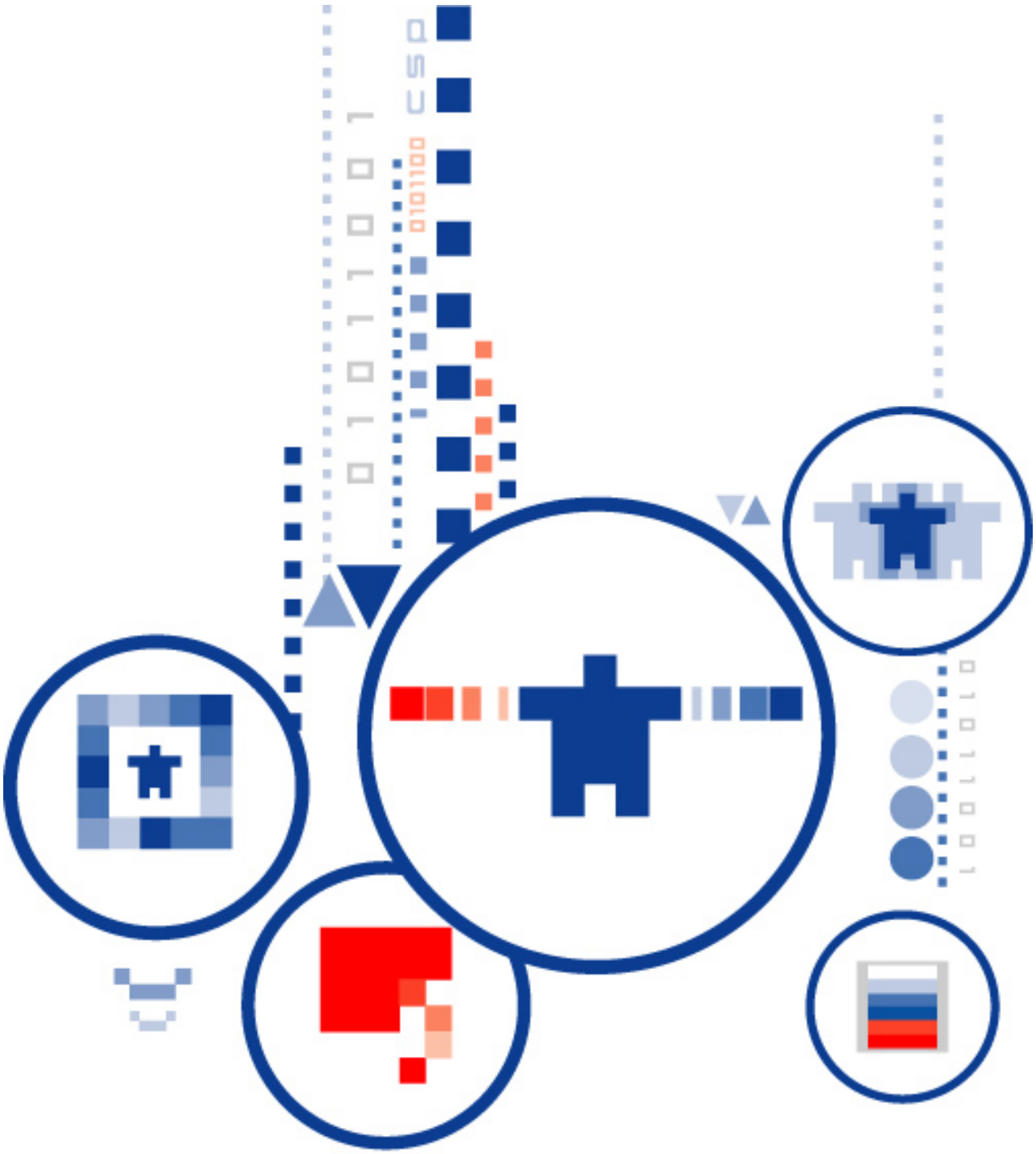


КриптоПро УЦ

программно–аппаратный комплекс
удостоверяющий центр

Руководство Оператора ЦУС VPN

СОДЕРЖАНИЕ

1. Требования для работы с приложением

Для установки и эксплуатации АРМ администратора ЦР необходимо следующее программное обеспечение:

- Операционная система - Microsoft Windows Server 2003 с установленным пакетом обновлений SP2 и выше, Microsoft Windows XP с установленным пакетом обновлений SP2 и выше, Microsoft Windows 7 с установленными пакетами обновлений, Microsoft Windows Server 2008 с установленным пакетом обновлений SP2 и выше, Microsoft Windows Server 2008 R2. Операционные системы могут быть как английской версии, так и русской;
- Microsoft Internet Explorer 7.0 (и выше);
- Средство криптографической защиты информации (СКЗИ) КриптоПро CSP версии 3.6.

.

2. Объекты управления

Все объекты управления Центра Регистрации располагаются в Базе Данных Центра Регистрации Удостоверяющего Центра. Объекты управления имеют состояния, зависящие от типа объекта. Изменение состояния объектов осуществляется с использованием методов объектов. Возможность доступа к методам объектов определяется правами доступа, соответствующими роли пользователя, запрашивающего методы.

Управление объектами ЦР обеспечивается Администратором ЦР и Оператором ЦР с выполнением следующих функций (предустановленные настройки):

Администратор ЦР:

- генерация ключей пользователей;
- изготовление сертификатов открытых ключей пользователей;
- отзыв сертификатов открытых ключей пользователей;
- приостановление/возобновление сертификатов открытых ключей пользователей;
- обработка запросов на изготовление сертификатов открытых ключей пользователей;
- обработка запросов на отзыв сертификатов открытых ключей пользователей;
- обработка запросов на приостановление/возобновление действия сертификатов открытых ключей пользователей;
- опубликование списка отозванных сертификатов.

Оператор ЦР:

- регистрация пользователей в Базе Данных Центра Регистрации;
- генерация первых ключей пользователя в процессе выполнения процедуры регистрации пользователей;
- изготовление первого сертификата открытого ключа пользователя;
- обработка запросов на регистрацию пользователей;
- обработка запросов на изготовление первого сертификата открытого ключа.

Далее по тексту документа вместо определений «Администратор ЦР» и «Оператор ЦР» будет использоваться единое определение – «администратор».

2.1. Пользователь

Пользователь УЦ — субъект прикладной системы, зарегистрированный в Базе Данных Центра Регистрации. Пользователем УЦ является физическое лицо, которое может представлять юридическое лицо.

2.2. Сертификат открытого ключа

Сертификат — цифровой документ, который содержит сведения о владельце открытого ключа, собственно открытый ключ пользователя и подписан электронной цифровой подписью его издателя, т.е. подписан на закрытом ключе уполномоченного лица Удостоверяющего Центра. Таким образом, выдавая сертификат, издатель удостоверяет подлинность связи между открытым ключом субъекта и информацией, которая его идентифицирует.

Состояния объекта:

- действующий – сертификат является действующим на текущий момент времени;
- отозванный – сертификат отозван (аннулирован) или действие его приостановлено на текущий момент времени;
- просроченный – срок действия сертификата открытого ключа истек;
- просроченный ключ – срок действия закрытого ключа, соответствующего открытому ключу, истек.

2.3. Запрос на регистрацию

Запрос на регистрацию — сообщение, содержащее необходимую информацию для регистрации пользователя в Базе Данных Центра Регистрации. Формируется при регистрации пользователя посредством АРМ пользователя. Передается по сети передачи данных в Центр Регистрации. Обработка осуществляется администратором с АРМ администратора ЦР. Результатом обработки является создание учетной записи пользователя в Базе Данных Центра Регистрации или сообщение об ошибке.

Состояния объекта:

- ожидающий – запрос установлен в очередь на обработку администратором;
- одобренный – запрос принят администратором, и пользователь зарегистрирован в Базе Данных ЦР;
- отклоненный – запрос отклонен администратором, пользователь не зарегистрирован в Базе Данных ЦР.

2.4. Запрос на сертификат

Запрос на сертификат — сообщение, содержащее необходимую информацию для изготовления сертификата открытого ключа. Формируется пользователем посредством АРМ пользователя или администратором посредством АРМ администратора ЦР. Результатом обработки запроса на сертификат является изготовление сертификата или сообщение об ошибке.

Состояния объекта:

- ожидающий - запрос установлен в очередь на обработку администратором;
- одобренный - запрос принят администратором, и сертификат по указанному запросу изготовлен;
- отклоненный - запрос отклонен администратором, сертификат не изготовлен;
- подтвержденный - запрос принят администратором, сертификат по указанному запросу изготовлен, пользователь подтвердил получение и установку на своем рабочем месте сертификата.

2.5. Запрос на отзыв сертификата

Запрос на отзыв сертификата — сообщение, содержащее необходимую информацию для выполнения процедуры отзыва, приостановления или возобновления действия сертификата пользователя. Формируется пользователем посредством АРМ пользователя или администратором посредством АРМ администратора ЦР. Результатом обработки является аннулирование (отзыв), приостановление или возобновление действия сертификата или сообщение об ошибке.

Состояния объекта:

- ожидающий – запрос установлен в очередь на обработку администратором;
- одобренный – запрос принят администратором, и сертификат по указанному запросу аннулирован (отозван) либо действие его приостановлено или возобновлено;

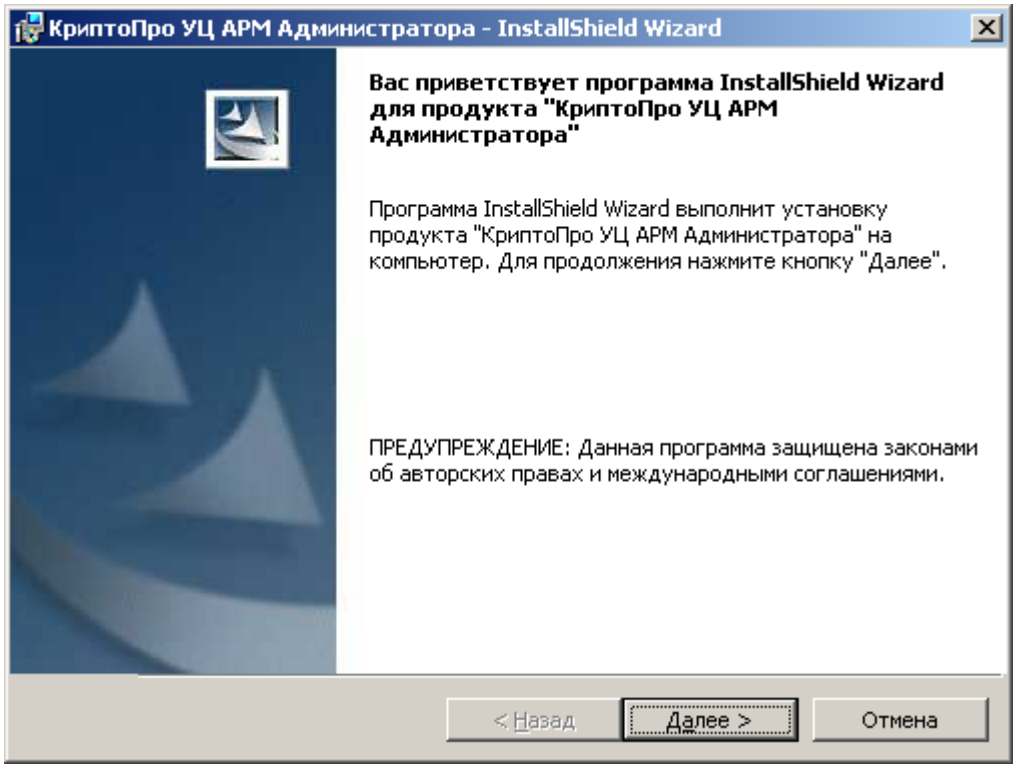
- отклоненный – запрос отклонен администратором, аннулирование (отзыв), приостановление или возобновление действия сертификата не произведено.

3. Установка АРМ Администратора ЦР и подключение привилегированного пользователя к Центру Регистрации

Для установки программного обеспечения АРМ администратора ЦР запустите приложение **CRAdmin.msi**.

После запуска программа установки выведет на экран диалоговое окно подтверждения продолжения установки (см. **Рисунок 1**).

Рисунок 1. Окно Мастера установки ПО АРМ администратора

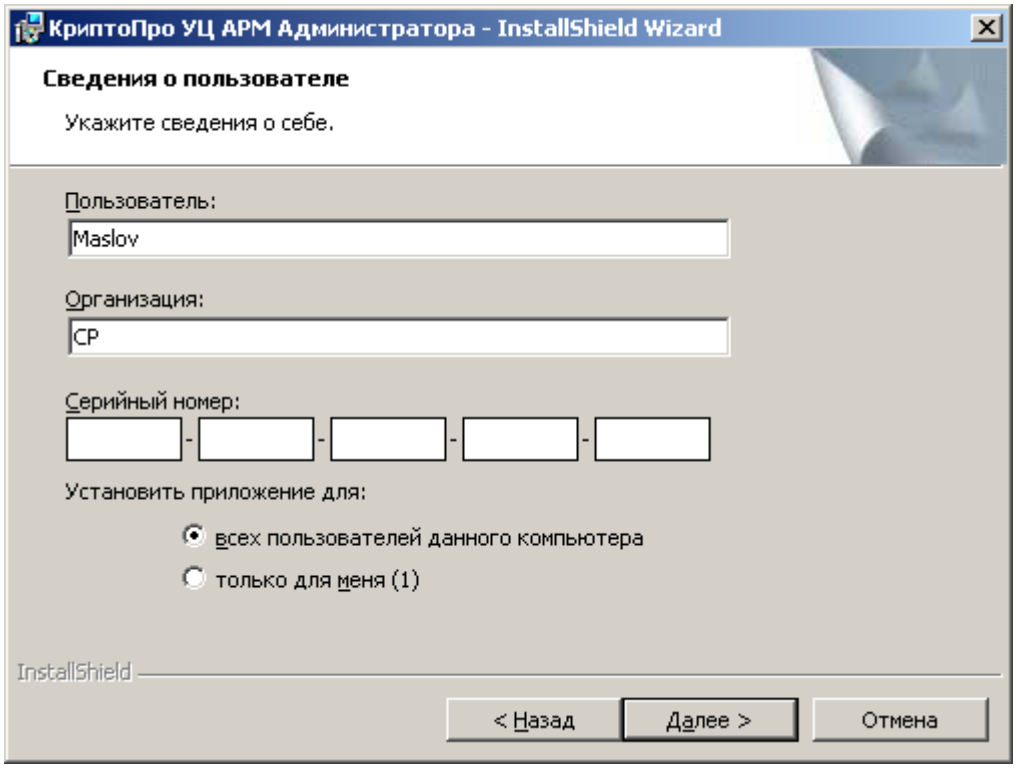


Для продолжения установки ПО АРМ Администратора необходимо нажать кнопку **Далее**. Для отмены установки ПО, нажать кнопку «Отмена».

В следующем окне необходимо ввести информацию о пользователе, производящем установку ПО, наименование организации и серийный номер предоставленной лицензии (см.Рисунок 2) – название организации и серийный номер лицензии должны полностью соответствовать данным, указанным в лицензии.

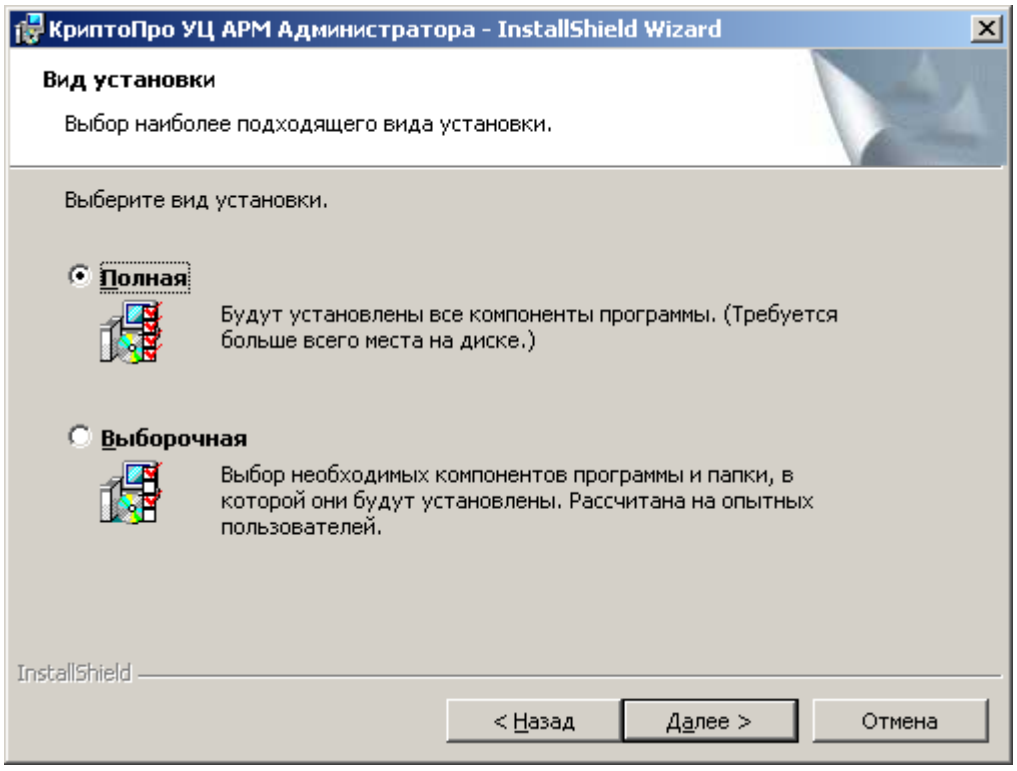
Если все поля для ввода серийного номера оставить пустыми, то программа установки будет использовать серийный номер ознакомительной лицензии, действующей в течение месяца.

Рисунок 2. Окно ввода информации о пользователе, организации и серийного номера лицензии Мастера установки АРМ администратора



После нажатия кнопки **Далее** на экран будет выведено диалоговое окно, в котором необходимо определить тип установки ПО (см.Рисунок 3).

Рисунок 3. Окно определения типа установки Мастера установки АРМ администратора

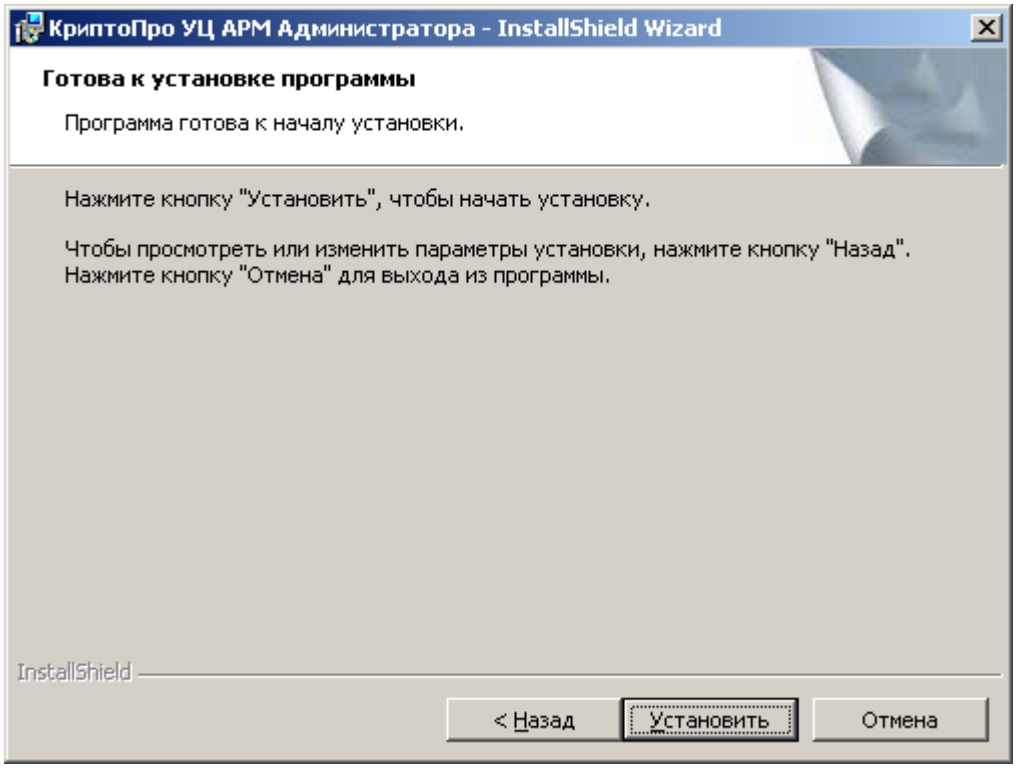


Тип установки **Полная** производит установку программного обеспечения АРМ Администратора в папку назначения, определенную по умолчанию. Таковой папкой является **Program Files\Crypto Pro** системного диска локального компьютера.

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

После определения начальных параметров Мастера установки на экран выводится диалоговое окно, в котором инициируется собственно операция установки (см. Рисунок 4).

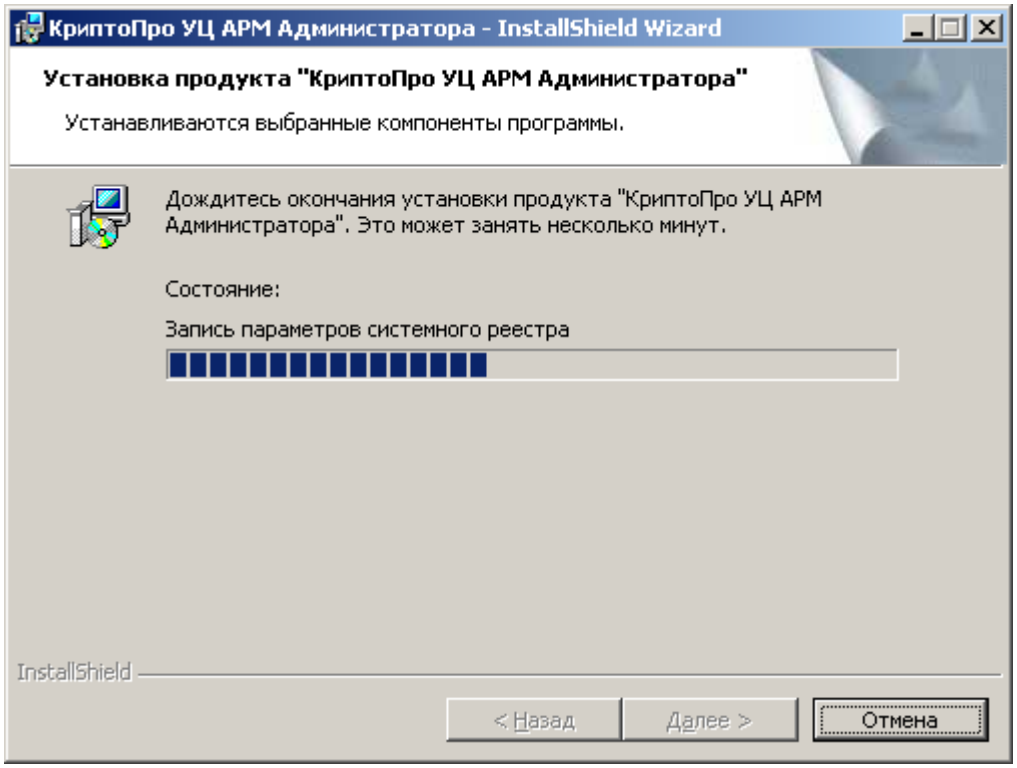
Рисунок 4. Окно подтверждения установки ПО Мастера установки АРМ администратора



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

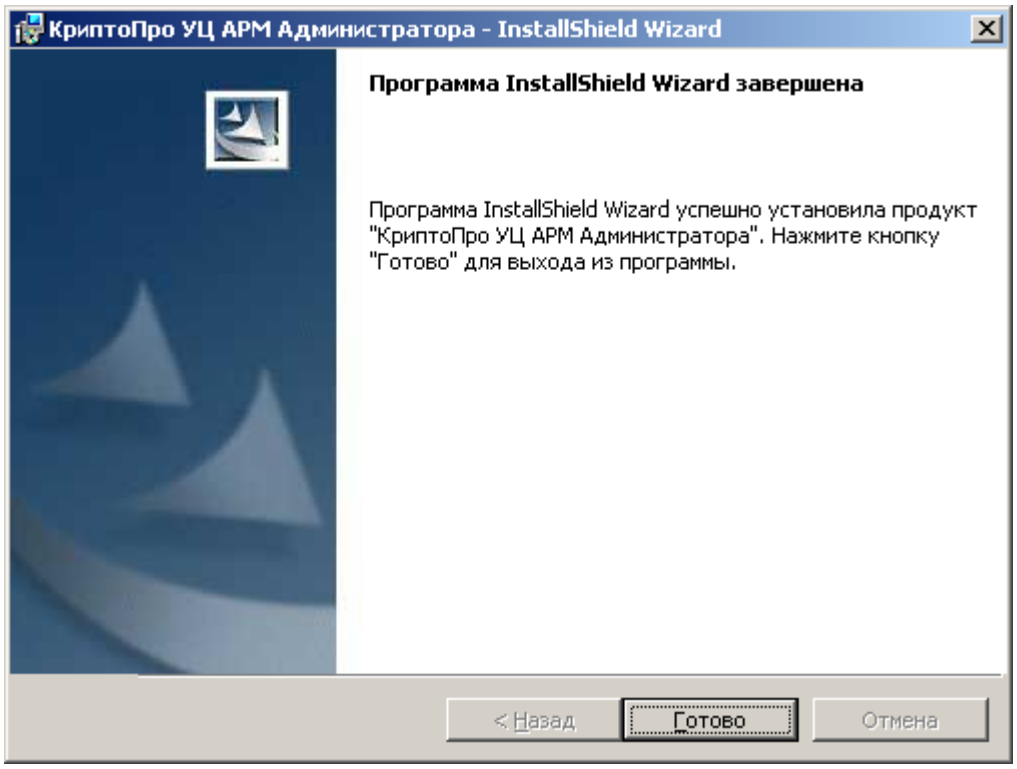
При выполнении операций установки, состояние процесса отображается в окне на экране.

Рисунок 5. Окно состояния установки Мастера установки АРМ администратора



Успешное завершение процесса установки ПО АРМ Администратора должно подтвердиться сообщением Мастера установки (см.Рисунок 6).

Рисунок 6. Окно окончания работы Мастера установки АРМ администратора



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

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

4. Конфигурация АРМ администратора ЦР в процессе эксплуатации

4.1. Настройка АРМ администратора ЦР после подключения к ЦР

После завершения создания подключения привилегированного пользователя с АРМ администратора ЦР к Центру Регистрации необходимо проверить правильность установки определенных параметров и произвести их настройку.

Указанные параметры задаются в окнах: **Свойства: АРМ администратора Центра Регистрации** и **Свойства: Центр Регистрации – Имя ЦР**.

Представленные в настоящем документе образцы диалоговых окон приводятся применительно к операционным системам семейства Windows 2000 и для операционных систем Windows XP , Windows 2003, Windows 7, Windows 2008 могут отличаться.

Конфигурация АРМ администратора ЦР в окне **Свойства: АРМ администратора Центра Регистрации** заключается в определении следующих параметров:

- Файл шаблона печати сертификатов (XSLT) – используется при печати сертификата открытого ключа на бумажном носителе;
- Файл шаблона формы для автономной работы (MHT) – используется для создания html-формы, обеспечивающей формирование ключей и запроса на изготовление сертификата открытого ключа пользователя без сетевого подключения к Центру Регистрации;
- Разрешить выбор CSP. При установке данного флага при генерации ключей пользователей администратор сможет изменить настроенный по умолчанию криптопровайдер и использовать любой другой, установленный на АРМ Администратора ЦР. При снятии данного флага будет использоваться криптопровайдер, настроенный по умолчанию;
- Запрашивать имя контейнера – при генерации ключей пользователей администратор сможет задать имя ключевого контейнера;
- CSP по умолчанию. При генерации ключей пользователей в диалоговом окне выбора криптопровайдера по умолчанию будет устанавливаться указанный в настоящей настройке криптопровайдер. Если не установлен флаг «Разрешить выбор CSP», то диалоговое окно отображаться не будет, и ключи будут формироваться в соответствии с данными настройками;

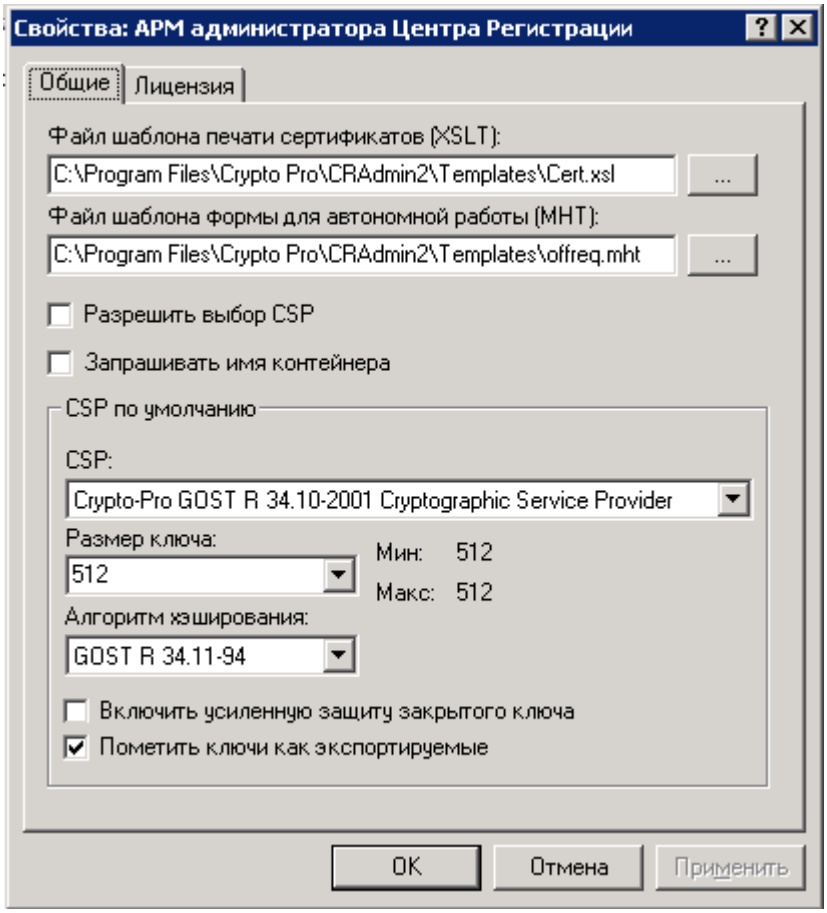
  Для выбранного криптопровайдера устанавливаются параметры генерации ключей:

  - Включить усиленную защиту ключа - При установке данного параметра каждая попытка обращения к закрытому ключу фиксируется системой, о чем пользователь будет получать соответствующее уведомление;
  - Пометить ключи как экспортируемые – При установке данного параметра возможен экспорт закрытых ключей с одного носителя на другой. При использовании СКЗИ «КриптоПро CSP», установка данного флага обеспечит возможность копирования ключевого контейнера с помощью сервисных функций СКЗИ «КриптоПро CSP». Установка данного флага рекомендуется;

- Текущая лицензия. Установка серийного номера лицензии на право пользования приложением АРМ администратора ЦР.

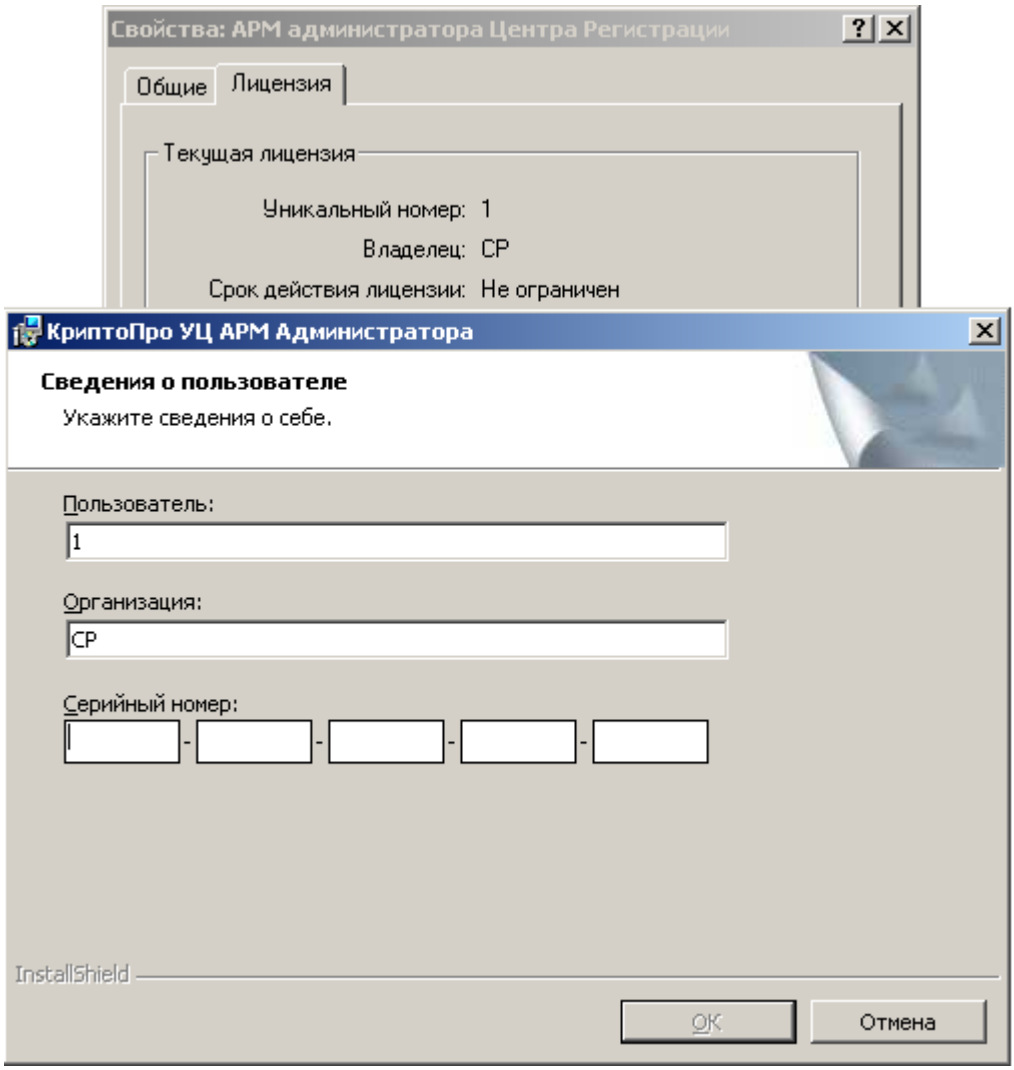
Для настройки указанных параметров в окне консоли **АРМ администратора ЦР** выделите правой кнопкой мыши узел **АРМ администратора Центра Регистрации** и в открывшемся контекстном меню выберите пункт **Свойства** (см. Рисунок 7).

Рисунок 7. Окно свойств АРМ администратора Центра Регистрации



В том случае, если при установке АРМ Администратора ЦР процедура ввода серийного номера лицензии была опущена, или требуется замена этих данных (например, в связи с окончанием времени действия лицензии), ввод серийного номера лицензии осуществляется на вкладке «**Лицензия**» окна **Свойства: АРМ Администратора Центра Регистрации** (см. Рисунок 8).

Рисунок 8. Ввод серийного номера лицензии

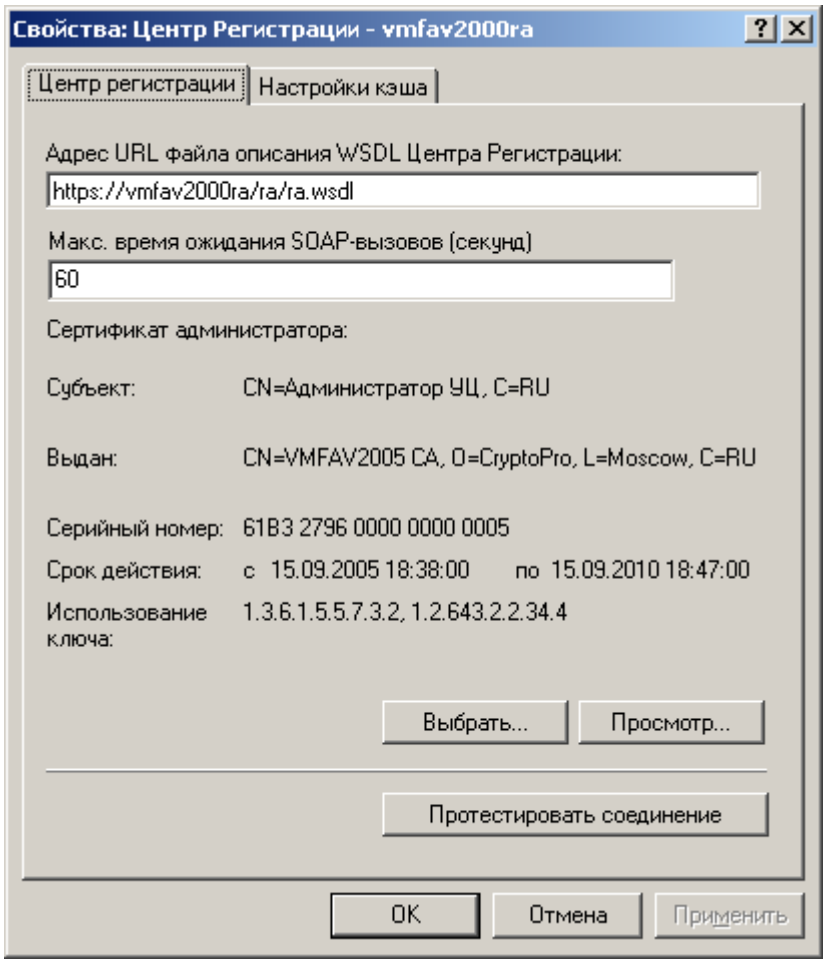


Конфигурация АРМ администратора ЦР в окне **Свойства: Центр Регистрации – Имя ЦР** заключается в определении следующих параметров:

- Адрес URL файла описания WSDL Центра Регистрации. Адрес подключения к Центру Регистрации;
- Макс. время ожидания SOAP-вызовов (секунд) – время, в течение которого ожидается получение ответа АРМ администратора ЦР от Центра Регистрации;
- Сертификат администратора. Сертификат привилегированного пользователя, на котором осуществляется подключение к Центру Регистрации;
- Настройки кэша. Указанная настройка позволяет обеспечить управление объемом пересылаемых данных из Центра Регистрации для отображения АРМ администратора ЦР.

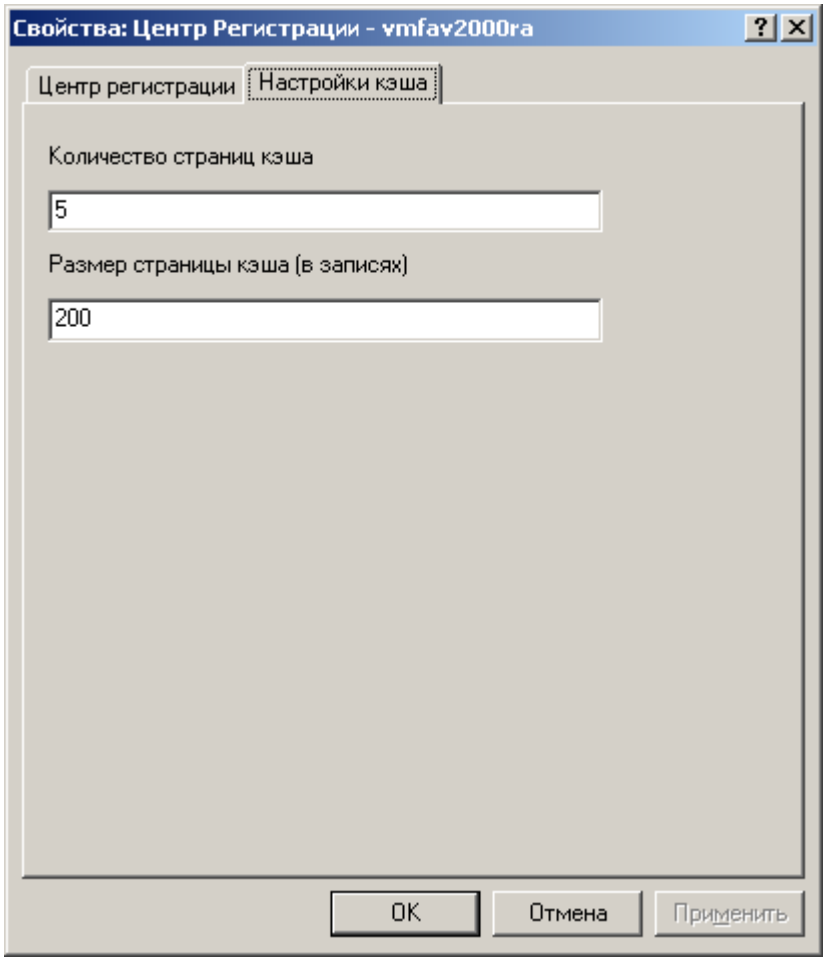
Для настройки указанных параметров в окне консоли **АРМ администратора ЦР** выделите правой кнопкой мыши узел подключения к Центру Регистрации **Центр Регистрации – Имя ЦР** и в открывшемся контекстном меню выберите пункт **Свойства** (см. Рисунок 9).

Рисунок 9. Окно настройки параметров подключений к Центру Регистрации



Установка настроек кэша производится на вкладке **Настройки кэша** окна **Центр Регистрации – Имя ЦР** (см. Рисунок 10).

Рисунок 10. Настройка кэша данных, предоставляемых Центром Регистрации



Настройки кэша позволяют обеспечить передачу информации с Центра Регистрации (передачу записей базы данных) определенными частями. Например, имея число выпущенных сертификатов более 300 и следующую настройку кэша: количество страниц – 3, размер страницы – 50, при открытии узла **Сертификаты** с ЦР будет запрошено 150 записей об изготовленных сертификатах. Если потребуется просмотреть запись о 151-ом сертификате, то с ЦР будет запрошена новая страница (50 записей), содержащая необходимую запись, которая перезапишет в кэше самую «старую» страницу - страницу, к которой не было обращений дольше всех остальных. Указанная настройка позволяет обеспечить эксплуатацию АРМ администратора в сильно распределенной системе с относительно малой пропускной способностью между ЦР и АРМ администратора.

В процессе эксплуатации программного обеспечения АРМ администратора ЦР доступно изменение указанных настроек. Процедура конфигурации параметров настроек АРМ администратора ЦР производится в следующих случаях:

- смена ключей и сертификата администратора, на котором осуществляется подключение к Центру Регистрации;
- смена файла-шаблона печати сертификата или изменение его местонахождения;
- смена файла-шаблона формы для автономной работы или изменение его местонахождения;
- смена доменного имени или расположения в сети сервера Центра Регистрации;

- изменение параметров генерации ключей;
- изменение параметров настройки кэша (количество страниц кэша и размер страницы кэша в записях).

После изменения URL Web-сервиса Центра Регистрации, с которым будет работать АРМ администратора ЦР и/или сертификата администратора, рекомендуется протестировать соединение с Центром Регистрации с помощью кнопки **Протестировать соединение**.

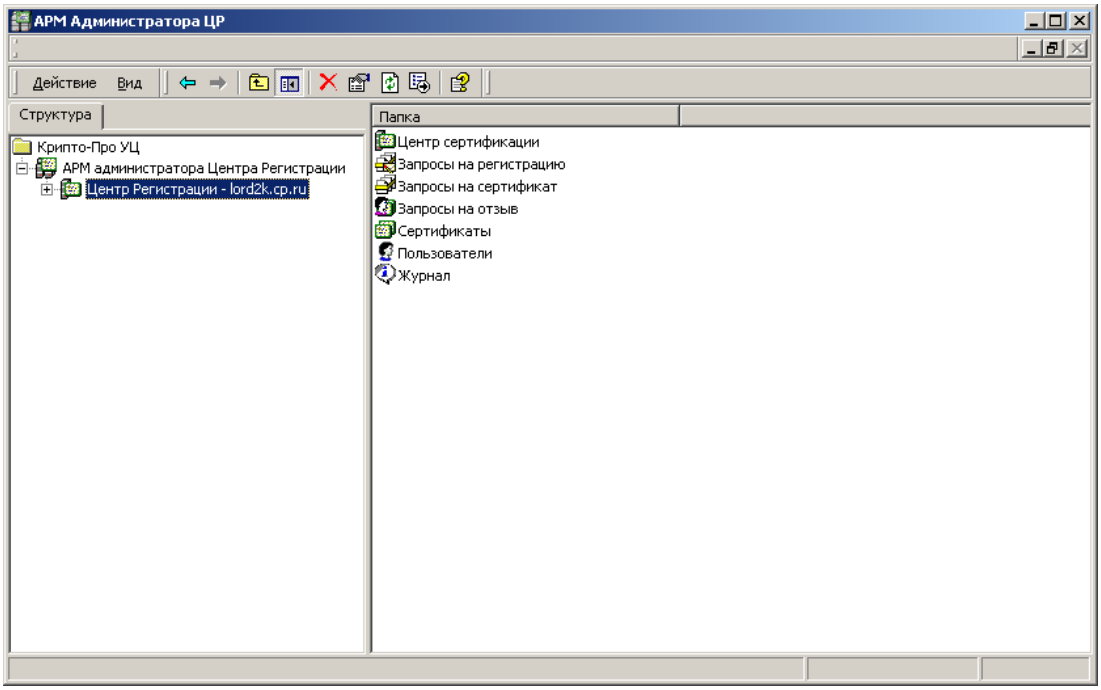
4.2. Запуск и интерфейс приложения АРМ администратора ЦР

4.2.1. Запуск и активация подключения к ЦР

Запуск приложения АРМ администратора осуществляется путем нажатия кнопки **Пуск** и выбора в меню **Программы** пункта **Крипто Про\АРМ Администратора ЦР**.

После открытия консоли АРМ администратора ЦР необходимо активизировать подключение к Центру Регистрации. Для этого нужно открыть ветку **АРМ администратора Центра Регистрации** в левой части консоли (дерево консоли) путем нажатия на крестик слева от строки и установить курсор (выделить подсветкой) на ветке подключения к ЦР (см. Рисунок 11).

Рисунок 11. Активизация подключения к ЦР в окне консоли АРМ администратора



В процессе активизации выполняется обращение к закрытому ключу администратора, соответствующему сертификату открытого ключа, выбранного для подключения. После этого выполняется аутентификация и авторизация администратора на Центре Регистрации. Данная процедура занимает от 5 секунд и больше в зависимости от качества канала связи. В случае если активизация подключения не может быть произведена (не может быть установлено соединение с ЦР), на экран будет выдано диагностическое сообщение. В случае успешного установления соединения слева от строки появиться крестик и список папок в правой части окна (см. Рисунок 11).

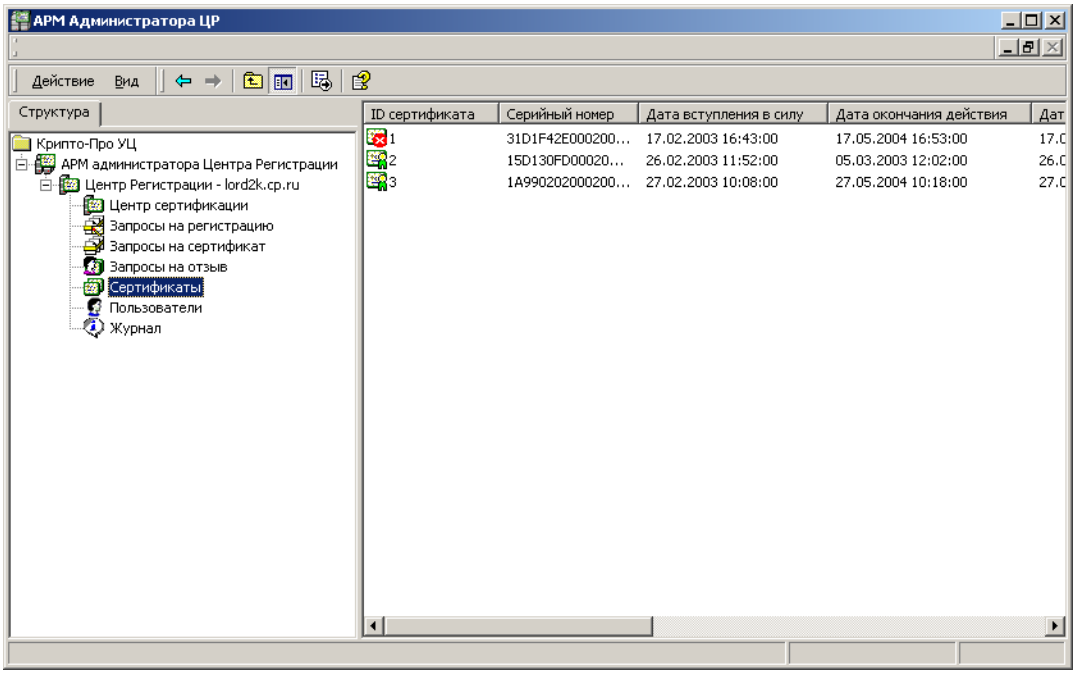
Открытие активированного подключения осуществляется путем нажатия на крестик слева от строки подключения к ЦР.

В том случае, если на консоли администратора создано несколько подключений, активировано может быть только одно из них. Активизация другого подключения приводит к деактивации предыдущего активного подключения к ЦР.

4.2.2. Просмотр содержимого активированного подключения

Содержимое активированного подключения представлено в виде списка папок. Активизация папки подключения происходит путем установки курсора на папку и появления содержимого папки в правой части окна (см. Рисунок 12).

Рисунок 12. Окно консоли администратора с активированными элементами дерева подключения

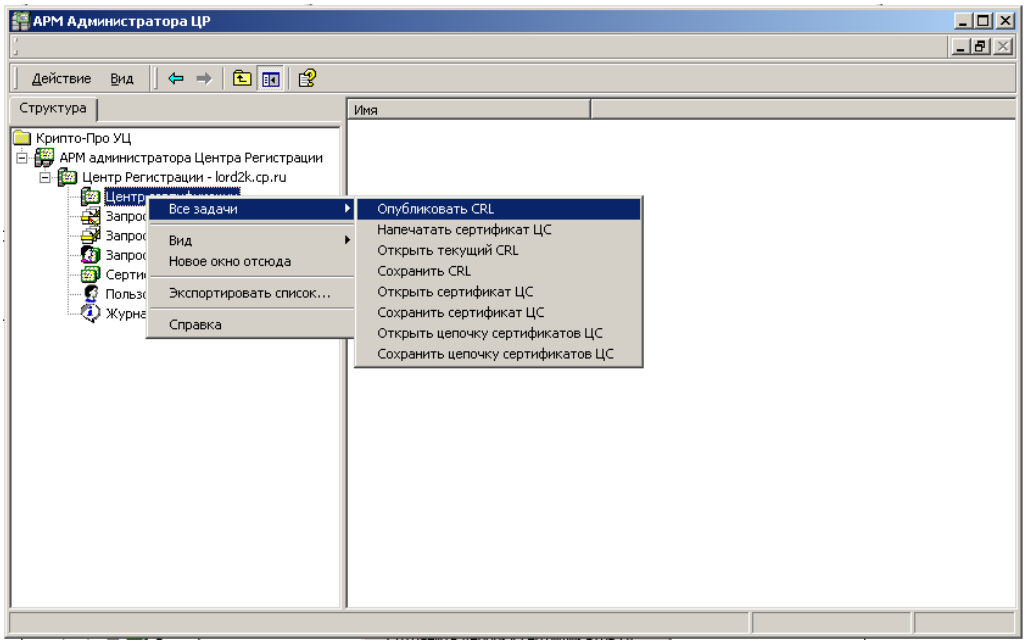


4.2.3. Контекстное меню папок и содержимого папок

Для каждой папки активированного подключения в левой части консоли или в списке содержимого папки в правой части окна существует контекстное меню, доступное по нажатию правой кнопки мыши после установки на него курсора.

Содержимое контекстного меню зависит от выбранной папки или элемента списка. Пример контекстного меню для элемента дерева **Центр Сертификации** приведен на Рисунок 13.

Рисунок 13. Пример контекстного меню в консоли администратора



Доступ к задачам (пункт меню **Все задачи**) возможен по пункту меню **Действие** консоли администратора.

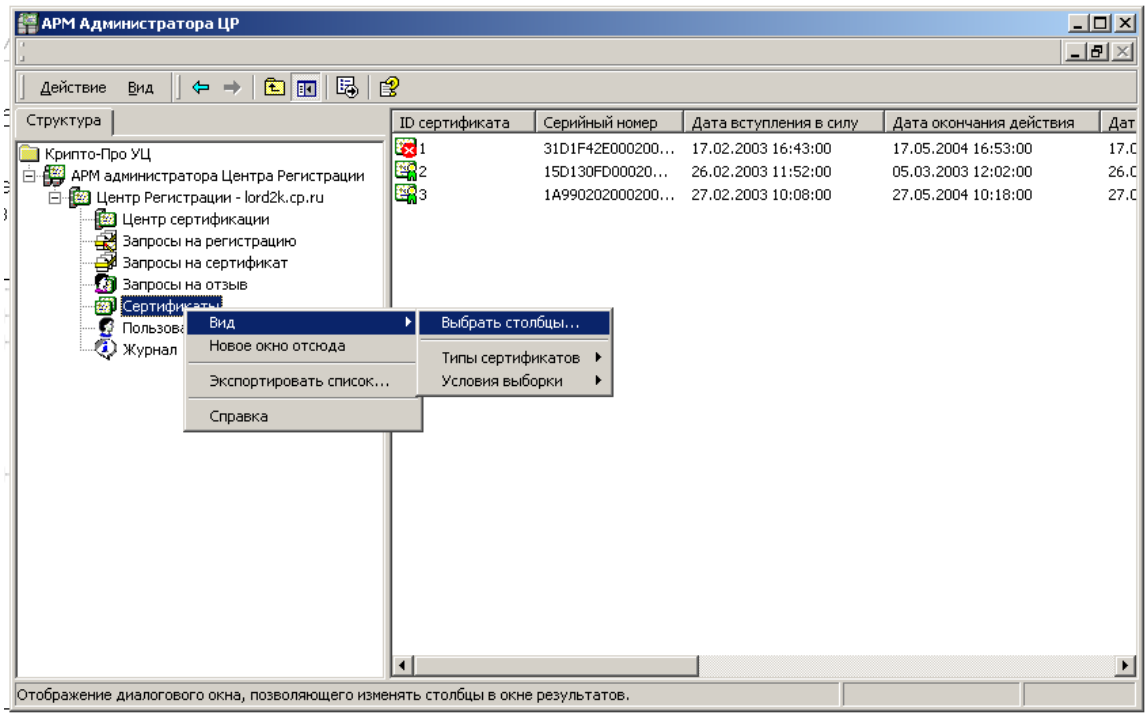
4.2.4. Управление отображением списка в правой части консоли

Содержимое папки, отображаемое в виде списка в правой части консоли, меняется в зависимости от выбранной папки в левой части консоли администратора.

Список представляет собой совокупность (таблицу) набора полей, отображающихся в списке (столбцов таблицы) и записей (строк таблицы).

АРМ администратора ЦР позволяет настраивать состав отображаемых полей для каждой папки. Для этого необходимо выбрать пункт **Вид/Выбрать столбцы** из контекстного меню элемента дерева (см. Рисунок 14).

Рисунок 14. Пункт меню настройки состава полей списка

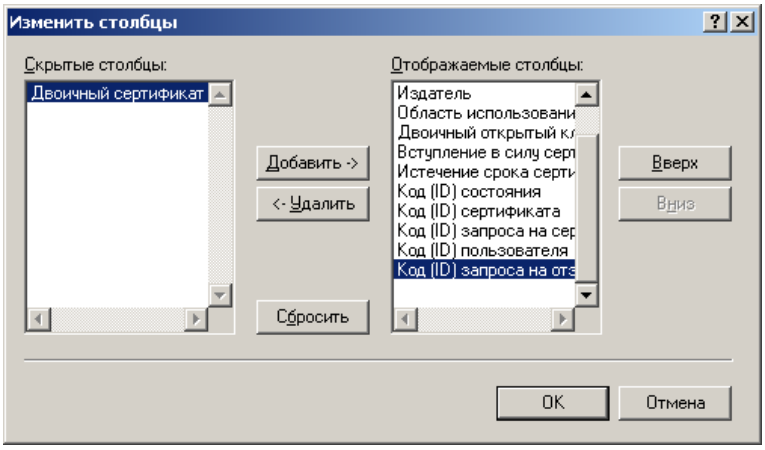


При выполнении данного пункта меню будет отображено диалоговое окно изменения состава полей, отображаемых для выбранной папки (см. Рисунок 15).

Данное окно содержит два списка: список скрытых полей (столбцов) и список отображаемых полей (столбцов).

Содержимое списков зависит от выбранной папки. По умолчанию все столбцы занесены в список отображаемых столбцов. Отказ от отображения столбца выполняется путем занесения его в список скрытых столбцов. Для этого необходимо установить курсор на нужной строке списка отображаемых столбцов и нажать кнопку Удалить. Обратная операция (отображение столбца) выполняется путем установки курсора на нужную строку в списке скрытых столбцов и нажатия кнопки Добавить.

Рисунок 15. Окно изменения состава полей списка содержимого папки



Кнопка **Сбросить** служит для отмены сделанных перемещений и приведения списков в состояние до начала редактирования списков.

Управление последовательностью отображения столбцов в списке осуществляется с использованием кнопок **Вверх** и **Вниз**.

4.2.5. Сортировка записей в списке консоли

Программное обеспечение АРМ администратора ЦР позволяет осуществлять сортировку записей (строк) списка в правой части консоли по возрастанию или убыванию значений выбранного столбца.

Сортировка осуществляется путем нажатия курсором на заголовок выбранного для сортировки столбца. Изменение направления сортировки осуществляется повторным нажатием курсора на заголовок столбца. Вершина треугольника, отображаемая в заголовке, указывает на направление сортировки.

4.2.6. Фильтрация записей в списке консоли

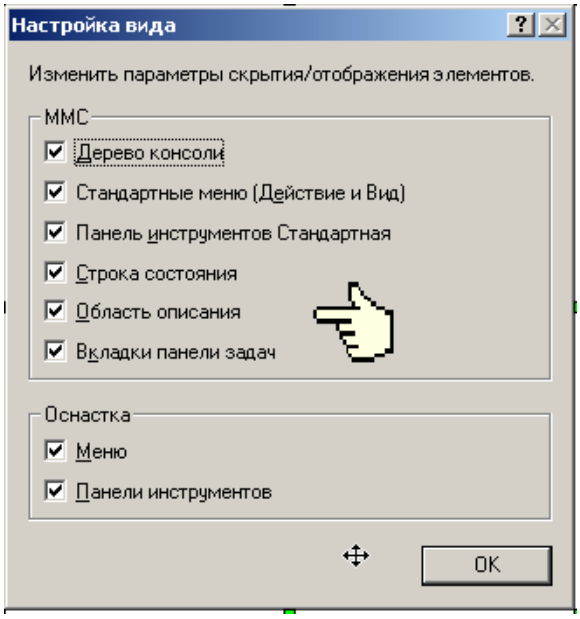
Программное обеспечение АРМ администратора позволяет работать не только со всем списком записей по содержимому папки в правой части консоли, но и с его подмножеством, построенным по разнообразным условиям (фильтрация записей).

4.2.6.1. Отображение области описания фильтрации записей в списке консоли

Для отображения условий выборки элементов списка консоли по фильтру необходимо произвести настройку области отображения. Для этого выберите пункт меню **Настроить** меню **Вид** консоли приложения.

В появившемся окне отметьте пункт **Область описания** (см. Рисунок 16).

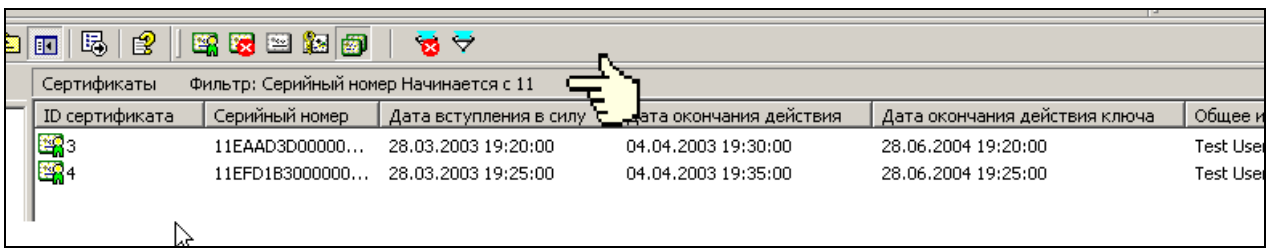
Рисунок 16. Настройка отображения области описания фильтрации записей



Закройте окно настройки.

