выделите изготовленный сертификат ключа подписи двойным нажатием левой кнопки мыши и просмотрите его в стандартном окне просмотра сертификатов;

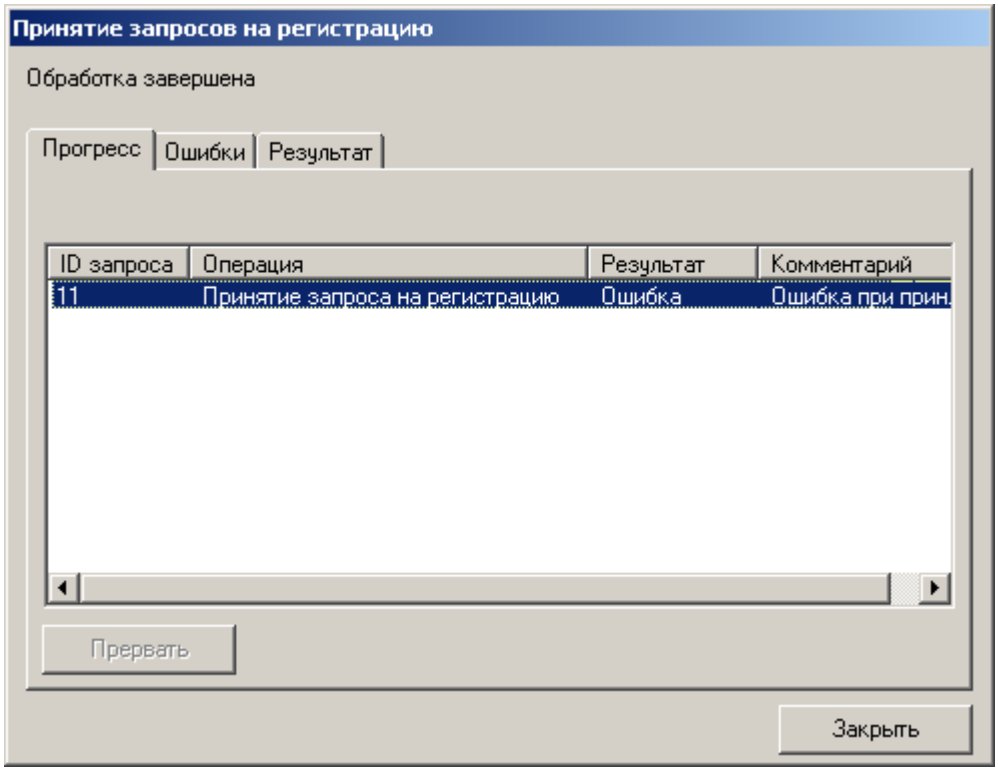
Рисунок 62. Стандартное окно просмотра сертификата

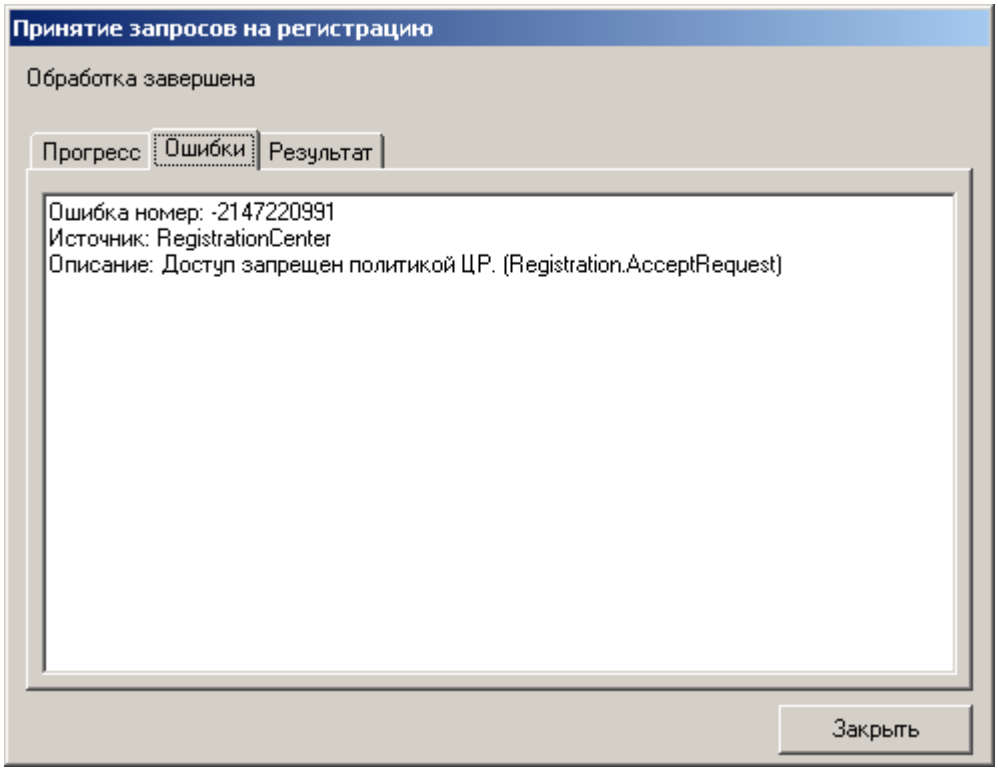


1.2.2.3. Наиболее часто встречающиеся ошибки, возникающие при регистрации пользователя в распределенном режиме

1. При принятии запроса на регистрацию (**АРМ Администратора ЦР –> Запросы на регистрацию -> Запрос -> Все задачи -> Принять**) в открывшемся окне, информирующем об окончании проделанных операций, появляется сообщение об ошибке

Рисунок 63. Ошибка при выполнении метода Registration.AcceptRequest





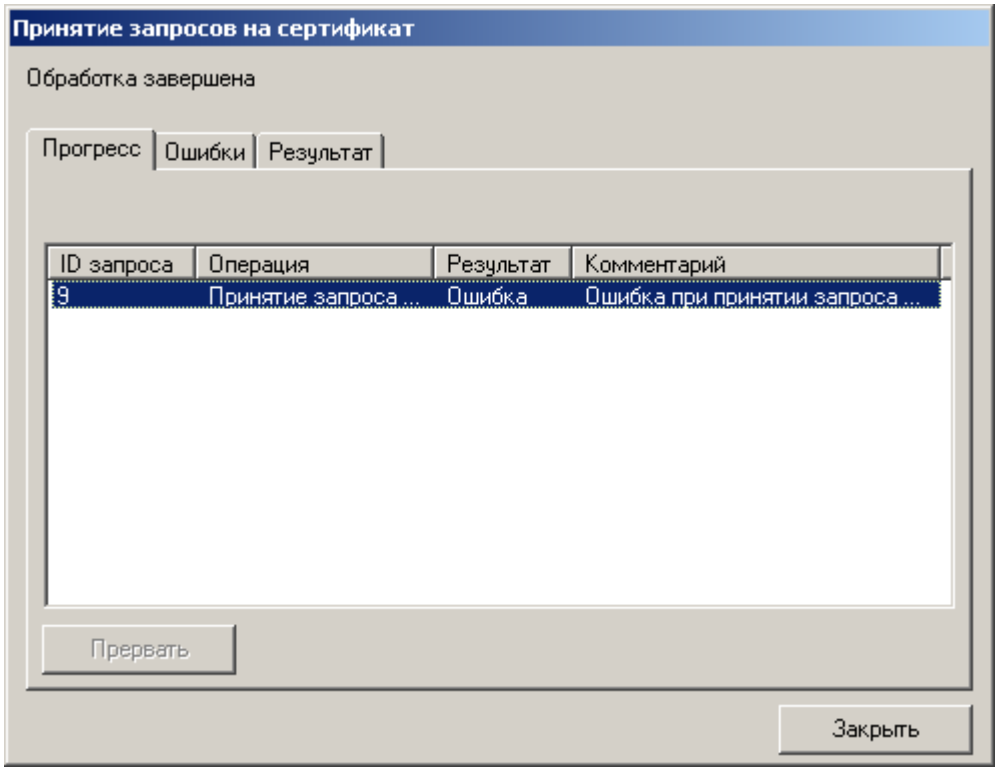
У привилегированного пользователя (**Оператора** или **Администратора**), производящего регистрацию пользователя в Удостоверяющем Центре, недостаточно прав на выполнение метода **Registration.AcceptRequest**.

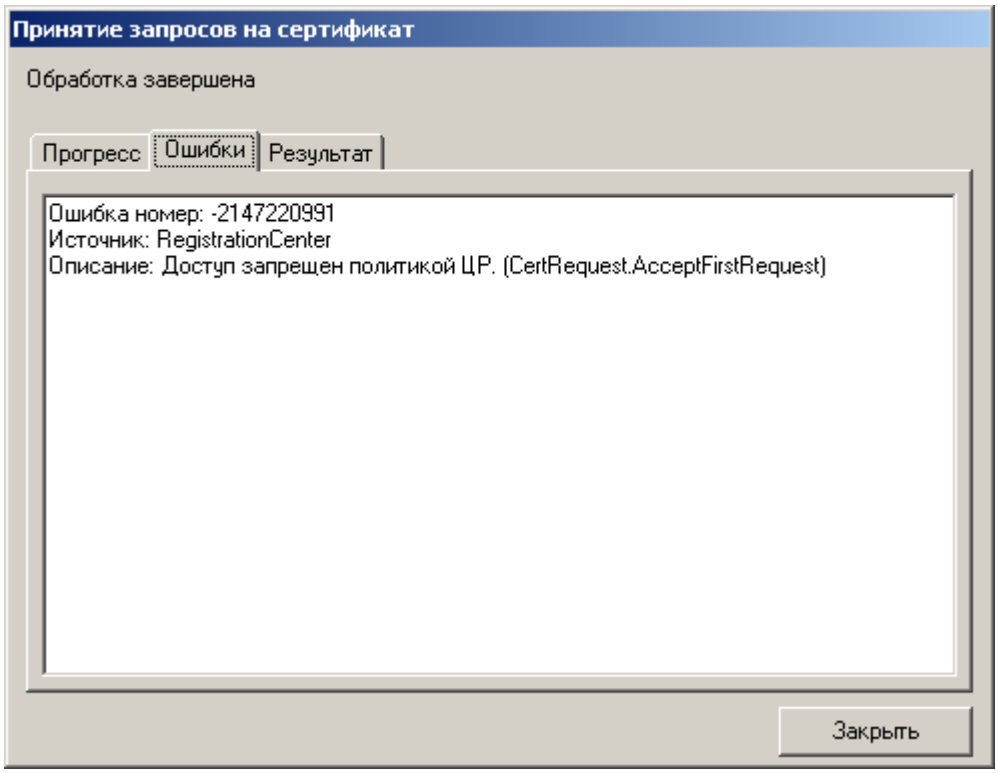
На Центре Регистрации необходимо осуществить настройку политики безопасности, позволяющую осуществлять выполнение указанного метода.

2. При принятии запроса на сертификат (**АРМ Администратора ЦР –> Запросы на сертификат -> Запрос -> Все задачи -> Принять**) в открывшемся окне,

информирующем об окончании проделанных операций, появляется сообщение об ошибке.

Рисунок 64. Ошибка при выполнении метода CertRequest.AcceptFirstRequest



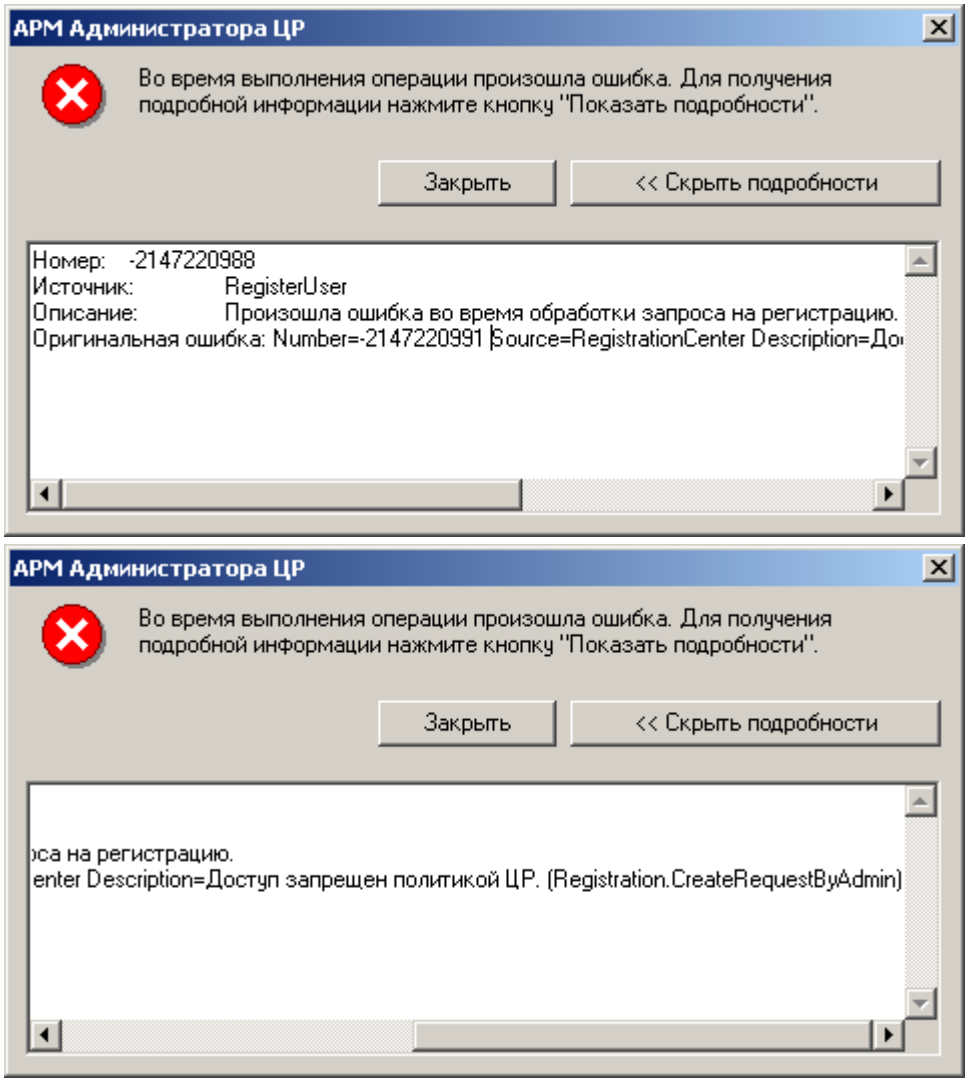


У привилегированного пользователя (**Оператора** или **Администратора**), производящего регистрацию пользователя в Удостоверяющем Центре, недостаточно прав на выполнение метода **CertRequest.AcceptFirstRequest**.

На Центре Регистрации необходимо осуществить настройку политики безопасности, позволяющую осуществлять выполнение указанного метода.

3. После нажатия на кнопку **Далее** в окне **Окончание регистрации пользователя** появляется сообщение:

Рисунок 65. Ошибка при выполнении метода Registration.CreateRequestByAdmin

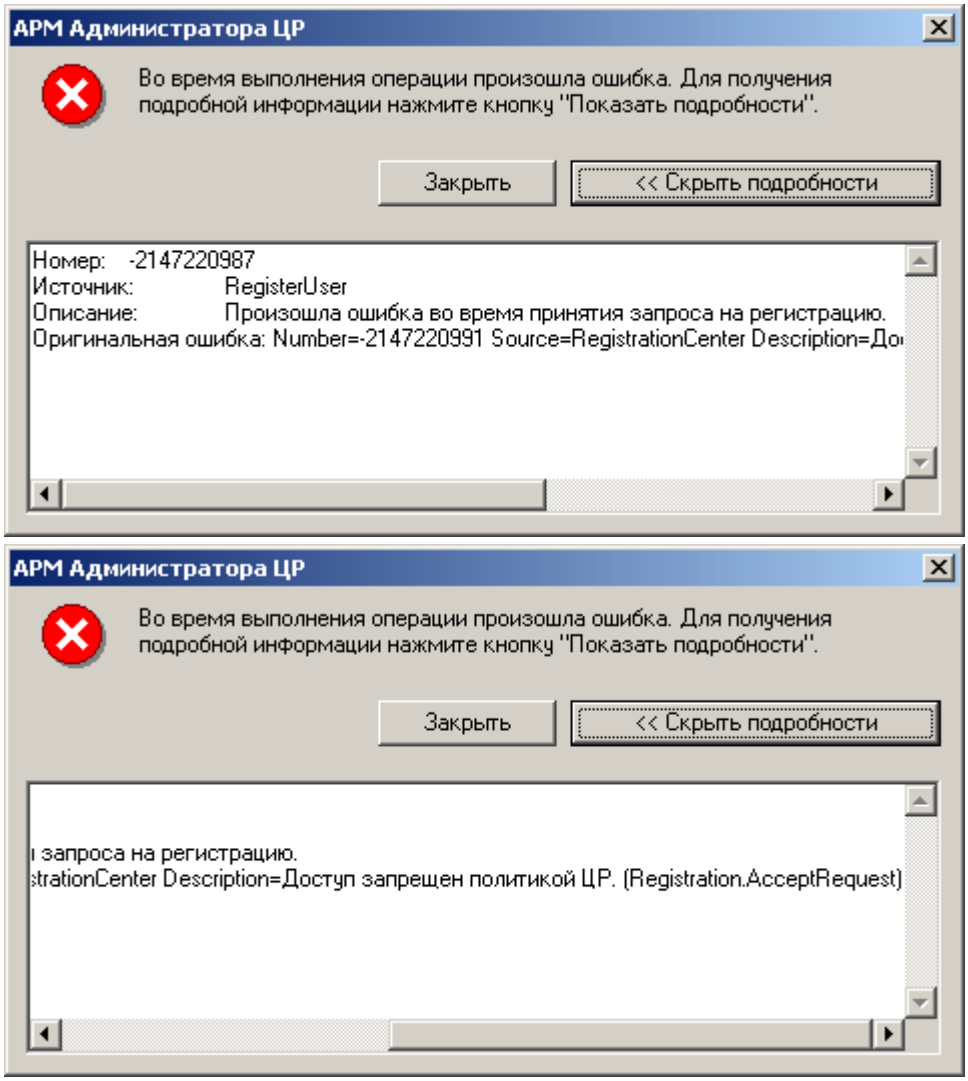


У привилегированного пользователя (**Оператора** или **Администратора**), производящего регистрацию пользователя в Удостоверяющем Центре, недостаточно прав на выполнение метода **Registration.CreateRequestByAdmin**.

На Центре Регистрации необходимо осуществить настройку политики безопасности, позволяющую осуществлять выполнение указанного метода.

4. После нажатия на кнопку **Далее** в окне **Окончание регистрации пользователя** появляется сообщение:

Рисунок 66. Ошибка при выполнении метода Registration.AcceptRequest



У привилегированного пользователя (**Оператора** или **Администратора**), производящего регистрацию пользователя в Удостоверяющем Центре, недостаточно прав на выполнение метода **Registration.AcceptRequest**.

На Центре Регистрации необходимо осуществить настройку политики безопасности, позволяющую осуществлять выполнение указанного метода.

При появлении сообщения об ошибке в системный журнал приложений (**Пуск/Программы/Администрирование/ПросмотрСобытий/Журнал Приложений**) заносится подробная информация о возникшей ситуации, анализ которой позволит точно определить причину ошибки.

1.3. Изготовление сертификата ключа подписи пользователя Удостоверяющего Центра

Изготовление сертификата ключа подписи в Удостоверяющем Центре осуществляется **Администратором** (при использовании настроек по умолчанию) и

может быть осуществлено в двух режимах: централизованном и распределенном. Выбор режима изготовления сертификата определяется владельцем Удостоверяющего Центра и устанавливается Регламентом Удостоверяющего Центра.

Централизованное изготовление сертификата ключа подписи осуществляется при личном прибытии пользователя (либо его уполномоченного представителя, действующего на основании соответствующей доверенности) в Удостоверяющий Центр. Распределенное, напротив, позволяет осуществить изготовление сертификата ключа подписи без прибытия в Удостоверяющий Центр, что удобно, например, при значительной территориальной удаленности Удостоверяющего Центра и конечных пользователей.

1.3.1. Изготовление сертификата ключа подписи в централизованном режиме

Изготовление сертификата ключа подписи в централизованном режиме осуществляется при личном прибытии пользователя (либо его уполномоченного представителя) в Удостоверяющий Центр.

Изготовление сертификата ключа подписи в централизованном режиме может осуществляться как с генерацией ключей в Удостоверяющем Центре, так и на основании запроса на сертификат, предоставляемого пользователем в Удостоверяющий Центр в виде файла (в последнем случае генерацию ключей осуществляет сам пользователь).

Основанием для изготовления сертификата ключа подписи является Заявление на изготовление сертификата.

Заявление на изготовление сертификата, оформляется установленным Регламентом образом, и должно содержать:

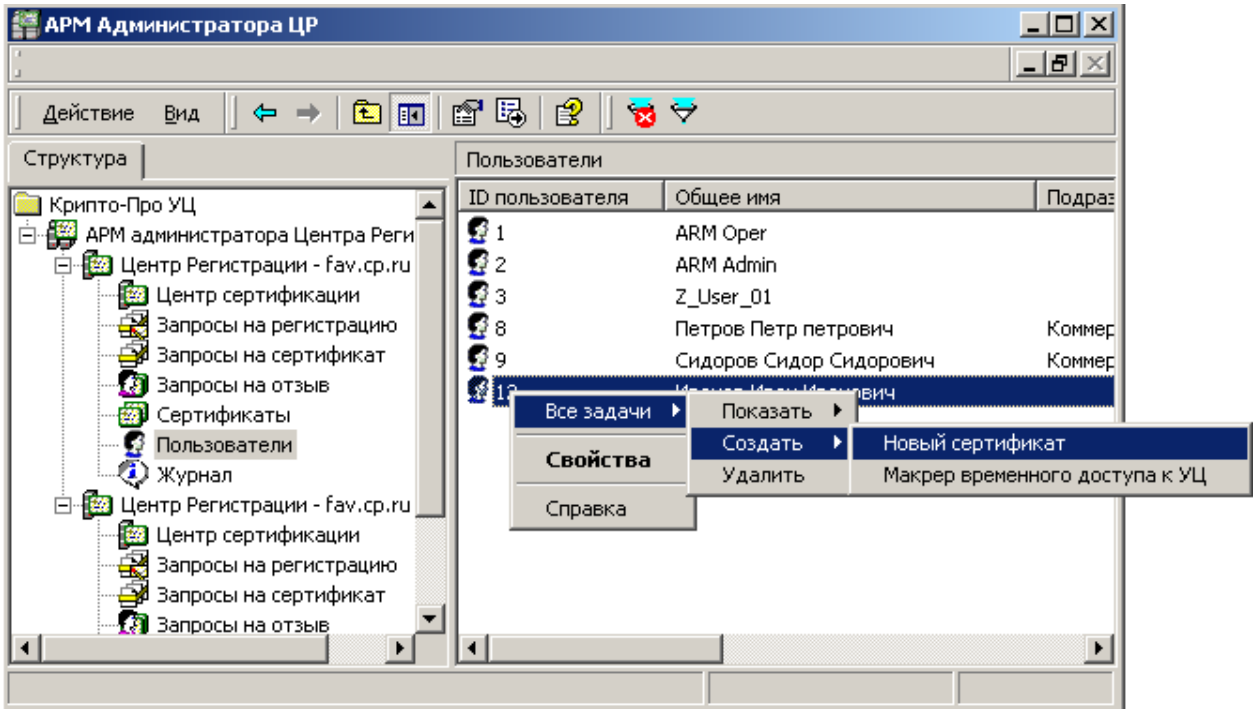
- идентификационные данные лица, на чье имя требуется изготовить сертификат;
- набор областей использования ключа и соответствующие этим областям объектные идентификаторы – OID'ы (содержание поля Extended Key Usage сертификата – наименование областей использования);
- В случае изготовления сертификата на основе предоставленного в виде файла запроса на сертификат – установленным образом оформленный бланк запроса на сертификат ключа подписи.

1.3.1.1. Изготовление сертификата ключа подписи в централизованном режиме с генерацией ключей в Удостоверяющем Центре.

Описание процесса изготовления сертификата ключа подписи в централизованном режиме с генерацией ключей в Удостоверяющем Центре:

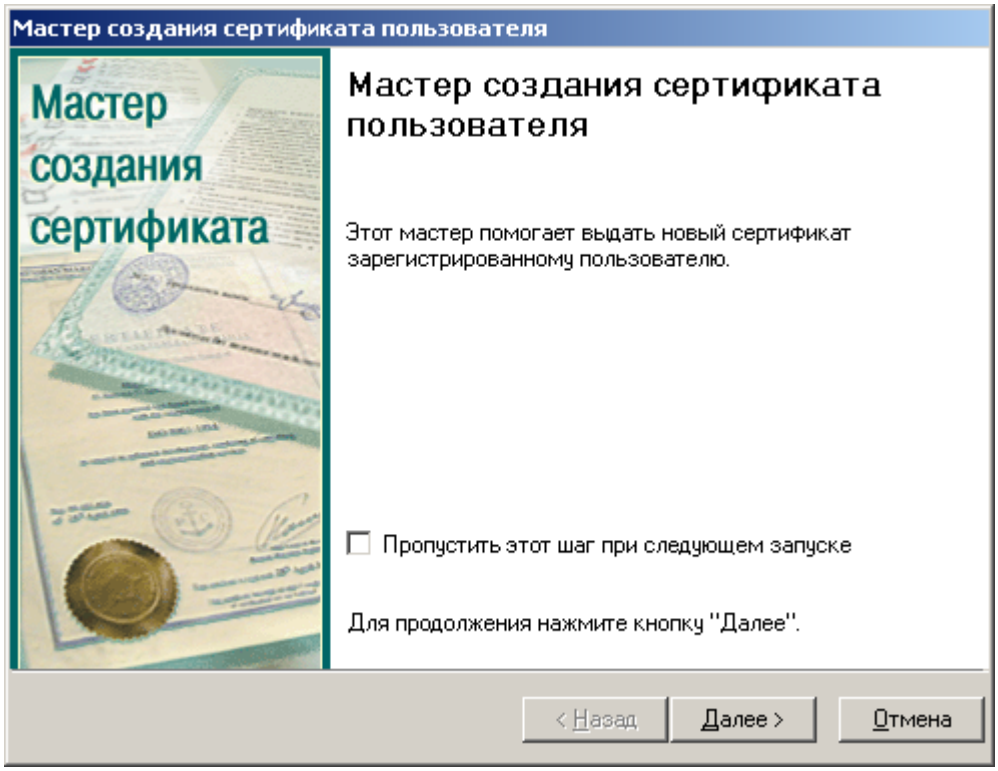
1. В окне **АРМ Администратора ЦР** выделите правой кнопкой мыши учетную запись пользователя, на имя которого требуется изготовить сертификат ключа подписи, в открывшемся контекстном меню выберите **Все задачи -> Создать -> Новый сертификат;**

Рисунок 67. Выбор пункта меню Новый сертификат



2. Запустится **Мастер создания сертификата.** Нажмите кнопку **Далее;**

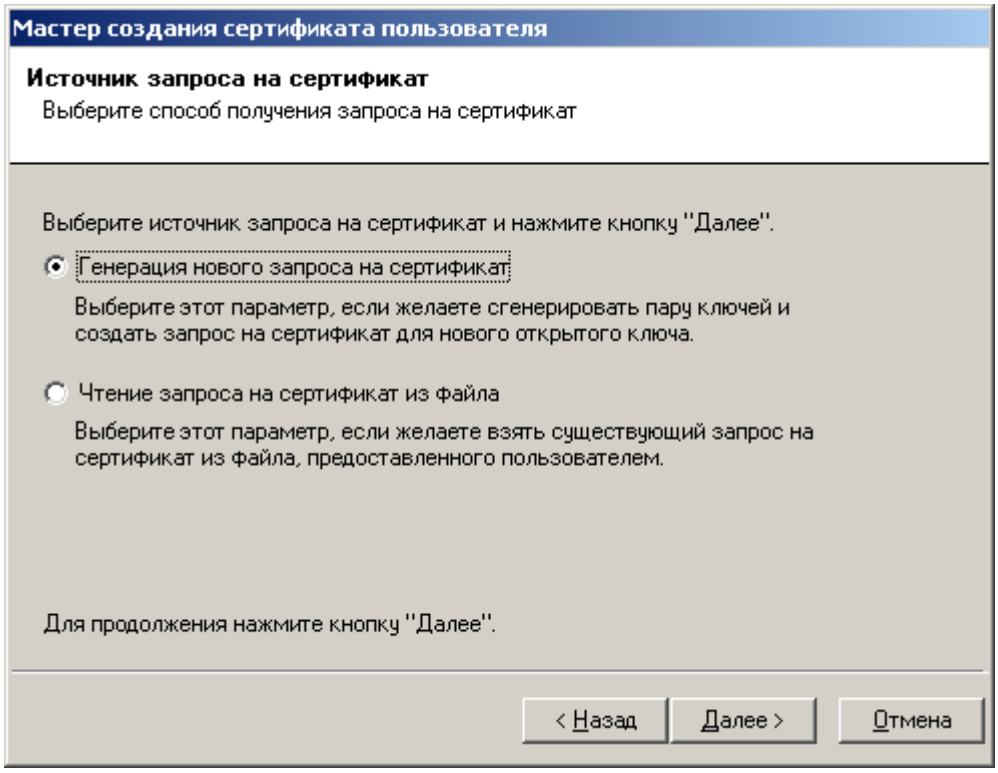
Рисунок 68. Первое окно Мастера создания сертификата



Для отключения вывода первого окна **Мастера создания сертификата пользователя** установите «галку» **Пропустить этот шаг при следующем запуске.**

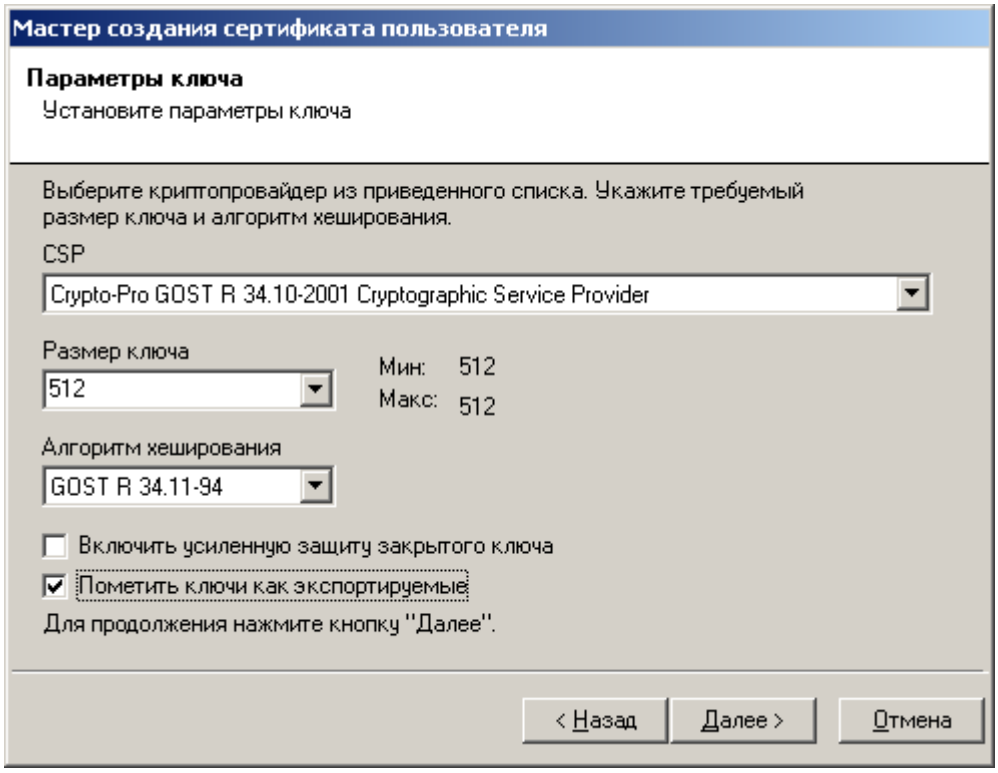
3. В окне **Источник запроса на сертификат** установите переключатель в положение **Генерация нового запроса на сертификат** и нажмите кнопку **Далее;**

Рисунок 69. Выбор генерации нового запроса на сертификат



4. Откроется окно **Параметры ключа**, в котором выберите необходимый криптопровайдер и установите/снимите «галку» **Пометить ключи как экспортируемые**. Нажмите кнопку **Далее;**

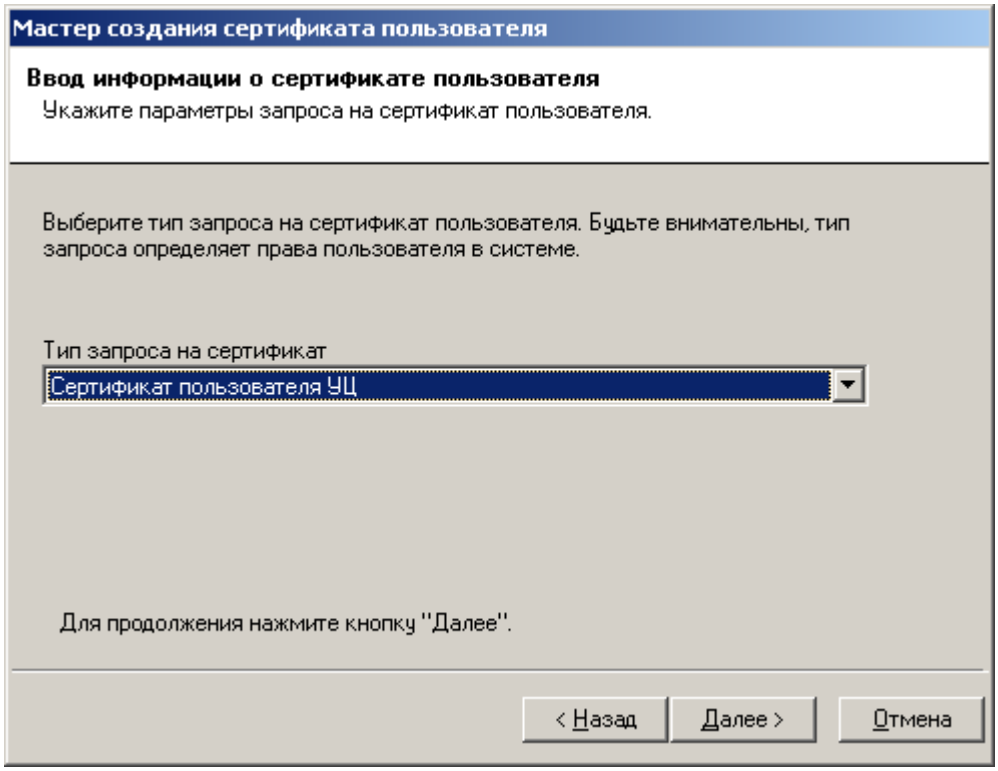
Рисунок 70. Настройка параметров генерации ключей



Установка переключателя **Пометить ключи как экспортируемые** позволит в дальнейшем пользователю скопировать закрытый ключ на иной носитель. Снятие этого флага приводит к невозможности копирования ключевого контейнера штатными средствами СКЗИ и операционной системы. Переключатель **Включить усиленную защиту ключа** применяется к закрытым ключам, сформированным предустановленными в системе криптопровайдерами иностранного производства (например, Microsoft Base Cryptographic Provider).

5. В окне **Ввод информации о сертификате пользователя** выберите необходимый шаблон сертификата. Шаблон сертификата содержит области использования ключа, которые требуется занести в сертификат. Выбор указанного шаблона осуществляется в соответствии с положениями Регламента Удостоверяющего Центра и на основании поданного Заявления на изготовление сертификата ключа подписи. После выбора необходимого шаблона сертификата нажмите кнопку **Далее;**

Рисунок 71. Выбор шаблона сертификата ключа подписи

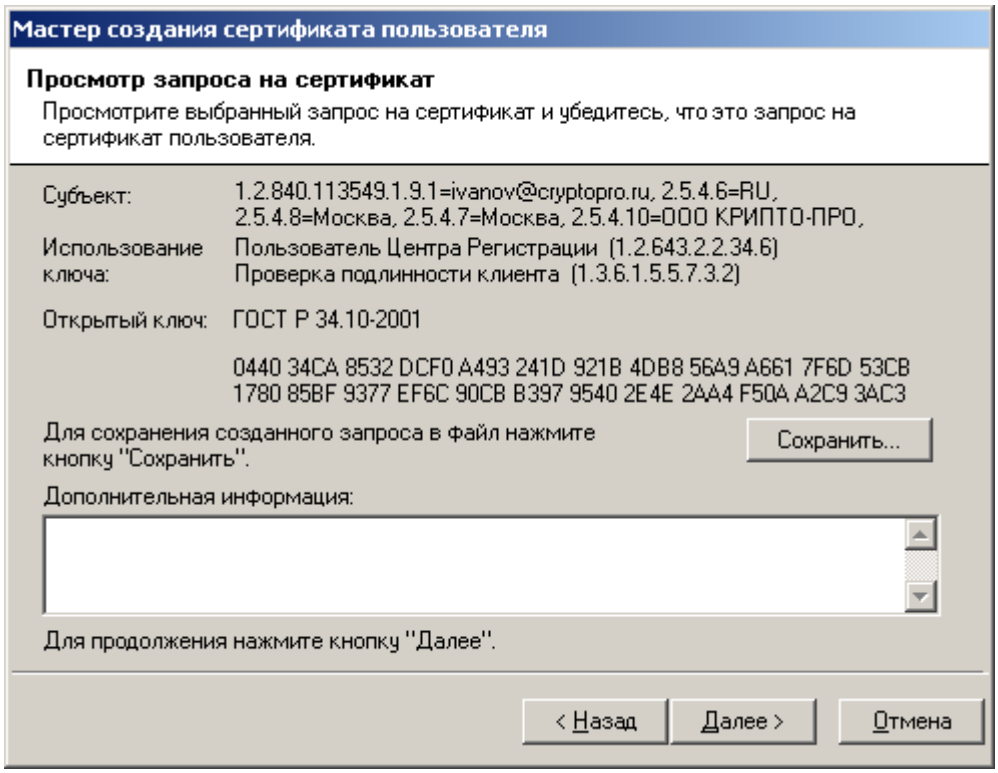


Описанная процедура требует от лица, осуществляющего изготовление сертификата ключа подписи, повышенного внимания, поскольку данные, содержащиеся в шаблоне сертификата определяют отношения, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение, и ошибка, допущенная на данном этапе, может привести к наделению пользователя дополнительными правами и привилегиями (к нелегитимному повышению его статуса).

6. Осуществите генерацию закрытого ключа на используемый ключевой носитель (например, Дискету 3,5" или eToken) и формирование запроса на сертификат ключа подписи. После осуществления указанных действий в окне **Просмотр запроса на сертификат** проверьте правильность указанных идентификационных данных (поле **Субъект**) и областей использования ключа (поле **Использование ключа**). При необходимости введите дополнительную справочную информацию о запросе и нажмите кнопку **Далее;**


Нажатие кнопки **Сохранить** позволяет сохранить сформированный запрос на сертификат в файле формата **PKCS#10.**

Рисунок 72. Окно просмотра запроса на сертификат



7. Откроется окно **Установка сертификата пользователя**, информирующее об успешном изготовлении сертификата ключа подписи и позволяющее:

- осуществить просмотр изготовленного сертификата, нажатием кнопки **Просмотр...;**
- сохранить изготовленный сертификат в виде файла формата **PKCS#7**, нажатием кнопки **Сохранить...;**
- установить изготовленный сертификат в контейнер секретного ключа (осуществляется установкой соответствующего переключателя);
- установить сертификат в хранилище (осуществляется установкой соответствующего переключателя);
- автоматически подтвердить запрос (осуществляется установкой соответствующего переключателя);

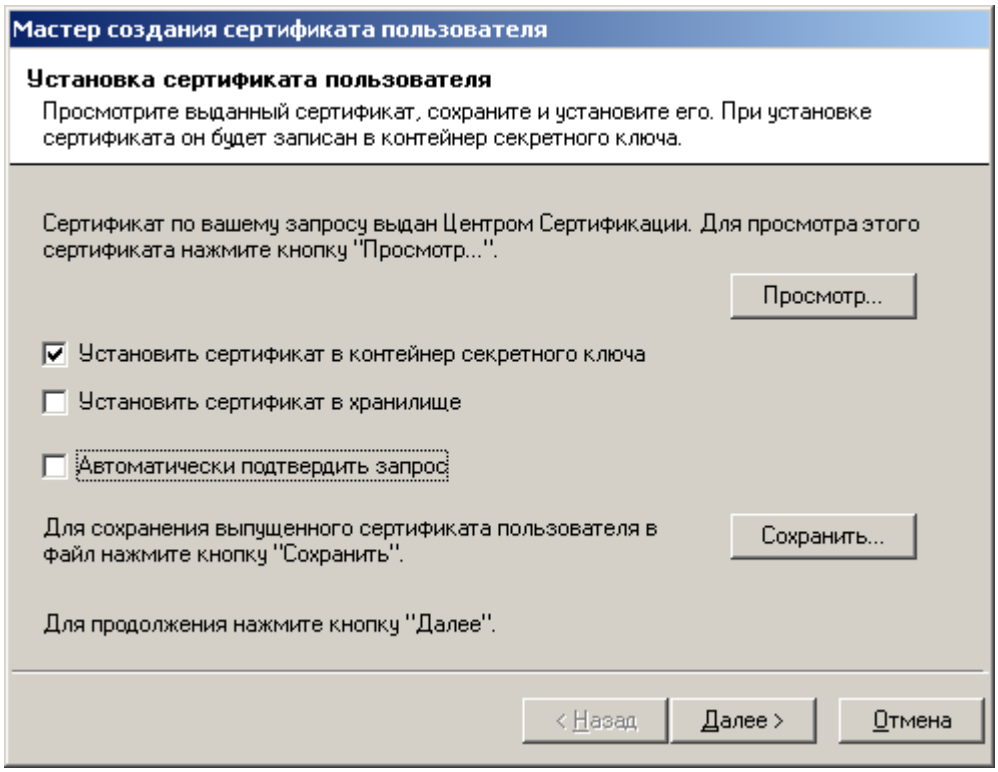
Осуществите установку переключателей, произведите необходимые действия и нажмите кнопку **Далее.**

Конкретная структура ключевого носителя определяется Регламентом Удостоверяющего Центра. Рекомендуется на ключевой носитель, помимо собственно контейнера секретного ключа, записывать файл изготовленного сертификата ключа подписи (кнопка **Сохранить...**) и дополнительно сохранять сертификат ключа подписи в контейнер секретного ключа (установка флага **Установить сертификат в контейнер секретного ключа**).

Выбор переключателя **Установить сертификат в хранилище** приводит к инсталляции изданного сертификата в хранилище **Сертификаты/Текущий пользователь/Другие пользователи** на ПЭВМ **АРМ администратора ЦР**. Использование данного переключателя удобно для организации защищенного почтового обмена между привилегированным пользователем и пользователями Удостоверяющего Центра (например, с использованием почтовых клиентов Microsoft Outlook, Microsoft Outlook Express)

Выбор переключателя **Автоматически подтвердить запрос** устанавливает статус данного запроса в состояние **Завершен** и не требует подтверждения пользователем установки изготовленного сертификата на своей ПЭВМ. Подтверждение пользователем установки осуществляется с использованием **АРМ зарегистрированного пользователя**, являющегося web-приложением Центра Регистрации Удостоверяющего Центра, и требует обязательного сетевого соединения между ПЭВМ пользователя и Центром Регистрации. Рекомендуется использовать указанный переключатель в случае автономного функционирования Удостоверяющего Центра.