После этого условие выборки будет отображаться в области отображения, расположенной над списком консоли (см. Рисунок 17).

Рисунок 17. Область отображения условий фильтрации



Настройка отображения области описания фильтрации записей в списке консоли установлена по умолчанию (действует после установки АРМ администратора ЦР), если используется консоль АРМ администратора ЦР, вызываемая из группы программ **Крипто-Про** (**Пуск/Программы/Крипто-Про/АРМ администратора ЦР**). Если создается персональная консоль с добавлением в нее оснастки **АРМ администратора Центра Регистрации ,** то для отображения значения фильтра выполните действия данного раздела документа.

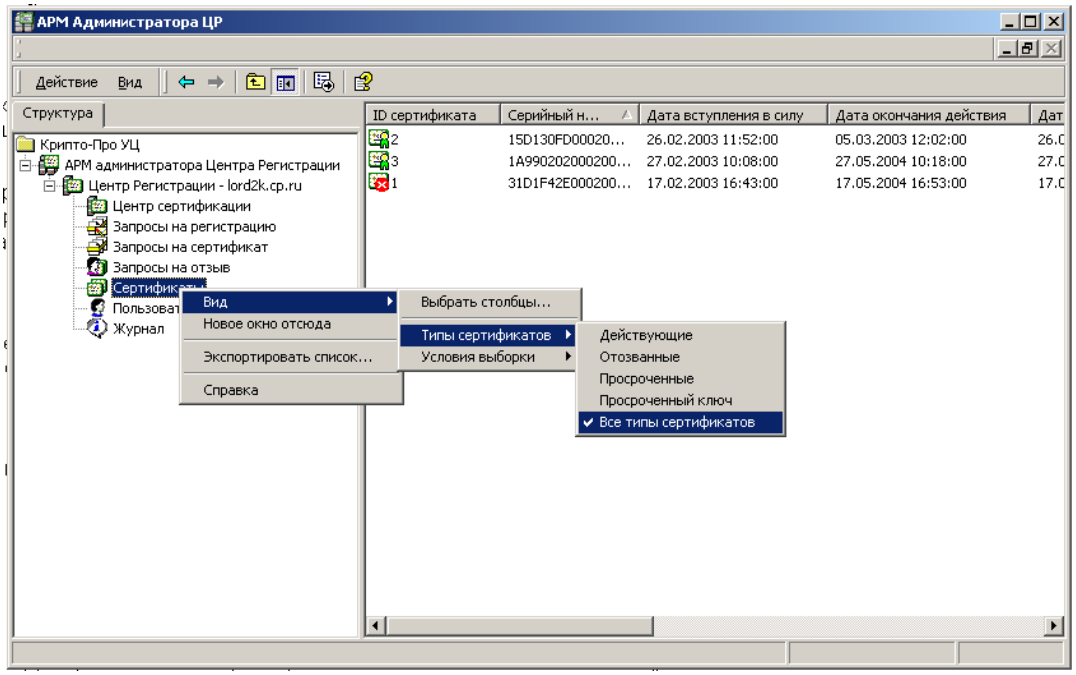
4.2.6.2. Фильтрация по типам записей

Фильтрация по типам записей, составляющих содержимое папки, применяется для следующих папок:

- Запросы на регистрацию;
- Запросы на сертификат;
- Запросы на отзыв;
- Сертификаты.

Для установления фильтра по типам записей необходимо из контекстного меню соответствующей папки выбрать пункт **Вид** и следующий пункт **Типы сертификатов** (см. Рисунок 18).

Рисунок 18. Окно выбора фильтрации записей по типу



По умолчанию установлен режим без фильтрации (все типы записей).

Установленные настройки по фильтрации для каждой папки сохраняются и будут актуальны при следующем сеансе работы с АРМ администратора ЦР.

4.2.6.3. Фильтрация по значениям полей записей

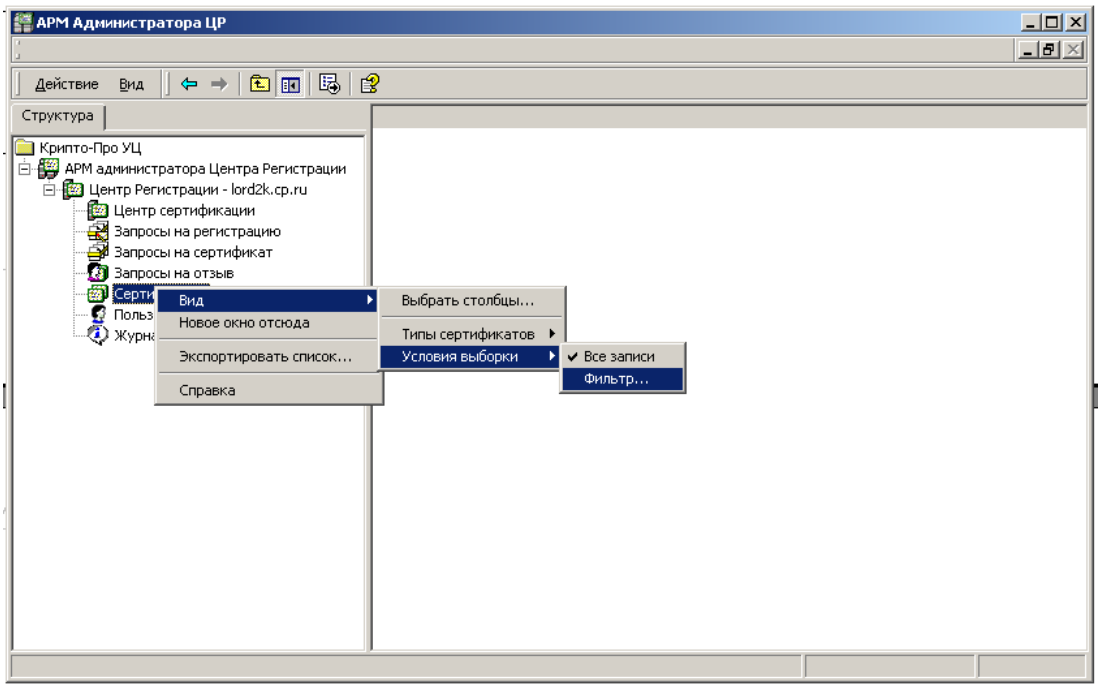
Фильтрация по значениям полей записей, составляющих содержимое папки, применяется для следующих папок:

- Запросы на регистрацию;
- Запросы на сертификат;

- Запросы на отзыв;
- Сертификаты;
- Пользователи.

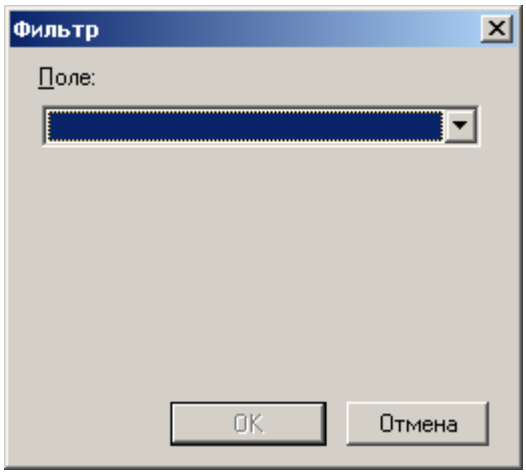
Для установления фильтра по типам записей необходимо из контекстного меню соответствующей папки выбрать пункт **Вид**, пункт **Условия выборки** и следующий пункт **Фильтр** (см. Рисунок 19).

Рисунок 19. Окно выбора фильтрации записей по значениям полей



После выполнения данного пункта контекстного меню будет отображено диалоговое окно определения поля записи для фильтрации (см. Рисунок 20).

Рисунок 20. Окно выбора поля для фильтрации по значению полей записей



В этом окне выпадающий список полей зависит от папки, к которой фильтрация применяется.

По умолчанию режим фильтрации по значениям полей не установлен.

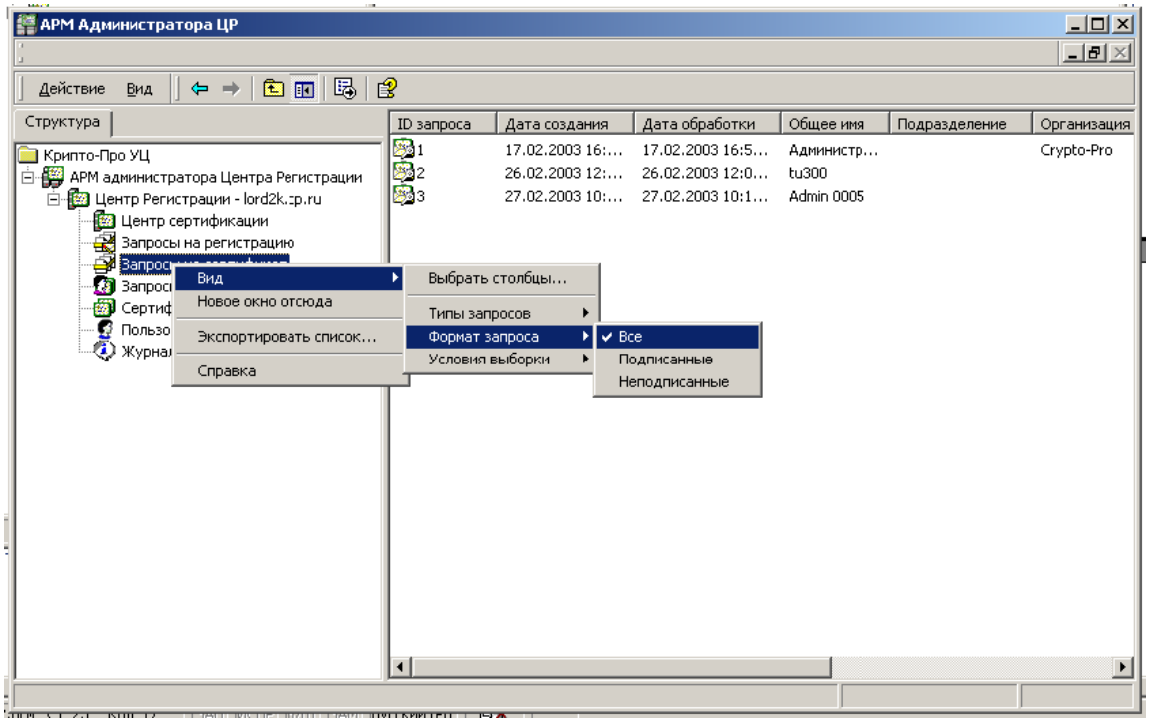
Данный режим фильтрации удобен к применению при большом количестве записей в папке. Его применение значительно сократит время получения и отображения информации по объектам управления Центра Регистрации.

4.2.6.4. Фильтрация по подписи запросов на сертификат

Для содержимого папки **Запросы на сертификат** может быть применен индивидуальный тип фильтрации по признаку *подписан*/*неподписан*.

Для установления фильтра по подписи запросов на сертификат необходимо из контекстного меню папки **Запросы на сертификат** выбрать пункт **Вид**, пункт **Формат запросов** (см. Рисунок 21).

Рисунок 21. Окно выбора фильтрации запросов на сертификат по признаку подписания



По умолчанию режим фильтрации запросов на сертификат по признаку подписания не установлен.

4.2.7. Просмотр свойств элементов управления

Объекты управления Центра Регистрации (см. раздел ☐) имеют свойства, просмотр которых доступен на консоли администратора.

Каждый элемент управления отображается в списке содержимого папки в виде набора полей. Значения полей просматриваются в списке. Для прокрутки списка полей используется ползунок, расположенный внизу окна списка полей.

Другие свойства элементов управления можно просмотреть с помощью окна свойств записи. Для этого используется контекстное меню консоли администратора.

С помощью пункта **Свойства** контекстного меню просматриваются:

- запросы на регистрацию;
- запросы на сертификат;
- запросы на отзыв (приостановление/возобновление действия) сертификата;
- пользователи;
- сертификаты.

Альтернативным способом просмотра объектов управления является двойное нажатие левой кнопки «мыши».

Примеры окон свойств объектов управления Центра Регистрации приведены на Рисунках 16 - 20:

Рисунок 22. Окно свойств запроса на сертификат

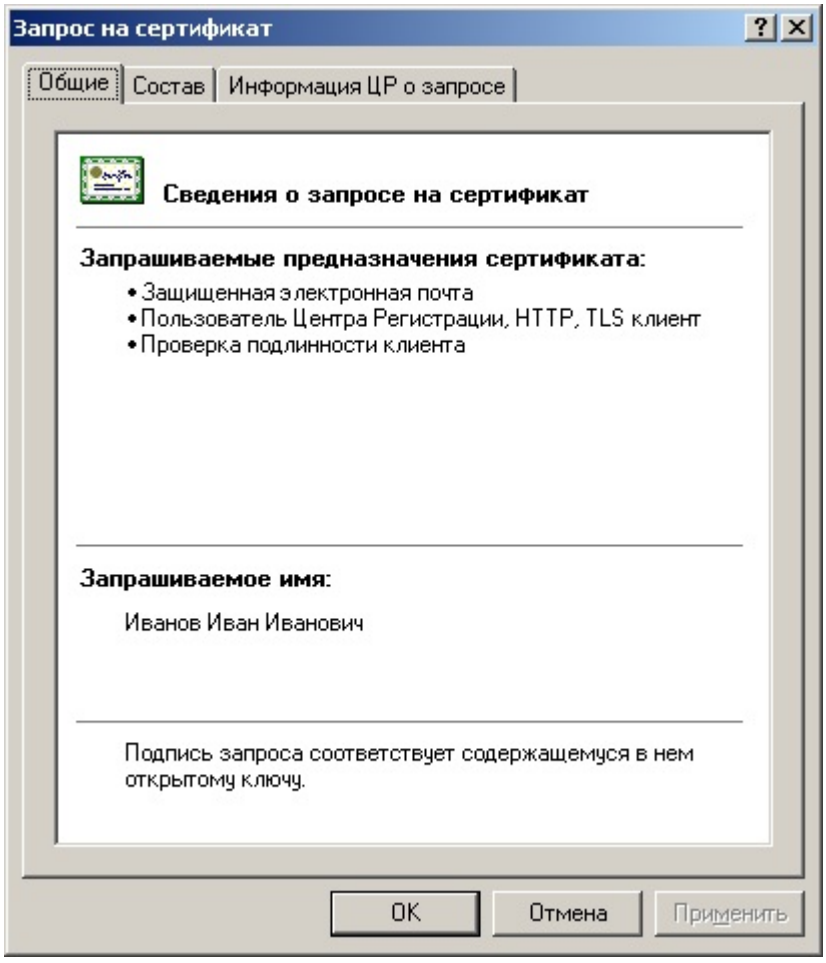


Рисунок 23. Окно свойств запроса на регистрацию

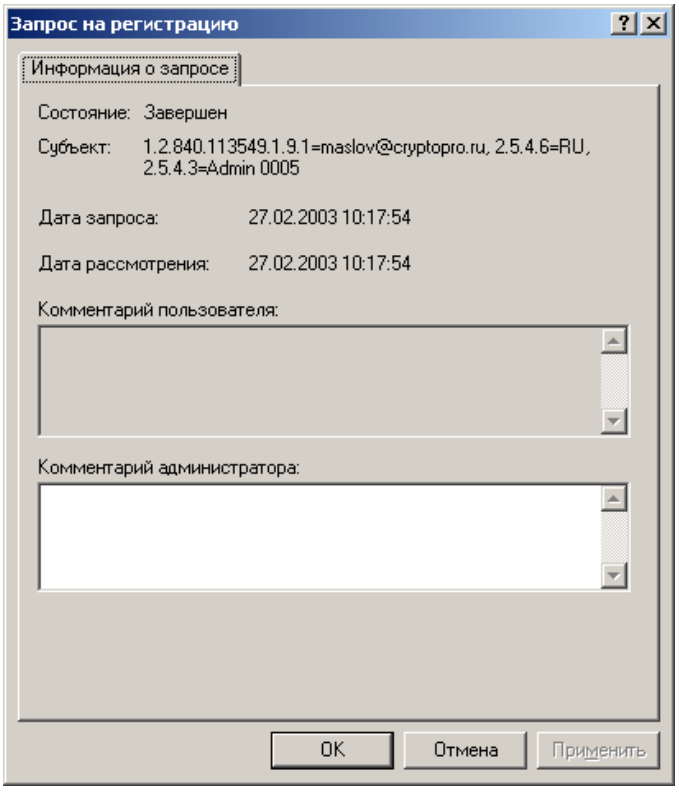


Рисунок 24. Окно свойств запроса на отзыв сертификата

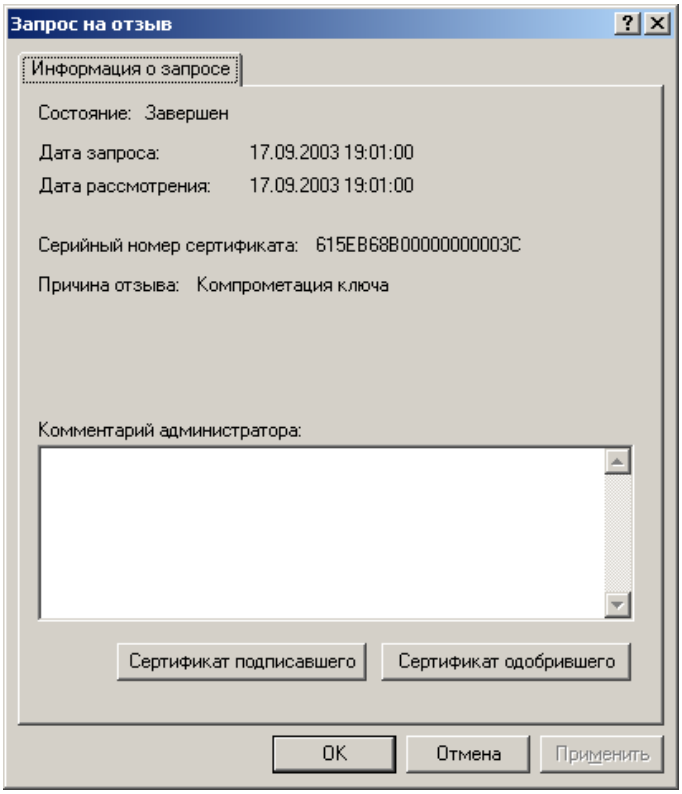


Рисунок 25. Окно свойств запроса на приостановление действия сертификата

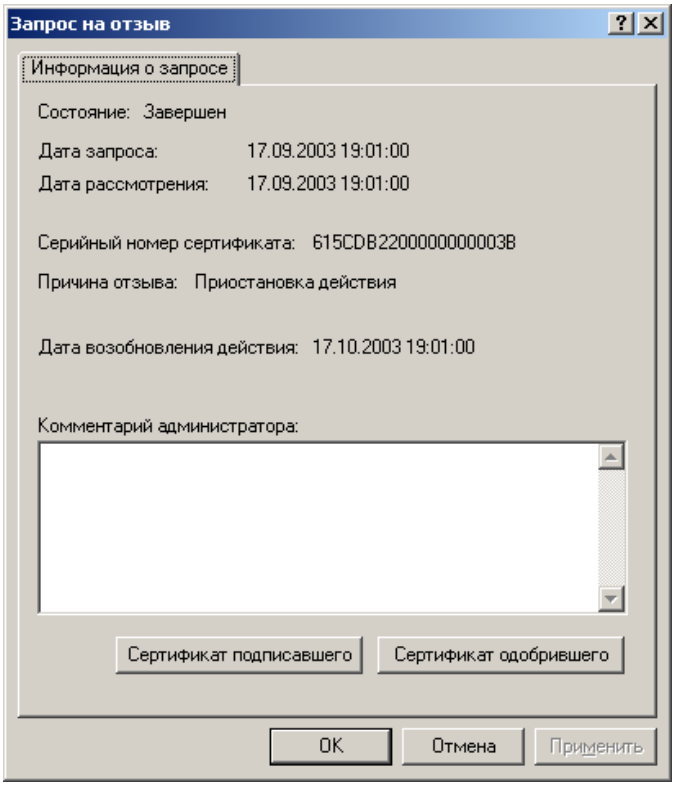
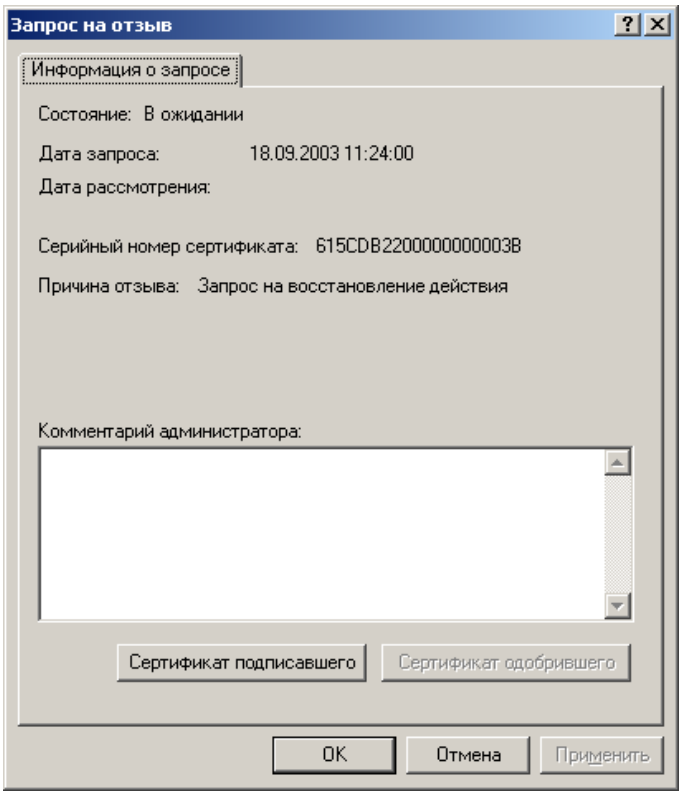


Рисунок 26. Окно свойств запроса на возобновление действия сертификата



4.2.8. Групповые операции над объектами

Программное обеспечение АРМ администратора ЦР поддерживает выполнение задач над группами объектов управления (записей) соответствующих папок.

Перечень задач, поддерживающих групповое выполнение операций над объектами, приведен в Таблица 1.

Таблица 1. Таблица допустимых задач, поддерживающих выполнение групповых операций

Наименование папки	Тип	Задачи узла, поддерживающие выполнение групповых операций
Запросы на регистрацию	Запросы ожидающие	Принять Отклонить
Запросы на сертификат	Запросы ожидающие	Принять Отклонить Экспортировать
	Запросы одобренные	Подтвердить Экспортировать
	Запросы отклоненные	Экспортировать
	Запросы подтвержденные	Экспортировать
Запросы на отзыв	Запросы ожидающие	Принять Отклонить Экспортировать
	Запросы одобренные	Экспортировать

	Запросы отклоненные	Экспортировать
Сертификаты	Все типы	Экспортировать
	Действующие	Отозвать Приостановить действие Экспортировать
	Отозванные	Возобновить действие (приостановленные - код 6) Экспортировать

Для выполнения групповой операции над объектами (записями) необходимо с помощью мыши и клавиш **Shift** и **Ctrl** на клавиатуре выделить группу записей, и, выбрав задачу из контекстного меню, выполнить ее.

Для групповой обработки необходимо выбирать только те записи, которые отображаются в текущей части списка окна. Если для выбора записей необходимо сделать вертикальную прокрутку списка, то выполните задачу в два или несколько приемов.

4.2.9. Предоставление информации о пользователе по объекту управления, связанному с ним

Программное обеспечение АРМ администратора ЦР позволяет произвести поиск пользователя по объекту управления, связанному с этим пользователем.

Данная операция применима к следующим объектам управления: запрос на сертификат, сертификат открытого ключа, запрос на отзыв сертификата.

Для получения информации о пользователе необходимо выделить правой кнопкой мыши объект управления и в открывшемся контекстном меню выбрать **Все задачи/Перейти к пользователю** (см. Рисунок 27). Откроется окно, содержащее учетную запись пользователя, связанного с объектом управления (см. Рисунок 28).

Рисунок 27. Поиск пользователя по объекту управления

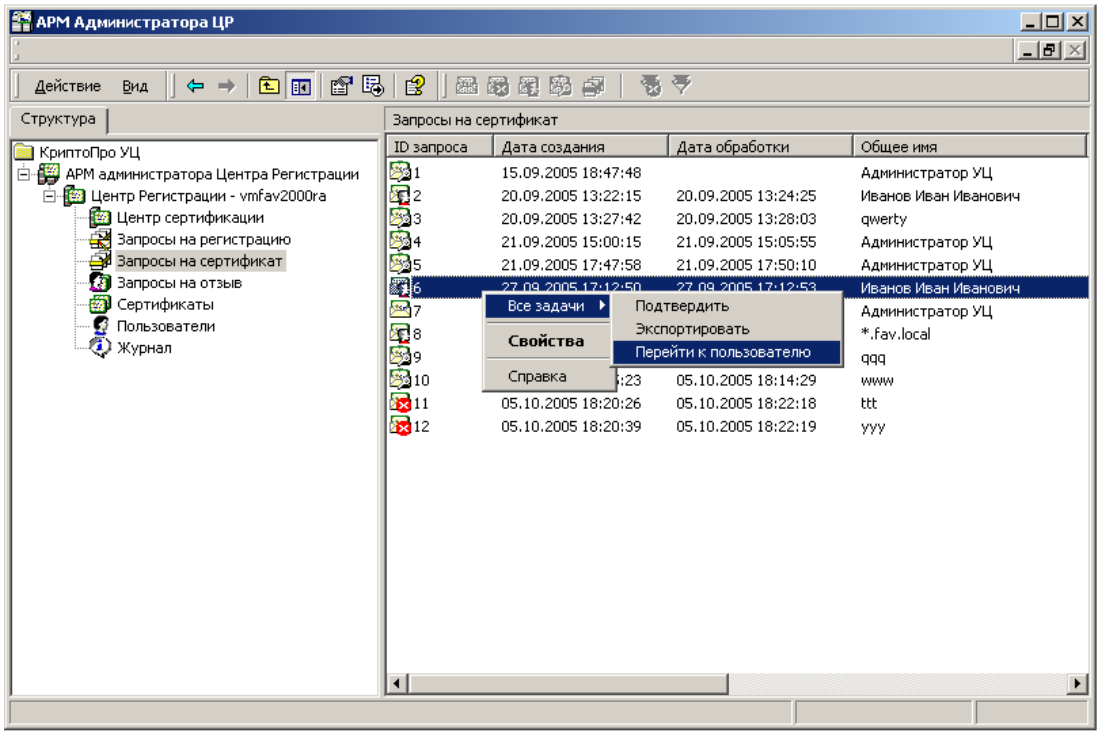
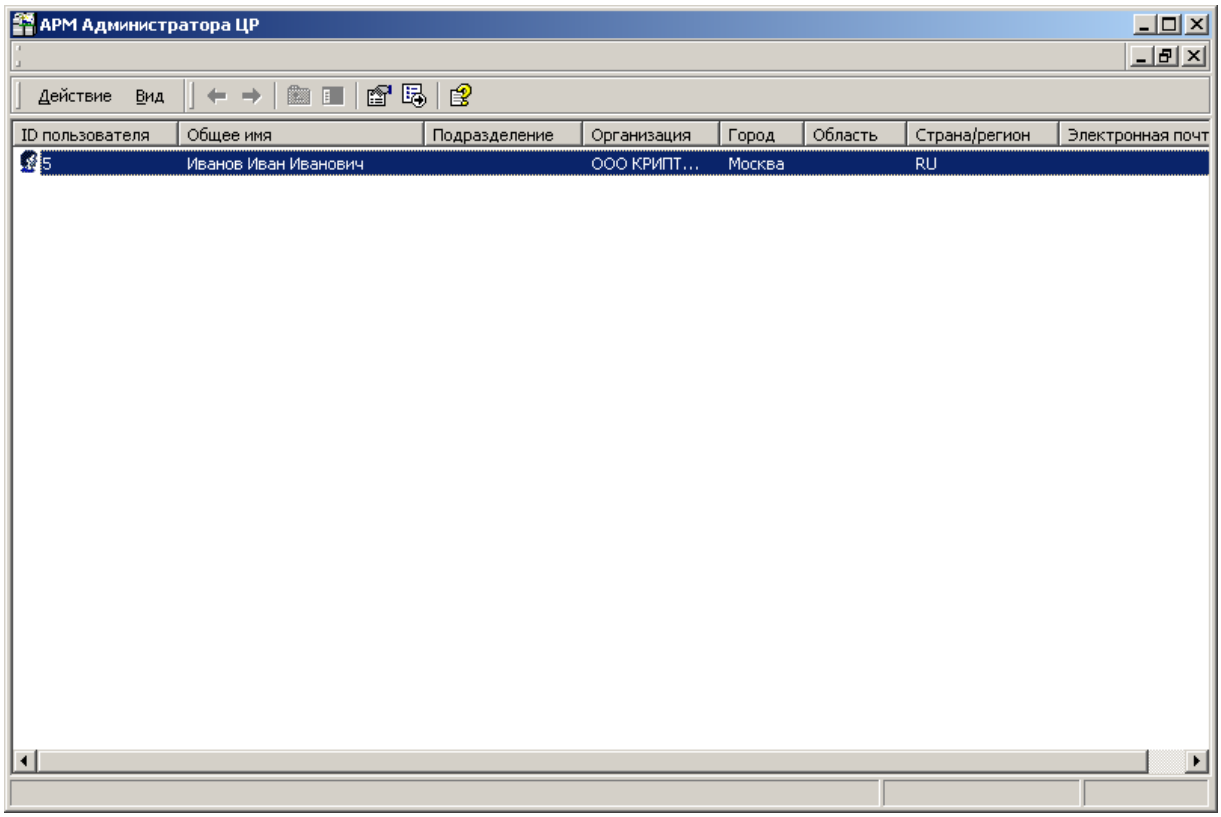


Рисунок 28. Отображение записи пользователя по объекту управления



5. Смена ключей и сертификата администратора

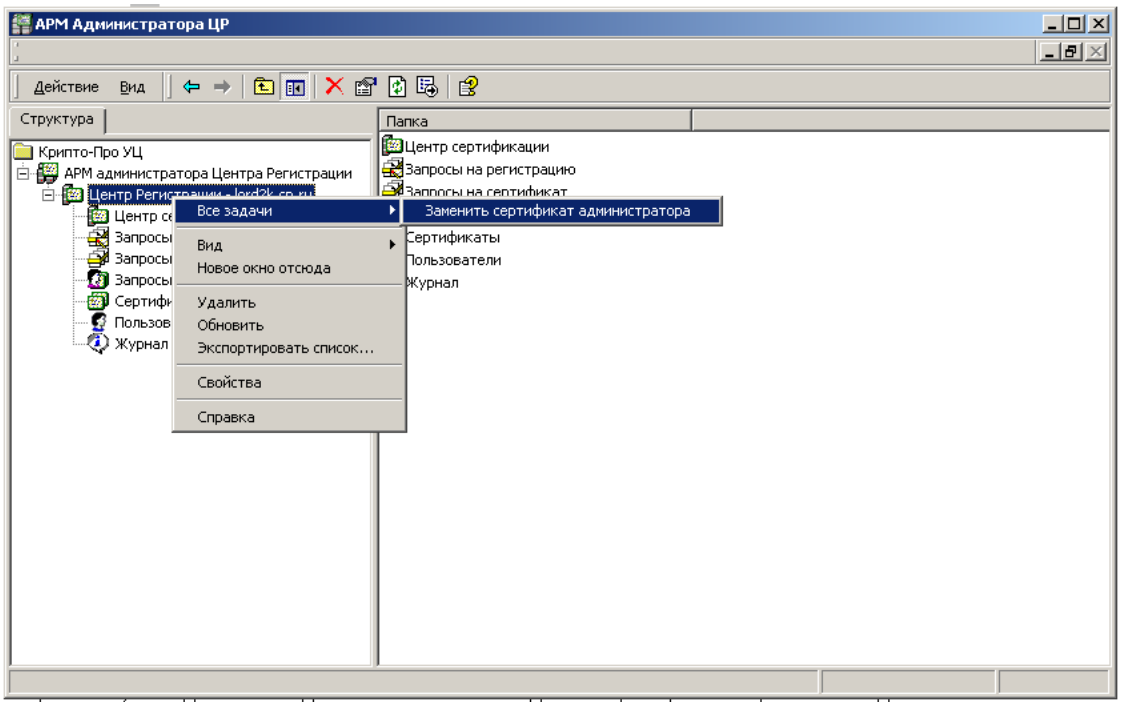
Ключи и сертификаты администратора обеспечивают аутентификацию и авторизацию на Центре Регистрации Удостоверяющего Центра.

Плановая смена ключей администратора производится в соответствии с регламентом, определенном в руководящих документах организации.

Регламент Удостоверяющего Центра – основной документ Удостоверяющего Центра, определяющий порядок регистрации пользователей в Удостоверяющем Центре, изготовление и управление сертификатами ключей подписей.

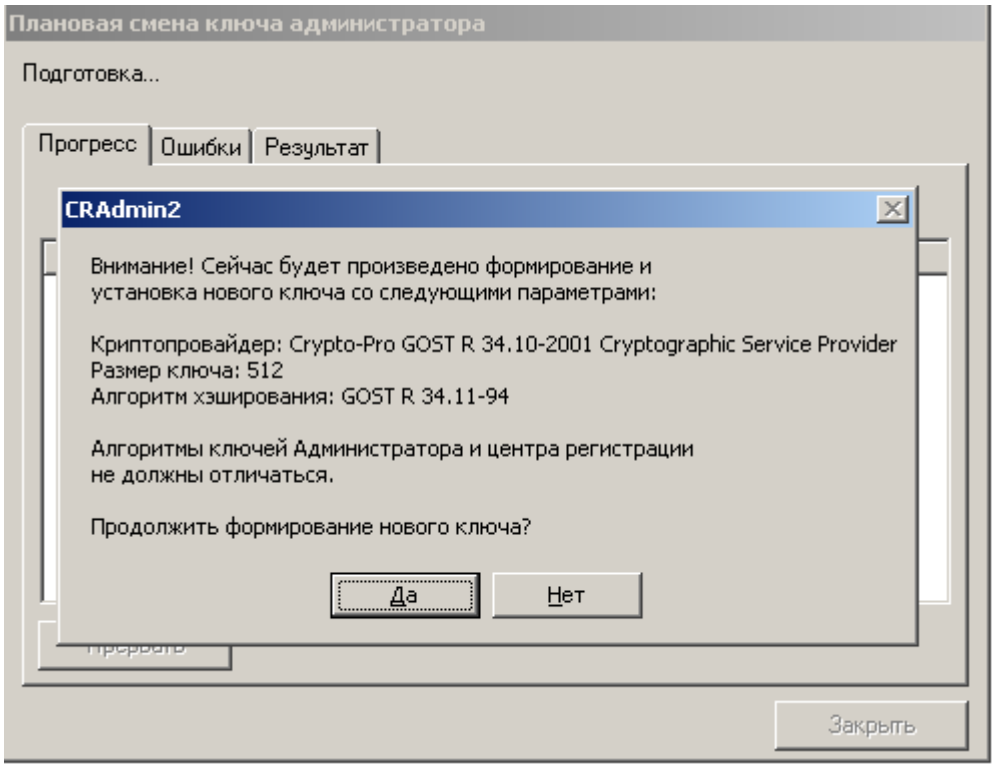
Плановая смена ключей администратора и изготовление сертификата открытого ключа производится с использованием задачи **Заменить сертификат администратора**, доступной в контекстном меню ветки (подключения) **Центр Регистрации** консоли администратора (см. Рисунок 29).

Рисунок 29. Задача плановой смены ключа администратора



При запуске данной задачи на консоли АРМ администратора ЦР отображается диалоговое окно приглашения на выполнение задачи плановой смены ключа администратора (см. Рисунок 30).

Рисунок 30. Окно приглашения задачи плановой смены ключа администратора

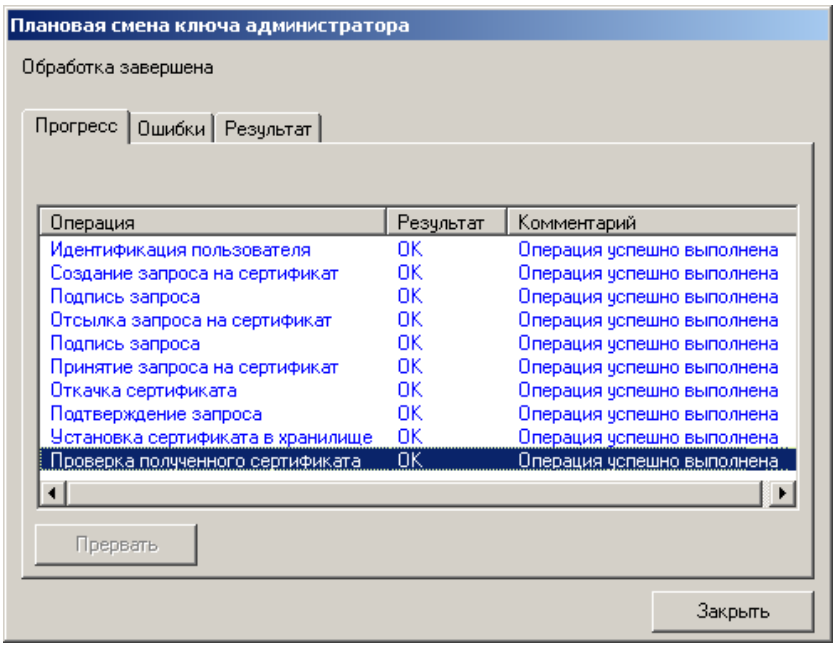


После нажатия кнопки **Да** происходит:

- генерация ключей;
- запись ключей на ключевой носитель;
- формирование и отправка запроса на новый сертификат администратора;
- получение выпущенного сертификата и установка на компьютере рабочего места администратора;
- деактивация подключения к ЦР;
- изменение параметра подключения к ЦР в части сертификата для аутентификации.

Успешное завершение задачи сопровождается отображением соответствующего окна (см. Рисунок 31).

Рисунок 31. Окно завершения задачи плановой смены ключа администратора



Внеплановая смена ключей администратора выполняется в соответствии с порядком, определенном регламентом Удостоверяющего Центра.

6. Регистрация пользователей Центра Регистрации

Под регистрацией пользователей понимается процедура идентификации пользователей и занесение учетной информации в реестр пользователей Удостоверяющего Центра.

Программное обеспечение Удостоверяющего Центра поддерживает следующие режимы регистрации пользователей:

- Централизованный режим;
- Распределенный режим.

Использование режимов определяется регламентом Удостоверяющего Центра и настройками параметров Центра Регистрации.

6.1. Централизованный режим

АРМ администратора обеспечивает технические мероприятия процедуры регистрации пользователей и выдачи первых ключей и сертификатов, заключающиеся в выполнении следующих процедур:

- ввод учетной информации, заносимой в сертификаты открытых ключей регистрируемого пользователя и создание учетной записи по регистрируемому пользователю в базе данных Центра Регистрации;
- генерации ключей регистрируемого пользователя и запись их на ключевой носитель;
- формирование запроса на регистрацию пользователя и его автоматическое принятие администратором, выполняющим процедуру регистрации;
- формирование запроса на сертификат открытого ключа;
- ввод дополнительной учетной информации, не заносимой в сертификаты открытого ключа;
- сохранение выпущенного сертификата на магнитный носитель в виде цепочки сертификатов, включающей сертификат корневого ЦС;
- сохранение на магнитном носителе списка отозванных сертификатов (CRL).

6.2. Распределенный режим

АРМ администратора обеспечивает технические мероприятия процедуры регистрации пользователей в распределенном режиме, заключающиеся в выполнении следующих процедур:

- обработке запроса на регистрацию пользователя;
- обработке запроса на сертификат открытого ключа регистрируемого пользователя.

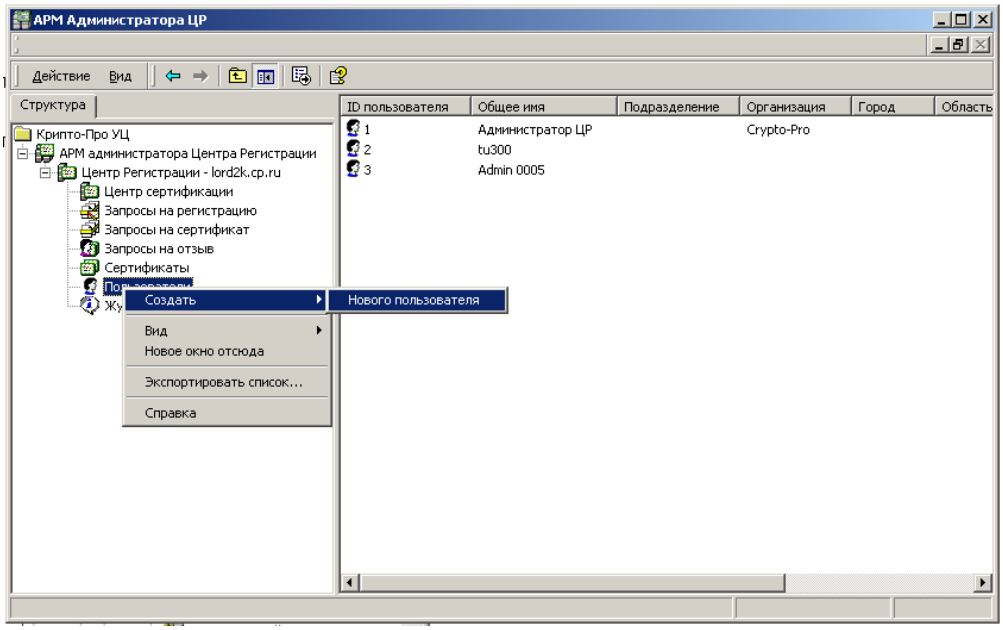
При регистрации пользователя в распределенном режиме используются организационные мероприятия, связанные с пересылкой пользователем посредством почтовой и курьерской связи документов в бумажной форме, являющихся основанием для регистрации пользователя и изготовления сертификата.

6.3. Мастер регистрации пользователей

Выполнение процедур регистрации в централизованном режиме выполняется с помощью Мастера регистрации пользователя.

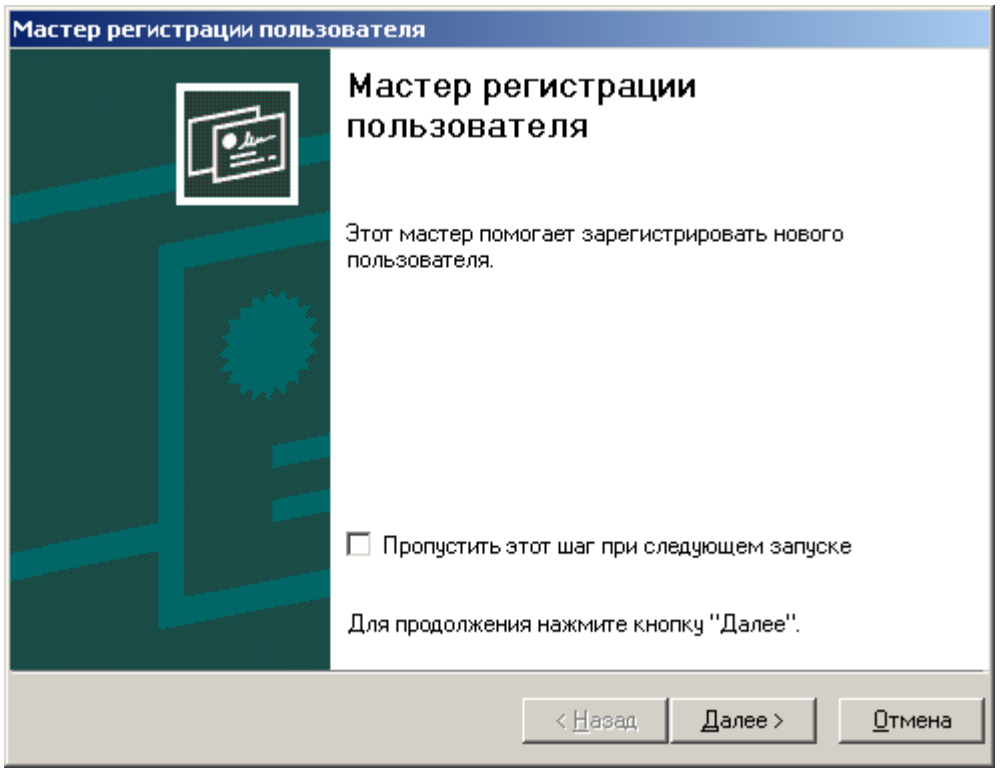
Запуск Мастера осуществляется путем выполнения задачи **Создать/Нового пользователя** в контекстном меню папки **Пользователи** (см. Рисунок 32).

Рисунок 32. Запуск задачи создания нового пользователя



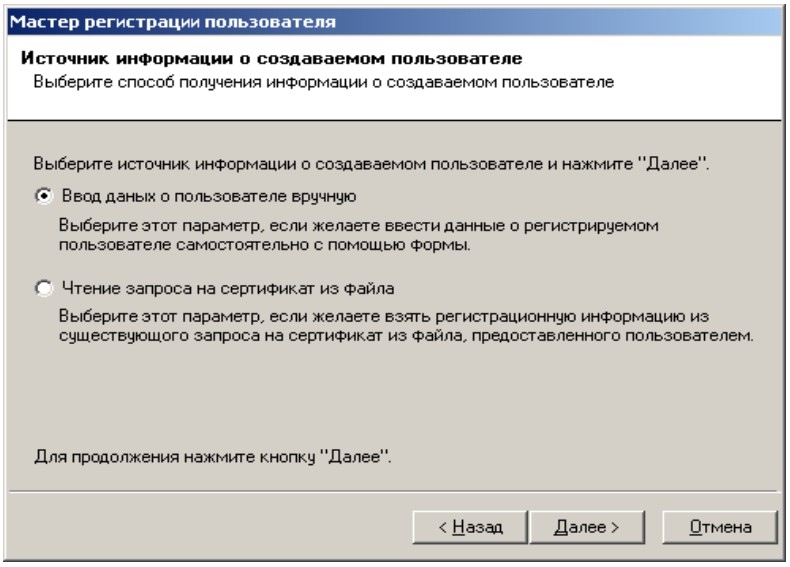
После запуска **Мастера регистрации** пользователя на экране отображается стартовое окно **Мастера** (Рисунок 33). Для отключения вывода данного окна при последующих запусках **Мастера** установите переключатель **Пропустить этот шаг при следующем запуске.** Нажмите кнопку **Далее.**

Рисунок 33. Стартовое окно мастера регистрации пользователя



Откроется окно выбора источника информации о создаваемом пользователе (см. Рисунок 34).

Рисунок 34. Окно определения источника запроса на сертификат в Мастере регистрации пользователя



Выбор пункта **Ввод данных о пользователе вручную** означает выполнение процедуры регистрации пользователя с вводом идентификационных данных пользователя администратором.

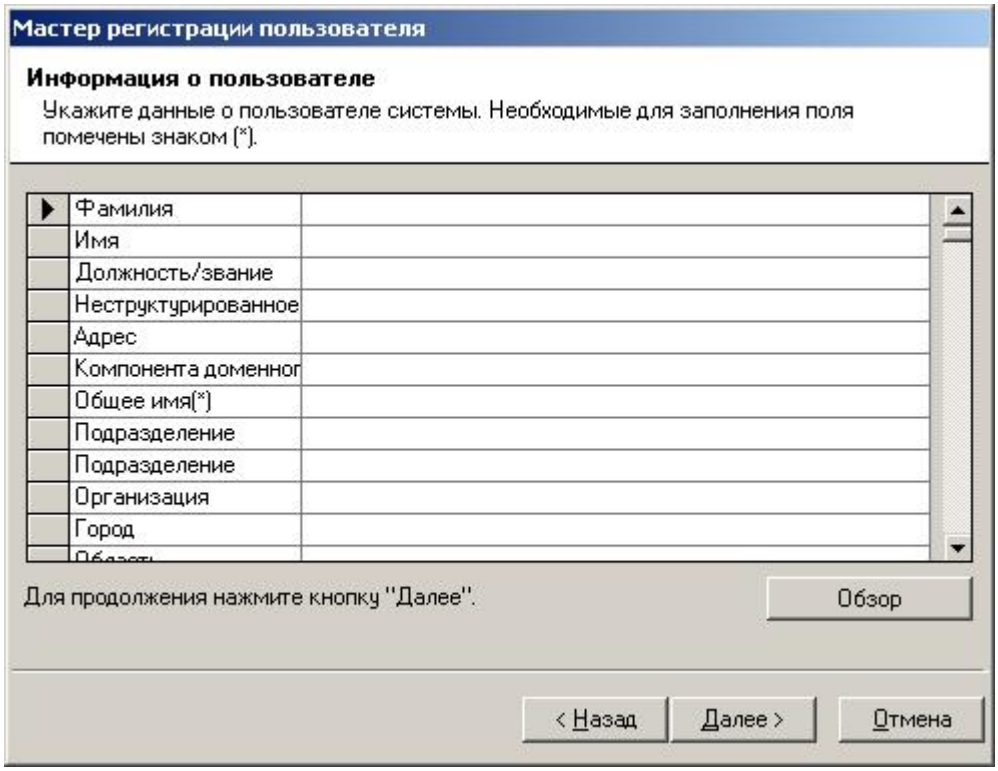
Выбор пункта **Чтение запроса на сертификат из файла** означает выполнение процедуры регистрации пользователя без изготовления ключей пользователя на рабочем месте администратора. Т.е. должен быть заранее подготовлен запрос на сертификат, удовлетворяющий требованиям политики имен и области использования ключей.

6.3.1. Работа Мастера регистрации пользователя при выборе опции **Ввод данных о пользователе вручную**

В случае выбора пункта **Ввод данных о пользователе вручную** отображается окно определения идентификационных данных регистрирующегося пользователя (см. Рисунок 35).

Если компьютер, на котором работает АРМ администратора, входит в домен, то становится активной кнопка Обзор, позволяющая выбрать пользователя Active Directory (AD) и автоматически заполнить значения полей создаваемого пользователя ЦР сведениями из AD.

Рисунок 35. Окно ввода информации о пользователе Мастера регистрации пользователя



Переход между полями идентификационных данных осуществляется с помощью левой кнопки мыши.

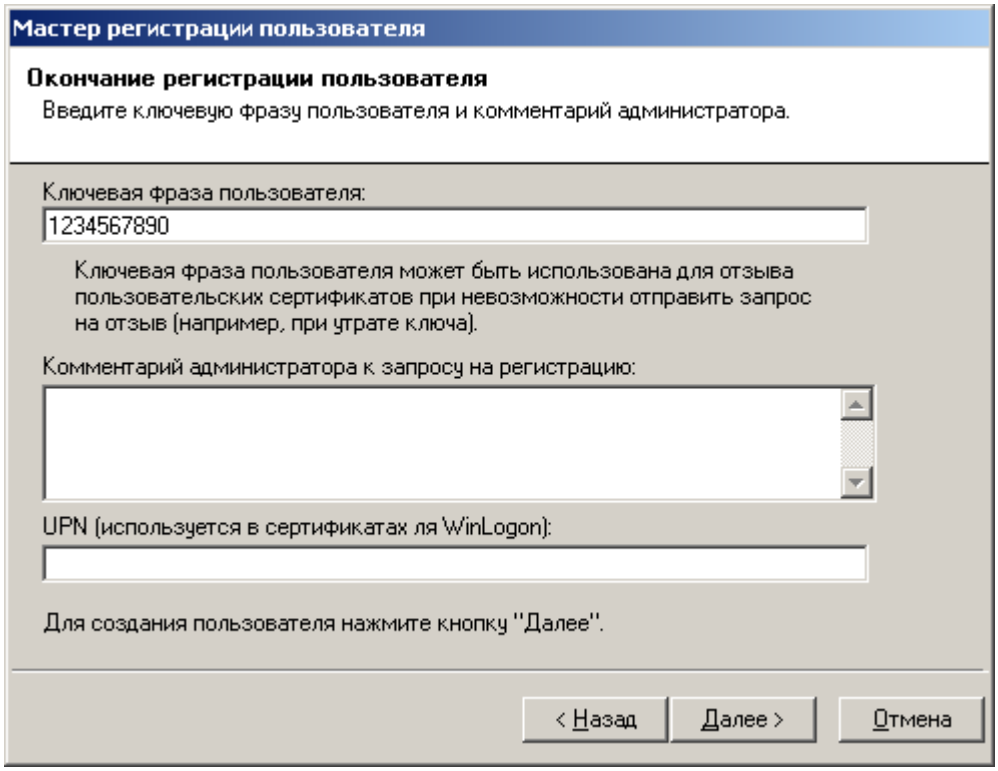
Состав полей, идентифицирующих пользователя на Центре Регистрации, зависит от настроек ПО Центра Регистрации (см. «КриптоПро УЦ. Центр Регистрации. Руководство по эксплуатации» пункт 2.2). Значения данных полей будут заноситься во все последующие сертификаты пользователя в качестве идентификационных данных владельца сертификата (поле Subject (Субъект) сертификата). Данная информация для зарегистрированного пользователя является постоянной и не подлежит изменению.

Если значения полей заполняются автоматически (при выборе пользователя из AD), то будут заполнены только те поля, которые разрешены в настройках Политики имен на Центре Регистрации. При этом, если в Политике имен на Центре Регистрации в свойствах какого-либо компонента имени заданное количество разрешенных компонентов имени больше 1, то информация из AD будет помещена в первое из одноимённых полей. В примере на Рисунке 29 имеется два компонента «Подразделение». Если у пользователя AD заполнен компонент «ou», то первое поле «Подразделение» получит значение из AD, а второе останется незаполненным.

В следующем окне **Мастера регистрации пользователя** (Рисунок 36) введите **Ключевую фразу** пользователя и, при необходимости, **Комментарий администратора** к запросу на регистрацию. Поле **UPN (используется в сертификатах для WinLogon)** необходимо для занесения доменного имени пользователя (в формате «имя пользователя домена@имя домена», например, user1@mydomain.ru) в сертификаты открытых ключей в расширение **Дополнительное имя субъекта**. Такие сертификаты используются для аутентификации пользователя в домене на основе сертификатов открытых ключей – Smart Card Winlogon.

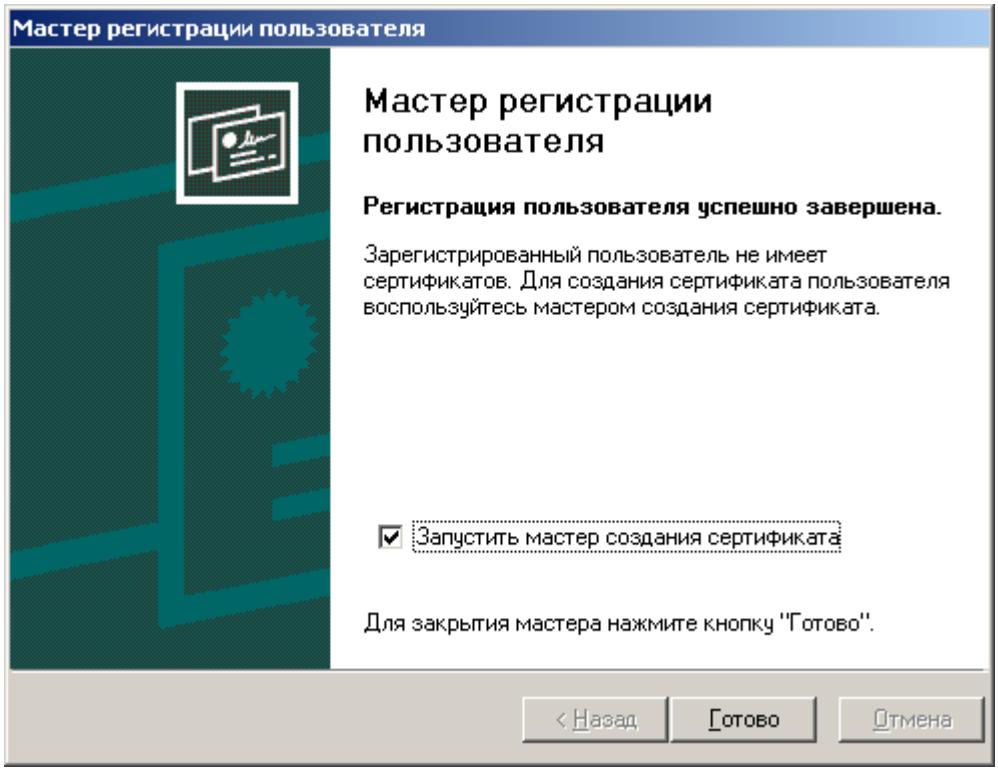
При выборе пользователя из AD поле UPN будет заполнено автоматически.

Рисунок 36. Задание ключевой фразы, комментария администратора и имени UPN при регистрации пользователя



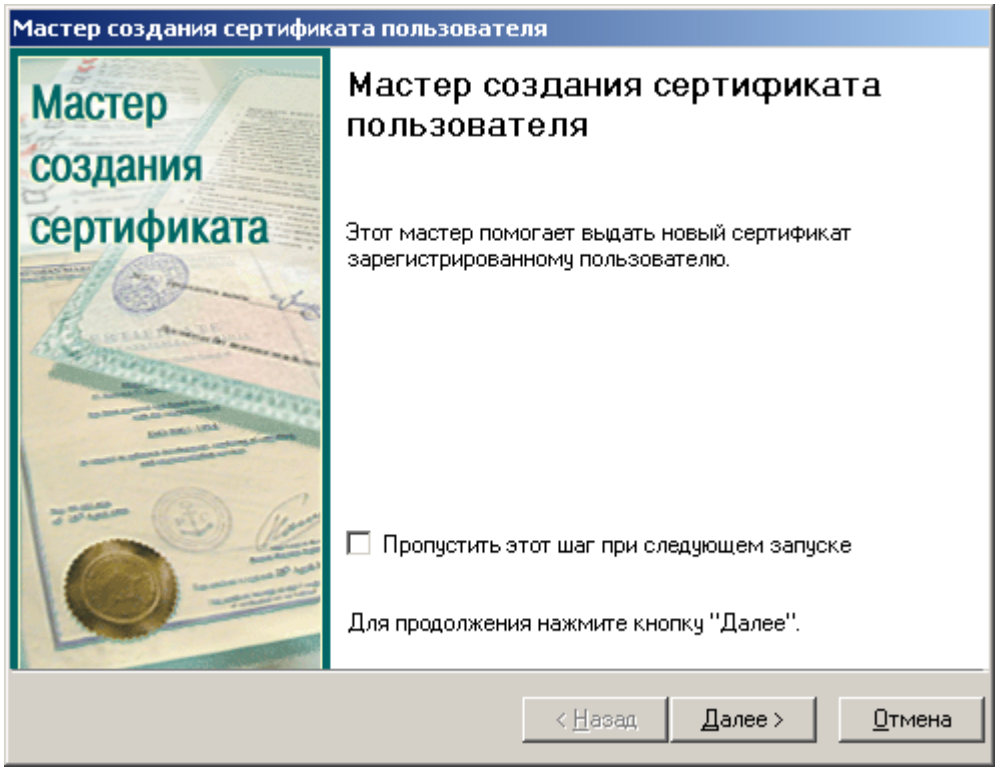
После ввода необходимых параметров нажмите кнопку **Далее**, появится завершающее окно **Мастера регистрации пользователя** (Рисунок 37). Установите в нем переключатель – **Запустить мастер создания сертификата**.