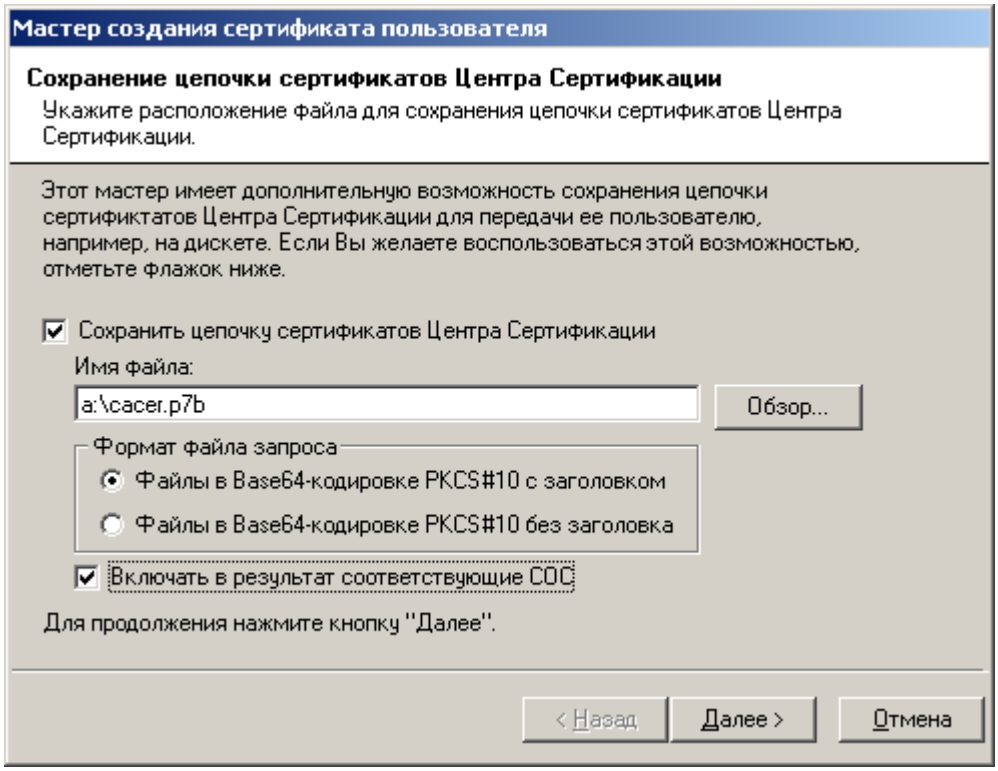
Рисунок 73. Окно просмотра и установки изданного сертификата пользователя



8. Окно **Сохранение цепочки сертификатов центра сертификации** позволяет сохранить все сертификаты издателей и списки отозванных сертификатов, обеспечивающие проверку статуса сертификатов, изданных Удостоверяющим Центром. Установите переключатели **Сохранить цепочку сертификатов Центра**

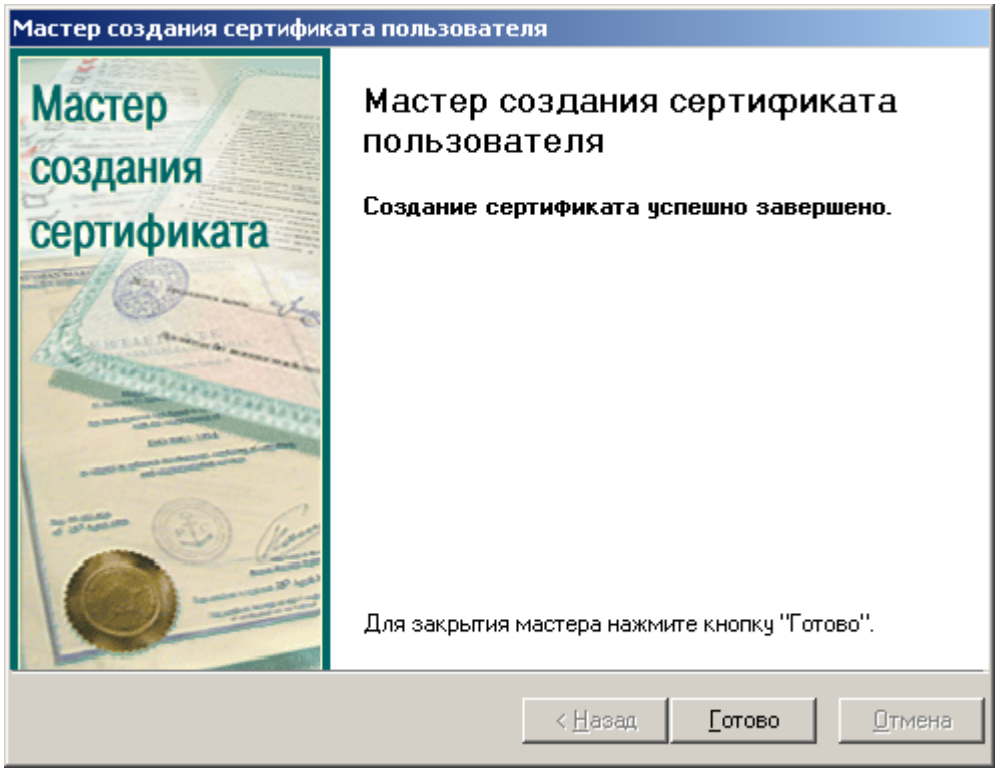
Сертификации и **Включать в результат соответствующие СОС** и введите полный путь для размещения указанных данных. Нажмите кнопку **Далее**;

Рисунок 74. Окно сохранения цепочки сертификатов и списка отозванных сертификатов



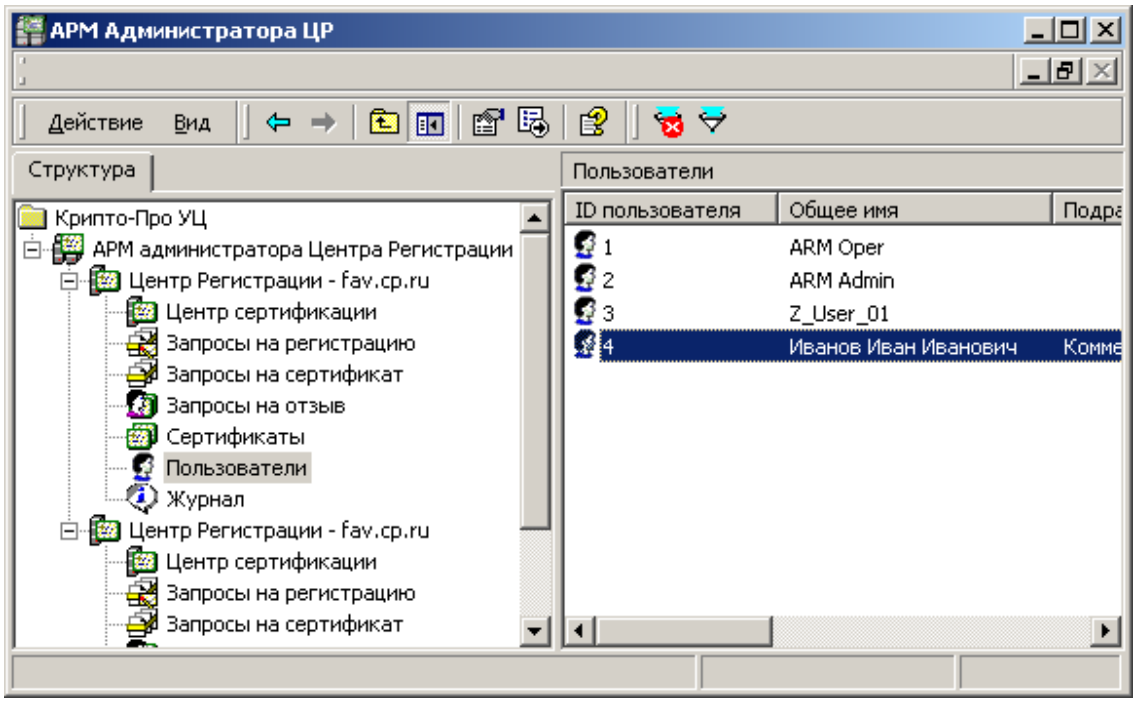
9. После успешного осуществления описанных действий откроется окно, информирующее об успешном изготовлении сертификата. Нажмите кнопку **Готово;**

Рисунок 75. Заключительное окно Мастера изготовления сертификата



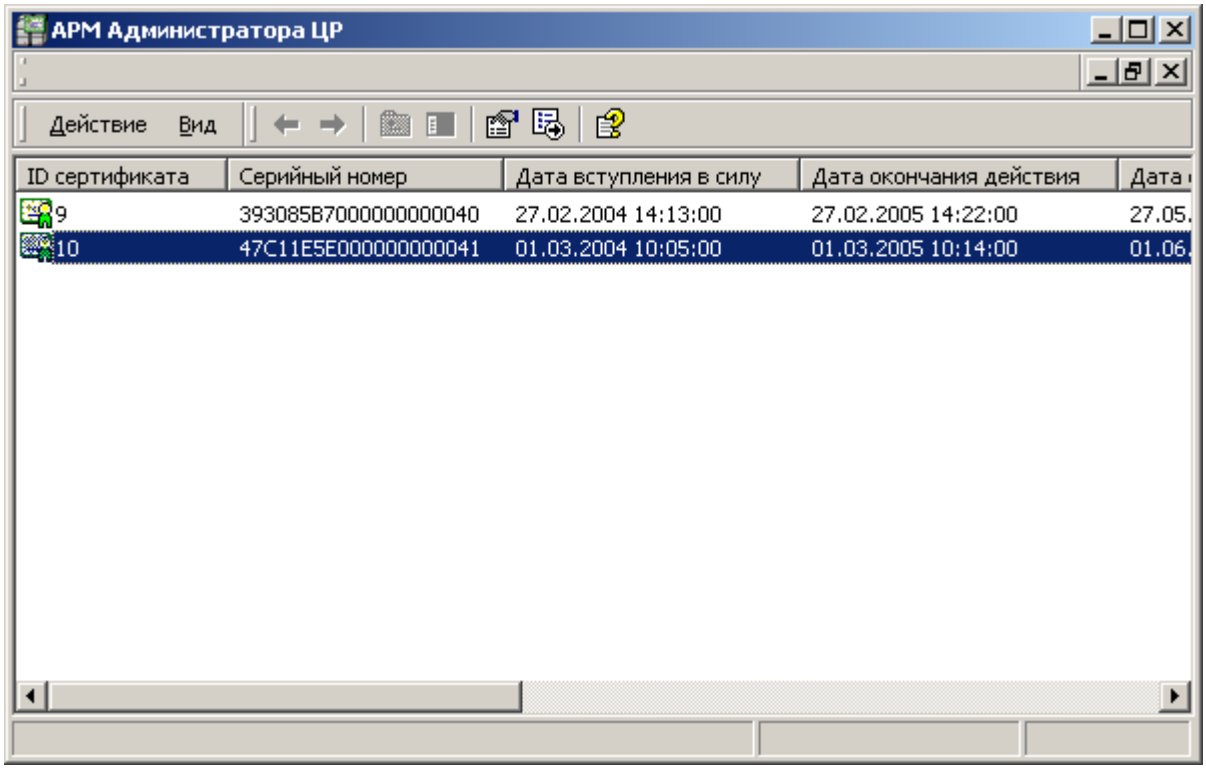
10. В левой части окна **АРМ администратора ЦР** выделите узел **Пользователи** и в правой части окна найдите учетную запись пользователя, на имя которого был изготовлен сертификат;

Рисунок 76. Просмотр учетных записей зарегистрированных пользователей



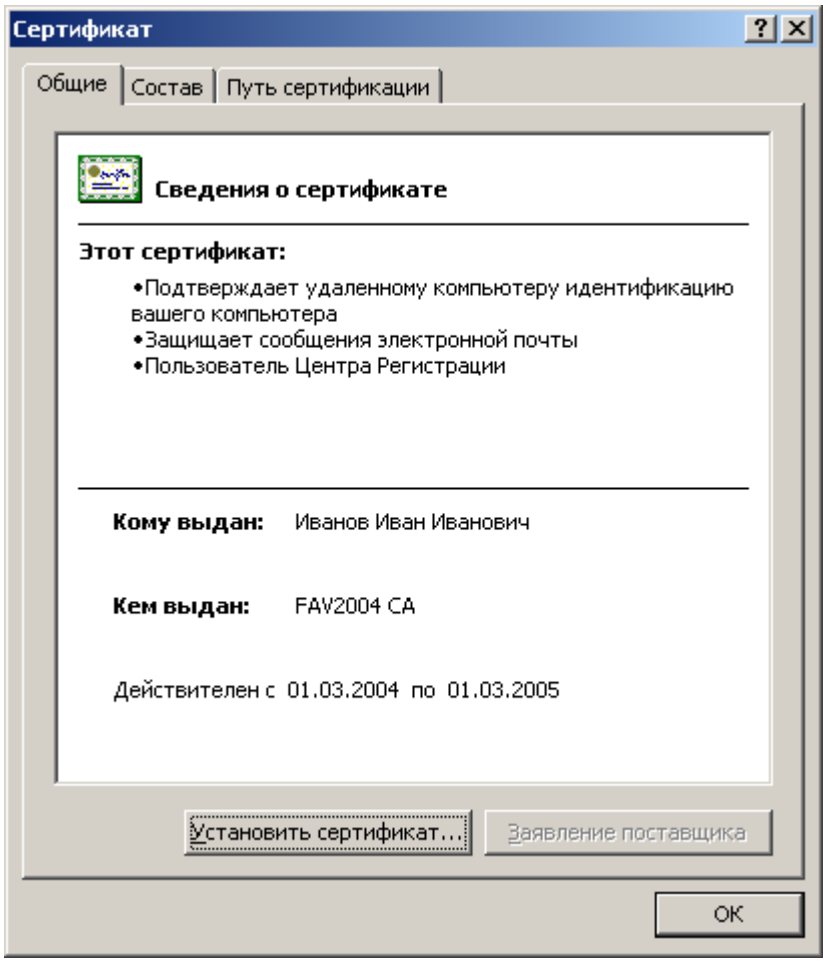
11. Правой кнопкой мыши выделите учетную запись пользователя и в контекстном меню выберите **Все задачи->Показать->Сертификаты;**

Рисунок 77. Окно просмотра изданных сертификатов пользователя



12. Выделите изготовленный сертификат ключа подписи двойным нажатием левой кнопки мыши и просмотрите его в стандартном окне просмотра сертификатов.

Рисунок 78. Стандартное окно просмотра сертификата



1.3.1.2. Изготовление сертификата ключа подписи в централизованном режиме с генерацией ключей самим пользователей

Описание процесса изготовления сертификата ключа подписи в централизованном режиме с генерацией ключей самим пользователем:

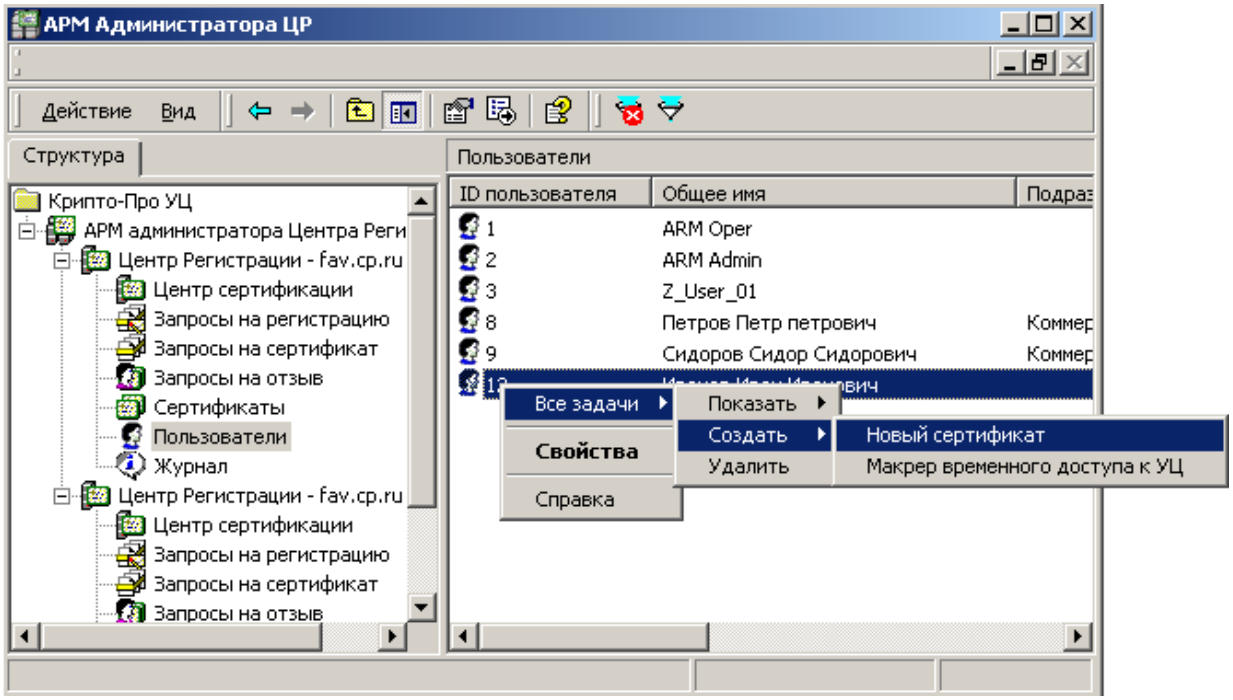
1. Формирование пользователем запроса на сертификат ключа подписи осуществляется с использованием сформированной html-формы для автономной работы, реализующих выполнение следующих функций:

- Генерация закрытого и открытого ключа подписи;
- Формирование запроса на сертификат ключа подписи и его сохранение в файле;
- Формирование запроса на сертификат ключа подписи, подпись ЭЦП запроса на действующем закрытом ключе и сохранение подписанного ЭЦП запроса в файл;
- Установка изготовленного сертификата ключа подписи.

Для изготовления сертификата ключа подписи пользователь предоставляет файл запроса на сертификат ключа подписи формата PKCS#10 и установленным образом оформленное Заявление на изготовление сертификата ключа подписи, либо файл, содержащий подписанный ЭЦП запрос на изготовление сертификата ключа подписи формата PKCS#7.

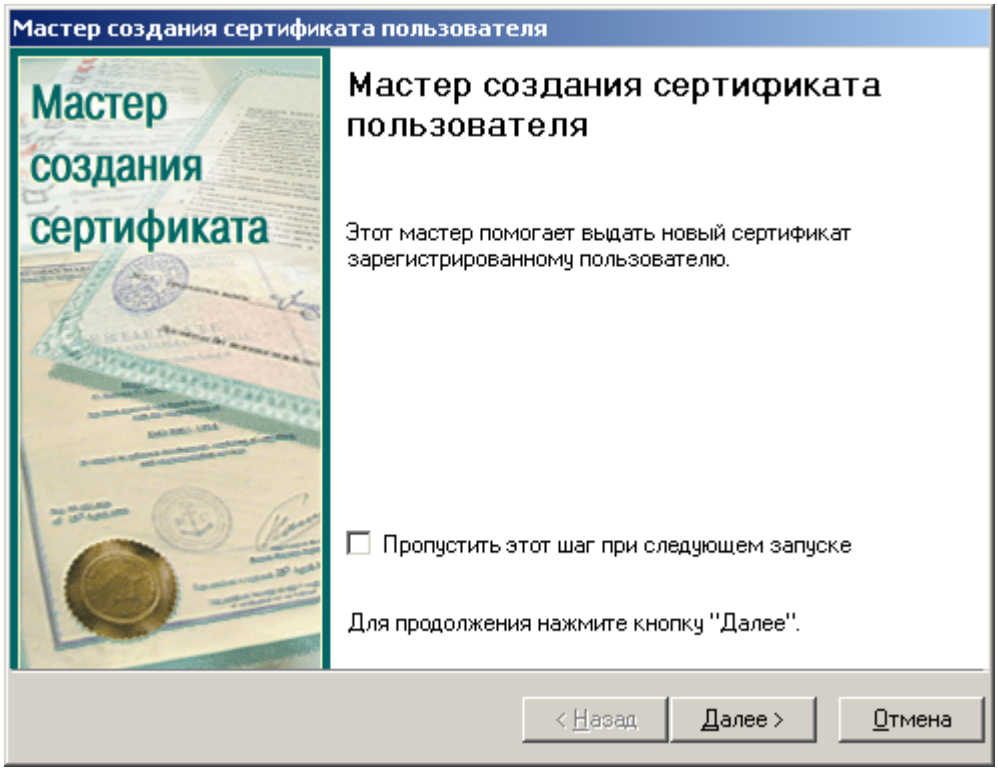
2. В окне **АРМ Администратора ЦР** выделите правой кнопкой мыши учетную запись пользователя, на имя которого требуется изготовить сертификат ключа подписи, в открывшемся контекстном меню выберите **Все задачи -> Создать -> Новый сертификат;**

Рисунок 79. Выбор пункта меню Создание нового сертификата



3. После запуска **Мастера создания сертификата** в открывшемся окне нажмите кнопку **Далее;**

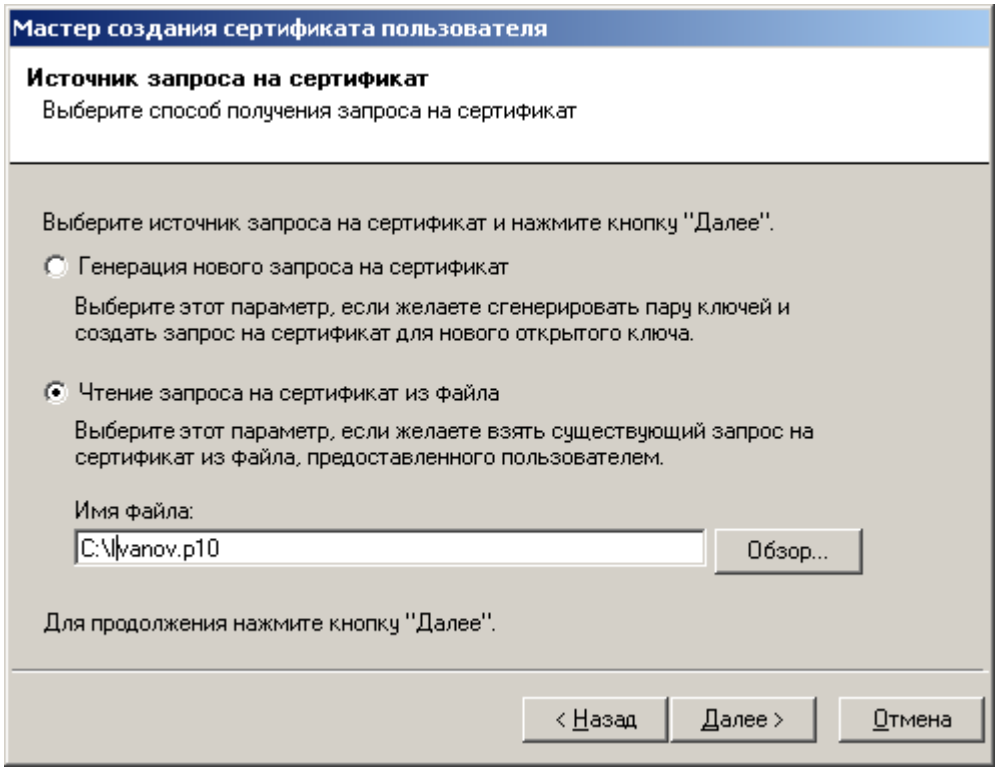
Рисунок 80. Первое окно Мастера создания сертификата пользователя



Для отключения вывода первого окна **Мастера создания сертификата пользователя** установите «галку» **Пропустить этот шаг при следующем запуске.**

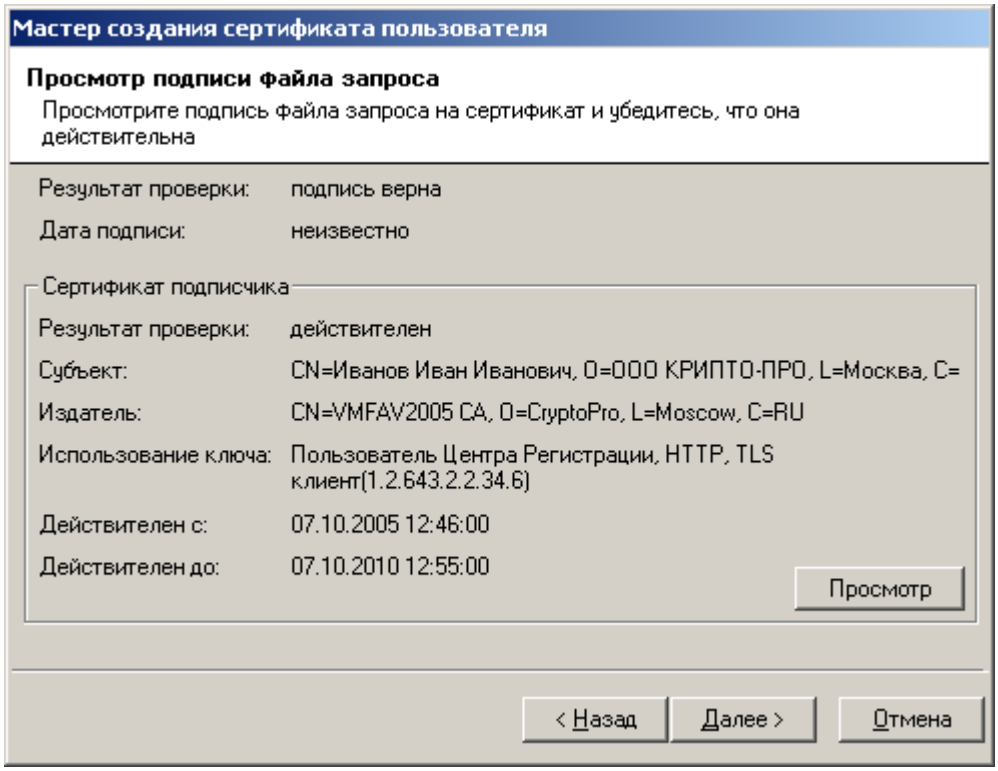
4. В открывшемся окне **Источник запроса на сертификат** выберите переключатель **Чтение запроса на сертификат из файла** и введите имя файла, содержащего запрос на сертификат ключа подписи и нажмите кнопку **Далее;**

Рисунок 81. Выбор способа получения запроса на сертификат из файла



В том случае, если предоставленный запрос на изготовление сертификата подписан ЭЦП пользователя, то откроется окно проверки ЭЦП этого запроса.

Рисунок 82. Окно проверки подписи запроса на сертификат

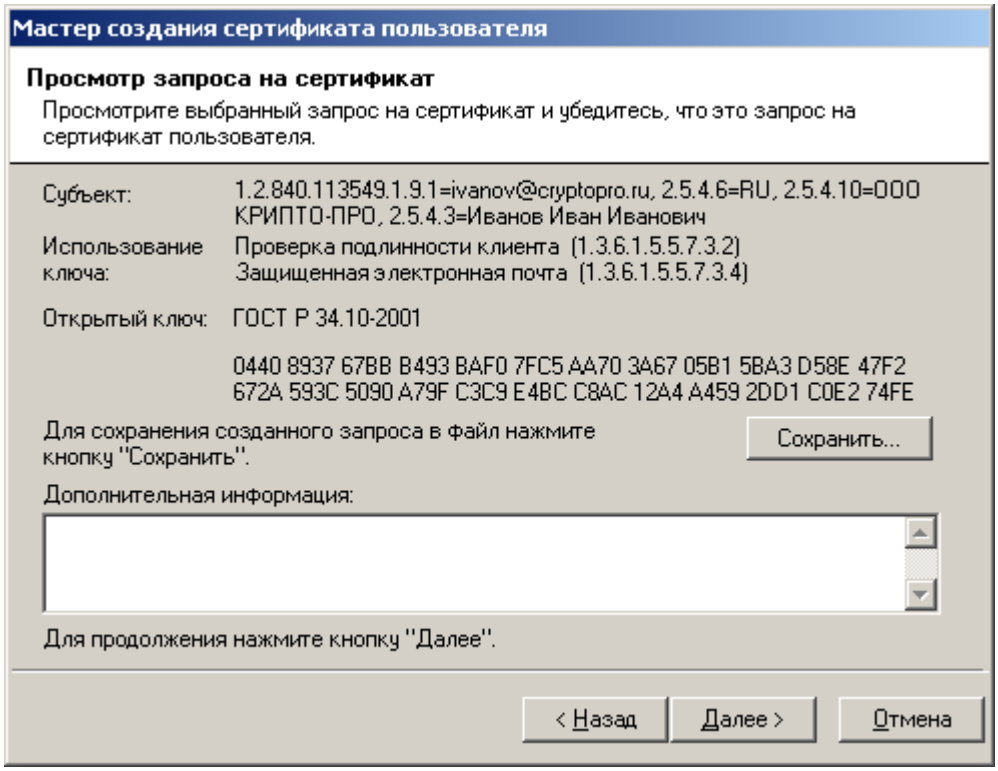


Нажатие на кнопку **Просмотр** позволяет просмотреть сертификат пользователя, подписавшего запрос в стандартном окне просмотра сертификата. Принятие решения по указанному запросу должно производиться в случае одновременного выполнения следующих условий: Результат проверки ЭЦП пользователя – **действителен**, Результат проверки сертификата подписчика – **действителен**.

Подписанный электронной цифровой подписью запрос на изготовление сертификата ключа подписи при соблюдении всех положений регламента Удостоверяющего Центра может рассматриваться как Заявление на изготовление сертификата ключа подписи в электронном виде. Необходимость предоставления Заявления в бумажном виде по этому запросу отпадает.

5. В окне **Просмотр запроса на сертификат** внимательно проверьте идентичность данных, указанных в полях **Субъект**, **Использование ключа**, **Открытый ключ** данным, содержащимся в Заявлении на изготовление сертификата (бланке запроса на сертификат). Только в случае полного совпадения этих данных нажмите кнопку **Далее;**

Рисунок 83. Окно просмотра запроса на сертификат



Описанная процедура требует от лица, осуществляющего изготовление сертификата ключа подписи, повышенного внимания, поскольку данные, содержащиеся в поле **Использование ключа** определяют отношения, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение, и ошибка, допущенная на данном этапе, может привести к наделению пользователя дополнительными правами и привилегиями (к нелегитимному повышению его статуса).

6. Откроется окно **Установка сертификата пользователя**, информирующее об успешном изготовлении сертификата ключа подписи и позволяющее:
   - осуществить просмотр изготовленного сертификата, нажатием кнопки **Просмотр...;**
   - сохранить изготовленный сертификат в виде файла формата **PKCS#7**, нажатием кнопки **Сохранить...;**
   - установить сертификат в хранилище (осуществляется установкой соответствующего переключателя);
   - автоматически подтвердить запрос (осуществляется установкой соответствующего переключателя).

   Осуществите установку переключателей, произведите необходимые действия и нажмите кнопку **Далее.**

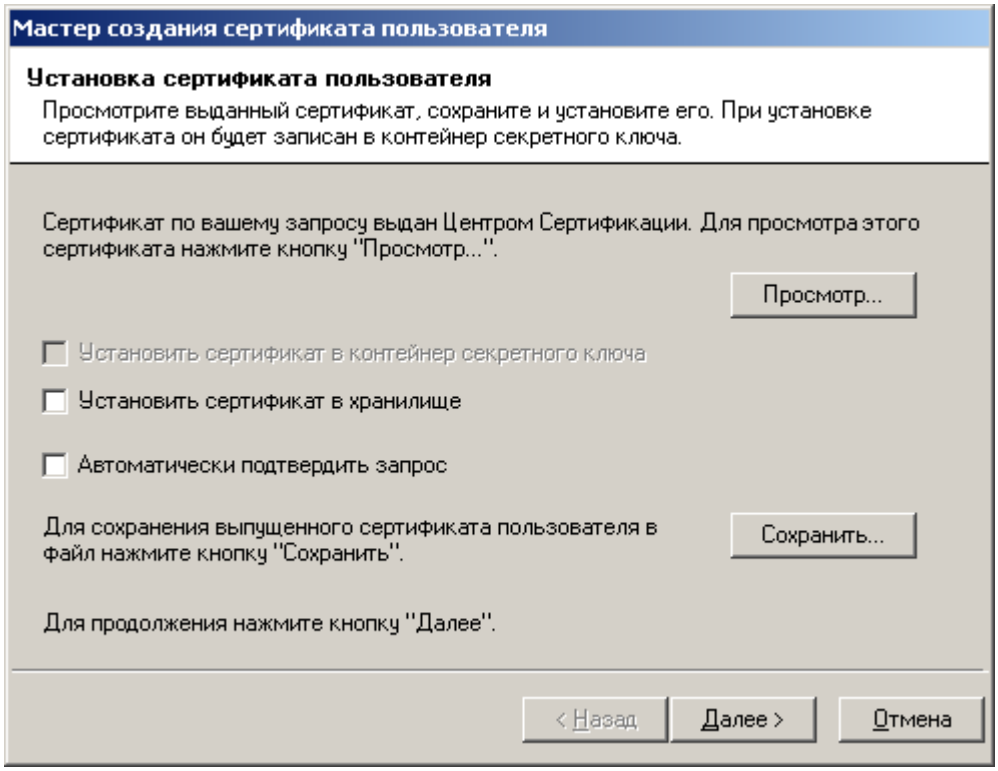
Порядок предоставления пользователю изготовленного сертификата ключа подписи определяется Регламентом Удостоверяющего Центра. В случае предоставления пользователю сертификата на сменном магнитном носителе удобно

воспользоваться кнопкой **Сохранить...** данного окна, и сохранить изданный сертификат на указанный носитель.

Выбор переключателя **Установить сертификат в хранилище** приводит к инсталляции изданного сертификата в хранилище **Сертификаты/Текущий пользователь/Другие пользователи** на ПЭВМ **АРМ Администратора ЦР**. Использование данного переключателя удобно для организации защищенного почтового обмена между привилегированным пользователем и пользователями Удостоверяющего Центра (например, с использованием почтовых клиентов Microsoft Outlook, Microsoft Outlook Express).

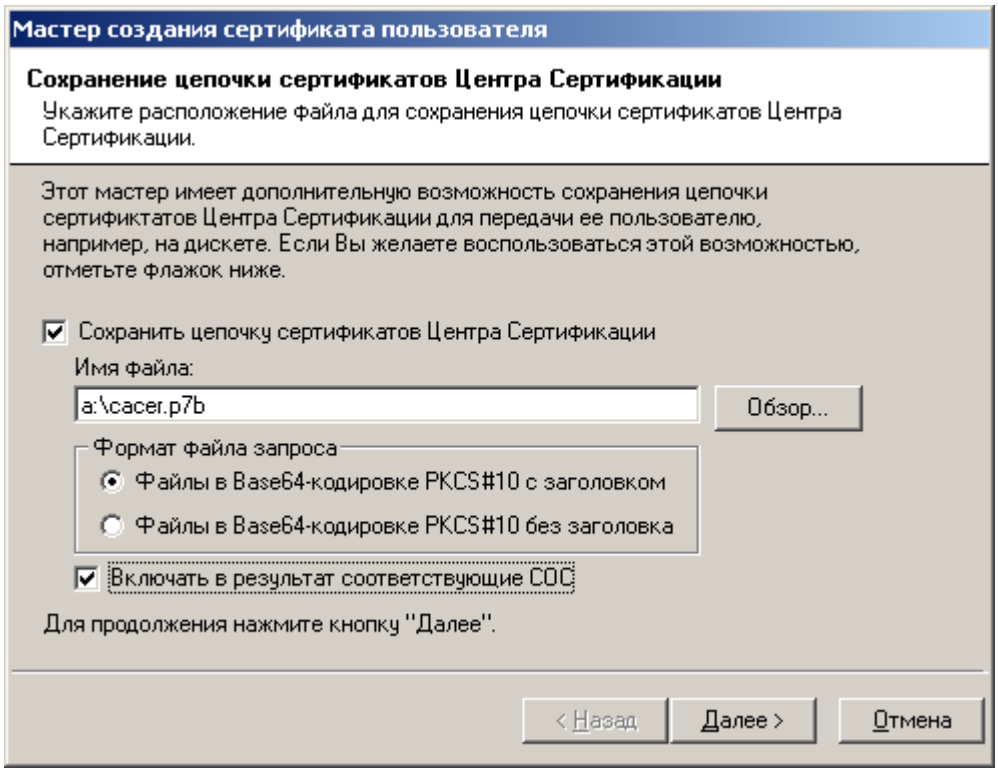
Выбор переключателя **Автоматически подтвердить запрос** устанавливает статус данного запроса в состояние **Завершен** и не требует подтверждения пользователем установки изготовленного сертификата на своей ПЭВМ. Подтверждение пользователем установки осуществляется с использованием АРМ зарегистрированного пользователя, являющегося web-приложением Центра Регистрации Удостоверяющего Центра, и требует обязательного сетевого соединения между ПЭВМ пользователя и Центром Регистрации. Рекомендуется использовать указанный переключатель в случае автономного функционирования Удостоверяющего Центра.

Рисунок 84. Окно просмотра и установки сертификата пользователя



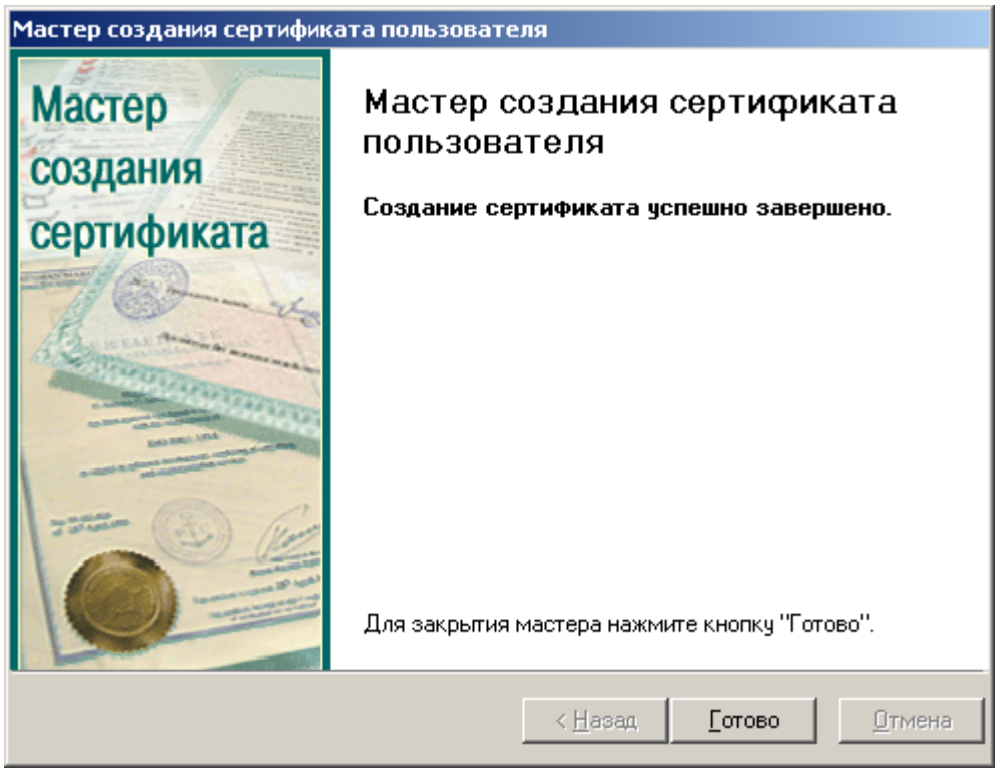
7. Окно **Сохранение цепочки сертификатов центра сертификации** позволяет сохранить все сертификаты издателей и списки отозванных сертификатов, обеспечивающие проверку статуса сертификатов, изданных Удостоверяющим Центром. Установите переключатели **Сохранить цепочку сертификатов Центра Сертификации** и **Включать в результат соответствующие СОС** и введите полный путь для размещения указанных данных. Нажмите кнопку **Далее**;

Рисунок 85. Окно сохранения цепочки сертификатов и списка отозванных сертификатов



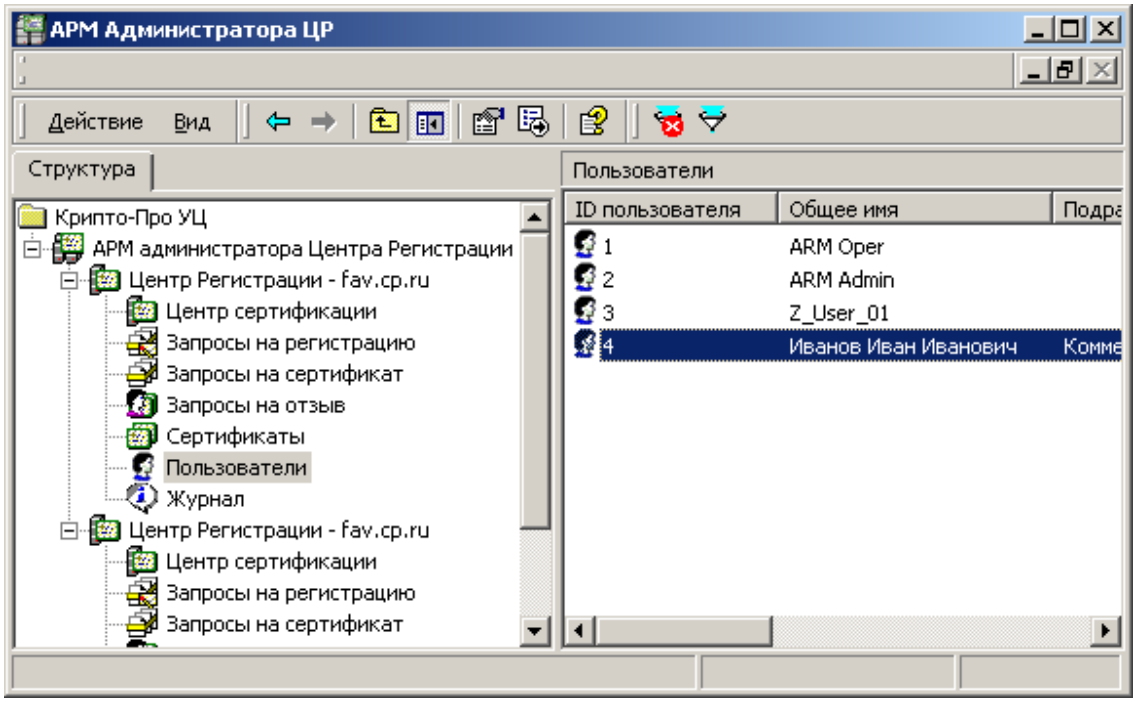
8. После успешного осуществления описанных действий откроется окно, информирующее об успешном изготовлении сертификата. Нажмите кнопку **Готово;**

Рисунок 86. Заключительное окно Мастера создания сертификата пользователя



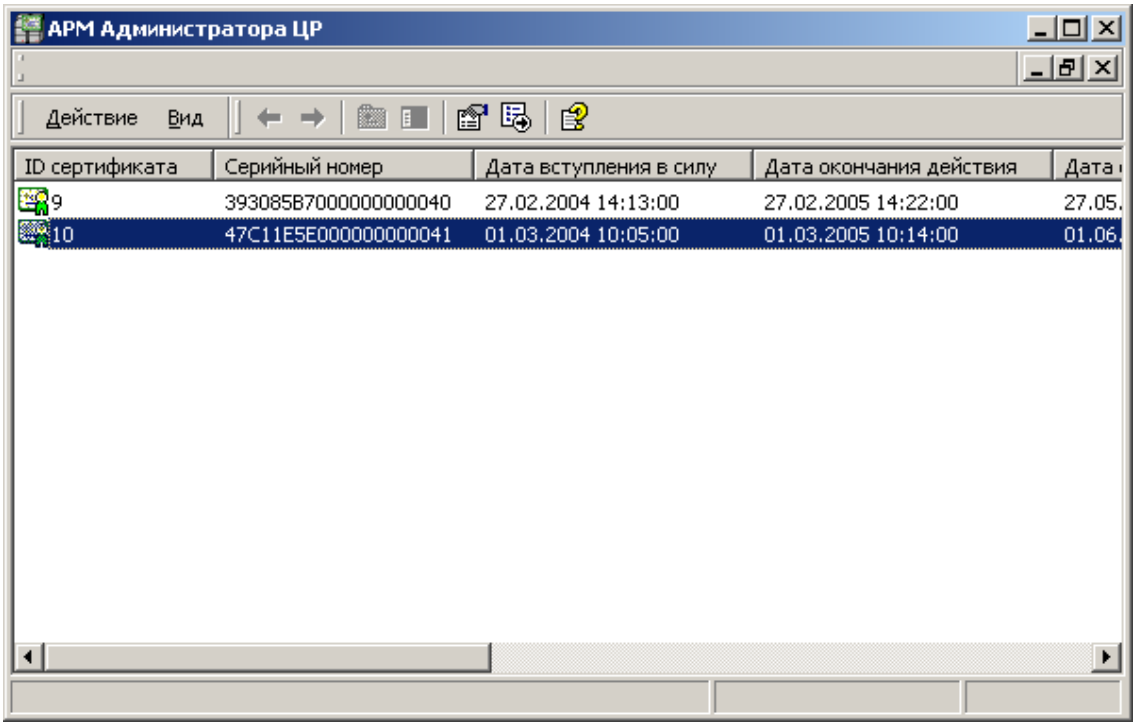
9. В левой части окна **АРМ администратора ЦР** выделите узел **Пользователи** и в правой части окна найдите учетную запись пользователя, на имя которого был изготовлен сертификат;

Рисунок 87. Просмотр учетных записей зарегистрированного пользователя



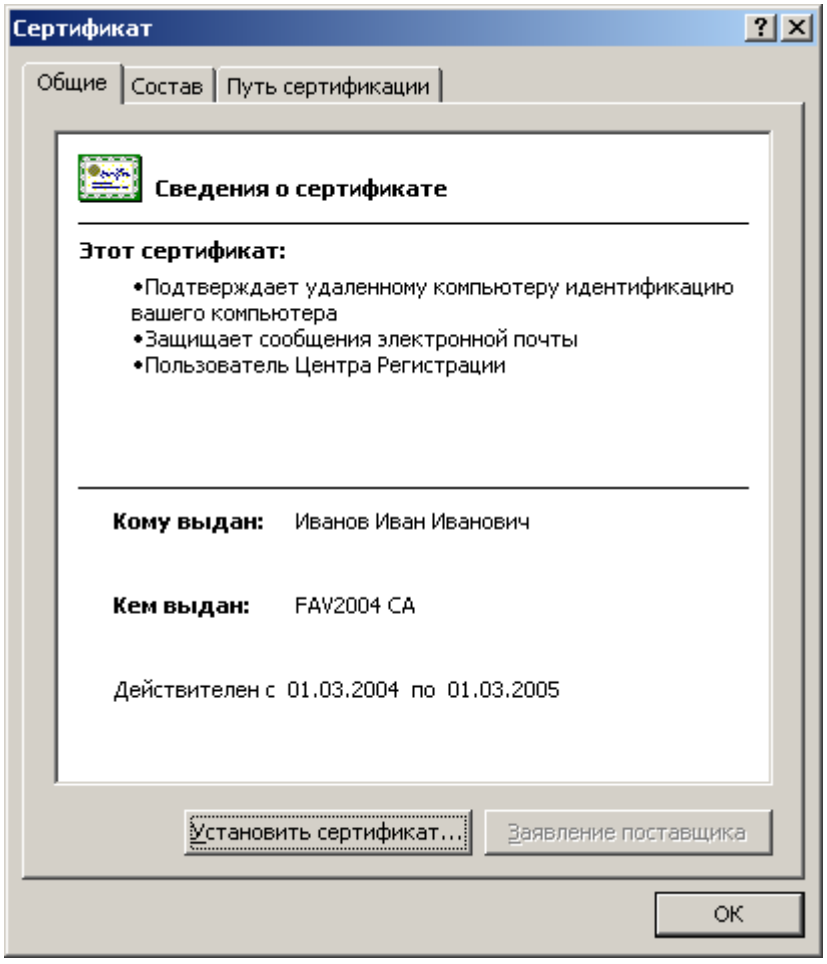
10. Правой кнопкой мыши выделите учетную запись пользователя и в контекстном меню выберите **Все задачи->Показать->Сертификаты;**

Рисунок 88. Окно просмотра сертификатов зарегистрированного пользователя



11. Выделите изготовленный сертификат ключа подписи двойным нажатием левой кнопки мыши и просмотрите его в стандартном окне просмотра сертификатов;

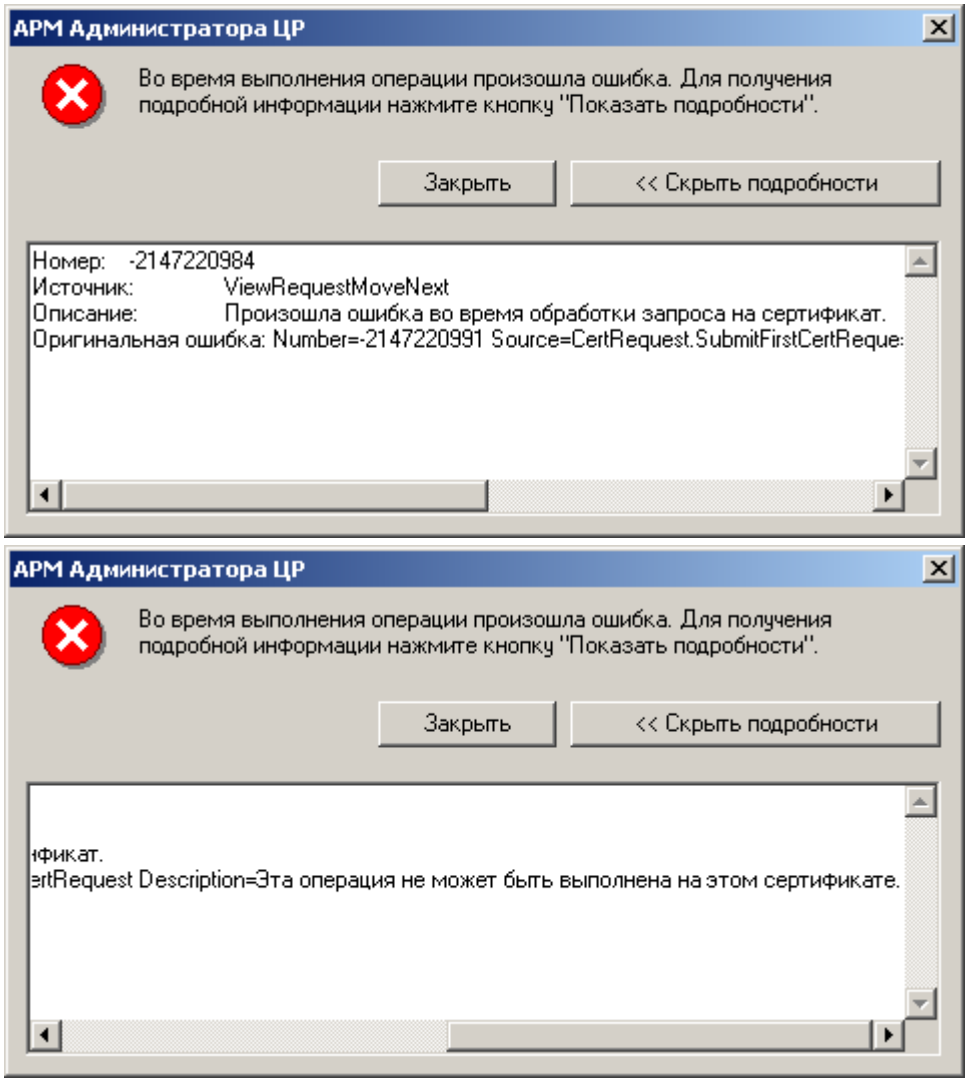
Рисунок 89. Стандартное окно просмотра сертификата



1.3.1.3. Наиболее часто встречающиеся ошибки, возникающие при изготовлении сертификата ключа подписи в централизованном режиме

1. После нажатия на кнопку **Далее** в окне **Просмотр запроса на сертификат** появляется сообщение

Рисунок 90. Ошибка при выполнении метода CertRequest. SubmitFirstCertRequest

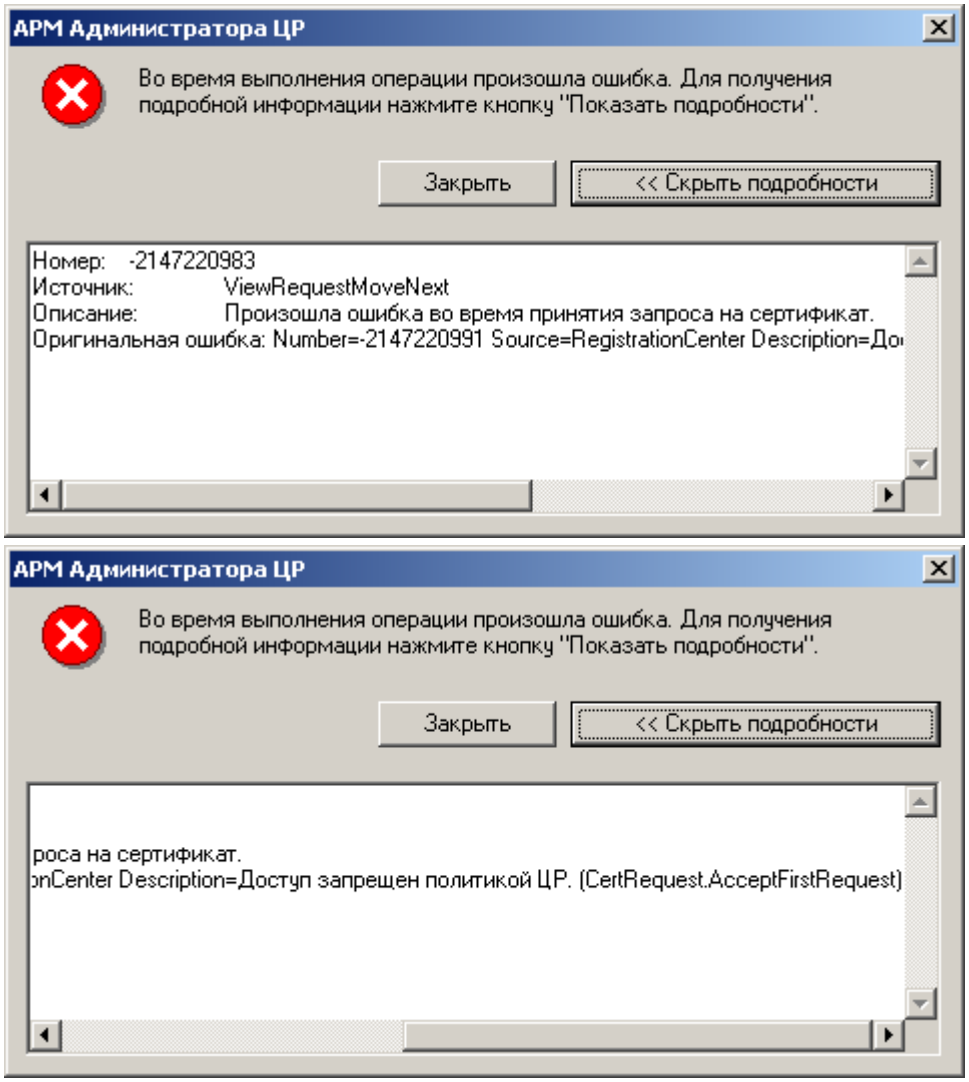


Привилегированный пользователь (**Оператор** или **Администратор**), производящий изготовление сертификата пользователя в Удостоверяющем Центре, не имеет прав на изготовление сертификата, содержащего области использования, указанные в шаблоне на сертификат.