Рисунок 37. Завершающее окно Мастера регистрации пользователя



Откроется стартовое окно **Мастера создания сертификата** (см. Рисунок 38). Для отключения вывода данного окна при последующем запуске **Мастера** установите переключатель **Пропустить этот шаг при следующем запуске.** Нажмите кнопку **Далее.**

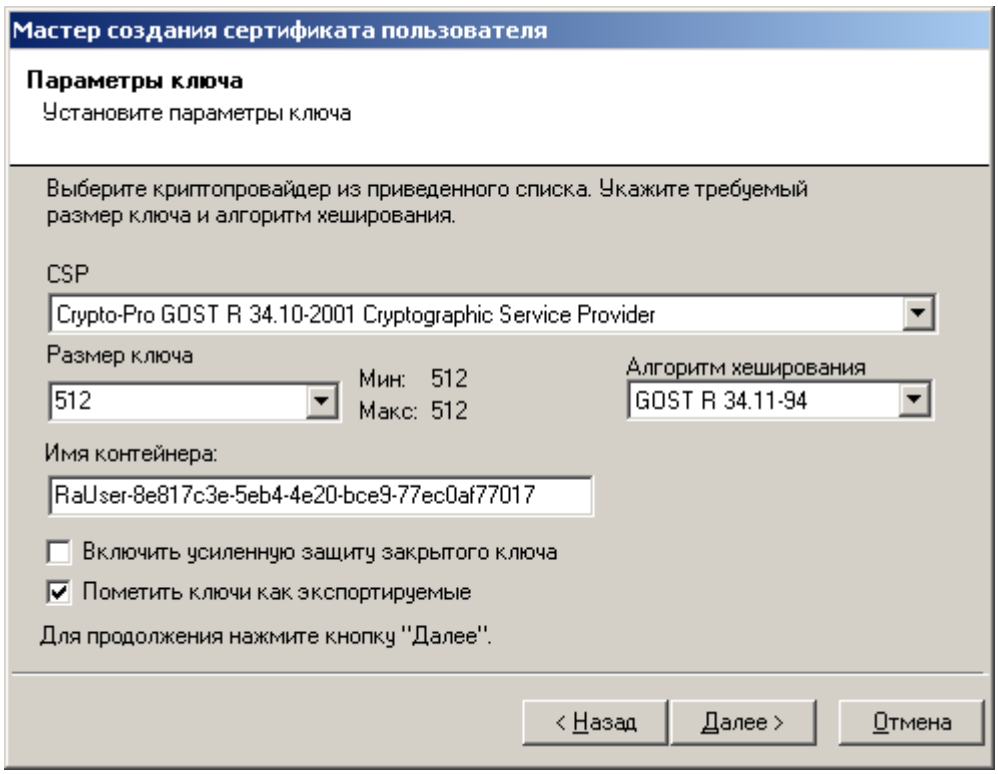
Рисунок 38. Стартовое окно Мастера создания сертификата



Запустится **Мастер создания сертификата** и в окне **Источник запроса на сертификат** выберите – **Генерация нового запроса на сертификат.**

В зависимости от настройки АРМ администратора ЦР (окно **Свойства: АРМ администратора Центра Регистрации**) в части выбора криптопровайдера (флаг **Разрешить выбор CSP**), следующим окном может быть диалоговое окно настройки параметров ключа (см. Рисунок 39).

Рисунок 39. Окно установки параметров генерации ключей Мастера создания сертификата

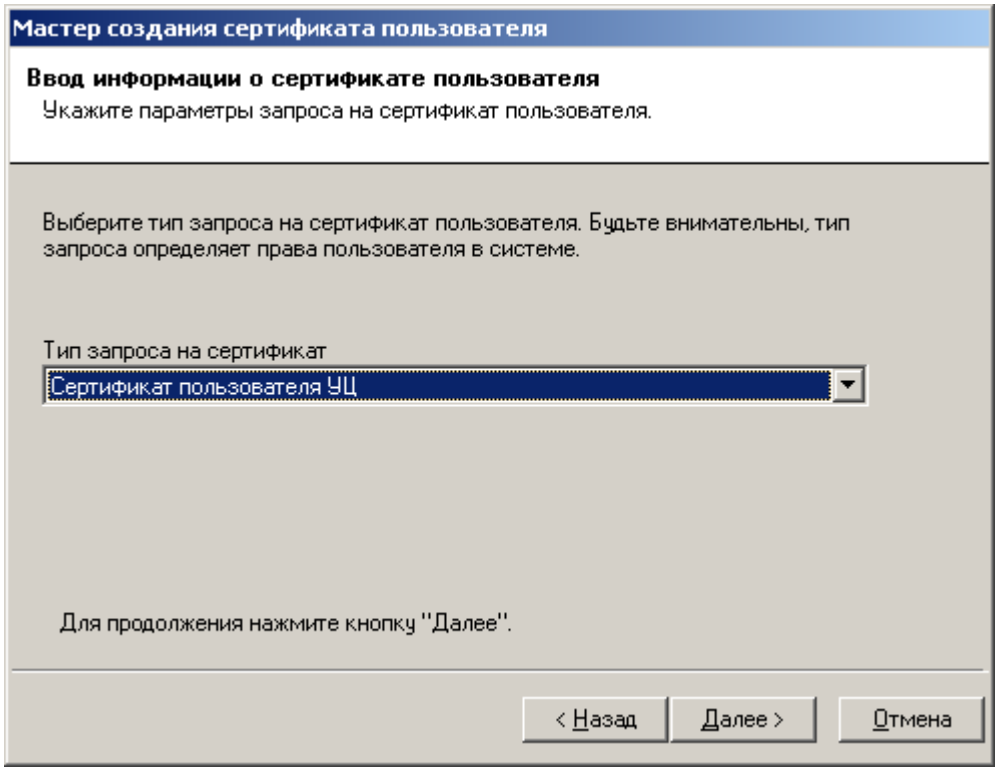


В том случае, если в настройках АРМ администратора ЦР (окно **Свойства: АРМ администратора Центра Регистрации**) установлен флаг **Запрашивать имя контейнера,** в окне установки параметров генерации ключа (см. Рисунок 39) поле «Имя контейнера» можно редактировать. Введите новое имя контейнера или оставьте предлагаемое по умолчанию.

Имя контейнера не должно содержать служебные символы: кавычки, слэши, апострофы и т.д. и не должно превышать 63 символов.

Следующим окном **Мастера** является окно определения типа сертификата (см. Рисунок 40).

Рисунок 40. Окно определения типа сертификата Мастера создания сертификата



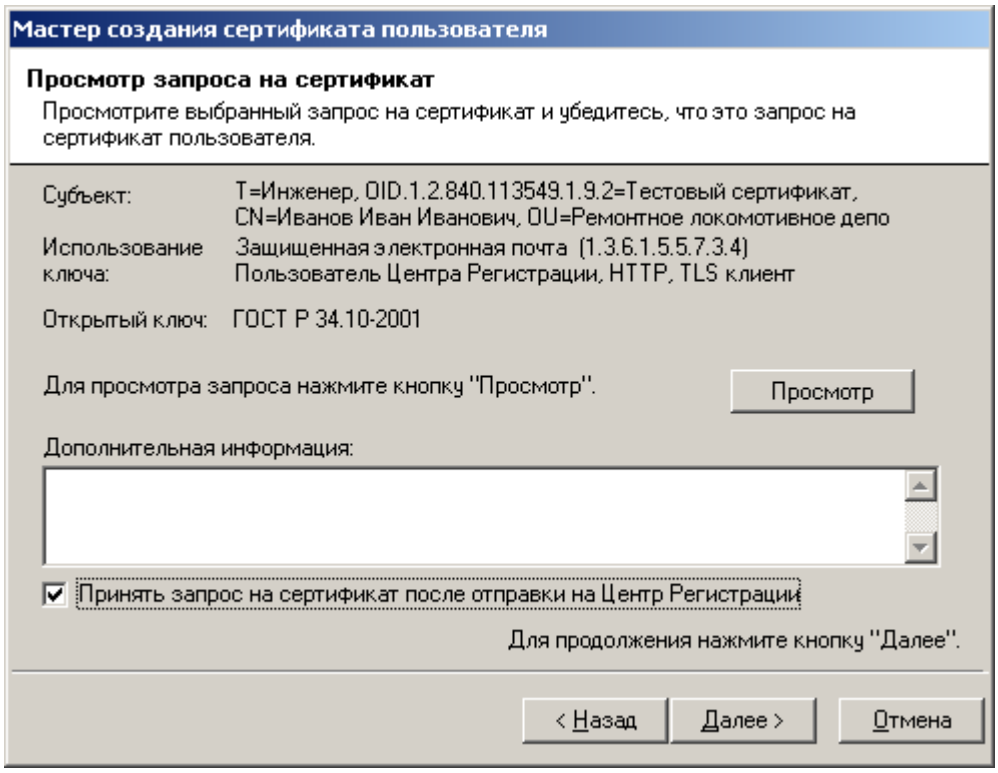
Тип сертификата (состав атрибутов расширения области применения сертификата) выбирается на основе шаблона на сертификат. Список шаблонов редактируется на Центре Регистрации.

После определения типа сертификата и задания имени контейнера (если такое окно появляется) выполняется генерация ключей, запись ключевой информации на ключевой носитель и формирование запроса на сертификат.

В следующем окне **Мастера** (см. Рисунок 41) необходимо проверить правильность указанных данных и, при необходимости, ввести дополнительную информацию о запросе. Данная информация сохраняется в базе данных Центра Регистрации, но не включается в выпускаемые сертификаты пользователя.

Если снять пометку «Принять запрос на сертификат после отправки на Центр Регистрации», то запрос на сертификат будет помещён на ЦР в очередь необработанных запросов.

Рисунок 41. Окно запроса на сертификат Мастера создания сертификата



Установка выпущенного сертификата в контейнер закрытого ключа (флаг **Установить сертификат в контейнер секретного ключа**) выполняется для технического обеспечения процедуры записи сертификата внутрь ключевого контейнера, расположенного на ключевом носителе, и последующей установки сертификата на рабочем месте пользователя. Данная опция возможна только для криптопровайдеров (CSP), обеспечивающих ее реализацию. К таким CSP относится СКЗИ «КриптоПро CSP».

Установка флага **Установить сертификат в хранилище** произведет установку сертификата со связкой с закрытым ключом в хранилище **Текущий пользователь/Другие пользователи/Сертификаты**. Использование данного флага позволит произвести последующий экспорт сертификата и соответствующего закрытого ключа в файл формата PKCS#12, при формировании ключей с использованием криптопровайдеров, поддерживающих хранение закрытых ключей только на жестком диске компьютера (например, Microsoft Base Cryptographic Provider, Microsoft Enhanced Cryptographic Provider и т.д.).

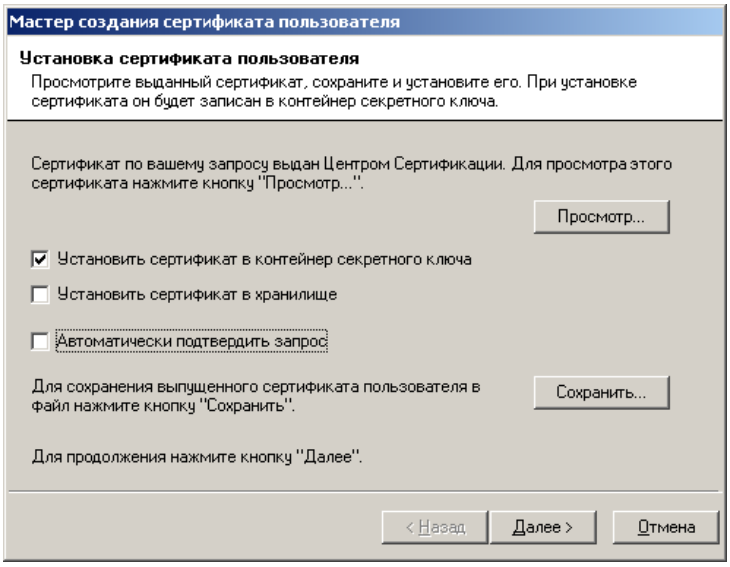
СКЗИ «КриптоПро CSP» не поддерживает экспорт сертификата и соответствующего закрытого ключа в файл формата PKCS#12.

Нажатие кнопки **Сохранить** позволяет сохранить изданный сертификат в виде файла.

Установка флага **Автоматически подтвердить запрос** произведет установку запроса на сертификат в состояние **Подтвержденный**.

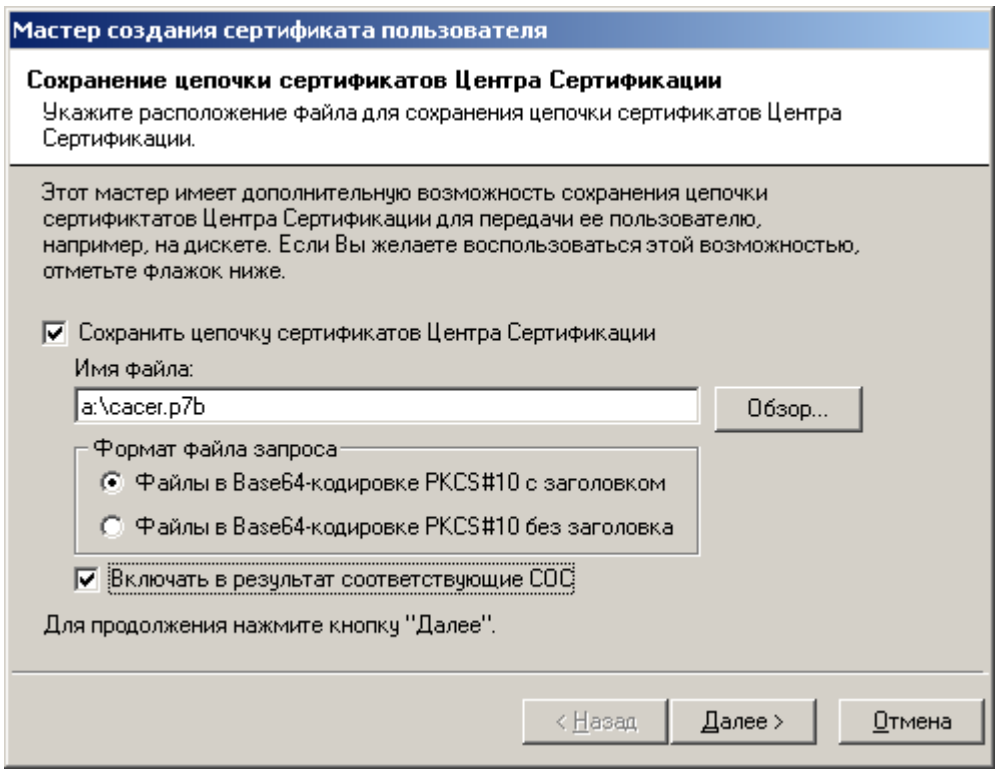
Определение указанных параметров осуществляется в окне **Установка сертификата пользователя** (см. Рисунок 42).

Рисунок 42. Окно установки выпущенного сертификата Мастера создания сертификата



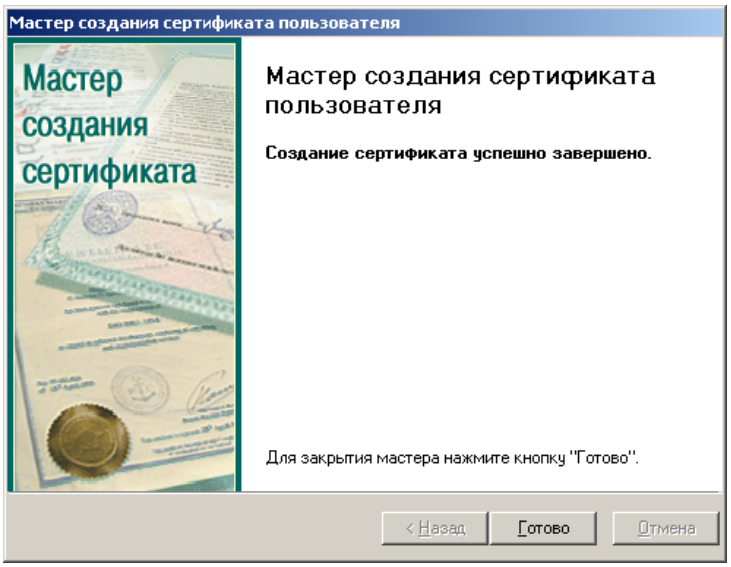
В следующем окне **Мастера** возможно сохранить цепочку сертификатов и список отозванных сертификатов в виде файла на магнитном носителе (см. Рисунок 43).

Рисунок 43. Окно сохранения цепочки сертификатов Мастера создания сертификата



Подтверждение успешной регистрации пользователя сопровождается соответствующим заключительным окном **Мастера** (см. Рисунок 44).

Рисунок 44. Заключительное окно работы Мастера создания сертификата

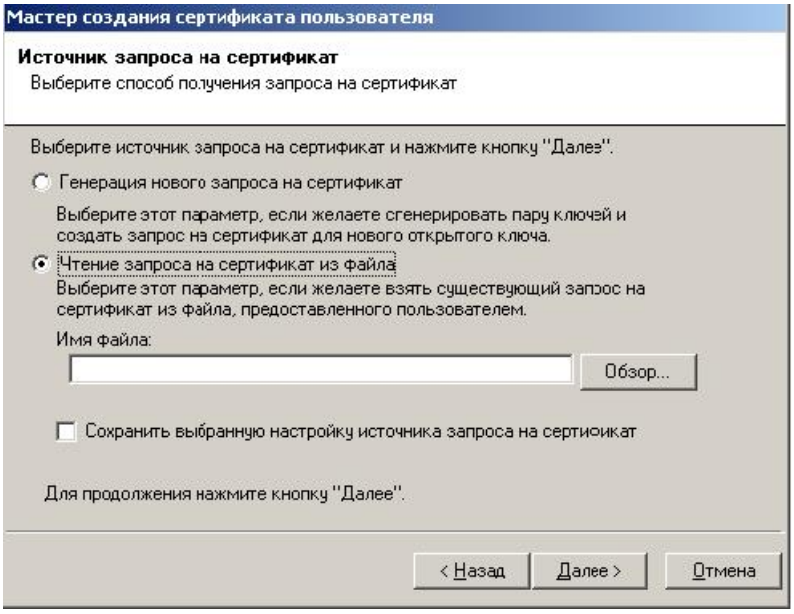


6.3.2. Работа Мастера регистрации пользователя при выборе опции **Чтение запроса на сертификат из файла**

В случае выбора пункта **Чтение запроса на сертификат из файла** окно расширяется полем ввода имени и расположения файла, содержащего запрос на сертификат регистрируемого пользователя (см. Рисунок 45).

Для выбора файла можно воспользоваться кнопкой **Обзор**.

Рисунок 45. Окно выбора файла с запросом на сертификат Мастера регистрации пользователя

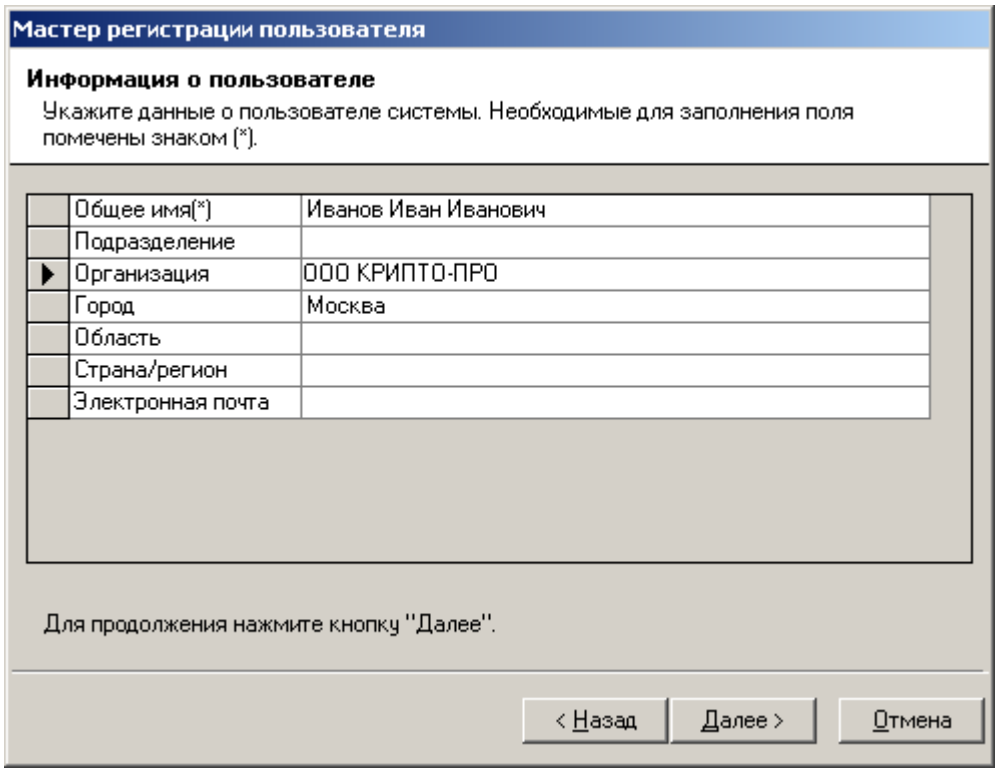


При данном режиме регистрации учетная информация о пользователе, заносимая в сертификаты, берется из запроса на сертификат.

Для удобства дальнейшего использования можно выбрать опцию «Сохранить выбранную настройку источника запроса на сертификат». Тогда, при создании последующих запросов на сертификат переключатель источника запроса на сертификат будет в выбранном положении.

В следующем окне **Мастера** (см. Рисунок 46) отображается идентификационная информация об учетных данных регистрируемого пользователя, содержащаяся в файле запроса на сертификат.

Рисунок 46. Окно просмотра идентификационных данных пользователя из запроса на сертификат



Нажмите кнопку **Далее** - откроется окно ввода секретной ключевой фразы пользователя, комментария администратора и имени UPN (см. Рисунок 36). После этого появится завершающее окно Мастера регистрации пользователя. Установите в нем переключатель – **Запустить мастер создания сертификата** см. (Рисунок 37).

Запустится **Мастер создания сертификата,** в окне **Источник запроса на сертификат** выберите – **Чтение запроса на сертификат из файла.**

В окне **Просмотра запроса на сертификат** укажите необходимую дополнительную справочную информацию. Данная информация не будет заноситься в сертификат. Также в данном окне возможно сохранить запрос на сертификат регистрируемого пользователя нажатием кнопки **Сохранить** (см. Рисунок 41). После нажатия на кнопку **Далее** данного окна запрос на сертификат через Центр Регистрации поступает в Центр Сертификации.

После успешного выпуска сертификата откроется окно **Установки сертификата** (см. Рисунок 42). Произведите необходимые настройки и нажмите кнопку **Далее**.

В следующем окне **Мастера** возможно определить (выбрать) возможность сохранения цепочки сертификатов и списка отозванных сертификатов в виде файла на магнитном носителе (см. Рисунок 43).

Подтверждением успешного окончания процедуры изготовления сертификата является отображение финального окна Мастера изготовления сертификата (см. Рисунок 44).

7. Управление ключами и сертификатами пользователей

Если регламентом Удостоверяющего Центра и конфигурацией ПО Центра Регистрации определен режим централизованного управления ключами и сертификатами пользователей, то в задачи администратора Центра Регистрации входит выполнение регламентных процедур:

- плановая и внеплановая смена ключей и сертификатов открытых ключей пользователей;
- отзыв (аннулирование) сертификатов открытых ключей пользователей;
- приостановление/возобновление действия сертификатов;

Порядок выполнения данных процедур определяется регламентом Удостоверяющего Центра.

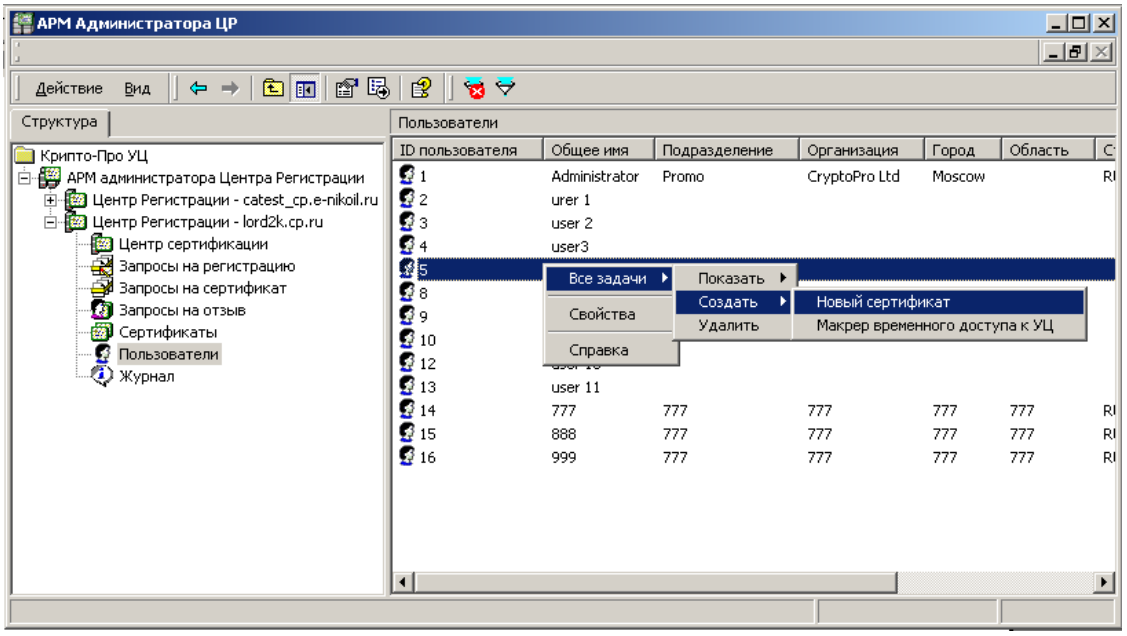
АРМ администратора обеспечивает выполнение следующих задач:

- генерация ключей и выпуск сертификатов открытых ключей пользователей;
- отзыв (аннулирование), приостановление/возобновление действия сертификатов открытых ключей пользователей.

7.1. Генерация ключей и выпуск сертификатов открытых ключей пользователей

Генерация новых ключей и выпуск сертификата открытого ключа для зарегистрированного пользователя выполняется с помощью задачи **Создать/Новый сертификат** из контекстного меню для записи папки **Пользователи** (см. Рисунок 47).

Рисунок 47. Запуск задачи выпуска нового сертификата пользователя

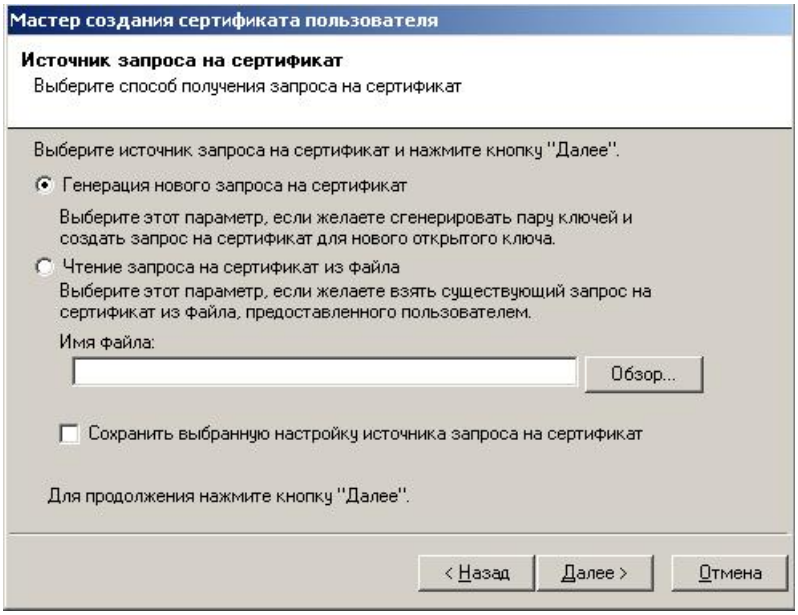


Создание нового сертификата пользователя выполняется с помощью **Мастера создания сертификата пользователя**.

В окне **Мастера** необходимо определить источник запроса на сертификат (см. Рисунок 48). Возможно два варианта:

- генерация ключей и формирование запроса на сертификат на рабочем месте администратора. Для этого необходимо выбрать пункт **Генерация нового запроса на сертификат**;
- на основании запроса на сертификат открытого ключа из файла, полученного от пользователя. Для этого необходимо выбрать пункт **Чтение запроса на сертификат из файла**.

Рисунок 48. Окно определения источника запроса на сертификат в Мастере создания сертификата пользователя



Для удобства дальнейшего использования можно выбрать опцию «Сохранить выбранную настройку источника запроса на сертификат». Тогда, при создании последующих запросов на сертификат переключатель источника запроса на сертификат будет в выбранном положении.

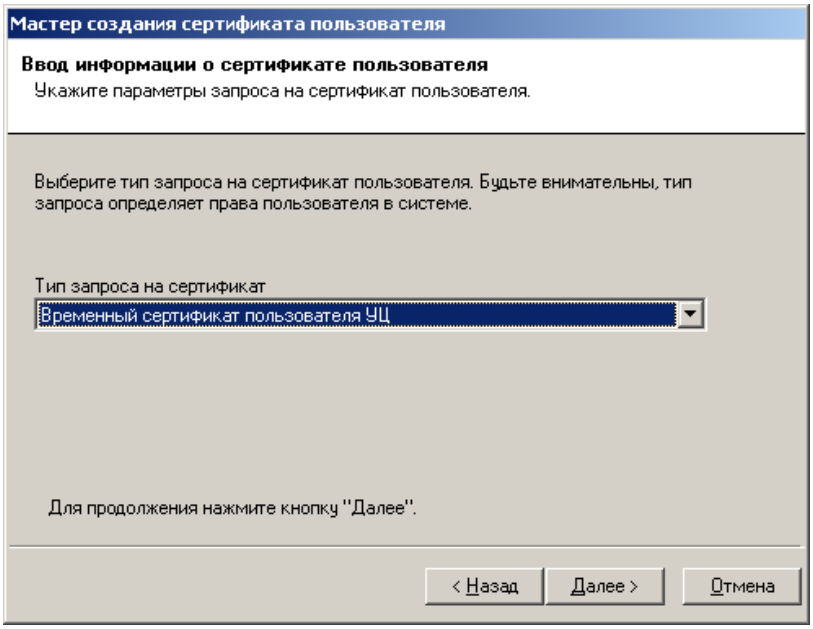
Последовательность дальнейших окон Мастера зависит от выбранного в окне определения источника запроса на сертификат пункта.

При выборе пункта **Генерация нового запроса на сертификат** в следующем окне необходимо выбрать шаблон сертификата для создаваемого сертификата (см. Рисунок 49).

В зависимости от настройки АРМ администратора ЦР (окно **Свойства: АРМ администратора Центра Регистрации**) в части выбора криптопровайдера перед окном выбора шаблона на сертификат может быть диалоговое окно настройки параметров ключа (см. Рисунок 39).

В том случае, если в настройках АРМ администратора ЦР (окно **Свойства: АРМ администратора Центра Регистрации**) установлен флаг **Запрашивать имя контейнера,** после выбора шаблона сертификата появится диалоговое окно ввода имени контейнера закрытого ключа (см. Рисунок 39). Введите имя контейнера или оставьте имя контейнера по умолчанию.

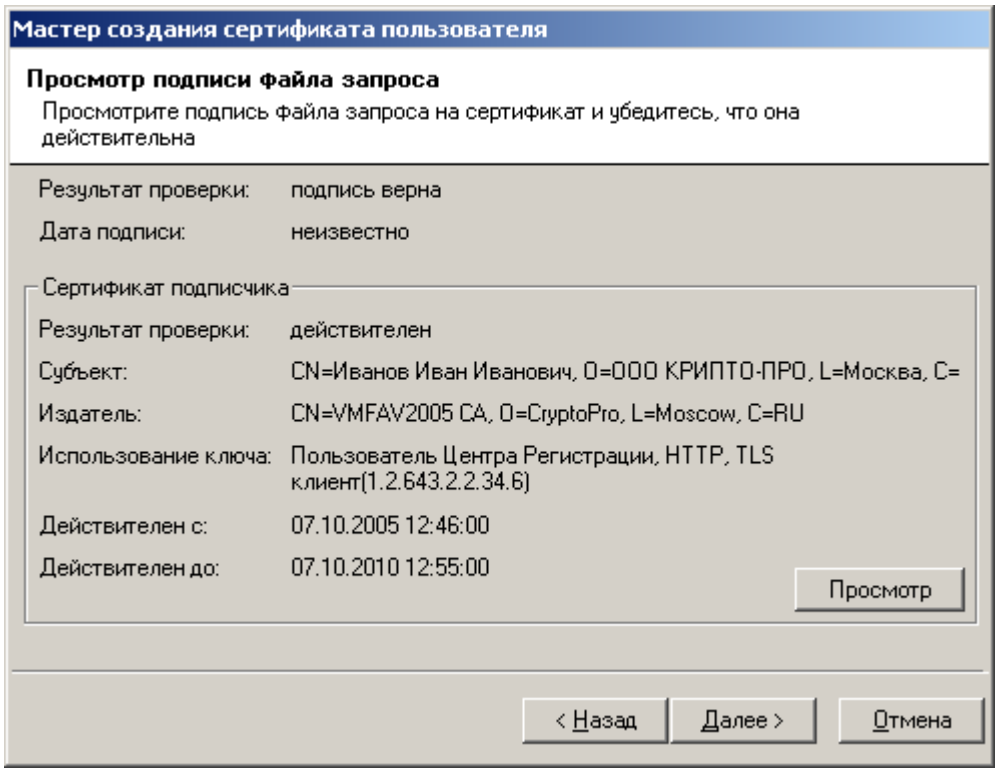
Рисунок 49. Окно выбора шаблона сертификата Мастера создания сертификата пользователя



При выборе пункта **Чтение запроса на сертификат из файла** окно выбора шаблона не отображается.

Если запрос на сертификат сформирован с помощью html-формы автономной работы пользователя и является подписанным ЭЦП документом (ЭЦП формируется на действующем закрытом ключе пользователя – например, при проведении процедуры плановой смены ключей), то появится окно **Просмотра подписи файла запроса** (см. Рисунок 50). Изготовление сертификата должно быть осуществлено только в том случае, если одновременно выполнены два условия: Результат проверки ЭЦП запроса **- подпись верна** и Результат проверки сертификата – **действителен.**

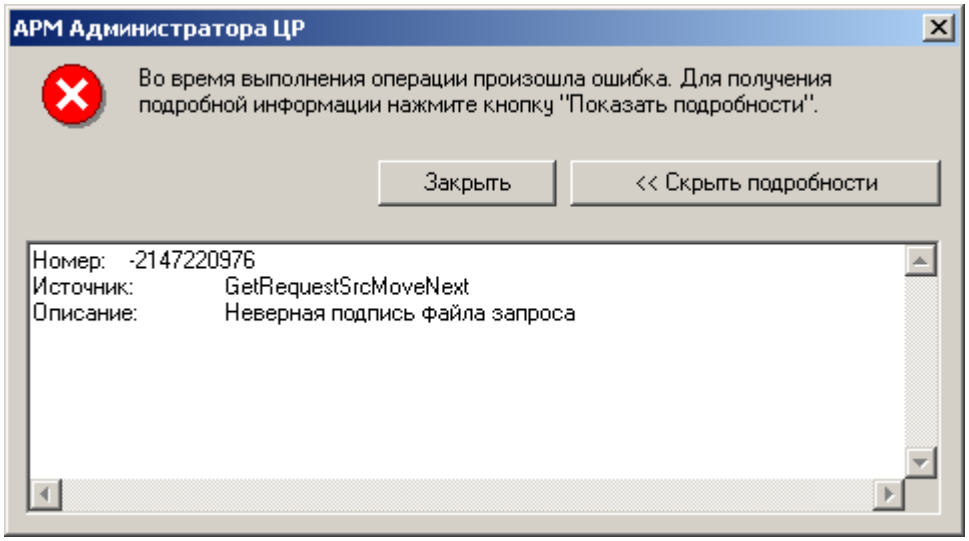
Рисунок 50. Окно просмотра подписи файла запроса



На практике количество условий, при выполнении которых может быть изготовлен сертификат, гораздо больше. Порядок и необходимые условия изготовления сертификата по подписанному запросу должны быть отражены в регламенте Удостоверяющего Центра.

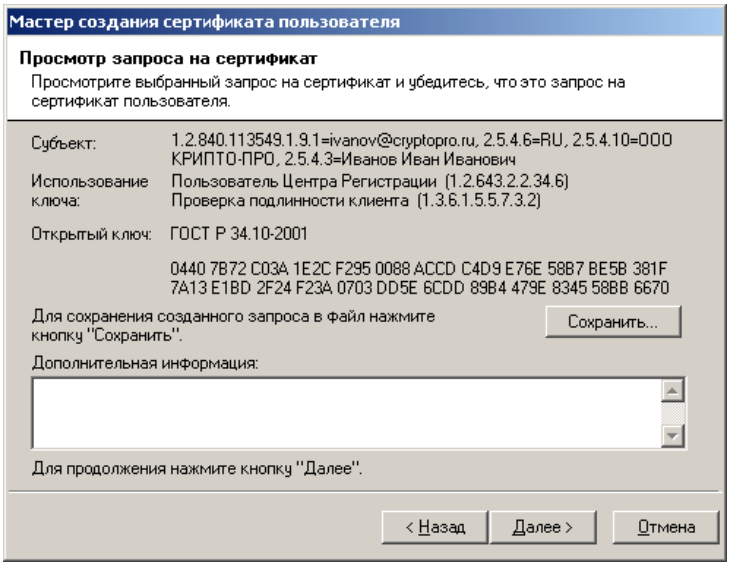
В том случае, если целостность подписанного запроса на изготовление сертификата была нарушена, либо сертификат, на котором подписан запрос, не действителен, то будет отображено окно с информацией о возникшей ошибке (см. Рисунок 51).

Рисунок 51. Ошибка при проверке подписи запроса на сертификат



Следующим окном **Мастера** будет окно просмотра запроса на сертификат (см. Рисунок 52). В нем отображается информация о владельце сертификата и области применения сертификата.

Рисунок 52. Окно просмотра запроса на сертификат Мастера создания сертификата пользователя

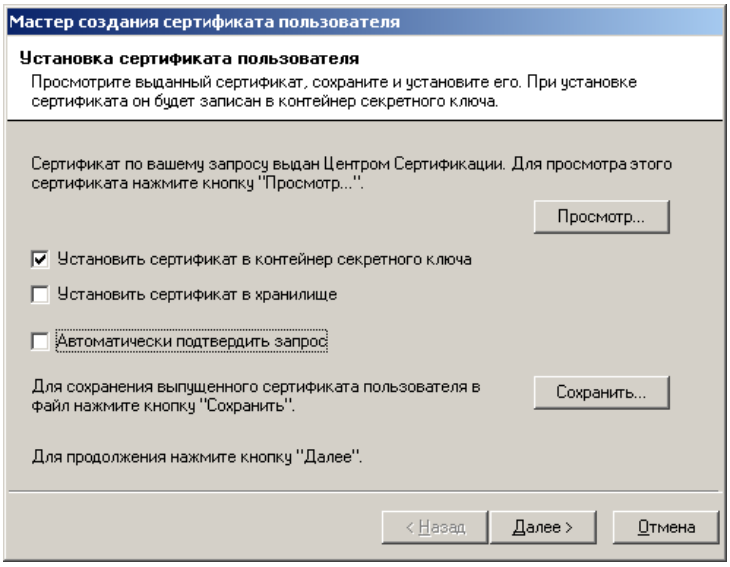


Нажатие на кнопку **Сохранить** позволит сохранить отображаемый запрос на сертификат в виде файла формата PKCS#10.

При нажатии на кнопку **Далее** данного окна запрос на сертификат через Центр Регистрации поступает в Центр Сертификации.

После успешного выпуска сертификата откроется окно **Установки сертификата** (см. Рисунок 53).

Рисунок 53. Окно установки выпущенного сертификата Мастера создания сертификата



Установка флага **Установить сертификат в хранилище** произведет установку сертификата со связкой с закрытым ключом в хранилище **Текущий пользователь/Другие пользователи/Сертификаты**. Использование данного флага позволит произвести последующий экспорт сертификата и соответствующего закрытого ключа в файл формата PKCS#12 при формировании ключей с использованием криптопровайдеров, поддерживающих хранение закрытых ключей только на жестком диске компьютера (например, Microsoft Base Cryptographic Provider, Microsoft Enhanced Cryptographic Provider и т.д.).

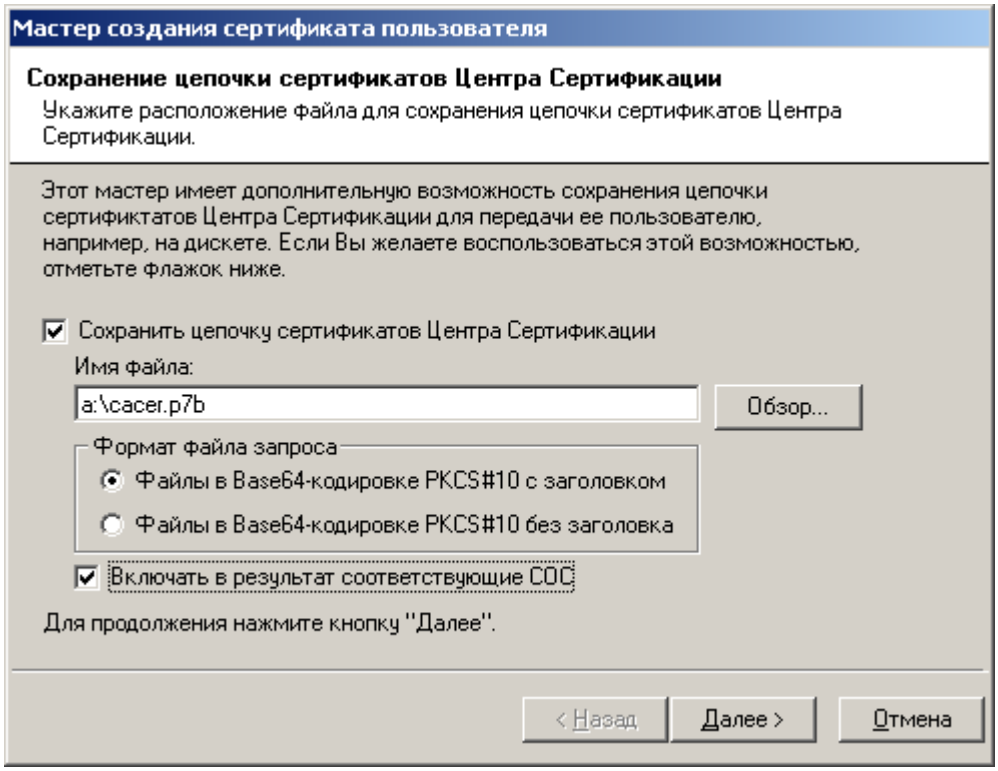
СКЗИ «КриптоПро CSP» не поддерживает экспорт сертификата и соответствующего закрытого ключа в файл формата PKCS#12.

Нажатие кнопки **Сохранить** позволяет сохранить изданный сертификат в виде файла.

Установка флага **Автоматически подтвердить запрос** произведет установку запроса на сертификат в состояние **Подтвержденный**.

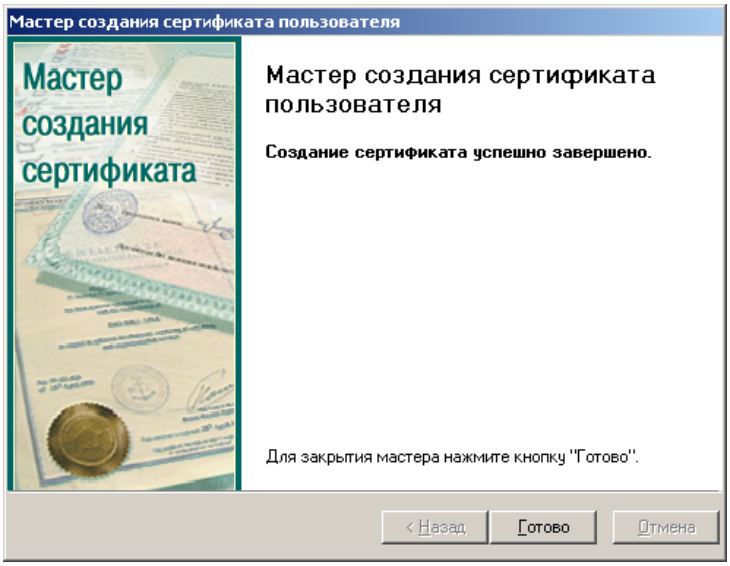
В следующем окне **Мастера** возможно сохранить цепочку сертификатов и список отозванных сертификатов в виде файла на магнитном носителе (см. Рисунок 54).

Рисунок 54. Окно сохранения цепочки сертификатов Мастера создания сертификата



Подтверждение успешной регистрации пользователя сопровождается соответствующим заключительным окном **Мастера** (см. Рисунок 55).

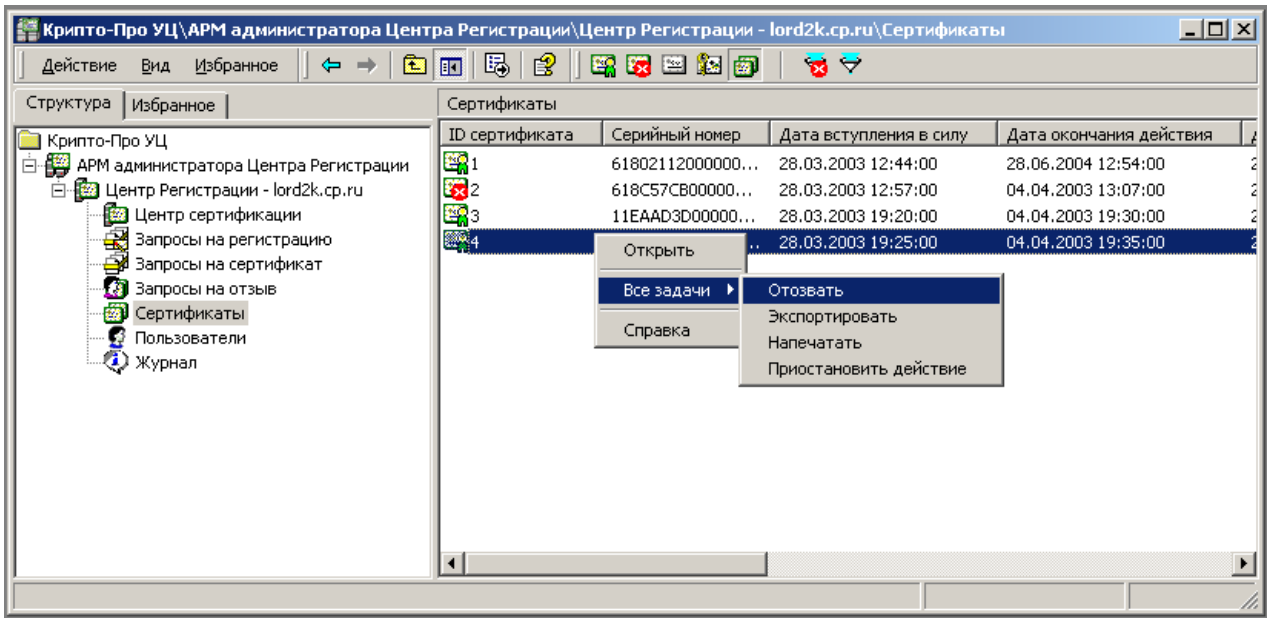
Рисунок 55. Заключительное окно работы Мастера создания сертификата



7.2. Отзыв (аннулирование) сертификатов открытых ключей пользователей

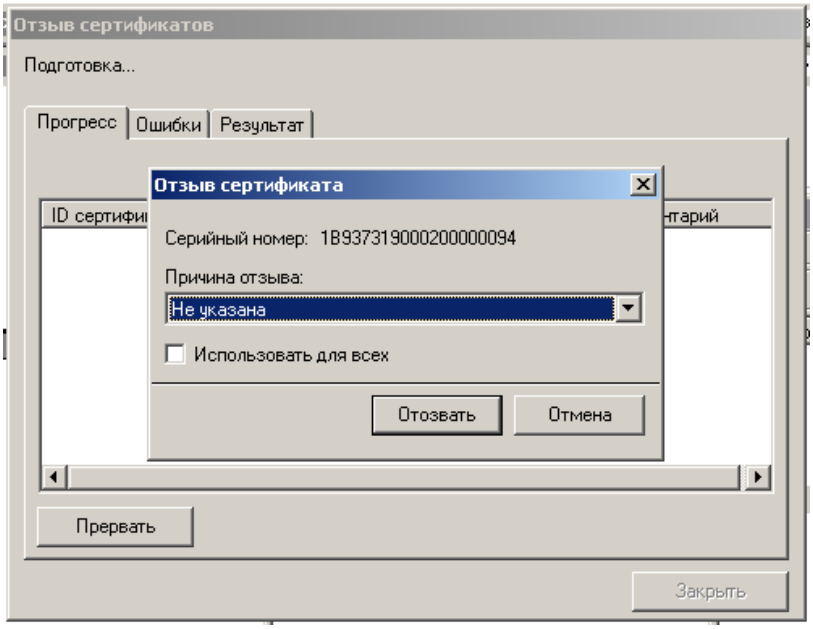
Отзыв сертификата открытого ключа для зарегистрированного пользователя выполняется с помощью задачи **Отозвать** из контекстного меню записи папки **Сертификаты** (см. Рисунок 56).

Рисунок 56. Запуск задачи отзыва сертификата пользователя



При запуске данной задачи, администратору будет выведено окно для указания причины отзыва сертификата (см. Рисунок 57).

Рисунок 57. Окно указания причины отзыва в задаче отзыва сертификата пользователя



При выполнении групповой операции над несколькими сертификатами, можно указать одну причину отзыва для всех сертификатов. Для этого нужно установить переключатель **Использовать для всех** в окне указания причины отзыва.

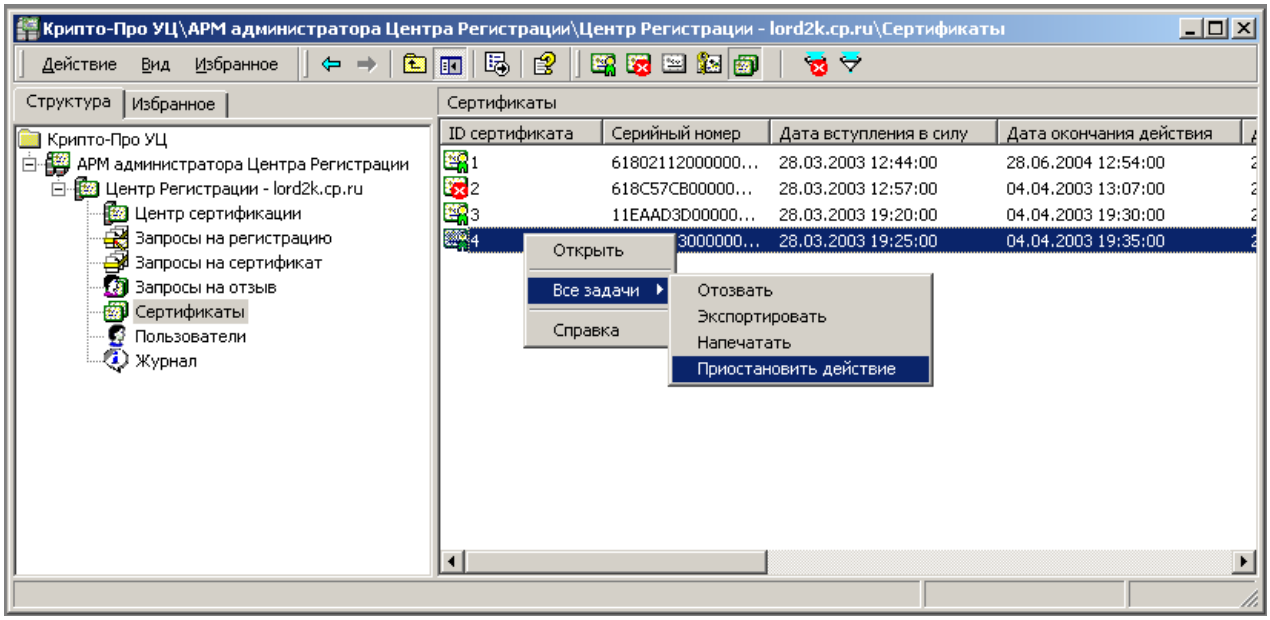
Нажатие кнопки **Отмена** в окне указания причины отзыва приведёт к появлению окна с вопросом **"Действительно хотите прервать операцию?"** и кнопками **Да**, **Нет**. Нажатие кнопки **Да** приведёт к завершению операции, нажатие кнопки **Нет** отменяет операцию для текущего сертификата и осуществляет переход к процессу обработки следующего сертификата из выбранных для групповой операции.

Запрос на отзыв сертификата будет отправлен через Центр Регистрации (осуществляется применение политик обработка запроса) на Центр Сертификации и в случае соответствия запроса политикам Центра Регистрации, сертификат будет помещен в список отозванных сертификатов (CRL) при его формировании.

7.3. Приостановление действия сертификатов открытых ключей пользователей

Приостановление действия сертификата пользователя осуществляется путем выбора сертификата (или сертификатов) из числа действующих сертификатов и запуска задачи **Приостановить действие** из контекстного меню (см. Рисунок 58).

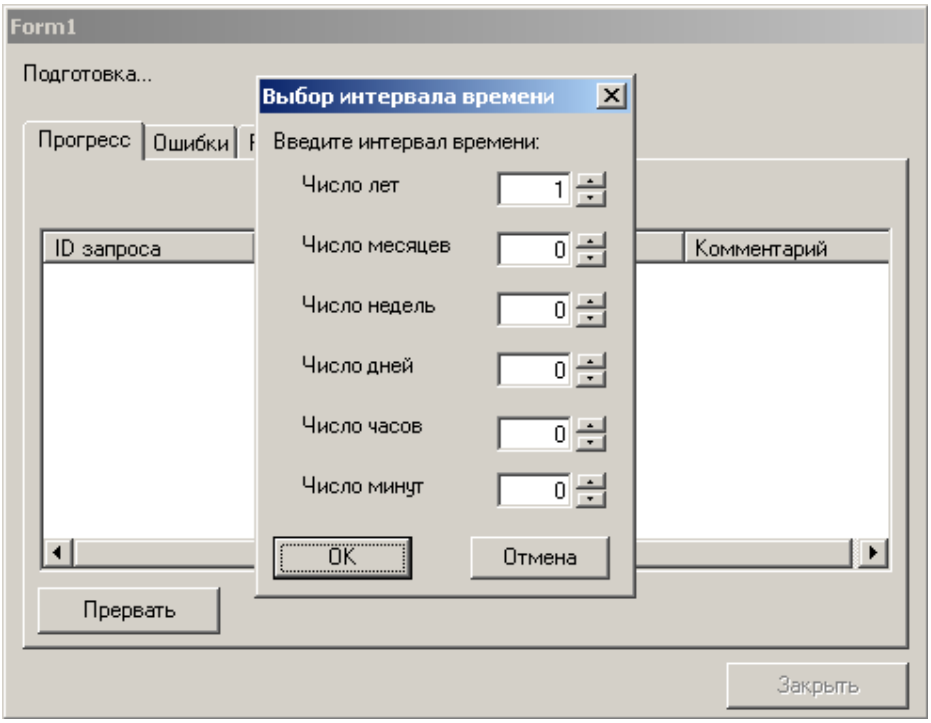
Рисунок 58. Запуск задачи приостановления действия сертификата пользователя



После начала выполнения задачи приостановления действия сертификата, администратору будет отображено окно (см. Рисунок 59), в котором необходимо указать период, на который приостанавливается действие сертификата открытого ключа пользователя.

Нажатие кнопки **Отмена** в окне указания срока приостановления действия приведёт к появлению окна с вопросом **"Действительно хотите прервать операцию?"** и кнопками **Да**, **Нет**. Нажатие кнопки **Да** приведёт к завершению операции, нажатие кнопки **Нет** отменяет операцию для текущего сертификата и осуществляет переход к процессу обработки следующего сертификата из выбранных для групповой операции.

Рисунок 59. Окно указания периода приостановления действия сертификата пользователя

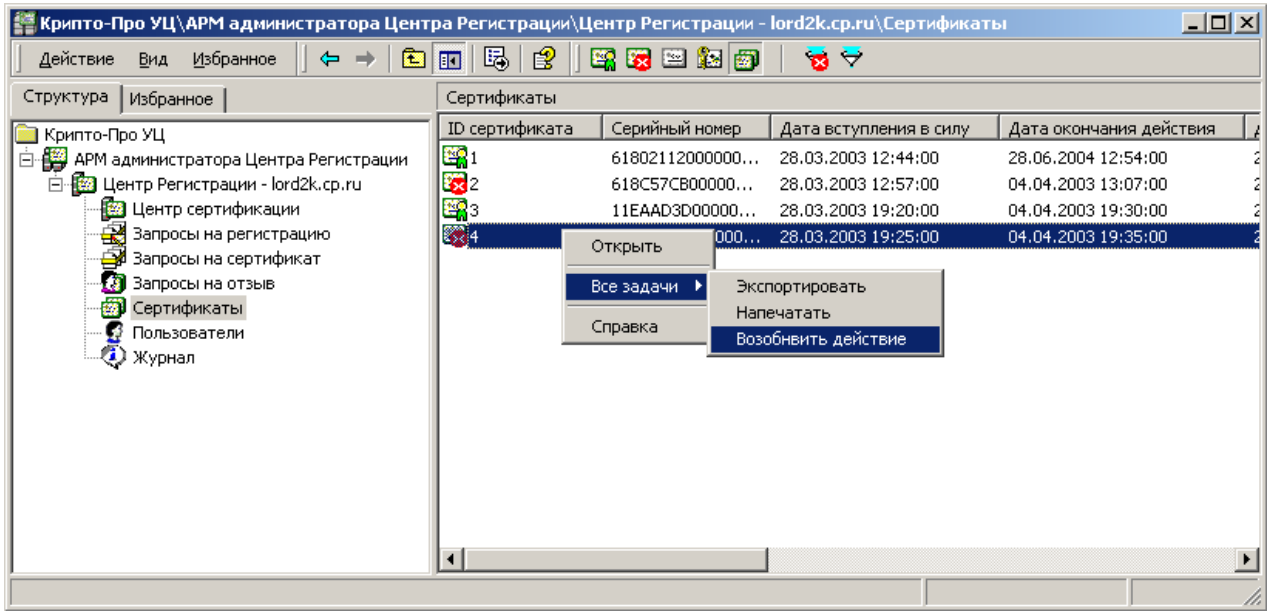


Запрос на приостановление действия сертификата будет отправлен через Центр Регистрации (осуществляется применение политик обработка запроса) на Центр Сертификации и в случае соответствия запроса политикам Центра Регистрации, сертификат будет помещен в список отозванных сертификатов (CRL) при его формировании. Код причины отзыва сертификата в CRL будет установлен **Приостановка действия(6)**.

7.4. Возобновление действия сертификатов открытых ключей пользователей

Возобновление действия ранее приостановленного сертификата пользователя осуществляется путем выбора сертификата (или сертификатов) из числа отозванных сертификатов и запуска задачи **Возобновить действие** из контекстного меню (см. Рисунок 60).

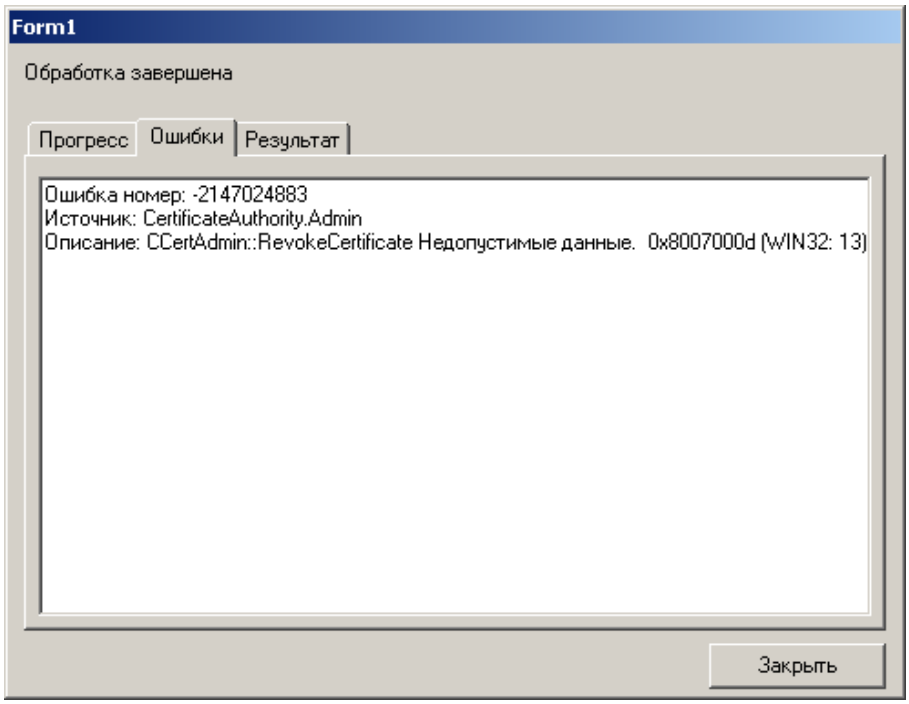
Рисунок 60. Запуск задачи возобновления действия сертификата пользователя



Операция будет успешно выполнена, если в качестве сертификата, из числа отозванных, будет выбран сертификат, у которого причиной отзыва была установлена **Приостановка действия(6).**

В противном случае будет диагностирована ошибка (см. Рисунок 61):

Рисунок 61. Сообщение об ошибке при попытке возобновления действия отозванного сертификата



Запрос на возобновление действия сертификата будет отправлен через Центр Регистрации (осуществляется применение политик, обработка запроса) на Центр Сертификации и в случае соответствия запроса политикам Центра Регистрации, сертификату будет присвоен статус **Действующий,** и он будет удален из списка отозванных сертификатов (CRL) при его формировании.