На Центре Регистрации осуществите настройку Политики обработки неподписанных запросов и добавьте необходимые области использования сертификата.

2. После нажатия на кнопку **Далее** в окне **Просмотр запроса на сертификат** появляется сообщение

Рисунок 91. Ошибка при выполнении метода CertRequest.AcceptFirstRequest

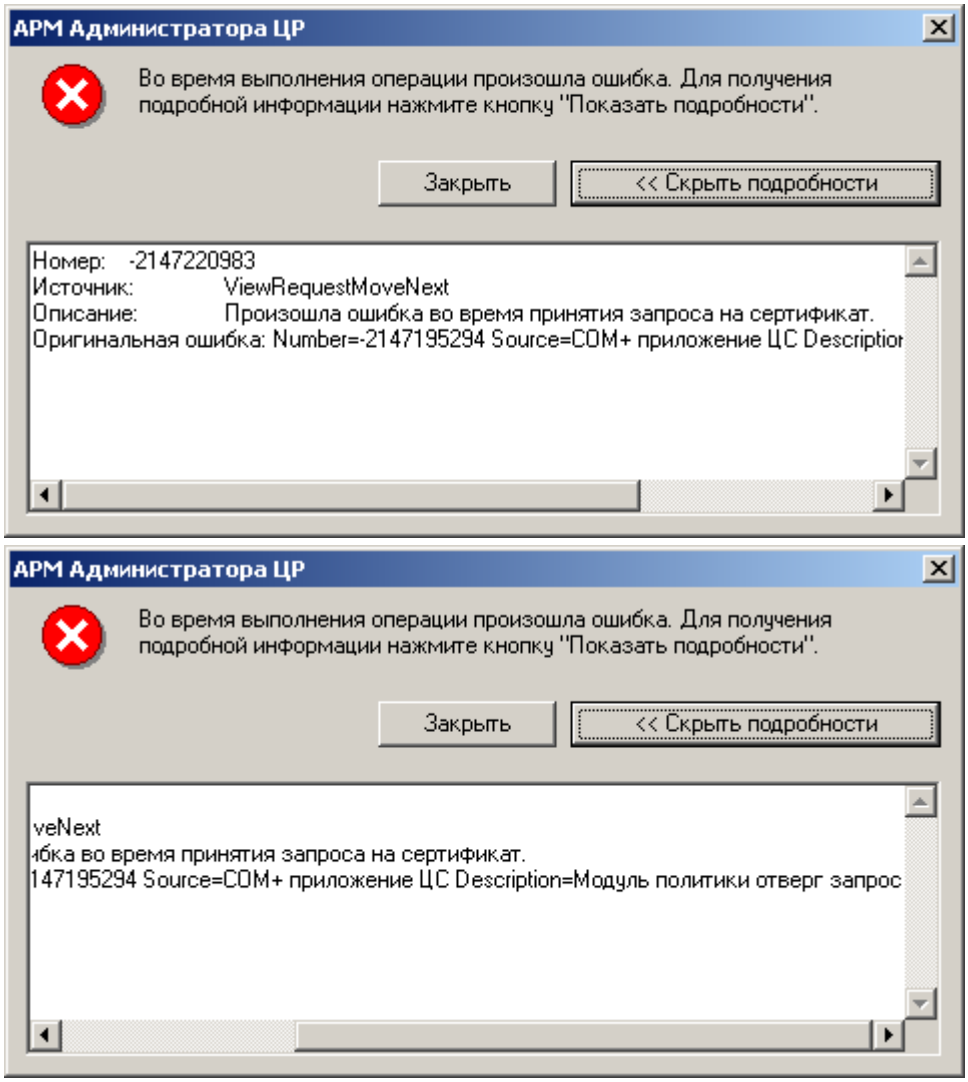


У привилегированного пользователя (**Оператора** или **Администратора**), производящего изготовление сертификата пользователя в Удостоверяющем Центре, недостаточно прав на выполнение метода **CertRequest.AcceptFirstRequest**.

На Центре Регистрации необходимо осуществить настройку политики безопасности, позволяющую осуществлять выполнение указанного метода.

3. После нажатия на кнопку **Далее** в окне **Просмотр запроса на сертификат** появляется сообщение

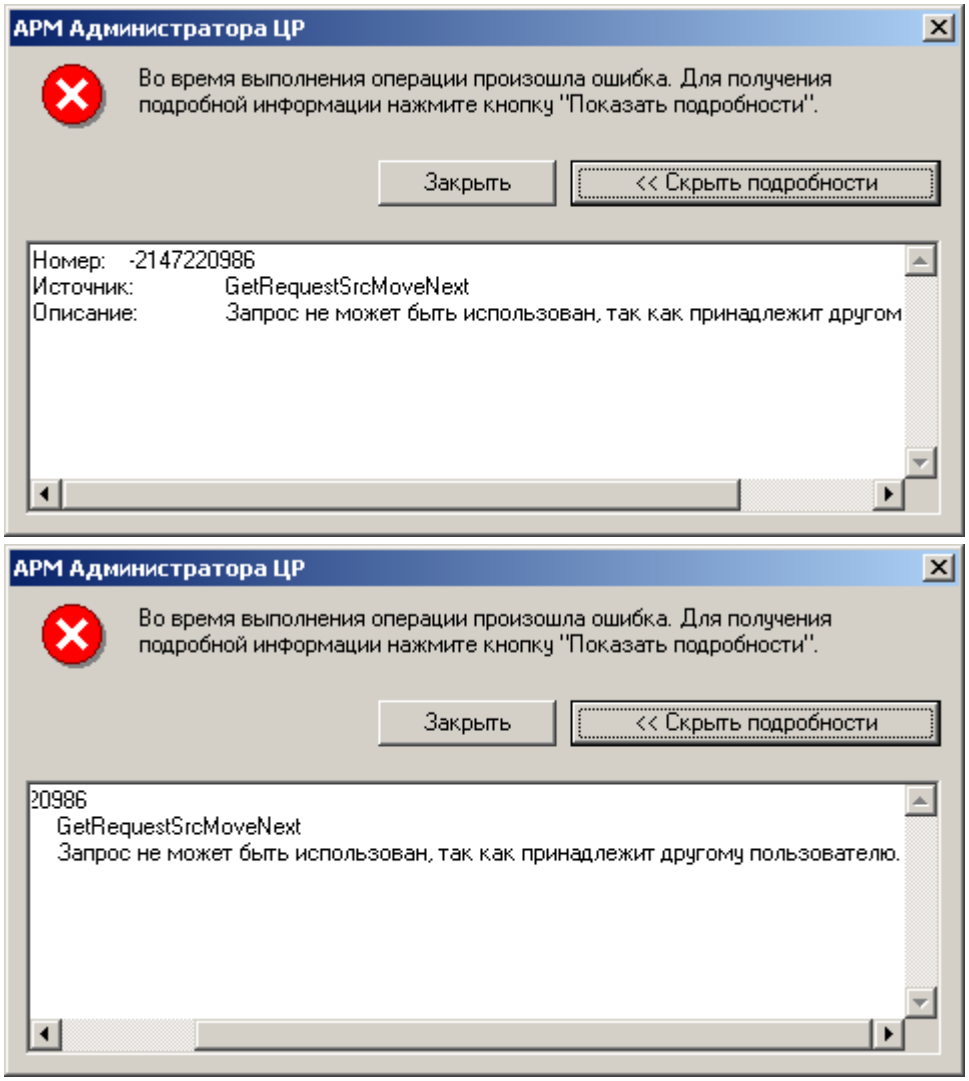
Рисунок 92. Ошибка при обработке запроса на сертификат Центром Сертификации



Модуль политики Центра сертификации отверг запрос – наиболее вероятная причина – на вкладке **Использование ключа** окна **Свойства Модуля политики Центра Сертификации** в списке разрешенных областей использования сертификата отсутствует хотя бы одна область, содержащаяся в запросе на сертификат.

4. После нажатия кнопки **Далее** в окне **Источник запроса на сертификат**, в случае выбора переключателя **Чтение запроса на сертификат из файла** появляется сообщение:

Рисунок 93. Ошибка соответствия идентификационных данных пользователя, содержащихся в запросе на сертифкат учетной записи пользователя



Идентификационные данные пользователя, содержащиеся в запросе на сертификат, отличны от идентификационных данных зарегистрированного пользователя, на имя которого требуется изготовить сертификат (например, выбран файл, содержащий запрос на сертификат другого пользователя), либо при формировании файла запроса была допущена ошибка (например, нарушен установленный порядок следования компонент имени субъекта).

При появлении сообщения об ошибке в системный журнал приложений (**Пуск/Программы/Администрирование/ПросмотрСобытий/Журнал Приложений**) заносится подробная информация о возникшей ситуации, анализ которой позволит точно определить причину ошибки.

1.3.2. Изготовление сертификата ключа подписи в распределенном режиме

Изготовление сертификата ключа подписи в распределенном режиме осуществляется без обязательного прибытия пользователя (или его уполномоченного представителя) в Удостоверяющий Центр, и удобно в случае отдаленного расположения пользователей от Удостоверяющего Центра (например, в разных субъектах Российской федерации).

Изготовление сертификатов пользователей в распределенном режиме может осуществляться посредством **АРМ пользователя с ключевым доступом**, предоставляемого Удостоверяющим Центром и требующего непосредственной связи пользователя с Центром Регистрации (например, с использованием сети общего пользования Internet).

Изготовление сертификата пользователя осуществляется на основе запроса на изготовление сертификата, переданного в электронном виде. Запрос на изготовление сертификата, передающийся при помощи **АРМ пользователя с ключевым доступом,** подписывается электронной цифровой подписью, которая формируется на действующем закрытом ключе пользователя и рассматривается как Заявление на изготовление сертификата.

Если Удостоверяющий Центр эксплуатируется в автономном режиме, или пользователь не соединен линиями связи с Центром Регистрации Удостоверяющего Центра, возможна организация распределенного изготовления сертификата ключа подписи на основе файла запроса на сертификат. В данном случае, при предоставлении указанного файла в Удостоверяющий Центр должна гарантироваться целостность файла запроса на сертификат, и **Администратор** Удостоверяющего Центра должен иметь возможность однозначно установить автора переданного запроса на сертификат.

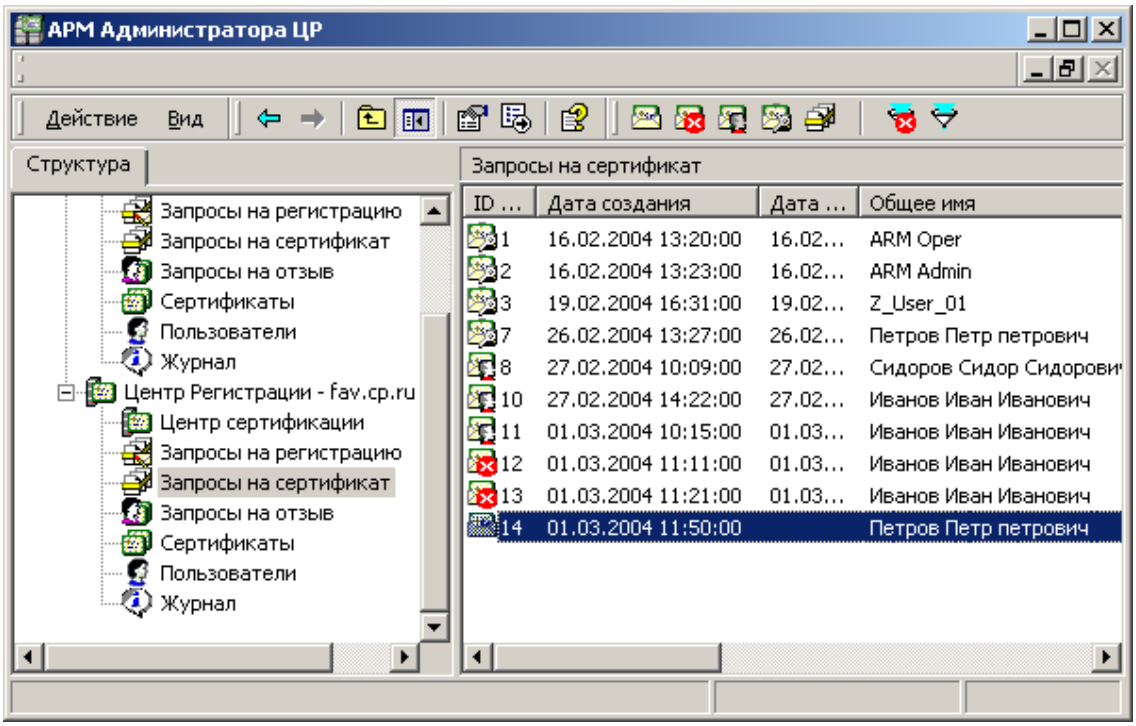
Например, передача подписанного почтового e-mail сообщения (пользователь обязательно должен быть владельцем действующего сертификата ключа подписи, и электронная цифровая подпись сообщения осуществляется на закрытом ключе, соответствующем указанному сертификату), содержащего в качестве вложения файл запроса на сертификат ключа подписи, обеспечит выполнение приведенных в предыдущем пункте требований.

1.3.2.1. Изготовление сертификата ключа подписи в распределенном режиме (с использованием **АРМ пользователя с ключевым доступом**)

Описание процесса изготовления сертификата ключа подписи в распределенном режиме (с использованием **АРМ пользователя с ключевым доступом**):

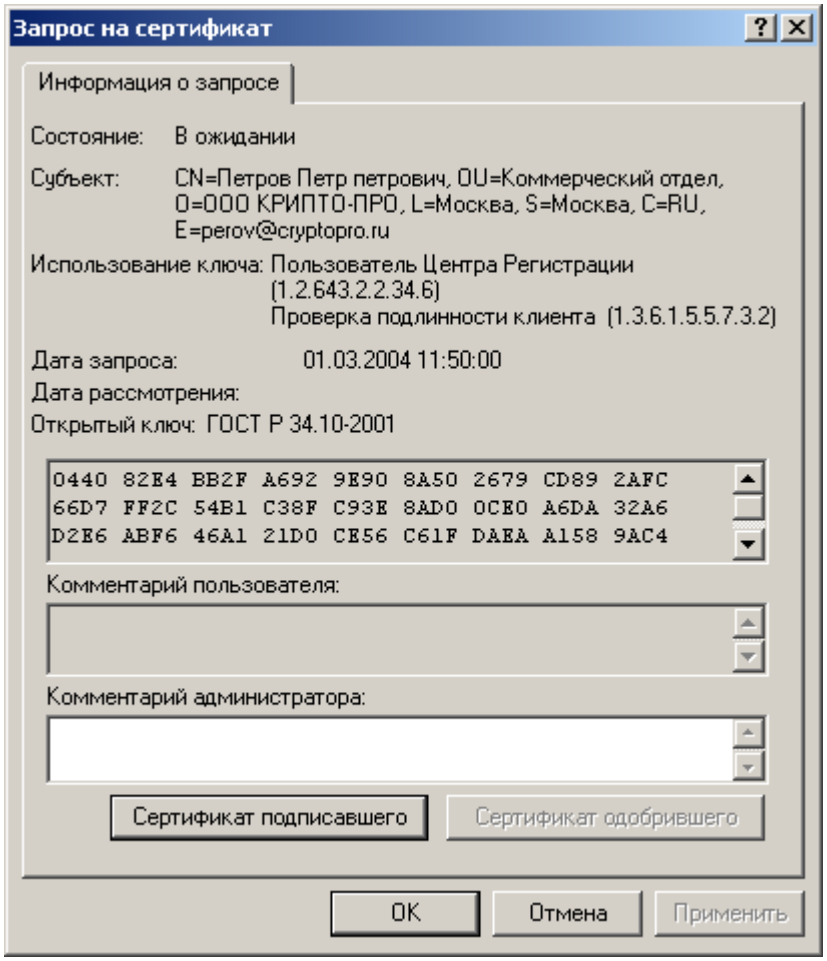
1. Пользователь Удостоверяющего Центра, являющийся владельцем сертификата ключа подписи, с помощью **АРМ пользователя с ключевым доступом** осуществляет на своем рабочем месте генерацию ключей, создание запроса на сертификат ключа подписи, формирование электронно-цифровой подписи запроса на сертификат на действующем закрытом ключе и направляет подписанный запрос в Удостоверяющий Центр.
2. После отправки запроса на изготовление сертификата в окне **АРМ администратора ЦР** в папке **Запросы на сертификат** появляется новый запрос, ожидающий обработки.

Рисунок 94. Окно просмотра запросов на изготовление сертификата ключа подписи



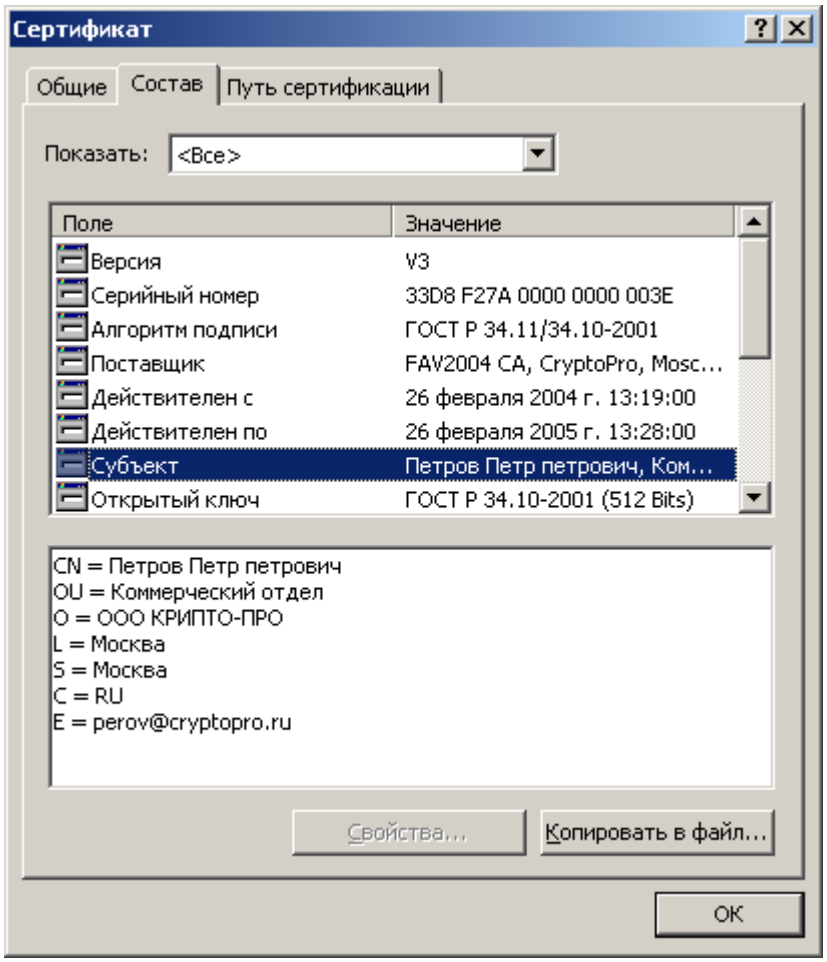
3. Выделите правой кнопкой мыши поступивший запрос на сертификат и в открывшемся контекстном меню выберите пункт **Свойства.** Откроется окно свойств запроса на сертификат.

Рисунок 95. Окно просмотра свойств запроса на сертификат



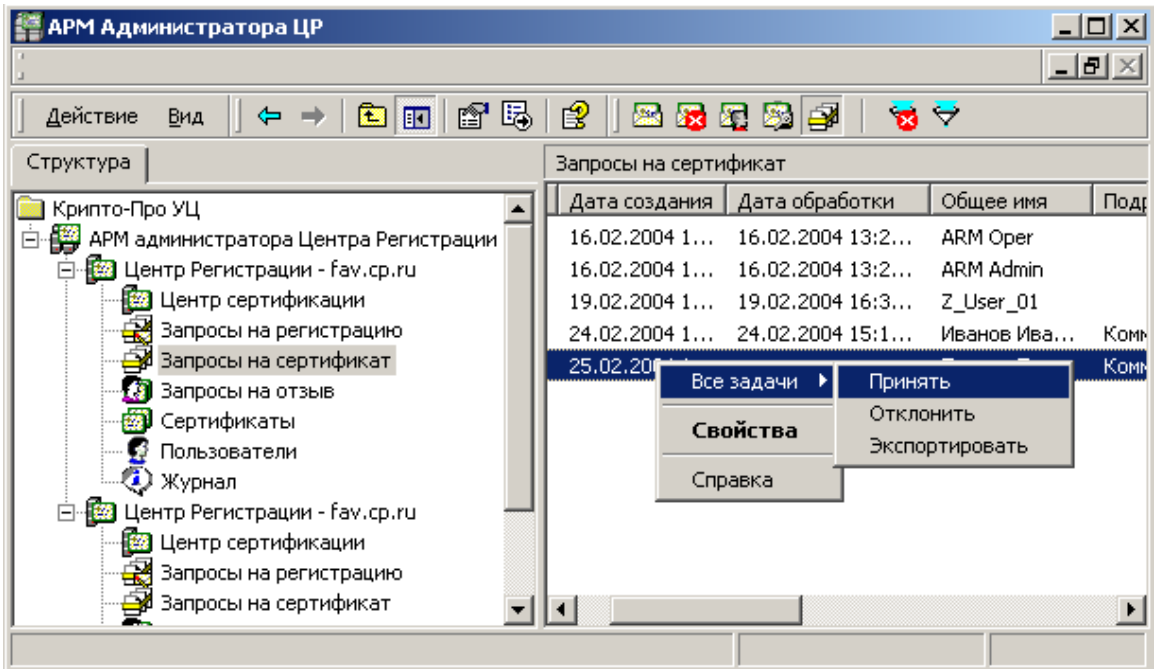
4. В окне **Запрос на сертификат** нажмите кнопку **Сертификат подписавшего**, осуществляющую просмотр сертификата зарегистрированного пользователя, направившего в Удостоверяющий Центр данный запрос.

Рисунок 96. Просмотр сертификата пользователя, подписавшего запрос на изготовление сертификата



5. Внимательно проверьте идентичность данных, содержащихся в поле **Субъект** окна **Запроса на сертификат**, данным, указанным в сертификате, на котором подписан данный запрос. В случае полного соответствия данных в окне свойств нажмите кнопку **ОК**, затем в окне **АРМ Администратора ЦР** выделите правой кнопкой мыши данный запрос на сертификат и в открывшемся контекстном меню выберите **Принять.**

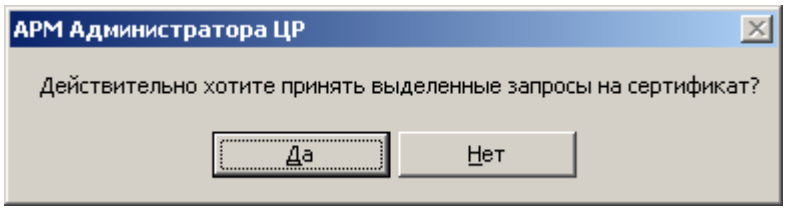
Рисунок 97. Принятие запроса на изготовление сертификата



Рекомендуется привилегированному пользователю, осуществляющему изготовление сертификата, удостовериться в том, что пользователь, на имя которого изготавливается сертификат ключа подписи, может быть владельцем сертификата, содержащего области использования (поле **Использование ключа** окна **Запрос на сертификат**), указанные в запросе на сертификат (хотя указанная проверка автоматически осуществляется на **АРМ пользователя с ключевым доступом**).

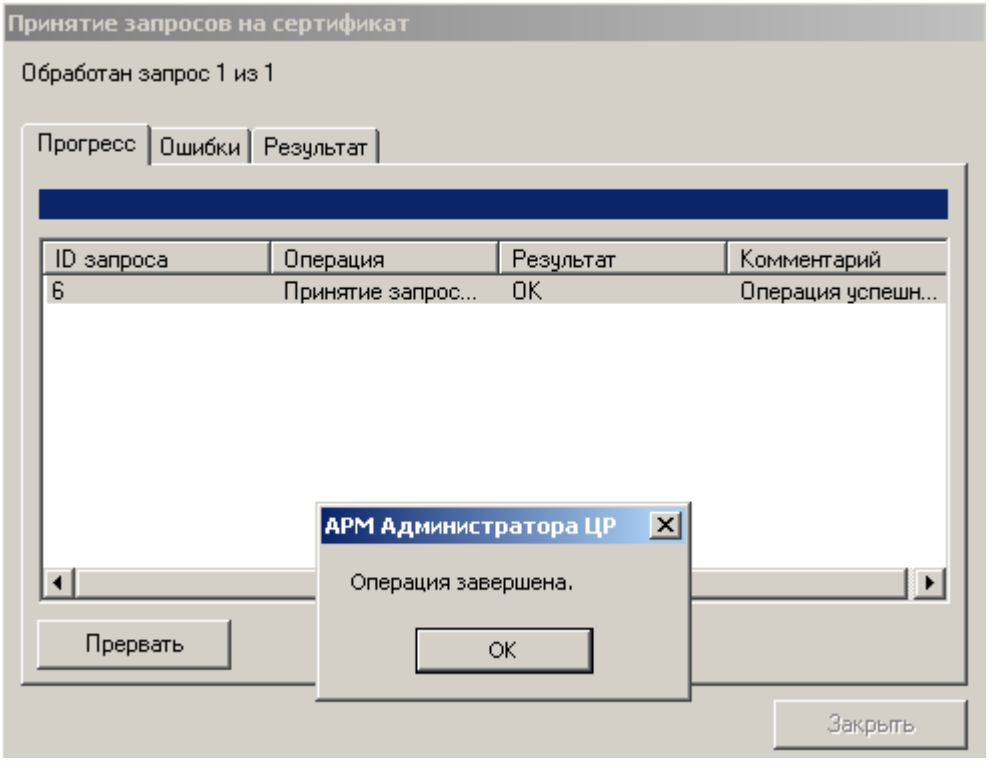
6. При принятии запроса на сертификат откроется предупреждающее окно, требующее подтверждения выбранных действий. Нажмите кнопку **Да**;

Рисунок 98. Окно подтверждения принятия запроса на сертификат



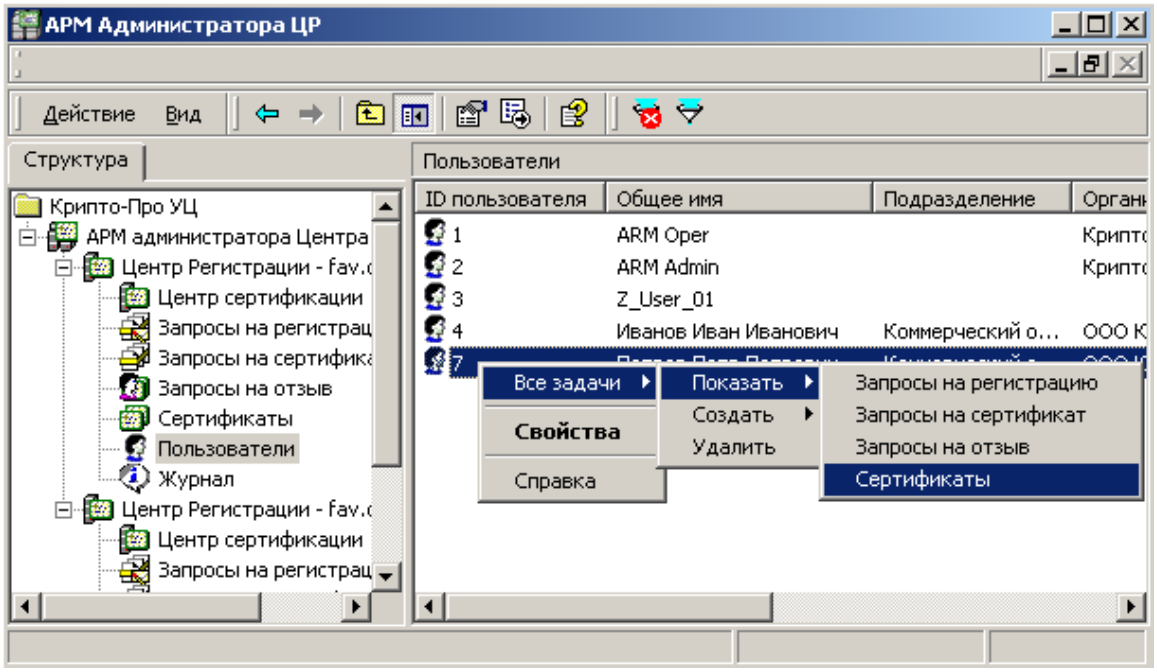
7. По окончании выполнения действий по изготовлению сертификата ключа подписи появится сообщение, информирующее об окончании указанных операций, и их результат;

Рисунок 99. Окно просмотра результата изготовления сертификата



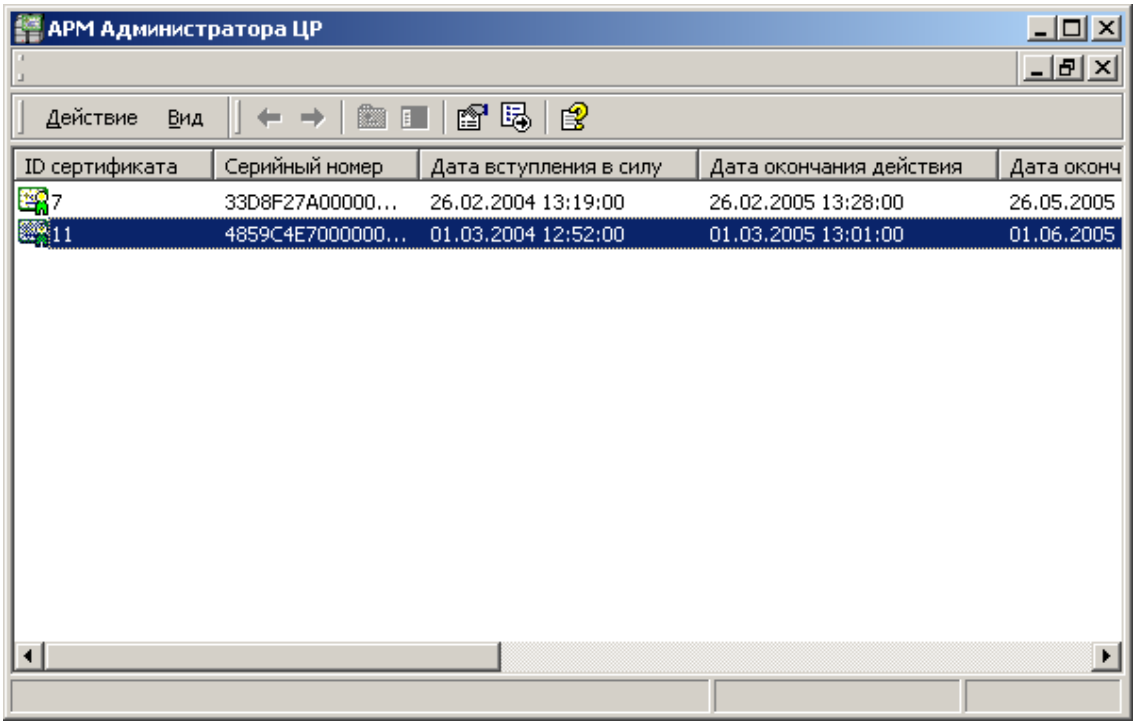
8. В правой области окна **АРМ Администратора ЦР** выделите левой кнопкой мыши узел **Пользователи**, затем в правой части окна выделите правой кнопкой мыши учетную запись пользователя, на имя которого был изготовлен сертификат, и в открывшемся контекстном меню выберите пункт **Все задачи -> Показать -> Сертификаты;**

Рисунок 100. Выбор пункта меню для просмотра сертификатов пользователя



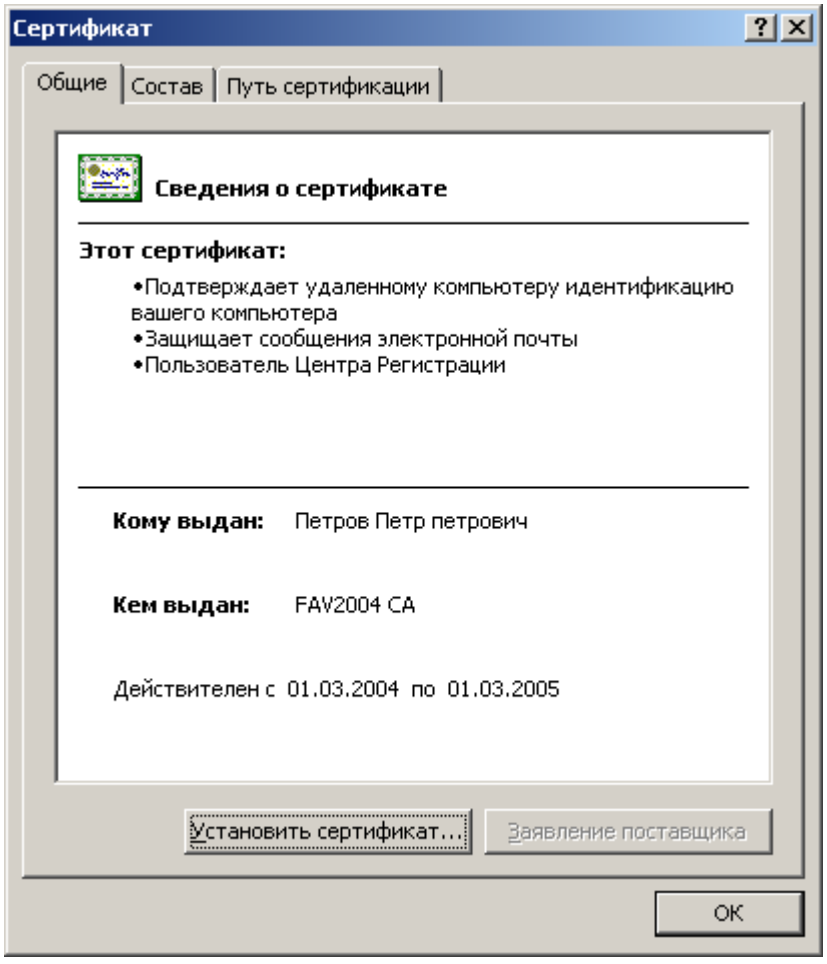
9. Откроется окно, содержащее список сертификатов пользователя;

Рисунок 101. Просмотр изготовленных сертификатов пользователя



10. Выделите изготовленный сертификат ключа подписи двойным нажатием левой кнопки мыши и просмотрите его в стандартном окне просмотра сертификатов;

Рисунок 102. Стандартное окно просмотра сертификата

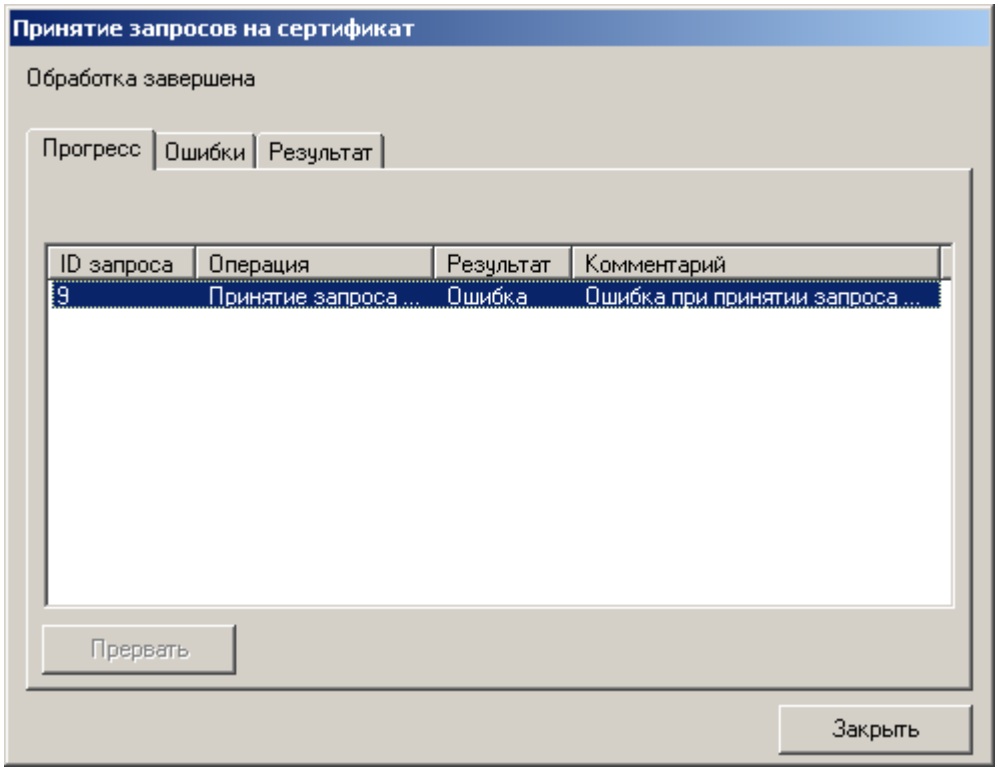


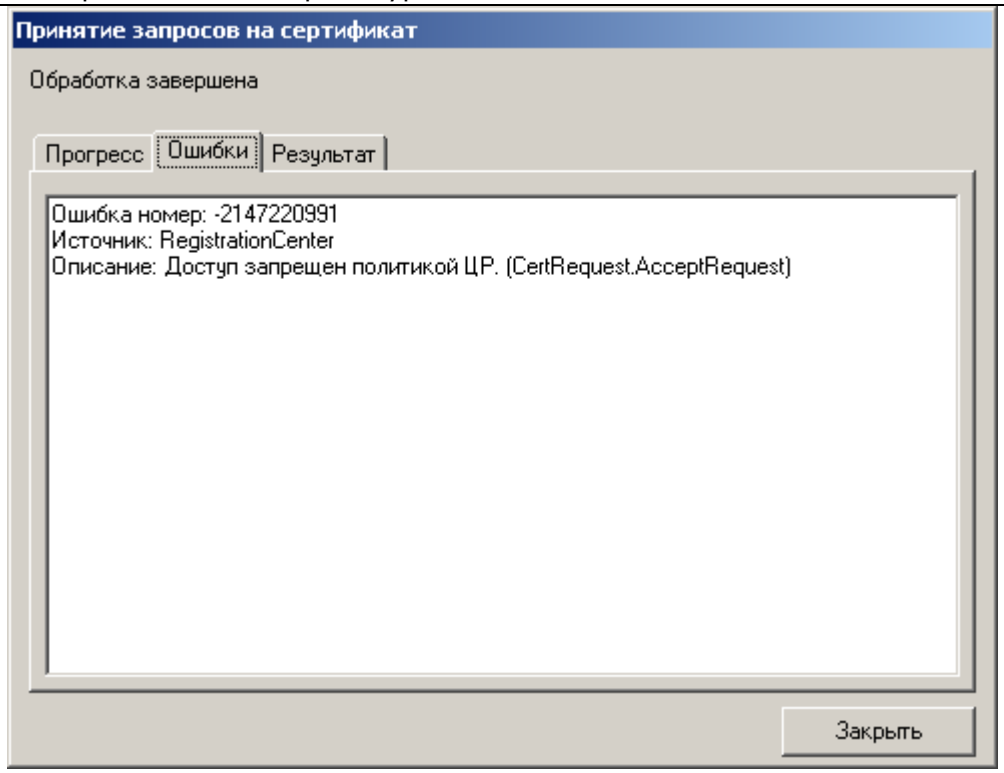
По окончании осуществления действий по изготовлению сертификата ключа подписи, целесообразно оповестить владельца изготовленного сертификата об этом. Для этого на Центре Регистрации необходимо настроить соответствующие задачи автоматического формирования и отправки почтовых сообщений (посредством электронной почты) в адрес владельца сертификата ключа подписи.

1.3.2.2. Наиболее часто встречающиеся ошибки, возникающие при изготовлении сертификата в распределенном режиме

1. При принятии запроса на сертификат (**АРМ Администратора ЦР –> Запросы на сертификат -> Запрос -> Все задачи -> Принять**) в открывшемся окне, информирующем об окончании проделанных операций, появляется сообщение об ошибке;

Рисунок 103. Ошибка при выполнении метода CertRequest.AcceptRequest



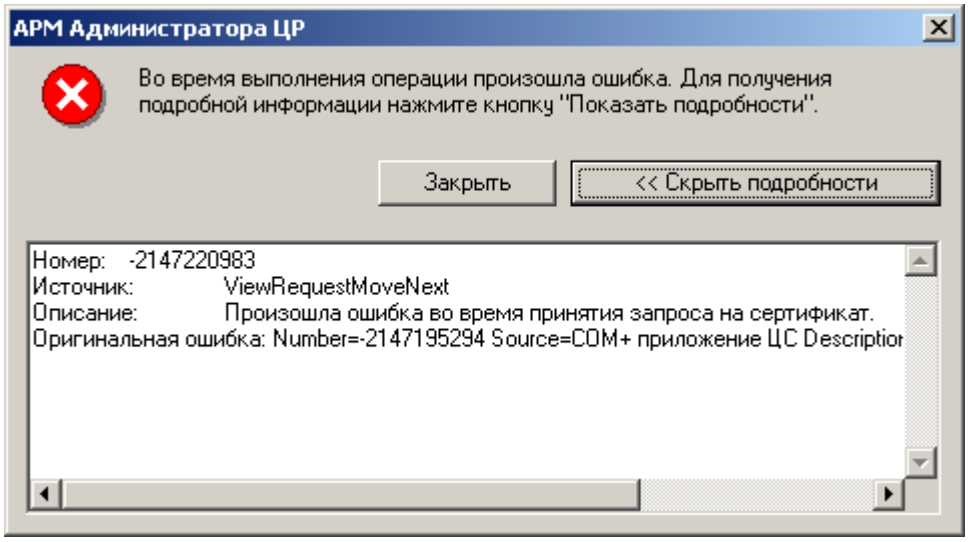


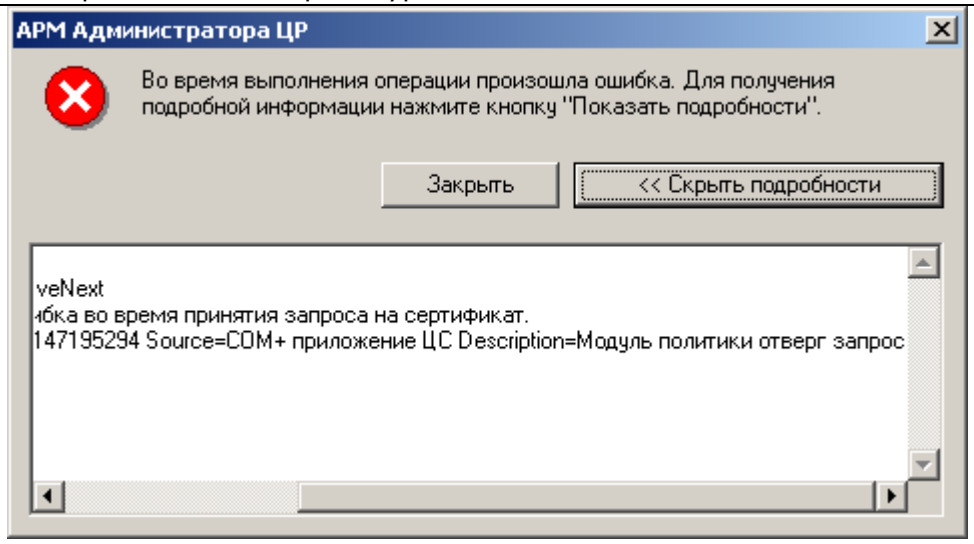
У привилегированного пользователя (**Оператора** или **Администратора**), производящего изготовление сертификата в Удостоверяющем Центре, недостаточно прав на выполнение метода **CertRequest.AcceptRequest**.

На Центре Регистрации необходимо осуществить настройку политики безопасности, позволяющую осуществлять выполнение указанного метода.

2. При принятии запроса на сертификат (**АРМ Администратора ЦР –> Запросы на сертификат -> Запрос -> Все задачи -> Принять**) в открывшемся окне, информирующем об окончании проделанных операций, появляется сообщение об ошибке;

Рисунок 104. Ошибка при обработке запроса на сертификат на Центре Сертификации





Модуль политики Центра сертификации отверг запрос – наиболее вероятная причина – на вкладке **Использование ключа** окна **Свойства Модуля политики Центра Сертификации** в списке разрешенных областей использования сертификата отсутствует хотя бы одна область, содержащаяся в запросе на сертификат.