8. Удаление зарегистрированных пользователей

АРМ администратора Центра Регистрации обеспечивает выполнение процедуры удаления зарегистрированного пользователя из реестра пользователей Центра Регистрации по запросу администратора.

Поскольку УЦ должен хранить информацию о пользователях, их запросах и сертификатах даже после окончания срока действия сертификатов пользователей, рекомендуется процедуру удаления пользователя производить только в случаях:

1) при регистрации пользователя была допущена ошибка в одном или нескольких компонентах имени;
2) регистрация пользователя была выполнена на основании юридически недействительных документов;
3) пользователь изначально был создан для тестов.

Технически возможно удаление зарегистрированных пользователей, отвечающих следующим критериям:

- Пользователь не имеет ни одного действующего сертификата открытого ключа;
- Пользователь не имеет ни одного сертификата открытого ключа с приостановленным сроком действия;
- Пользователь не имеет ни одного необработанного запроса на сертификат открытого ключа, стоящего в очереди (не имеет запросов в состоянии **Ожидающий**)
- Пользователь не является привилегированным.

При удалении пользователя удаляется вся информация по пользователю из базы данных Центра Регистрации.

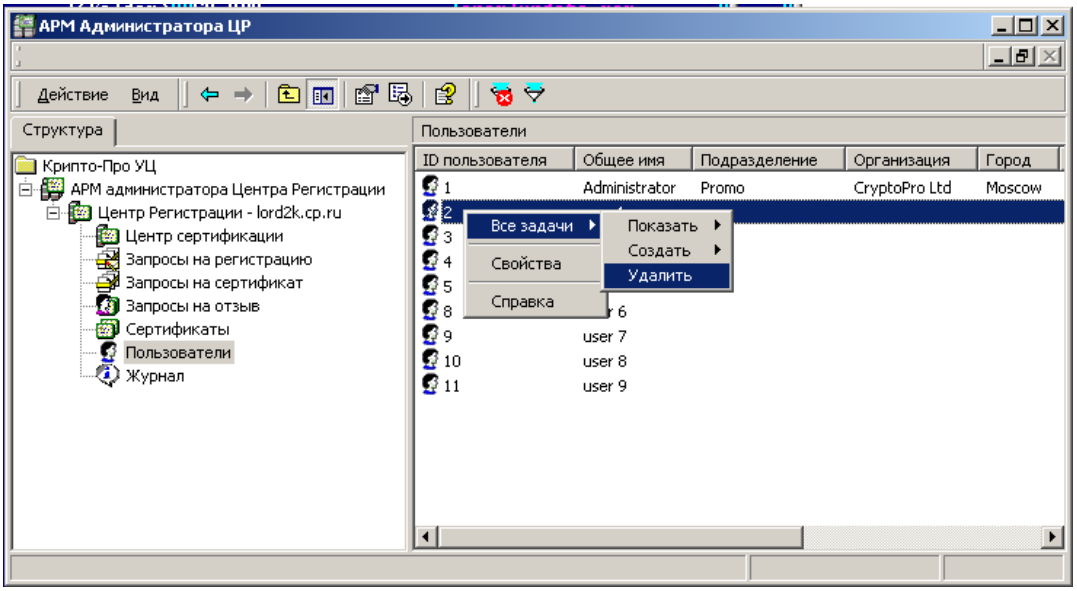

Информация, хранящаяся в эталонной базе данных сертификатов Центра Сертификации, при данной процедуре не изменяется.

Выполнять удаление привилегированного пользователя не рекомендуется.

Технически удаление привилегированного пользователя возможно, если на УЦ в данный момент нет пользователей, для которых этот привилегированный пользователь выполнял отправку и/или принятие запросов на сертификат.

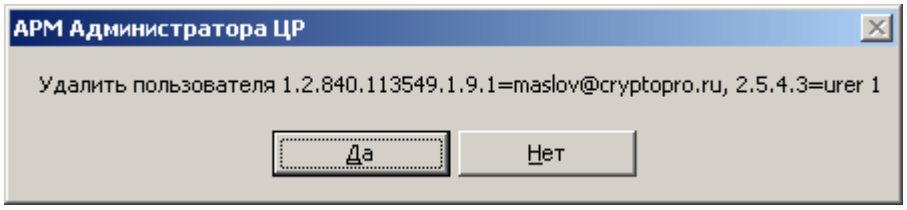
Для запуска задачи удаления пользователя необходимо выбрать пользователя из списка и выбрать в контекстном меню пункт **Удалить** (см. Рисунок 62).

Рисунок 62. Запуск задачи удаления зарегистрированного пользователя



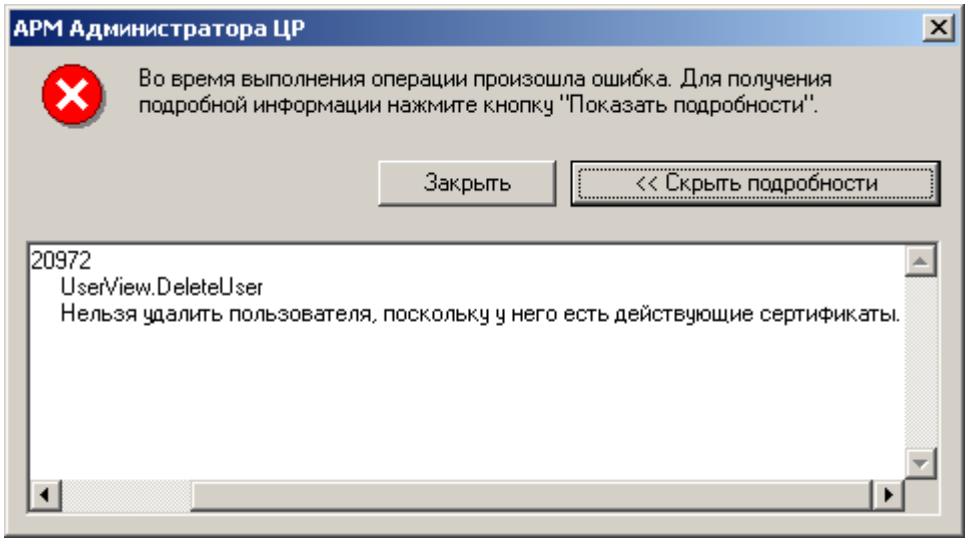
В следующем окне отображается информация по значениям атрибута имени пользователя (см. Рисунок 63). Администратору необходимо убедиться в правильном выборе удаляемого пользователя.

Рисунок 63. Окно предупреждения при удалении пользователя



В случае если выбранный пользователь не удовлетворяет критериям для удаления, отображается окно с соответствующим диагностическим сообщением (см. Рисунок 64).

Рисунок 64. Окно сообщения о невозможности удаления пользователя



Если выбранный пользователь удовлетворяет критериям для удаления, то пользователь удаляется из реестра (базы данных) Центра Регистрации.

9. Обработка запросов пользователей поступивших и стоящих в очереди на Центре Регистрации

Одной из задач администратора Центра Регистрации является выполнение регламентных процедур по обработке поступающих от пользователей запросов на Центр Регистрации.

Подлежат обработке следующие запросы:

- запросы на регистрацию пользователя (если регламентом Удостоверяющего Центра предусмотрена распределенная регистрация пользователя, и Центр Регистрации сконфигурирован для поддержки регистрации пользователей в распределенном режиме);
- запросы на сертификат открытого ключа (если регламентом Удостоверяющего Центра предусмотрена возможность распределенного управления ключами и сертификатами, и Центр Регистрации сконфигурирован для поддержки данного режима);
- запросы на отзыв сертификата открытого ключа, приостановление, возобновление его действия (если регламентом Удостоверяющего Центра предусмотрена возможность распределенного управления ключами и сертификатами, и Центр Регистрации сконфигурирован для поддержки данного режима).

Все поступающие на обработку запросы имеют тип **Ожидающие** и отображаются в списке соответствующей папки при установке фильтрации по типу записей, с наименованием типа **Ожидающие**.

Под обработкой понимается регламентная процедура изменения типа объекта управления (запроса) из типа **Ожидающие** в тип **Одобренные** или **Отклоненные**. Порядок изменения состояния определяется регламентом Удостоверяющего Центра и соответствующими инструкциями администратора.

Технически на консоли администратора изменение состояния (обработка) запросов выполняется с помощью соответствующих задач из контекстного меню для выбранного запроса. К таким задачам относятся:

- Принять;
- Отклонить.

Контекстные меню **Запроса на регистрацию**, **Запроса на сертификат**, **Запроса на отзыв сертификата,** стоящих в очереди на обработку, приведены на Рисунок 65,Рисунок 66 и Рисунок 67 соответственно.

Рисунок 65. Контекстное меню запроса на регистрацию, стоящего в очереди на обработку

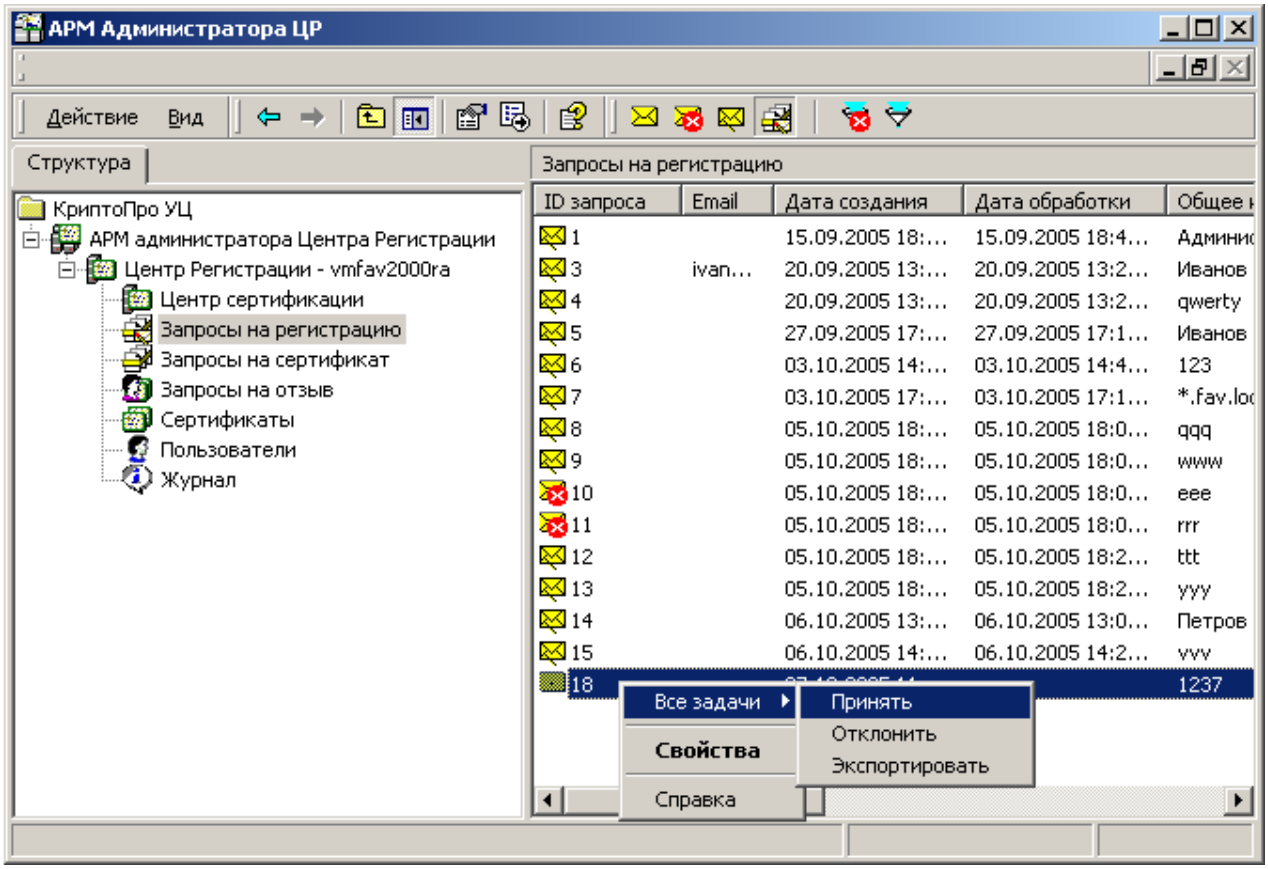


Рисунок 66. Контекстное меню запроса на изготовление сертификата, стоящего в очереди на обработку

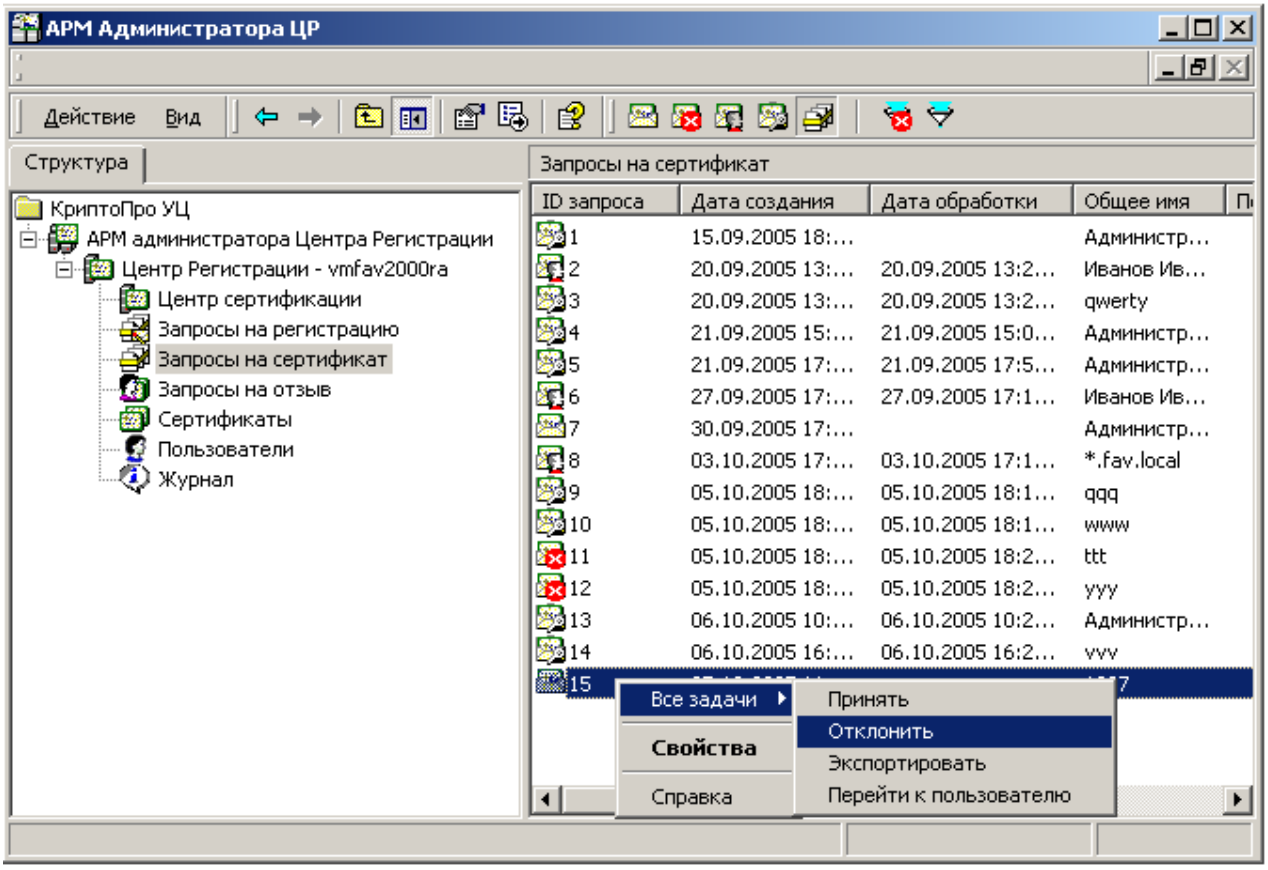
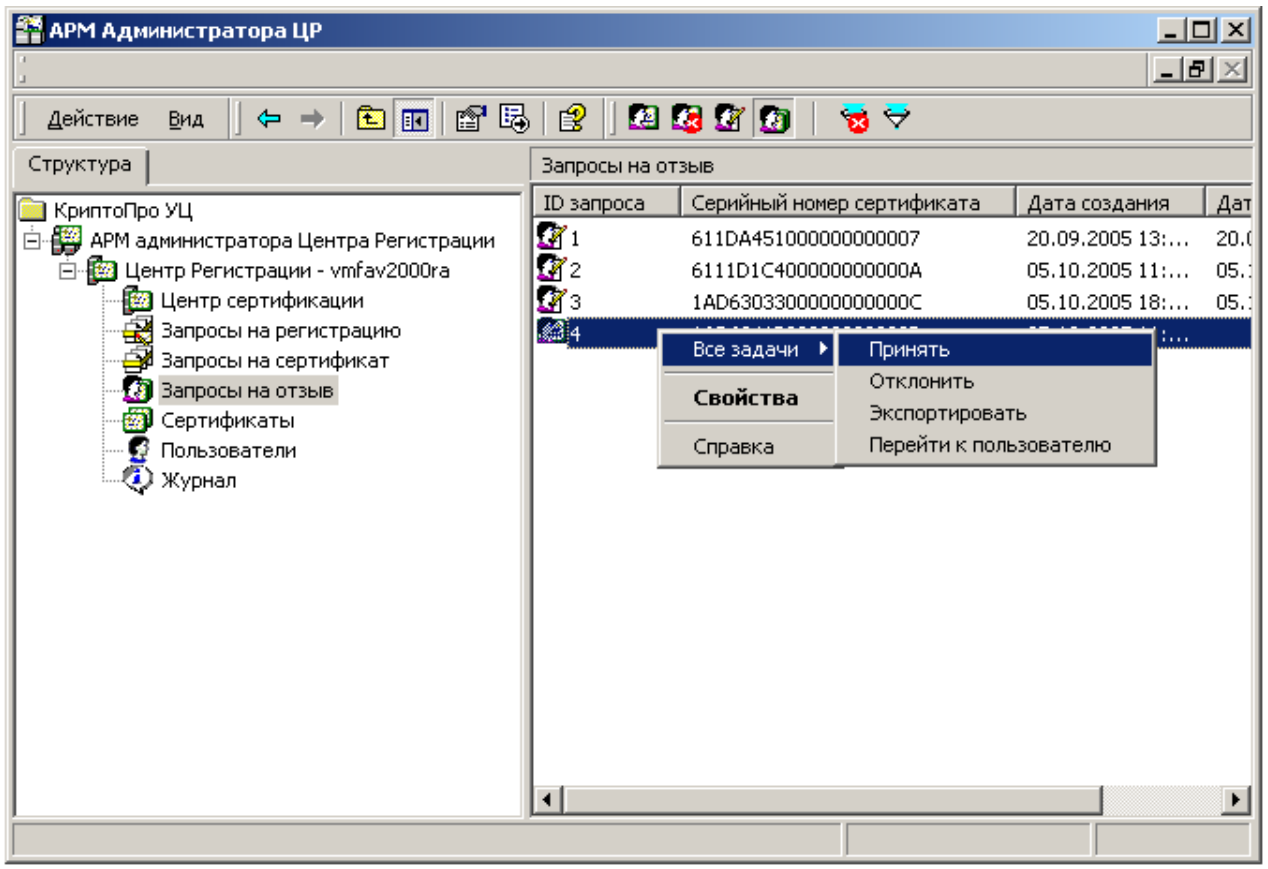


Рисунок 67. Контекстное меню запроса на отзыв сертификата, стоящего в очереди на обработку



Для того чтобы выполнить задачу, необходимо:

1. Открыть список записей (запросов пользователей) соответствующей папки;
2. Найти и установить курсор в списке на нужную запись;
3. Для идентификации записи рекомендуется:
    a. открыть окно свойств запроса и проанализировать информацию в нем;
    b. ввести комментарии администратора в окне свойств запроса;
4. Нажать правую кнопку мыши для вызова контекстного меню;
5. Выбрать из списка задач контекстного меню пункт, содержащий наименование требуемой задачи.

10. Печать сертификатов открытых ключей пользователей

Программное обеспечение АРМ администратора ЦР позволяет осуществить формирование формы для печати сертификата пользователя на бумажный носитель.

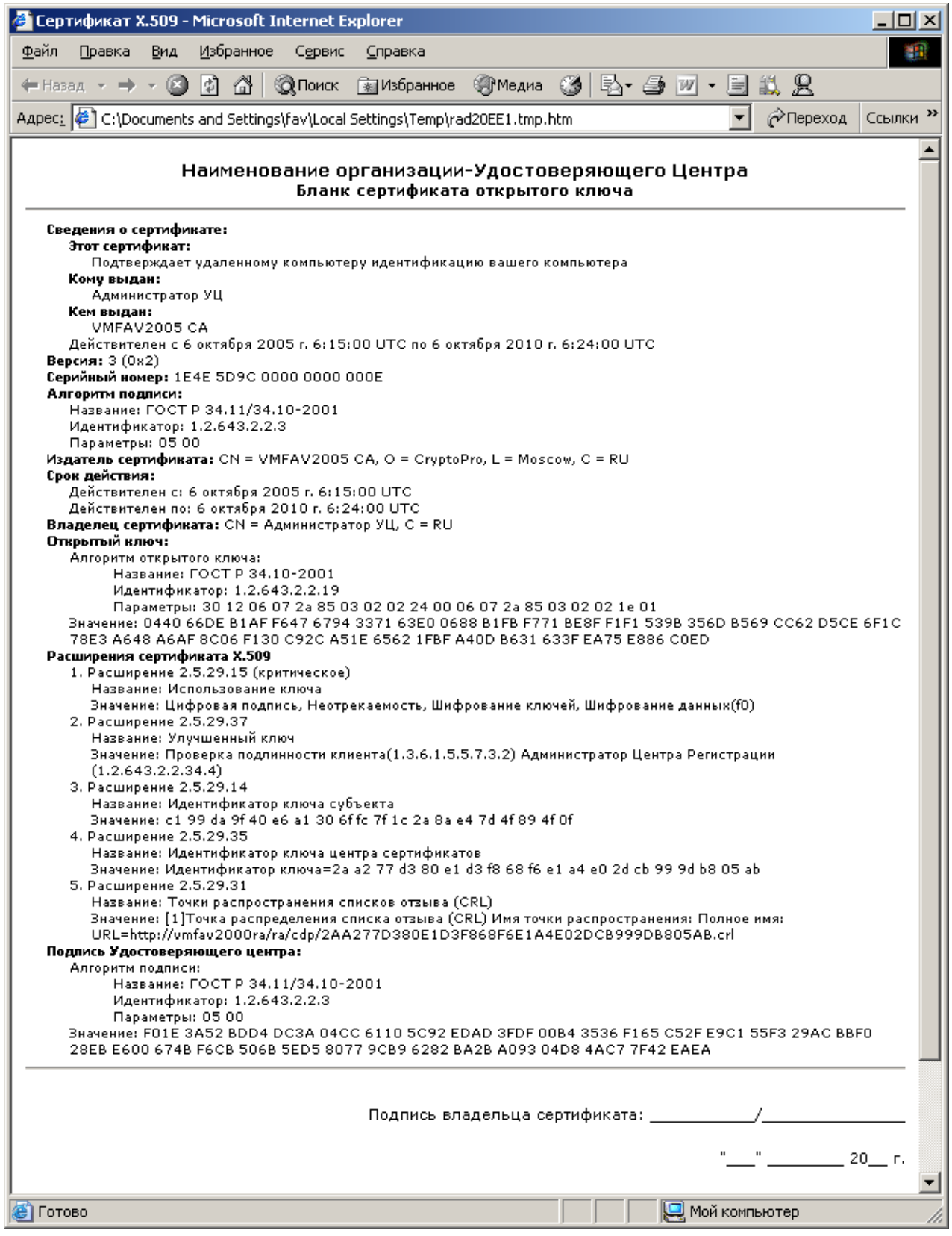
Шаблон формы сертификата описывается в файле **Cert.xls**, по умолчанию расположенном в папке **Templates** каталога установки ПО АРМ администратора ЦР.

Данный файл может корректироваться для приведения формы печати сертификата в соответствии с требованиями конкретного Удостоверяющего Центра.

Имя и размещение файла с шаблоном формы сертификата задается в окне свойств оснастки АРМ администратора (см. Рисунок 7).

Сформированная форма для печати сертификата в HTML-формате отображается в окне браузера MS IE, из которого и происходит вывод формы на бумажный носитель с помощью стандартных средств приложения MS IE (см. Рисунок 68).

Рисунок 68. Окно просмотра сертификата для вывода на бумажный носитель



Наименование организации-Удостоверяющего Центра
Бланк сертификата открытого ключа

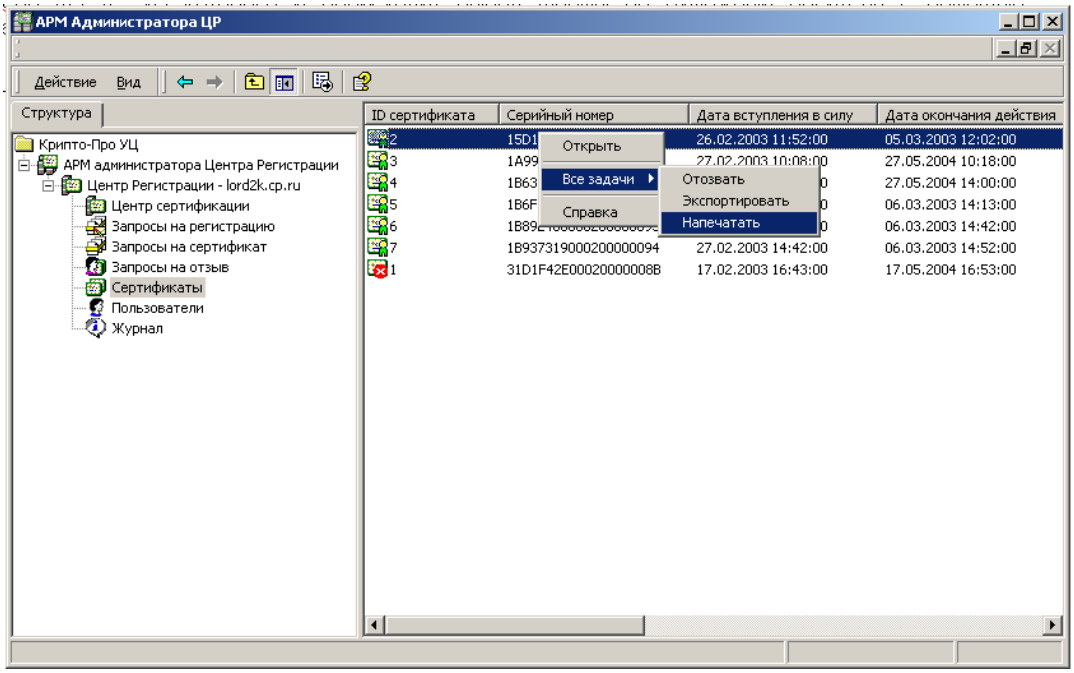
Сведения о сертификате:
Этот сертификат:
Подтверждает удаленному компьютеру идентификацию вашего компьютера
Кому выдан:
Администратор УЦ
Кем выдан:
VMFAV2005 CA
Действителен с 6 октября 2005 г. 6:15:00 UTC по 6 октября 2010 г. 6:24:00 UTC
Версия: 3 (0x2)
Серийный номер: 1E4E 5D9C 0000 0000 000E
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001
Идентификатор: 1.2.643.2.2.3
Параметры: 05 00
Издатель сертификата: CN = VMFAV2005 CA, O = CryptoPro, L = Moscow, C = RU
Срок действия:
Действителен с: 6 октября 2005 г. 6:15:00 UTC
Действителен по: 6 октября 2010 г. 6:24:00 UTC
Владелец сертификата: CN = Администратор УЦ, C = RU
Открытый ключ:
Алгоритм открытого ключа:
Название: ГОСТ Р 34.10-2001
Идентификатор: 1.2.643.2.2.19
Параметры: 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03 02 02 1e 01
Значение: 0440 66DE B1AF F647 6794 3371 63E0 0688 B1FB F771 BE8F F1F1 539B 356D B569 CC62 D5CE 6F1C 78E3 A648 A6AF 8C06 F130 C92C A51E 6562 1FBF A40D B631 633F EA75 E886 C0ED
Расширения сертификата X.509
1. Расширение 2.5.29.15 (критическое)
Название: Использование ключа
Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных(f0)
2. Расширение 2.5.29.37
Название: Улучшенный ключ
Значение: Проверка подлинности клиента(1.3.6.1.5.5.7.3.2) Администратор Центра Регистрации (1.2.643.2.2.34.4)
3. Расширение 2.5.29.14
Название: Идентификатор ключа субъекта
Значение: c1 99 da 9f 40 e6 a1 30 6f fc 7f 1c 2a 8a e4 7d 4f 89 4f 0f
4. Расширение 2.5.29.35
Название: Идентификатор ключа центра сертификатов
Значение: Идентификатор ключа=2a a2 77 d3 80 e1 d3 f8 68 f6 e1 a4 e0 2d cb 99 9d b8 05 ab
5. Расширение 2.5.29.31
Название: Точки распространения списков отзыва (CRL)
Значение: [1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://vmfav2000ra/ra/cdp/2AA277D380E1D3F868F6E1A4E02DCB999DB805AB.crl
Подпись Удостоверяющего центра:
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001
Идентификатор: 1.2.643.2.2.3
Параметры: 05 00
Значение: F01E 3A52 BDD4 DC3A 04CC 6110 5C92 EDAD 3FDF 00B4 3536 F165 C52F E9C1 55F3 29AC BBF0 28EB E600 674B F6CB 506B 5ED5 8077 9CB9 6282 BA2B A093 04D8 4AC7 7F42 EAEA

Подпись владельца сертификата: _____/_____

"___" _____ 20__ г.

Формирование формы для печати сертификата происходит при выполнении задачи **Печать** из контекстного меню для записи папки **Сертификаты** (см. Рисунок 69).

Рисунок 69. Запуск задачи печати сертификата пользователя

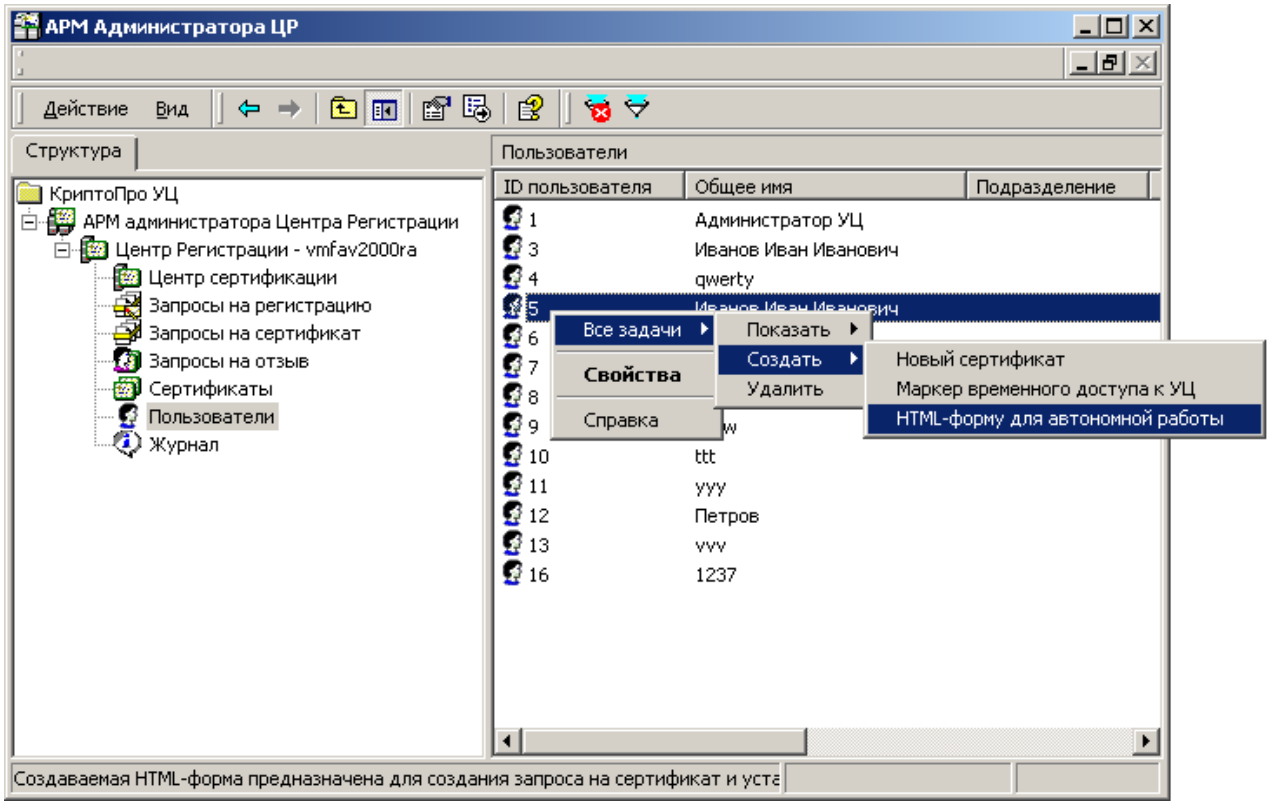


11. Формирование html-формы для автономной работы пользователя Удостоверяющего Центра

Html-форма автономной работы пользователя Удостоверяющего Центра позволяет пользователю без подключения к Центру Регистрации генерировать ключи, формировать запросы на сертификат открытого ключа и устанавливать изданный Удостоверяющим Центром сертификат открытого ключа на своем рабочем месте.

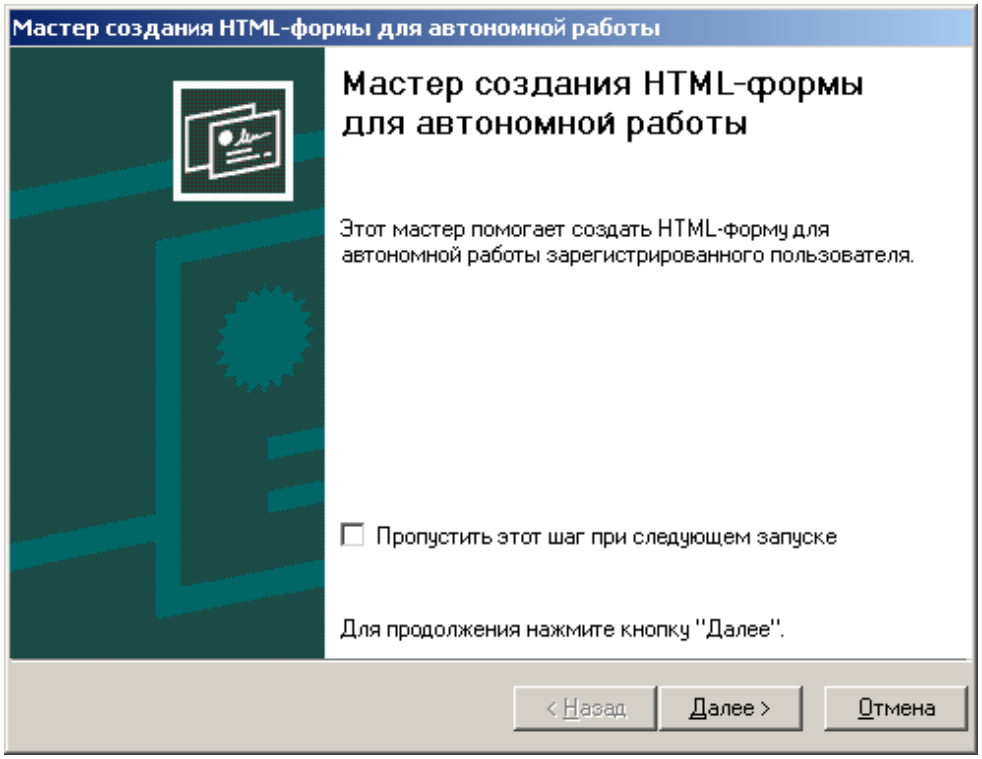
Для создания настоящей формы необходимо в окне просмотра учетных записей зарегистрированных пользователей выделить правой кнопкой мыши учетную запись пользователя, для которого необходимо сформировать html-форму автономной работы, и в открывшемся контекстном меню выбрать **Все задачи/Создать/HTML-форму для автономной работы** (см. Рисунок 70).

Рисунок 70. Запуск задачи создания html-формы для автономной работы пользователя



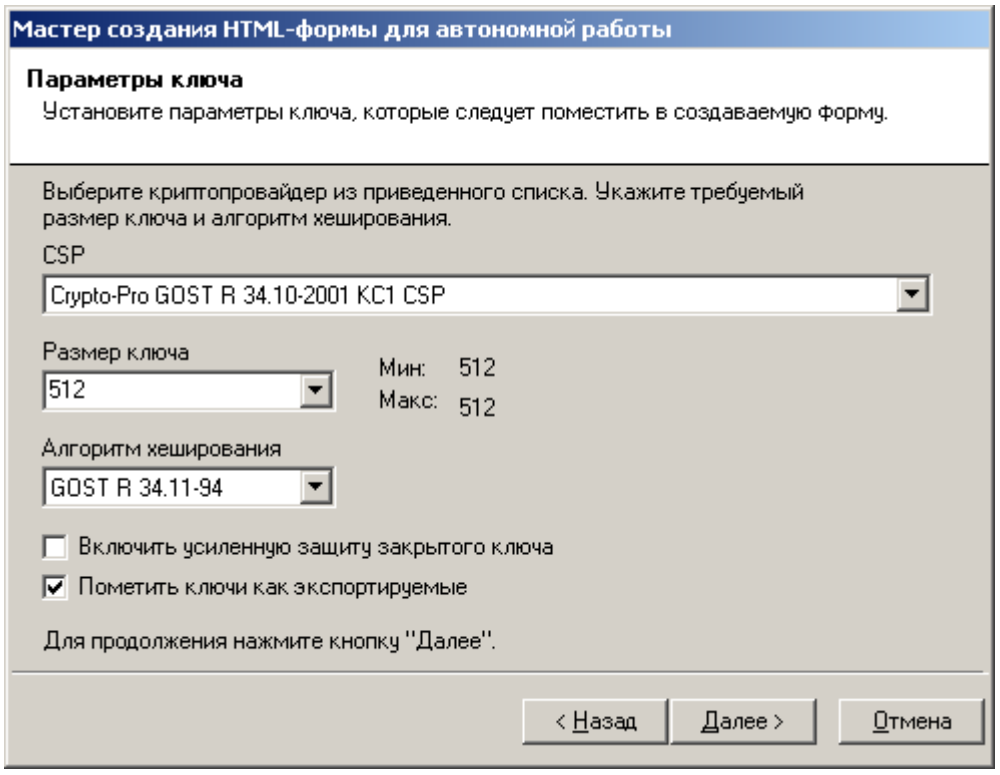
Откроется стартовое окно Мастера создания html-формы для автономной работы (см. Рисунок 71). Для отключения вывода данного окна при последующих запусках Мастера установите переключатель Пропустить этот шаг при следующем запуске. Нажмите кнопку Далее.

Рисунок 71. Стартовое окно Мастера создания html-формы для автономной работы



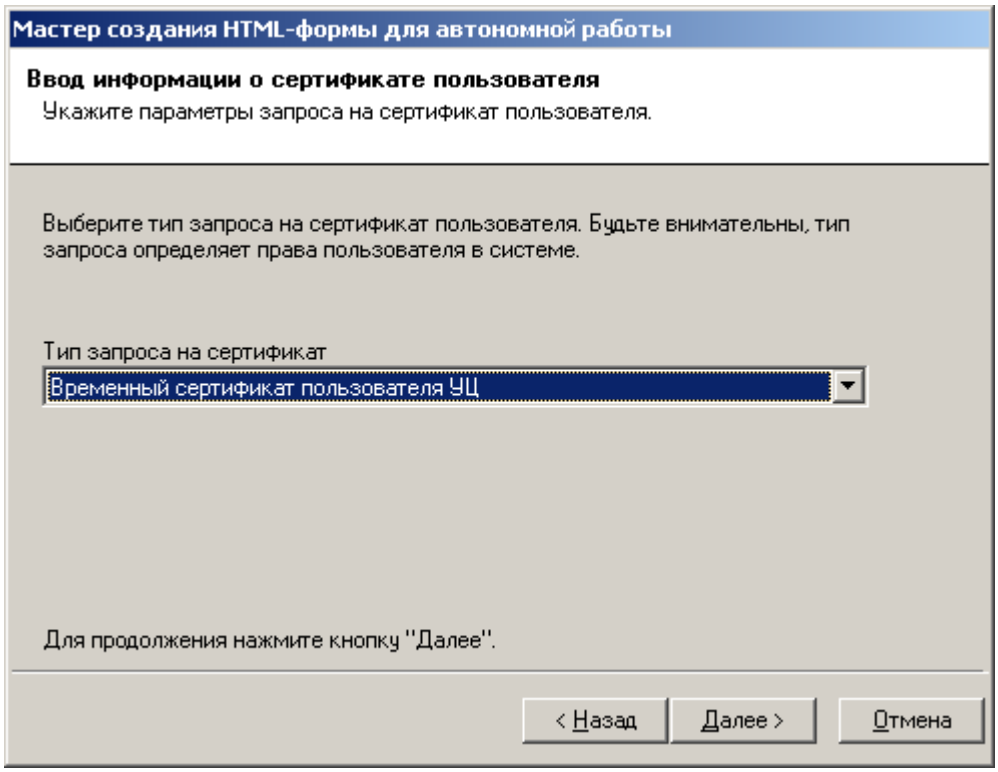
В зависимости от настройки АРМ администратора ЦР (окно **Свойства: АРМ администратора Центра Регистрации**) в части выбора криптопровайдера (флаг **Разрешить выбор CSP**), следующим окном может быть диалоговое окно настройки параметров генерации ключей (см. Рисунок 72).

Рисунок 72. Окно установки параметров генерации ключей Мастера создания html-формы для автономной работы



Следующим окном **Мастера** является окно определения типа сертификата (см. Рисунок 73).

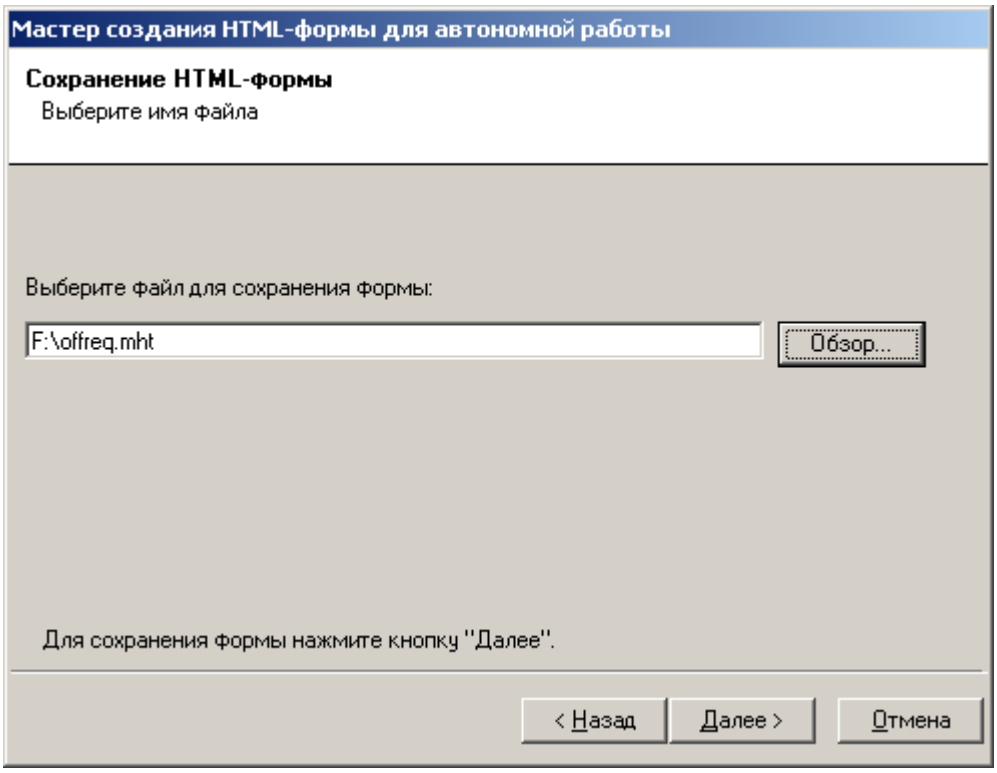
Рисунок 73. Окно определения типа сертификата Мастера создания html-формы для автономной работы



Тип сертификата (состав атрибутов расширения области применения сертификата) выбирается на основе шаблона на сертификат. Список шаблонов редактируется на Центре Регистрации.

В окне сохранения созданной формы **Сохранение html-формы** укажите место сохранения имя файла (см. Рисунок 74). Для удобства выполнения данной операции воспользуйтесь кнопкой **Обзор**.

Рисунок 74. Окно сохранения созданной html-формы



После удачного сохранения html-формы появится финальное окно **Мастера создания html-формы**. Нажмите кнопку **Готово**.

В результате работы данного **Мастера** будет создана html-форма, с помощью которой пользователь без сетевого подключения к Центру Регистрации сможет сформировать ключи и запрос на изготовление сертификата открытого ключа в соответствии с параметрами генерации ключей и областями использования ключей, а также после получения изданного сертификата произвести его установку на своем рабочем месте.

12. Маркер временного доступа

12.1. Определение маркера временного доступа

Маркер временного доступа представляет собой совокупность следующей информации:

- Идентификатор маркера временного доступа;
- Пароль маркера временного доступа.

Идентификатор маркера временного доступа представляет собой натуральное число.

Пароль маркера временного доступа представляет собой символьную последовательность длиной в 6 символов, состоящую из букв латинского алфавита, цифр и специальных символов.

Идентификатор маркера временного доступа и пароль маркера временного доступа находятся между собой во взаимно однозначном соответствии.

Маркер временного доступа формируется Центром Регистрации с использованием приложения **АРМ администратора ЦР**.

Маркер временного доступа имеет ограничения по сроку действия. По умолчанию срок действия маркера временного доступа составляет 1 месяц. Маркер временного доступа становится неактивным: 1) после подтверждения получения сертификата открытого ключа, поступающего от пользователя на Центр Регистрации в момент установки сертификата на рабочем месте пользователя и 2) после истечения срока действия маркера.

12.2. Использование маркера временного доступа

Маркер временного доступа предназначен для идентификации и аутентификации пользователя Удостоверяющего Центра в процессе его взаимодействия с Центром Регистрации ПК «КриптоПро УЦ» посредством использования веб-приложений Центра Регистрации.

Маркер временного доступа используется в следующих случаях:

- При регистрации пользователя УЦ в распределенном режиме с использованием АРМ регистрации пользователя;
- Для предоставления возможности зарегистрированному пользователю, не имеющему ни одного действующего ключа и сертификата открытого ключа, выполнить на своем рабочем месте следующие задачи:
    - Сформировать ключи;
    - Сформировать запрос на сертификат открытого ключа и поставить его в очередь Центра Регистрации на обработку;
    - Сформировать бланк запроса на сертификат открытого ключа для печати его на бумажном носителе;
    - Получить и установить выпущенный сертификат открытого ключа.

При регистрации пользователя УЦ в распределенном режиме с использованием АРМ регистрации, маркер временного доступа создается пользователю автоматически в процессе выполнения процедуры регистрации.

Для зарегистрированного пользователя, маркер временного доступа создается администратором Центра Регистрации.

12.3. Создание маркера временного доступа для зарегистрированного пользователя

Новый маркер временного доступа может быть создан зарегистрированному пользователю, у которого:

- есть маркер временного доступа, но срок его действия истёк;
- есть непросроченный маркер временного доступа, но пользователь забыл пароль доступа этого маркера;
- есть действующий сертификат, но секретный ключ, соответствующий этому сертификату, неработоспособен;
- есть непросроченный сертификат, но истёк срок действия секретного ключа, соответствующего этому сертификату;
- истёк срок действия сертификата.

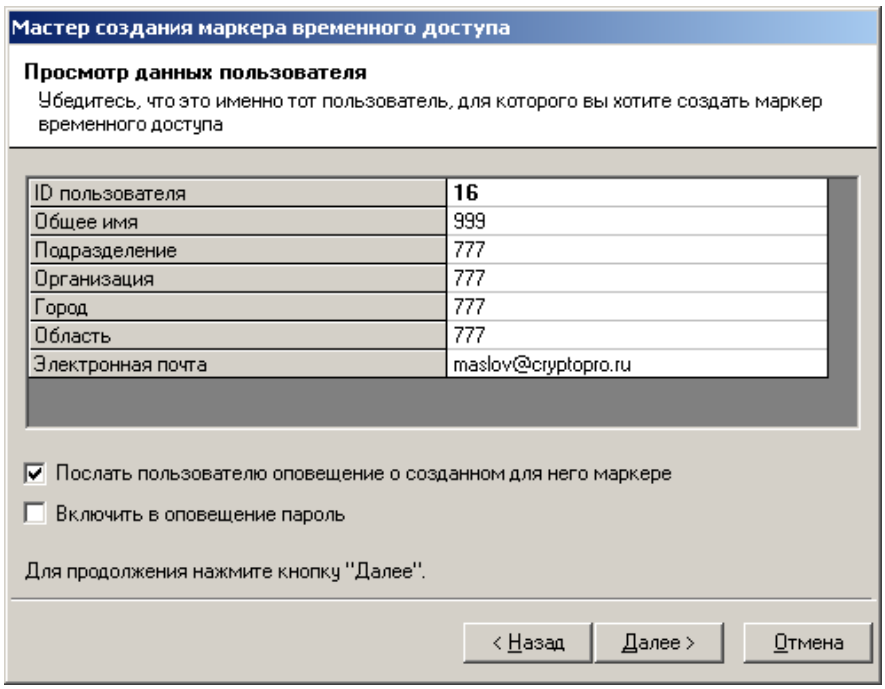
Для создания маркера временного доступа зарегистрированному пользователю необходимо выполнить задачу **Создать Маркер временного доступа** в приложении **АРМ администратора Центра Регистрации** (см. Рисунок 75).

Рисунок 75. Запуск задачи создания маркера временного доступа

Дальнейшие действия по созданию маркера временного доступа осуществляются с использованием **Мастера создания маркера временного доступа**.

Вследствие того, что создание маркера временного доступа понижает надежность системы в части аутентификации зарегистрированных пользователей, убедитесь, что выбран необходимый пользователь для данной операции (см. Рисунок 76).

Рисунок 76. Просмотр данных пользователя Мастера создания маркера временного доступа

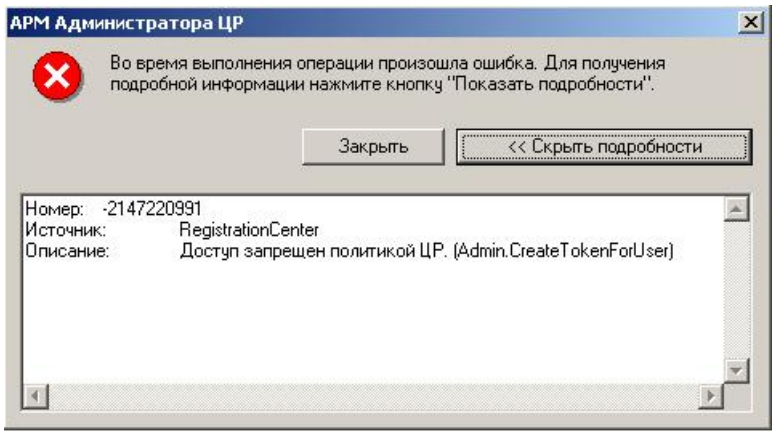


Установка опции **Послать пользователю оповещение о созданном для него маркере** обеспечивает отправку почтового сообщения в адрес пользователя с уведомлением о создании маркера доступа.

Если установить опцию **Включить в оповещение пароль**, то почтовое сообщение будет также содержать пароль маркера временного доступа.

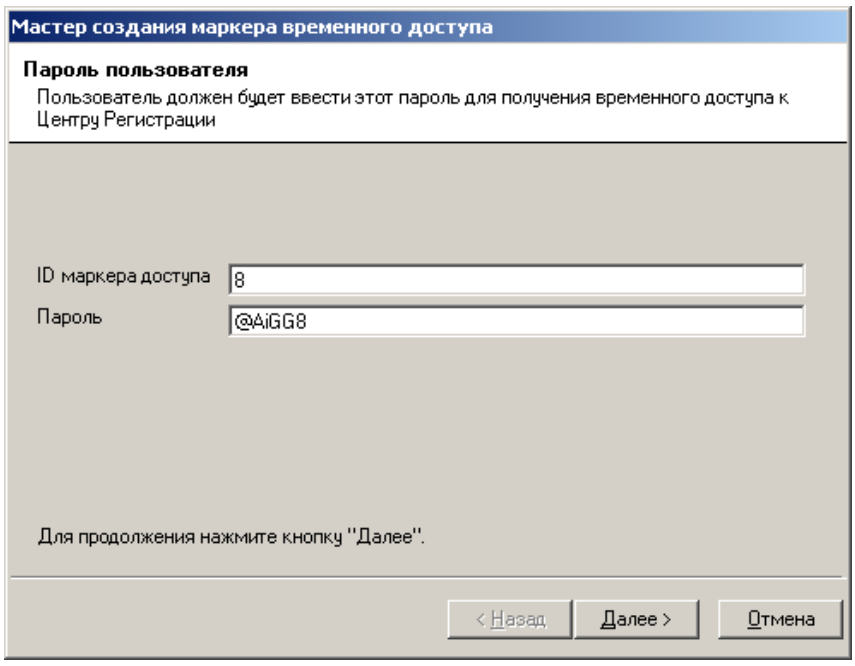
Если для роли, под которой делается попытка создания маркера временного доступа на АРМе, это действие не разрешено на ЦР, то выводится стандартное окно с сообщением об ошибке. Пример окна отображен ниже (см. Рисунок 77).

Рисунок 77. Окно ошибки о невозможности создания маркера временного доступа



После создания маркера временного доступа, Мастер отображает его в диалоговом окне (см. Рисунок 78).

Рисунок 78. Окно отображения созданного маркера временного доступа Мастера создания маркера временного доступа



Администратору, выполняющему процедуру создания маркера временного доступа для зарегистрированного пользователя, требуется запомнить его и сообщить данный маркер пользователю (например, по телефону).

Для завершения процедуры нажмите кнопку **Далее,** откроется финальное окно **Мастера**, информирующее об успешном создании маркера – нажмите кнопку **Готово**.

13. Объекты Центра Сертификации

Администратору с использованием консоли предоставляется доступ к некоторым объектам Центра Сертификации. К этим объектам относятся:

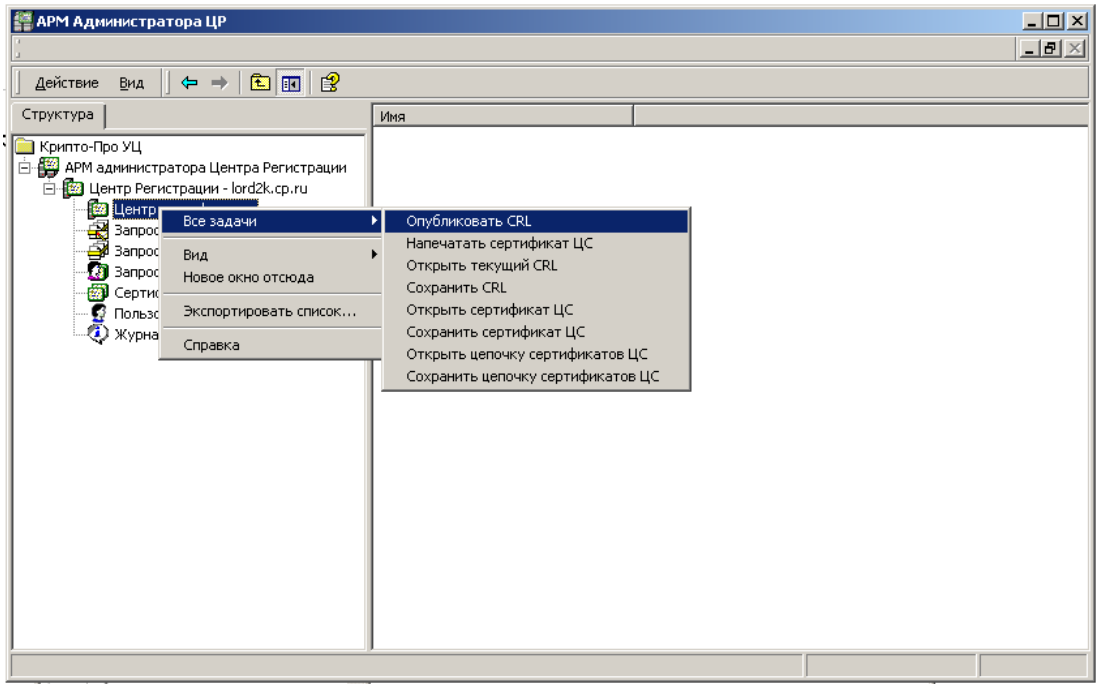
- сертификат Центра Сертификации. Данный объект представляет собой сертификат Центра Сертификации, к которому подключен Центр Регистрации из активного подключения к ЦР;
- цепочка сертификатов Центра Сертификации. Данный объект представляет собой последовательность (цепочку) сертификатов, начиная с сертификата корневого Центра Сертификации, промежуточных Центров Сертификации в иерархии и заканчивая Центром Сертификации, к которому подключен Центр Регистрации из активного подключения к ЦР;
- список отозванных сертификатов Центра Сертификации. Данный объект представляет собой список отозванных сертификатов Центра Сертификации, к которому подключен Центр Регистрации из активного подключения к ЦР.

Для объектов Центра Сертификации возможно выполнение следующих задач:

- сертификат Центра Сертификации;
  - печать – формирование формы для печати;
  - открыть – отображение сертификата в окне свойств сертификата;
  - сохранить – сохранение сертификата в виде файла на магнитном носителе в формате Base-64.
- цепочка сертификатов Центра Сертификации;
  - открыть – отображение цепочки сертификатов в окне свойств цепочки сертификатов;
  - сохранить – сохранение цепочки сертификатов в виде файла (p7b) на магнитный носитель в формате Base-64.
- список отозванных (аннулированных) сертификатов Центра Сертификации (CRL)
  - опубликовать – создание запроса на выпуск CRL с текущей датой актуальности;
  - открыть – отображение CRL в окне свойств списка отозванных сертификатов;
  - сохранить – сохранение CRL в виде файла на магнитный носитель в формате Base-64.

Выполнение задач осуществляется из контекстного меню задач папки **Центр Сертификации** текущего активного подключения к ЦР (см. Рисунок 79).

Рисунок 79. Окно задач элемента Центр Сертификации текущего активного подключения к ЦР



14. Протоколирование работы

Программным обеспечением Центра Регистрации ведется протоколирование работы в базу данных Центра Регистрации.

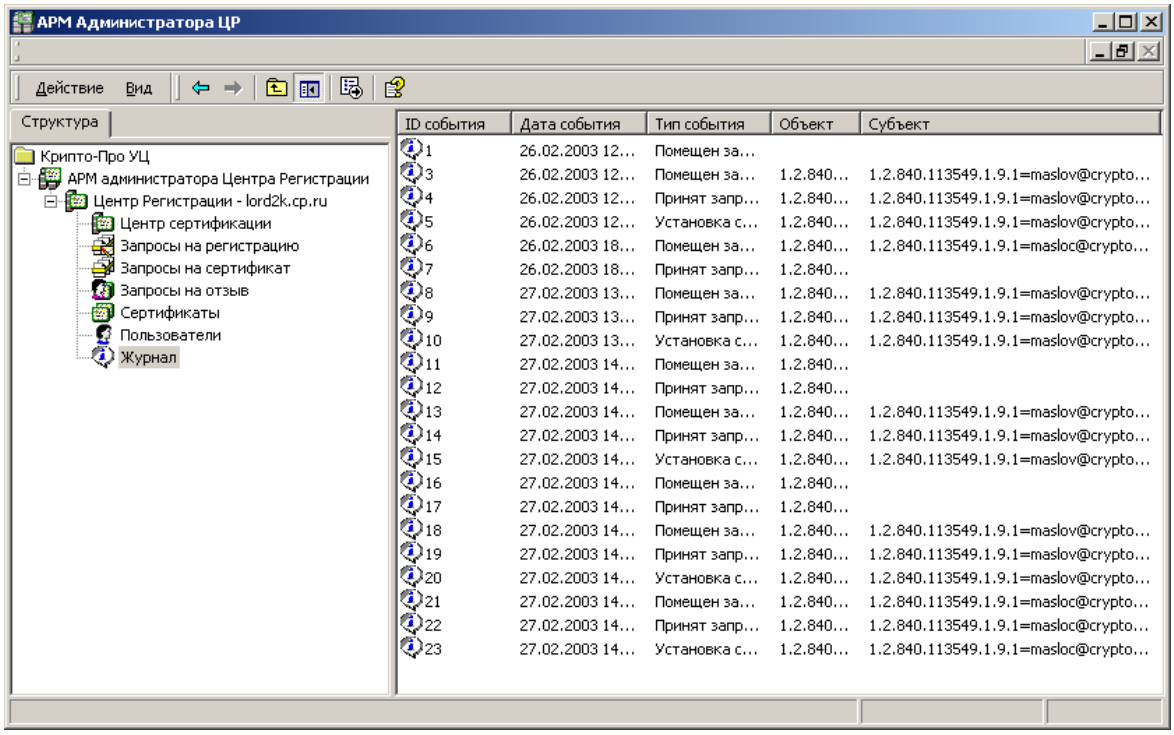
Протоколирование работы включает в себя фиксацию следующих событий:

- факты регистрации администраторов, пользователей и приложений;
- факты изготовления сертификатов;
- факты отзыва, приостановления, возобновления действия сертификатов;
- факты прохождения запросов на сертификаты и ответов на них;
- факты сохранения и очищения журнала.

Протоколирование работы Центра Регистрации выполняется в автоматическом режиме, подразумевая постоянную запись в журнал всех вышеперечисленных событий.

АРМ администратора ЦР предоставляет возможность просматривать журнал работы Центра Регистрации. Эта функциональность представлена в папке **Журнал**.

Рисунок 80. Папка Журнал.



Журнал организован в виде списка, состоящего из следующих столбцов:

- Идентификатор события – уникальный номер зарегистрированного события;
- Дата события – дата и время наступления события;
- Тип события – тип события;
- Объект – пользователь, выполнивший действие;
- Субъект – пользователь, для объектов, управления которого было выполнено действие;
- Информация – дополнительная информация о событии.

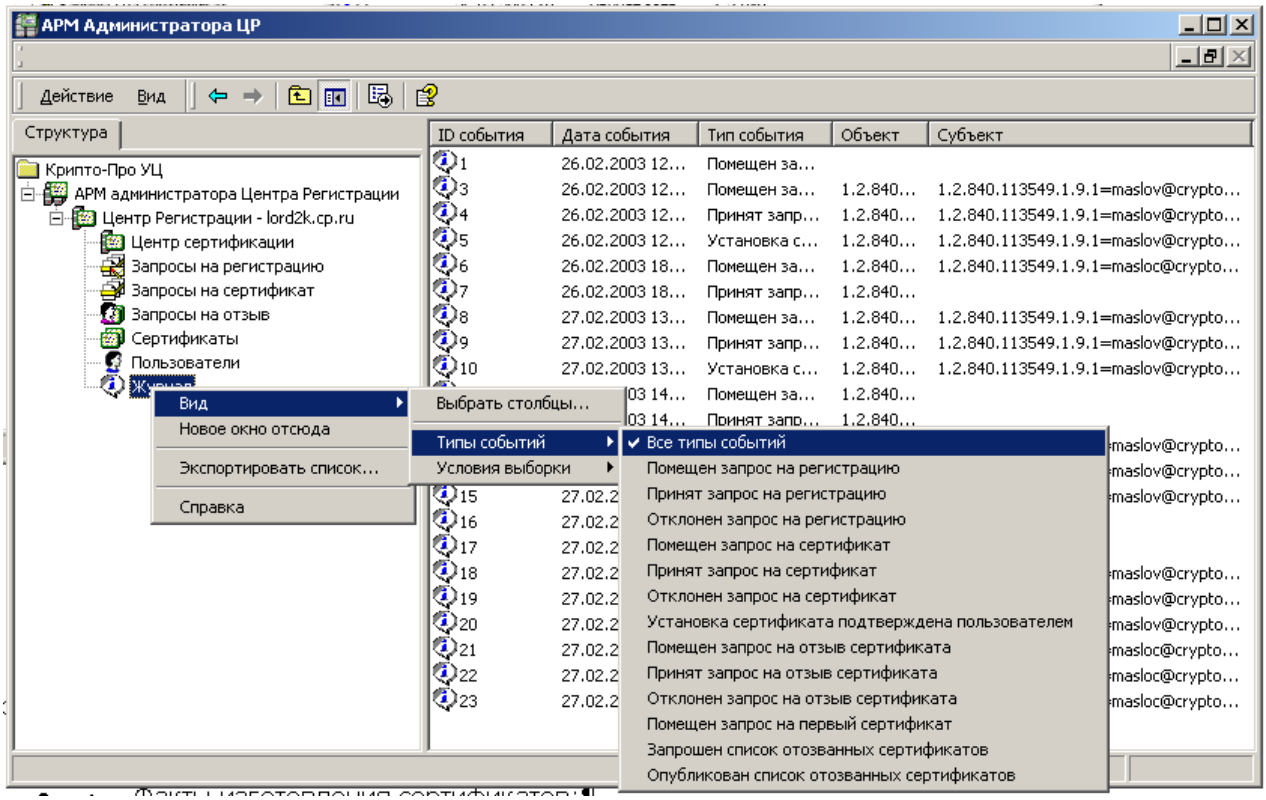
Для анализа журнала событий Центра Регистрации может использоваться фильтрация журнала, выполняемая через контекстное меню папки **Журнал** (см. Рисунок 81).

Фильтрация может осуществляться по типу событий или по значению полей событий (условия выборки).

Например, при фильтрации по значению полей событий доступны следующие поля событий:

- Идентификатор события;
- Дата события;
- Тип события;
- Объект;
- Субъект;
- Комментарий;
- Важность события.

Рисунок 81. Окно задач папки Журнал



Работа с журналом регистрации событий подробно рассматривается в Разделе 16 настоящего руководства «Журнал регистрации событий Центра Регистрации».

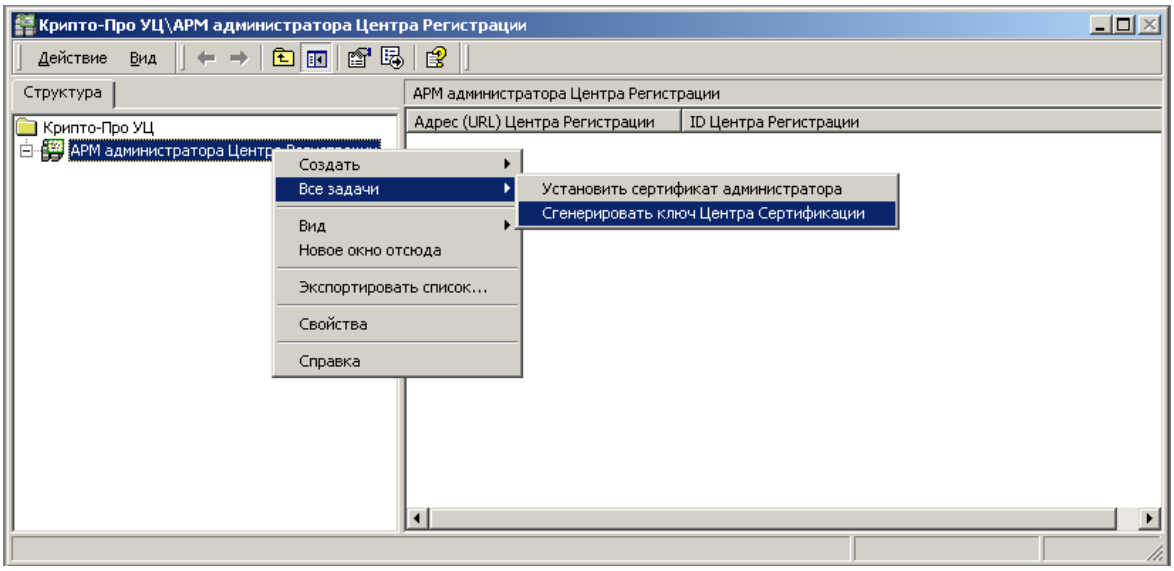
15. Генерация ключей Центра Сертификации

Программное обеспечение АРМ администратора предоставляет возможность выполнить процедуру генерации ключей Центра Сертификации Удостоверяющего Центра (своего или подчиненного) и записи их на ключевой носитель, для последующего использования при установке Центра Сертификации УЦ.

Процедура генерации ключей Центра Сертификации должна быть выполнена на рабочем месте администратора, не имеющего подключений к линиям связи (режим offline).

Для выполнения процедуры генерации ключей Центра Сертификации запустите задачу **Сгенерировать ключ Центра Сертификации** из контекстного меню узла **АРМ администратора Центра Регистрации** консоли (см. Рисунок 82).

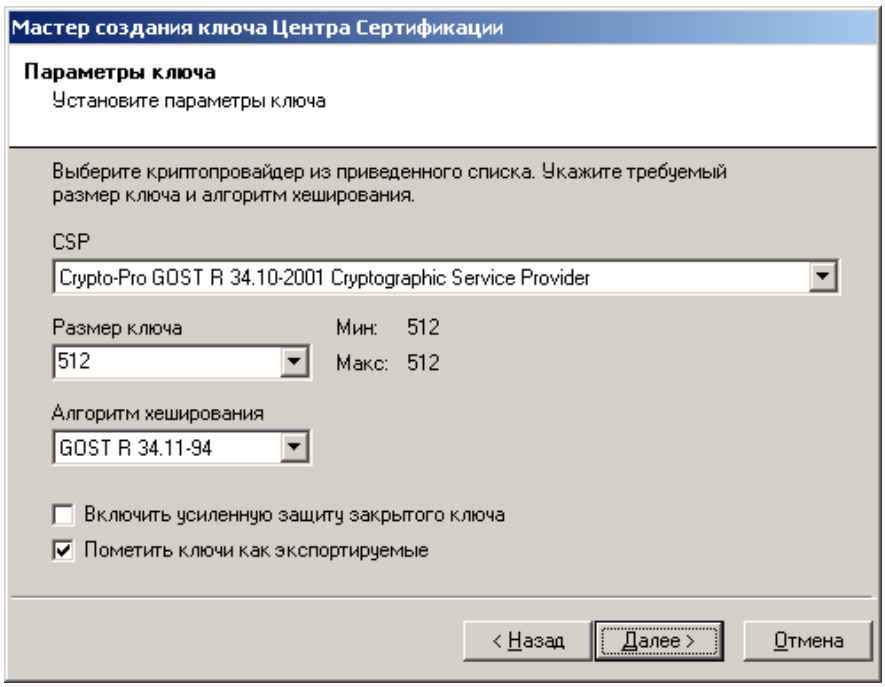
Рисунок 82. Запуск задачи генерации ключей Центра Сертификации



Далее необходимо следовать указаниям Мастера создания ключа Центра Сертификации.

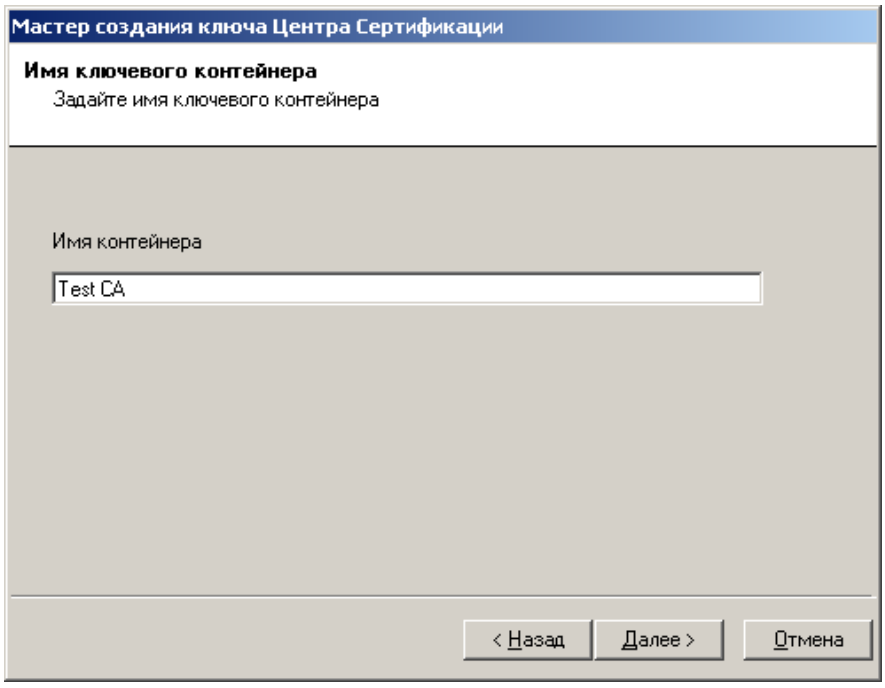
В окне определения параметров ключа **Мастера** (см. Рисунок 83) выберите алгоритм формирования ключа (список CSP). Появление данного окна зависит от параметра **Разрешить выбор CSP** окна свойств АРМ (см. Рисунок 7).

Рисунок 83. Окно определения параметров ключа Мастера создания ключа ЦС



В следующем окне Мастера необходимо задать имя создаваемого ключевого контейнера для ключей ЦС (см. Рисунок 84).

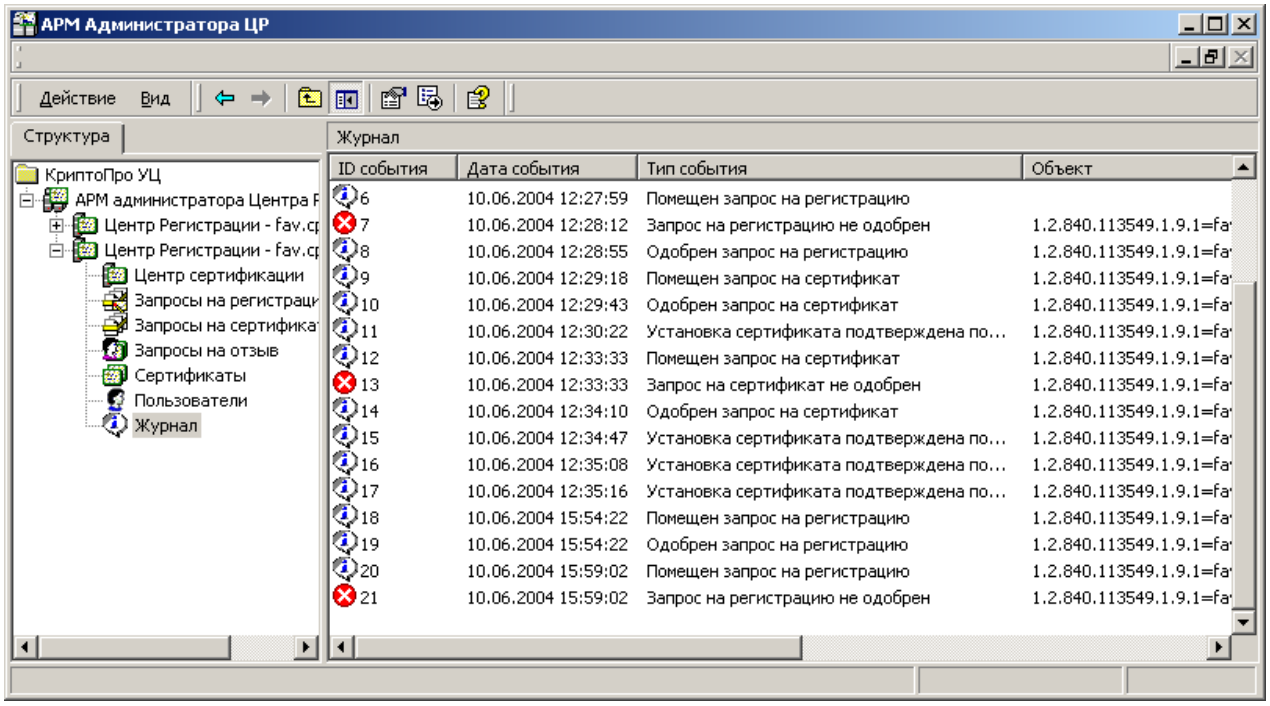
Рисунок 84. Окно определения имени ключевого контейнера Мастера создания ключа ЦС



16. Журнал регистрации событий Центра Регистрации

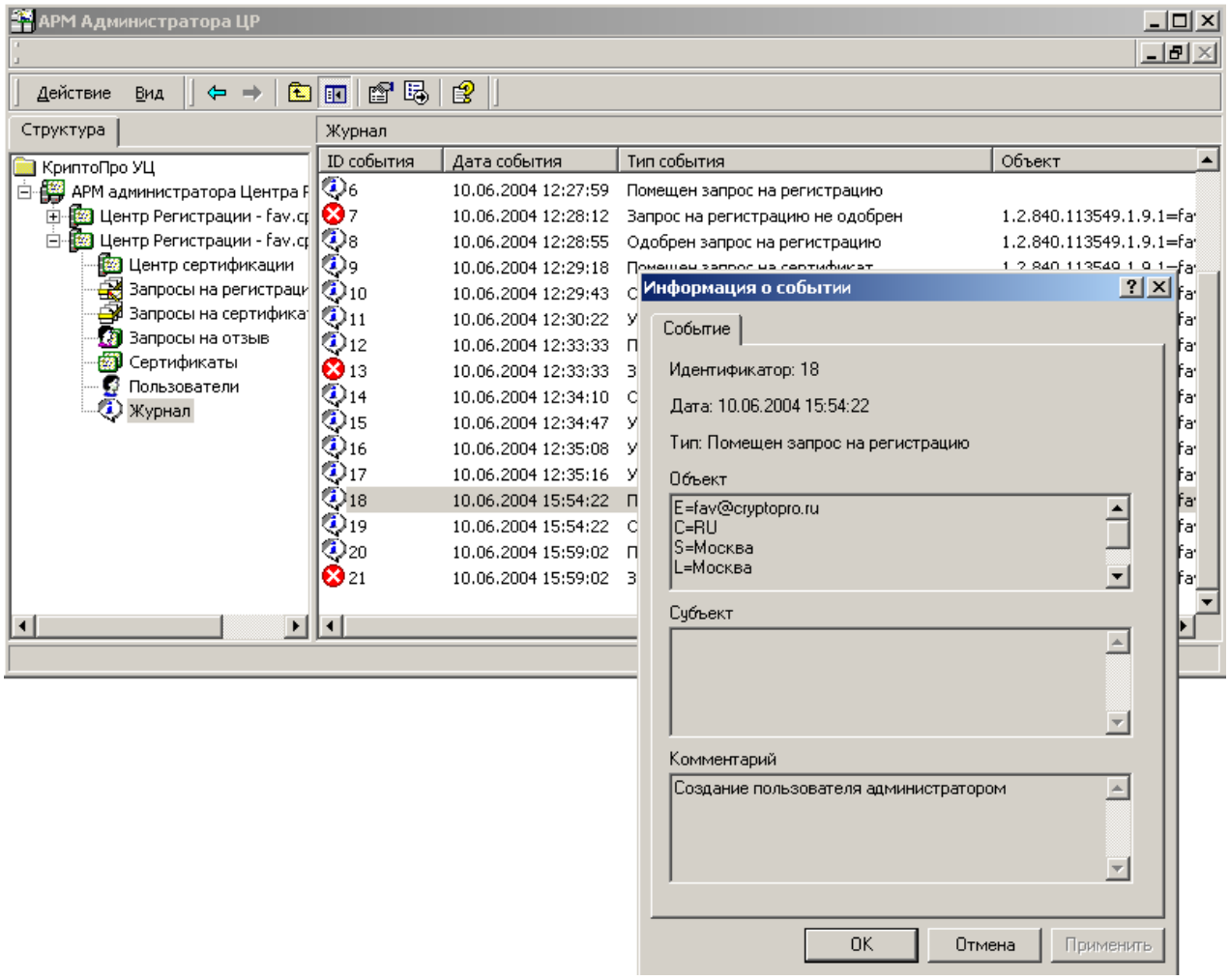
Журнал регистрации событий Центра Регистрации представляет собой последовательный набор записей в базе данных Центра Регистрации. Каждая запись представляется в виде отдельной строки, содержащей определенные информационные поля. Просмотр записей журнала регистрации событий осуществляется с помощью программного обеспечения **АРМ администратора ЦР** посредством узла **Журнал.**

Рисунок 85. Журнал регистрации событий Центра Регистрации



Подробный просмотр события осуществляется двойным нажатием левой кнопки мыши, либо выбором пункта меню **Свойства** контекстного меню, открывающегося при нажатии правой кнопки мыши.

Рисунок 86. Окно просмотра информации о событии



В состав записи о событии входят следующие информационные поля:

- Важность – важность события (Обычная, Предупреждение, Ошибка)
- ID события – уникальный номер зарегистрированного события;
- Дата события – дата и время наступления события;
- Тип события – тип события;
- Объект – пользователь, выполнивший действие;
- Субъект – пользователь, для объектов управления которого было выполнено действие;
- Информация – дополнительная информация о событии.

Некоторые события, фиксирующиеся в журнале, не содержат значения некоторых полей. Например, поля Объект и Субъект могут содержать только идентификационные данные тех лиц, которые зарегистрированы в Удостоверяющем Центре. Поэтому, например, при регистрации пользователя в распределенном режиме (пользователь сам формирует и передает запрос на регистрацию) событие «Помещен запрос на регистрацию» не содержит значений полей Объект и Субъект – Объектом и Субъектом является регистрирующийся пользователь, а он еще не зарегистрирован в УЦ, либо при выполнении Администратором задачи Центра Сертификации «Опубликовать

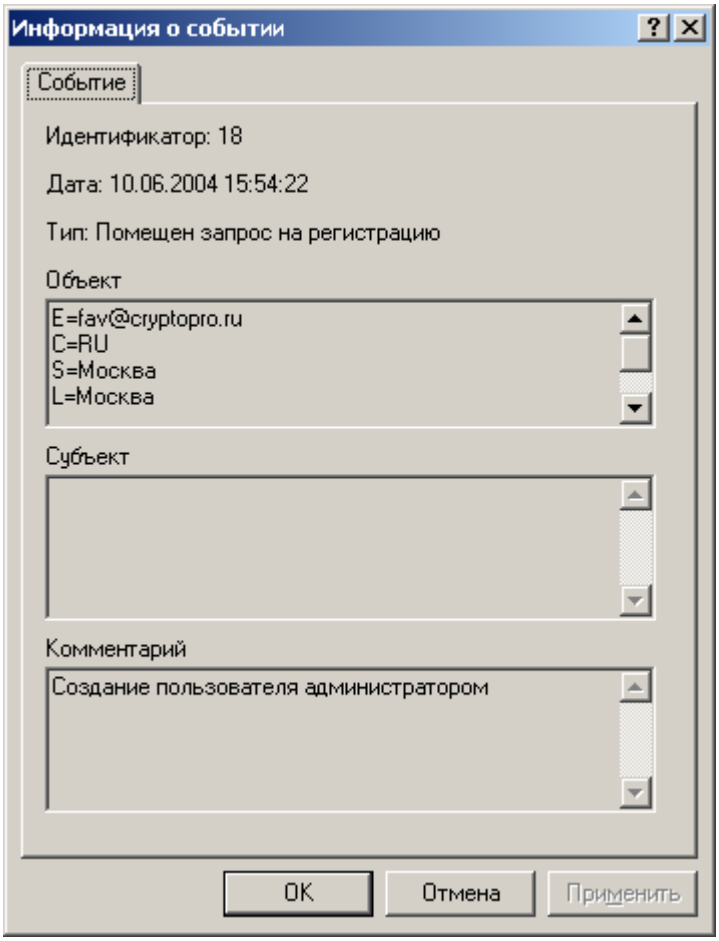
текущий CRL» событие «Опубликован список отозванных сертификатов» не содержит значения поля Субъект, поскольку список отозванных сертификатов не принадлежит к объекту управления какого-либо зарегистрированного пользователя.

16.1. Описание событий, регистрирующихся в Журнале

В журнале осуществляется автоматическая регистрация следующих типов событий:

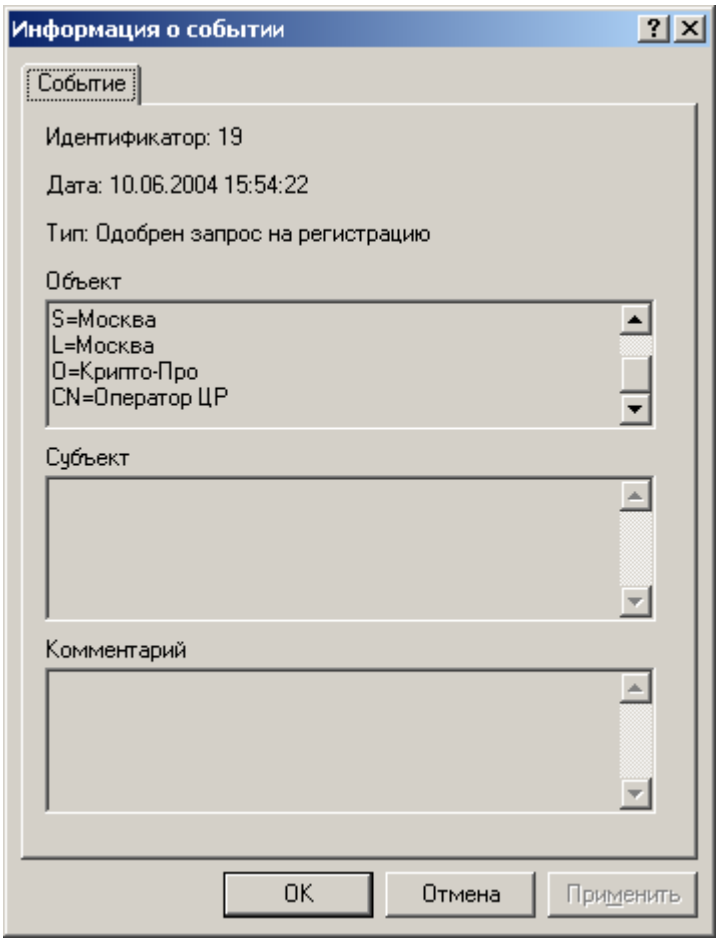
- **Помещен запрос на регистрацию** – данное событие возникает при успешном выполнении методов Registration.CreateRequest и Registration.CreateRequestByAdmin (важность события – обычная). Вызов метода Registration.CreateRequest происходит при регистрации пользователя в распределенном режиме, т.е. непосредственно регистрирующимся лицом, поэтому поля Объект и Субъект данного события пусты. Вызов метода Registration.CreateRequestByAdmin осуществляется с АРМ Администратора ЦР привилегированным пользователем (идентификационные данные приведены в поле Объект), на что указывает содержание поля Комментарий – «Создание пользователя администратором»;

Рисунок 87. Событие Помещен запрос на регистрацию



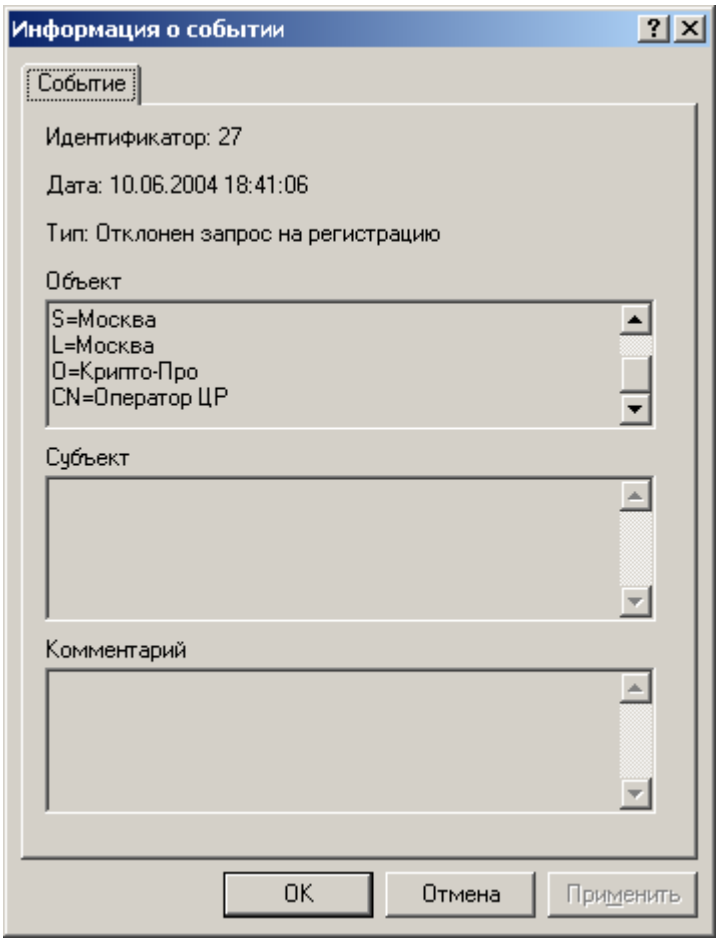
- **Одобрен запрос на регистрацию** – данное событие возникает при успешном выполнении метода Registration.AcceptRequest (важность события – обычная). Поле Объект данного события содержит идентификационные данные пользователя выполнившего указанный метод;

Рисунок 88. Событие Одобрен запрос на регистрацию



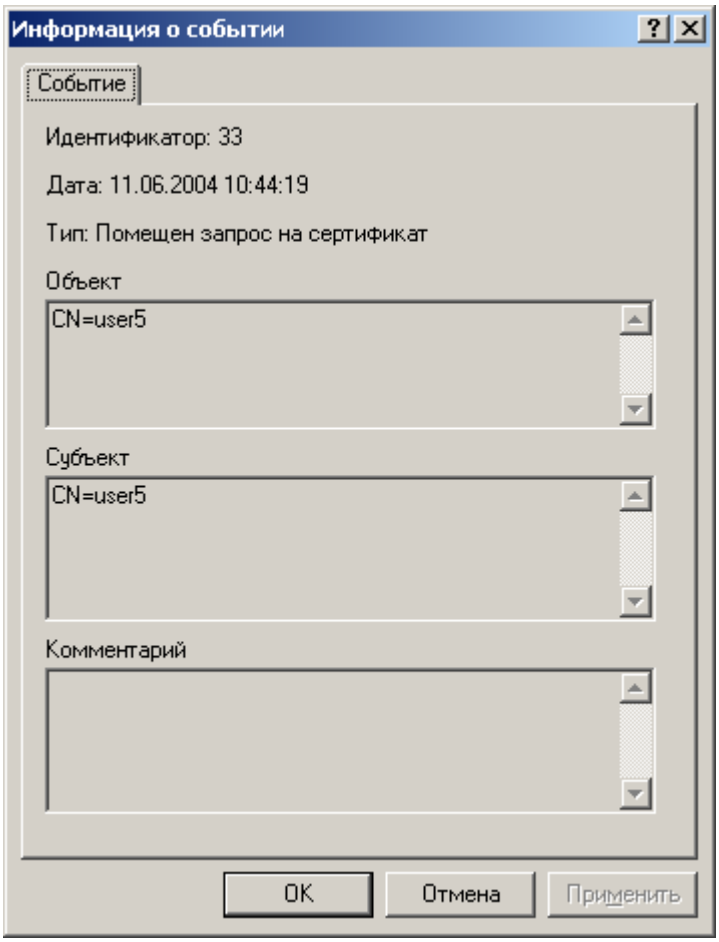
- **Отклонен запрос на регистрацию** – данное событие возникает при успешном выполнении метода Registration.DenyRequest (важность события – предупреждение). Поле Объект данного события содержит идентификационные данные пользователя выполнившего указанный метод;

Рисунок 89. Событие Отклонен запрос на регистрацию



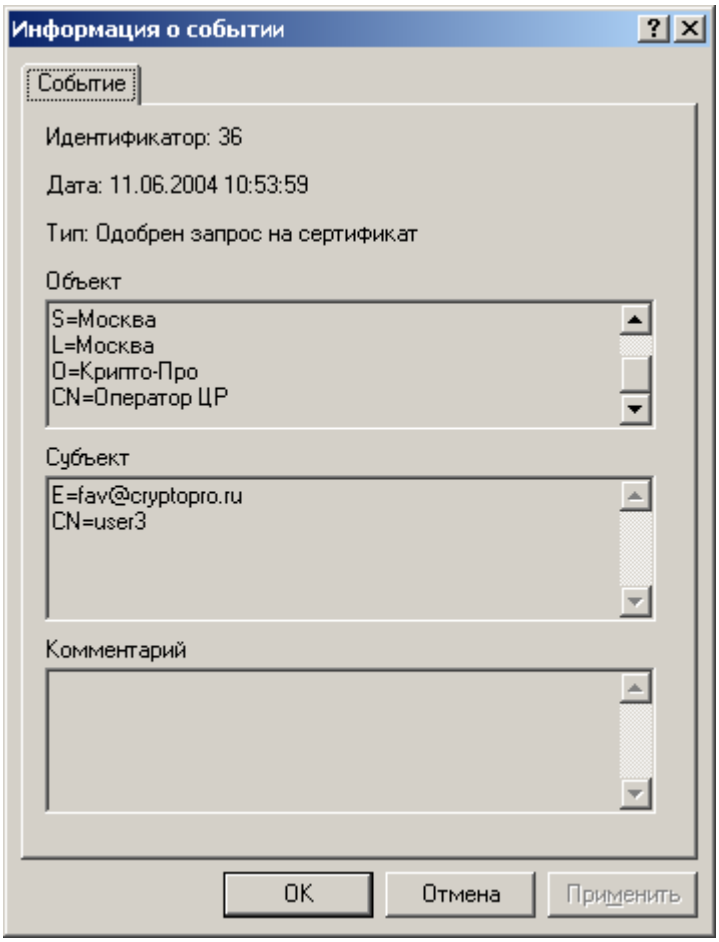
- **Помещен запрос на сертификат** – данное событие возникает при успешном выполнении метода CertRequest.SubmitRequest (важность события – обычная). Обработка метода CertRequest.SubmitRequest осуществляется в соответствии с политикой «Обработка подписанных запросов». В связи с этим на успешное выполнение указанного метода влияют два типа настроек Центра Регистрации : Настройки разрешений на выполнение метода и Настройки политики обработки подписанных запросов;

Рисунок 90. Событие Помещен запрос на сертификат



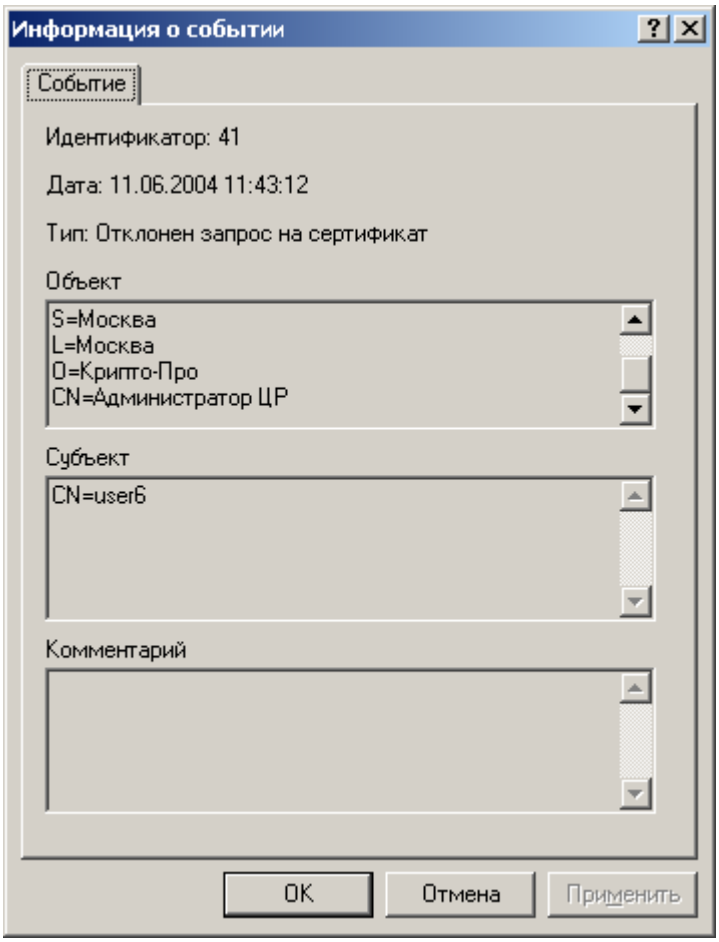
- **Одобрен запрос на сертификат** - данное событие возникает при успешном выполнении метода CertRequest.AcceptRequest и CertRequest.AcceptFirstRequest (важность события – обычная). Поле Объект данного события содержит идентификационные данные пользователя, выполнившего указанный метод, поле Субъект – идентификационные данные пользователя, содержащиеся в запросе на сертификат;

Рисунок 91. Событие Одобрен запрос на сертификат



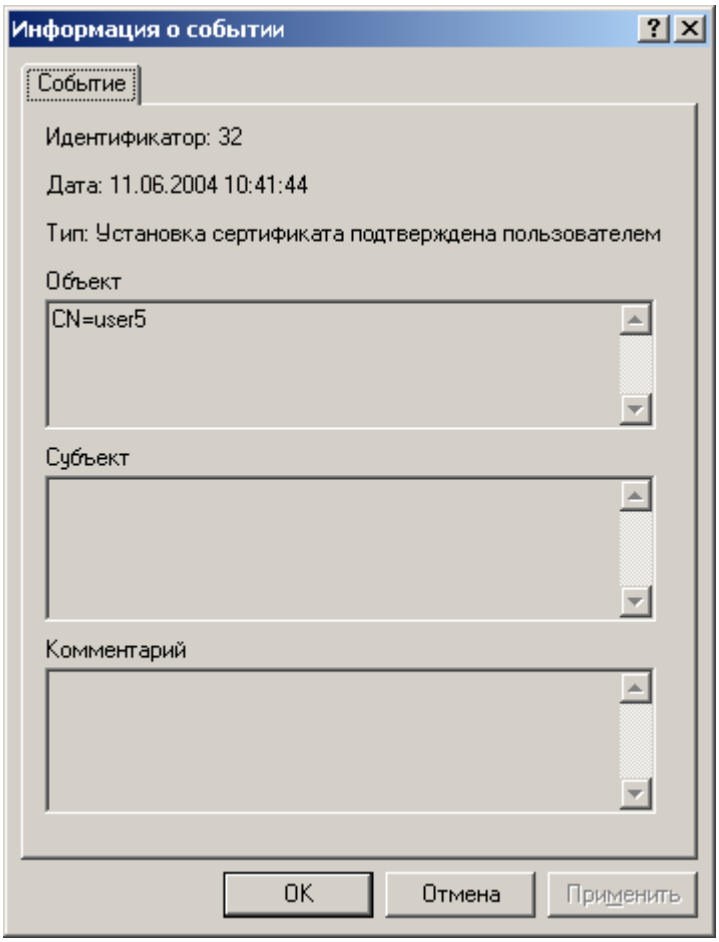
- **Отклонен запрос на сертификат** - данное событие возникает при успешном выполнении метода CertRequest.DenyRequest (важность события – предупреждение). Поле Объект данного события содержит идентификационные данные пользователя, выполнившего указанный метод, поле Субъект – идентификационные данные пользователя, содержащиеся в запросе на сертификат;

Рисунок 92. Событие Отклонен запрос на сертификат



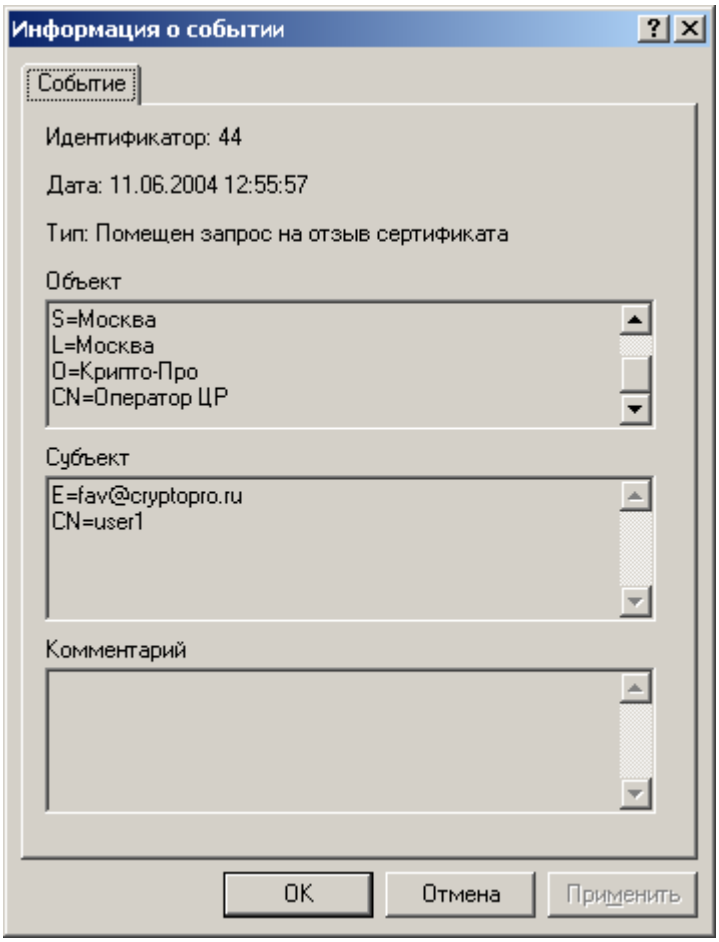
- **Установка сертификата подтверждена пользователем** - данное событие возникает при успешном выполнении метода CertRequest.ConfirmRequest (важность события – обычная). Поле Объект данного события содержит идентификационные данные пользователя, выполнившего указанный метод, поле Субъект – идентификационные данные пользователя, установка сертификата которого была подтверждена;

Рисунок 93. Установка сертификата подтверждена пользователем



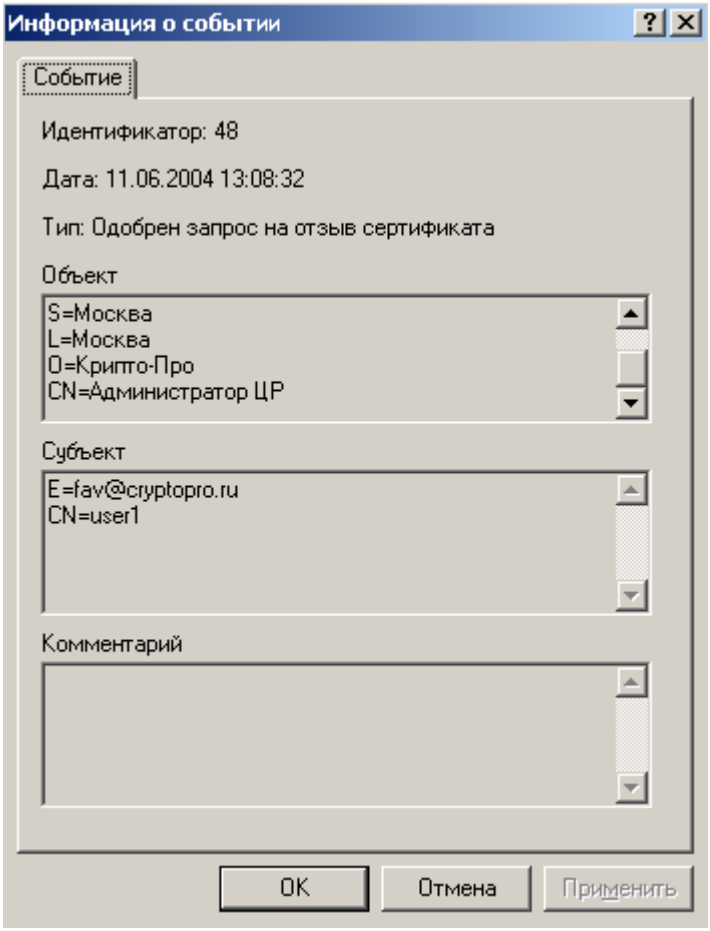
- **Помещен запрос на отзыв сертификата** - данное событие возникает при успешном выполнении методов RevokeRequest.SubmitRequest, RevokeRequest.SubmitHoldRequest и RevokeRequest.SubmitUnHoldRequest (важность события – обычная). Обработка указанных методов осуществляется в соответствии с политикой «Обработка запросов на отзыв». В связи с этим на успешное выполнение указанного метода влияют два типа настроек Центра Регистрации : Настройки разрешений на выполнение метода и Настройки политики обработки запросов на отзыв;

Рисунок 94. Событие Помещен запрос на отзыв сертификата



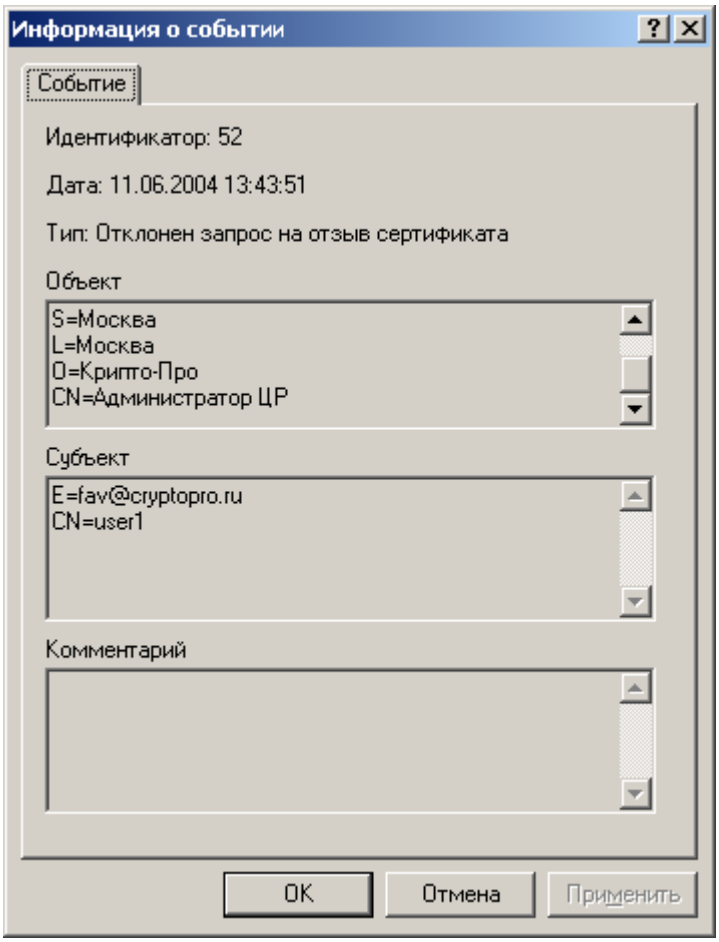
- **Одобрен запрос на отзыв сертификата** - данное событие возникает при успешном выполнении метода RevokeRequest.AcceptRequest (важность события – обычная). Поле Объект данного события содержит идентификационные данные пользователя, выполнившего указанный метод, поле Субъект – идентификационные данные пользователя, сертификат которого был отозван;

Рисунок 95. Одобрен запрос на отзыв сертификата



- **Отклонен запрос на отзыв сертификата** - данное событие возникает при успешном выполнении метода RevokeRequest.DenyRequest (важность события – предупреждение). Поле Объект данного события содержит идентификационные данные пользователя, выполнившего указанный метод, поле Субъект – идентификационные данные пользователя, сертификат которого планировалось отозвать;

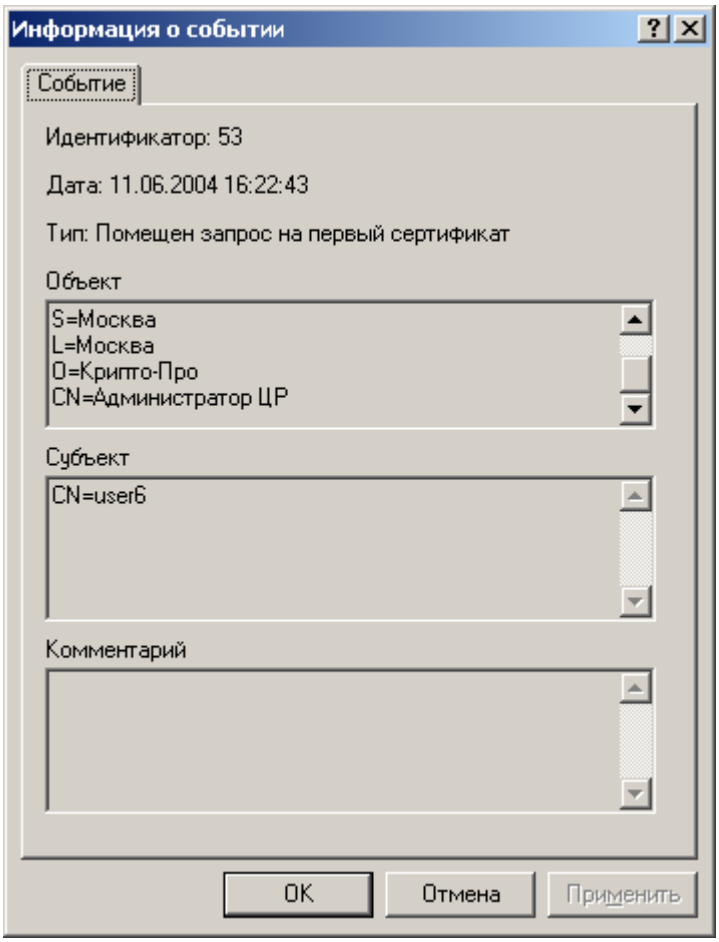
Рисунок 96. Событие Отклонен запрос на отзыв сертификата



Описанные события «Помещен запрос на отзыв сертификата», «Одобрен запрос на отзыв сертификата», «Отклонен запрос на отзыв сертификата» относятся не только к операциям, связанным непосредственно с аннулированием (отзывом) сертификатов. Данные события относятся также и к запросам на приостановление и возобновление действия сертификатов. Точное определение типа запроса осуществляется на основе свойств рассматриваемых запросов, содержащихся в узле «Запросы на отзыв» приложения АРМ Администратора ЦР.

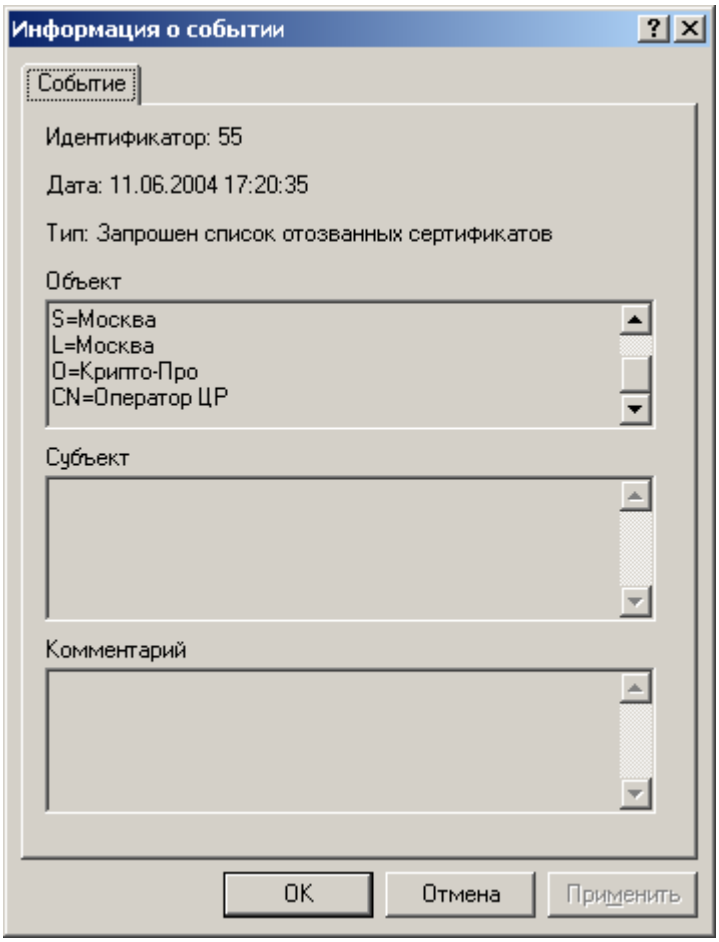
- **Помещен запрос на первый сертификат** - данное событие возникает при успешном выполнении метода CertRequest.SubmitFirstRequest (важность события – обычная). Обработка метода CertRequest.SubmitFirstRequest осуществляется в соответствии с политикой «Обработка неподписанных запросов». В связи с этим на успешное выполнение указанного метода влияют два типа настроек Центра Регистрации : Настройки разрешений на выполнение метода и Настройки политики обработки неподписанных запросов;

Рисунок 97. Событие Помещен запрос на первый сертификат



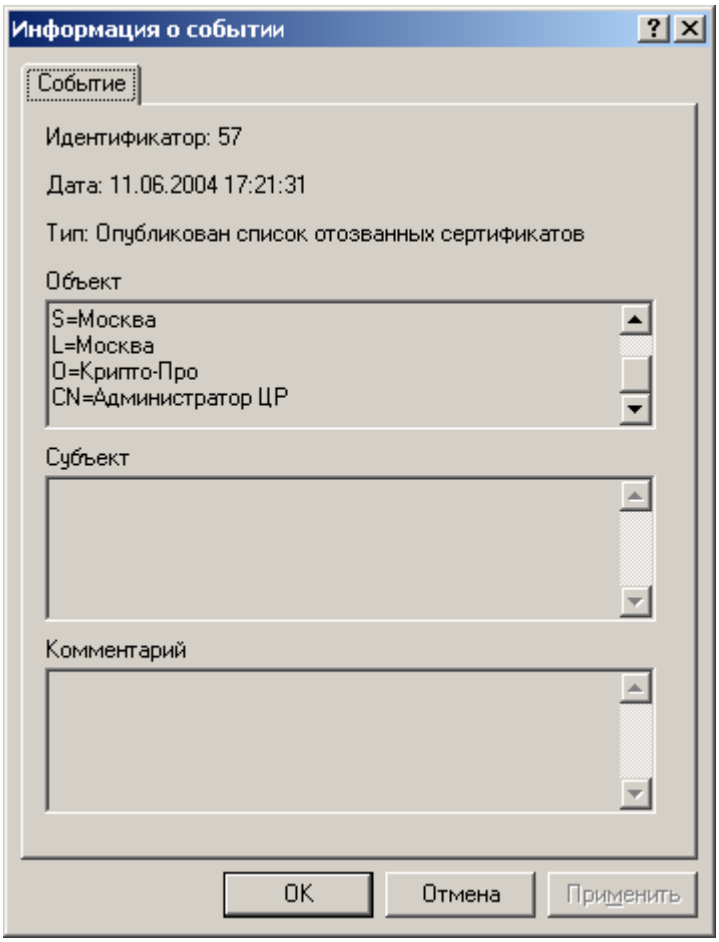
- **Запрошен список отозванных сертификатов** - данное событие возникает при успешном выполнении метода CertView.GetCRL (важность события – обычная). Поле Объект данного события содержит идентификационные данные пользователя, запросившего список отозванных сертификатов;

Рисунок 98. Событие Запрошен список отозванных сертификатов



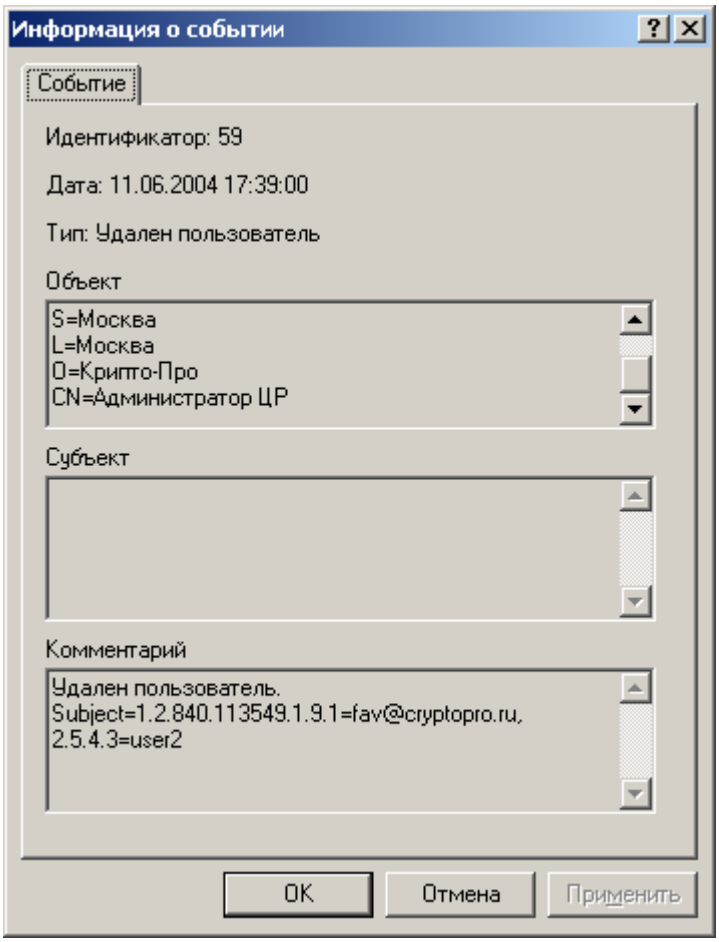
- **Опубликован список отозванных сертификатов** - данное событие возникает при успешном выполнении метода Admin.PublishCRL (важность события – обычная). Поле Объект данного события содержит идентификационные данные пользователя, направившего запрос на публикацию списка отозванных сертификатов;

Рисунок 99. Событие Опубликован список отозванных сертификатов



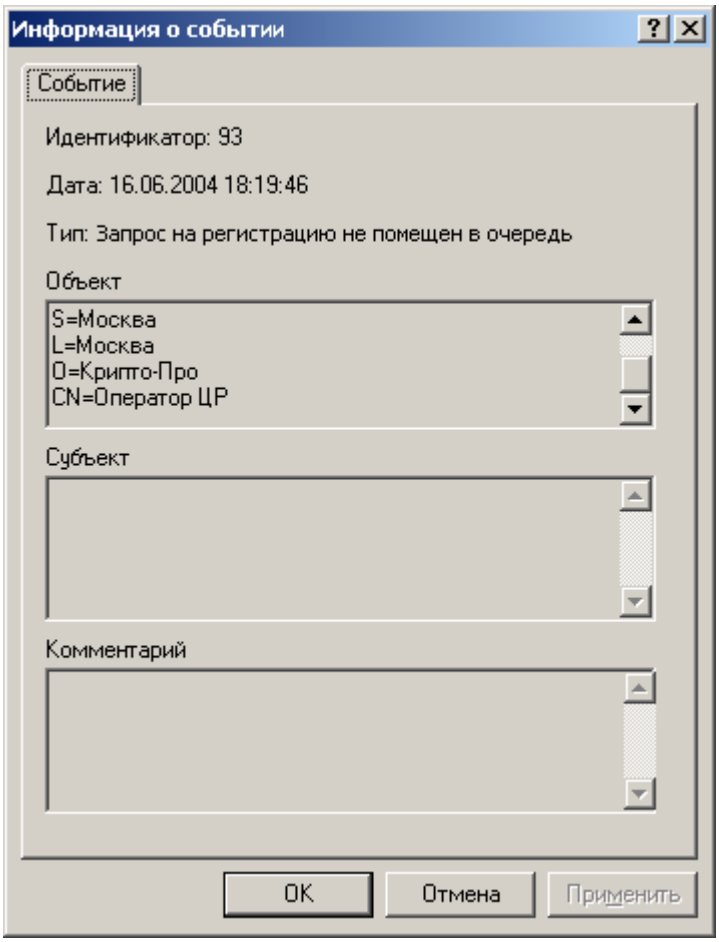
- **Удален пользователь** - данное событие возникает при успешном выполнении метода UserView.DeleteUser (важность события – обычная). Поле Объект данного события содержит идентификационные данные пользователя, выполнившего удаление учетной записи пользователя, поле Комментарий – идентификационные данные удаленного пользователя;

Рисунок 100. Событие Удален пользователь



- **Запрос на регистрацию не помещен в очередь** – данное событие возникает при выполнении методов Registration.CreateRequest и Registration.CreateRequestByAdmin в том случае, если успешное выполнение пользователем одного из указанных методов противоречит настройкам политик Центра Регистрации (важность события – ошибка). Вызов метода Registration.CreateRequest происходит при регистрации пользователя в распределенном режиме, т.е. непосредственно регистрирующимся лицом, поэтому поля Объект и Субъект данного события пусты. Вызов метода Registration.CreateRequestByAdmin осуществляется с АРМ Администратора ЦР привилегированным пользователем (идентификационные данные приведены в поле Объект);

Рисунок 101. Событие Запрос на регистрацию не помещен в очередь

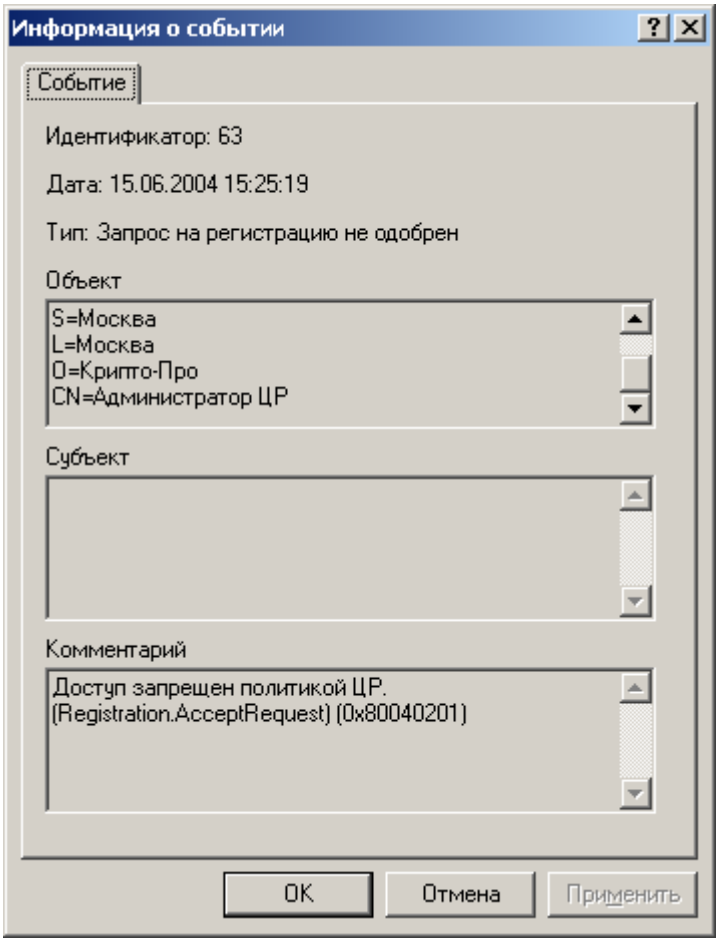


Здесь и далее использование выражения «важность события – ошибка» не означает регистрацию в системе ошибки при работе АРМ Администратора ЦР (такого рода сообщения отображаются в журнале приложений операционной системы). Возникновение таких событий происходит по причине настроек политик Центра Регистрации.