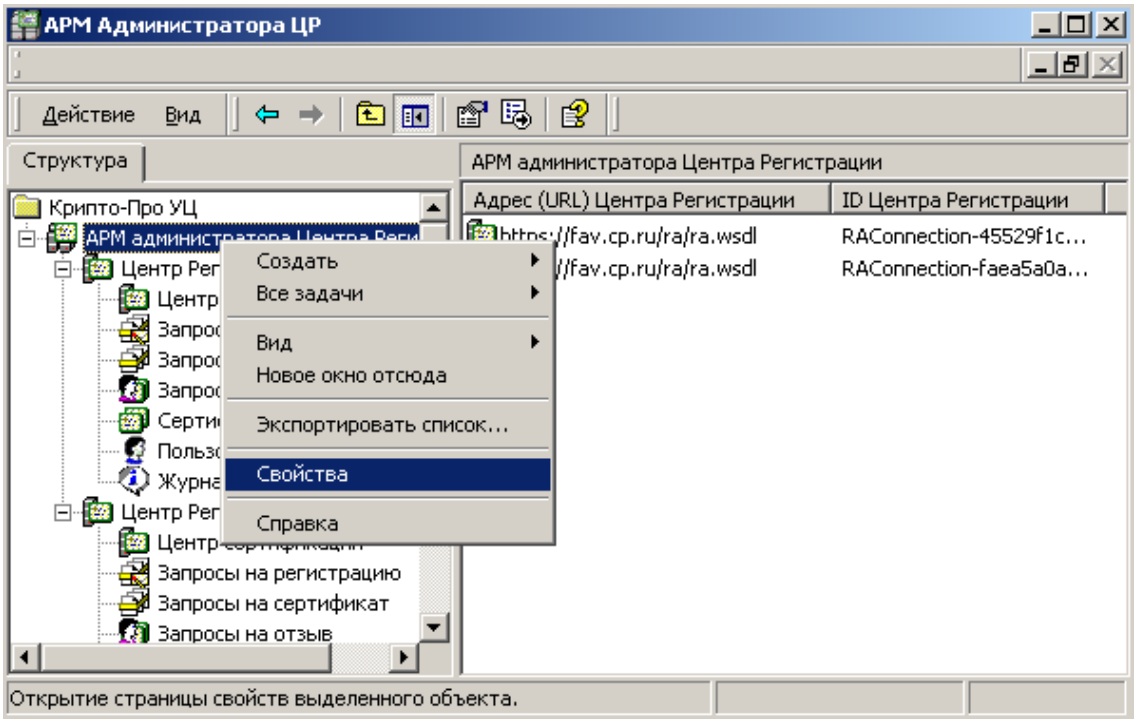
1.4. Формирование бланка сертификата ключа подписи на бумажном носителе

Структура и формат бланка сертификата ключа подписи определяется в специальном файле – шаблоне бланка сертификата ключа подписи. В состав **АРМ администратора ЦР** входит стандартный шаблон бланка сертификата ключа подписи, на основании которого можно сформировать необходимый шаблон, удовлетворяющий требованиям (в том числе и требованиям к дизайну), установленным в конкретной Организации. Стандартный шаблон бланка сертификата ключа подписи по умолчанию располагается на ПЭВМ **АРМ Администратора ЦР** по адресу **%SystemDrive%\Documents and Settings\All Users\Application Data\Crypto Pro\RA\Inetpub\1\UI\Cert.xsl.**

Описание процесса формирования бланка сертификата ключа подписи:

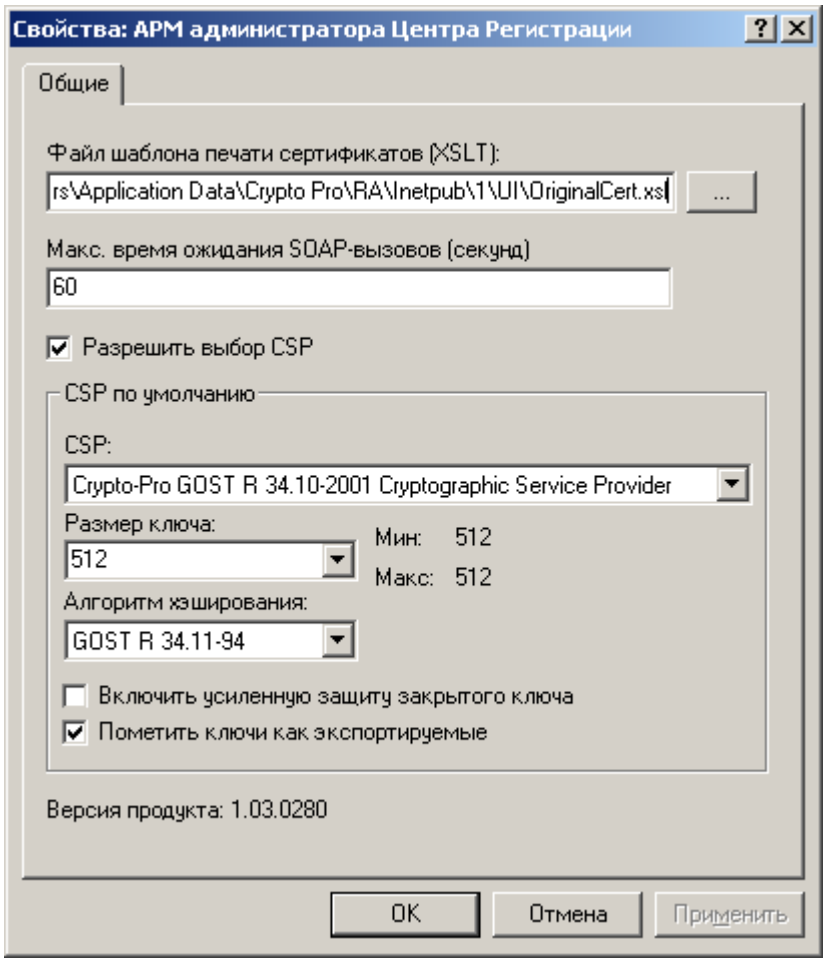
1. В окне **АРМ администратора ЦР** выделите правой кнопкой мыши узел АРМ администратора Центра Регистрации и в открывшемся контекстном меню выберите **Свойства;**

Рисунок 105. Запуск окна просмотра свойств АРМ администратора ЦР



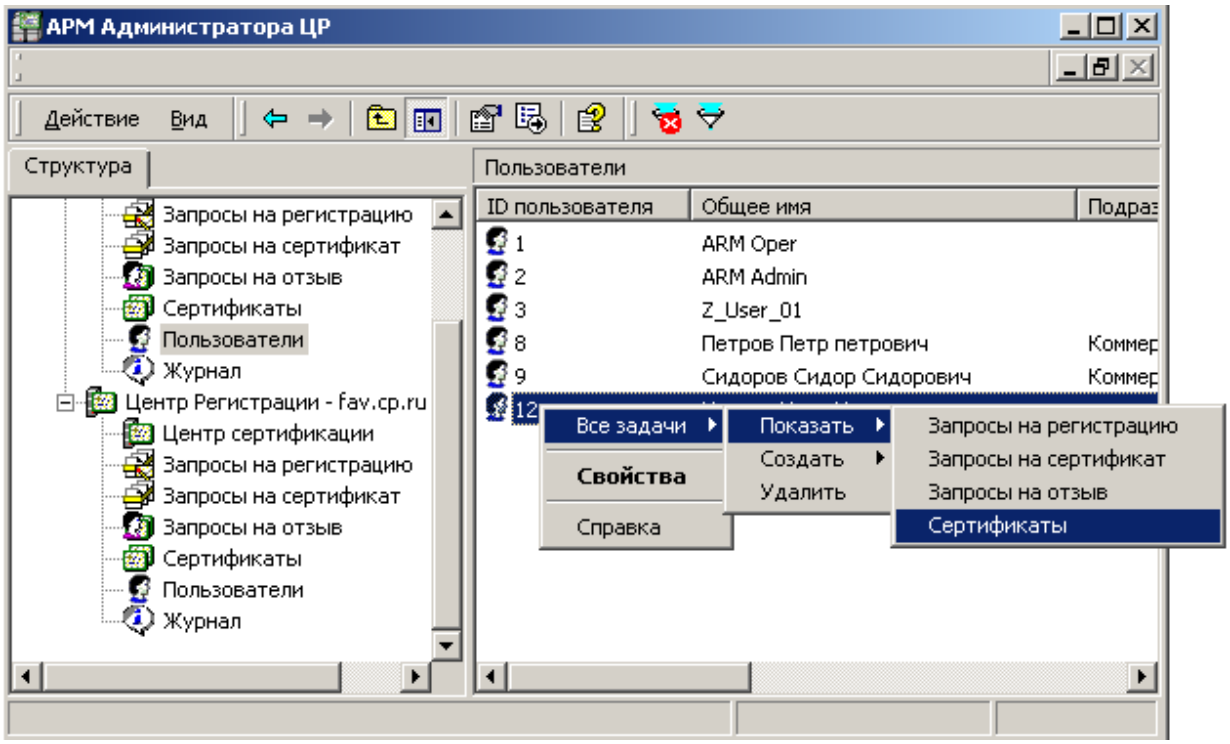
2. В окне **Свойства: АРМ администратора Центра Регистрации** с помощью кнопки **"..."** выберите необходимый файл шаблона бланка сертификата ключа подписи в поле **Файл шаблона печати сертификатов (XSLT):**

Рисунок 106. Окно Свойства: АРМ администратора Центра Регистрации - выбор файла шаблона бланка сертификата



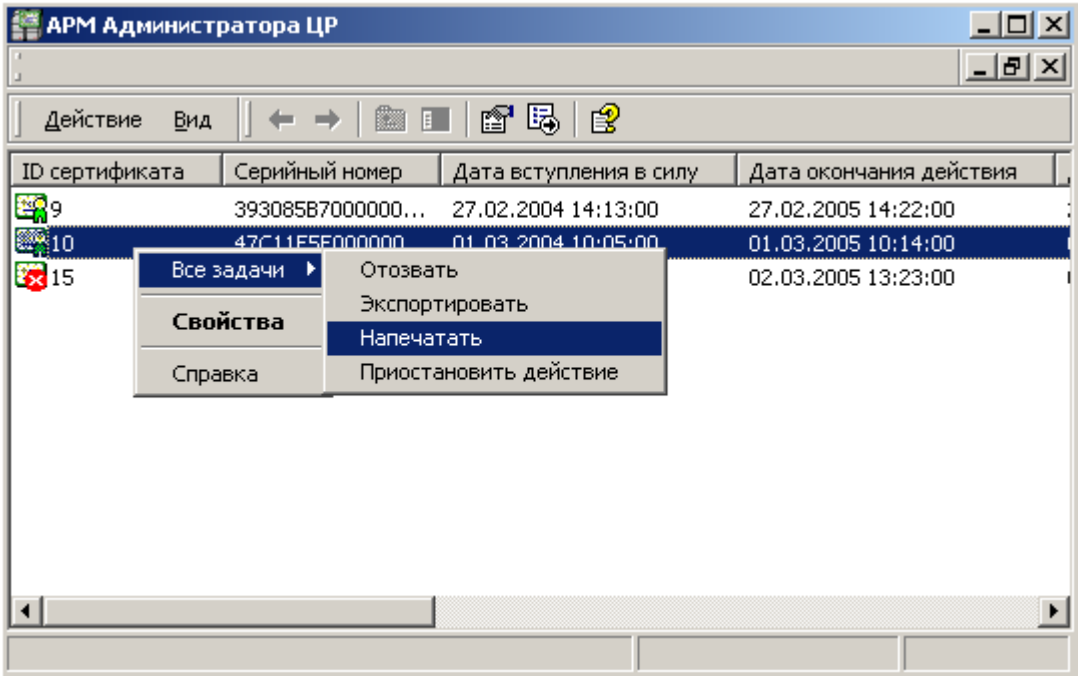
3. В окне **АРМ Администратора ЦР** выделите правой кнопкой мыши учетную запись пользователя и в открывшемся контекстном меню выберите **Все задачи -> Показать -> Сертификаты;**

Рисунок 107. Выбор пункта меню для просмотра сертификатов зарегистрированного пользователя



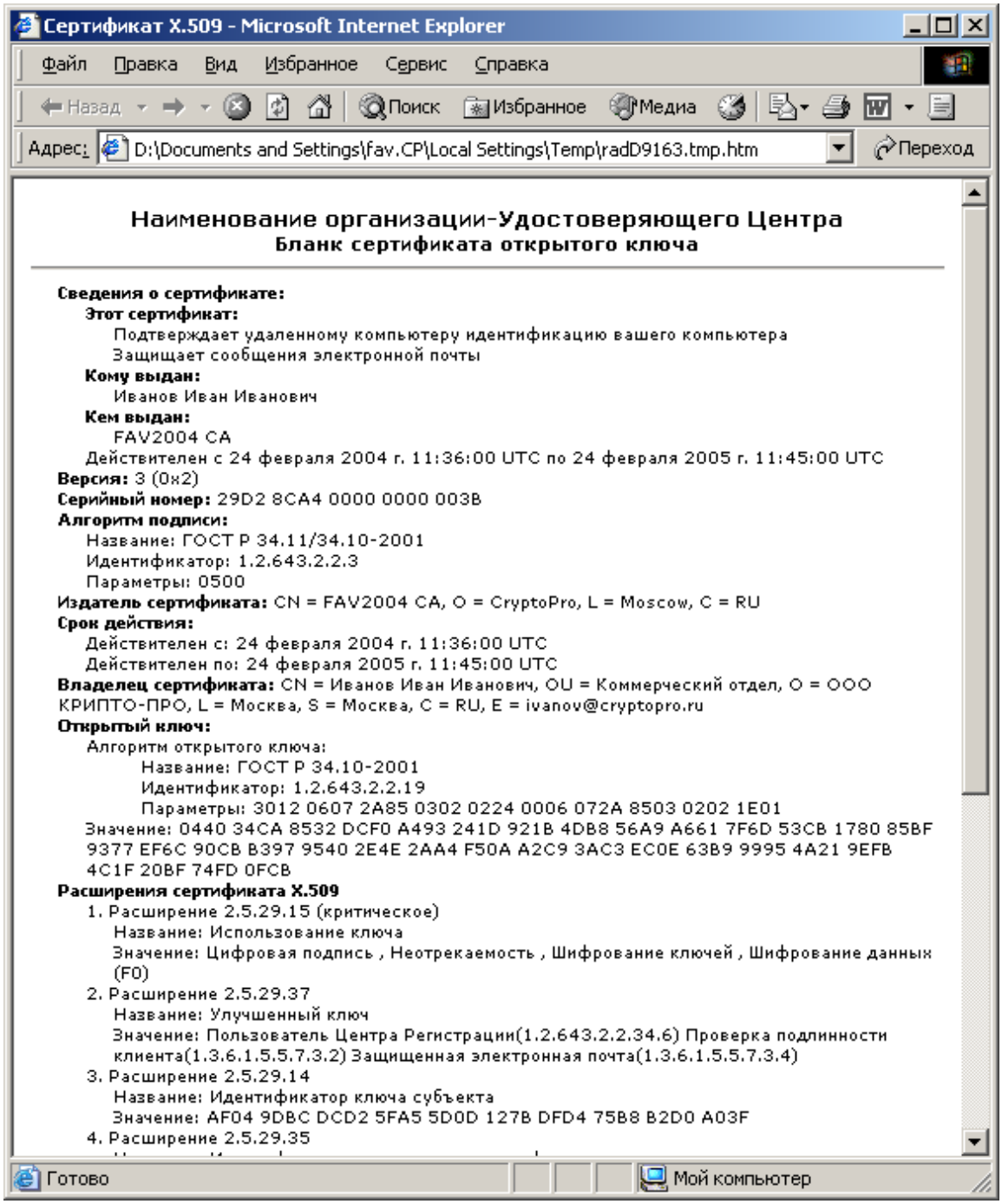
4. Выделите правой кнопкой мыши сертификат ключа подписи, для которого необходимо сформировать бланк сертификата, и в контекстном меню выберите **Все задачи -> Напечатать;**

Рисунок 108. Выбор пункта меню для печати сертификата



5. Откроется окно бланка сертификата ключа подписи

Рисунок 109. Бланк сертификата ключа подписи



6. В окне **Сертификат X.509** выберите меню **Файл/Печать...** и распечатайте бланк сертификата ключа подписи в 2-х экземплярах;

Бланк сертификата ключа подписи можно распечатать из узла **Сертификаты** окна **АРМ Администратора ЦР**. В этом случае в правой области окна **АРМ Администратора ЦР** выделите узел **Сертификаты**, в раскрывшемся списке выберите необходимый сертификат ключа подписи (убедиться в правильности выбора сертификата можно двойным нажатием левой кнопки мыши на сертификате) правой кнопки мыши и осуществите действия, описанные в пунктах 4-5 настоящего раздела.


Необходимость формирования бланков сертификатов ключей подписи (и их последующее визирование) вызвана пунктом 3 статьи 9 ФЗ №1 «Об электронной цифровой подписи» от 10.01.2002: «При изготовлении сертификатов ключей подписей Удостоверяющим Центром оформляются в форме документов на бумажных носителях два экземпляра сертификата ключа подписи, которые заверяются собственноручными подписями владельца сертификата ключа подписи и уполномоченного лица Удостоверяющего Центра, а также печатью Удостоверяющего Центра. Один экземпляр сертификата ключа подписи выдается владельцу сертификата ключа подписи, второй - остается в Удостоверяющем Центре».

1.5. Отзыв сертификата ключа подписи пользователя

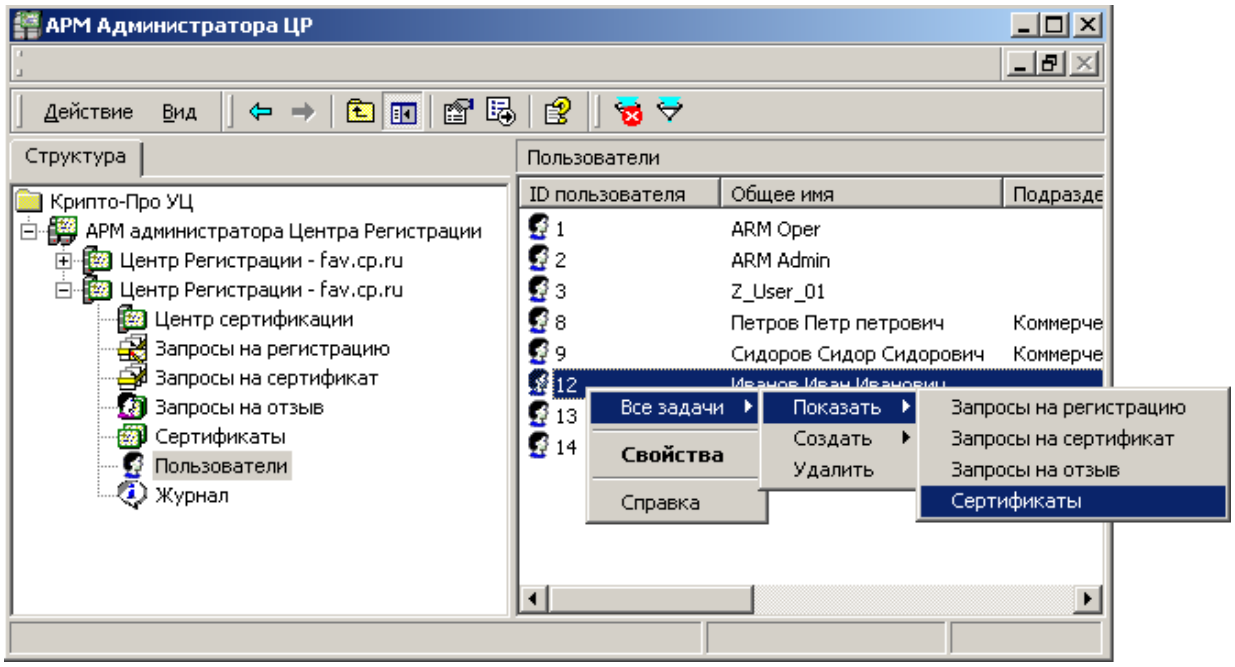
Отзыв сертификата ключа подписи осуществляется на основании запроса на отзыв сертификата ключа подписи. Запрос на отзыв сертификата ключа подписи может быть сформирован **Администратором** на **АРМ Администратора ЦР** (централизованный режим - в данном случае основанием для формирования запроса на отзыв сертификата является Заявление на отзыв сертификата, направленное пользователем в бумажном виде в Удостоверяющем центр), либо пользователем на своем рабочем месте с использованием **АРМ пользователя с ключевым доступом** (распределенный режим – запрос на отзыв сертификата подписывается на закрытом ключе пользователя и рассматривается Удостоверяющим Центром, как Заявление на отзыв сертификата ключа подписи).

1.5.1. Отзыв сертификата ключа подписи пользователя (запрос на отзыв сертификата ключа подписи формируется на **АРМ Администратора ЦР**)

Описание процедуры отзыва сертификата ключа подписи пользователя при формировании запроса на отзыв сертификата на **АРМ Администратора ЦР**:

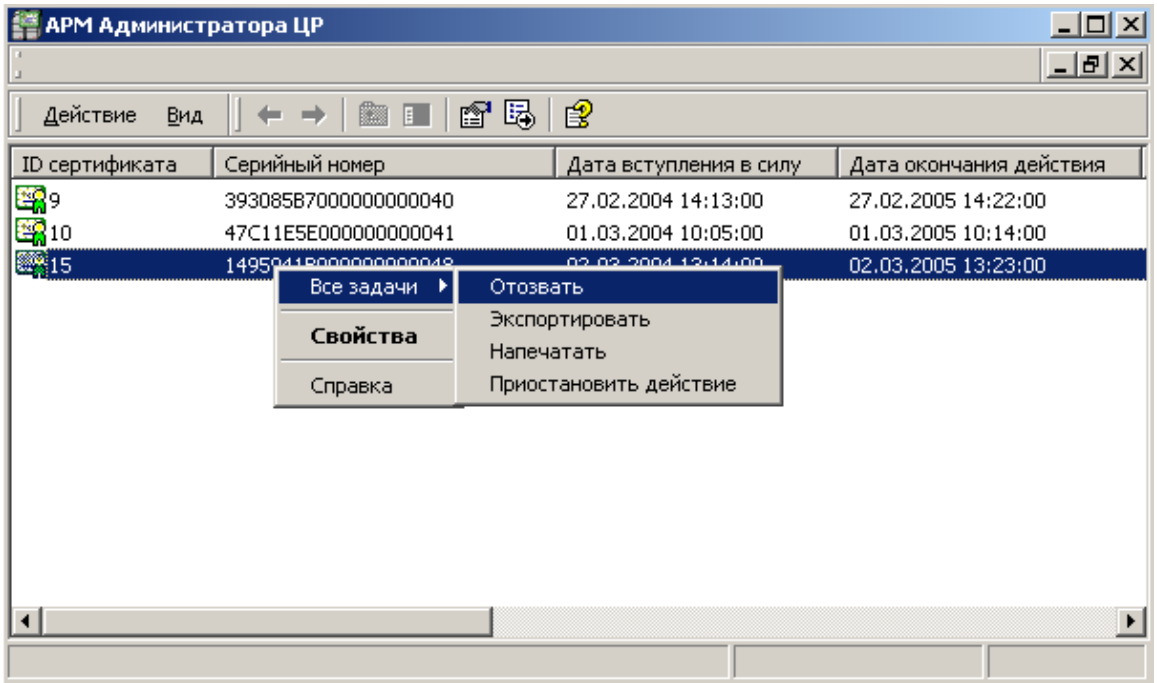
1. В окне **АРМ Администратора ЦР** выделите правой кнопкой мыши учетную запись пользователя, сертификат ключа подписи которого требуется отозвать, в открывшемся контекстном меню выберите **Все задачи -> Показать -> Сертификаты;**

Рисунок 110. Окно выбора пункта меню для просмотра сертификатов пользователя



2. Выделите правой кнопкой мыши сертификат ключа подписи, который необходимо отозвать, и в контекстном меню выберите **Все задачи -> Отозвать;**

Рисунок 111. Выбор пункта меню для отзыва сертификата



В Заявлении на отзыв сертификата ключа подписи, подаваемом в Удостоверяющий Центр в бумажном виде, должны быть указаны следующие сведения:

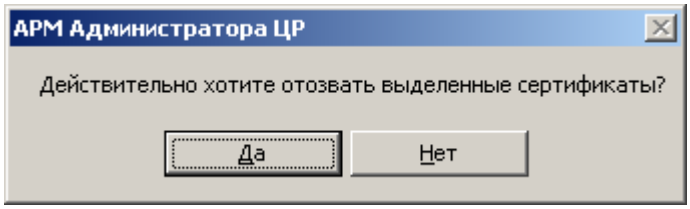
- Серийный номер отзываемого сертификата;

- Идентификационные данные пользователя – владельца данного сертификата;
- Причина отзыва сертификата.

Именно на основании приведенных данных **Администратор** осуществляет отзыв сертификата ключа подписи.

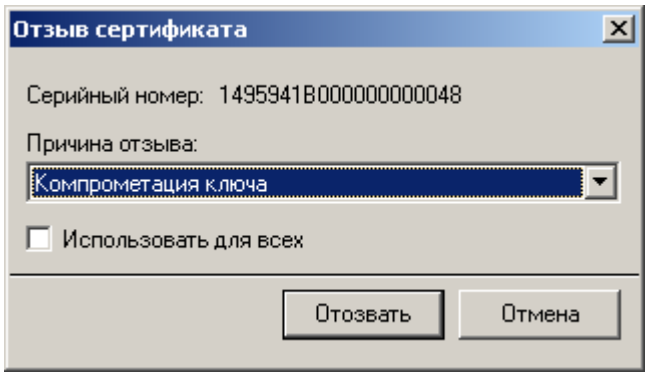
3. Откроется предупреждающее окно, требующее подтверждения отзыва сертификата. Нажмите кнопку **Да**;

Рисунок 112. Окно подтверждения отзыва сертификата



4. Откроется окно **Отзыв сертификата**, в нем укажите причину отзыва данного сертификат ключа подписи (например, компрометация ключа) и нажмите кнопку **Отозвать;**

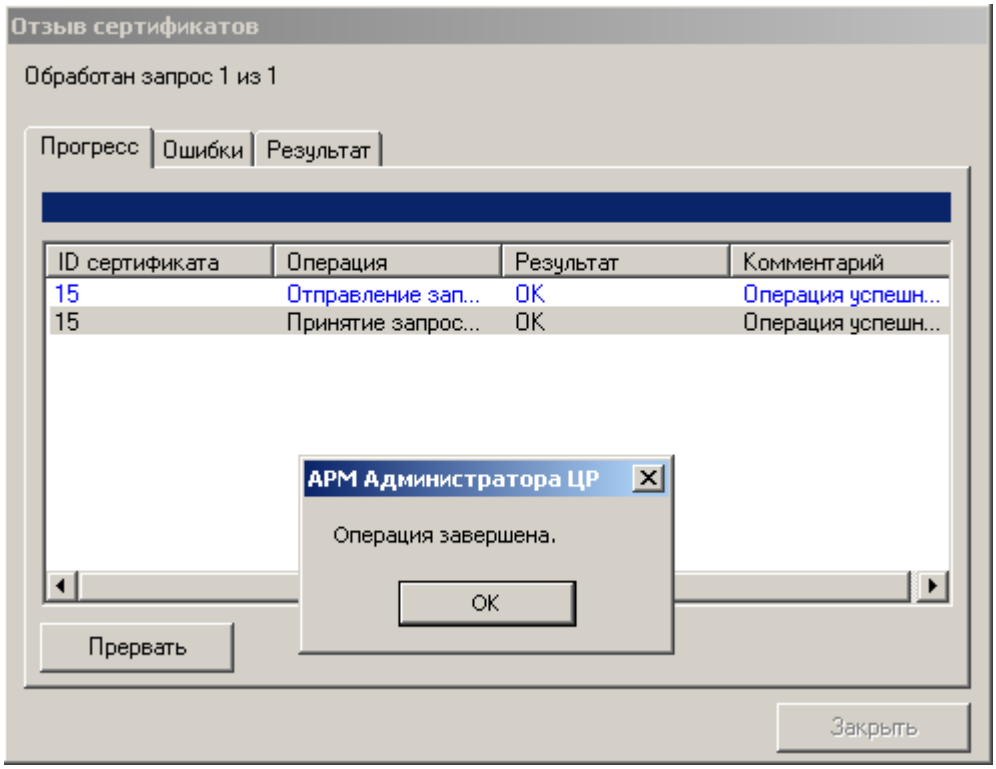
Рисунок 113. Окно ввода причины отзыва сертификата



Установка переключателя **Использовать для всех** применяется при отзыве сразу нескольких сертификатов, отзываемых по одной и той же причине, и позволяет не указывать **Администратору** причину отзыва для каждого сертификата.

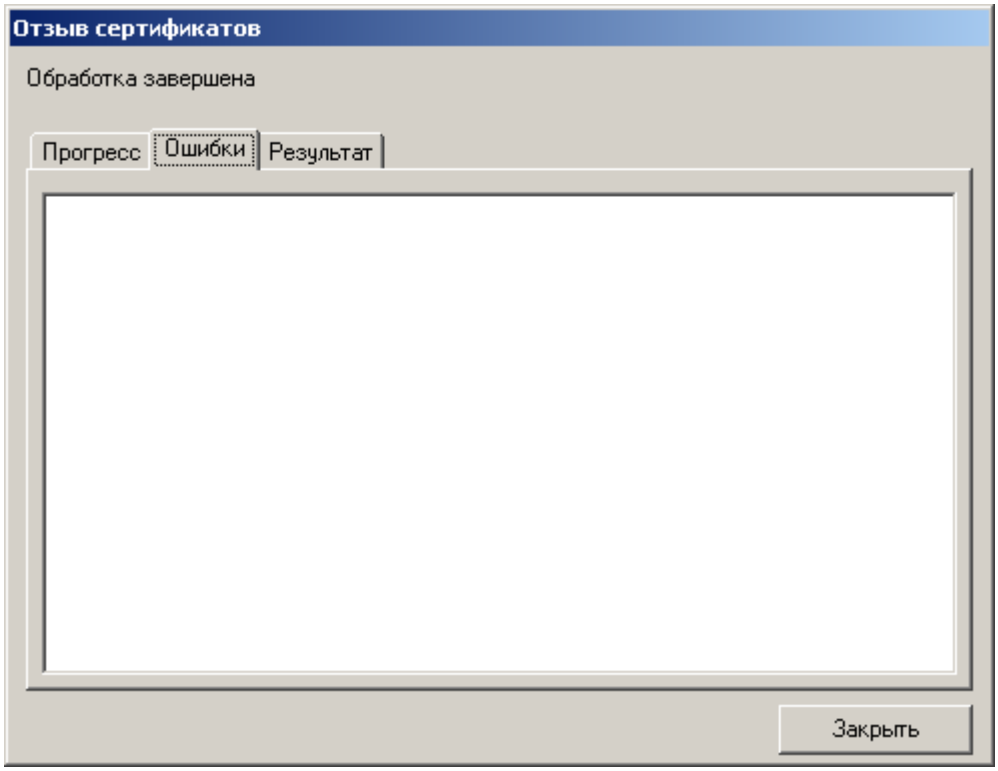
5. По окончании выполнения действий по отзыву сертификата ключа подписи появится сообщение, информирующее об окончании указанных операций, и их результат;

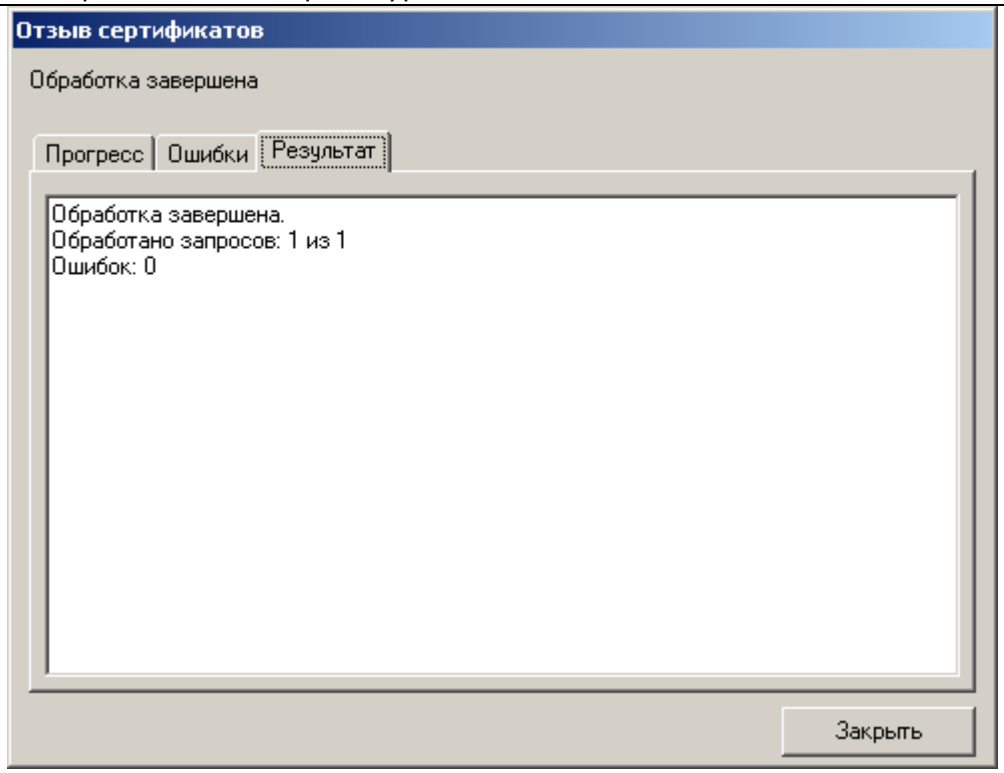
Рисунок 114. Окно просмотра результата отзыва сертификата



6. В окне **Операция завершена** нажмите кнопку **ОК** и убедитесь в том, что действия были выполнены без ошибок;

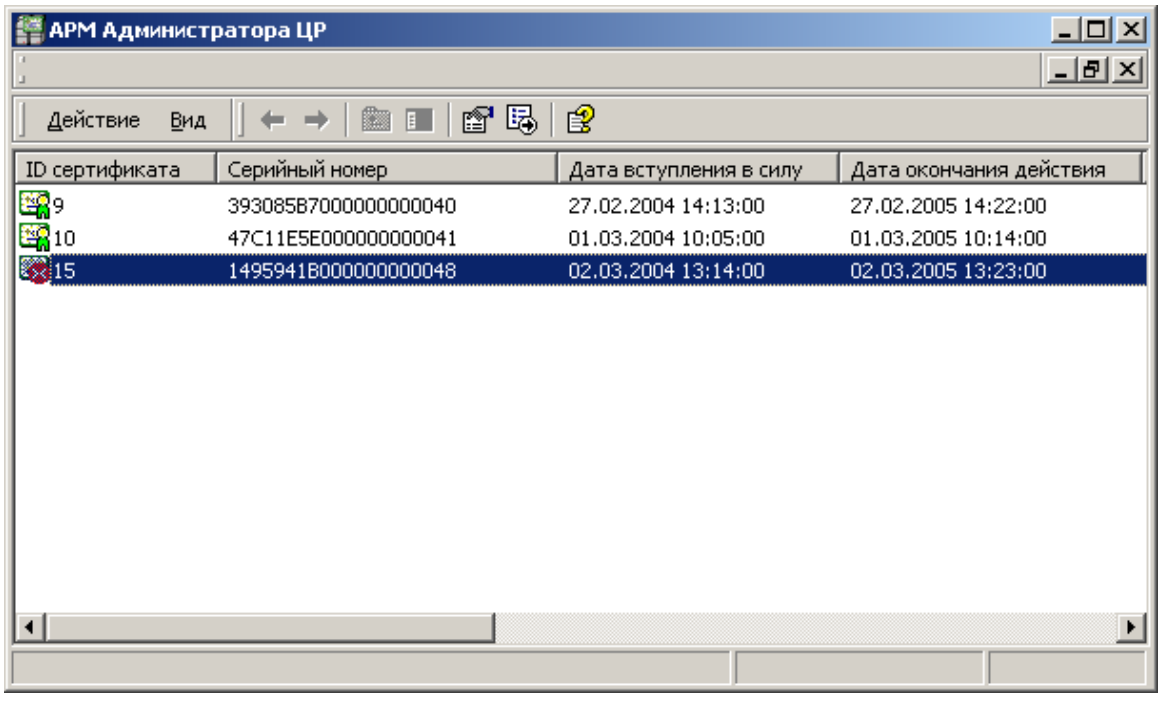
Рисунок 115. Окно просмотра возможных ошибок при отзыве сертификата





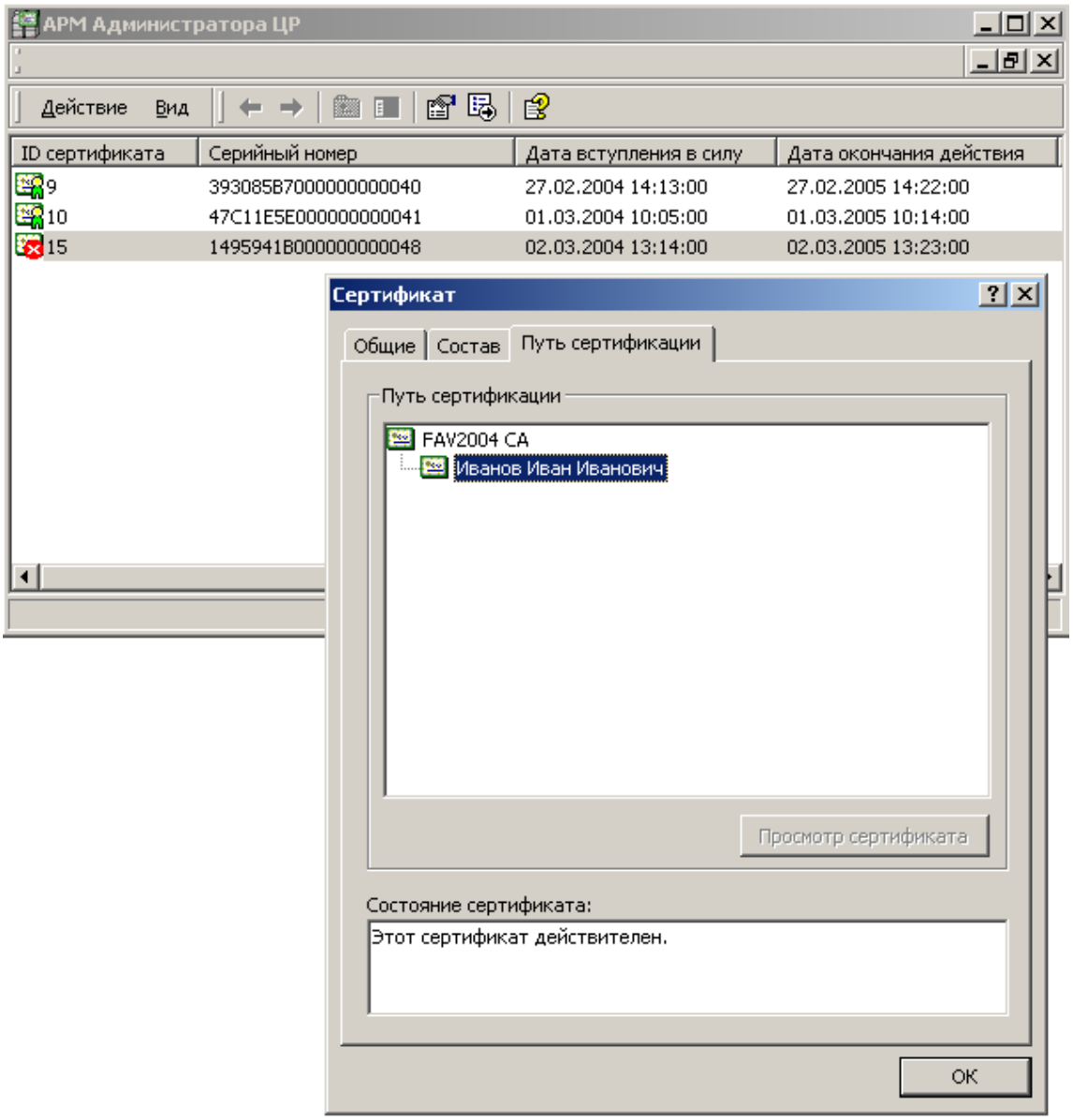
7. Нажмите кнопку **Закрыть**. Отозванный сертификат будет помечен как **не действительный** (красный круг с белым крестом внутри);

Рисунок 116. Окно просмотра сертификатов пользователя



Просмотр сертификатов ключей подписи в **АРМ Администратора ЦР** осуществляется стандартными средствами ОС Windows, поэтому отозванные сертификаты в стандартном окне просмотра сертификатов отображаются как действующие.

Рисунок 117. Просмотр отозванного сертификата в стандартном окне просмотра сертификатов



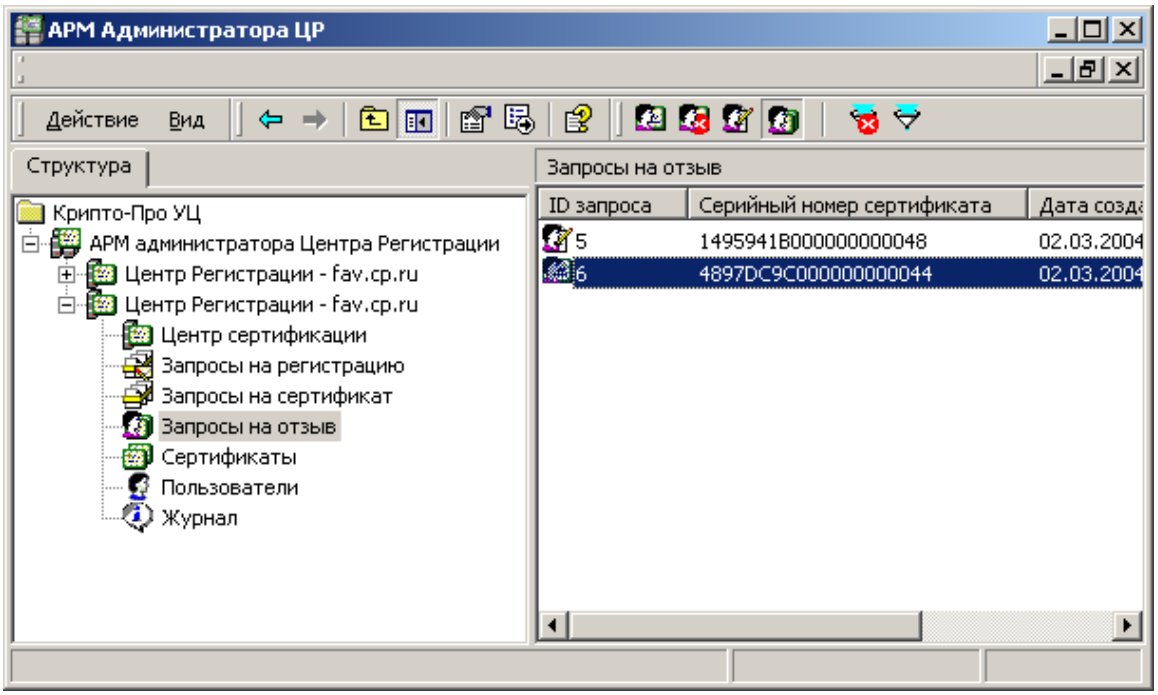
1.5.2. Отзыв сертификата ключа подписи пользователя (запрос на отзыв сертификата ключа подписи формируется пользователем с использованием **АРМ пользователя с ключевым доступом**)

Описание процедуры отзыва сертификата ключа подписи пользователя при формировании запроса на отзыв сертификата с использованием **АРМ пользователя с ключевым доступом:**

1. Пользователь Удостоверяющего Центра, являющийся владельцем сертификата ключа подписи, с помощью **АРМ пользователя с ключевым доступом** формирует запрос на отзыв сертификата ключа подписи, подписывает его электронной цифровой подписью и направляет в Удостоверяющий Центр;

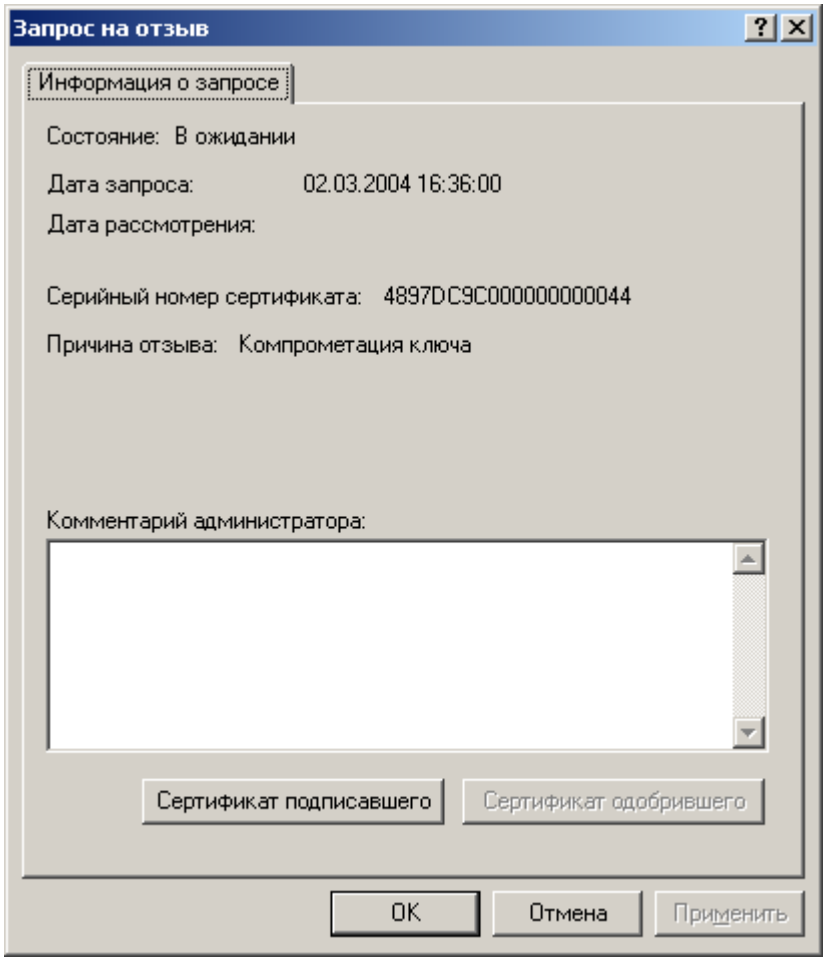
2. После отправки пользователем запроса на отзыв сертификата в окне **АРМ администратора ЦР** в папке **Запросы на отзыв** появляется новый запрос, ожидающий обработки;

Рисунок 118. Окно просмотра запросов на отзыв сертификата



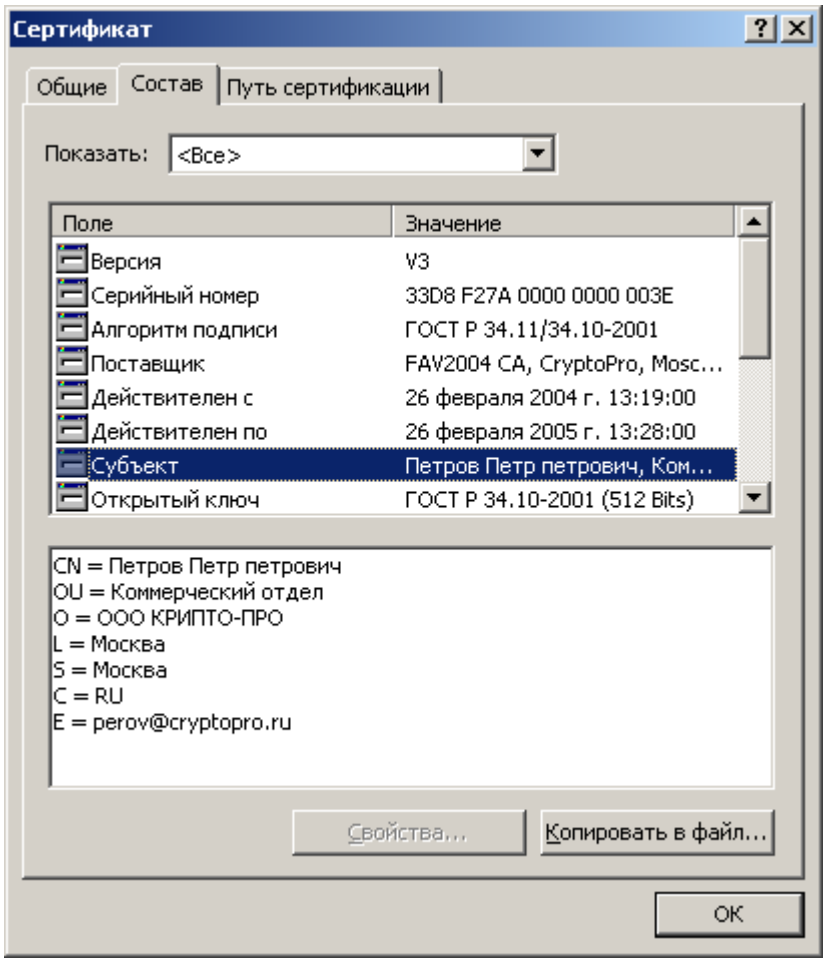
3. Выделите правой кнопкой мыши поступивший запрос на отзыв сертификата и в открывшемся контекстном меню выберите пункт **Свойства.** Откроется окно свойств запроса на отзыв сертификата;

Рисунок 119. Окно просмотра свойств запроса на отзыв сертификата



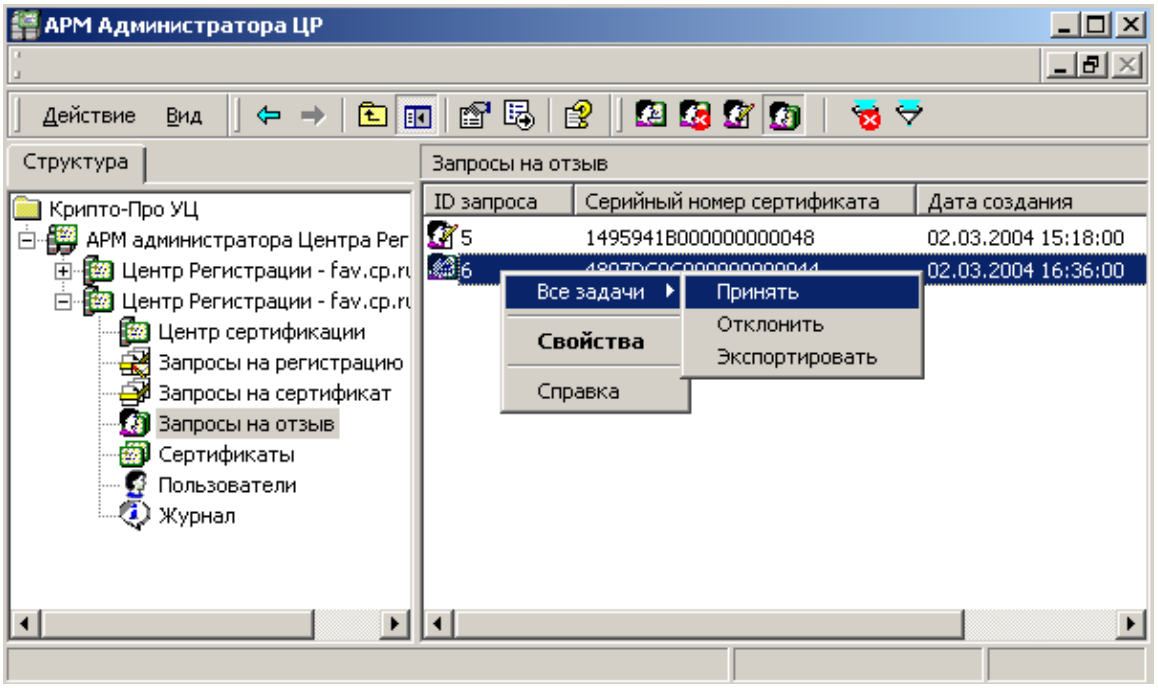
4. В окне **Запрос на отзыв** нажмите кнопку **Сертификат подписавшего**, осуществляющую просмотр сертификата зарегистрированного пользователя, направившего в Удостоверяющий Центр данный запрос;