Пример: Настройки политик Центра Регистрации в стандартной конфигурации не позволяют Администратору осуществлять регистрацию пользователей (эти функции возлагаются на Оператора). При попытке Администратором выполнить указанные действия на экране появляется соответствующее сообщение о невозможности осуществления операций и в Журнал заносится запись с признаком важности события – ошибка. Указанному событию присваивается такой признак по причине акцентирования внимания лиц, обеспечивающих безопасную эксплуатацию Удостоверяющего Центра в целях выявления возможных нарушителей установленного регламентом порядка взаимодействия Удостоверяющего Центра и пользователей.

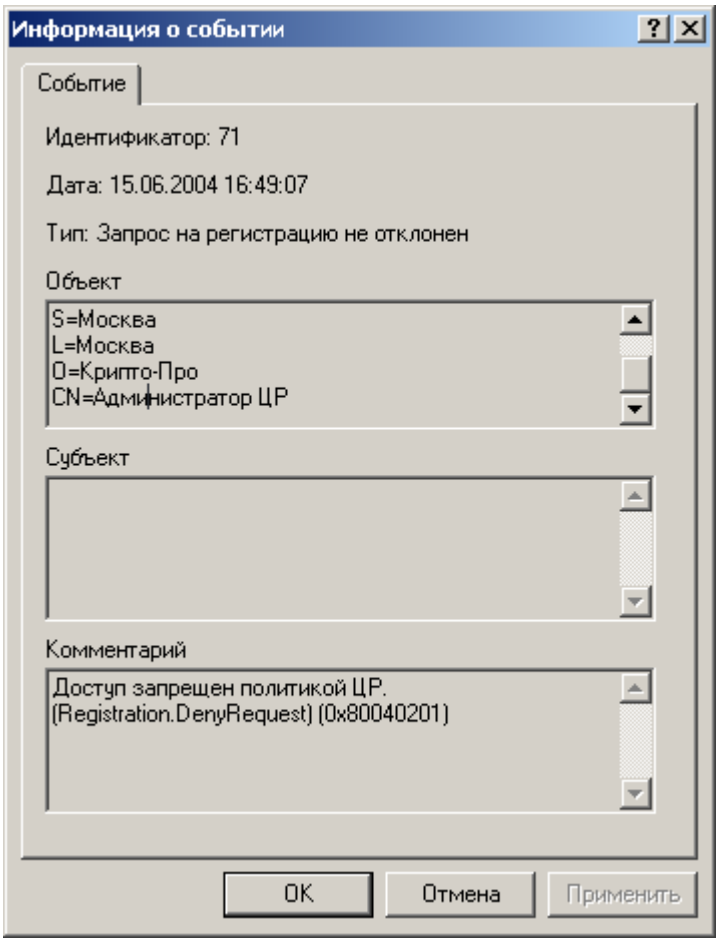
- **Запрос на регистрацию не одобрен** - данное событие возникает при выполнении метода Registration.AcceptRequest в том случае, если успешное выполнение указанного метода противоречит настройкам политик Центра Регистрации (важность события – ошибка). Поле Объект данного события содержит идентификационные данные пользователя, выполнившего указанный метод, поле Комментарий содержит краткое описание причины возникновения события – пользователь, выполнявший метод Registration.AcceptRequest, не имел прав на осуществление указанных действий;

Рисунок 102. Событие Запрос на регистрацию не одобрен



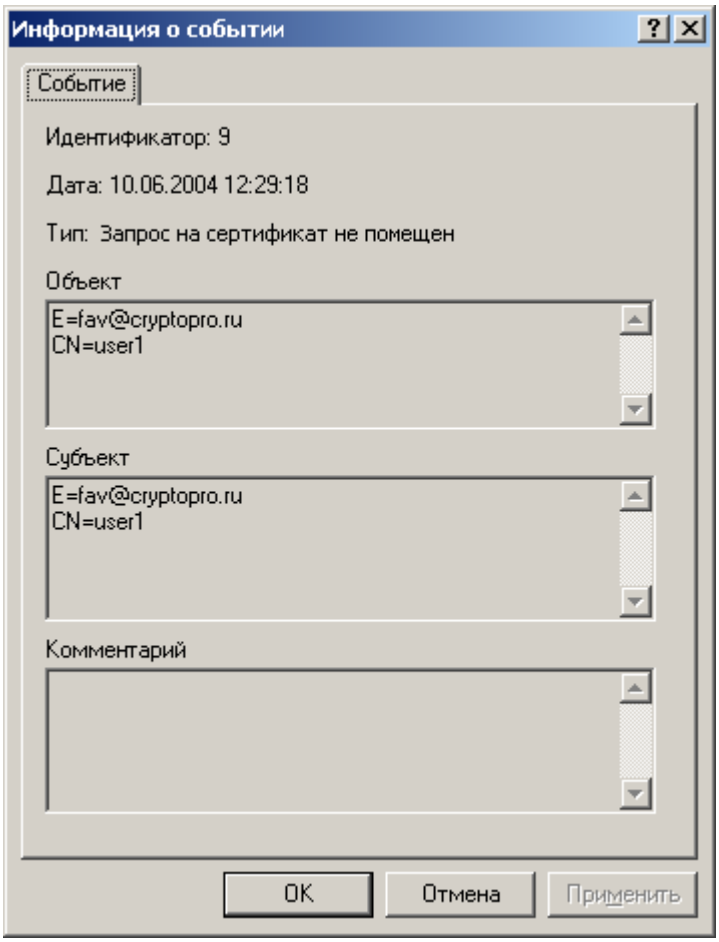
- **Запрос на регистрацию не отклонен** - данное событие возникает при выполнении метода Registration.DenyRequest в том случае, если успешное выполнение указанного метода противоречит настройкам политик Центра Регистрации (важность события – ошибка). Поле Объект данного события содержит идентификационные данные пользователя выполнившего указанный метод, поле Комментарий содержит краткое описание причины возникновения события - пользователь, выполнявший метод Registration.DenyRequest, не имел прав на осуществление указанных действий;

Рисунок 103. Событие Запрос на регистрацию не отклонен



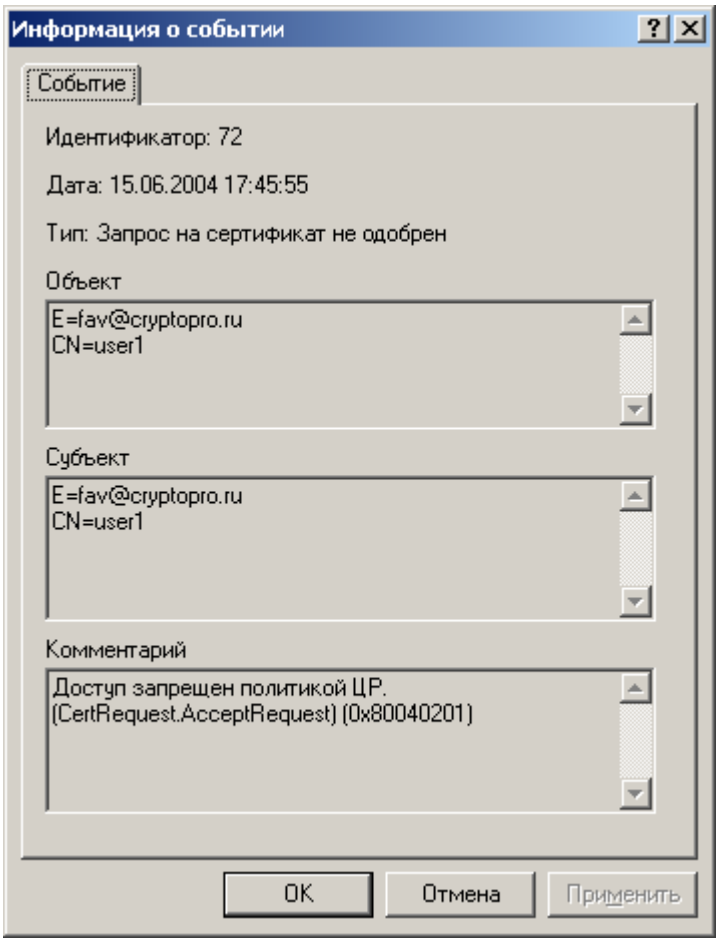
- **Запрос на сертификат не помещен** - данное событие возникает при выполнении метода CertRequest.SubmitRequest в том случае, если успешное выполнение указанного метода противоречит настройкам политик Центра Регистрации (важность события – ошибка). Обработка метода CertRequest.SubmitRequest осуществляется в соответствии с политикой «Обработка подписанных запросов». В связи с этим на выполнение указанного метода влияют два типа настроек Центра Регистрации : Настройки разрешений на выполнение метода и Настройки политики обработки подписанных запросов;

Рисунок 104. Событие Запрос на сертификат не помещен



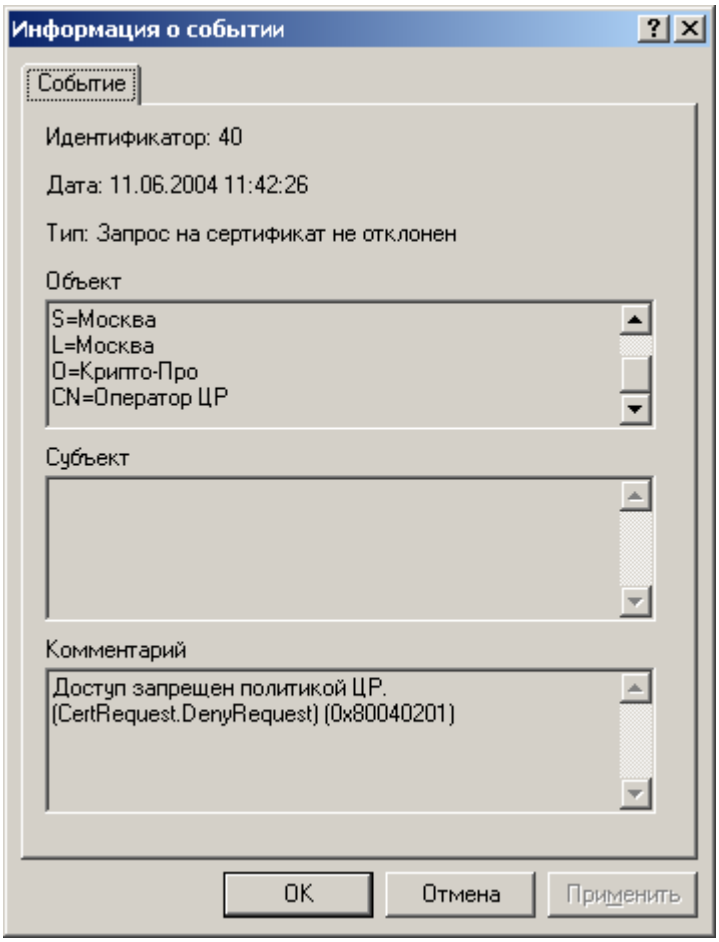
- **Запрос на сертификат не одобрен** - данное событие возникает при выполнении методов CertRequest.AcceptRequest и CertRequest.AcceptFirstRequest в том случае, если успешное выполнение пользователем одного из указанных методов противоречит настройкам политик Центра Регистрации (важность события – ошибка). Поле Объект данного события содержит идентификационные данные пользователя, выполнившего указанный метод, поле Субъект – идентификационные данные пользователя, содержащиеся в запросе на сертификат, поле Комментарий содержит краткое описание причины возникновения события - пользователь, выполнявший метод CertRequest.AcceptRequest либо CertRequest.AcceptFirstRequest не имел прав на осуществление указанных действий;

Рисунок 105. Событие Запрос на сертификат не одобрен



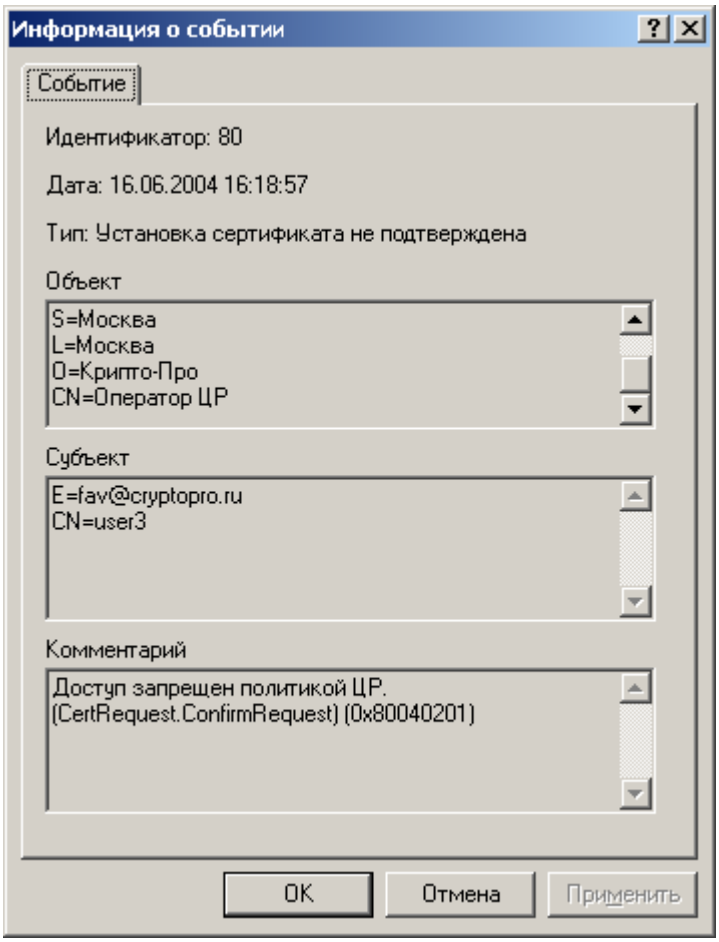
- **Запрос на сертификат не отклонен** - данное событие возникает при выполнении метода CertRequest.DenyRequest в том случае, если успешное выполнение пользователем данного метода противоречит настройкам политик Центра Регистрации (важность события – ошибка). Поле Объект данного события содержит идентификационные данные пользователя, выполнившего указанный метод, поле Субъект – идентификационные данные пользователя, содержащиеся в запросе на сертификат, поле Комментарий содержит краткое описание причины возникновения события - пользователь, выполнявший метод CertRequest.DenyRequest не имел прав на осуществление указанных действий;

Рисунок 106. Событие Запрос на сертификат не отклонен



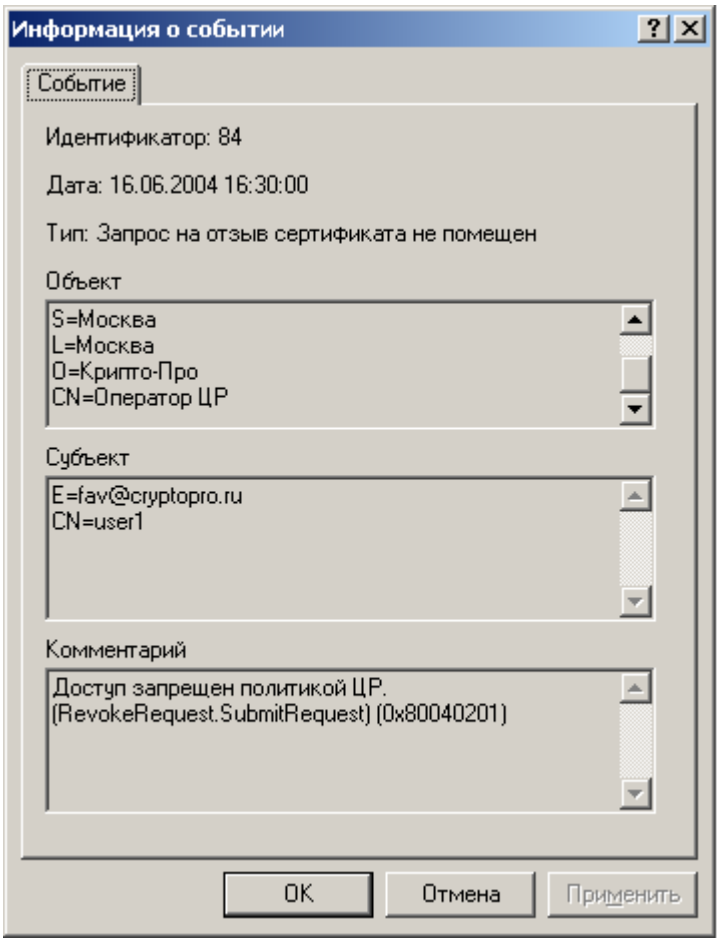
- **Установка сертификата не подтверждена** - данное событие возникает при выполнении метода CertRequest.ConfirmRequest в том случае, если успешное выполнение пользователем данного метода противоречит настройкам политик Центра Регистрации (важность события – ошибка). Поле Объект данного события содержит идентификационные данные пользователя, выполнившего указанный метод, поле Субъект – идентификационные данные пользователя – владельца сертификата, установку которого не удалось подтвердить, поле Комментарий содержит краткое описание причины возникновения события - пользователь, выполнявший метод CertRequest.ConfirmRequest не имел прав на осуществление указанных действий;

Рисунок 107. Событие Установка сертификата не подтверждена



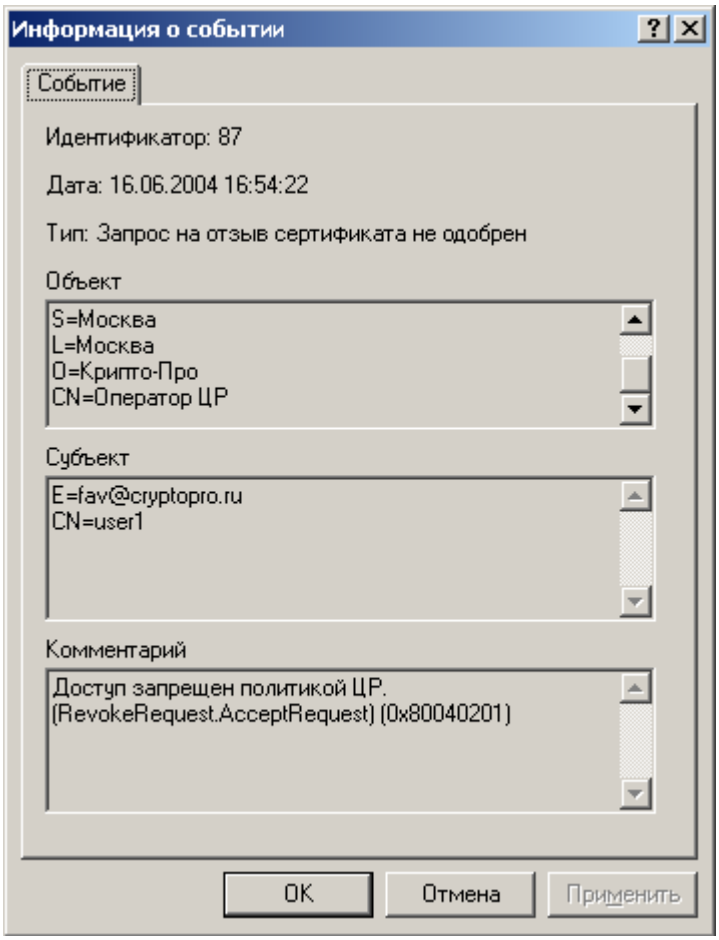
- **Запрос на отзыв сертификата не помещен** - данное событие возникает при выполнении методов RevokeRequest.SubmitRequest, RevokeRequest.SubmitHoldRequest и RevokeRequest.SubmitUnHoldRequest в том случае, если успешное выполнение пользователем данных методов противоречит настройкам политик Центра Регистрации (важность события – ошибка). Обработка указанных методов осуществляется в соответствии с политикой «Обработка запросов на отзыв». В связи с этим на выполнение указанного метода влияют два типа настроек Центра Регистрации: Настройки разрешений на выполнение метода и Настройки политики обработки запросов на отзыв. Поле Объект данного события содержит идентификационные данные пользователя, выполнившего указанный метод, поле Субъект – идентификационные данные пользователя, содержащиеся в запросе на сертификат, поле Комментарий содержит краткое описание причины возникновения события - пользователь, выполнявший один из трех указанных методов, не имел прав на осуществление указанных действий;

Рисунок 108. Событие Запрос на отзыв сертификата не помещен



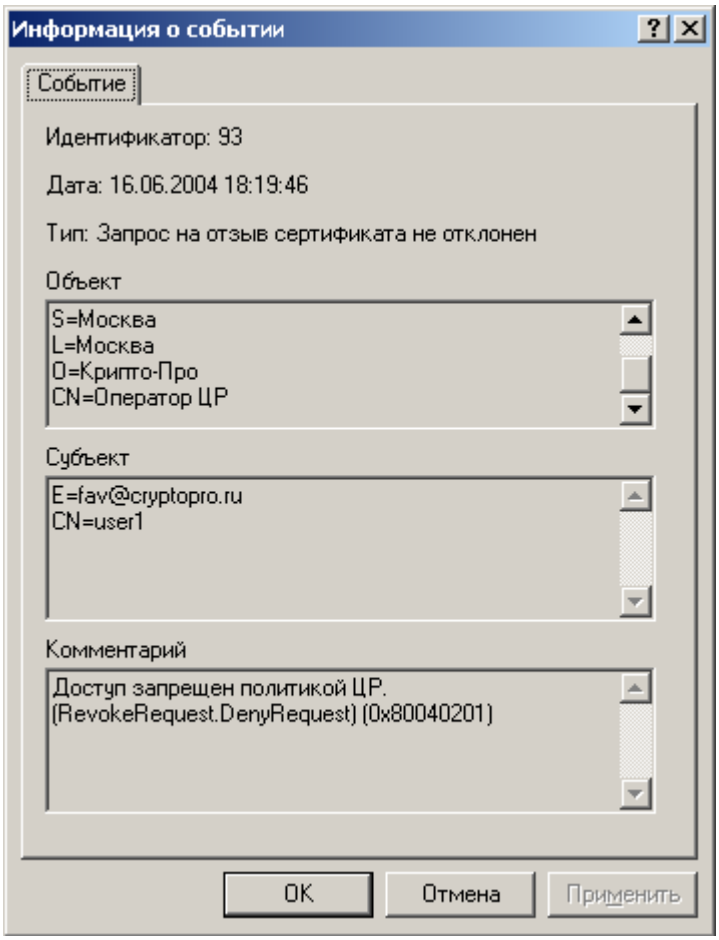
- **Запрос на отзыв сертификата не одобрен** - данное событие возникает при выполнении метода RevokeRequest.AcceptRequest в том случае, если успешное выполнение пользователем данного метода противоречит настройкам политик Центра Регистрации (важность события – ошибка). Поле Объект данного события содержит идентификационные данные пользователя, выполнившего указанный метод, поле Субъект – идентификационные данные пользователя, сертификат которого планировалось отозвать, поле Комментарий содержит краткое описание причины возникновения события - пользователь, выполнявший метод RevokeRequest.AcceptRequest, не имел прав на осуществление указанных действий;

Рисунок 109. Событие Запрос на отзыв сертификата не одобрен



- **Запрос на отзыв сертификата не отклонен** - данное событие возникает при выполнении метода RevokeRequest.DenyRequest в том случае, если успешное выполнение пользователем данного метода противоречит настройкам политик Центра Регистрации (важность события – ошибка). Поле Объект данного события содержит идентификационные данные пользователя, выполнившего указанный метод, поле Субъект – идентификационные данные пользователя, сертификат которого планировалось отозвать, поле Комментарий содержит краткое описание причины возникновения события - пользователь, выполнявший метод RevokeRequest.DenyRequest, не имел прав на осуществление указанных действий;

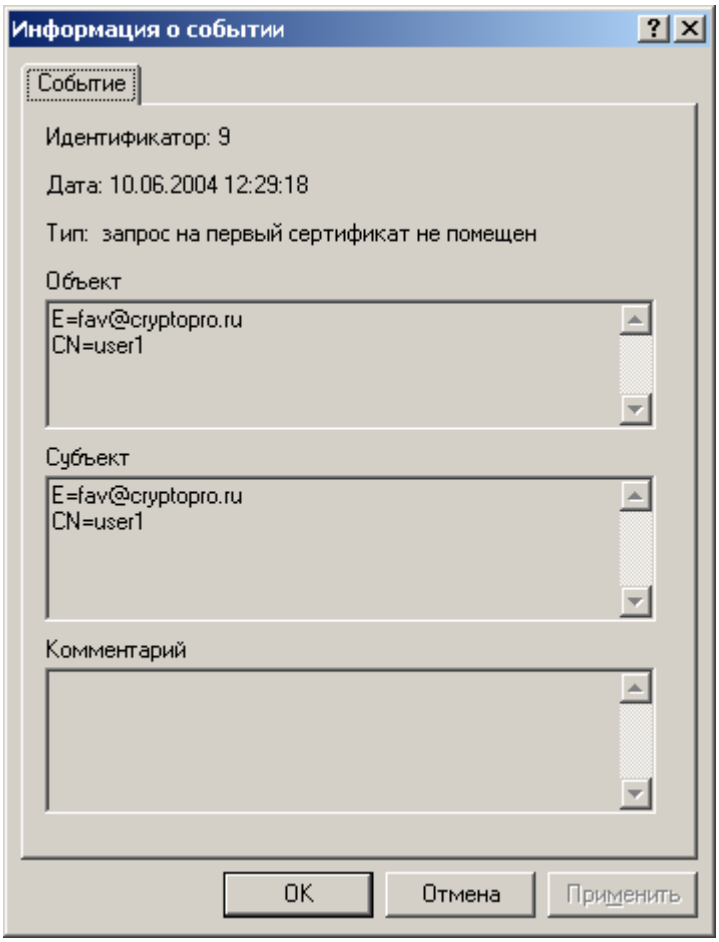
Рисунок 110. Событие Запрос на отзыв сертификата не отклонен



Описанные события «Запрос на отзыв сертификата не помещен», «Запрос на отзыв сертификата не одобрен», «Запрос на отзыв сертификата не отклонен» относятся не только к операциям, связанным непосредственно с аннулированием (отзывом) сертификатов. Данные события относятся также и к запросам на приостановление и возобновление действия сертификатов. Точное определение типа запроса осуществляется на основе свойств рассматриваемых запросов, содержащихся в узле «Запросы на отзыв» приложения АРМ Администратора ЦР.

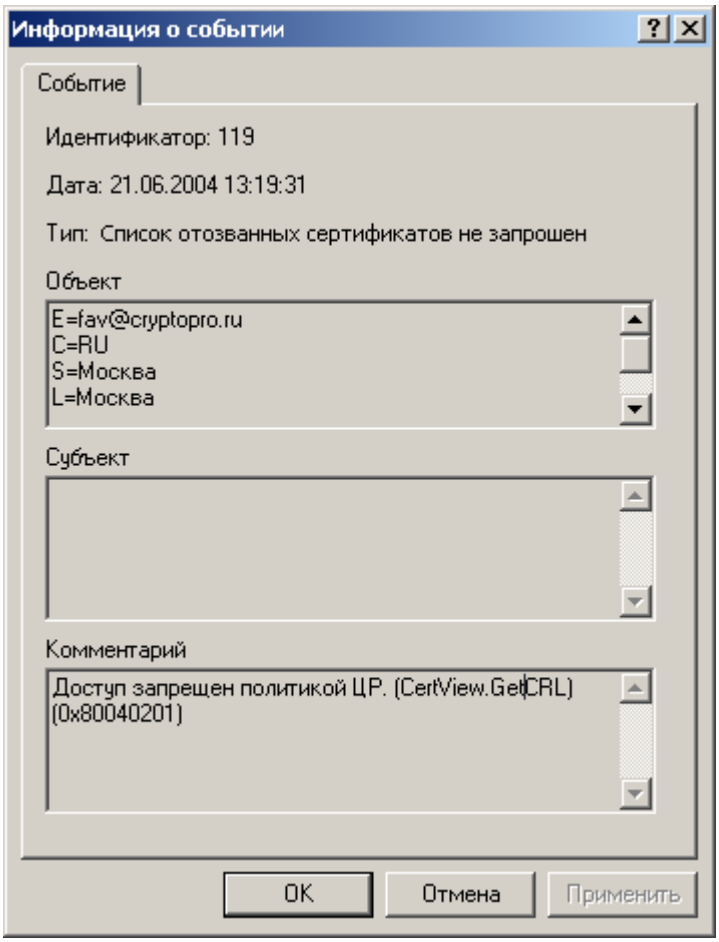
- **Запрос на первый сертификат не помещен** - данное событие возникает при выполнении метода CertRequest.SubmitFirstRequest в том случае, если успешное выполнение указанного метода противоречит настройкам политик Центра Регистрации (важность события – ошибка). Обработка метода CertRequest.SubmitFirstRequest осуществляется в соответствии с политикой «Обработка неподписанных запросов». В связи с этим на выполнение указанного метода влияют два типа настроек Центра Регистрации : Настройки разрешений на выполнение метода и Настройки политики обработки неподписанных запросов;

Рисунок 111. Событие Запрос на первый сертификат не помещен



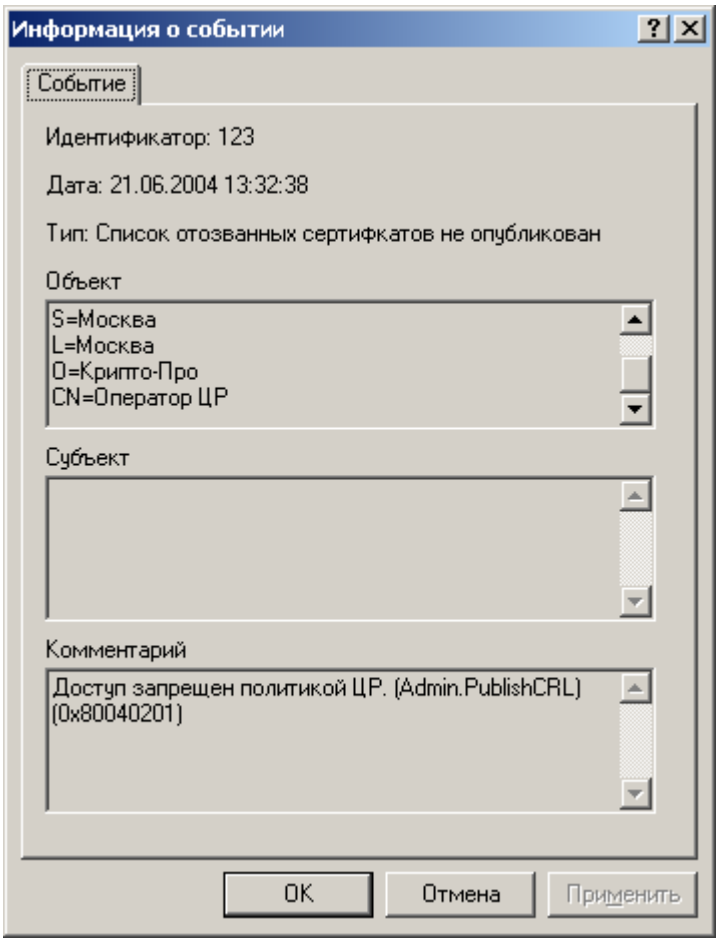
- **Список отозванных сертификатов не запрошен** - данное событие возникает при выполнении метода CertView.GetCRL в том случае, если успешное выполнение указанного метода противоречит настройкам политик Центра Регистрации (важность события – ошибка). Поле Объект данного события содержит идентификационные данные пользователя, запросившего список отозванных сертификатов, поле Комментарий содержит краткое описание причины возникновения события - пользователь, выполнявший метод CertView.GetCRL, не имел прав на осуществление указанных действий;

Рисунок 112. Событие Список отозванных сертификатов не запрошен



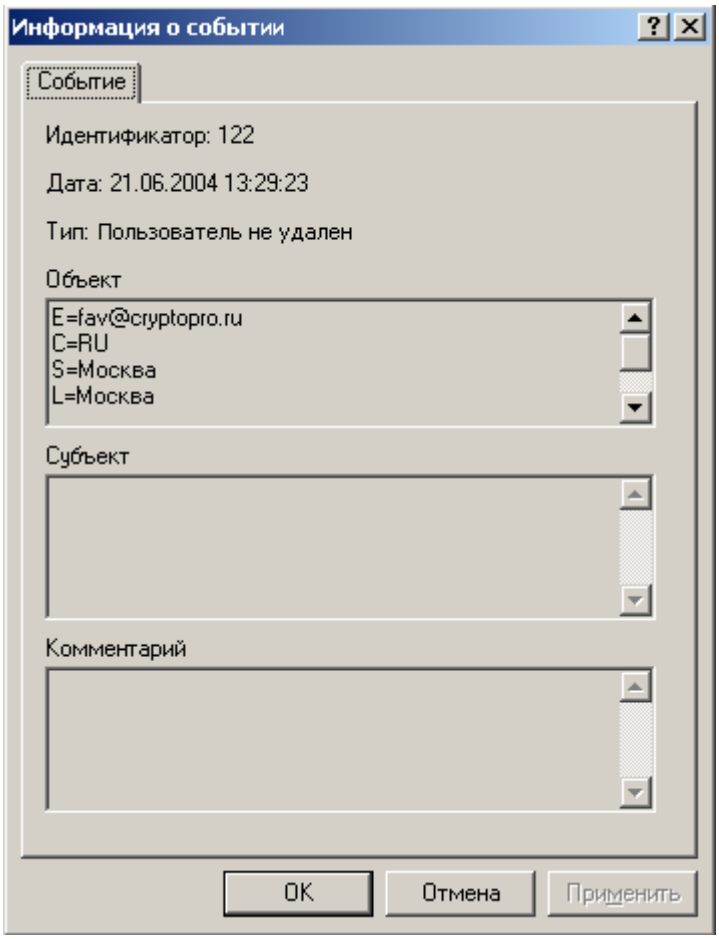
- **Список отозванных сертификатов не опубликован** - данное событие возникает при выполнении метода Admin.PublishCRL в том случае, если успешное выполнение указанного метода противоречит настройкам политик Центра Регистрации (важность события – ошибка). Поле Объект данного события содержит идентификационные данные пользователя, направившего запрос на публикацию списка отозванных сертификатов, поле Комментарий содержит краткое описание причины возникновения события - пользователь, выполнявший метод Admin.PublishCRL, не имел прав на осуществление указанных действий;

Рисунок 113. Событие Список отозванных сертификатов не опубликован



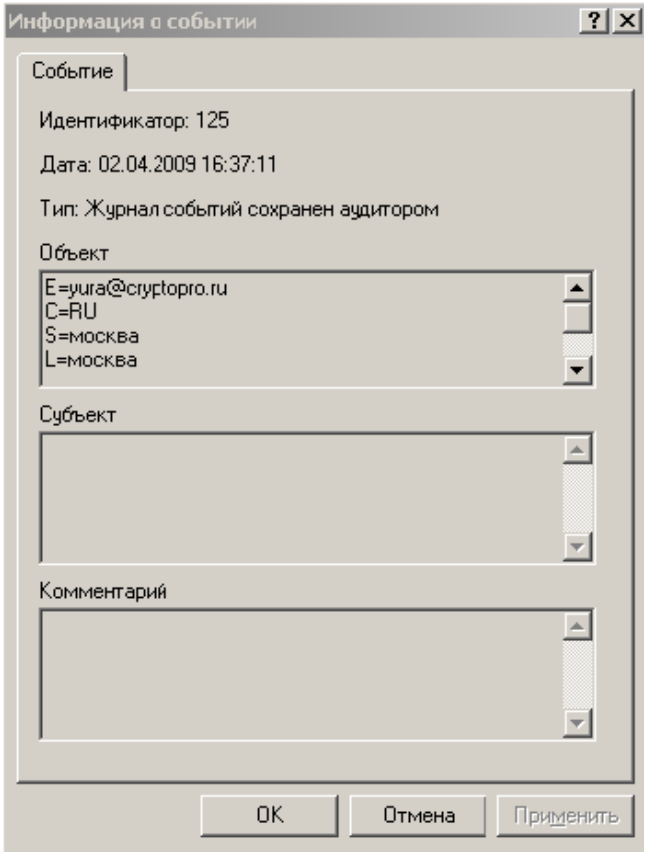
- **Пользователь не удален -** данное событие возникает при выполнении метода UserView.DeleteUser в том случае, если успешное выполнение указанного метода противоречит настройкам политик Центра Регистрации (важность события – ошибка). Поле Объект данного события содержит идентификационные данные пользователя, пытавшегося выполнить удаление учетной записи пользователя;

Рисунок 114. Событие Пользователь не удален



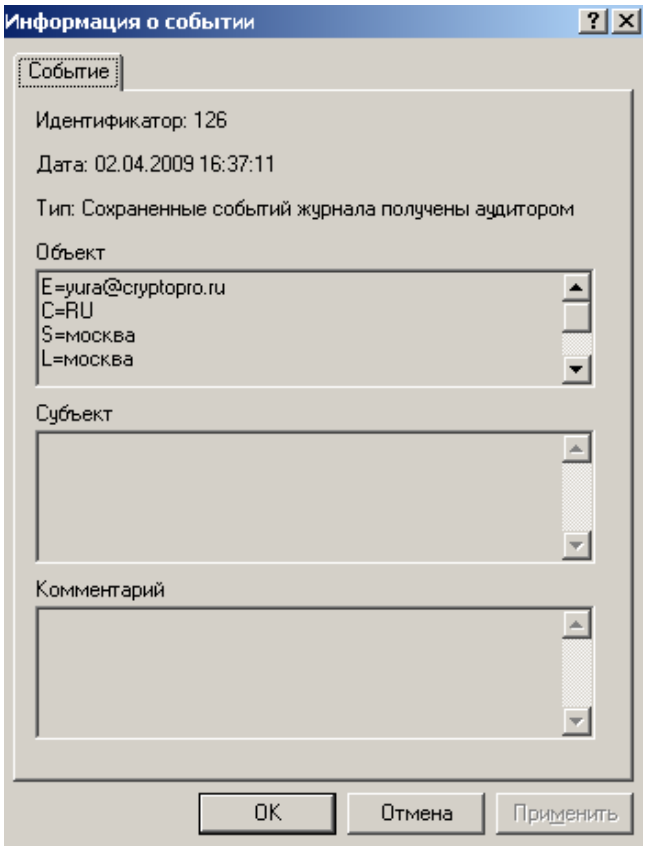
- **Журнал событий сохранен аудитором –** данное событие возникает при успешном выполнении метода Audit.SaveLog (важность события – обычная). Поле Объект данного события содержит идентификационные данные пользователя, выполнившего сохранение журнала;

Рисунок 115. Событие журнал событий сохранен аудитором



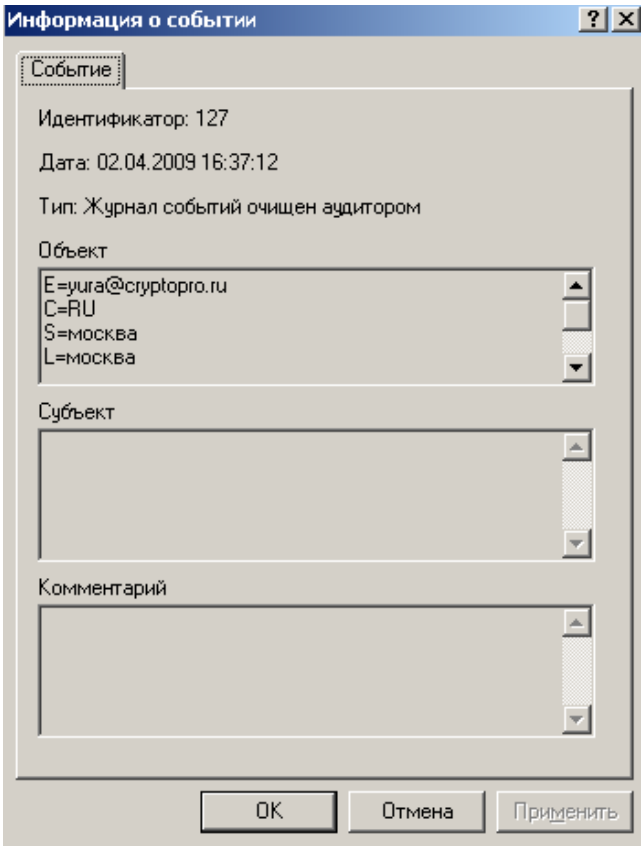
- **Сохраненные события журнала получены аудитором -** данное событие возникает при успешном выполнении метода Audit.GetSavedLog (важность события – обычная). Поле Объект данного события содержит идентификационные данные пользователя, выполнившего сохранение журнала;

Рисунок 116. Событие сохраненные события журнала получены аудитором



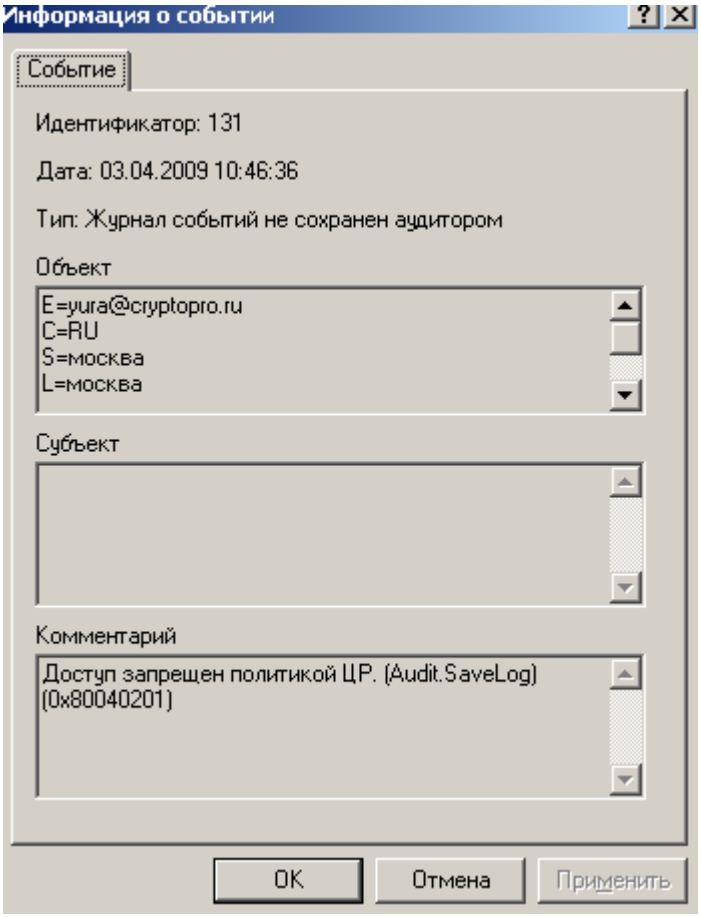
- **Журнал событий очищен аудитором -** данное событие возникает при успешном выполнении метода Audit.DeleteSavedLog (важность события – обычная). Поле Объект данного события содержит идентификационные данные пользователя, выполнившего очищение журнала;

Рисунок 117. Событие журнал событий очищен аудитором



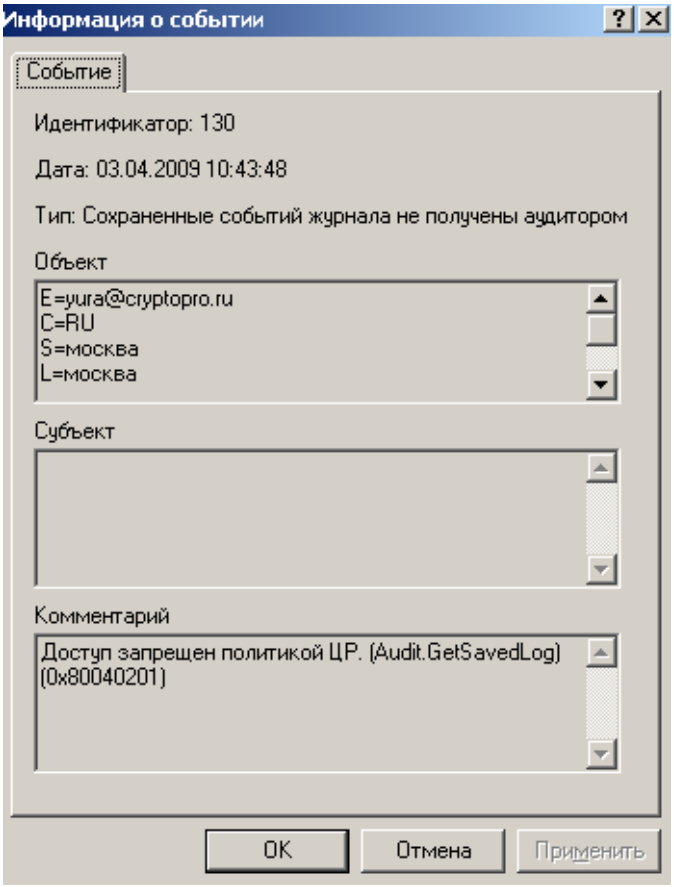
- **Журнал событий не сохранен аудитором -** данное событие возникает при выполнении метода Audit.SaveLog в том случае, если успешное выполнение указанного метода противоречит настройкам политик Центра Регистрации (важность события – ошибка). Поле Объект данного события содержит идентификационные данные пользователя, пытавшегося сохранить журнал, поле Комментарий содержит краткое описание причины возникновения события;

Рисунок 118. Событие журнал событий не сохранен аудитором



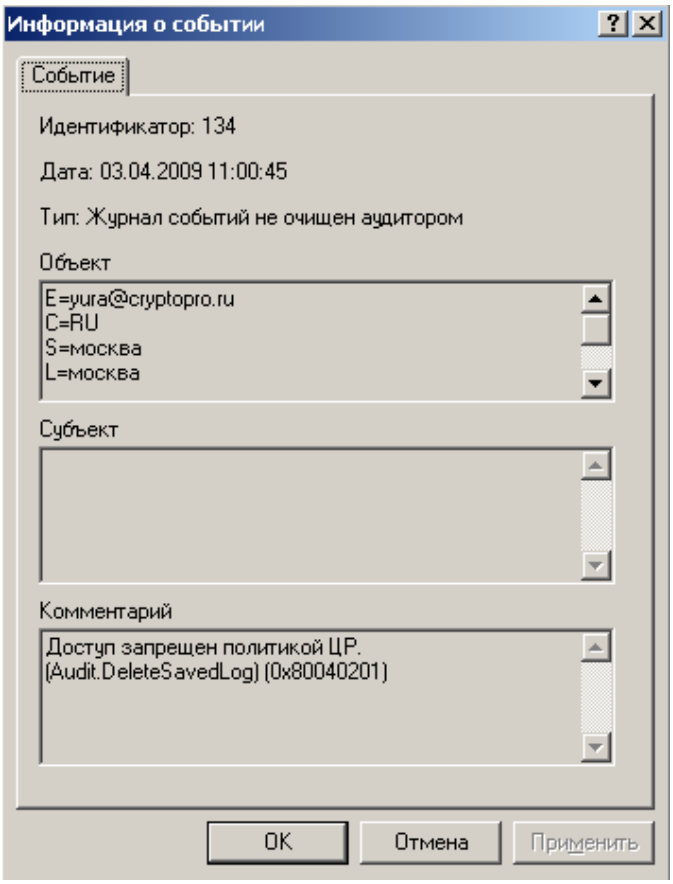
- **Сохраненные события журнала не получены аудитором -** данное событие возникает при выполнении метода Audit.GetSavedLog в том случае, если успешное выполнение указанного метода противоречит настройкам политик Центра Регистрации (важность события – ошибка). Поле Объект данного события содержит идентификационные данные пользователя, пытавшегося сохранить журнал, поле Комментарий содержит краткое описание причины возникновения события;

Рисунок 119. Событие сохраненные события журнала не получены аудитором



- **Журнал событий не очищен аудитором -** данное событие возникает при выполнении метода Audit.DeleteSavedLog в том случае, если успешное выполнение указанного метода противоречит настройкам политик Центра Регистрации (важность события – обычная). Поле Объект данного события содержит идентификационные данные пользователя, пытавшегося очистить журнал, поле Комментарий содержит краткое описание причины возникновения события;

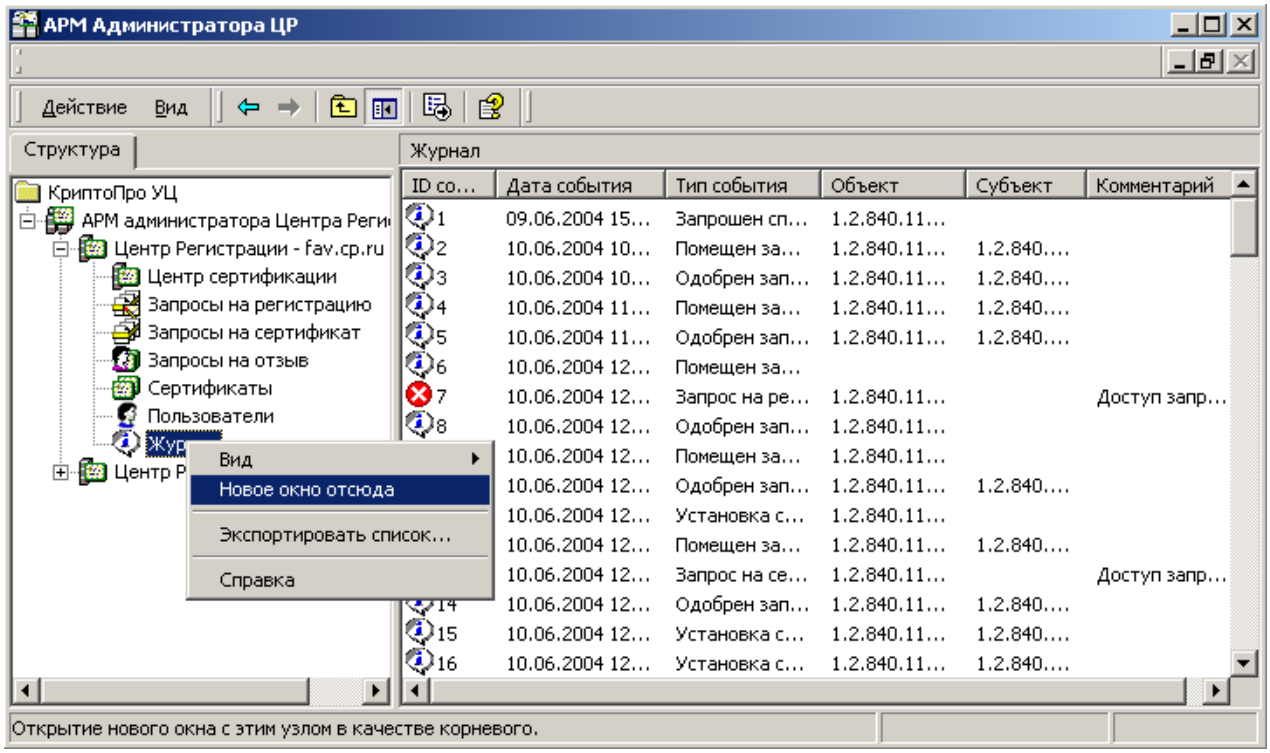
Рисунок 120. Событие журнал событий не очищен аудитором



16.2. Работа с Журналом регистрации событий

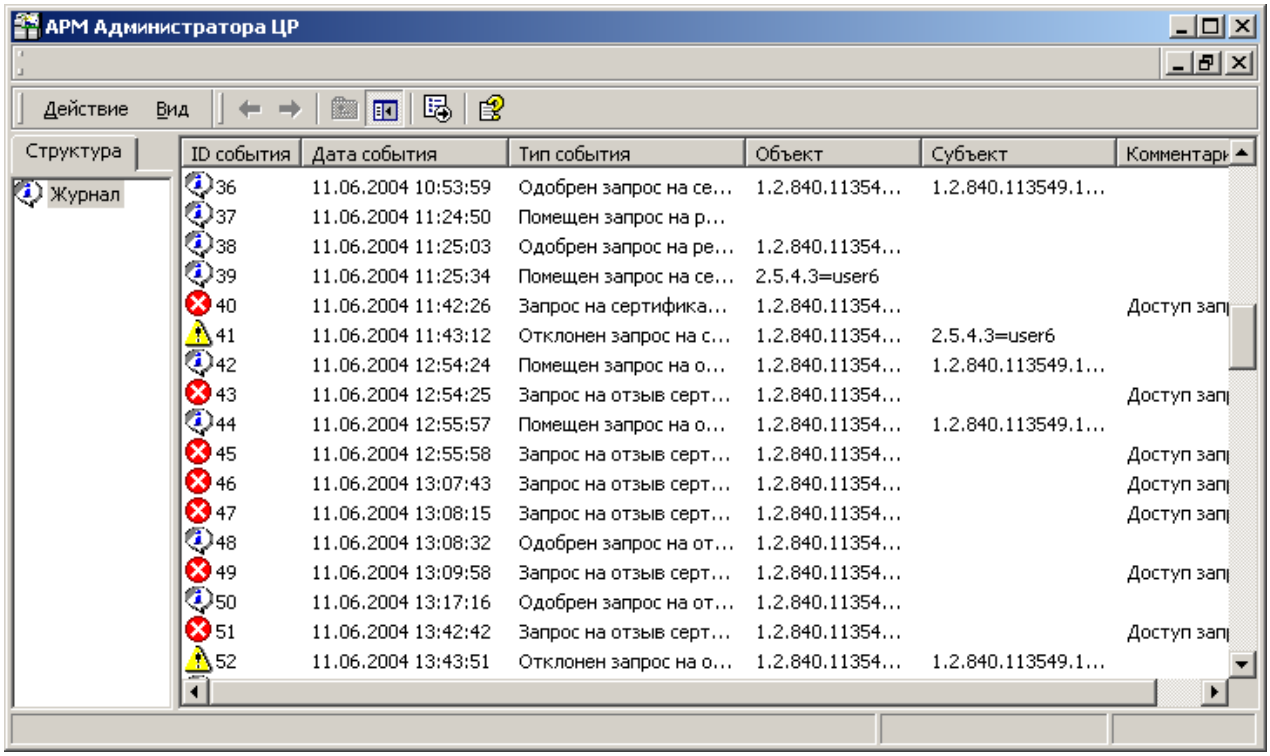
Для удобства работы с записями журнала имеется возможность просмотра зарегистрированных событий в отдельном окне. Для этого в консоли **АРМ Администратора ЦР** выделите правой кнопкой мыши узел **Журнал** и, в открывшемся контекстном меню, выберите пункт «Новое окно отсюда».

Рисунок 121. Выбор режима просмотра записей Журнала в новом окне



Откроется окно консоли **Журнал,** в правой части которого отображается список зарегистрированных событий

Рисунок 122. Просмотр Журнала регистрации событий в отдельном окне



Каждое событие **Журнала** регистрации событий представляет собой последовательность полей, порядок и отображение которых может быть изменено соответствующими настройками. Изменение указанных настроек осуществляется в окне «Изменить столбцы», для вызова которого необходимо выделить правой кнопкой мыши

узел **Журнал**, и в открывшемся контекстном меню выбрать пункт **Вид -> Выбрать столбцы.**

Рисунок 1238. Вызов окна "Изменить столбцы"

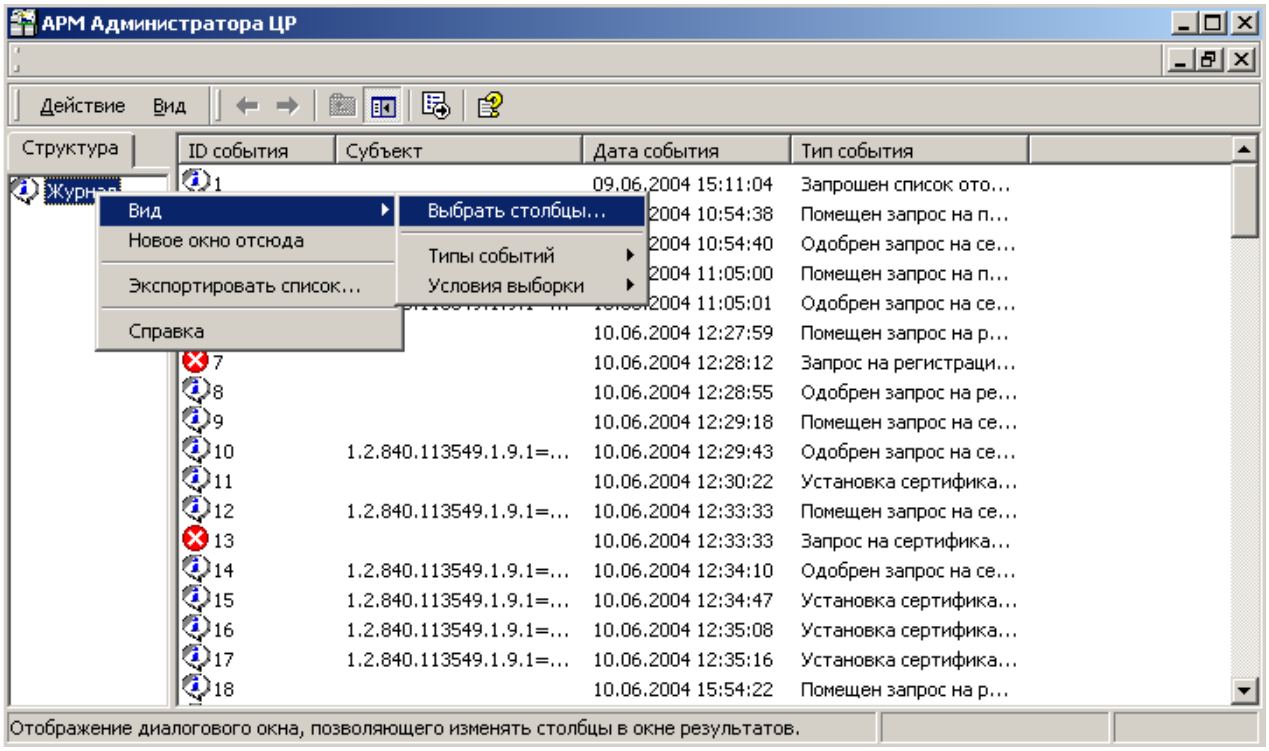
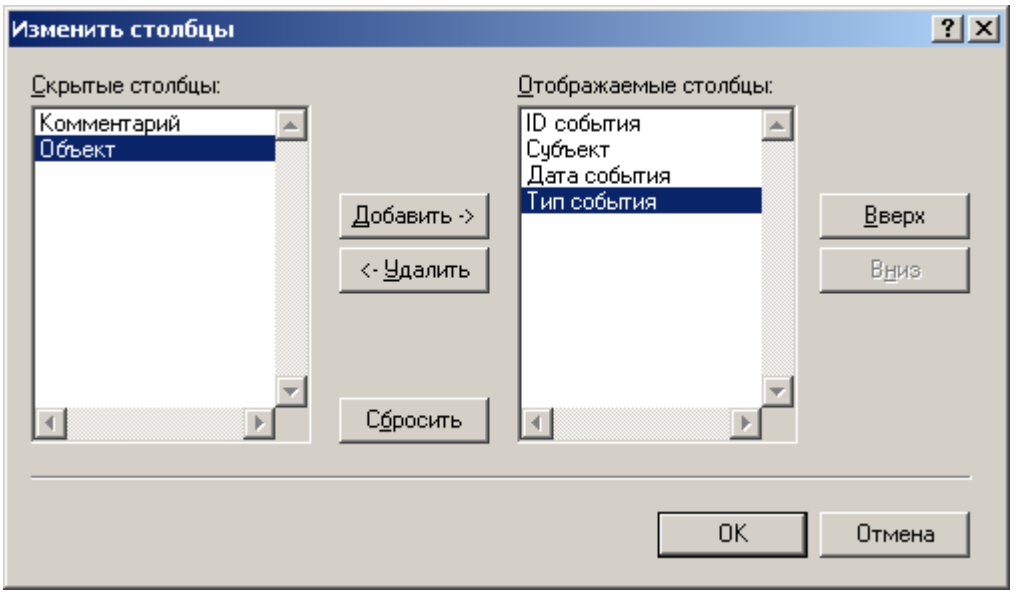


Рисунок 1249. Окно Изменить столбцы



Правая область окна **Изменить столбцы** – «Отображаемые столбцы» содержит список названий столбцов, которые будут отображаться в окне просмотра Журнала регистрации событий. Последовательность отображения столбцов (слева - направо) соответствует последовательности, указанной в приведенной области (сверху – вниз). Для изменения порядка отображения столбцов необходимо воспользоваться кнопками «Вверх» и «Вниз». Нажатие кнопки «Вверх» приводит к замене местами выделенного пункта на вышестоящий, нажатие кнопки «Вниз» - на нижестоящий.


Столбец «ID события» всегда находится первым, и его положение не может быть изменено.

Добавление и удаление столбцов из списка «Отображаемые столбцы» осуществляется с помощью кнопок «Добавить» и «Удалить». При нажатии на кнопку «Добавить» выделенное в списке «Скрытые столбцы» наименование столбца будет удалено из указанного списка и добавлено в список «Отображаемые столбцы».

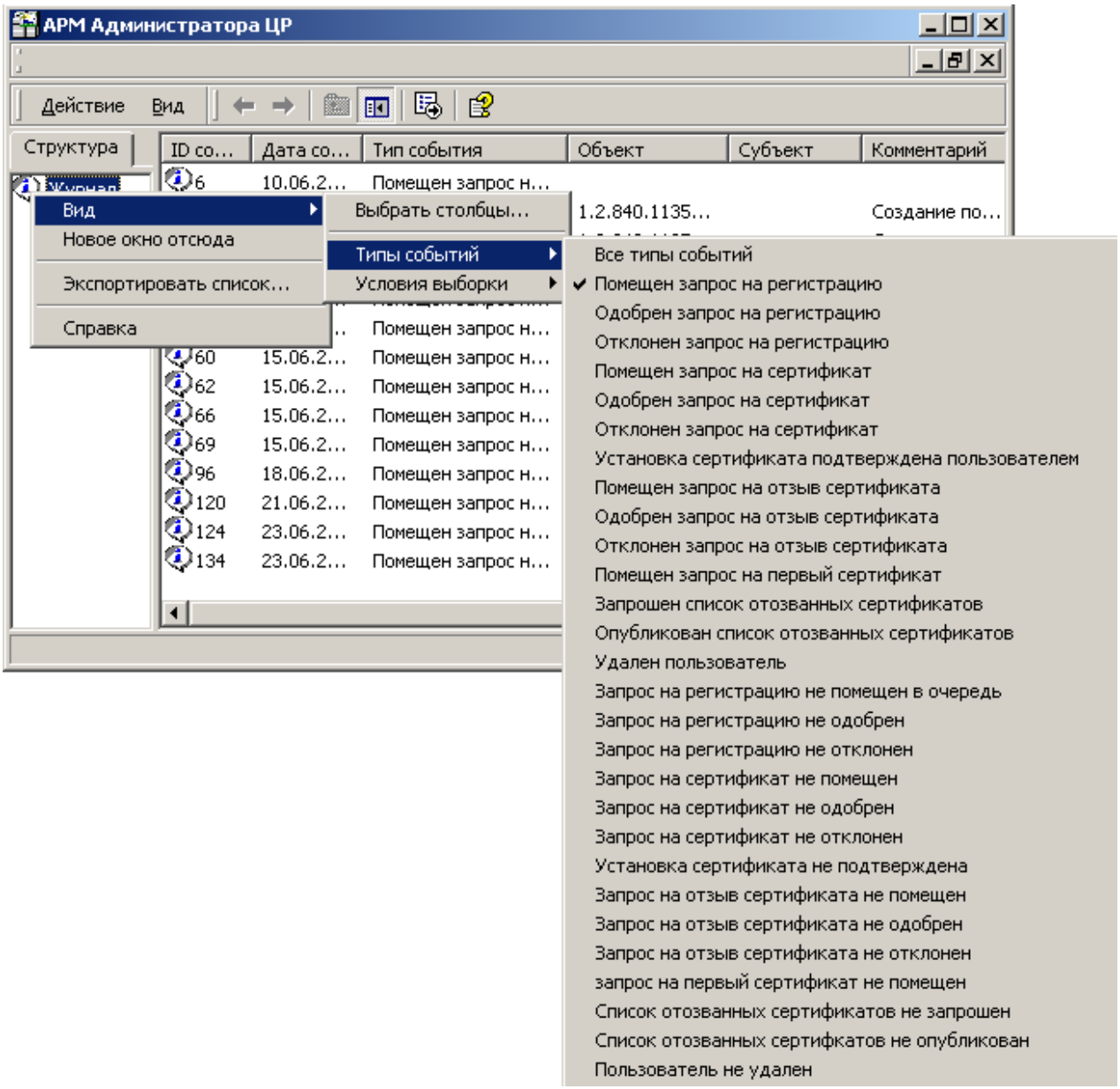
При нажатии на кнопку «Удалить» выделенное в списке «Отображаемые столбцы» наименование столбца будет удалено из указанного списка и добавлено в список «скрытые столбцы».


Столбец «ID события» не может быть удален из списка «Отображаемые столбцы»

Нажатие на кнопку «Сбросить» приводит к восстановлению отображения столбцов по умолчанию, т.е. к отображению всех столбцов в следующем порядке: «ID события», «Дата события», «Тип события», «Объект», «Субъект», «Комментарий».

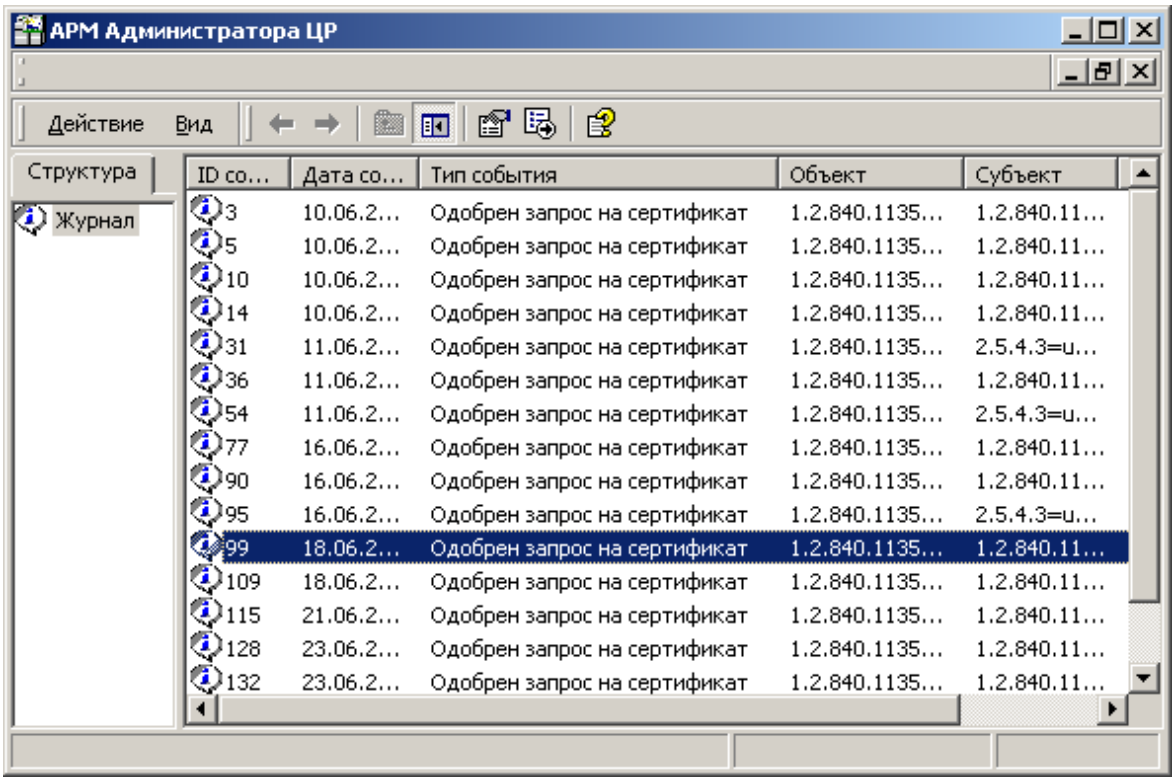
По желанию пользователя в окне Журнала зарегистрированных событий могут отображаться только события определенного типа. Для этого необходимо выделить правой кнопкой мыши узел **Журнал** и в открывшемся контекстном меню выбрать **Вид –> Типы событий** и указать необходимый тип события.

Рисунок 125. Выбор необходимого типа события



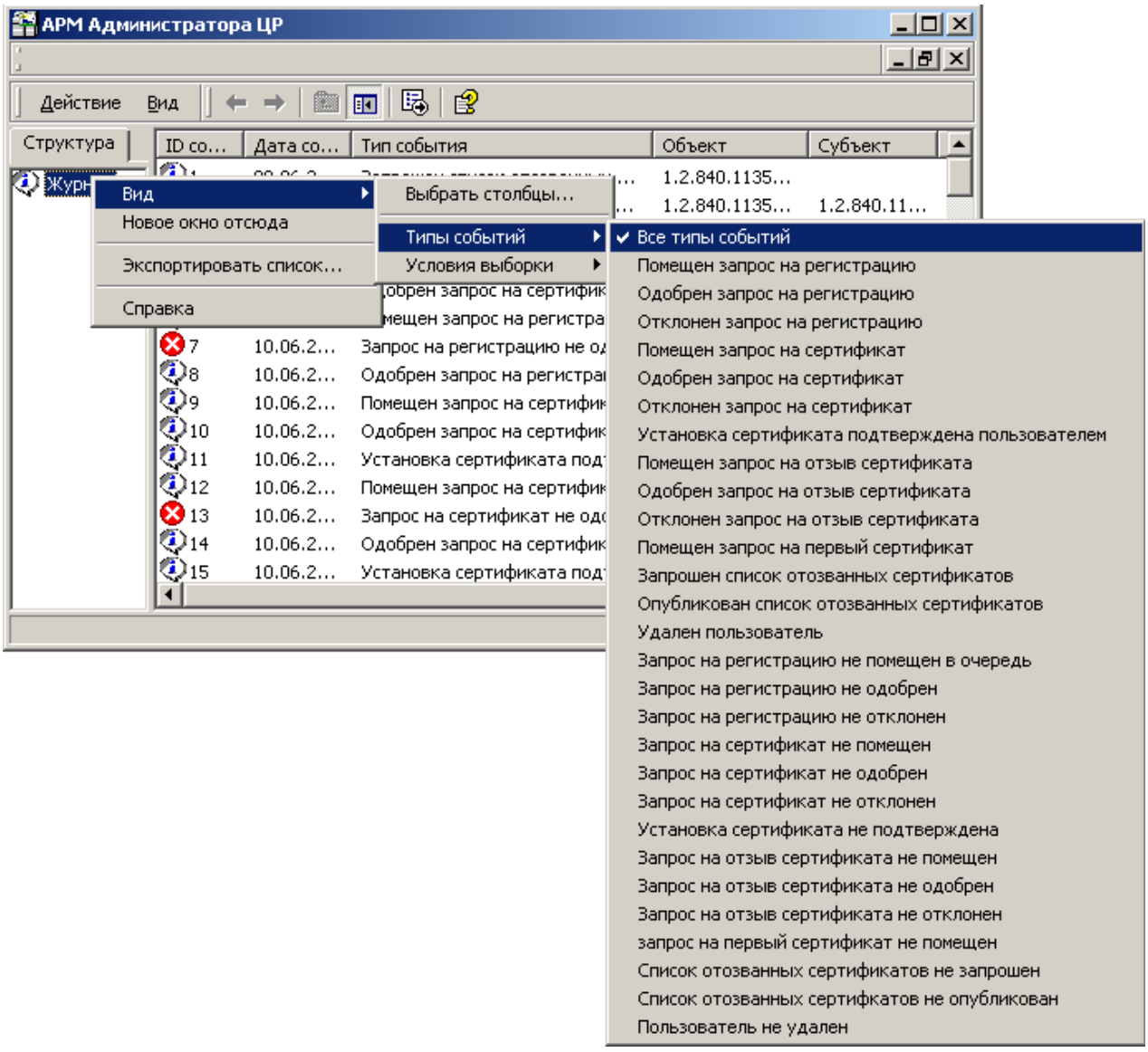
Например, для выбора всех событий типа **Одобрен запрос на сертификат** необходимо правой кнопкой мыши выделить узел **Журнал**, затем в открывшемся контекстном меню выбрать **Вид -> Типы событий - > Одобрен запрос на сертификат.** Окно просмотра зарегистрированных событий будет содержать только события типа **Одобрен запрос на сертификат.**

Рисунок 126. Пример отображения событий одного типа



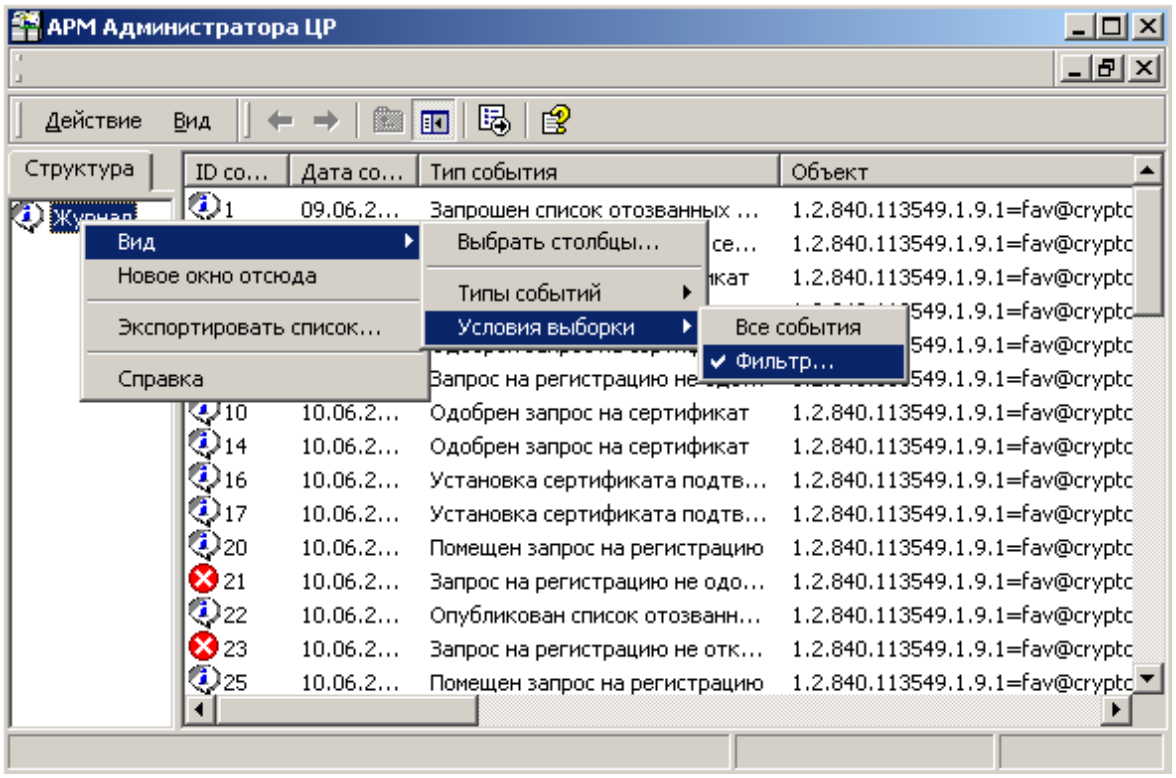
Для просмотра всех зарегистрированных событий выделите правой кнопкой мыши узел **Журнал** и, в открывшемся контекстном меню, выберите **Вид -> Типы событий -> Все типы событий.**

Рисунок 127. Выбор всех зарегистрированных типов событий



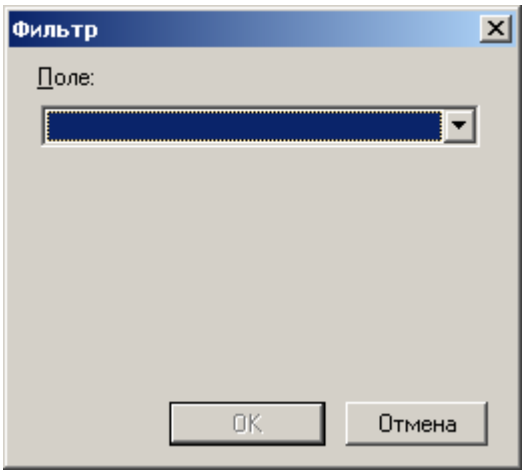
АРМ Администратора Центра Регистрации позволяет производить фильтрацию зарегистрированных в **Журнале** событий по содержанию полей. Для этого необходимо выделить правой кнопкой мыши узел **Журнал,** в открывшемся контекстном меню выбрать **Вид -> Условия выборки -> Фильтр...**

Рисунок 128. Задание фильтра просмотра зарегистрированных событий



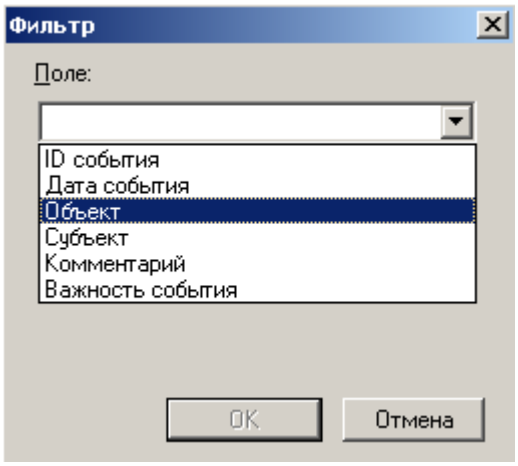
Откроется окно настройки **Фильтра**

Рисунок 129. Настройка фильтра Журнала регистрации событий



Фильтрация может быть осуществлена по содержимому следующих полей: «ID события», «Дата события», «Объект», «Субъект», «Комментарий», «Важность события». Выбор поля фильтрации осуществляется в раскрывающемся списке **Поле**

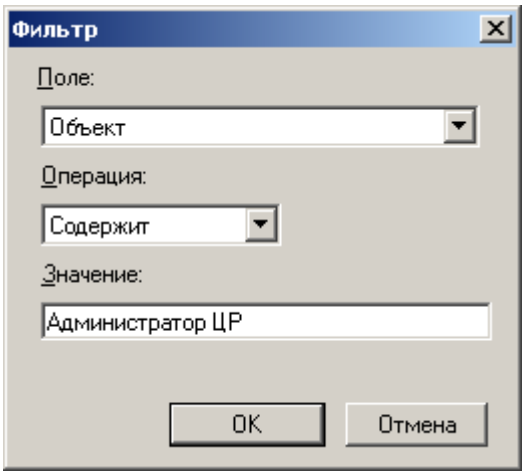
Рисунок 130. Выбор поля фильтрации



После выбора необходимого поля фильтрации введите условия отбора зарегистрированных событий, после чего в окне **Фильтр** нажмите кнопку **OK**.

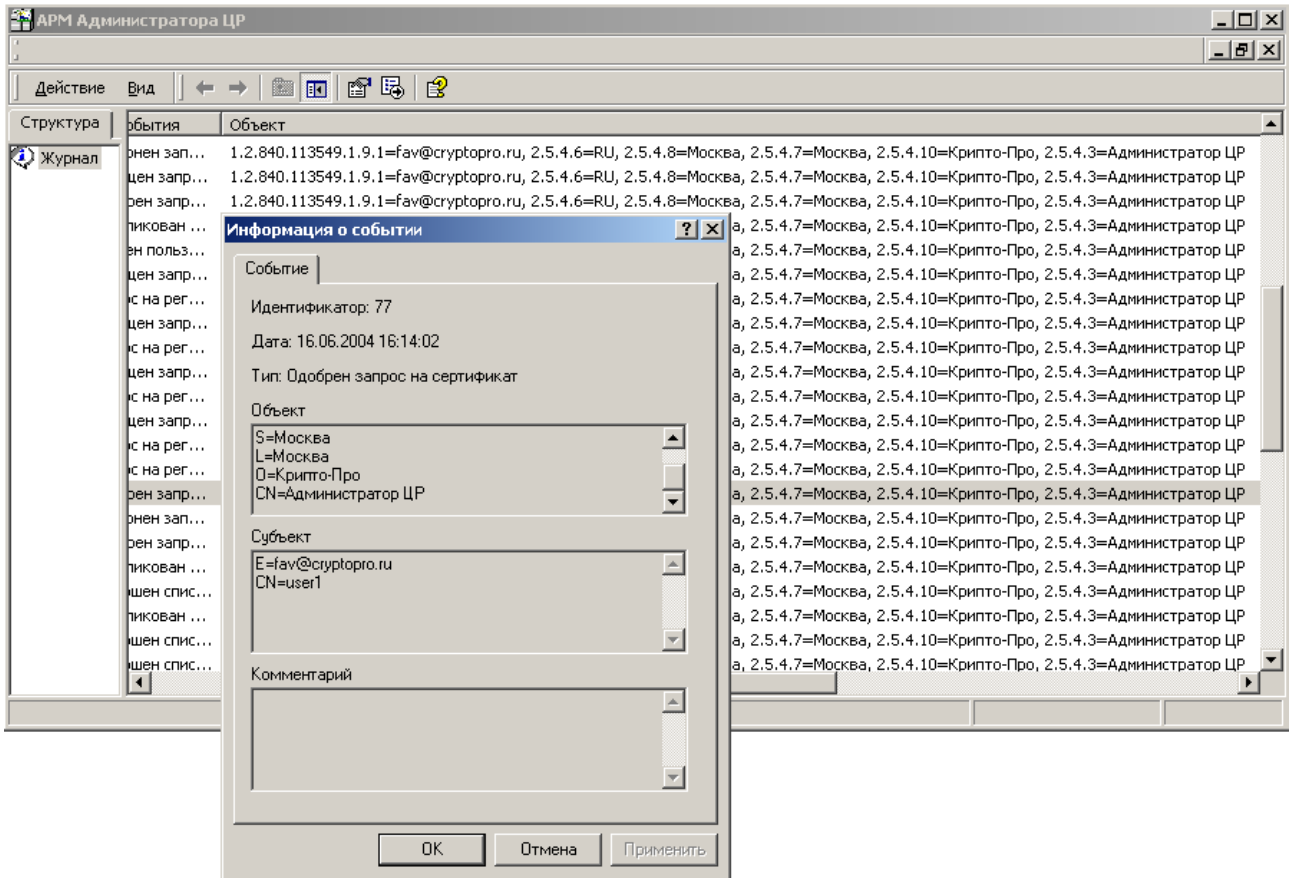
Например, для просмотра событий, выполнение которых осуществлял Администратор (в данном примере это привилегированный пользователь с псевдонимом Администратор ЦР) необходимо осуществить следующие действия: Выделить правой кнопкой мыши узел **Журнал**, в открывшемся контекстном меню выбрать **Вид -> Условия выборки - > Фильтр.** Затем в области окна **Поле** необходимо выбрать значение **Объект**, в области окна **Операция** – значение **Содержит** и в области окна **Значение** ввести **Администратор ЦР**.

Рисунок 131. Задание параметров Фильтра



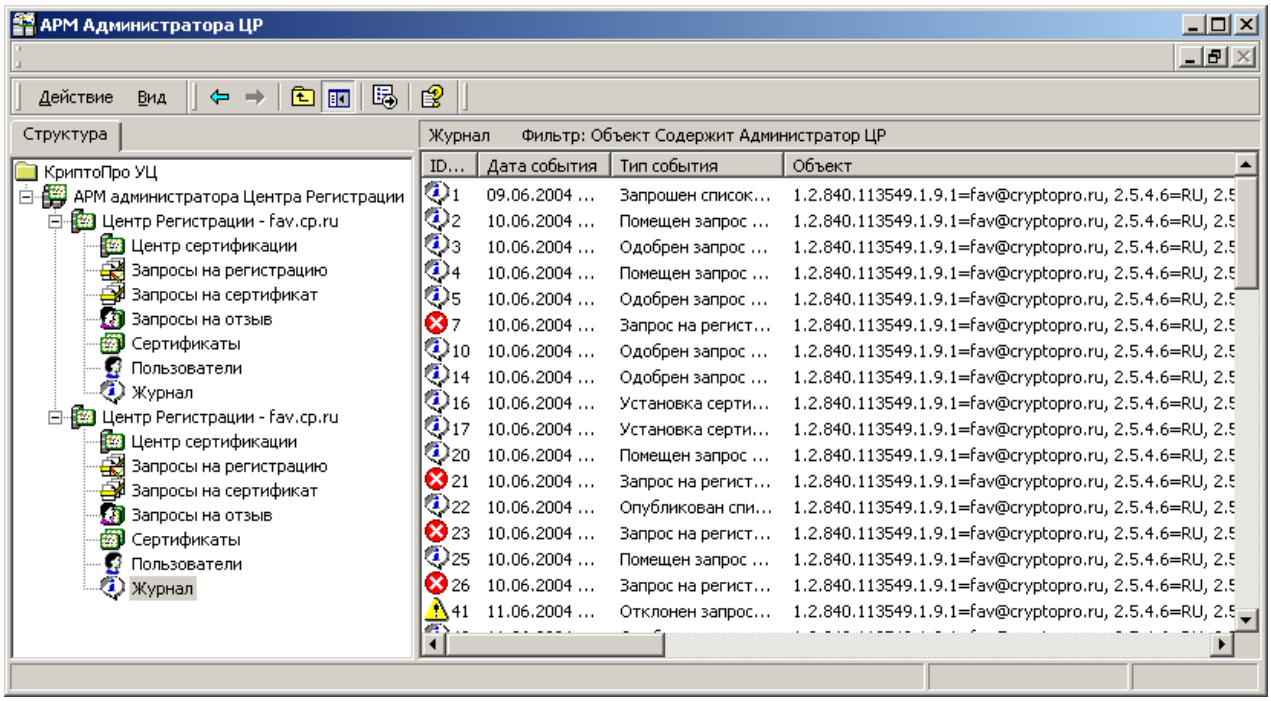
Нажатие кнопки **OK** в окне настроек фильтра осуществит фильтрацию зарегистрированных событий журнала в соответствии с установленными условиями.

Рисунок 132. Просмотр событий журнала с использованием фильтра



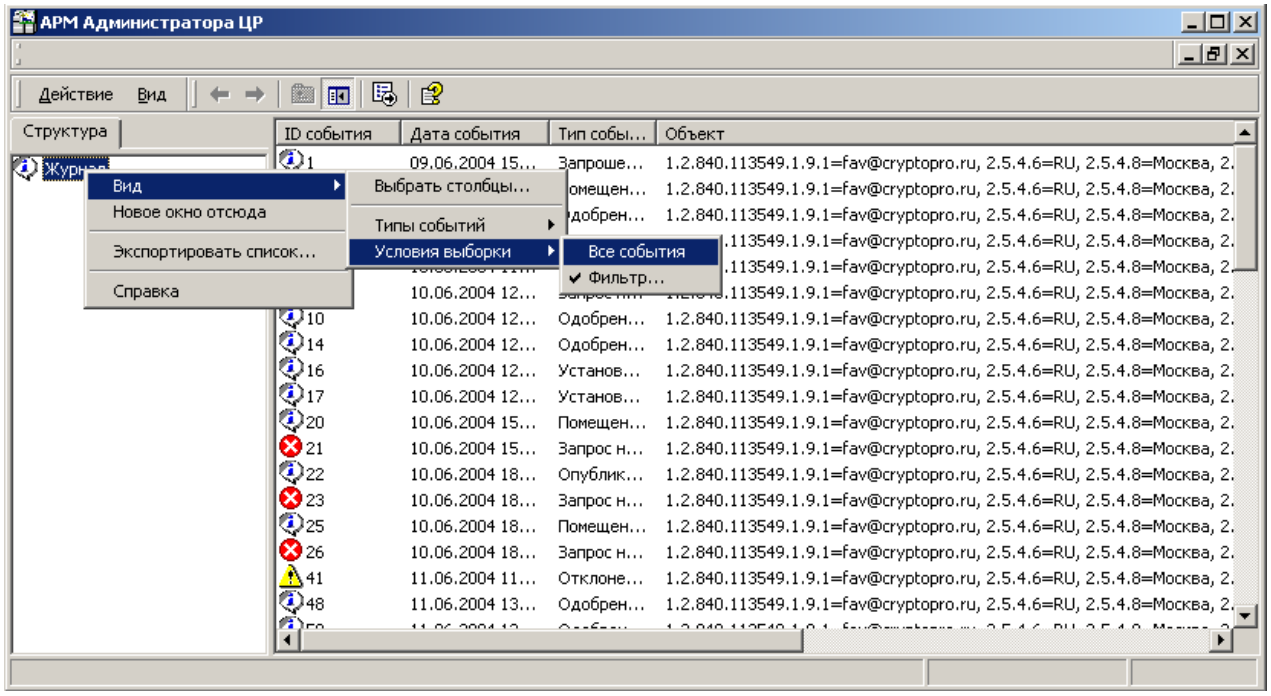
При просмотре **Журнала** посредством выбора одноименного узла в списке объектов управления Центра Регистрации в верхней строке области просмотра событий выводится информация о параметрах используемого фильтра (если фильтр не используется, то поле содержит только запись Журнал).

Рисунок 133. Отображение параметров фильтрации событий Журнала



Для отмены использования фильтра и осуществления просмотра всех зарегистрированных событий **Журнала**, выделите правой кнопкой мыши узел **Журнал** и в открывшемся контекстном меню выберите **Вид** -> **Условия выборки** –> **Все события.**

Рисунок 134. Отмена использования фильтрации событий Журнала



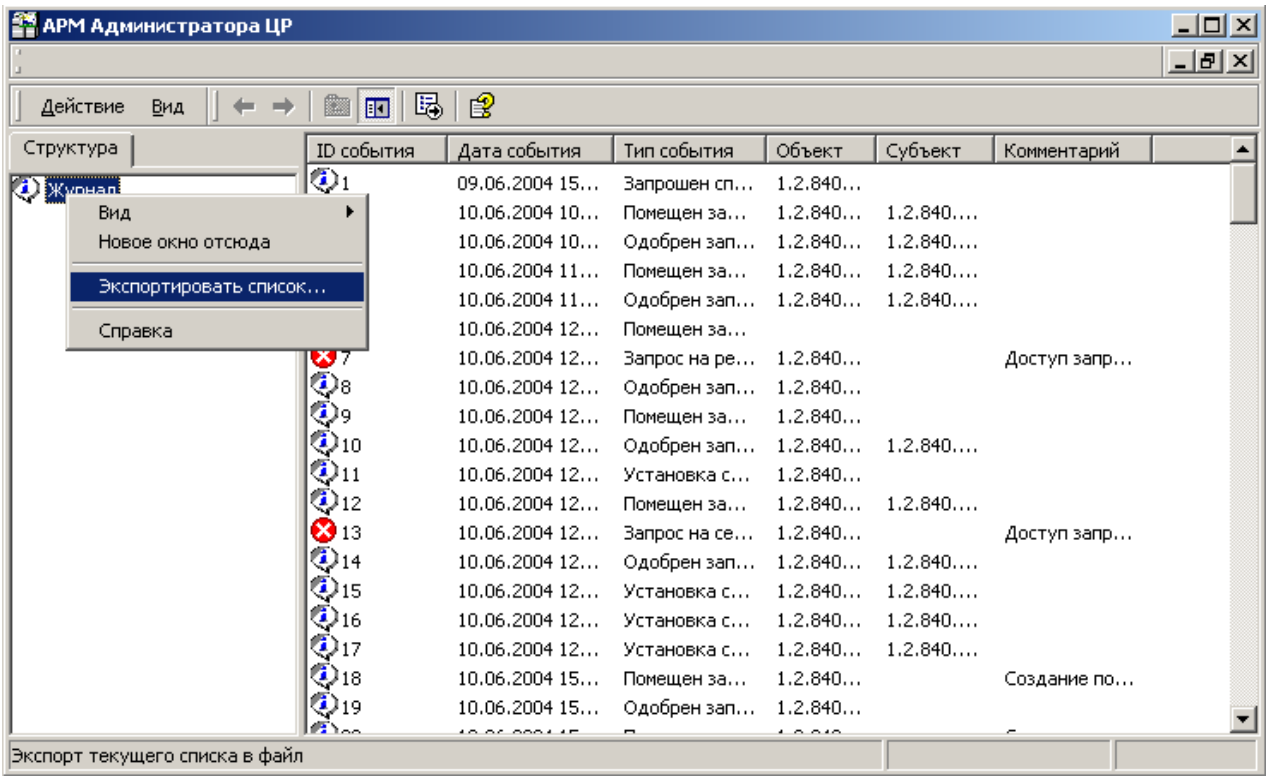
Журнал зарегистрированных событий может быть экспортирован во внешний файл и представлен в виде следующих форматов:

- Текст (разделитель – табуляция) (.txt);
- Текст (разделитель – запятая) (.csv);

- Текст Юникода (разделитель – табуляция) (.txt);
- Текст Юникода (разделитель – запятая) (.csv);

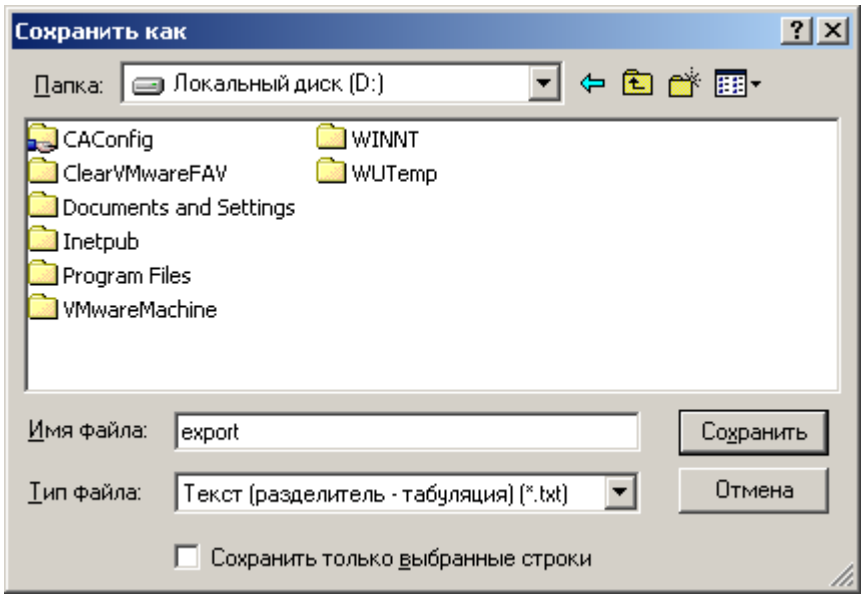
Для осуществления экспорта отображаемых событий выделите правой кнопкой мыши узел **Журнал,** в открывшемся контекстном меню выберите **Экспортировать список**.

Рисунок 135. Экспорт списка событий Журнала



Откроется окно **Сохранить как**, в котором укажите расположение и имя выходного файла, а также задайте его формат, после чего нажмите **Сохранить**

Рисунок 136. Окно определения имени, расположения и формата выходного файла



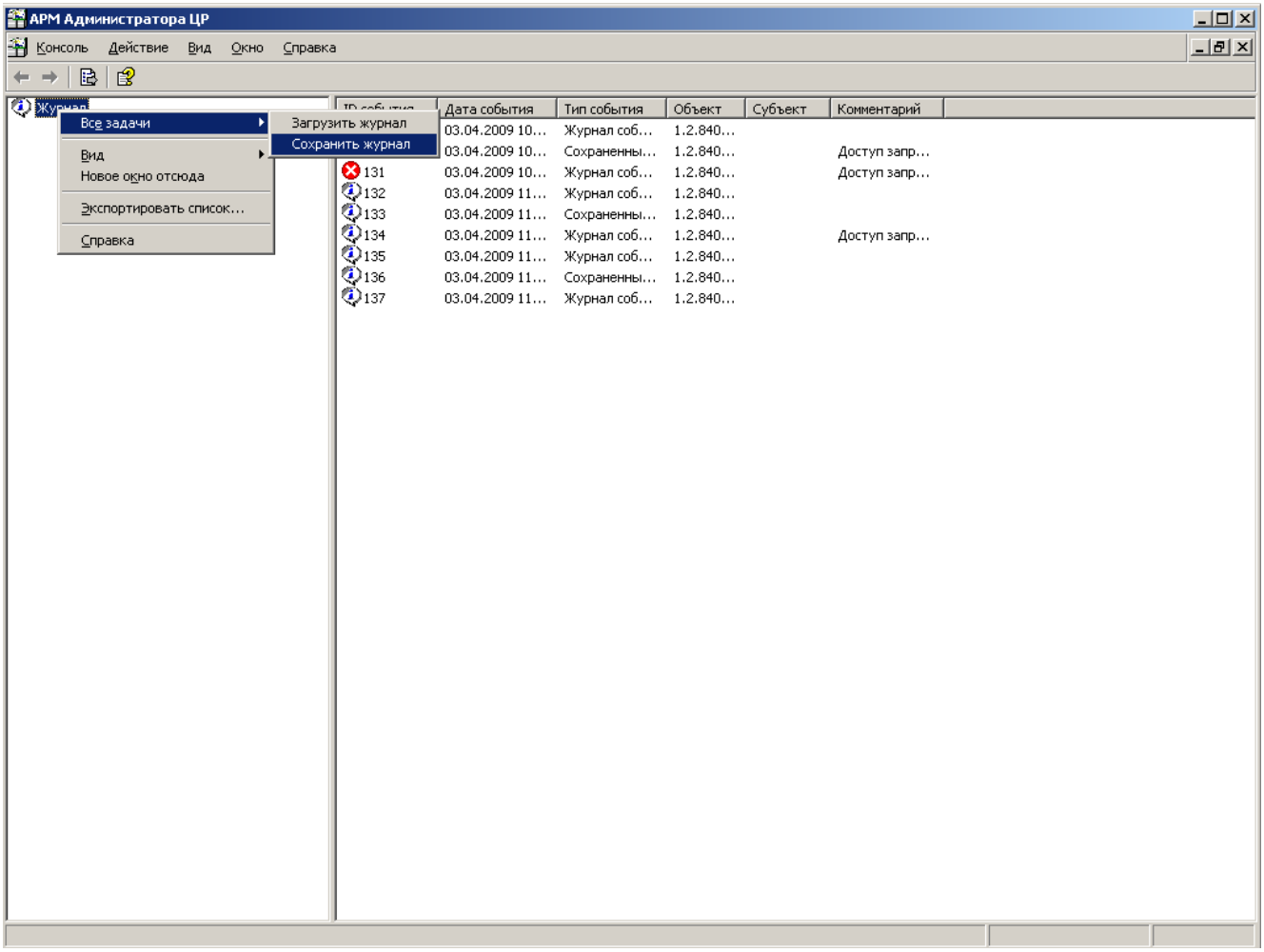
Экспортируются именно те события, которые отображаются в текущем окне просмотра **Журнала**, т.о. при использовании фильтров в выходной файл будут занесены только те события, которые удовлетворяют условиям фильтрации.

Установка переключателя **Сохранить только выбранные строки** окна **Сохранить как** вызовет экспорт только выделенных событий.

Журнал зарегистрированных событий ЦР может быть сохранен во внешний файл и подписан сертификатом администратора аудита в виде файла с расширением **.p7b** для очищения места в журнале АРМ администратора ЦР.

Для осуществления сохранения журнала выделите правой кнопкой мыши узел **Журнал,** в открывшемся контекстном меню выберите **Все задачи, Сохранить журнал.**

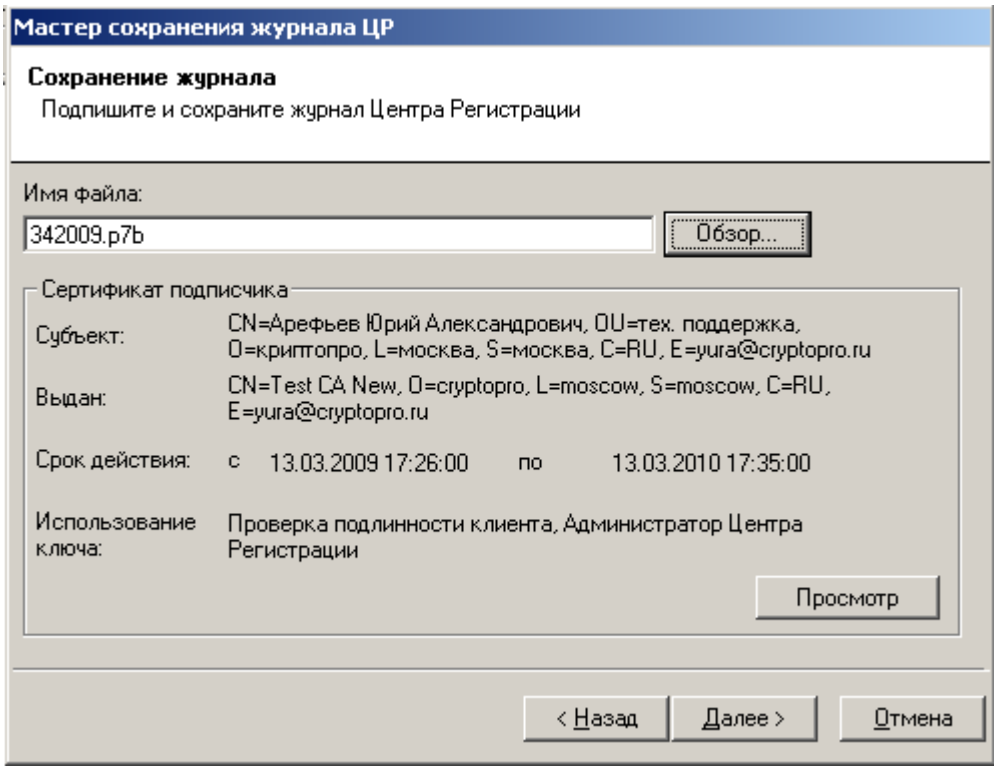
Рисунок 137. Сохранение Журнала событий ЦР



Откроется окно приветствия Мастера Сохранения журнала ЦР, в котором необходимо нажать **Далее** (при необходимости можно установить галочку “пропустить этот шаг при следующем запуске”), после чего откроется окно Мастера Сохранения

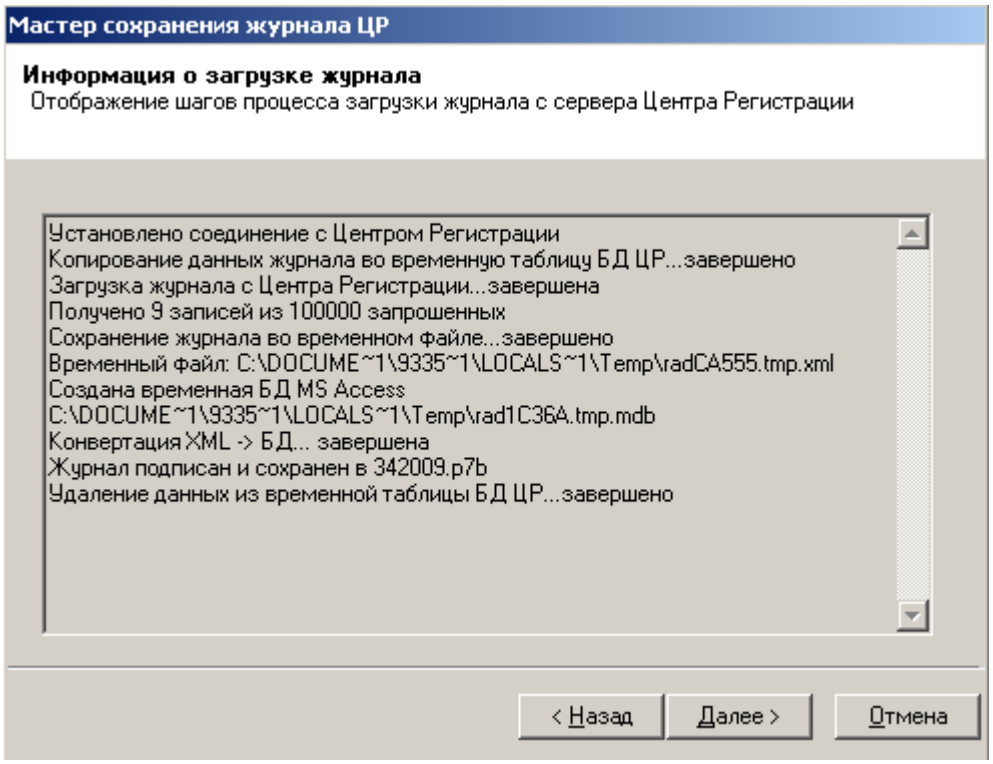
журнала ЦР, в котором можно выбрать имя файла (и путь для его сохранения – при нажатии кнопки обзор), и можно просмотреть сертификат, которым данный файл будет подписан.

Рисунок 138. Мастер Сохранения журнала событий ЦР



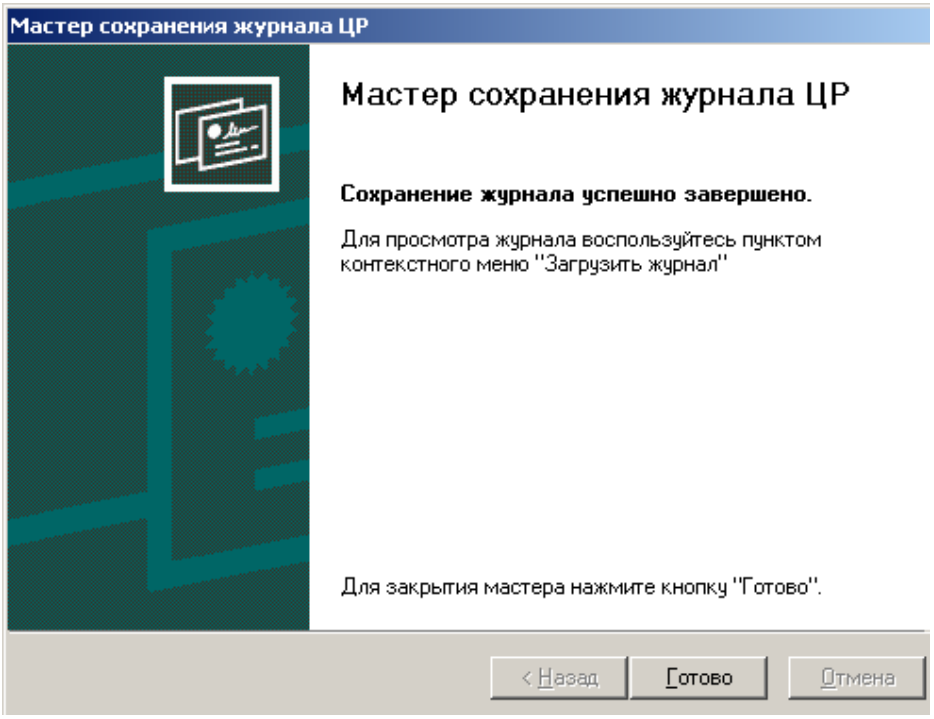
После нажатия клавиши **Далее** появится окно с результатами выполнения действий по созданию файла, его подписи и очистки журнала событий ЦР.

Рисунок 139. Информация о загрузке журнала событий ЦР



После этого мастер выдаст окно об успешном выполнении сохранения журнала.

Рисунок 140. Успешное выполнение сохранения журнала событий ЦР

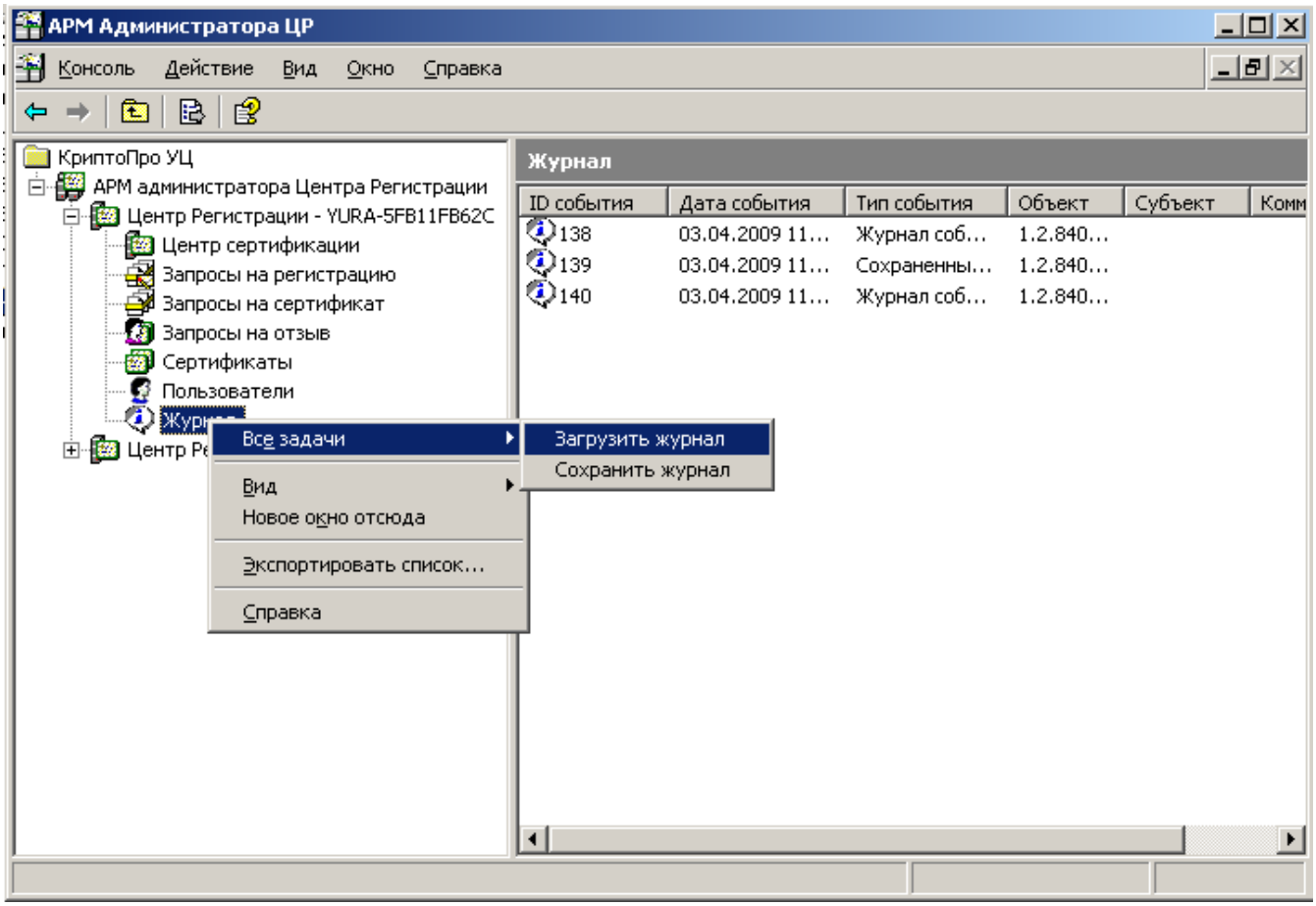


После нажмите на кнопку **Готово.**

После выполнения процедуры сохранения журнала все события удаляются из журнала АРМ администратора ЦР, о чем в нем появляются соответствующие записи событий (журнал событий сохранен аудитором, сохраненные события журнала получены аудитором, журнал событий очищен аудитором). Для просмотра сохраненного журнала есть возможность загрузить его в АРМ администратора ЦР, для этого необходимо выделите

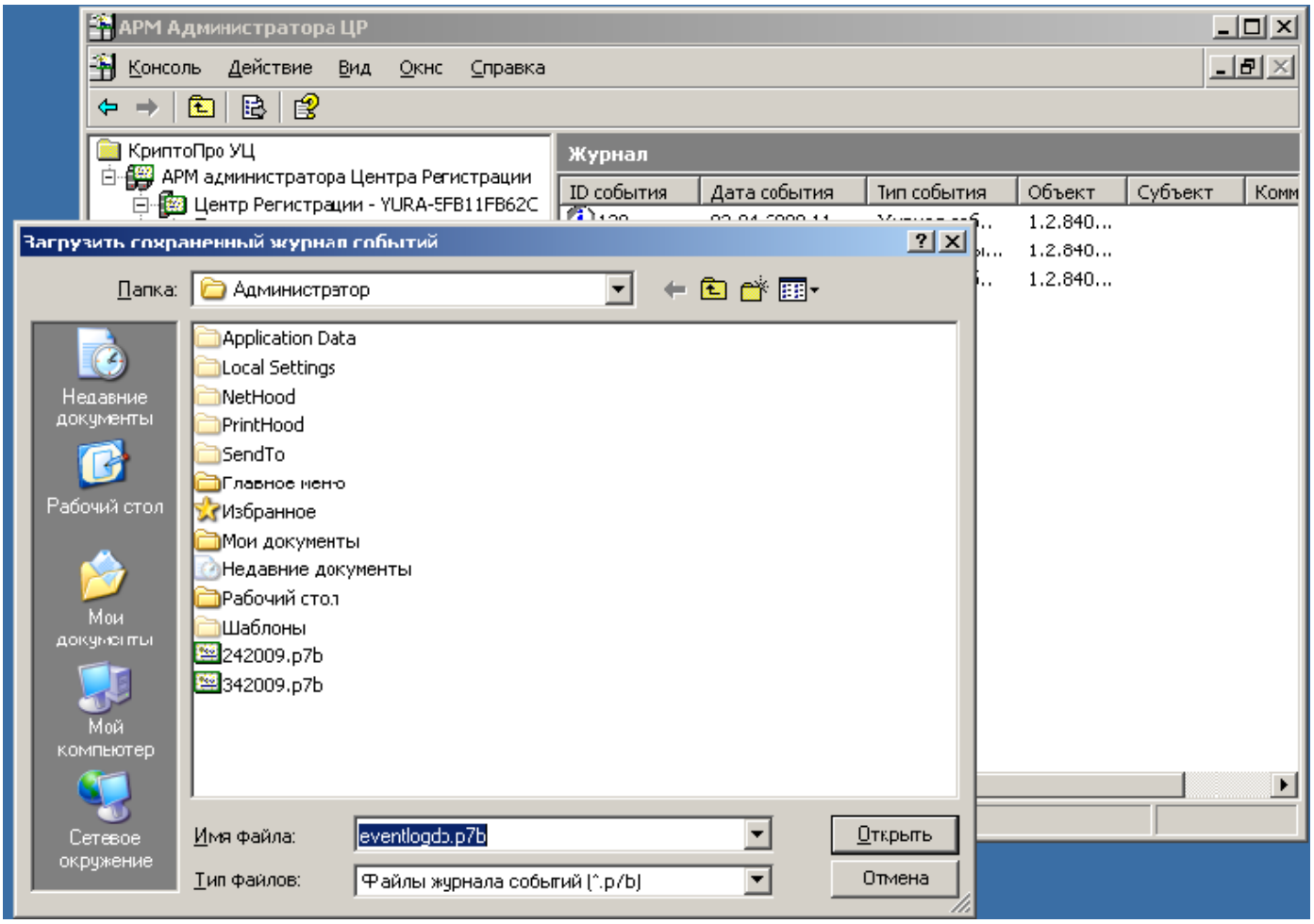
правой кнопкой мыши узел **Журнал,** в открывшемся контекстном меню выберите **Все задачи, Загрузить журнал.**

Рисунок 141. Загрузка журнала событий ЦР



Откроется окно, в котором необходимо выбрать файл для загрузки.