Рисунок 120. Сертификат пользователя, направившего запрос на отзыв сертификата



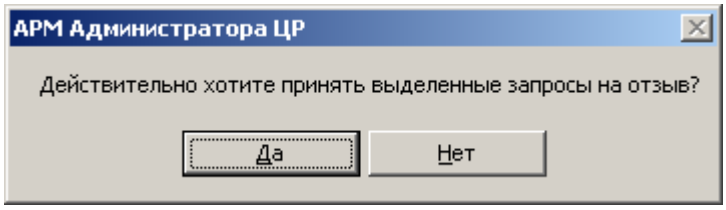
5. Убедитесь в том, что лицо, направившее запрос на отзыв сертификата – владелец сертификата, открывающегося при нажатии на кнопку **Сертификат подписавшего**, является владельцем сертификата ключа подписи, который требуется отозвать. Затем в окне **АРМ Администратора ЦР** выделите правой кнопкой мыши данный запрос на отзыв сертификата и в открывшемся контекстном меню выберите **Принять;**

Рисунок 121. Принятие запроса на отзыв сертификата



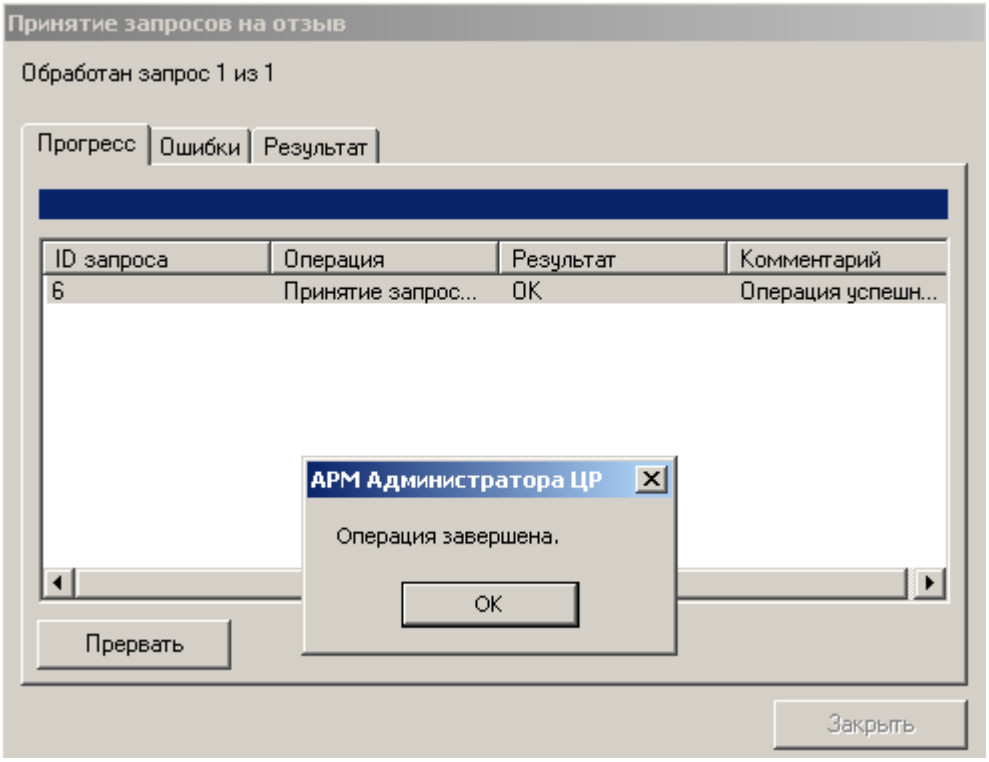
6. При принятии запроса на отзыв сертификата откроется предупреждающее окно, требующее подтверждения выбранных действий. Нажмите кнопку **Да;**

Рисунок 122. Окно подтверждения принятия запроса на отзыв сертификата



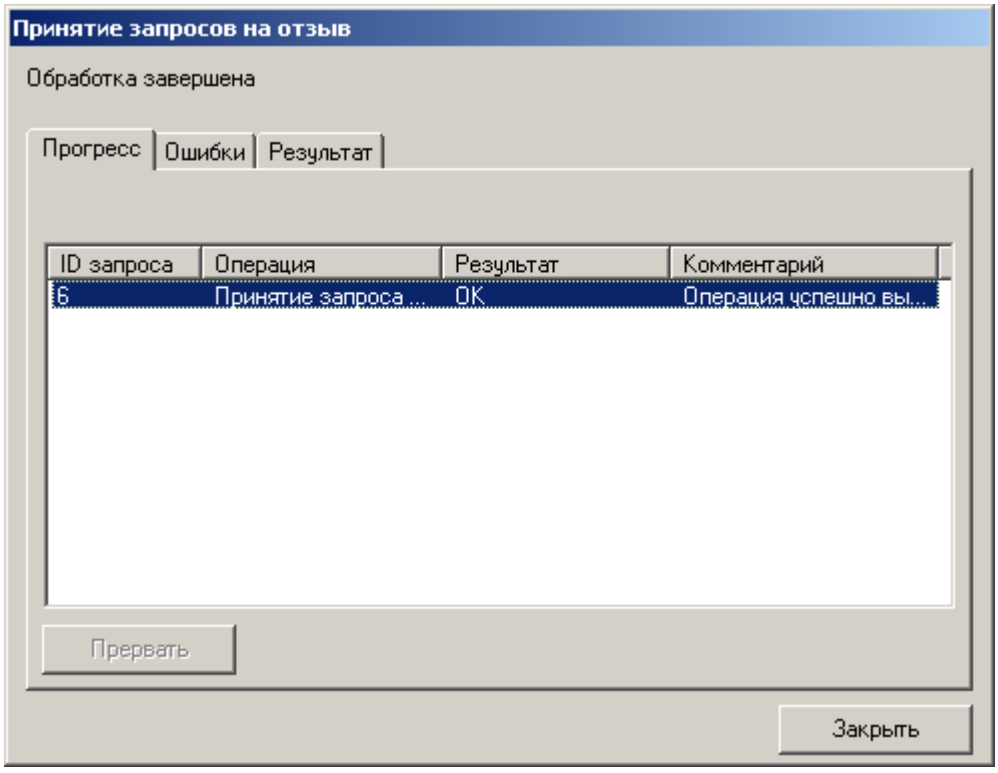
7. По окончании выполнения действий по отзыву сертификата ключа подписи появится сообщение, информирующее об окончании указанных операций, и их результат;

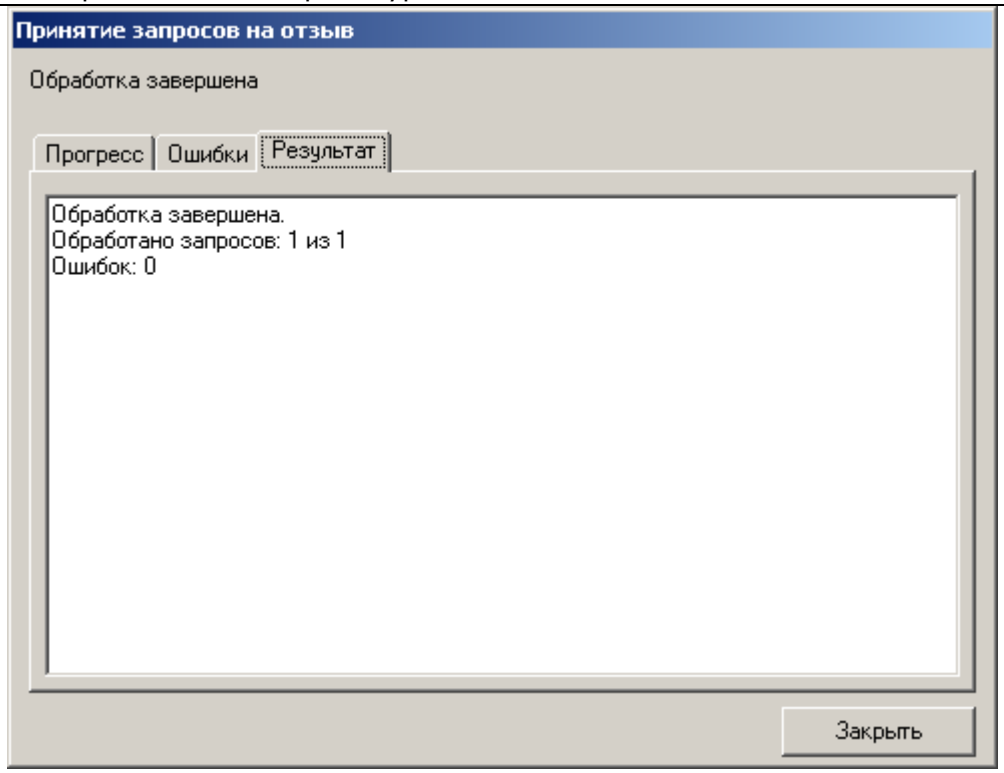
Рисунок 123. Окно просмотра результата отзыва сертификата



8. В окне **Операция завершена** нажмите кнопку **ОК** и убедитесь в том, что действия были выполнены без ошибок;

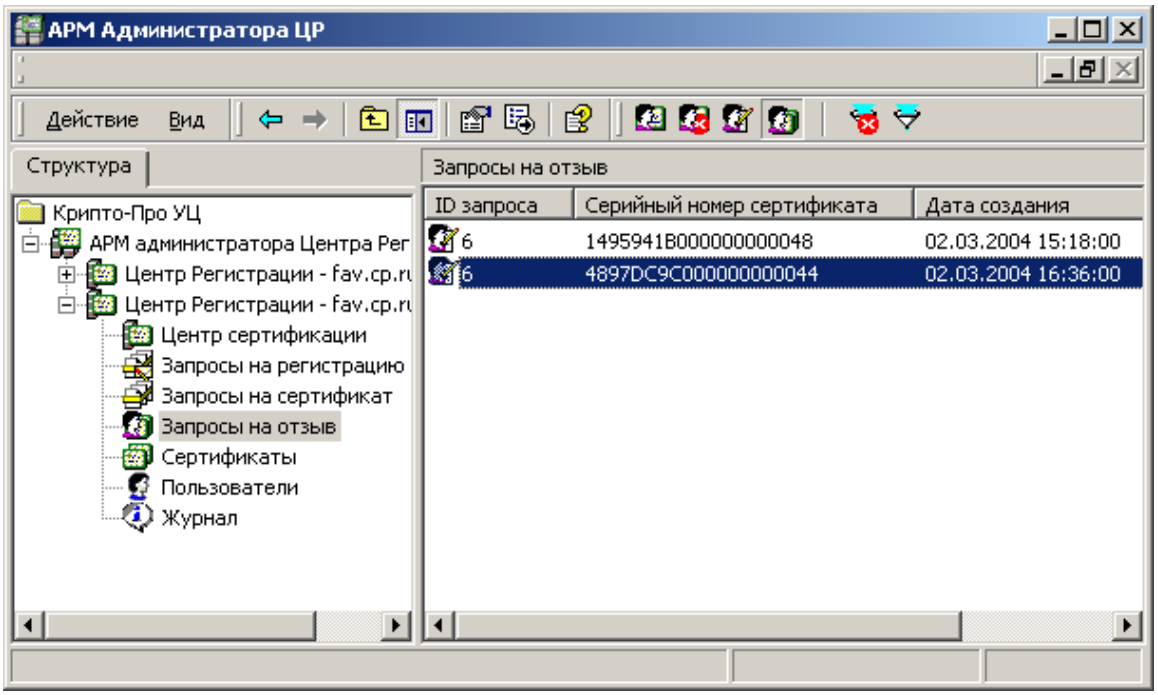
Рисунок 124. Окно просмотра ошибок, возникших при отзыве сертификата





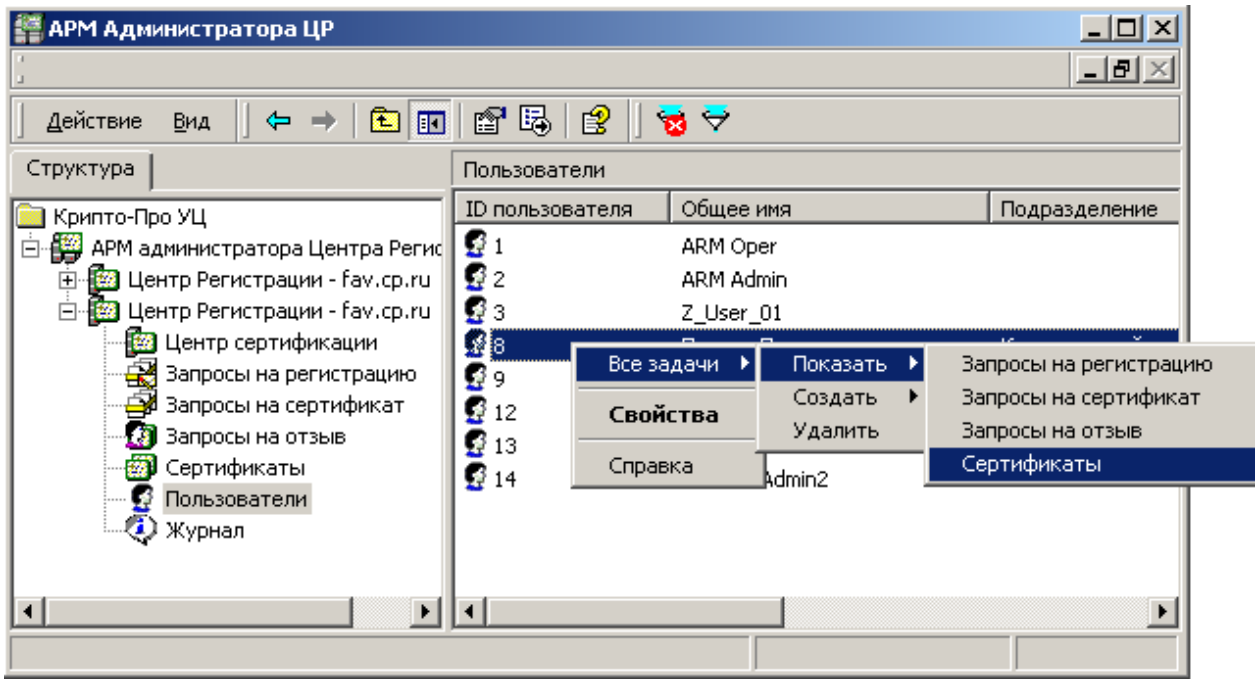
9. Нажмите кнопку **Закрыть.** Запрос на отзыв сертификата будет помечен как одобренный;

Рисунок 125. Окно просмотра запросов на отзыв



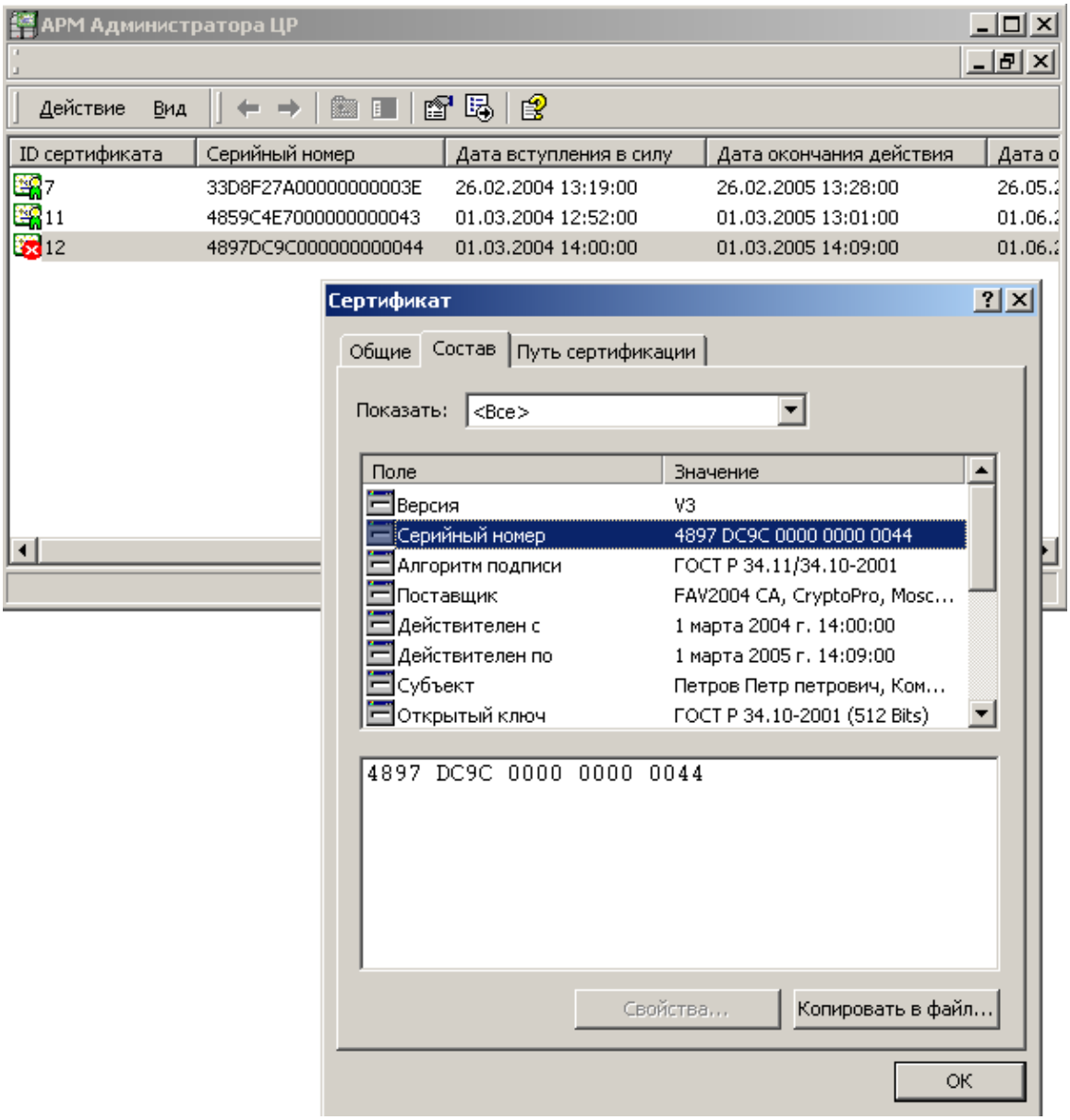
10. В левой части окна **АРМ администратора ЦР** выберите левой кнопкой мыши узел **Пользователи**. В правой части окна отобразится список зарегистрированных в Удостоверяющем Центре пользователей. Выделите правой кнопкой мыши учетную запись пользователя, сертификат которого был отозван, и в открывшемся контекстном меню выберите **Все задачи -> Показать -> Сертификаты;**

Рисунок 126. Выбор пункта меню для просмотра сертификатов пользователя



11. Откроется список сертификатов выбранного пользователя, в котором отозванный сертификат помечен как **не действительный** (красный круг с белым крестом внутри);

Рисунок 127. Окно просмотра сертификатов и отозванный сертификат пользователя

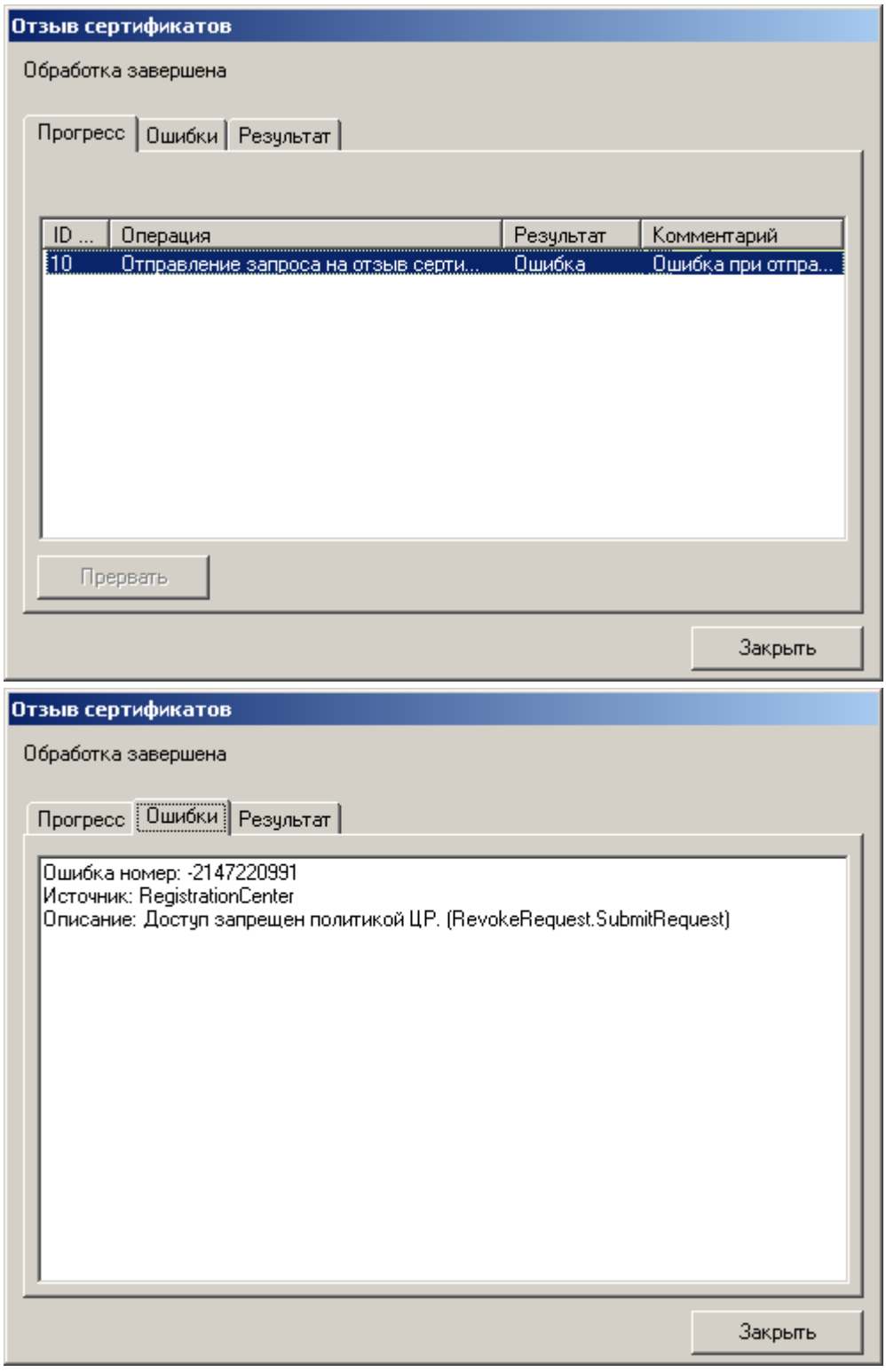


Просмотр сертификатов ключей подписи в **АРМ Администратора ЦР** осуществляется стандартными средствами ОС Windows, поэтому отозванные сертификаты в стандартном окне просмотра сертификатов отображаются как действующие.

1.5.3. Наиболее часто встречающиеся ошибки, возникающие при отзыве сертификата ключа подписи

1. При отзыве сертификата с **АРМ Администратора ЦР** привилегированным пользователем в окне **Отзыв сертификатов - Обработка завершена** возникает ошибка:

Рисунок 128. Ошибка при выполнении метода RevokeRequest.SubmitRequest

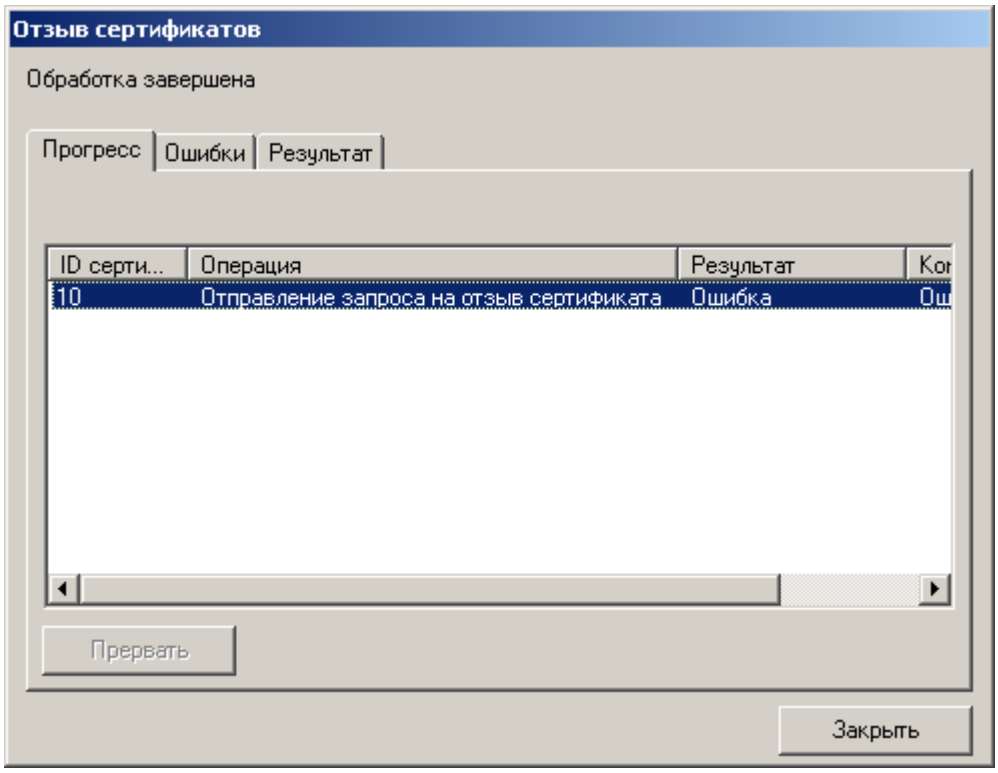


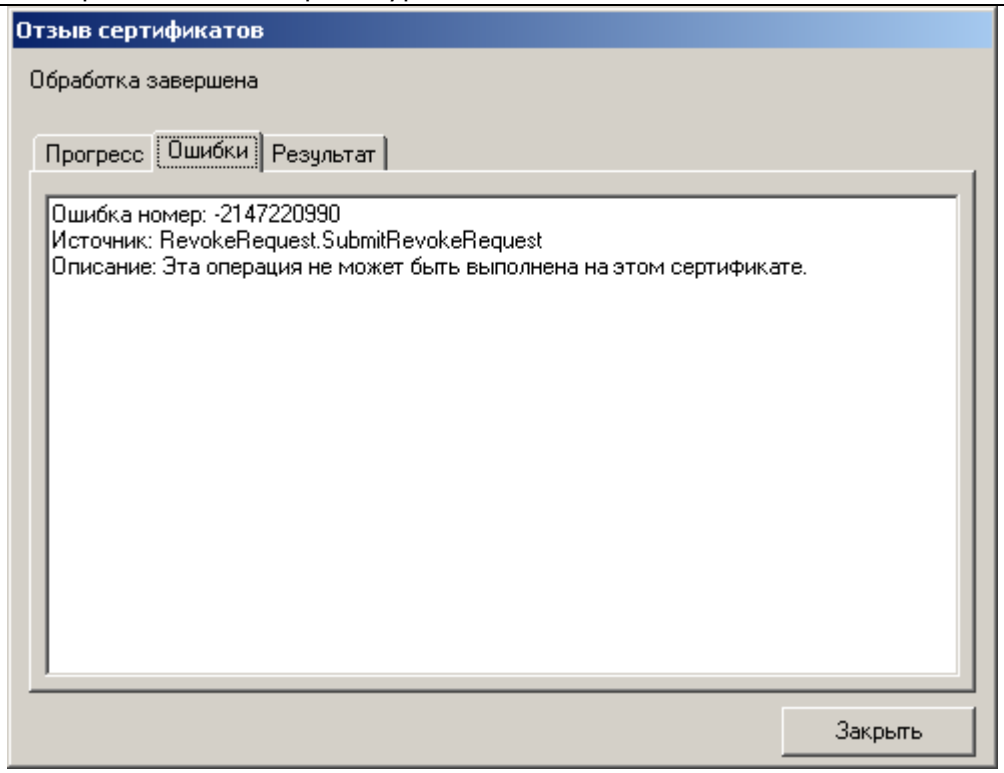
У привилегированного пользователя (**Оператора** или **Администратора**), производящего отзыв сертификата, недостаточно прав на выполнение метода **RevokeRequest.SubmitRequest**.

На Центре Регистрации необходимо осуществить настройку политики безопасности, позволяющую осуществлять выполнение указанного метода.

2. При отзыве сертификата с **АРМ Администратора ЦР** привилегированным пользователем в окне **Отзыв сертификатов - обработка завершена** возникает ошибка:

Рисунок 129. Ошибка при выполнении метода RevokeRequest.SubmitRevokeRequest



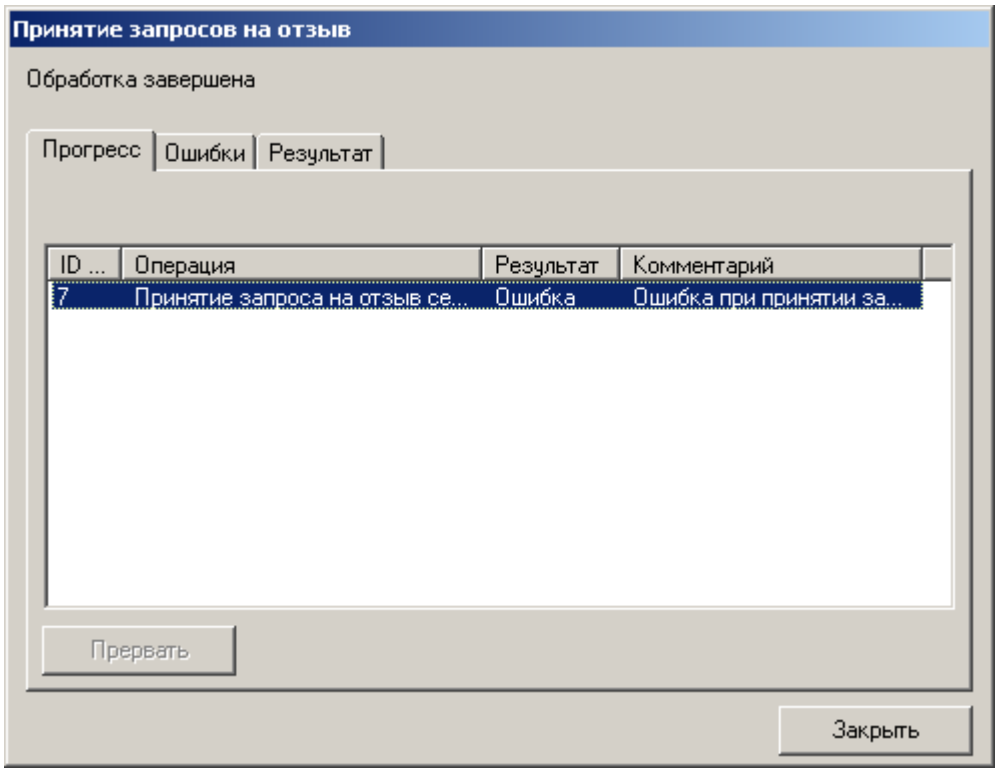


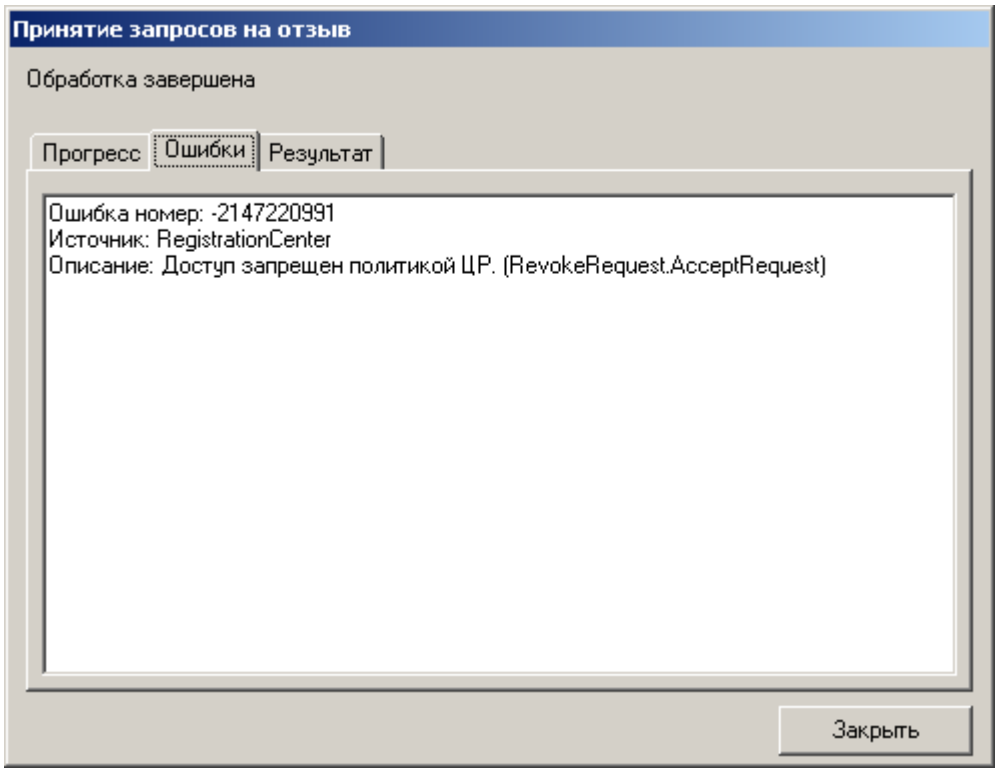
Отзываемый сертификат содержит хотя бы одну область использования (поле **Extended Key Usage**), присутствие которой в сертификате не позволяет привилегированному пользователю (**Оператору** или **Администратору**) отозвать указанный сертификат (данная область использования отсутствует в списке разрешенных для указанного привилегированного пользователя).

На Центре Регистрации осуществите настройку Политики обработки запросов на отзыв и для привилегированного пользователя, осуществляющего отзыв сертификатов, добавьте необходимые области использования сертификата.

3. При отзыве сертификата с **АРМ Администратора ЦР** привилегированным пользователем в окне **Отзыв сертификатов - обработка завершена** возникает ошибка:

Рисунок 130. Ошибка при выполнении метода RevokeRequest.AcceptRequest





У привилегированного пользователя (**Оператора** или **Администратора**), производящего отзыв сертификата, недостаточно прав на выполнение метода **RevokeRequest.AcceptRequest**.

На Центре Регистрации необходимо осуществить настройку политики безопасности, позволяющую осуществлять выполнение указанного метода.

1.6. Приостановление действия сертификата ключа подписи пользователя

Приостановление действия сертификата ключа подписи осуществляется на основании запроса на приостановление действия сертификата ключа подписи. Запрос на приостановление действия сертификата ключа подписи может быть сформирован **Администратром** на **АРМ Администратора ЦР** (централизованный режим - в данном случае основанием для формирования запроса является Заявление на приостановление действия сертификата, направленное пользователем в бумажном виде в Удостоверяющий Центр), либо пользователем на своем рабочем месте с использованием **АРМ пользователя с ключевым доступом** (распределенный режим – запрос на приостановление действия сертификата подписывается на закрытом ключе пользователя и рассматривается Удостоверяющим Центром, как Заявление на приостановление действия сертификата ключа подписи).


Основанием для приостановления действия сертификата ключа подписи также может являться устное сообщение, полученное **Администратором** от пользователя посредством телефонной связи (если данный вариант предусмотрен Регламентом Удостоверяющего Центра). В этом случае для обеспечения аутентификации пользователя используется секретное слово, полученное пользователем при регистрации в Удостоверяющем Центре.

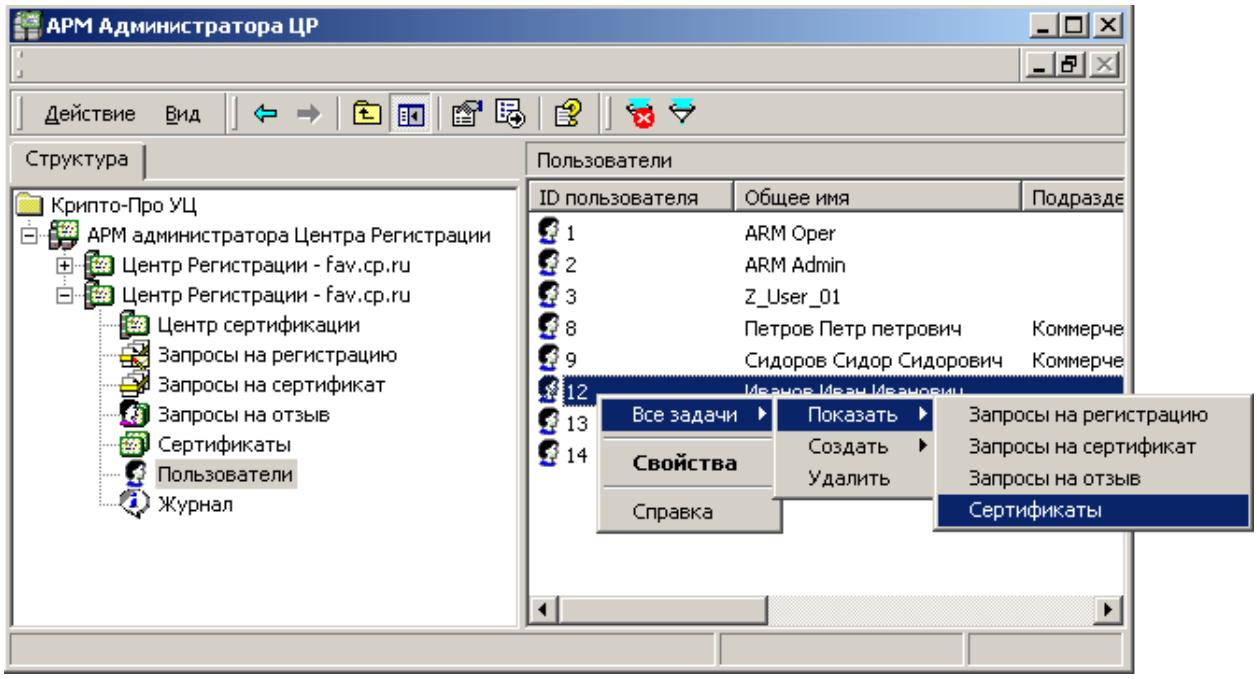

Действие сертификата ключа подписи приостанавливается на определенный срок. В том случае, если до истечения указанного срока действие сертификата ключа подписи не возобновлено, сертификат ключа подписи аннулируется (отзывается) Удостоверяющим Центром.

1.6.1. Приостановление действия сертификата ключа подписи пользователя (запрос на приостановление действия сертификата ключа подписи формируется на **АРМ Администратора ЦР**)

Описание процедуры приостановления действия сертификата ключа подписи пользователя при формировании запроса на приостановление действия сертификата на **АРМ Администратора ЦР**:

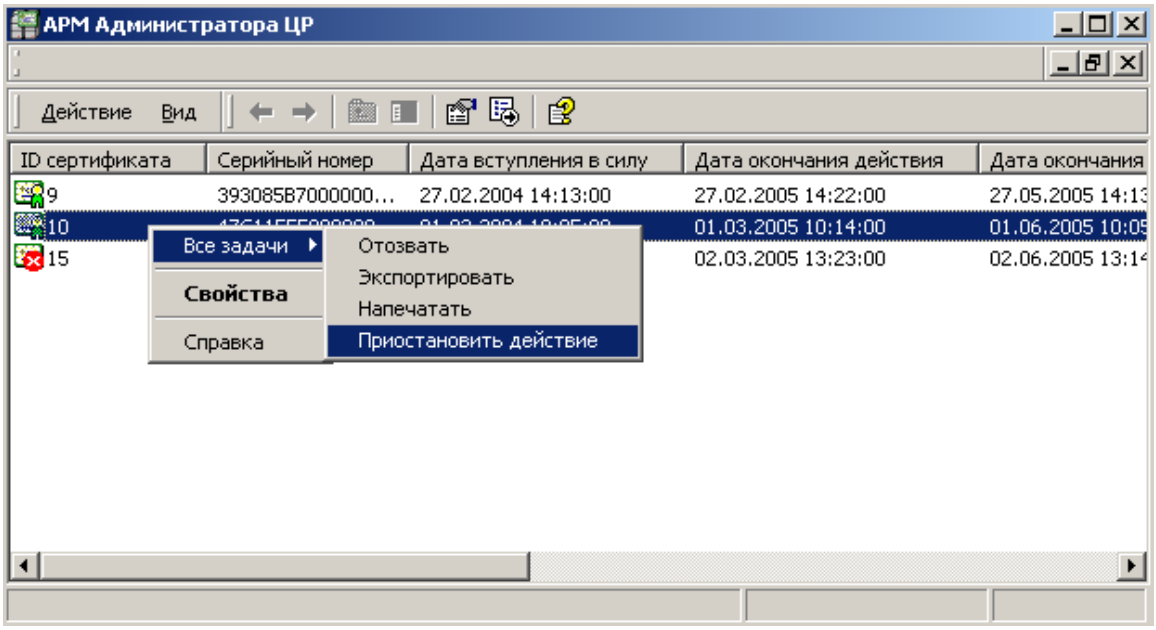
1. В окне **АРМ Администратора ЦР** выделите правой кнопкой мыши учетную запись пользователя, действие сертификата ключа подписи которого требуется приостановить, в открывшемся контекстном меню выберите **Все задачи -> Показать -> Сертификаты.**

Рисунок 131. Выбор пункта меню для просмотра сертификатов зарегистрированного пользователя



2. Выделите правой кнопкой мыши сертификат ключа подписи, действие которого необходимо приостановить, и в контекстном меню выберите **Все задачи -> Приостановить действие;**

Рисунок 132. Выбор пункта меню для приостановления действия сертификата пользователя



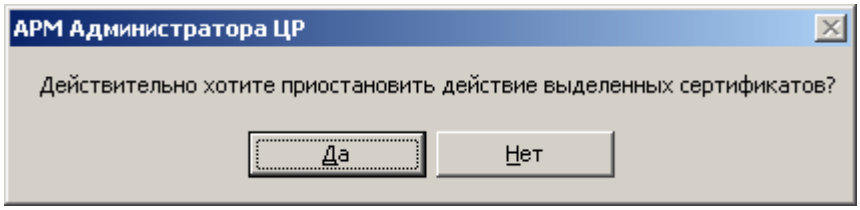
В Заявлении на приостановление действия сертификата ключа подписи, подаваемом в Удостоверяющий Центр в бумажном виде, должны быть указаны следующие сведения:

- Серийный номер сертификата, действие которого требуется приостановить;
- Идентификационные данные пользователя – владельца данного сертификата;
- Срок, на который необходимо приостановить действие сертификата.

Именно на основании приведенных в Заявлении данных **Администратор** осуществляет приостановление действия сертификата ключа подписи.

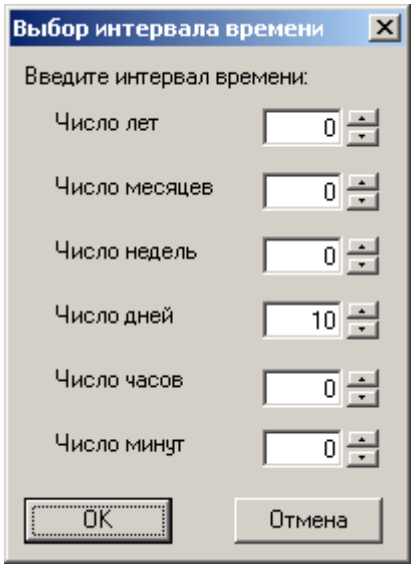
3. Откроется предупреждающее окно, требующее подтверждения приостановления действия сертификата. Нажмите кнопку **Да**;

Рисунок 133. Окно подтверждения приостановления действия сертификата



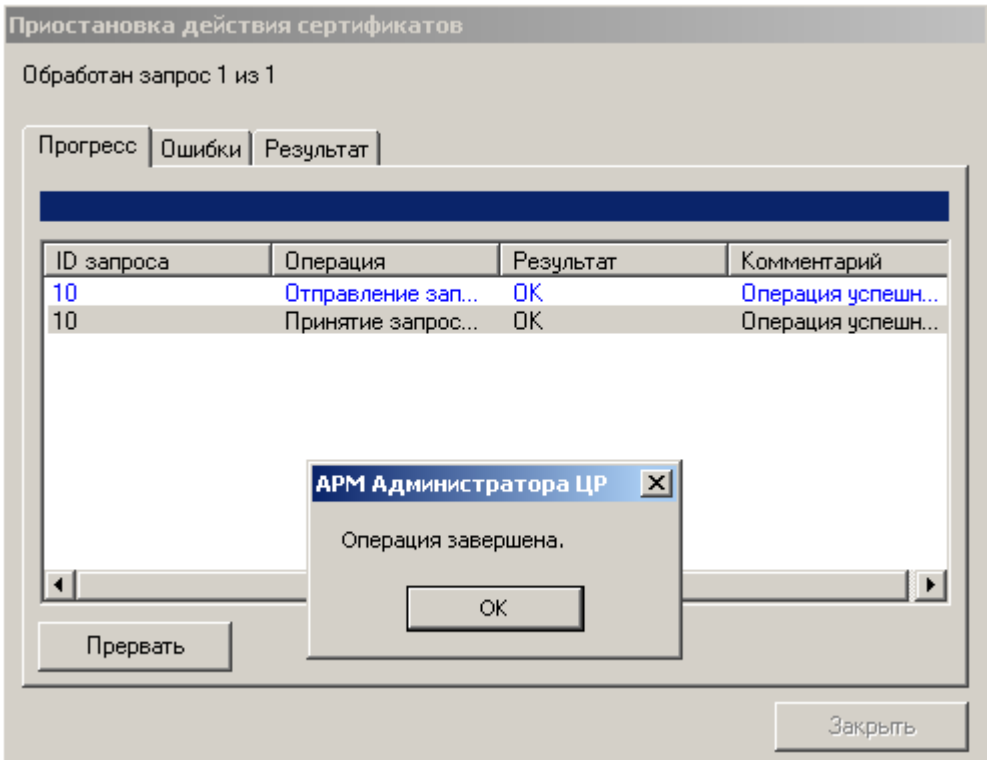
4. Выберите срок, на который действие сертификата будет приостановлено, и нажмите кнопку **ОК;**

Рисунок 134. Окно ввода срока, на который действие сертификата будет приостановлено



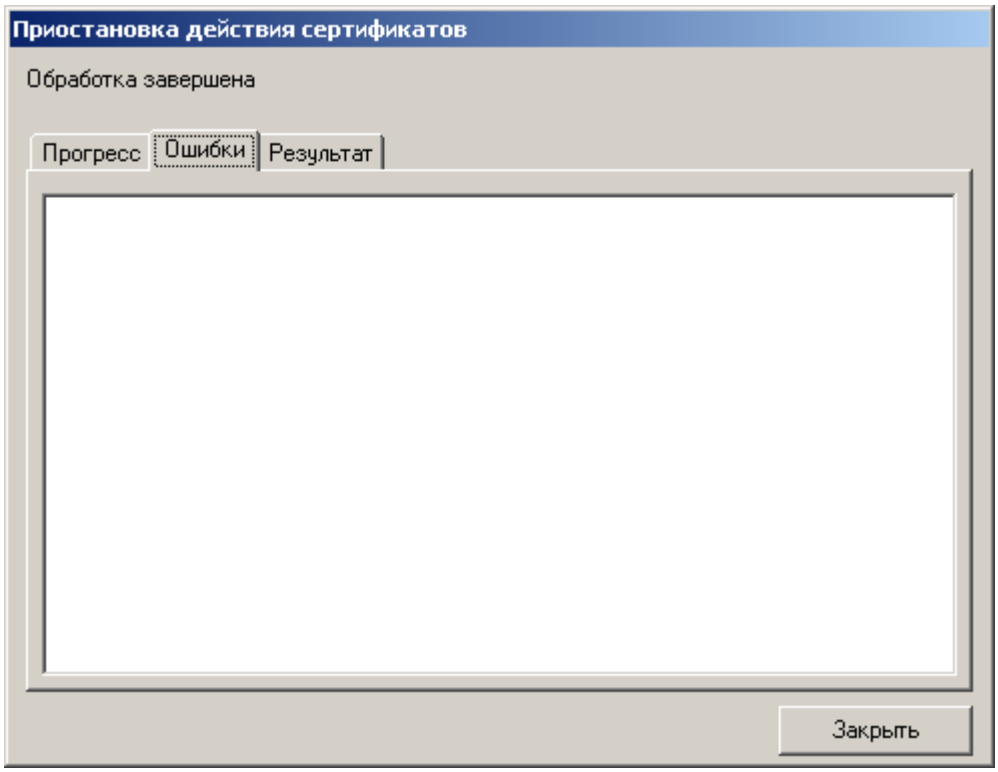
5. По окончании выполнения действий по приостановлению действия сертификата ключа подписи появится сообщение, информирующее об окончании указанных операций, и их результат;

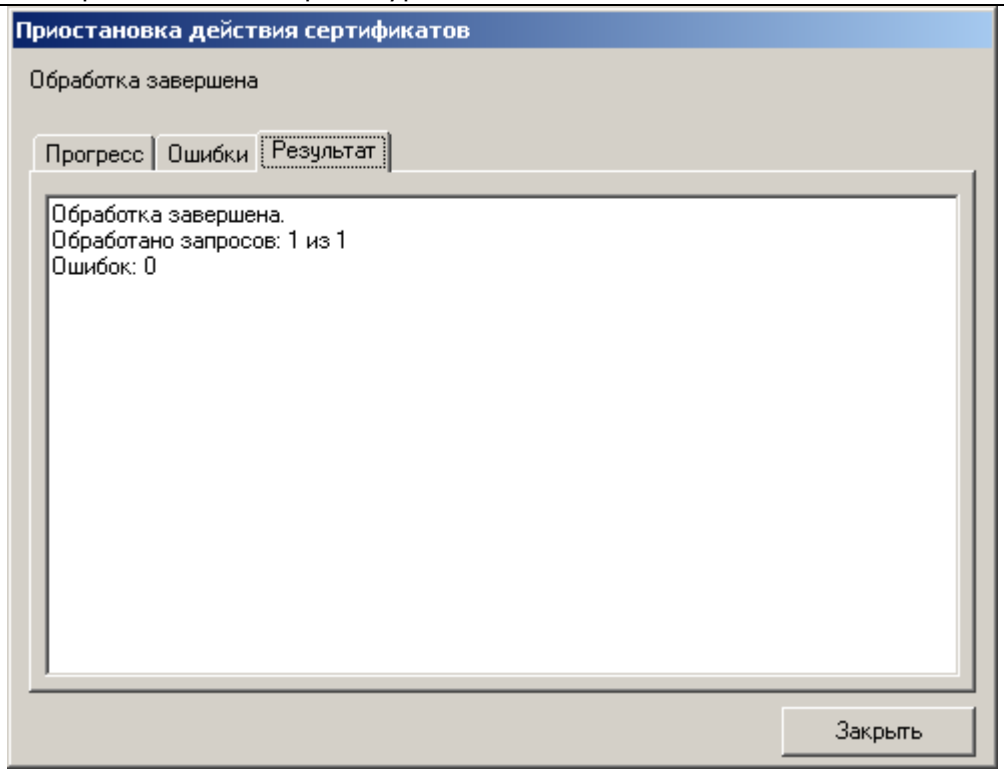
Рисунок 135. Окно просмотра результата приостановления действия сертификата



6. В окне **Операция завершена** нажмите кнопку **ОК** и убедитесь в том, что действия были выполнены без ошибок;

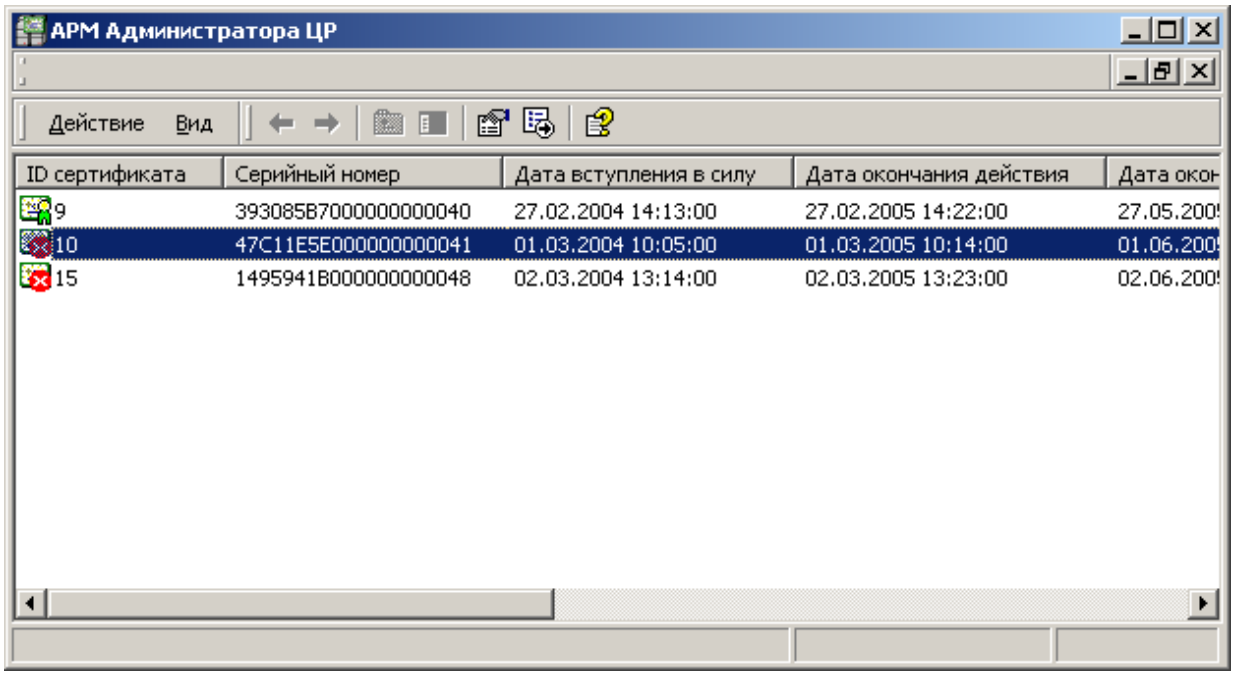
Рисунок 136. Окно просмотра возможных ошибок при приостановлении действия сертификата





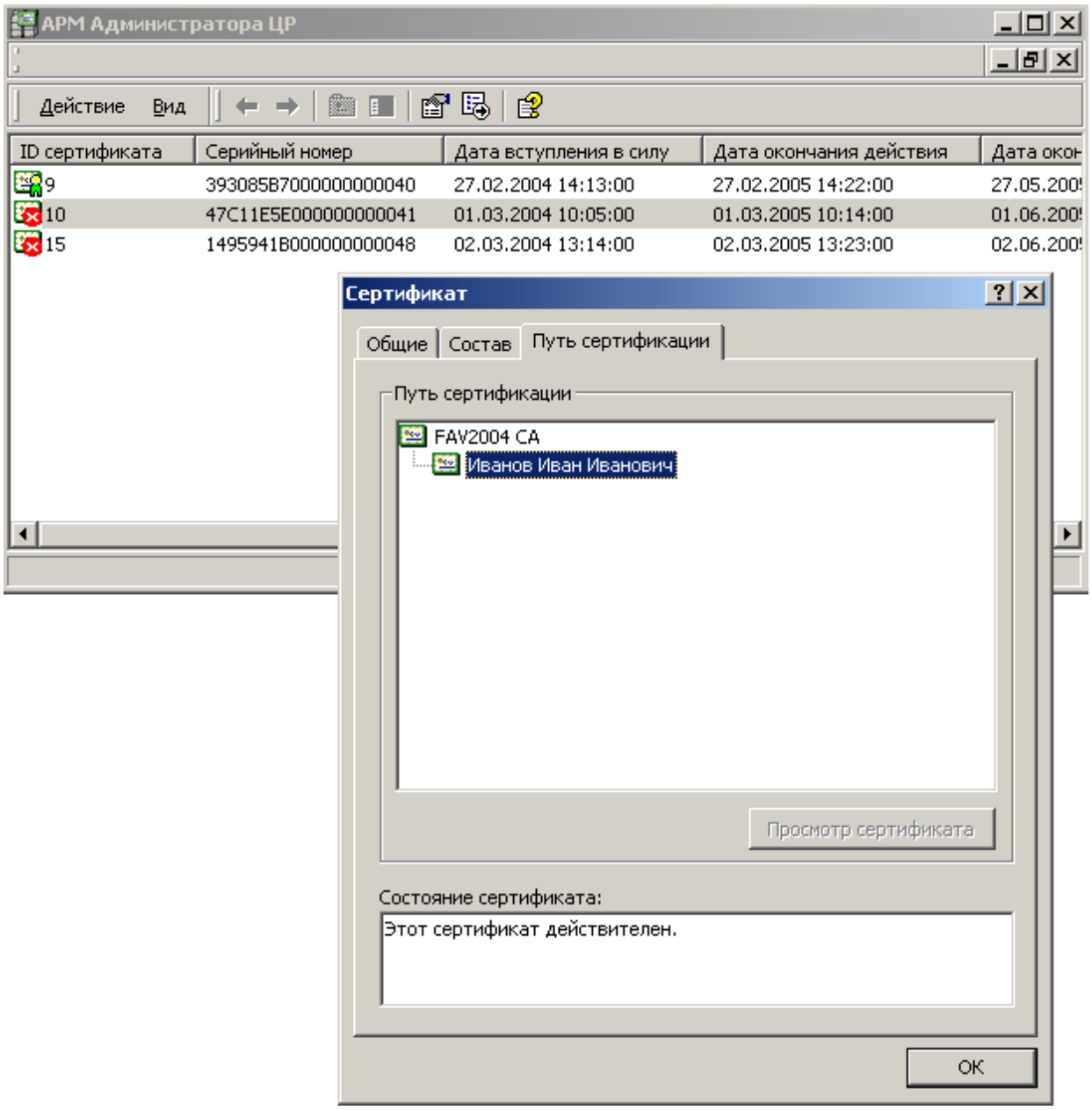
7. Нажмите кнопку **Закрыть**. Сертификат, действие которого было приостановлено, будет помечен как **не действительный** (красный круг с белым крестом внутри);

Рисунок 137. Окно просмотра сертификатов пользователя



Просмотр сертификатов ключей подписи в **АРМ Администратора ЦР** осуществляется стандартными средствами ОС Windows, поэтому сертификаты, действие которых было приостановлено, в стандартном окне просмотра сертификатов отображаются как действующие.

Рисунок 138. Просмотр сертификата пользователя, действие которого было приостановлено



1.6.2. Приостановление действия сертификата ключа подписи пользователя (запрос на приостановление действия сертификата ключа подписи формируется пользователем с использованием **АРМ пользователя с ключевым доступом**)

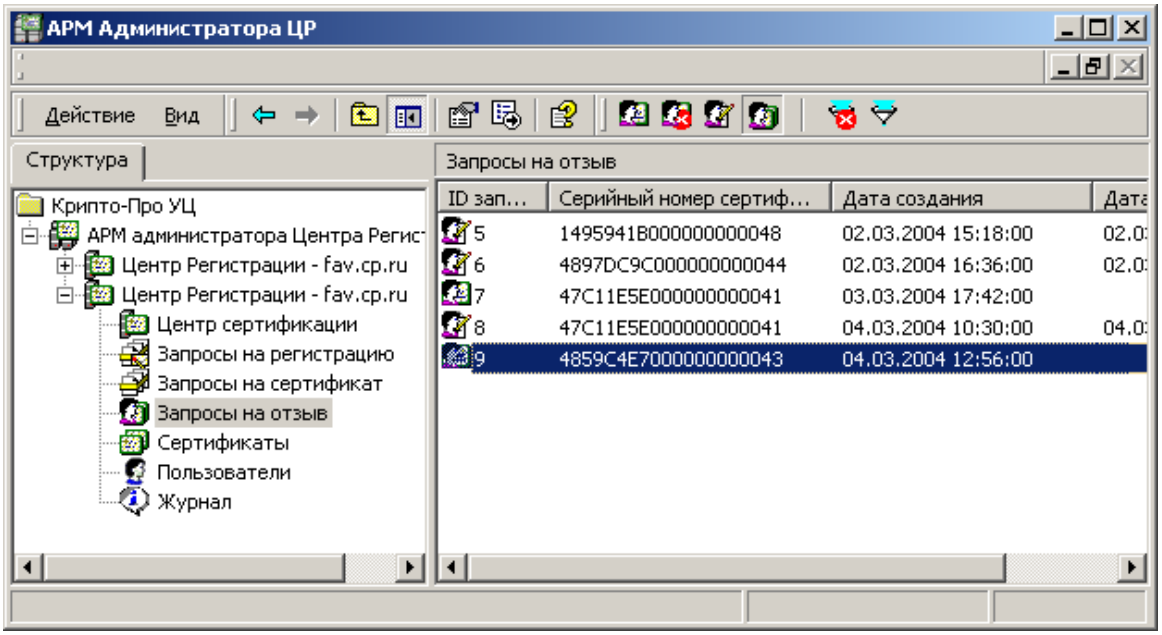
Описание процедуры приостановления действия сертификата ключа подписи пользователя при формировании запроса на приостановление действия сертификата с использованием **АРМ пользователя с ключевым доступом:**

1. Пользователь Удостоверяющего Центра, являющийся владельцем сертификата ключа подписи, с помощью **АРМ пользователя с ключевым доступом** формирует

запрос на приостановление действия сертификата ключа подписи, подписывает его электронной цифровой подписью и направляет в Удостоверяющий Центр;

2. После отправки пользователем запроса на приостановление действия сертификата в окне **АРМ администратора ЦР** в папке **Запросы на отзыв** появляется новый запрос, ожидающий обработки;

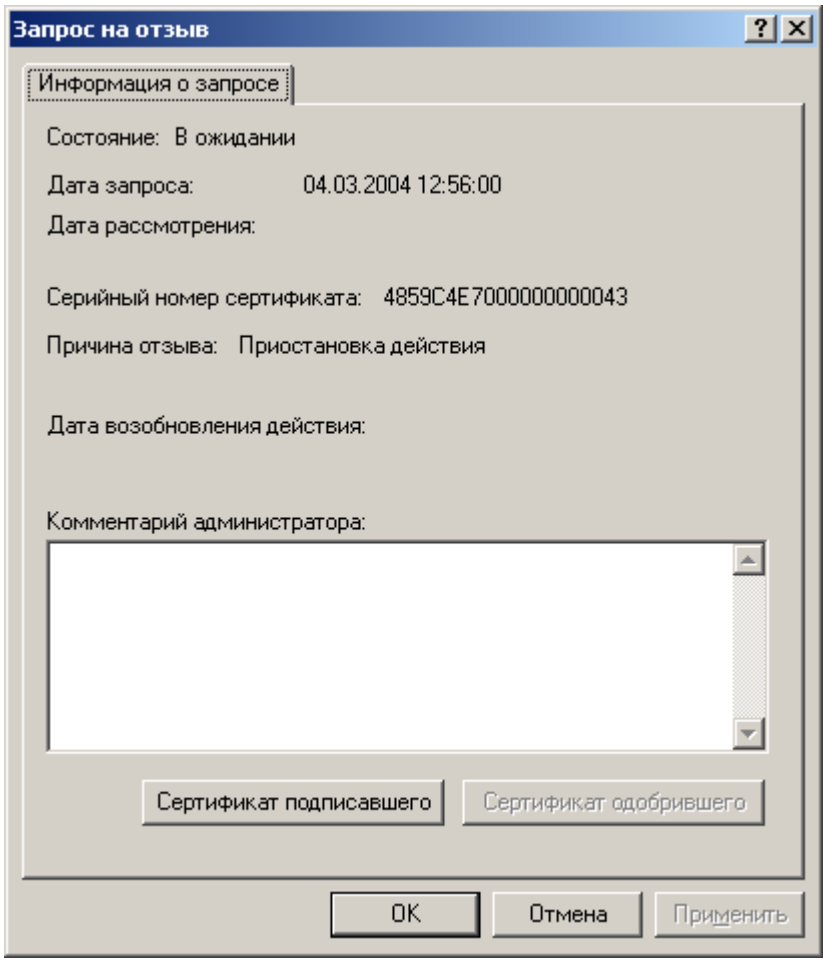
Рисунок 139. Окно просмотра запросов на приостановление действия сертификатов



Запросы на приостановление действия сертификата размещаются в папке **Запросы на отзыв.** Установление принадлежности запроса определенному классу (является ли запрос запросом на отзыв или запросом на приостановление действия сертификата) осуществляется в окне просмотра **Свойств** данного запроса.

3. Выделите правой кнопкой мыши поступивший запрос и в открывшемся контекстном меню выберите пункт **Свойства.** Откроется окно свойств запроса;

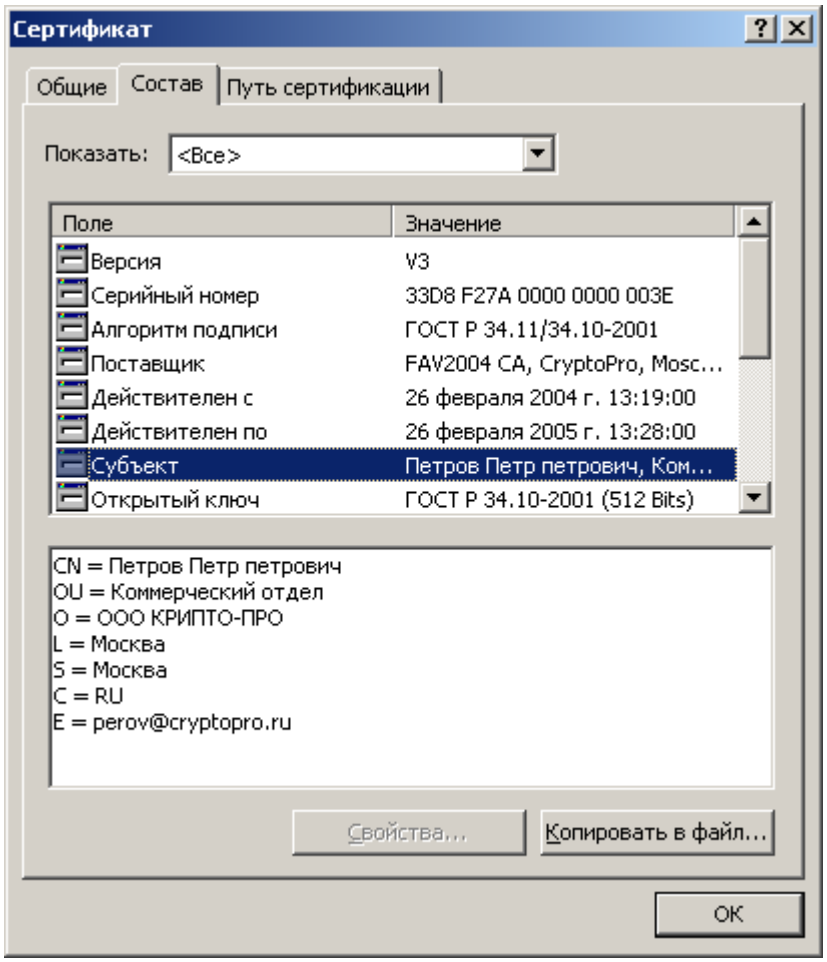
Рисунок 140. Окно просмотра свойств запроса на приостановление действия сертификата



Свойства запроса на приостановление действия сертификата отображаются в окне **Запрос на отзыв.** Наличие в поле **Причина отзыва** значения **Приостановка действия** свидетельствует о том, что указанный запрос является запросом на приостановление действия сертификата.

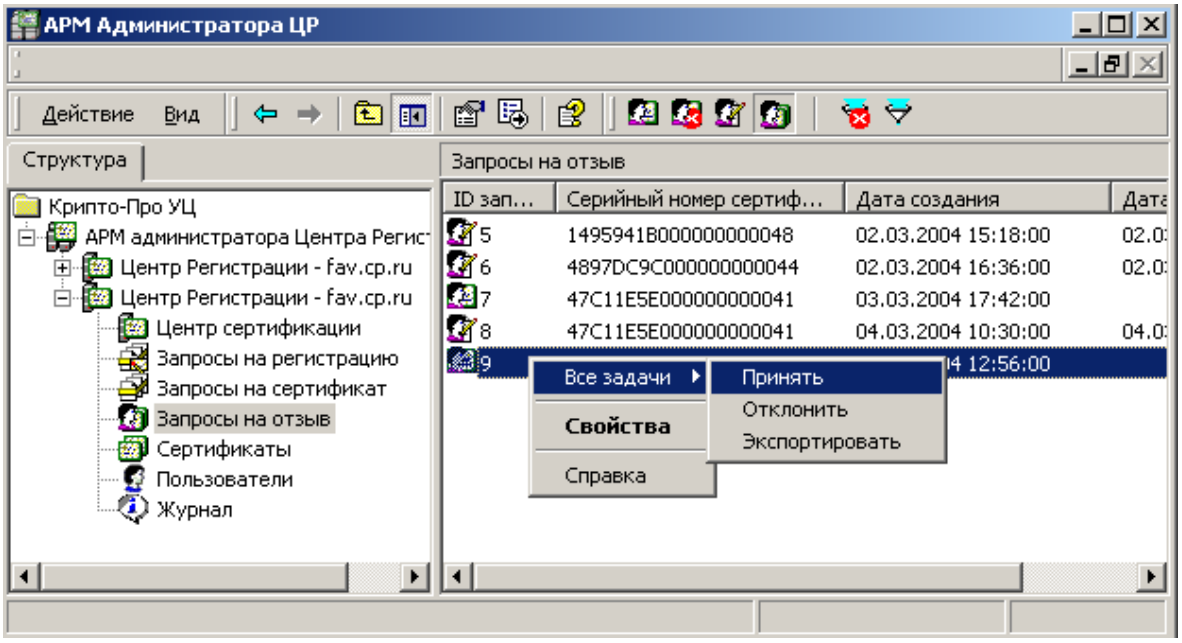
4. В открывшемся окне нажмите кнопку **Сертификат подписавшего**, осуществляющую просмотр сертификата зарегистрированного пользователя, направившего в Удостоверяющий Центр данный запрос;

Рисунок 141. Просмотр сертификата пользователя, отправившего запрос на приостановление действия сертификата



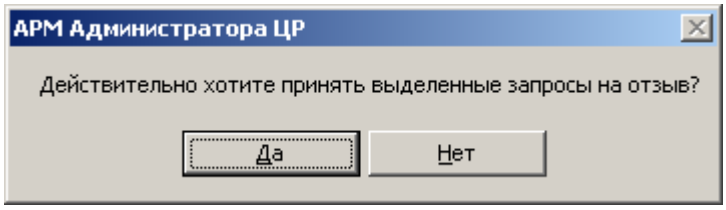
5. Убедитесь в том, что лицо, направившее запрос на приостановление действия сертификата – владелец сертификата, открывающегося при нажатии на кнопку **Сертификат подписавшего**, является владельцем сертификата ключа подписи, действие которого требуется приостановить. Затем в окне **АРМ Администратора ЦР** выделите правой кнопкой мыши данный запрос и в открывшемся контекстном меню выберите **Принять;**

Рисунок 142. Выбор пункта меню для принятия запроса на приостановление действия сертификата



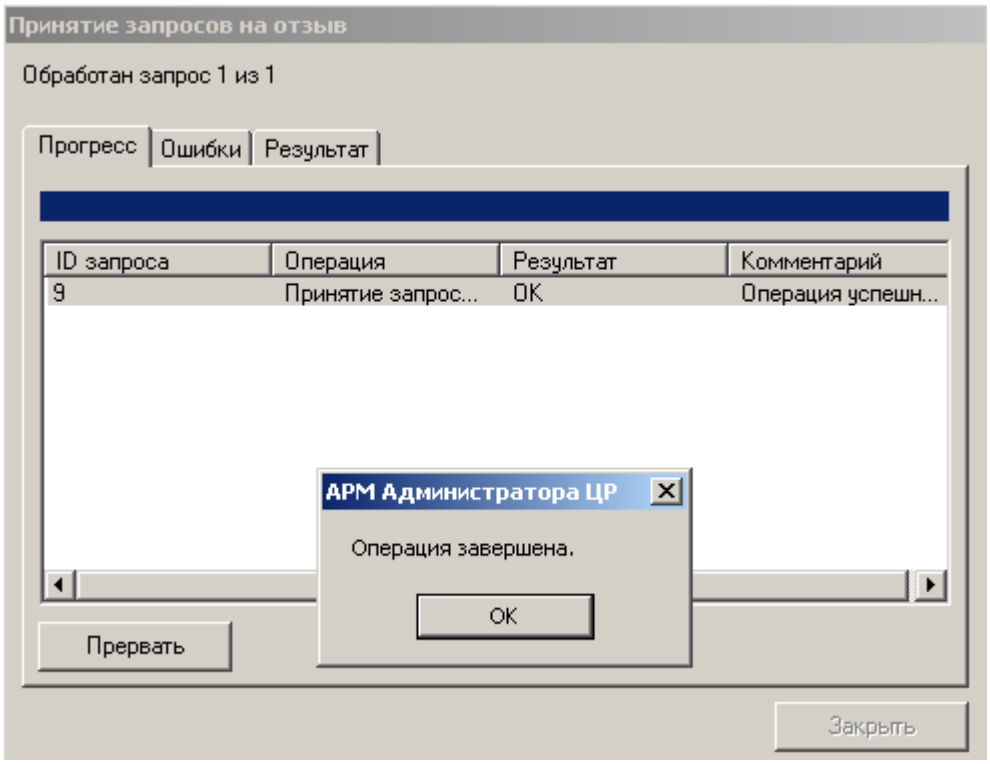
6. При принятии запроса на приостановление действия сертификата откроется предупреждающее окно, требующее подтверждения выбранных действий. Нажмите кнопку **Да;**

Рисунок 143. Окно подтверждения принятия запроса на приостановление действия сертификата



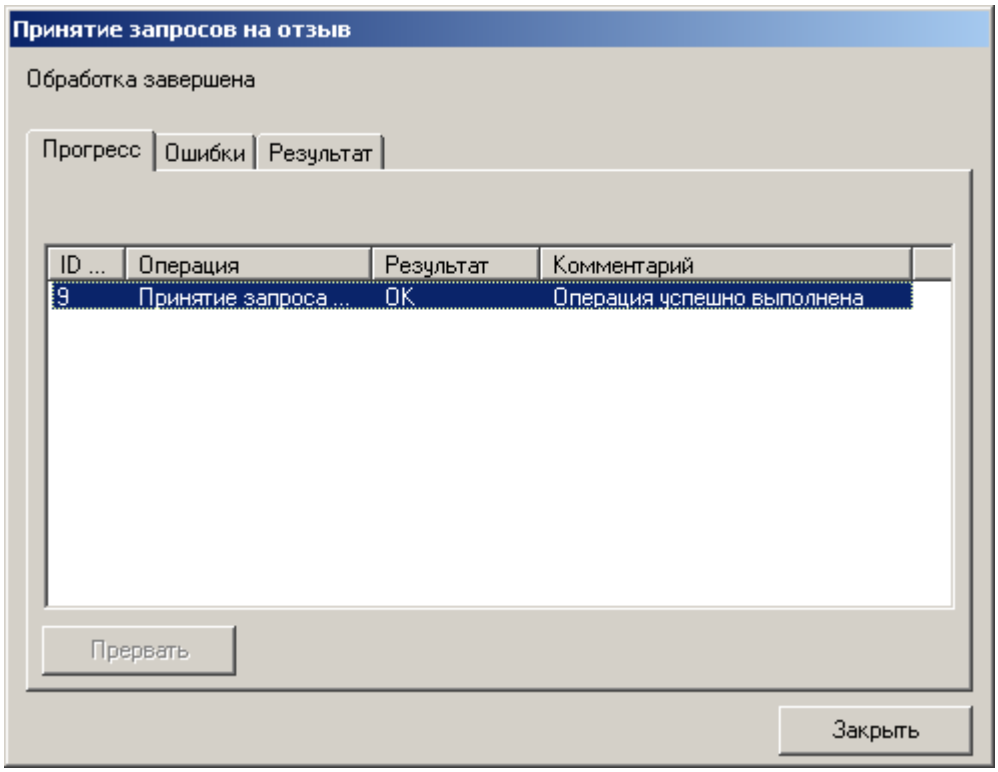
7. По окончании выполнения действий по приостановлению действия сертификата ключа подписи появится сообщение, информирующее об окончании указанных операций, и их результат;

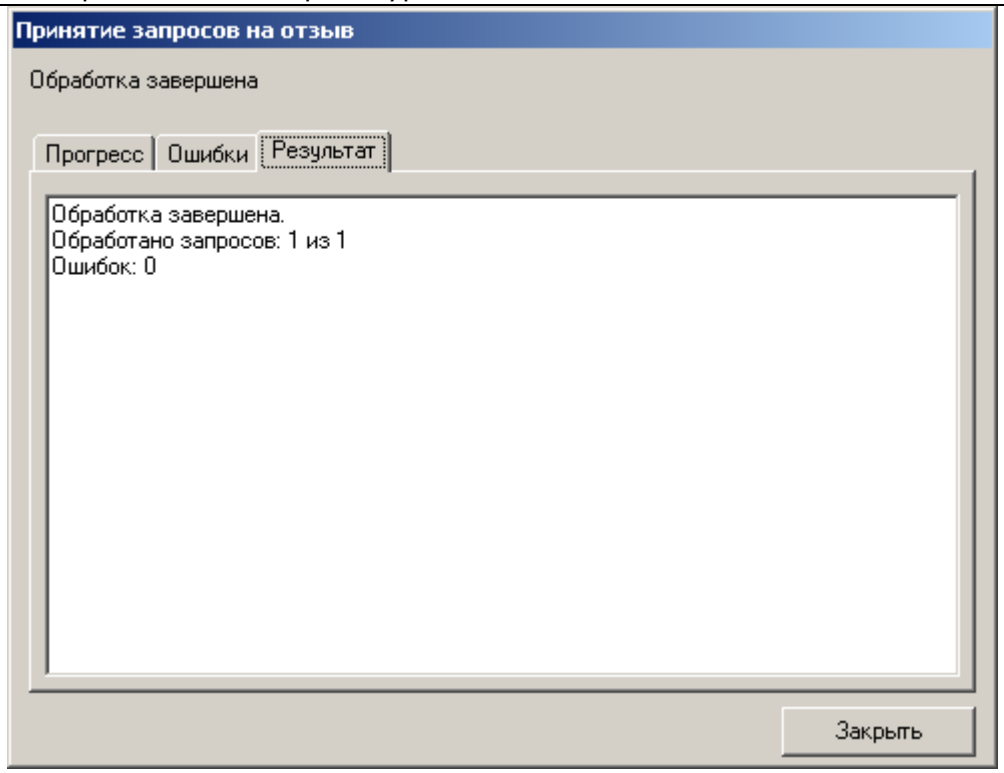
Рисунок 144. Окно просмотра результата приостановления действия сертификата



8. В окне **Операция завершена** нажмите кнопку **ОК** и убедитесь в том, что действия были выполнены без ошибок;

Рисунок 145. Окно просмотра ошибок, возникших при приостановлении действия сертификата

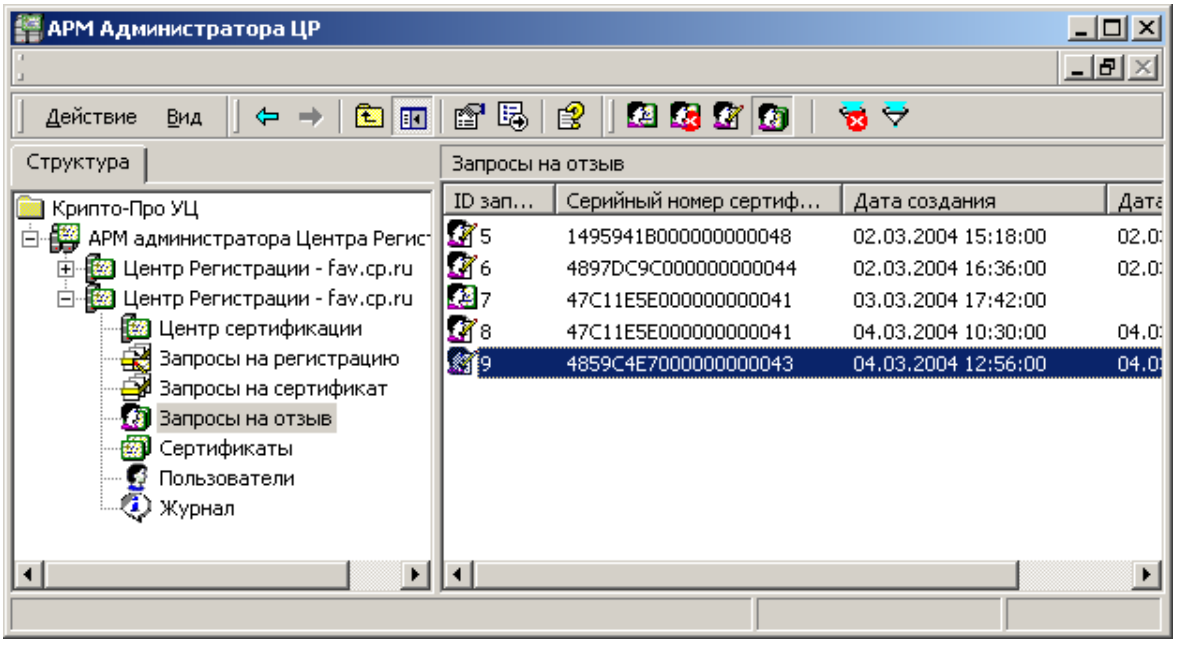




9. Нажмите кнопку **Закрыть.** Запрос на приостановление действия сертификата будет помечен как одобренный;

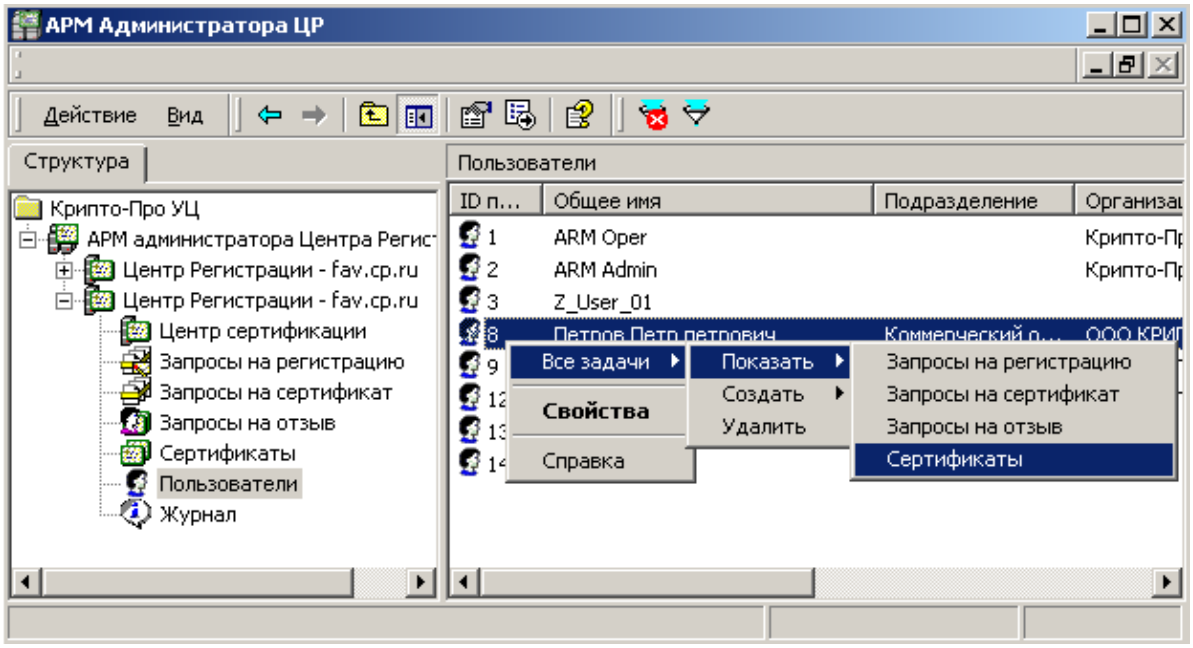
Окно **Принятие запросов на отзыв – Обработка завершена** применяется для просмотра результатов операций по принятию запросов, связанных как с отзывом, так и с приостановлением действия сертификата ключа подписи.

Рисунок 146. Окно просмотра запросов на приостановление действия сертификатов



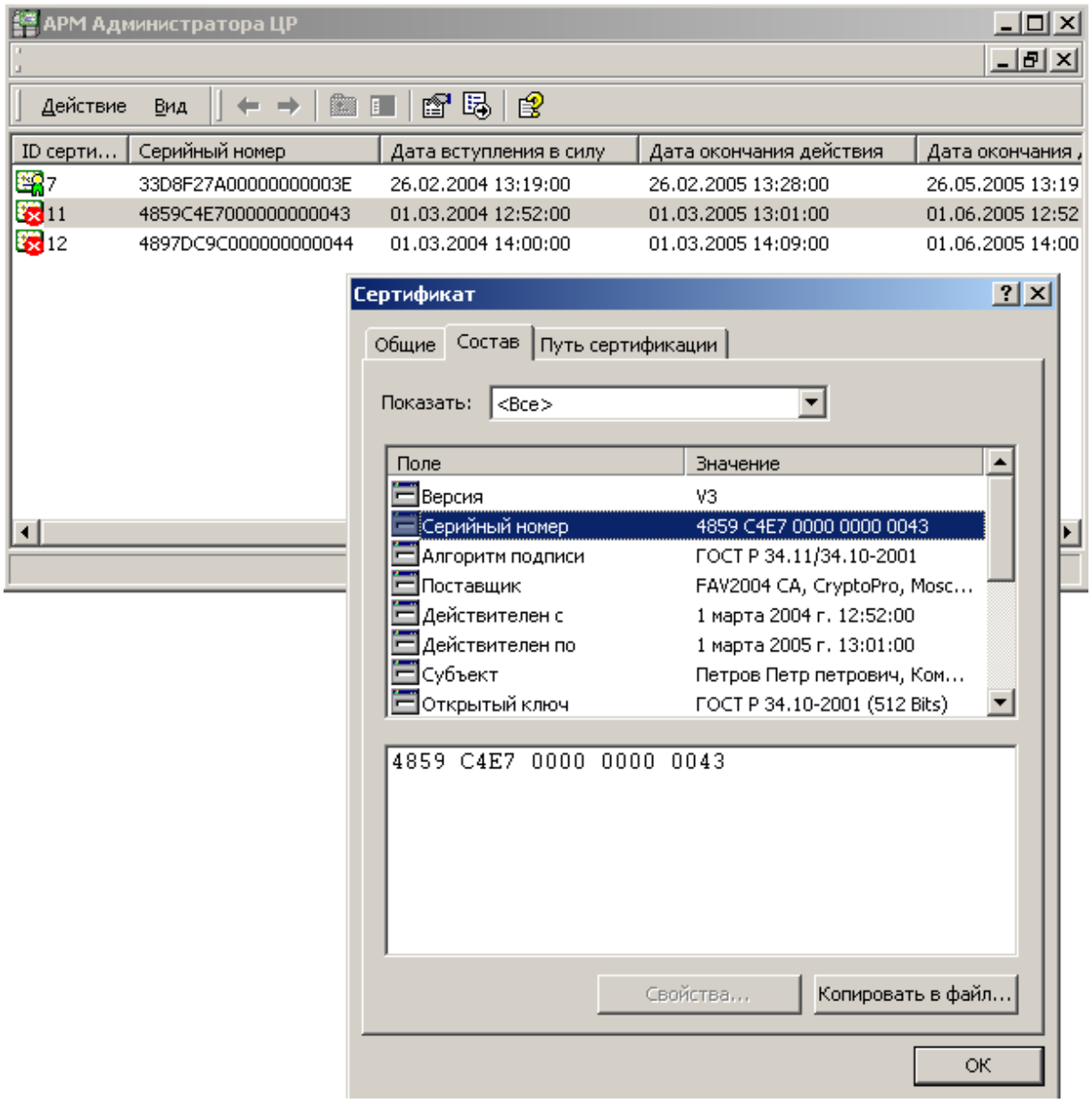
10. В левой части окна **АРМ администратора ЦР** выберите левой кнопкой мыши узел **Пользователи**. В правой части окна отобразится список зарегистрированных в Удостоверяющем Центре пользователей. Выделите правой кнопкой мыши учетную запись пользователя, действие сертификата которого было приостановлено, и в открывшемся контекстном меню выберите **Все задачи -> Показать -> Сертификаты;**

Рисунок 147. Выбор пункта меню для просмотра сертификатов зарегистрированного пользователя



11. Откроется список сертификатов выбранного пользователя, в котором сертификат, действие которого приостановлено, помечен как **не действительный** (красный круг с белым крестом внутри);

Рисунок 148. Просмотр сертификатов пользователя и сертификата, действие которого приостановлено

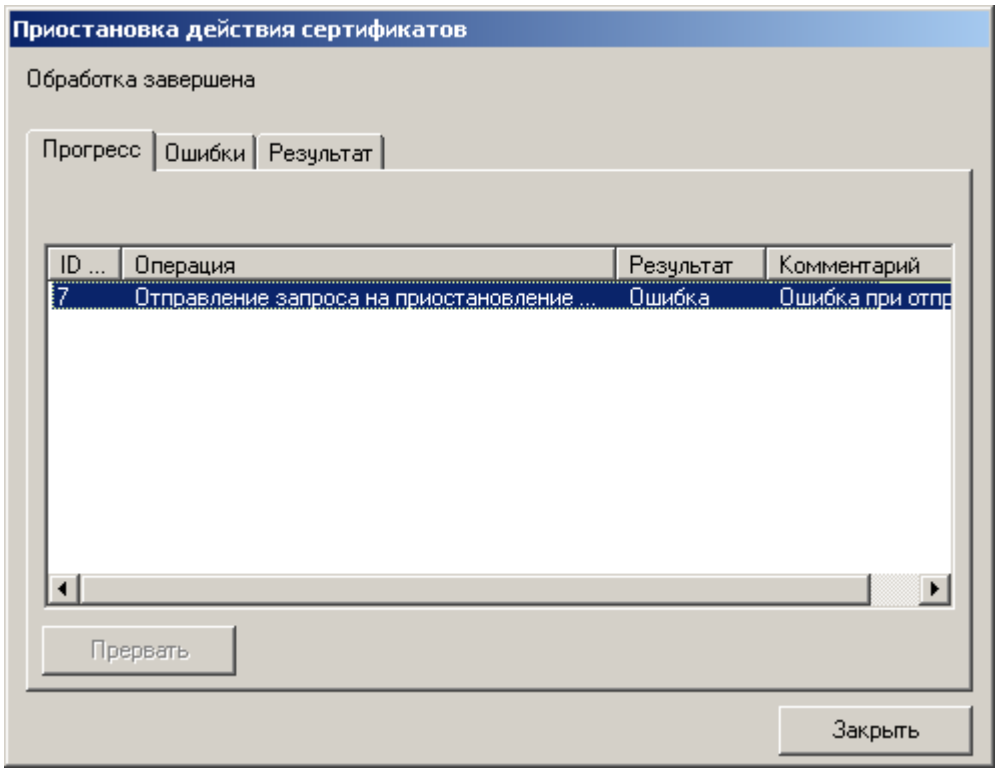


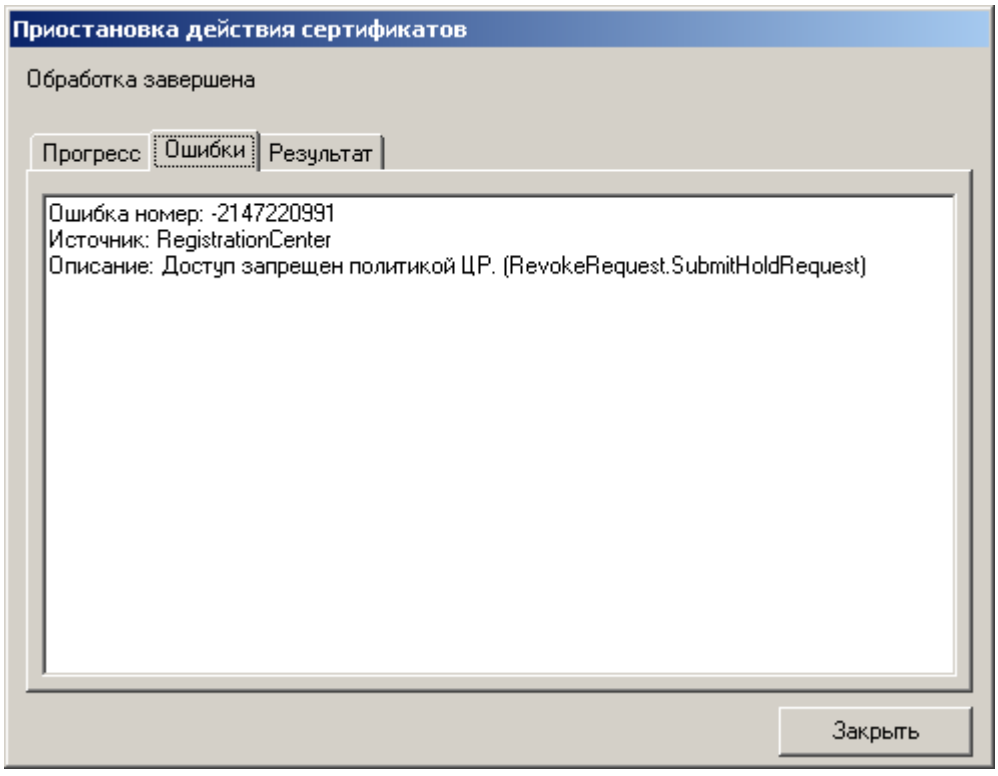
Просмотр сертификатов ключей подписи в **АРМ Администратора ЦР** осуществляется стандартными средствами ОС Windows, поэтому сертификаты, действие которых приостановлено в стандартном окне просмотра сертификатов отображаются как действующие.

1.6.3. Наиболее часто встречающиеся ошибки, возникающие при осуществлении действий по приостановлению действия сертификата

1. При приостановлении действия сертификата с **АРМ Администратора ЦР** привилегированным пользователем в окне **Приостановка действия сертификатов - Обработка завершена** возникает ошибка:

Рисунок 149. Ошибка при выполнении метода RevokeRequest.SubmitHoldRequest



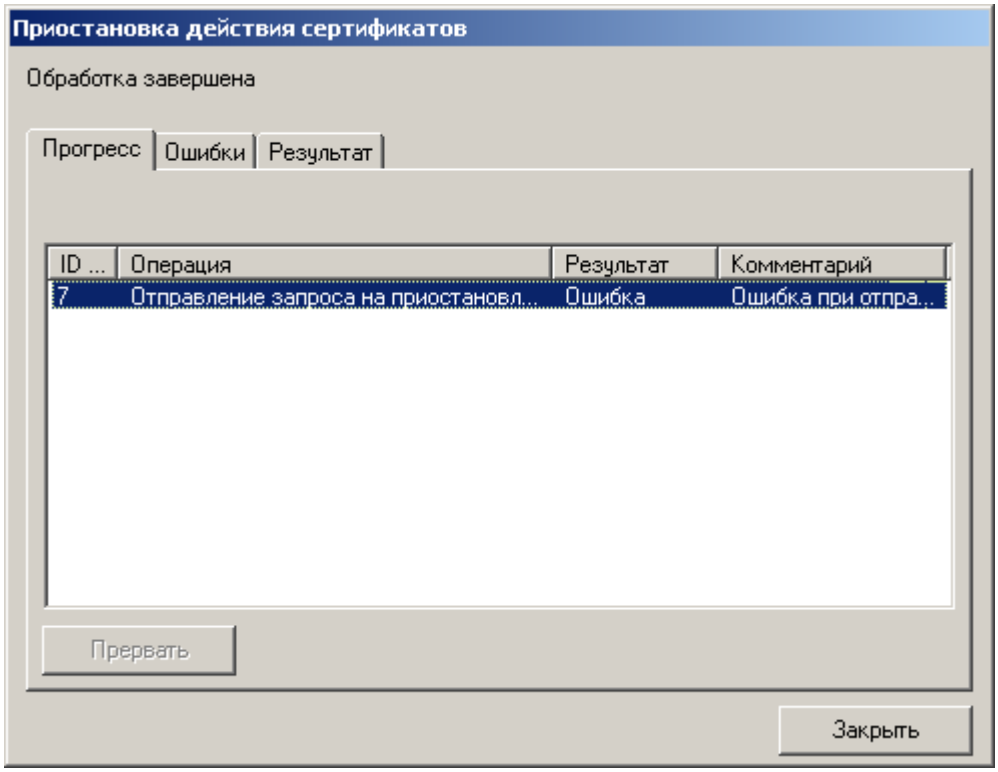


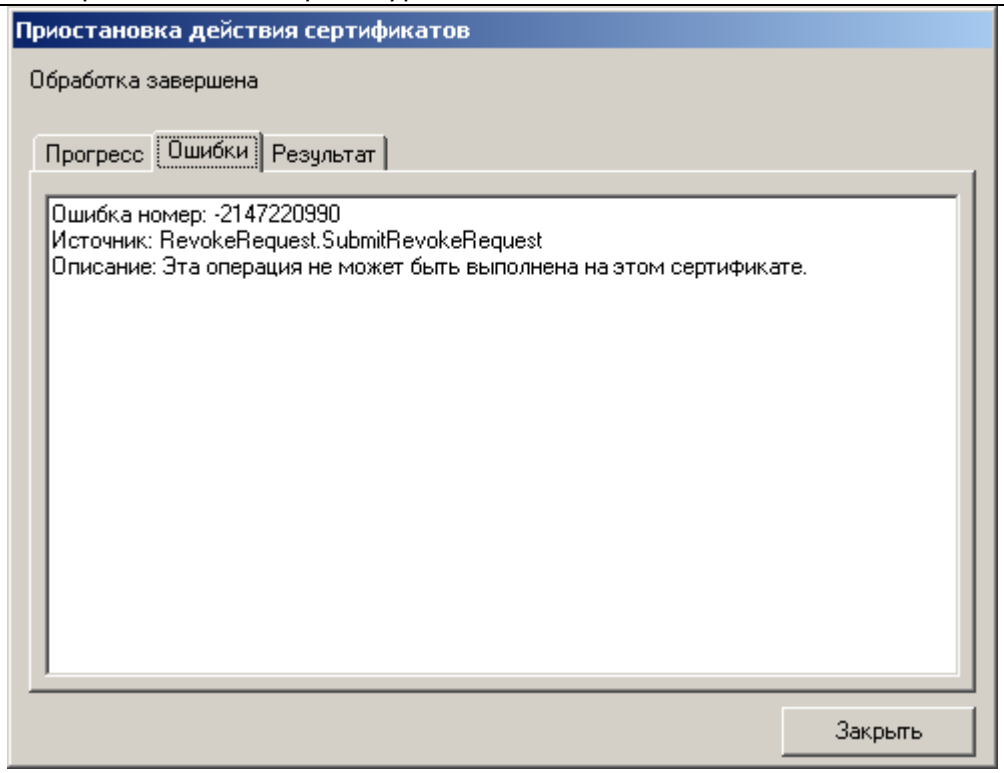
У привилегированного пользователя (**Оператора** или **Администратора**), производящего приостановление действия сертификата, недостаточно прав на выполнение метода **RevokeRequest.SubmitHoldRequest**.

На Центре Регистрации необходимо осуществить настройку политики безопасности, позволяющую осуществлять выполнение указанного метода.

2. При приостановлении действия сертификата с **АРМ Администратора ЦР** привилегированным пользователем в окне **Приостановка действия сертификатов - Обработка завершена** возникает ошибка:

Рисунок 150. Ошибка при выполнении метода RevokeRequest.SubmitHoldRequest – у привилегированного пользователя недостаточно прав



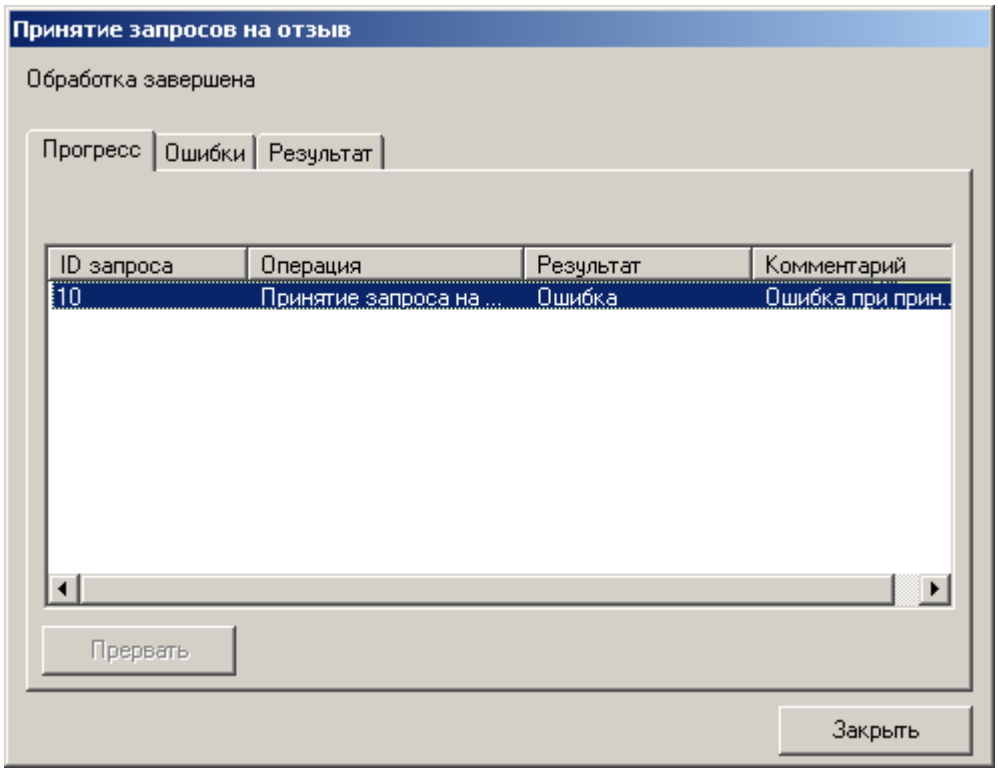


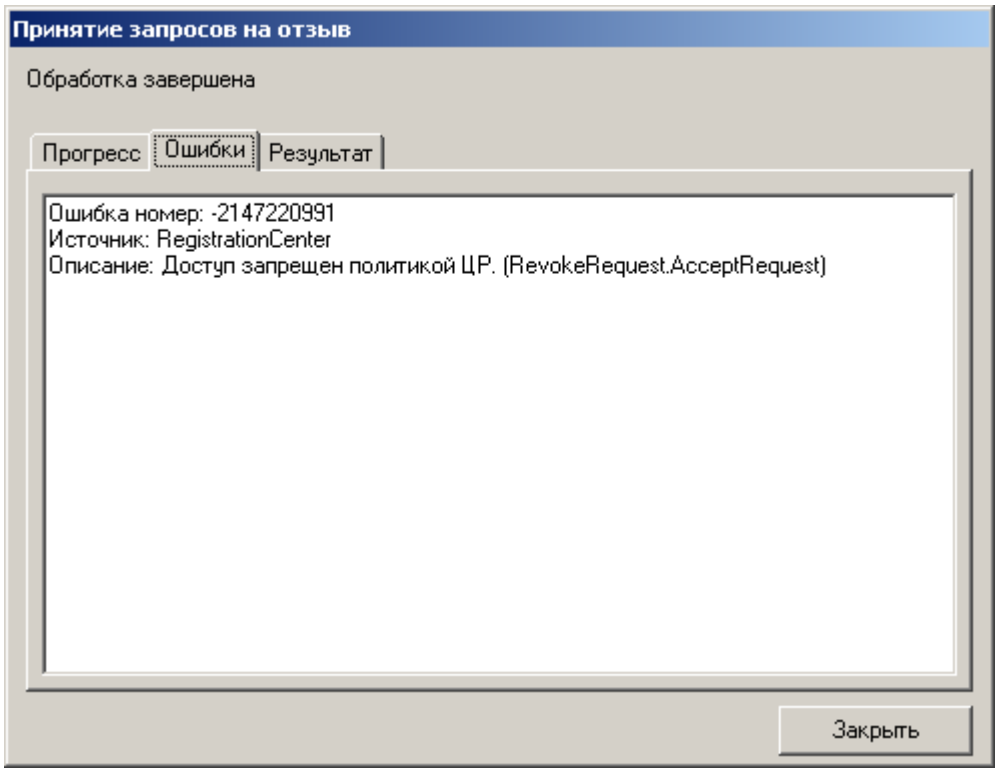
Сертификат, действие которого требуется приостановить, содержит хотя бы одну область использования (поле **Extended Key Usage**), присутствие которой в сертификате не позволяет привилегированному пользователю (**Оператору** или **Администратору**) приостановить действие указанного сертификата (данная область использования отсутствует в списке разрешенных для указанного привилегированного пользователя).

На Центре Регистрации осуществите настройку Политики обработки запросов на отзыв и для привилегированного пользователя, осуществляющего приостановление действия сертификатов, добавьте необходимые области использования сертификата.

3. При принятии существующего запроса на приостановление действия сертификата с **АРМ Администратора ЦР** привилегированным пользователем в окне **Принятие запроса на отзыв - Обработка завершена** возникает ошибка:

Рисунок 151. Ошибка при выполнении метода RevokeRequest.AcceptRequest





У привилегированного пользователя (**Оператора** или **Администратора**), производящего приостановление действия сертификата, недостаточно прав на выполнение метода **RevokeRequest.AcceptRequest**.

На Центре Регистрации необходимо осуществить настройку политики безопасности, позволяющую осуществлять выполнение указанного метода.

1.7. Возобновление действия сертификата ключа подписи пользователя

Возобновление действия сертификата ключа подписи осуществляется на основании запроса на возобновление действия сертификата ключа подписи. Запрос на возобновление действия сертификата ключа подписи может быть сформирован **Администратором** на **АРМ Администратора ЦР** (централизованный режим - в данном случае основанием для формирования запроса является Заявление на возобновление действия сертификата, направленное пользователем в бумажном виде в Удостоверяющий Центр), либо пользователем на своем рабочем месте с использованием **АРМ пользователя с ключевым доступом** (распределенный режим – запрос на возобновление действия сертификата подписывается на действующем закрытом ключе пользователя и рассматривается Удостоверяющим Центром, как Заявление на возобновление действия сертификата ключа подписи - пользователь должен быть владельцем как минимум одного действующего сертификата ключа подписи).

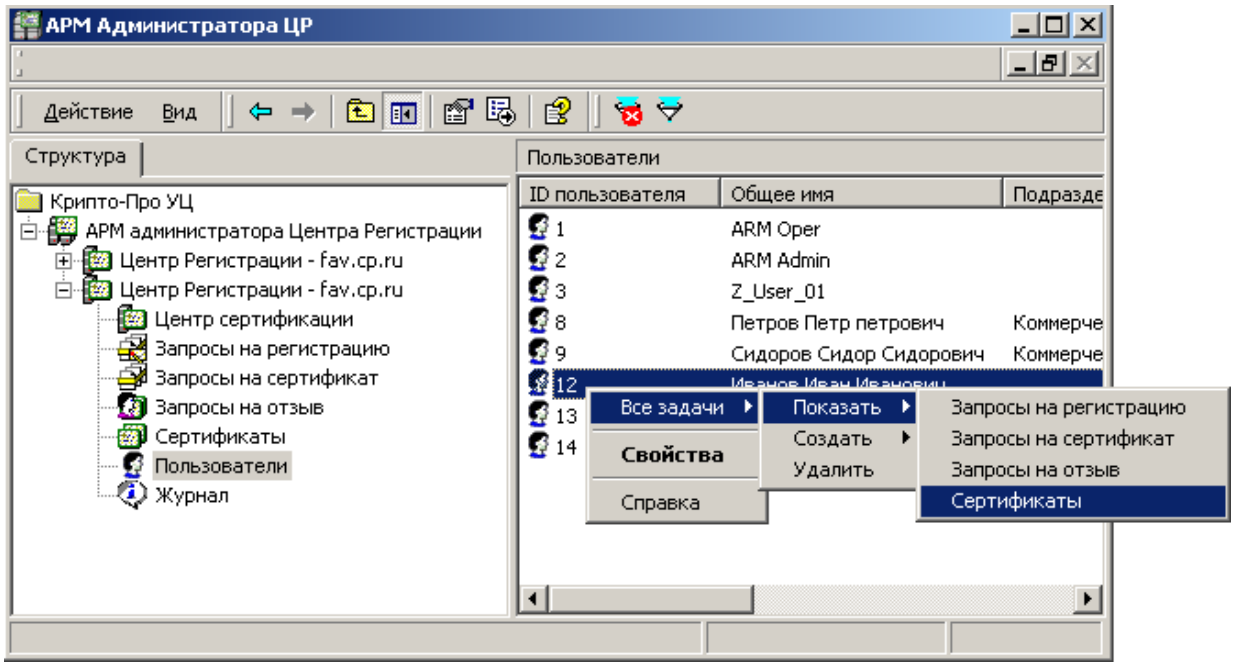

Возобновление действия сертификата может быть осуществлено исключительно в течение срока, на который действия сертификата было приостановлено.

1.7.1. Возобновление действия сертификата ключа подписи пользователя (запрос на возобновление действия сертификата ключа подписи формируется на **АРМ Администратора ЦР**)

Описание процедуры возобновления действия сертификата ключа подписи пользователя при формировании запроса на возобновление действия сертификата на **АРМ Администратора ЦР:**

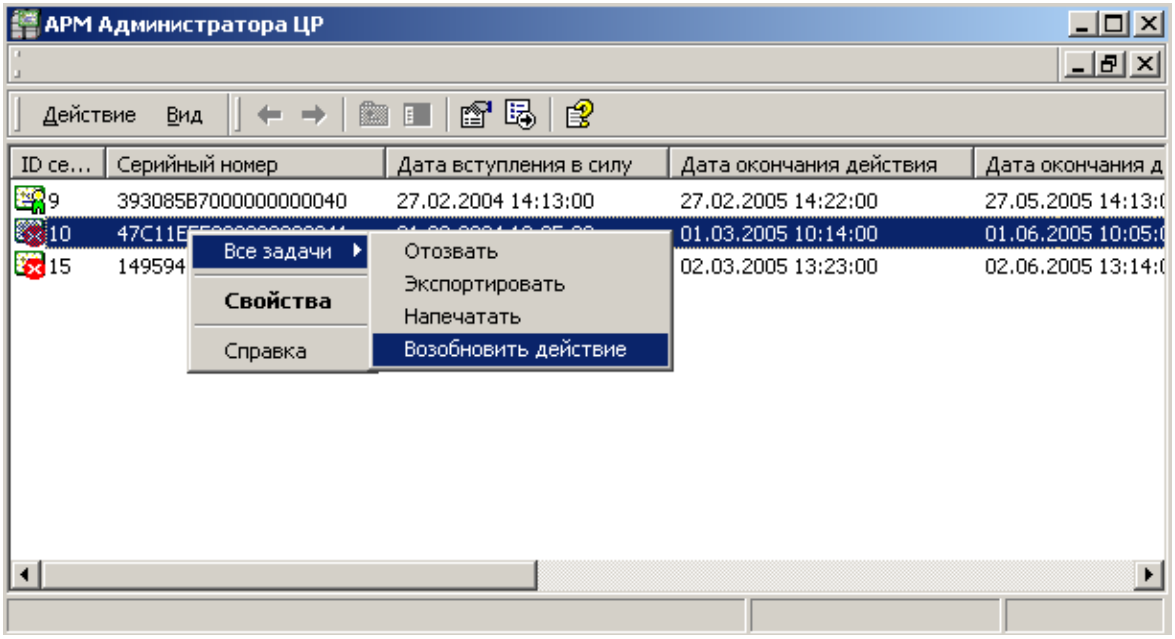
1. В окне **АРМ Администратора ЦР** выделите правой кнопкой мыши учетную запись пользователя, действие сертификата ключа подписи которого требуется возобновить, в открывшемся контекстном меню выберите **Все задачи -> Показать -> Сертификаты;**

Рисунок 152. Выбор пункта меню для просмотра сертификатов зарегистрированного пользователя



2. Выделите правой кнопкой мыши сертификат ключа подписи, действие которого необходимо возобновить, и в контекстном меню выберите **Все задачи -> Возобновить действие;**

Рисунок 153. Выбор пункта меню для возобновления действия сертификата



В Заявлении на возобновление действия сертификата ключа подписи, подаваемом в Удостоверяющий Центр в бумажном виде, должны быть указаны следующие сведения:

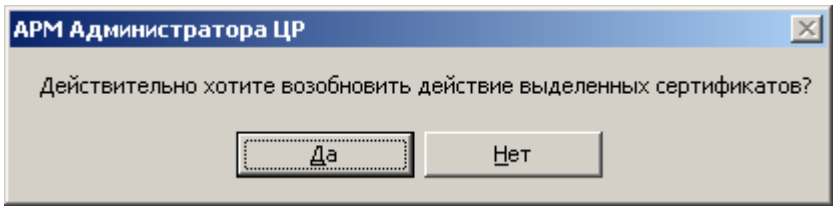
- Серийный номер сертификата, действие которого требуется возобновить;

- Идентификационные данные пользователя – владельца данного сертификата.

Именно на основании приведенных в Заявлении данных **Администратор** осуществляет возобновление действия сертификата ключа подписи.

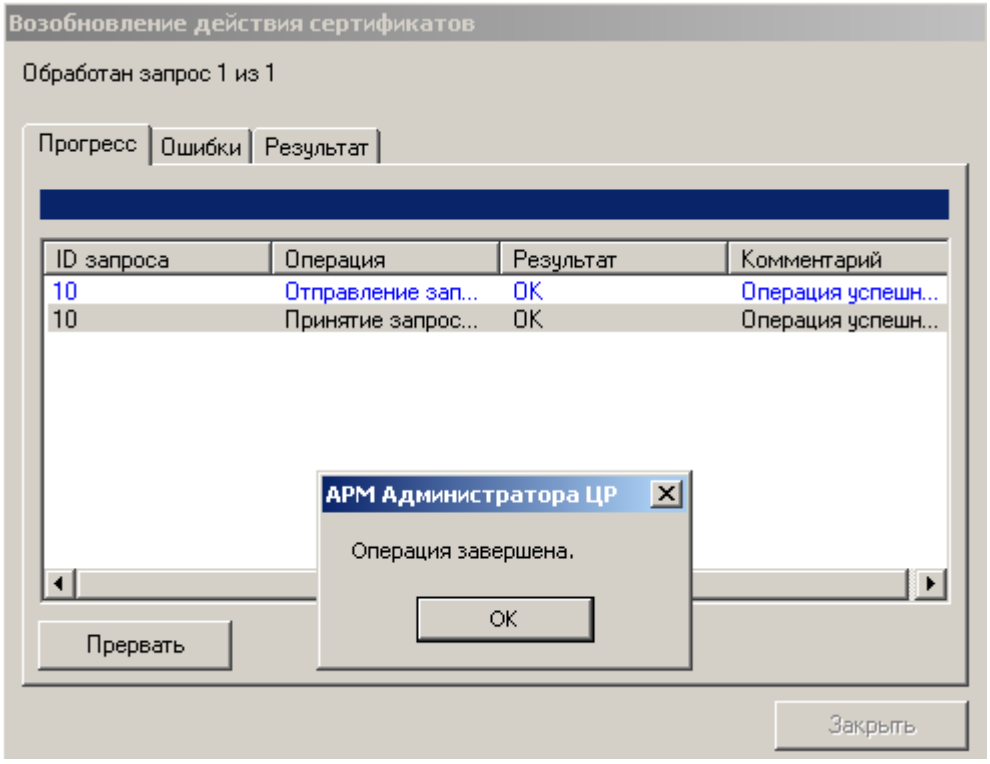
3. Откроется предупреждающее окно, требующее подтверждения возобновления действия сертификата. Нажмите кнопку **Да**;

Рисунок 154. Окно подтверждения возобновления действия сертификата



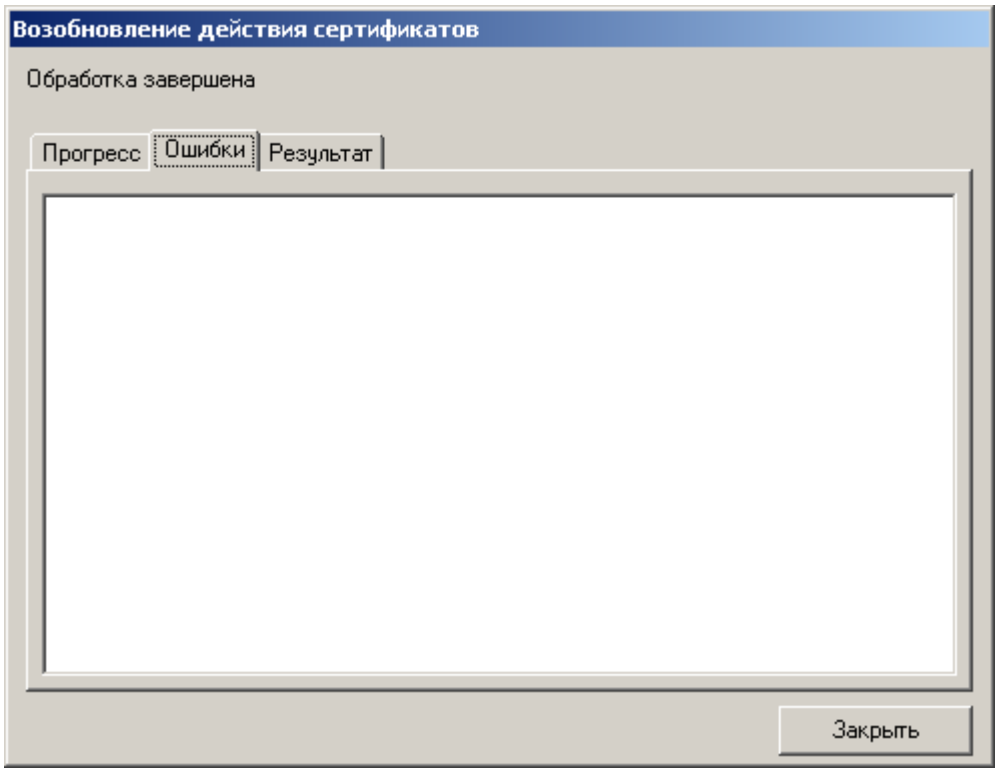
4. По окончании выполнения действий по возобновлению действия сертификата ключа подписи появится сообщение, информирующее об окончании указанных операций, и их результат;

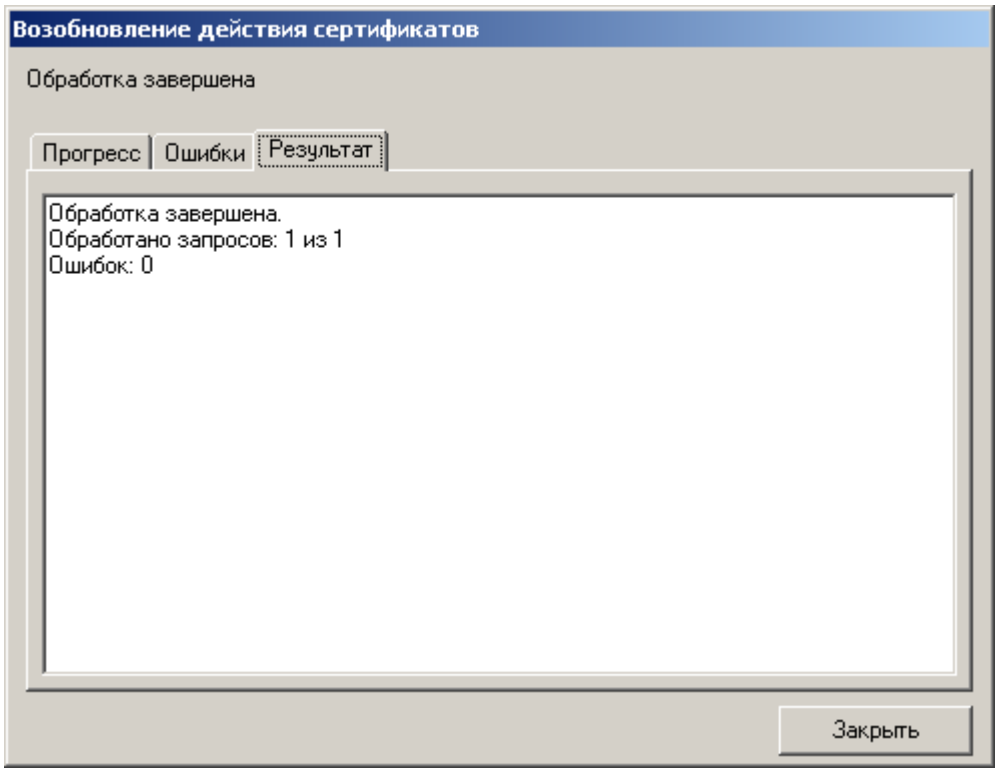
Рисунок 155. Окно просмотра результата возобновления действия сертификата



5. В окне **Операция завершена** нажмите кнопку **ОК** и убедитесь в том, что действия были выполнены без ошибок;

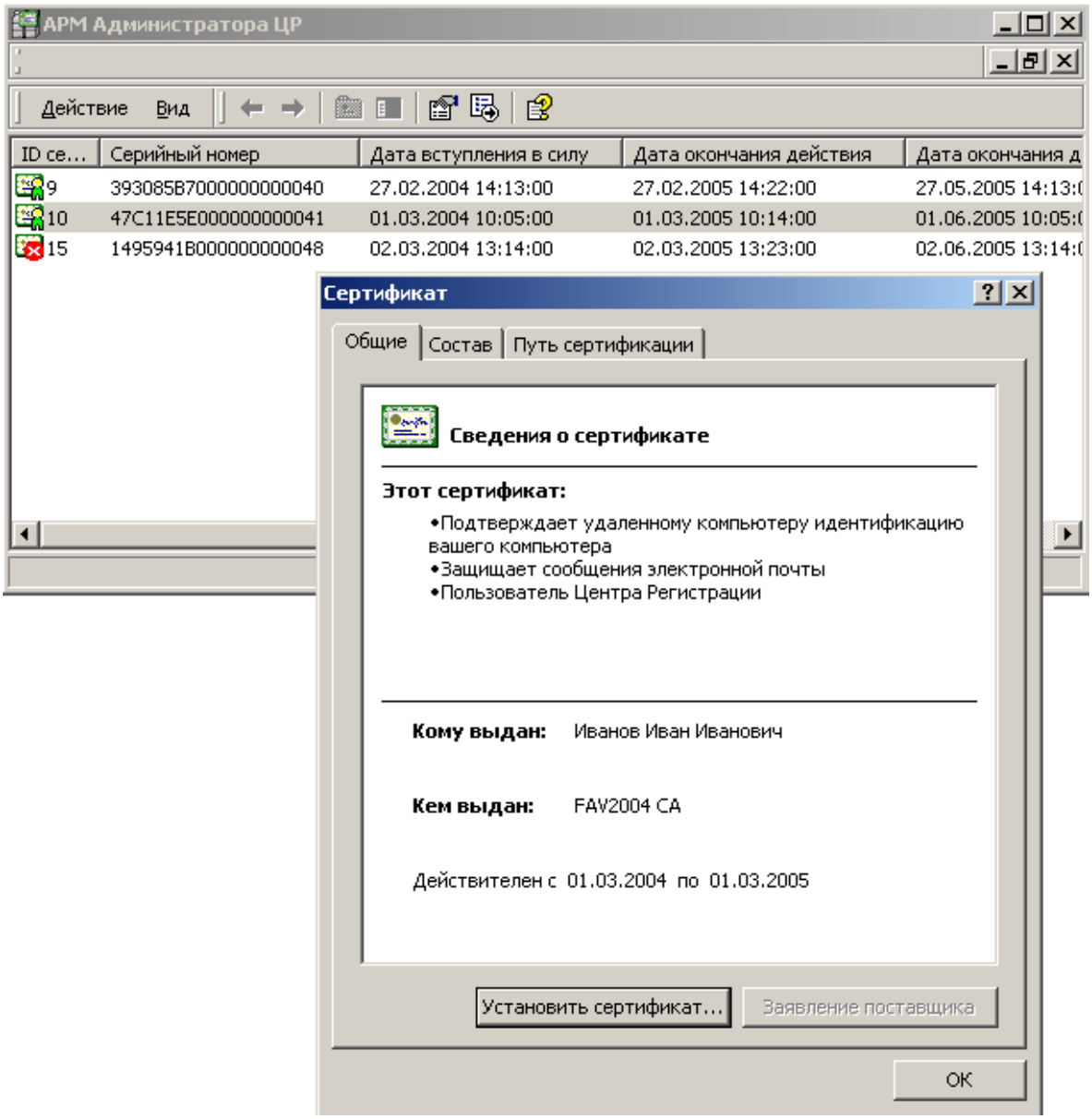
Рисунок 156. Окно просмотра ошибок, возникших при возобновлении действия сертификата





6. Нажмите кнопку **Закрыть**. Сертификат, действие которого было возобновлено, будет помечен как **действительный** (печать на сертификате).

Рисунок 157. Окно просмотра сертификатов пользователя и сертификата, действие которого было возобновлено



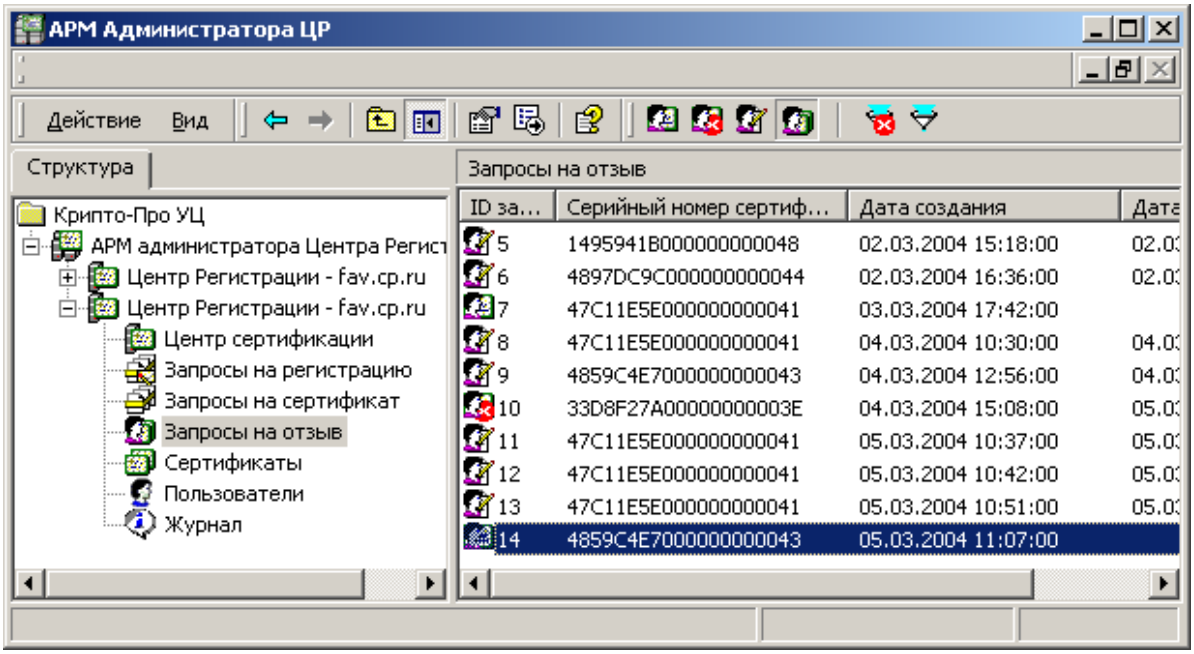
1.7.2. Возобновление действия сертификата ключа подписи пользователя (запрос на возобновление действия сертификата ключа подписи формируется пользователем с использованием **АРМ пользователя с ключевым доступом**)

Описание процедуры возобновления действия сертификата ключа подписи пользователя при формировании запроса на возобновление действия сертификата с использованием **АРМ пользователя с ключевым доступом:**

1. Пользователь Удостоверяющего Центра, являющийся владельцем действующего сертификата ключа подписи, с помощью **АРМ пользователя с ключевым доступом** формирует запрос на возобновление действия сертификата ключа подписи, подписывает его электронной цифровой подписью и направляет в Удостоверяющий Центр;

2. После отправки пользователем запроса на возобновление действия сертификата в окне **АРМ администратора ЦР** в папке **Запросы на отзыв** появляется новый запрос, ожидающий обработки;

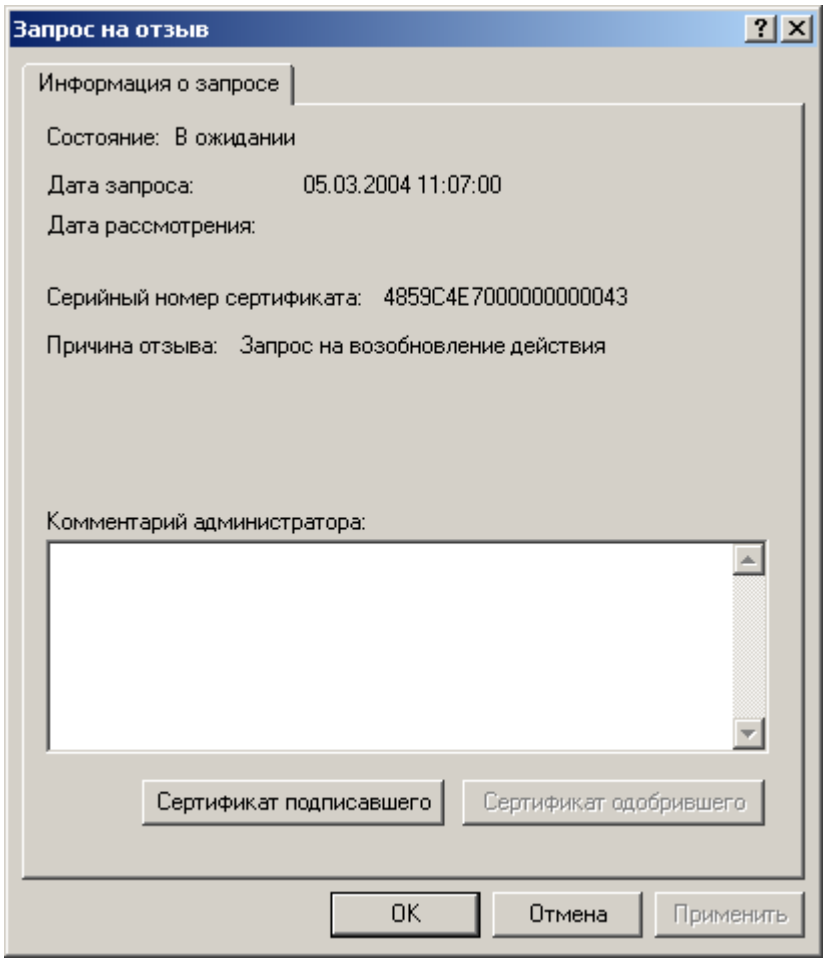
Рисунок 158. Окно просмотра запросов на возобновление действия сертификата пользователя



Запросы на возобновление действия сертификата размещаются в папке **Запросы на отзыв.** Установление принадлежности запроса определенному классу (является ли запрос запросом на отзыв, запросом на приостановление действия сертификата или запросом на возобновление действия сертификата) осуществляется в окне просмотра **Свойств** данного запроса.

3. Выделите правой кнопкой мыши поступивший запрос и в открывшемся контекстном меню выберите пункт **Свойства.** Откроется окно свойств запроса;

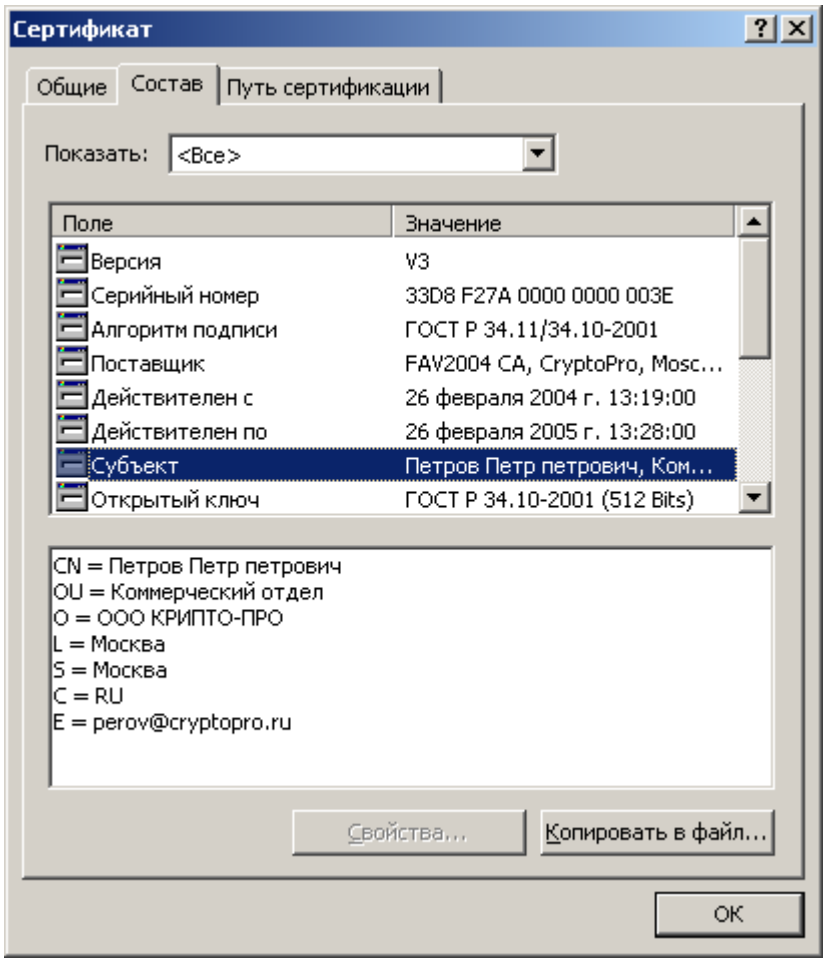
Рисунок 159. Окно просмотра свойств запроса на возобновление действия сертификата



Свойства запроса на возобновление действия сертификата отображаются в окне **Запрос на отзыв.** Наличие в поле **Причина отзыва** значения **Запрос на возобновление действия** свидетельствует о том, что указанный запрос является запросом на возобновление действия сертификата.

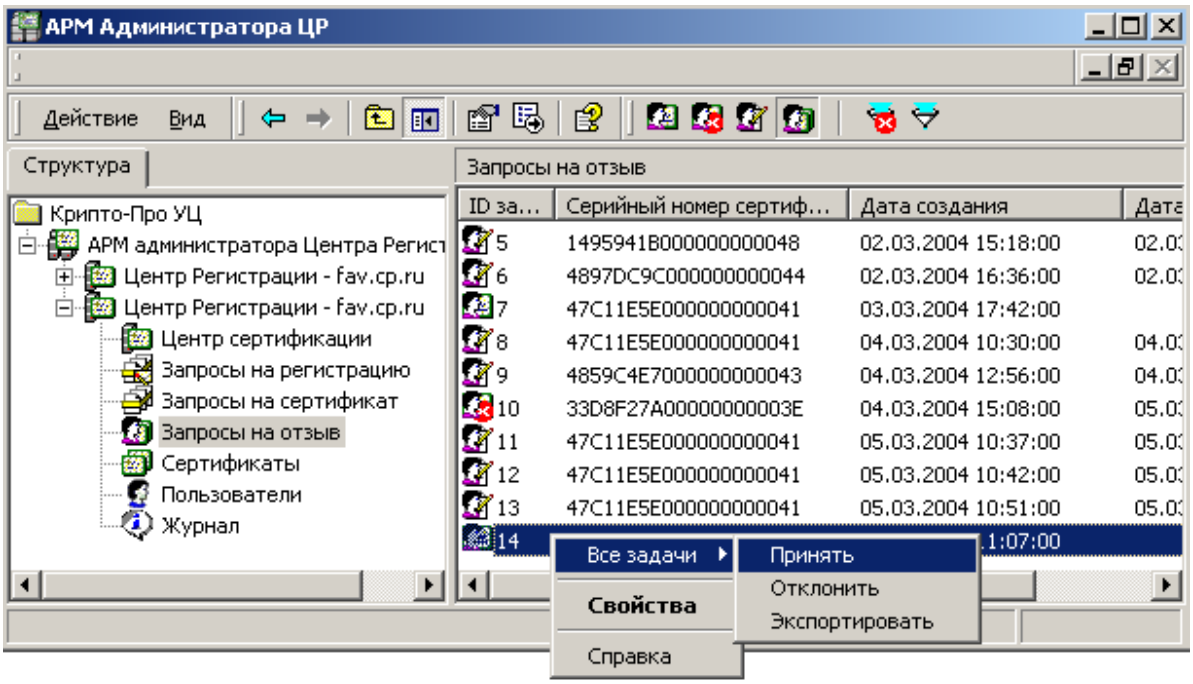
4. В открывшемся окне нажмите кнопку **Сертификат подписавшего**, осуществляющую просмотр сертификата зарегистрированного пользователя, направившего в Удостоверяющий Центр данный запрос;

Рисунок 160. Просмотр сертификата пользователя, направившего запрос на возобновление действия сертификата



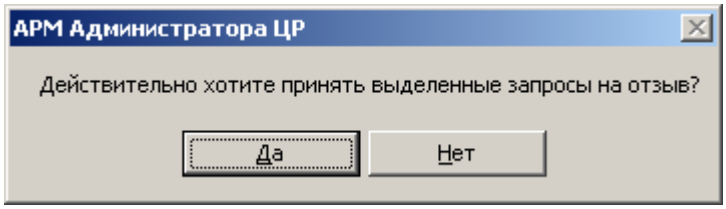
5. Убедитесь в том, что лицо, направившее запрос на возобновление действия сертификата – владелец сертификата, открывающегося при нажатии на кнопку **Сертификат подписавшего**, является владельцем сертификата ключа подписи, действие которого требуется возобновить. Затем в окне **АРМ Администратора ЦР** выделите правой кнопкой мыши данный запрос и в открывшемся контекстном меню выберите **Принять;**

Рисунок 161. Выбор пункта меню для принятия запроса на возобновление действия сертификата



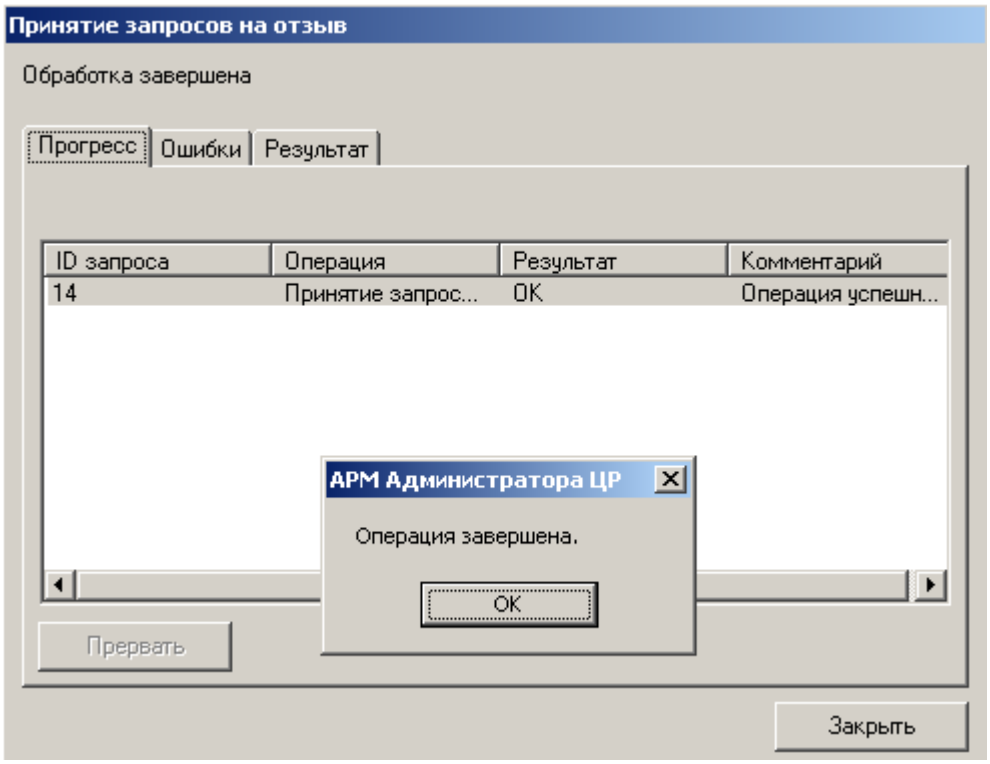
6. При принятии запроса на возобновление действия сертификата откроется предупреждающее окно, требующее подтверждения выбранных действий. Нажмите кнопку **Да;**

Рисунок 162. Окно подтверждения принятия запроса на возобновление действия сертификата



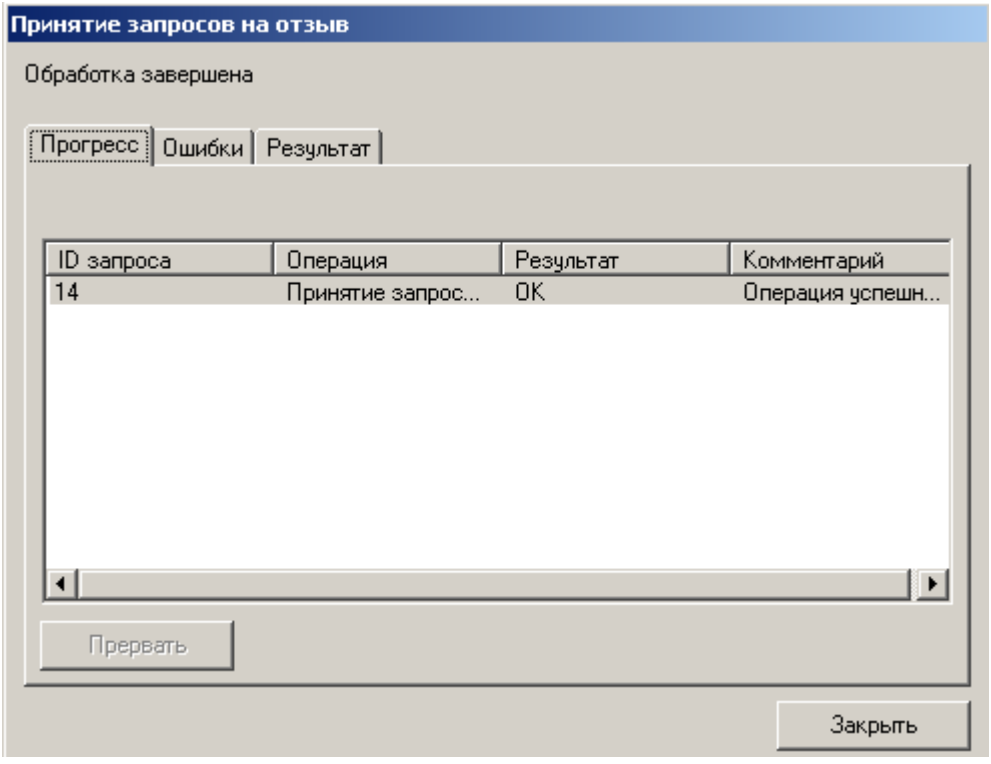
7. По окончании выполнения действий по возобновлению действия сертификата ключа подписи появится сообщение, информирующее об окончании указанных операций, и их результат;

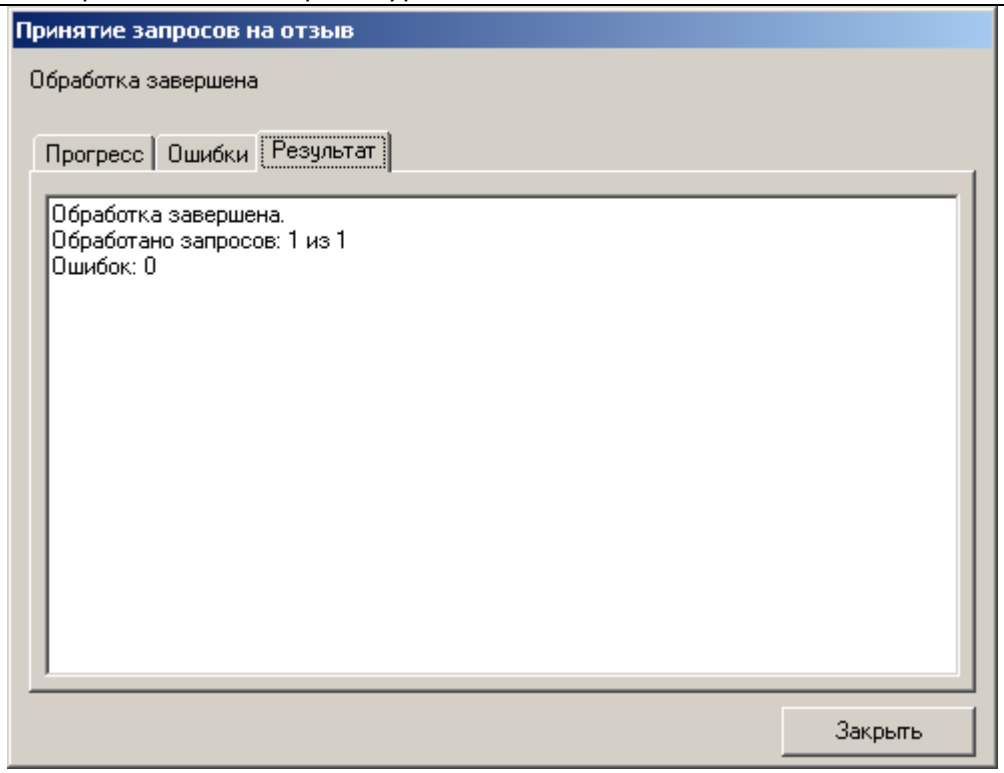
Рисунок 163. Окно просмотра результата возобновления действия сертификата



8. В окне **Операция завершена** нажмите кнопку **ОК** и убедитесь в том, что действия были выполнены без ошибок;

Рисунок 164. Окно просмотра ошибок, возникших при возобновлении действия сертификата

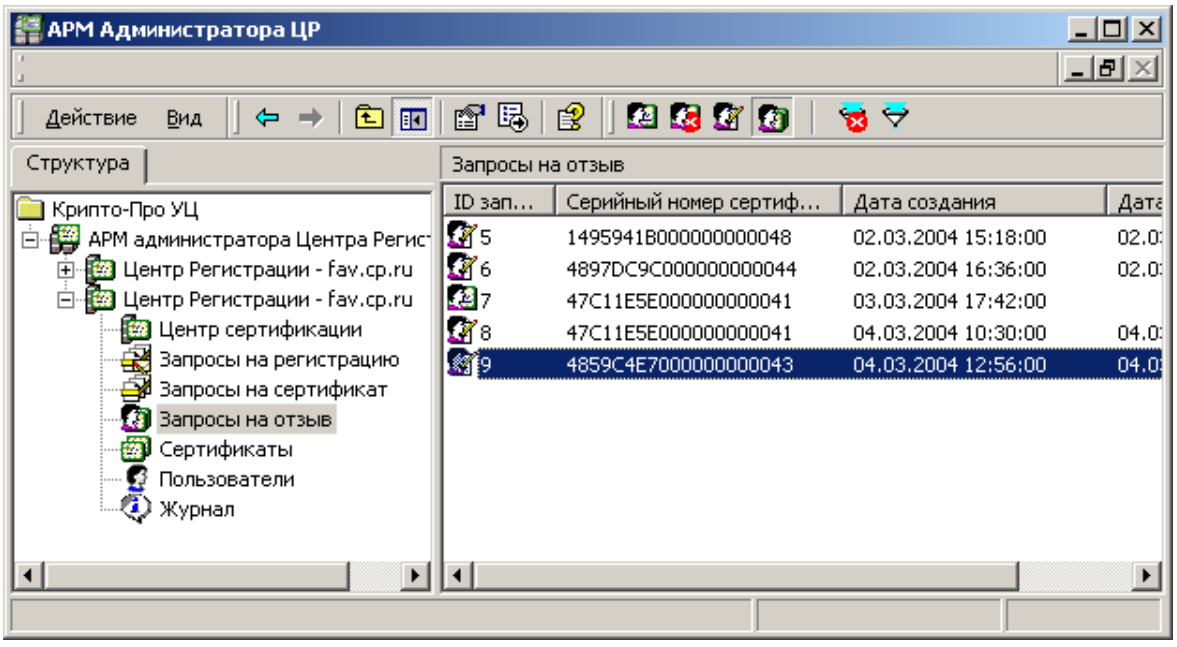




9. Нажмите кнопку **Закрыть.** Запрос на возобновление действия сертификата будет помечен как одобренный;

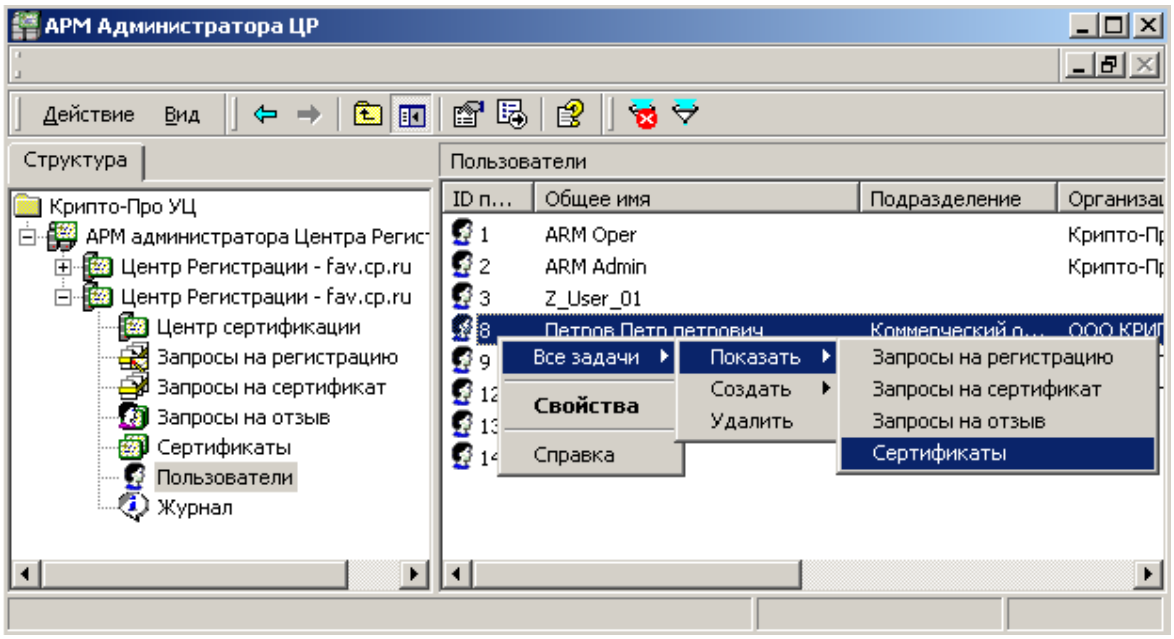
Окно **Принятие запросов на отзыв – Обработка завершена** применяется для просмотра результатов операций по принятию запросов, связанных как с отзывом, так и с приостановлением и возобновлением действия сертификата ключа подписи

Рисунок 165. Окно просмотра запросов на возобновление действия сертификата



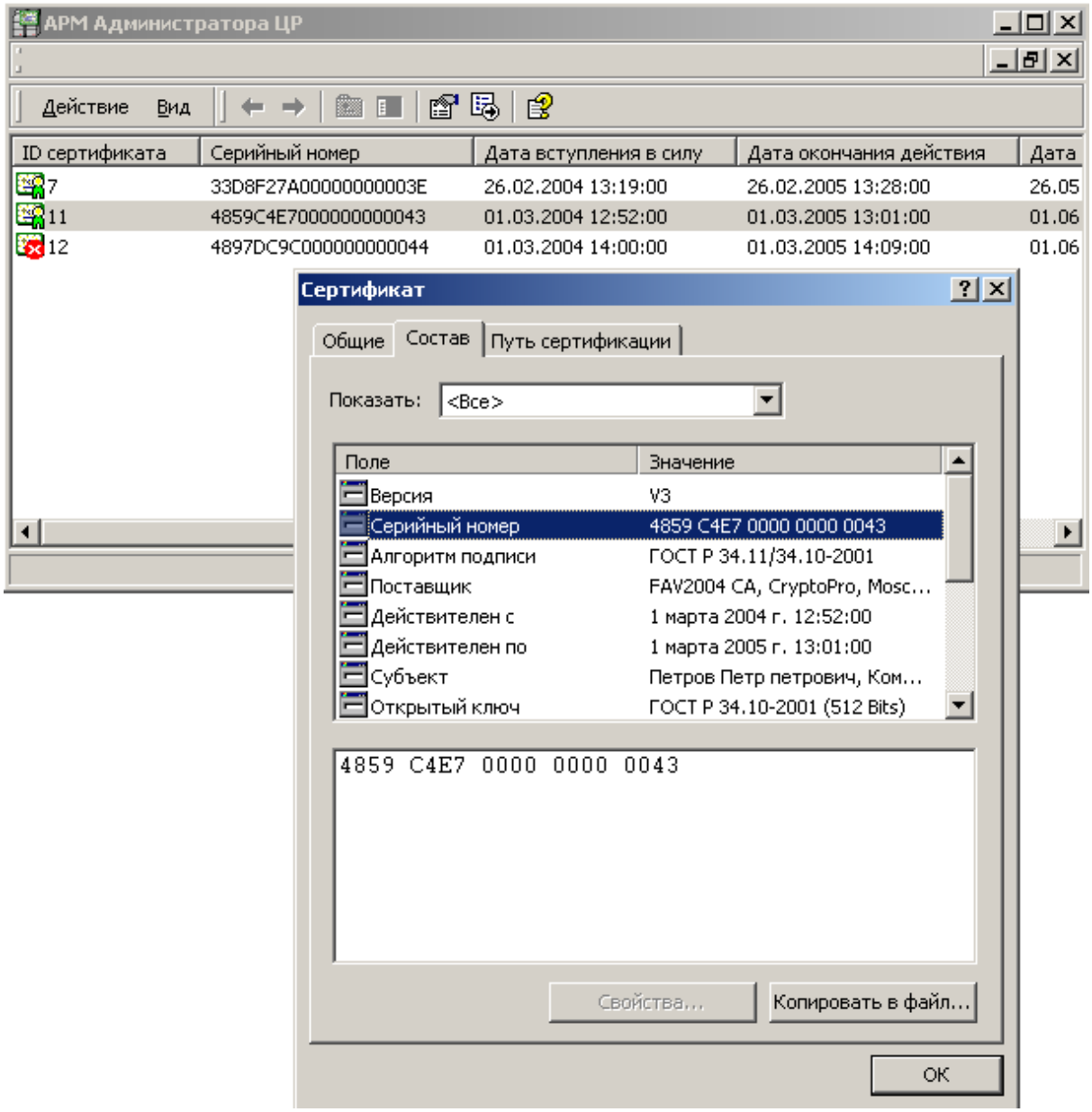
10. В левой части окна **АРМ администратора ЦР** выберите левой кнопкой мыши узел **Пользователи**. В правой части окна отобразится список зарегистрированных в Удостоверяющем Центре пользователей. Выделите правой кнопкой мыши учетную запись пользователя, действие сертификата которого было возобновлено, и в открывшемся контекстном меню выберите **Все задачи -> Показать -> Сертификаты;**

Рисунок 166. Выбор пункта меню для просмотра сертификатов зарегистрированного пользователя



11. Откроется список сертификатов выбранного пользователя, в котором сертификат, действие которого возобновлено, помечен как **действительный** (печать на сертификате).

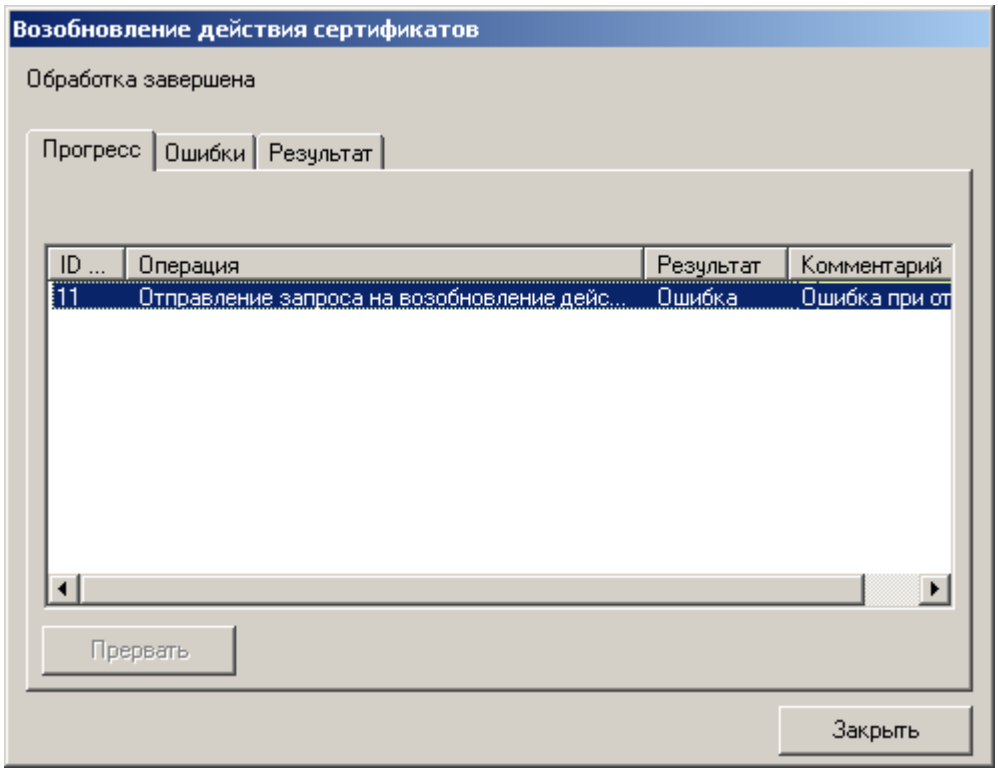
Рисунок 167. Просмотр сертификатов пользователя и сертификата, действие которого возобновлено

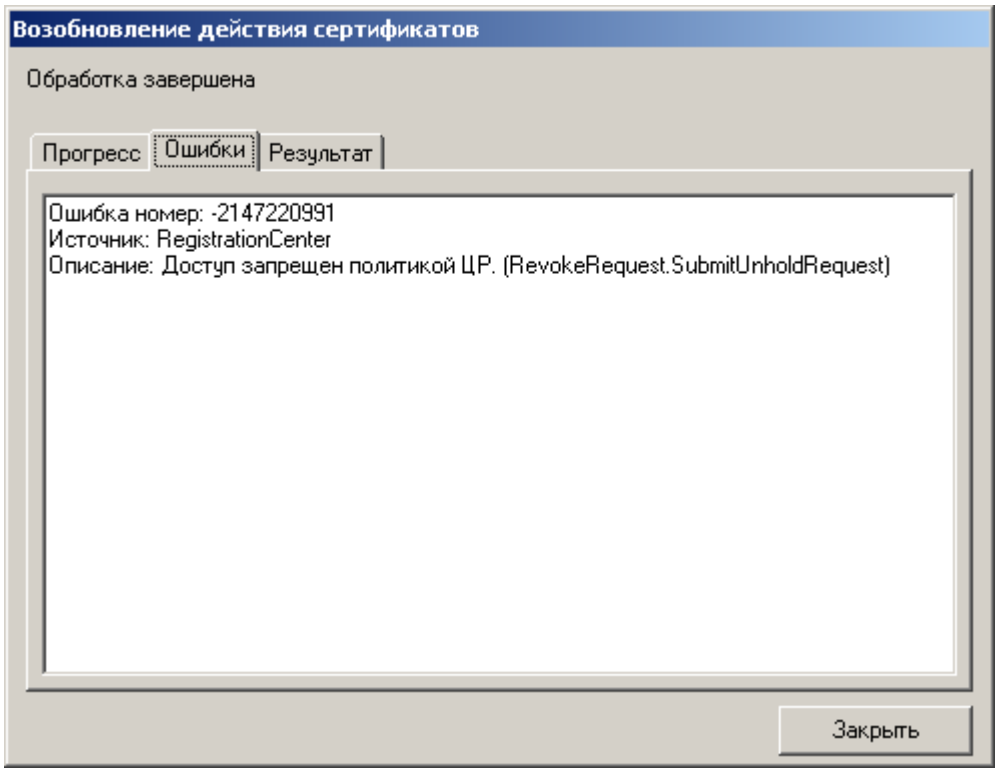


1.7.3. Наиболее часто встречающиеся ошибки, возникающие при осуществлении действий по возобновлению действия сертификата

1. При возобновлении действия сертификата с **АРМ Администратора ЦР** привилегированным пользователем в окне **Возобновление действия сертификатов - Обработка завершена** возникает ошибка:

Рисунок 168. Ошибка при выполнении метода RevokeRequest.SubmitUnholdRequest



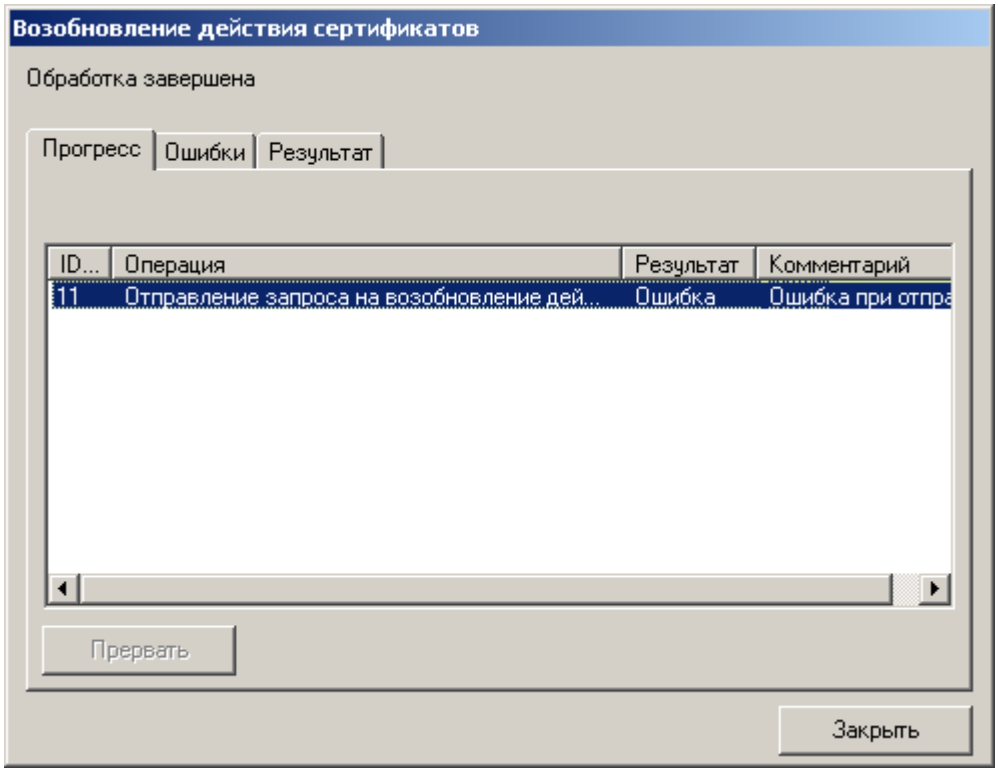


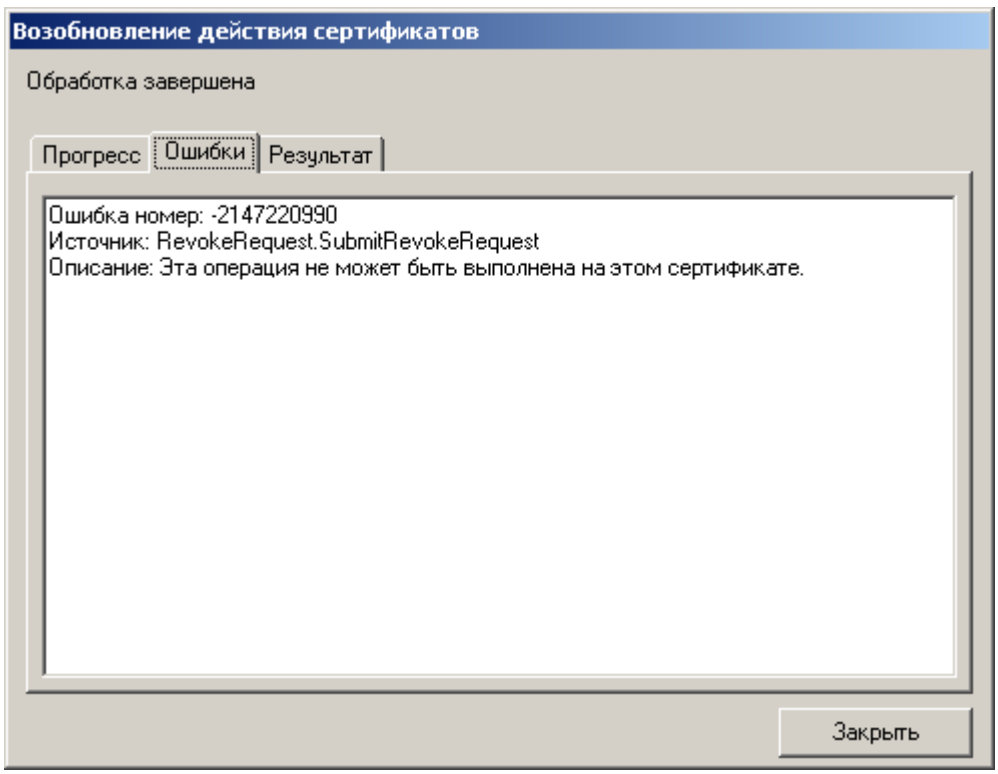
У привилегированного пользователя (**Оператора** или **Администратора**), производящего возобновление действия сертификата, недостаточно прав на выполнение метода **RevokeRequest.SubmitUnholdRequest**.

На Центре Регистрации необходимо осуществить настройку политики безопасности, позволяющую осуществлять выполнение указанного метода.

2. При возобновлении действия сертификата с **АРМ Администратора ЦР** привилегированным пользователем в окне **Возобновление действия сертификатов - Обработка завершена** возникает ошибка:

Рисунок 169. Ошибка при выполнении метода RevokeRequest.SubmitRevokeRequest





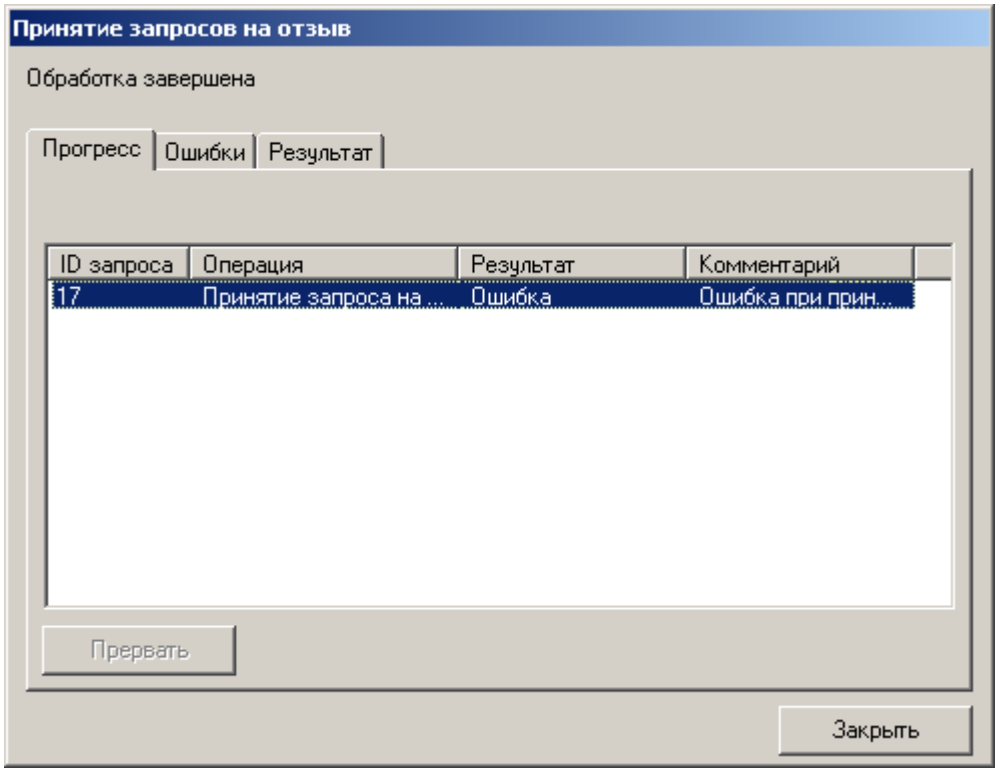
Сертификат, действие которого требуется возобновить, содержит хотя бы одну область использования (поле **Extended Key Usage**), присутствие которой в сертификате не позволяет привилегированному пользователю (**Оператору** или

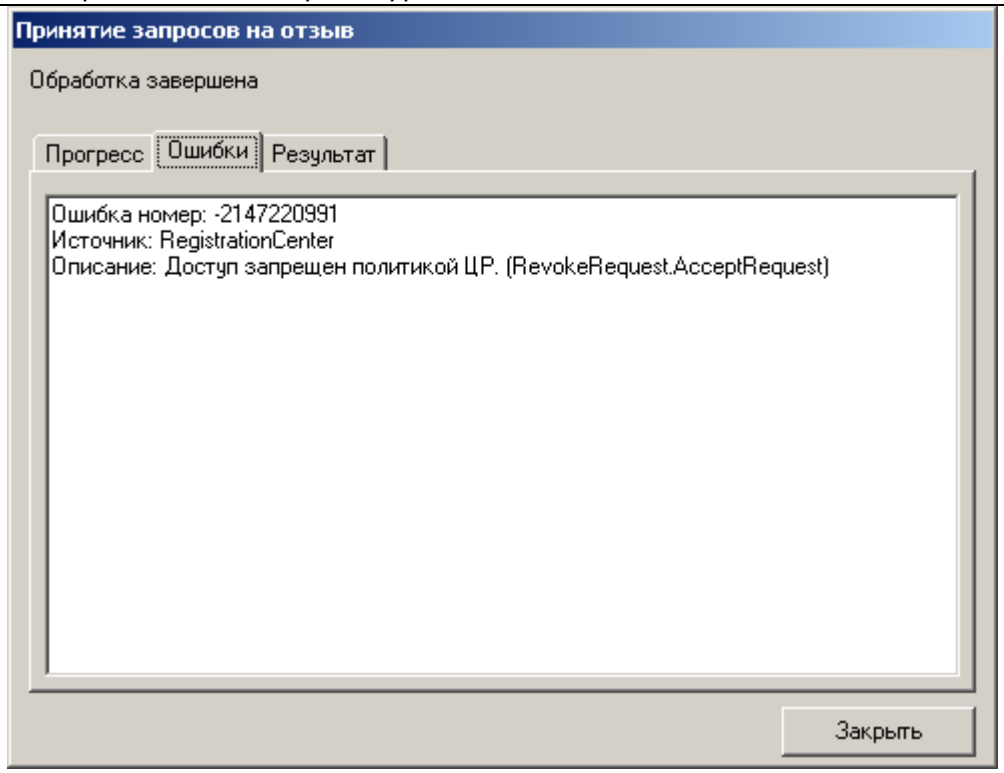
Администратору) возобновить действие указанного сертификата (данная область использования отсутствует в списке разрешенных для указанного привилегированного пользователя).

На Центре Регистрации осуществите настройку Политики обработки запросов на отзыв и для привилегированного пользователя, осуществляющего приостановление действия сертификатов, добавьте необходимые области использования сертификата.

3. При принятии существующего запроса на возобновление действия сертификата с **АРМ Администратора ЦР** привилегированным пользователем в окне **Принятие запроса на отзыв - Обработка завершена** возникает ошибка:

Рисунок 170. Ошибка при выполнении метода RevokeRequest.AcceptRequest



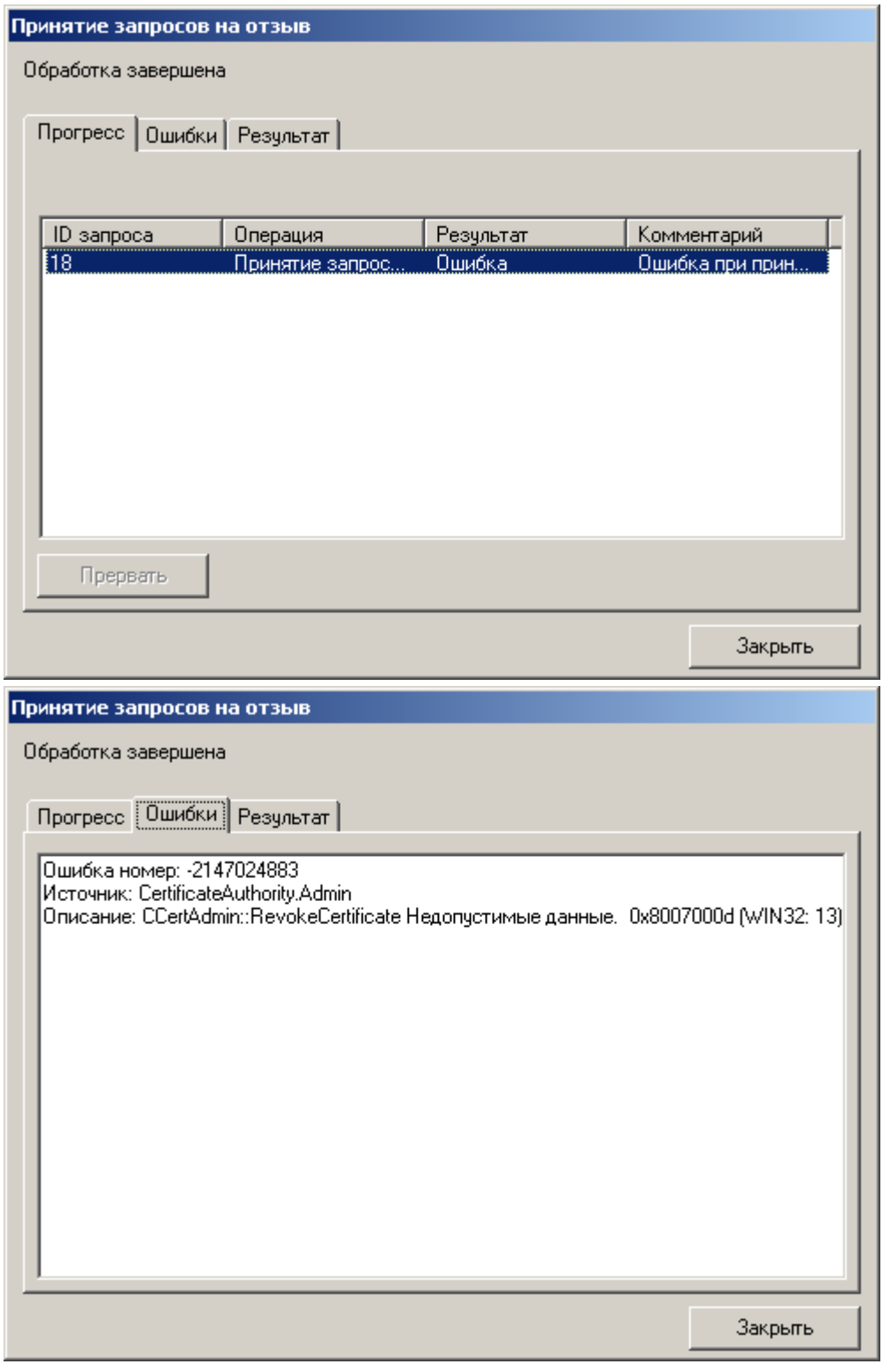


У привилегированного пользователя (**Оператора** или **Администратора**), производящего возобновление действия сертификата, недостаточно прав на выполнение метода **RevokeRequest.AcceptRequest**.

На Центре Регистрации необходимо осуществить настройку политики безопасности, позволяющую осуществлять выполнение указанного метода.

4. При принятии существующего запроса на возобновление действия сертификата с **АРМ Администратора ЦР** привилегированным пользователем в окне **Принятие запроса на отзыв - Обработка завершена** возникает ошибка:

Рисунок 171. Ошибка при попытке возобновления действия отозванного сертификата



Сертификат ключа подписи, действие которого необходимо возобновить, ранее уже был отозван.

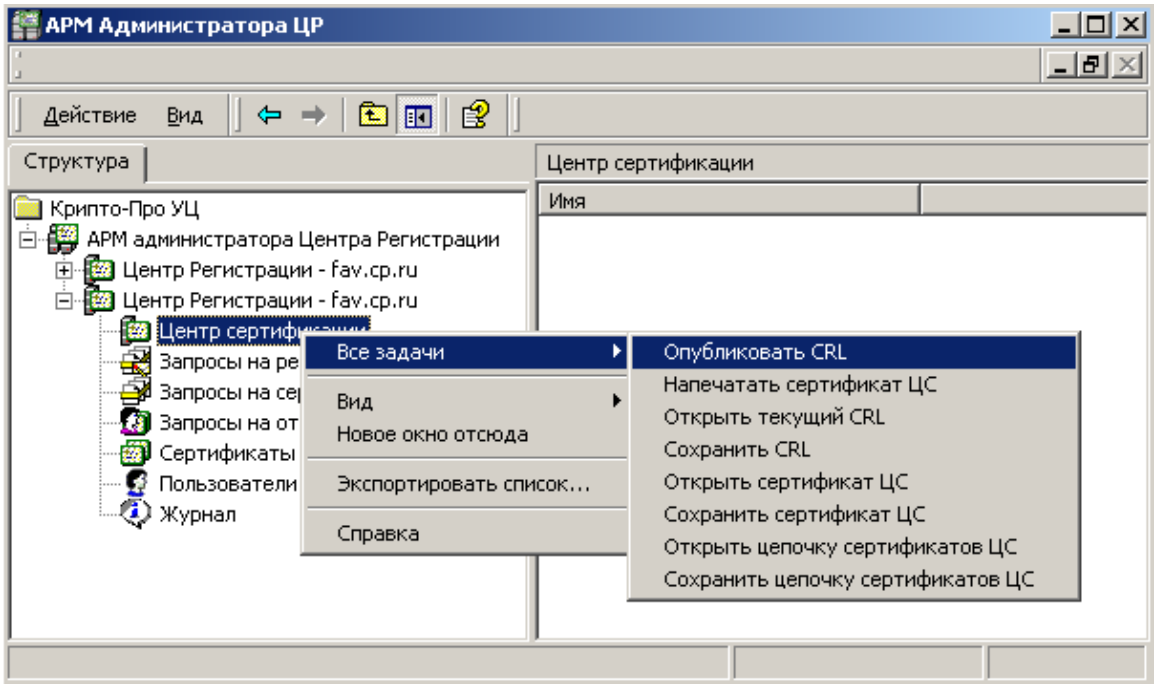
1.8. Изготовление списка отозванных сертификатов ключей подписи

После осуществления отзыва, приостановления и возобновления действия сертификатов Удостоверяющий Центр должен оповестить пользователей об изменении статуса сертификата. Оповещение осуществляется путем занесения (в случае возобновления действия сертификата – исключения) информации о сертификате в список отозванных сертификатов и публикации (рассылке) нового актуального списка отозванных сертификатов.

Описание процедуры изготовления нового списка отозванных сертификатов с использованием **АРМ Администратора ЦР:**

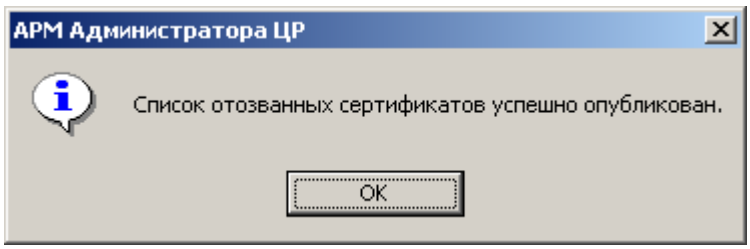
1. В окне **АРМ Администратора ЦР** выделите правой кнопкой мыши узел **Центр сертификации** и в открывшемся контекстном меню выберите пункт **Все задачи -> Опубликовать CRL;**

Рисунок 172. Выбор пункта меню для публикации списка отозванных сертификатов



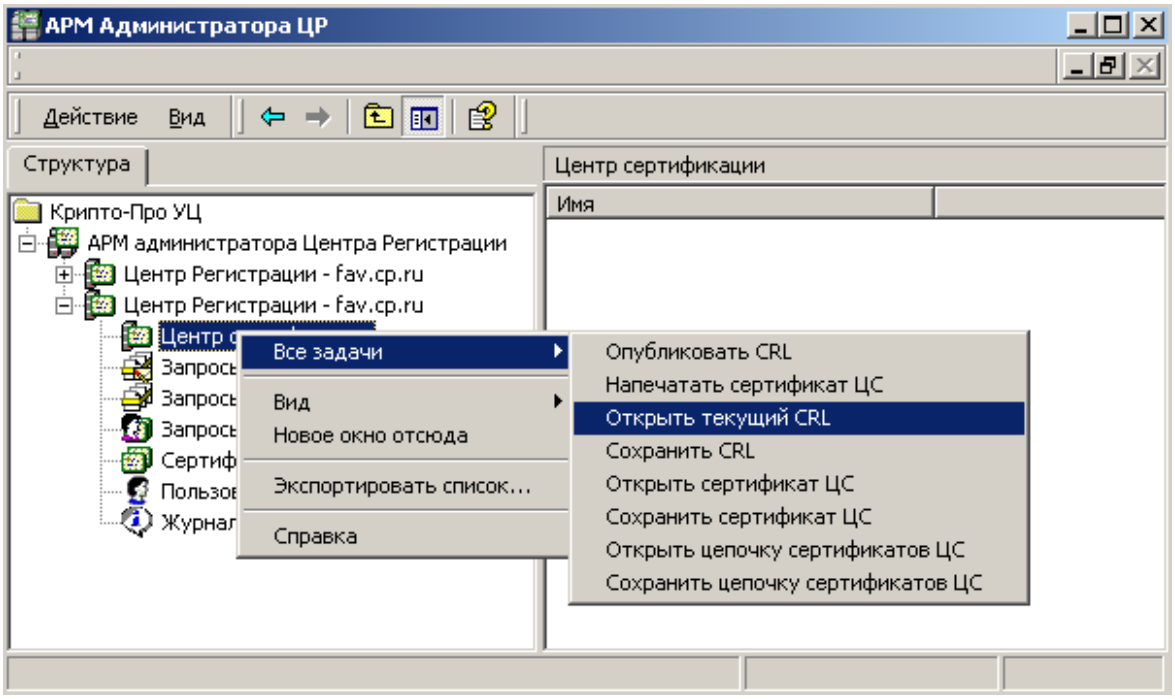
2. После успешного выполнения задачи публикации CRL откроется окно, информирующее пользователя об этом. Нажмите кнопку **ОК;**

Рисунок 173. Окно, информирующее об успешной публикации списка отозванных сертификатов



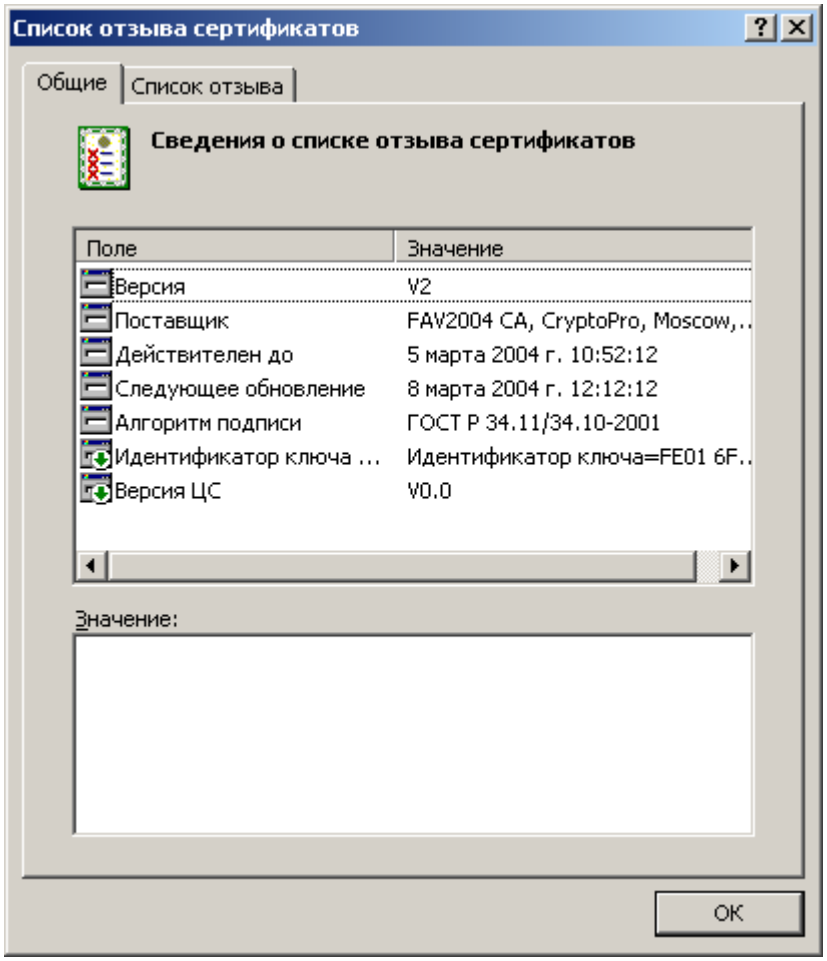
3. В окне **АРМ Администратора ЦР** выделите правой кнопкой мыши узел Центр сертификации и в открывшемся контекстном меню выберите пункт **Все задачи -> Открыть текущий CRL;**

Рисунок 174. Выбор пункта меню для просмотра Списка отозванных сертификатов



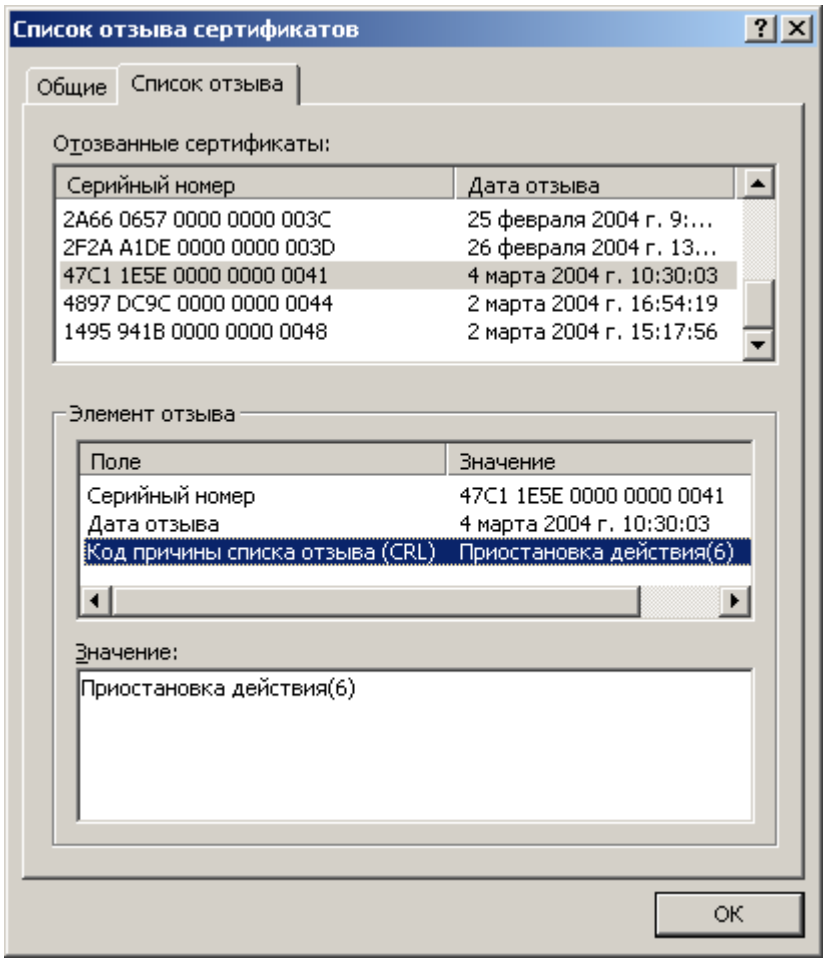
4. Откроется текущий список отозванных сертификатов;

Рисунок 175. Окно просмотра Списка отозванных сертификатов



Информация о сертификате, действие которого было приостановлено, заносится в список отозванных сертификатов с указанием причины **Приостановка действия (код – 6).**

Рисунок 176. Информация о сертификате, действие которого приостановлено, заносимая в Список отозванных сертификатов



Публикация списка отозванных сертификатов (CRL) и его размещение в необходимой точке распространения (CDP) может осуществляться автоматически с помощью настройки определенных задач Центра Регистрации.

2. Перечень терминов

Аутентификация

Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Закрытый ключ

Криптографический ключ, который хранится пользователем системы в тайне. Он используется для формирования электронной цифровой подписи и/или шифрования данных.

Запрос на сертификат

Сообщение, содержащее необходимую информацию для получения сертификата. Формируется в АРМ Пользователя или в АРМ Администратора, после чего передается через Центр Регистрации Центру Сертификации, где и обрабатывается. Результатом обработки является выпущенный сертификат или сообщение об ошибке.

Запрос на отзыв сертификата.

Сообщение, содержащее необходимую информацию для отзыва сертификата. Формируется в АРМ Пользователя или в АРМ Администратора, после чего передается через Центр Регистрации Центру Сертификации, где и обрабатывается. Результатом обработки является отзыв сертификата или сообщение об ошибке.

Идентификация

Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Ключ (криптографический ключ).

Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

Ключевая пара

Открытый и закрытый ключи.

Ключевой носитель

Объект системы, который может содержать один или несколько ключевых контейнеров. Каждый ключевой контейнер содержит следующую информацию: только ключ подписи, только ключ шифрования, ключ подписи и ключ шифрования одновременно. Дополнительно, ключевой контейнер содержит служебную информацию, необходимую для обеспечения криптографической защиты ключей и их целостности. Каждый контейнер является полностью самостоятельным и содержит всю необходимую информацию для работы как с самим контейнером, так и с закрытыми ключами.

Компрометация ключа

Утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

1. Потеря ключевых носителей.
2. Потеря ключевых носителей с их последующим обнаружением.
3. Увольнение сотрудников, имевших доступ к ключевой информации.
4. Нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа.
5. Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.
6. Нарушение печати на сейфе с ключевыми носителями.
7. Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и

доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника)

Различают два вида компрометации секретного ключа: **явную** и **неявную**. Первые четыре события должны трактоваться как явная компрометация ключей. Три следующих события требуют специального рассмотрения в каждом конкретном случае.

Открытый ключ

Криптографический ключ, который связан с закрытым ключом с помощью особого математического соотношения. Открытый ключ известен другим пользователям системы и предназначен для проверки электронной цифровой подписи и шифрования. При этом открытый ключ не позволяет вычислить закрытый ключ.

Плановая смена ключей

Смена ключей с установленной в системе периодичностью, не вызванная компрометацией ключей.

Проверка электронной подписи документа

Проверка соотношения, связывающего хэш-функцию документа, подпись под этим документом и открытый ключ подписавшего пользователя. Если рассматриваемое соотношение оказывается выполненным, то подпись признается правильной, а сам документ - подлинным, в противном случае документ считается измененным, а подпись под ним - недействительной.

Сертификат

Цифровой документ, который содержит открытый ключ субъекта и подписан электронной цифровой подписью его издателя. Сертификат также содержит сведения о владельце открытого ключа, например, информацию, которая его дополнительно идентифицирует. Таким образом, выдавая сертификат, издатель удостоверяет подлинность связи между открытым ключом субъекта и информацией, которая его идентифицирует.

Формат сертификата определен в рекомендациях ITU-T 1997 года X.509 [X.509] и рекомендациях IETF 1999 года RFC 2459 [RFC 2459].

Список отзыва

Список отозванных сертификатов (CRL – Certificate Revocation List). УЦ поддерживает отзыв сертификатов и публикацию списков отозванных сертификатов. Пользователи УЦ могут получить эту информацию и записать ее в свое локальное хранилище, чтобы использовать для последующей проверки сертификатов.

Центр Сертификации (Удостоверяющий Центр)

Компонент Удостоверяющего Центра. Выполняет функции службы сертификации: выпуск сертификатов, отзыв сертификатов, а также генерацию списков отзыва.

Центр Регистрации

Компонент Удостоверяющего Центра. Выполняет функции промежуточного звена, осуществляющего передачу запросов от пользователей и администраторов Центра Регистрации центру сертификации. В процессе этой передачи осуществляется аутентификация пользователя, проверка корректности передаваемой им информации, а также фиксация этой информации в базе данных ЦР.

Шифрование

Процесс зашифрования или расшифрования.

Шифрование информации – взаимнооднозначное математическое (криптографическое) преобразование, зависящее от ключа (секретный параметр преобразования), которое ставит в соответствие блоку открытой информации, представленной в некоторой цифровой кодировке, блок шифрованной информации, также представленной в цифровой кодировке. Термин шифрование объединяет в себе два процесса: зашифрование и расшифрование информации.

Если зашифрование и расшифрование осуществляются с использованием одного и того же ключа, то такой алгоритм криптографического преобразования называется симметричным, в противном случае — асимметричным.

Прочитать зашифрованное сообщение (информацию) может только пользователь, имеющий тот же секретный ключ шифрования.

Электронная цифровая подпись (ЭЦП)

Данные, добавляемые к блоку данных, полученные в результате его криптографического преобразования, зависящего от секретного ключа и блока данных, которые позволяют приемнику данных удостовериться в целостности блока данных и подлинности источника данных, а так же обеспечить защиту от подлога со стороны приемника данных.

Проверка электронной цифровой подписи под блоком открытой информации производится с помощью криптографического преобразования и открытого ключа, соответствующего секретному ключу, участвовавшему в процессе установки ЭЦП.

Microsoft Management Console

Административная консоль, позволяющая создавать и сохранять средства управления программным и аппаратным обеспечением в рамках операционной системы Windows. Такие средства называются MMC-консолями.

3. 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
УЦ	Удостоверяющий Центр
ЭЦП	Электронная цифровая подпись

4. Перечень рисунков

Лист регистрации изменений

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