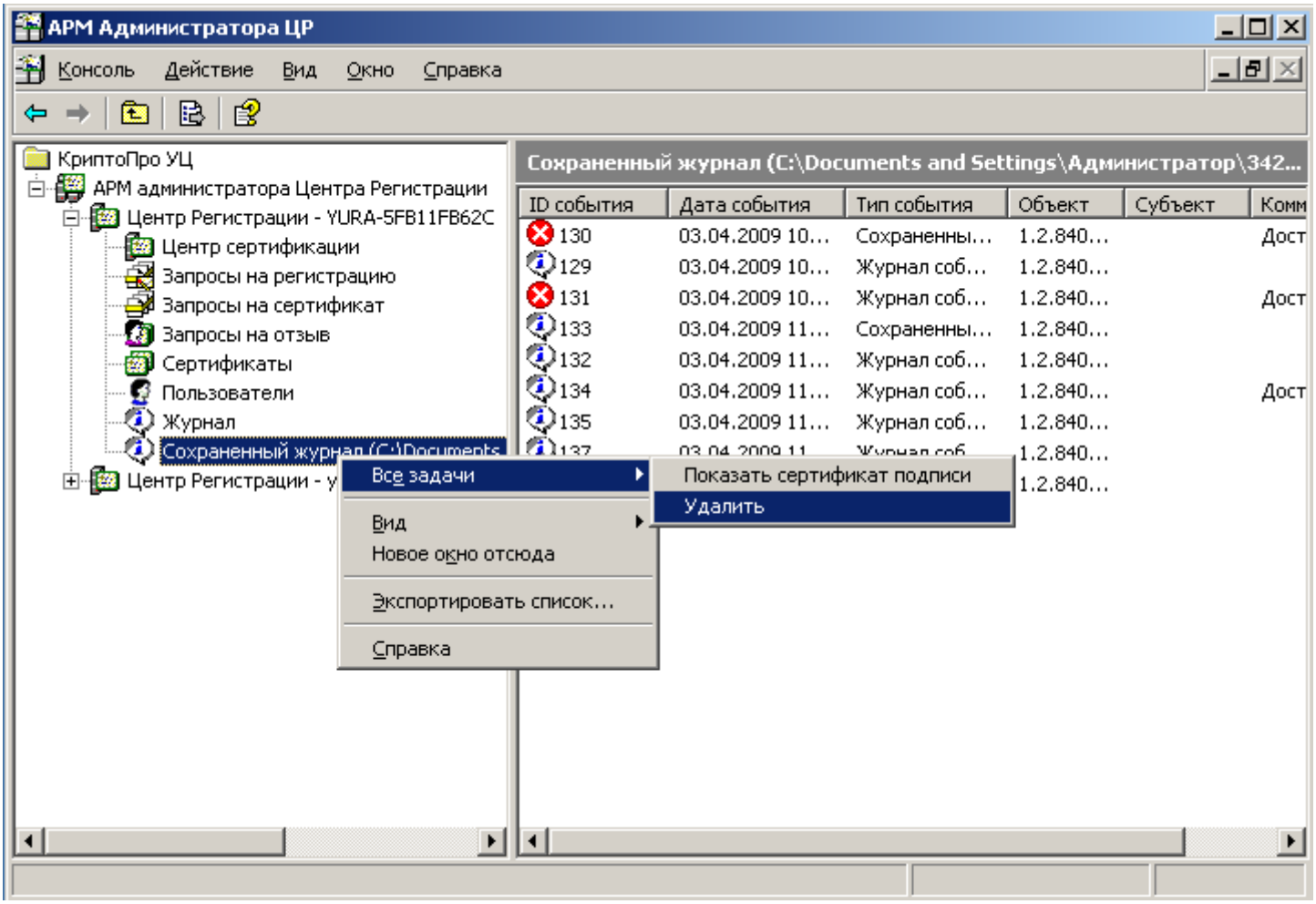
Рисунок 142. Окно выбора файла для загрузки журнала событий ЦР



После выбора файла для загрузки необходимо выбрать его и нажать кнопку **Открыть.** В АРМ администратора ЦР появится дополнительный узел **Сохраненный журнал (путь к файлу)**. В дальнейшем работа с загруженным журналом ЦР аналогична работе с обычным журналом ЦР.

Для загруженного журнала ЦР есть возможность его удаления из АРМ администратора ЦР и просмотра сертификата, которым он был подписан. Для этого необходимо выделите правой кнопкой мыши узел **Сохраненный журнал...,** в открывшемся контекстном меню выберите **Все задачи** и выберите необходимое действие.

Рисунок 143. Окно выбора функций Показать сертификат подписи и Удаление для загруженного журнала событий ЦР



17. Экспорт объектов управления

АРМ Администратора Центра Регистрации предоставляет возможность экспорта объектов управления, хранящихся в базе данных Центра Регистрации, во внешние файлы. Необходимость использования указанных объектов может быть вызвана осуществлением регламентных процедур по проведению разбора конфликтных ситуаций.

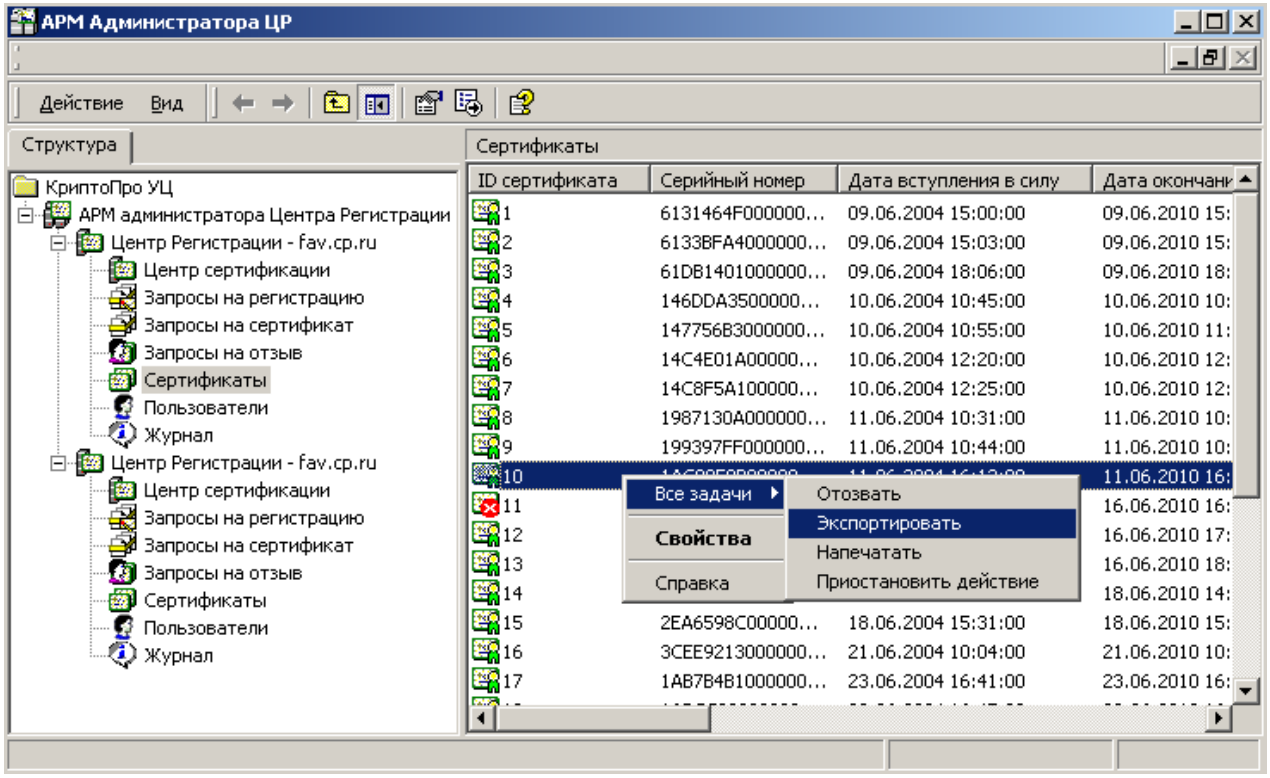
Экспорту могут быть подвергнуты следующие объекты управления:

- Сертификаты открытых ключей подписей;
- Запросы на изготовление сертификатов открытых ключей подписей;
- Запросы на отзыв, приостановление и возобновление действия сертификатов открытых ключей подписей.

17.1. Экспорт сертификатов открытых ключей подписей

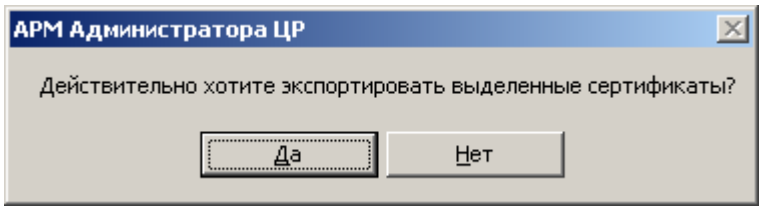
Для осуществления экспорта сертификата открытого ключа в окне просмотра изготовленных сертификатов узла **Сертификаты** выделите правой кнопкой мыши сертификат, который требуется экспортировать, в открывшемся контекстном меню выберите **Все задачи** -> **Экспортировать.**

Рисунок 14439. Экспорт сертификата ключа подписи



Откроется предупреждающее сообщение, требующее подтвердить выбор указанного действия, нажмите кнопку **Да**

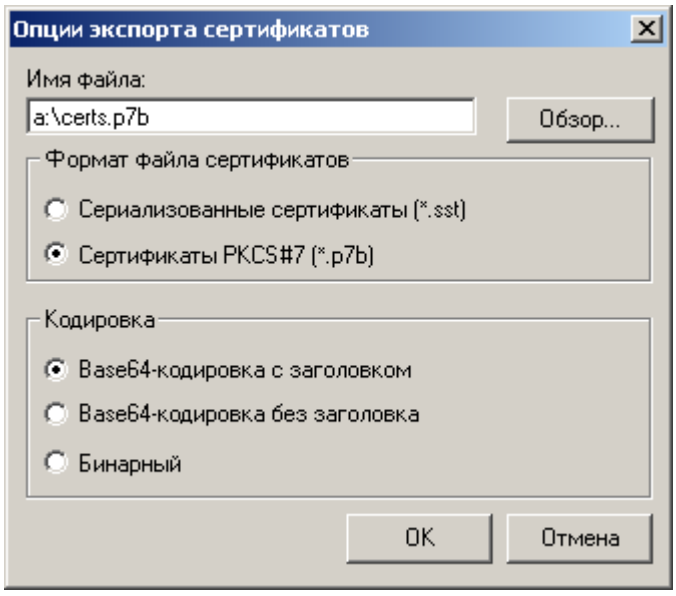
Рисунок 145. Подтверждение экспорта сертификата



Откроется окно **Опции экспорта сертификатов**, в котором установите нужные параметры экспорта, позволяющие определить:

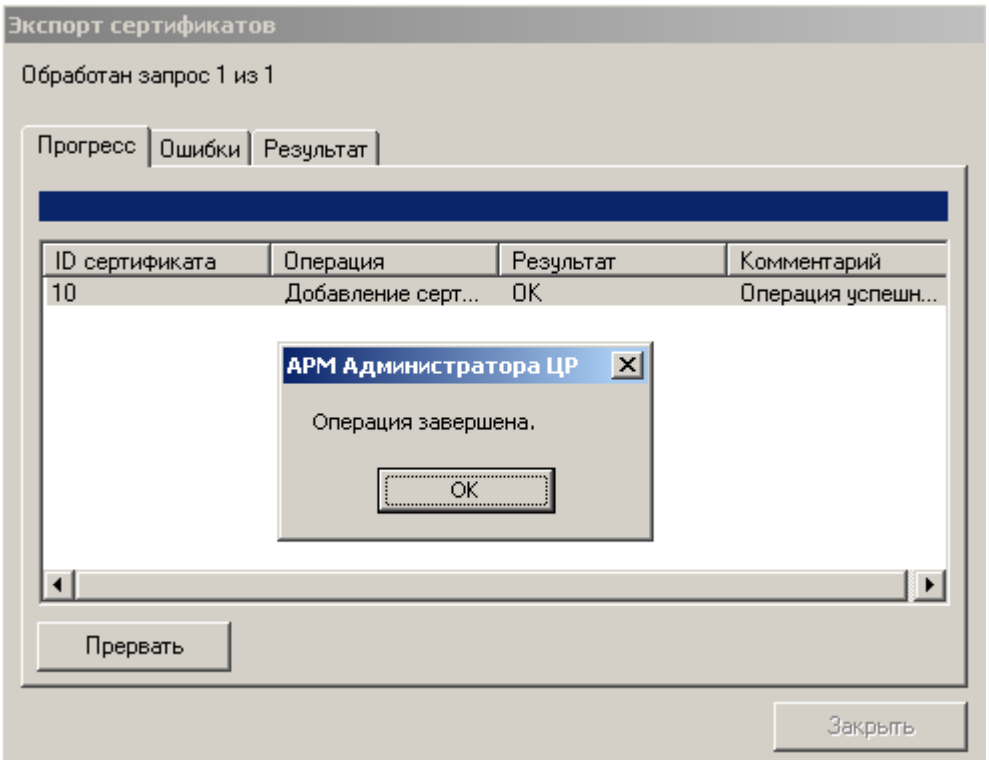
- размещение и имя выходного файла - поле **Имя файла** (для указания папки размещения выходного файла рекомендуется воспользоваться кнопкой **Обзор** данного окна);
- формат выходного файла – переключатель **Формат файла сертификатов**, позволяющий указать формат выходного файла - **PKCS#7 (.p7b)** или **Microsoft Serialized Certificate Store (.sst);**
- кодировку выходного файла – переключатель **Кодировка** (Base64 с заголовком, Base64 без заголовка, Бинарный (DER)).

Рисунок 146. Задание опций экспорта сертификатов



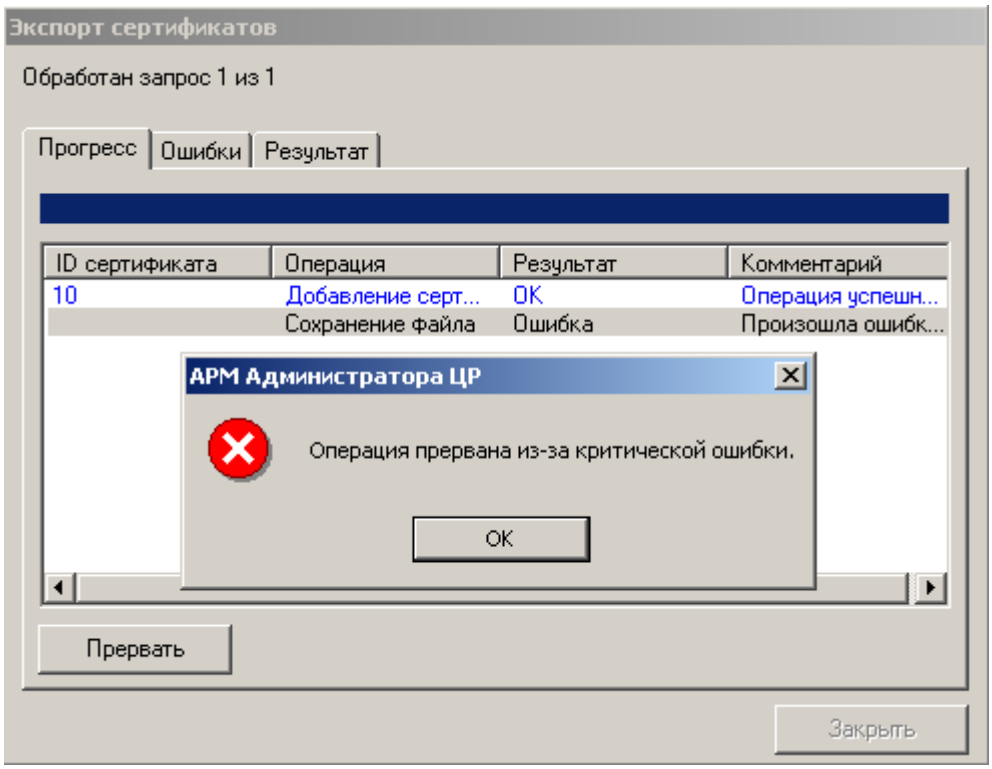
После задания необходимых параметров нажмите кнопку **OK**. Успешное выполнение экспорта сертификата вызовет появление сообщения **Операция завершена**, и в окне экспорта сертификатов будет отображена запись с результатом выполнения данного действия.

Рисунок 147. Успешное завершение процедуры экспорта сертификата



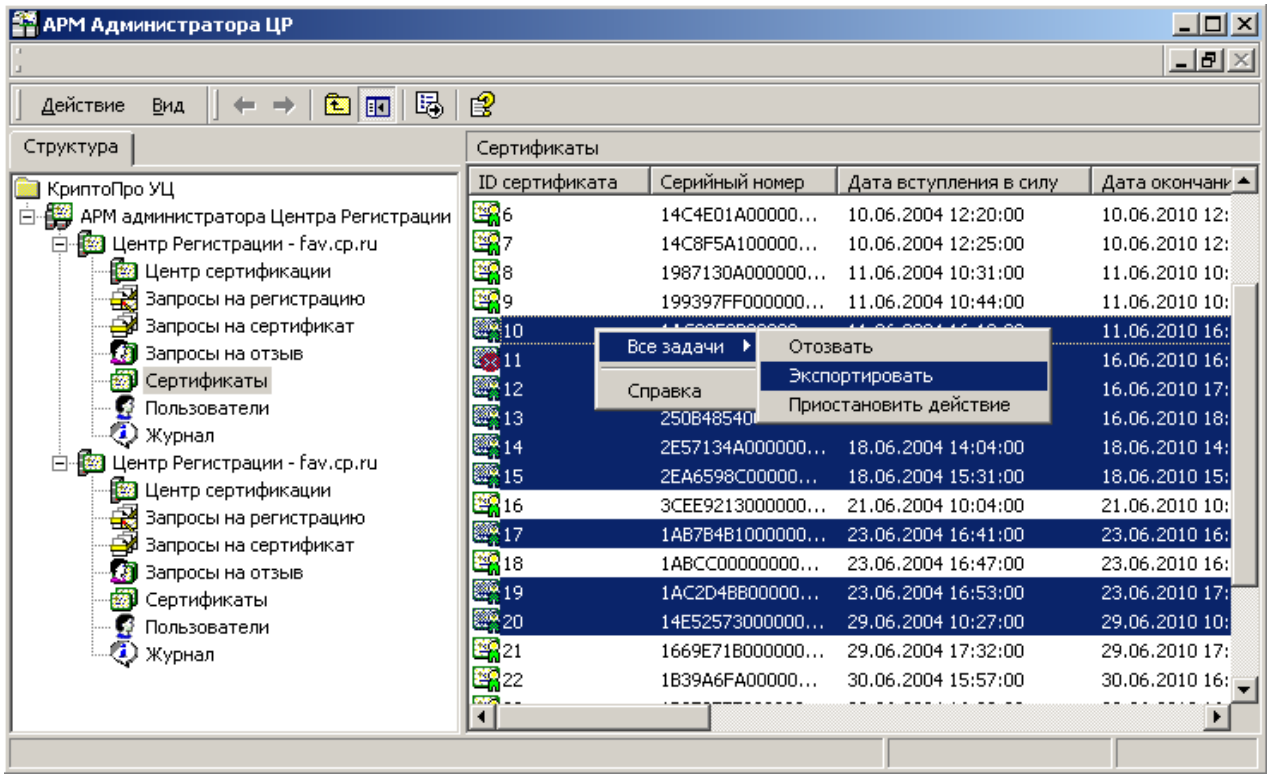
При появлении ошибки в процессе экспорта сертификата ключа подписи отображается соответствующее сообщение, а в окне **Экспорт сертификатов** указывается подробная причина ее возникновения. Наиболее часто встречающейся ошибкой является событие, вызванное отсутствием внешнего носителя либо его защитой от записи.

Рисунок 148. Сообщение об ошибке при экспорте сертификата



Для одновременного экспорта нескольких сертификатов ключей подписей (экспорта сертификатов в один выходной файл) выделите сертификаты, которые необходимо экспортировать, кликните на них правой кнопкой мыши и, в открывшемся контекстном пункте меню, выберите **Все задачи** -> **Экспортировать.**

Рисунок 149. Экспорт группы сертификатов в один файл

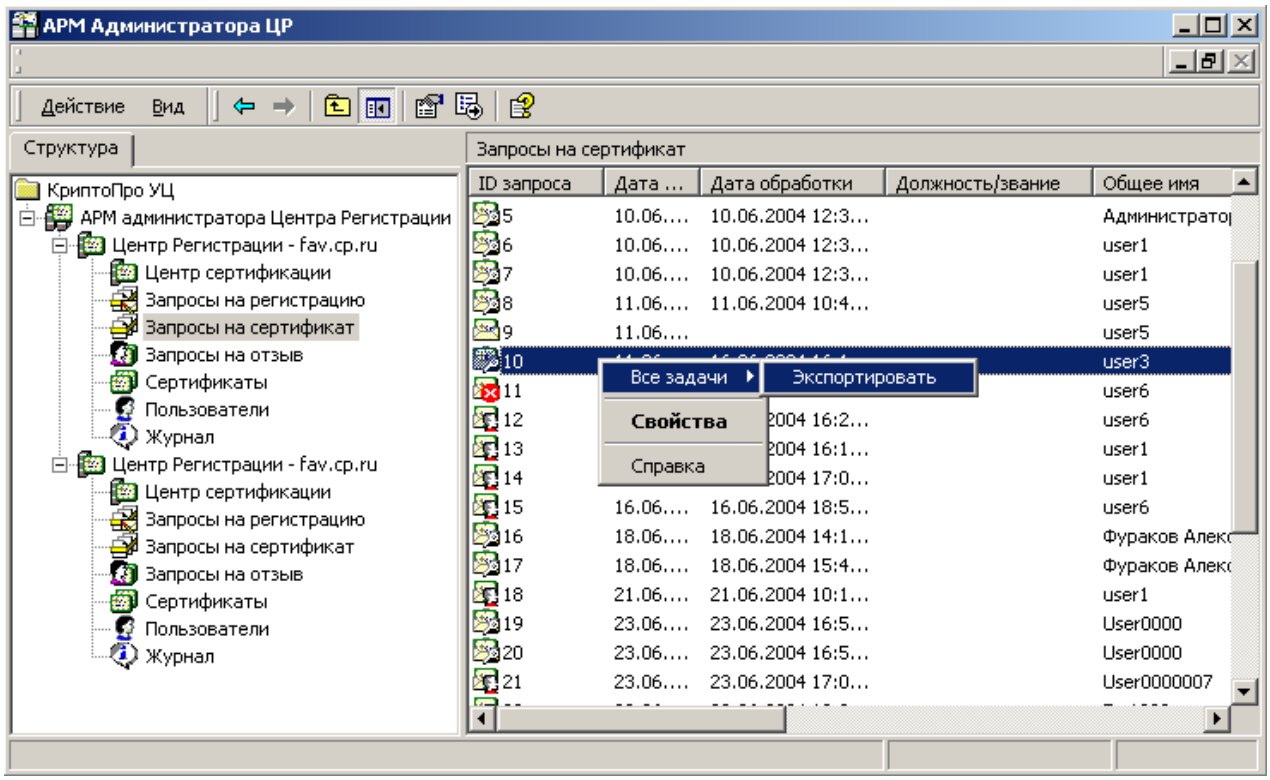


Экспорт сертификата (сертификатов) ключа подписи также может быть осуществлен в окне просмотра сертификатов конкретного пользователя. Порядок выполнения указанной процедуры аналогичен описанному в п. 17.1.

17.2. Экспорт запросов на изготовление сертификатов открытых ключей

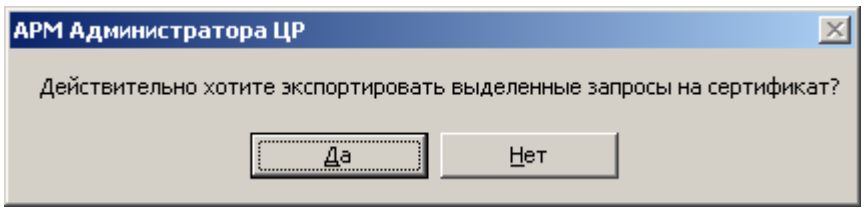
Для осуществления экспорта запроса на сертификат открытого ключа в окне просмотра запросов узла **Запросы на сертификат** выделите правой кнопкой мыши запрос на сертификат, который требуется экспортировать, в открывшемся контекстном меню выберите **Все задачи** -> **Экспортировать.**

Рисунок 150. Экспорт запроса на сертификат ключа подписи



Откроется предупреждающее сообщение, требующее подтвердить выбор указанного действия, нажмите кнопку **Да.**

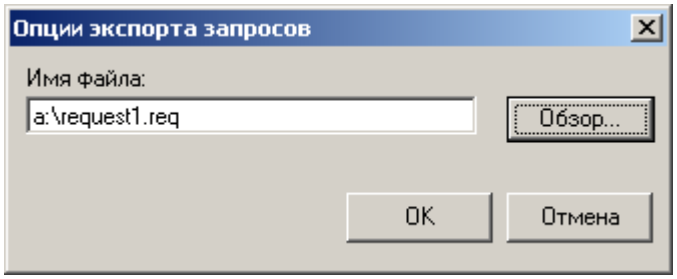
Рисунок 151. Подтверждение экспорта запроса на сертификат



Откроется окно **Опции экспорта запросов**, в котором установите путь размещения и имя выходного файла запроса на сертификат (для указания папки

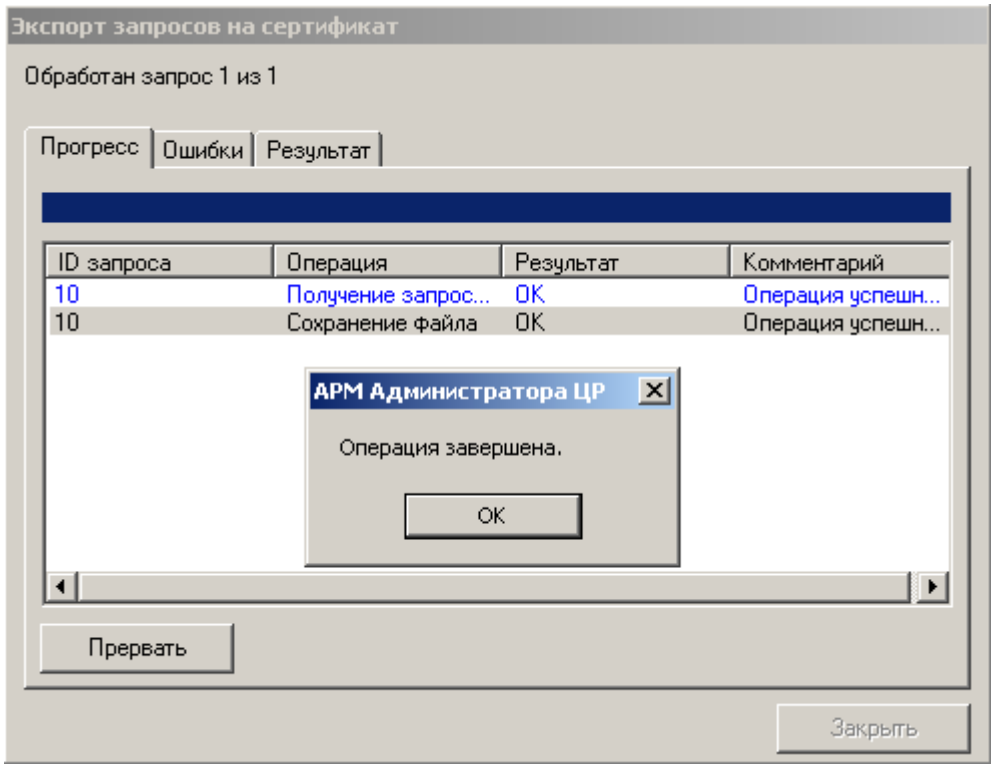
размещения выходного файла рекомендуется воспользоваться кнопкой **Обзор** данного окна), после чего нажмите кнопку **ОК.**

Рисунок 152. Задание опций экспорта запроса на сертификат



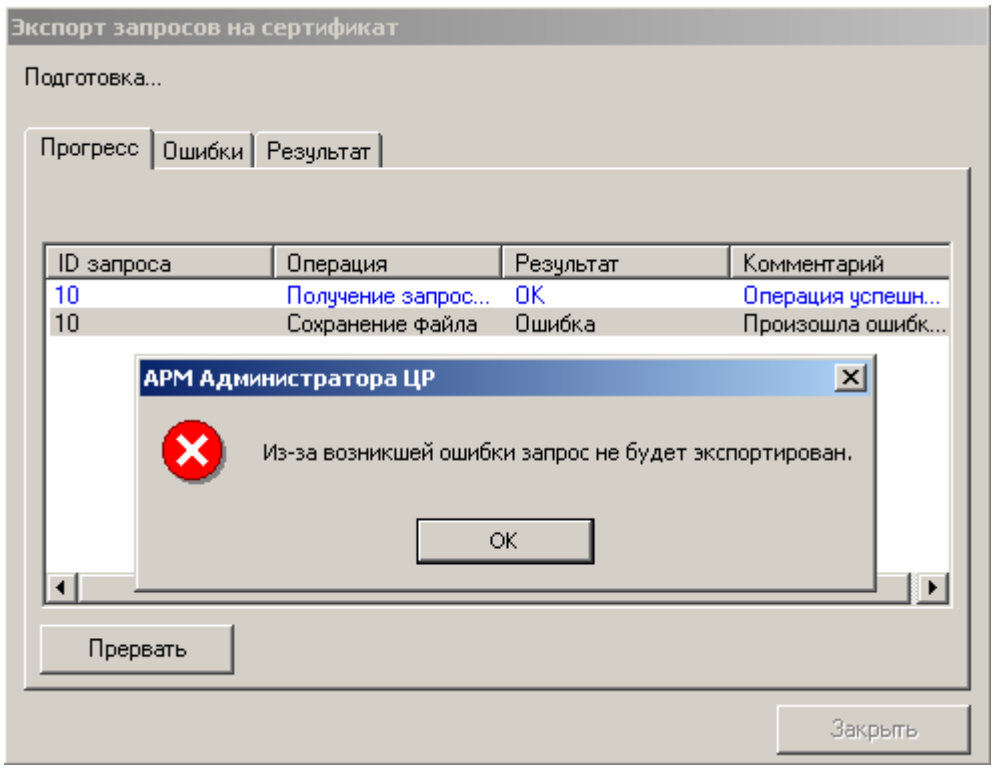
Успешное выполнение экспорта запроса на сертификат вызовет появление сообщения **Операция завершена,** и в окне **Экспорт запросов на сертификат** будет отображена запись с результатом выполнения данного действия.

Рисунок 153. Успешное завершение процедуры экспорта запроса на сертификат



При появлении ошибки в процессе экспорта запроса на сертификат отображается соответствующее сообщение, а в окне **Экспорт запросов на сертификат** указывается подробная причина ее возникновения. Наиболее часто встречающейся ошибкой является событие, вызванное отсутствием внешнего носителя либо его защитой от записи.

Рисунок 154. Сообщение об ошибке при экспорте запроса на сертификат



В базе данных Центра Регистрации запрос на сертификат может быть представлен в следующих форматах:

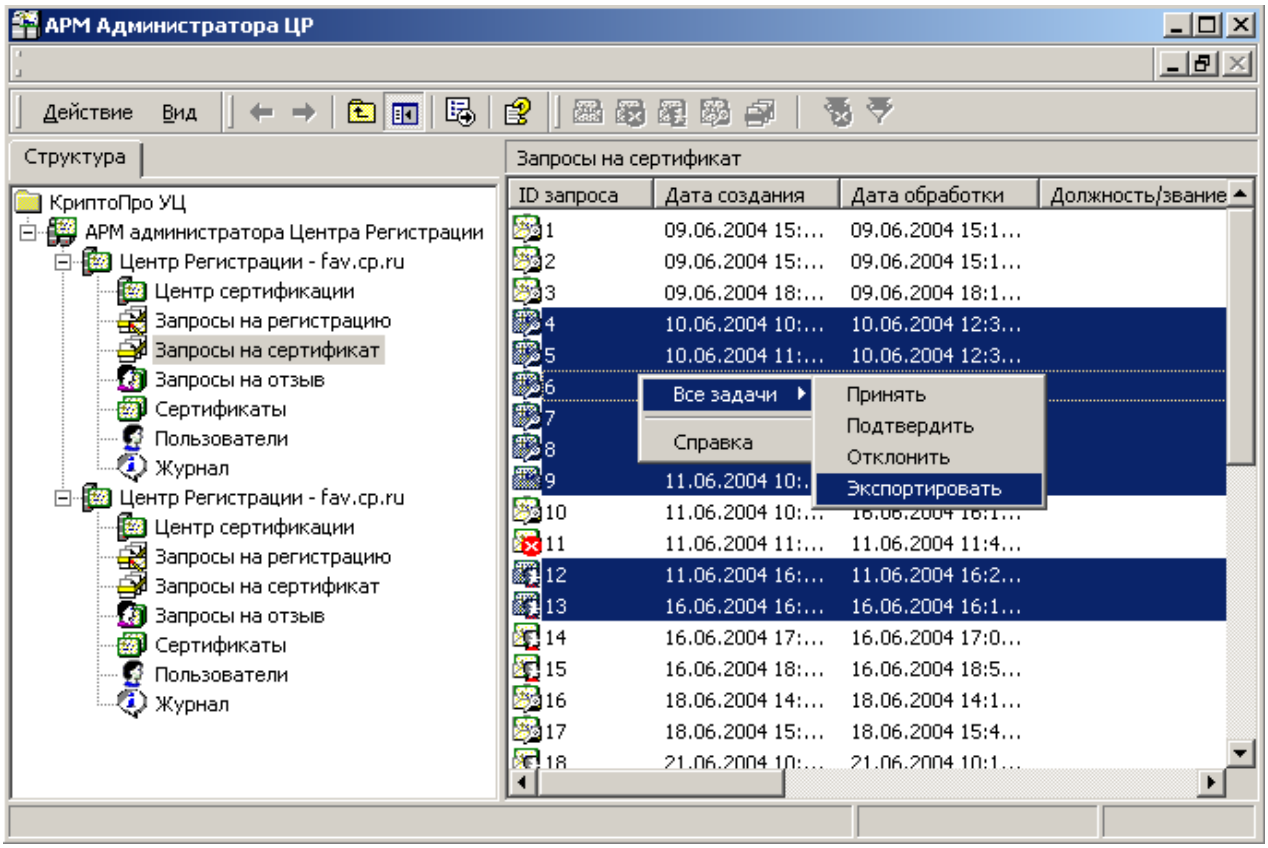
- в формате PKCS#10 в кодировке Base64 (собственно запрос на сертификат определенный стандартом PKCS#10). В данном формате представлены следующие запросы (данные запросы в окне просмотра свойств запроса на сертификат позиционируются как неподписанные):
  - поступившие на Центр Регистрации от пользователя, обладающего маркером временного доступа (посредством АРМ пользователя), и еще не одобренные привилегированным пользователем УЦ;
  - поступившие на Центр Регистрации от пользователя, посредством передачи файла запроса на сертификат формата PKCS#10, зарегистрированные на Центре Регистрации, но еще не одобренные привилегированным пользователем УЦ;
- в формате PKCS#7 в кодировке Base64 – документ с электронной цифровой подписью. В качестве подписываемых данных используется запрос на сертификат формата PKCS#10, а ЭЦП выполнена на закрытом ключе пользователя (привилегированного пользователя) Удостоверяющего Центра. В данном формате представлены следующие запросы:
  - поступившие на Центр Регистрации от пользователя с использованием подключения на действующем сертификате (посредством АРМ пользователя) и еще не одобренные привилегированным пользователем УЦ;
  - поступившие на Центр Регистрации от пользователя, обладающего маркером временного доступа (посредством АРМ пользователя), и уже одобренные привилегированным пользователем УЦ;
  - поступившие на Центр Регистрации от пользователя, посредством передачи файла запроса на сертификат формата PKCS#10, зарегистрированные на Центре Регистрации и одобренные привилегированным пользователем УЦ;

- в формате PKCS#7 в кодировке Base64 – документ с электронной цифровой подписью, ЭЦП выполнена на закрытом ключе привилегированного пользователя УЦ. В качестве подписываемых данных используется документ формата PKCS#7, представляющий собой запрос, поступивший на Центр Регистрации от пользователя с использованием подключения на действующем сертификате (посредством АРМ пользователя). В данном формате представлены следующие запросы:
  - поступившие на Центр Регистрации от пользователя с использованием подключения на действующем сертификате (посредством АРМ пользователя) и одобренные привилегированным пользователем УЦ.

Для одновременного экспорта нескольких запросов на сертификаты выделите запросы, которые необходимо экспортировать, кликните на них правой кнопкой мыши и в открывшемся контекстном меню выберите **Все задачи** -> **Экспортировать.**

В данном случае каждый запрос на сертификат будет сохранен в отдельном файле, и последовательно для каждого запроса будет появляться окно указания имени и размещения выходного файла для этого запроса.

Рисунок 155. Экспорт группы запросов на сертификат



Экспорт запроса (запросов) на сертификат также может быть осуществлен в окне просмотра запросов на сертификат конкретного пользователя. Порядок выполнения указанной процедуры аналогичен описанному в п. 17.2.

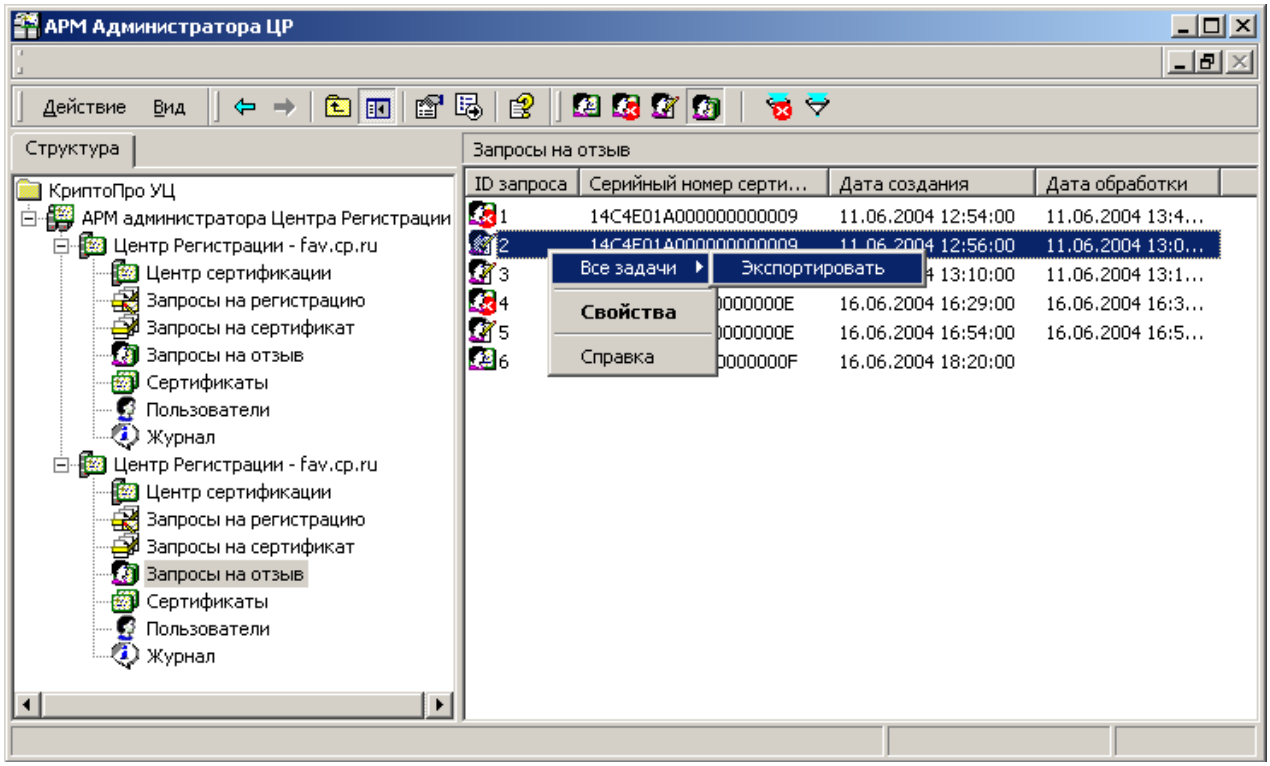
17.3. Экспорт запросов на отзыв, приостановление и возобновление действия сертификатов открытых ключей подписей

Для осуществления экспорта запроса на отзыв, приостановление и возобновление действия сертификата открытого ключа в окне просмотра запросов узла **Запросы на отзыв** выделите правой кнопкой мыши запрос, который требуется экспортировать, в открывшемся контекстном меню выберите **Все задачи** -> **Экспортировать.**

В окне просмотра запросов узла **Запросы на отзыв** помимо запросов на отзыв размещаются запросы на приостановление и возобновление действия сертификатов. Определение типа запроса осуществляется в окне просмотра его Свойств (для этого необходимо дважды кликнуть левой кнопкой мыши необходимый запрос, либо выделить его правой кнопкой мыши и в открывшемся контекстном меню выбрать пункт **Свойства**). Содержание поля **Причина отзыва** – **Приостановка действия** указывает на то, что данный запрос является Запросом на приостановление действия сертификата. Содержание поля **Причина отзыва** – **Запрос на возобновление действия** указывает на то, что данный запрос является Запросом на возобновление действия сертификата.

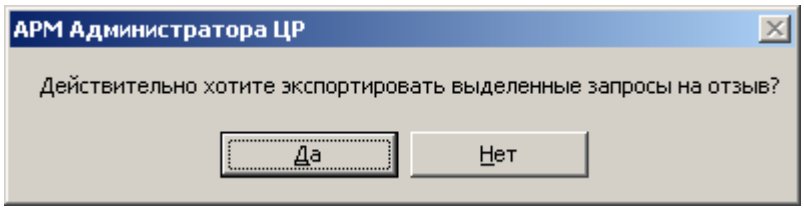
В данном разделе экспорт указанных запросов будет рассмотрен на примере экспорта запроса на отзыв сертификата. Процедуры экспорта запросов на приостановление и возобновление действия сертификата осуществляется аналогично экспорту запроса на отзыв сертификата.

Рисунок 156. Экспорт запроса на отзыв сертификата



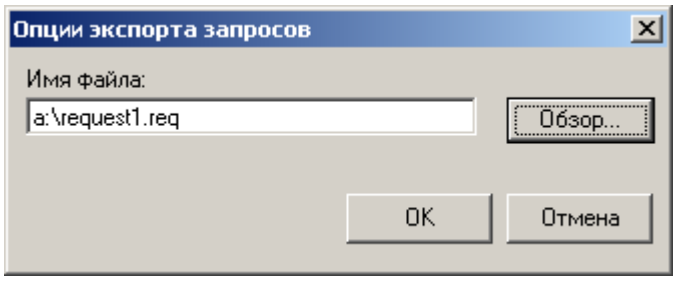
Откроется предупреждающее сообщение, требующее подтвердить выбор указанного действия, нажмите кнопку **Да**

Рисунок 157. Подтверждение экспорта запроса на отзыв сертификата



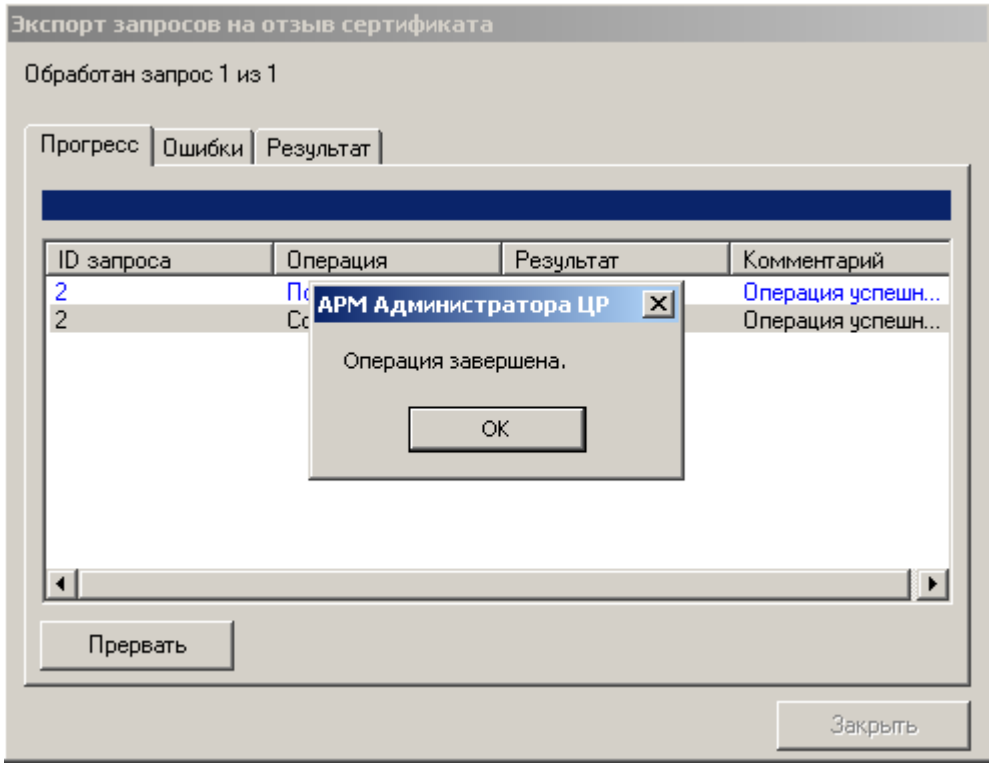
Откроется окно **Опции экспорта запросов**, в котором установите путь размещения и имя выходного файла запроса на отзыв сертификата (для указания папки размещения выходного файла рекомендуется воспользоваться кнопкой **Обзор** данного окна) после чего нажмите кнопку **ОК**

Рисунок 158. Задание опций экспорта запроса на отзыв сертификата



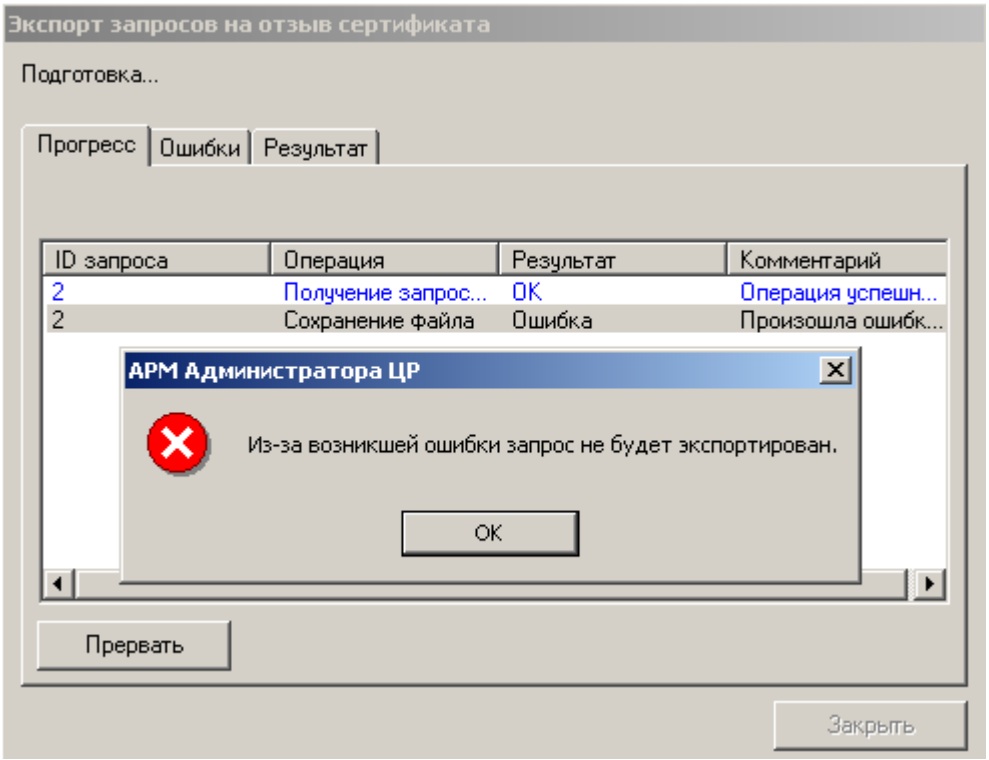
Успешное выполнение экспорта запроса на отзыв сертификата вызовет появление сообщения **Операция завершена** и в окне **Экспорт запросов на отзыв сертификата** будет отображена запись с результатом выполнения данного действия.

Рисунок 159. Успешное завершение процедуры экспорта запроса на отзыв сертификата



При появлении ошибки в процессе экспорта запроса на отзыв сертификата отображается соответствующее сообщение, а в окне **Экспорт запросов на отзыв сертификата** указывается подробная причина ее возникновения. Наиболее часто встречающейся ошибкой является событие, вызванное отсутствием внешнего носителя либо его защитой от записи.

Рисунок 160. Сообщение об ошибке при экспорте запроса на отзыв сертификата



В базе данных Центра Регистрации запрос на отзыв сертификата может быть представлен в следующих форматах:

- в формате PKCS#7 в кодировке Base64 – документ с электронной цифровой подписью, выполненной на закрытом ключе пользователя (привилегированного пользователя) Удостоверяющего Центра (a1). В качестве подписываемых данных используется строка следующего формата: «SN=CertificateSerialNumber, RC=ReasonCode, SC=SomeComment», где:

  - CertificateSerialNumber - серийный номер отзываемого сертификата открытого ключа;

  - ReasonCode - код причины отзыва из следующего перечня допустимых значений: "0" - Не указана; "1" - Компрометация ключа; "2" - Компрометация ЦС; "3" - Изменение принадлежности; "4" - Сертификат заменен; "5" - Прекращение работы;

  - SomeComment - текстовое значение комментария.

  В данном формате представлены следующие запросы:

  - поступившие на Центр Регистрации как от пользователя с использованием подключения на действующем сертификате (посредством АРМ пользователя), так и поступившие от привилегированного пользователя (посредством АРМ Администратора ЦР), но еще не одобренные привилегированным пользователем УЦ;

- поступившие на Центр Регистрации от пользователя с использованием подключения на действующем сертификате (посредством АРМ пользователя) и поступившие от привилегированного пользователя (посредством АРМ Администратора ЦР), но отклоненные привилегированным пользователем ЦР.

- в формате PKCS#7 в кодировке Base64 – документ с электронной цифровой подписью, ЭЦП выполнена на закрытом ключе привилегированного пользователя УЦ. В качестве подписываемых данных используется документ формата PKCS#7, представляющий собой запрос, структура которого описана выше (a1). В данном формате представлены следующие запросы:
  - поступившие на Центр Регистрации от пользователя с использованием подключения на действующем сертификате (посредством АРМ пользователя) и поступившие от привилегированного пользователя (посредством АРМ Администратора ЦР), и уже одобренные привилегированным пользователем УЦ.

В базе данных Центра Регистрации запрос на приостановление действия сертификата может быть представлен в следующих форматах:

- в формате PKCS#7 в кодировке Base64 – документ с электронной цифровой подписью, выполненной на закрытом ключе пользователя (привилегированного пользователя) Удостоверяющего Центра (b1). В качестве подписываемых данных используется строка следующего формата: «SN=CertificateSerialNumber, RC=ReasonCode, HD=HoldDuration, SC=SomeComment», где:

  - CertificateSerialNumber - серийный номер отзываемого сертификата открытого ключа;

  - ReasonCode - «6» – приостановление действия;

  - HoldDuration – срок, на который приостанавливается действие сертификата, в следующем формате: Y-M-W-D-H-M, где: Y – число лет; M – число месяцев; W – число недель; D – число дней; H – число часов; M – число минут;

  - SomeComment - текстовое значение комментария.

  В данном формате представлены следующие запросы:
  - поступившие на Центр Регистрации как от пользователя с использованием подключения на действующем сертификате (посредством АРМ пользователя), так и поступившие от привилегированного пользователя (посредством АРМ Администратора ЦР), но еще не одобренные привилегированным пользователем УЦ;
  - поступившие на Центр Регистрации от пользователя с использованием подключения на действующем сертификате (посредством АРМ пользователя) и поступившие от привилегированного пользователя (посредством АРМ Администратора ЦР), но отклоненные привилегированным пользователем ЦР;

- в формате PKCS#7 в кодировке Base64 – документ с электронной цифровой подписью, ЭЦП выполнена на закрытом ключе привилегированного пользователя УЦ. В качестве подписываемых данных используется документ формата PKCS#7, представляющий собой запрос, структура которого описана выше (b1). В данном формате представлены следующие запросы:
  - поступившие на Центр Регистрации от пользователя с использованием подключения на действующем сертификате (посредством АРМ пользователя) и поступившие от привилегированного пользователя

(посредством АРМ Администратора ЦР), и уже одобренные привилегированным пользователем УЦ.

В базе данных Центра Регистрации запрос на возобновление действия сертификата может быть представлен в следующих форматах:

- в формате PKCS#7 в кодировке Base64 – документ с электронной цифровой подписью, выполненной на закрытом ключе пользователя (привилегированного пользователя) Удостоверяющего Центра (с1). В качестве подписываемых данных используется строка следующего формата: «SN=CertificateSerialNumber, RC=ReasonCode, SC=SomeComment», где:

  - CertificateSerialNumber - серийный номер отзываемого сертификата открытого ключа;

  - ReasonCode - «-1» - возобновление действия;

  - SomeComment - текстовое значение комментария.

  В данном формате представлены следующие запросы:

  - поступившие на Центр Регистрации как от пользователя с использованием подключения на действующем сертификате (посредством АРМ пользователя), так и поступившие от привилегированного пользователя (посредством АРМ Администратора ЦР), но еще не одобренные привилегированным пользователем УЦ;
  - поступившие на Центр Регистрации от пользователя с использованием подключения на действующем сертификате (посредством АРМ пользователя) и поступившие от привилегированного пользователя (посредством АРМ Администратора ЦР), но отклоненные привилегированным пользователем ЦР;

- в формате PKCS#7 в кодировке Base64 – документ с электронной цифровой подписью, ЭЦП выполнена на закрытом ключе привилегированного пользователя УЦ. В качестве подписываемых данных используется документ формата PKCS#7, представляющий собой запрос, структура которого описана выше (с1). В данном формате представлены следующие запросы:

  - поступившие на Центр Регистрации от пользователя с использованием подключения на действующем сертификате (посредством АРМ пользователя) и поступившие от привилегированного пользователя (посредством АРМ Администратора ЦР), и уже одобренные привилегированным пользователем УЦ.

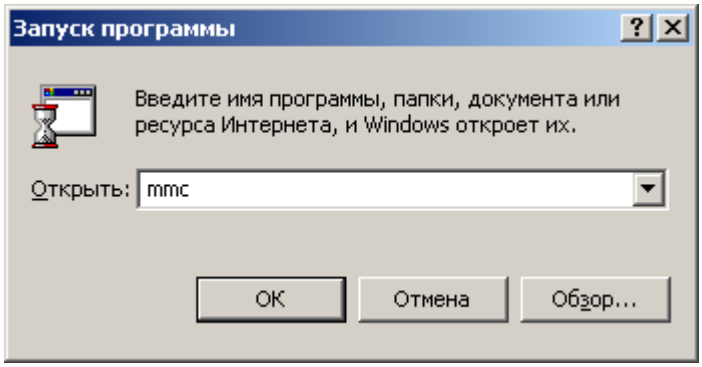
Экспорт запросов на отзыв, приостановление и возобновление действия сертификата также может быть осуществлен в окне просмотра **Запросов на отзыв** конкретного пользователя. Порядок выполнения указанной процедуры аналогичен описанному в п. 17.3.

18. Использование АРМ администратора ЦР в консоли управления MMC

Программное обеспечение АРМ администратора ЦР реализовано в виде изолированной оснастки Microsoft Management Console (MMC) и может использоваться совместно с другими средствами администрирования, реализованными в соответствии с указанным интерфейсом в рамках одной консоли управления.

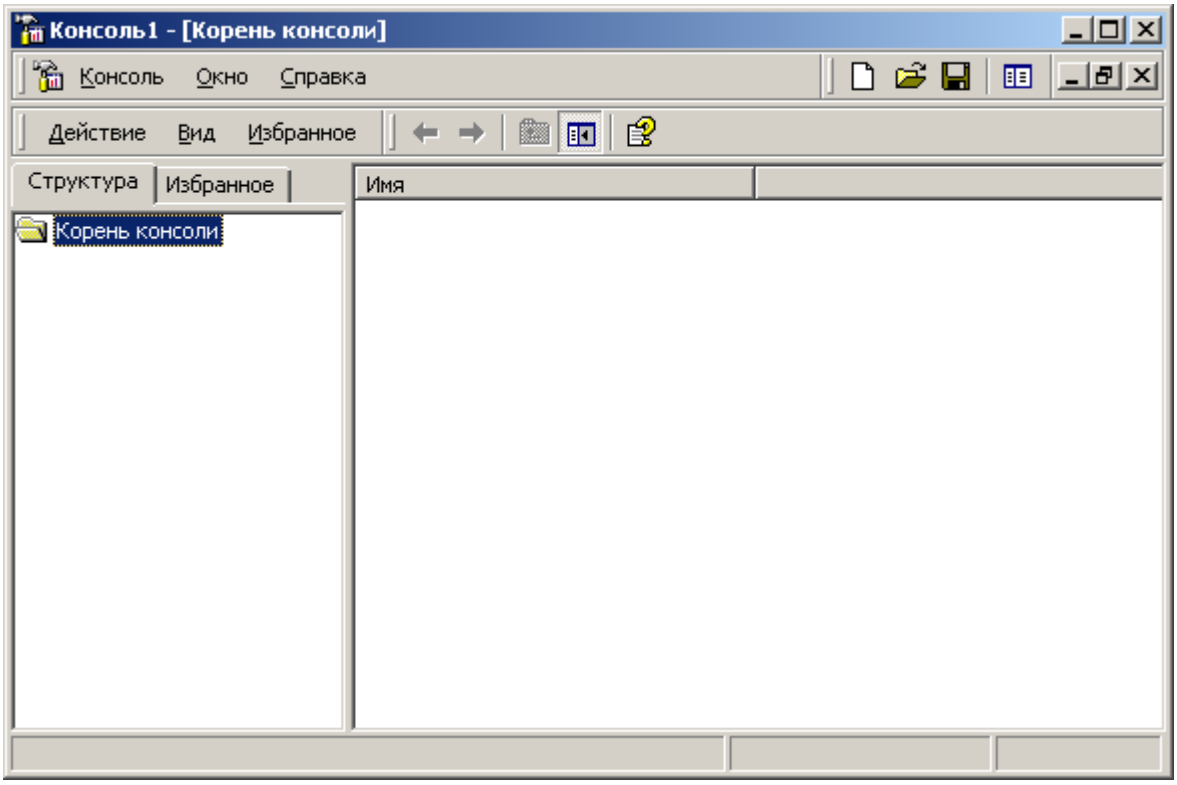
Для создания новой консоли управления нажмите **Пуск\Выполнить,** в окне **Запуск программы** введите **MMC** и нажмите кнопку **ОК.**

Рисунок 161. Запуск консоли mmc



Откроется окно консоли **Консоль1.**

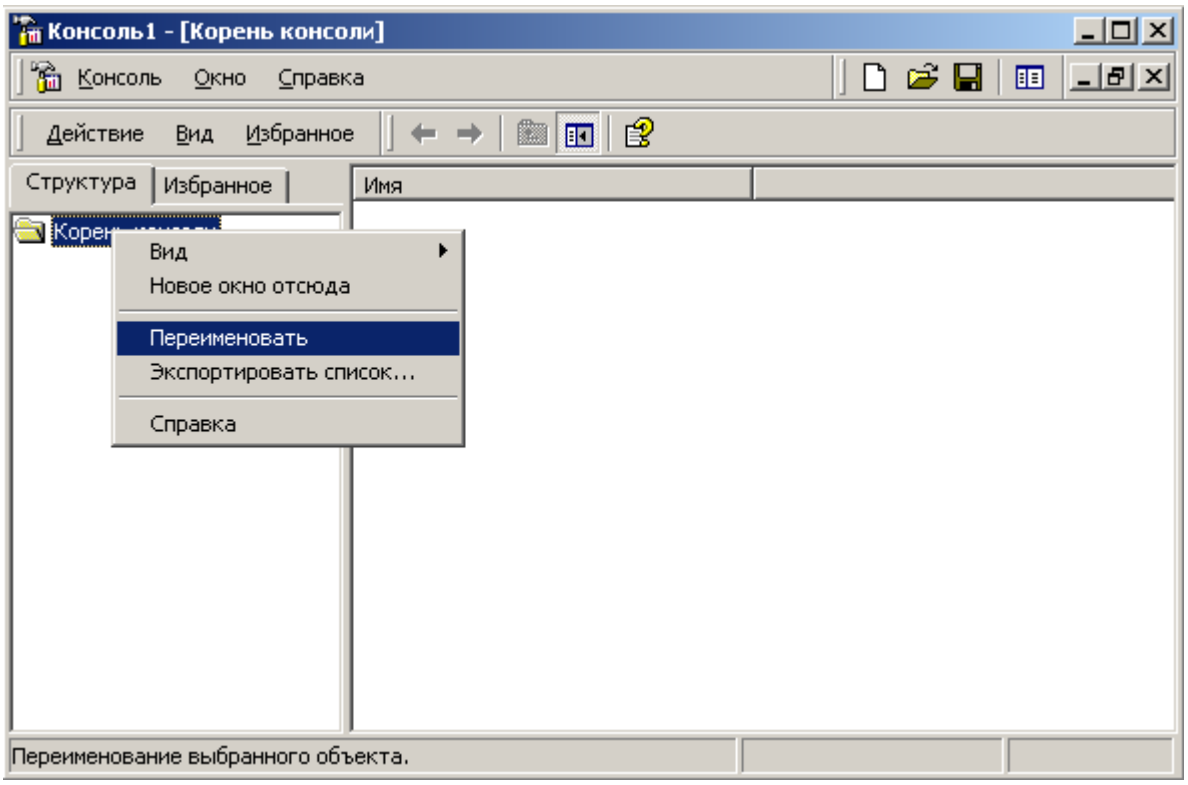
Рисунок 162. Окно консоли Консоль1



Для удобства и отражения функциональности созданной консоли управления переименуйте узел **Корень консоли** в **Администрирование УЦ**. Для этого выберите

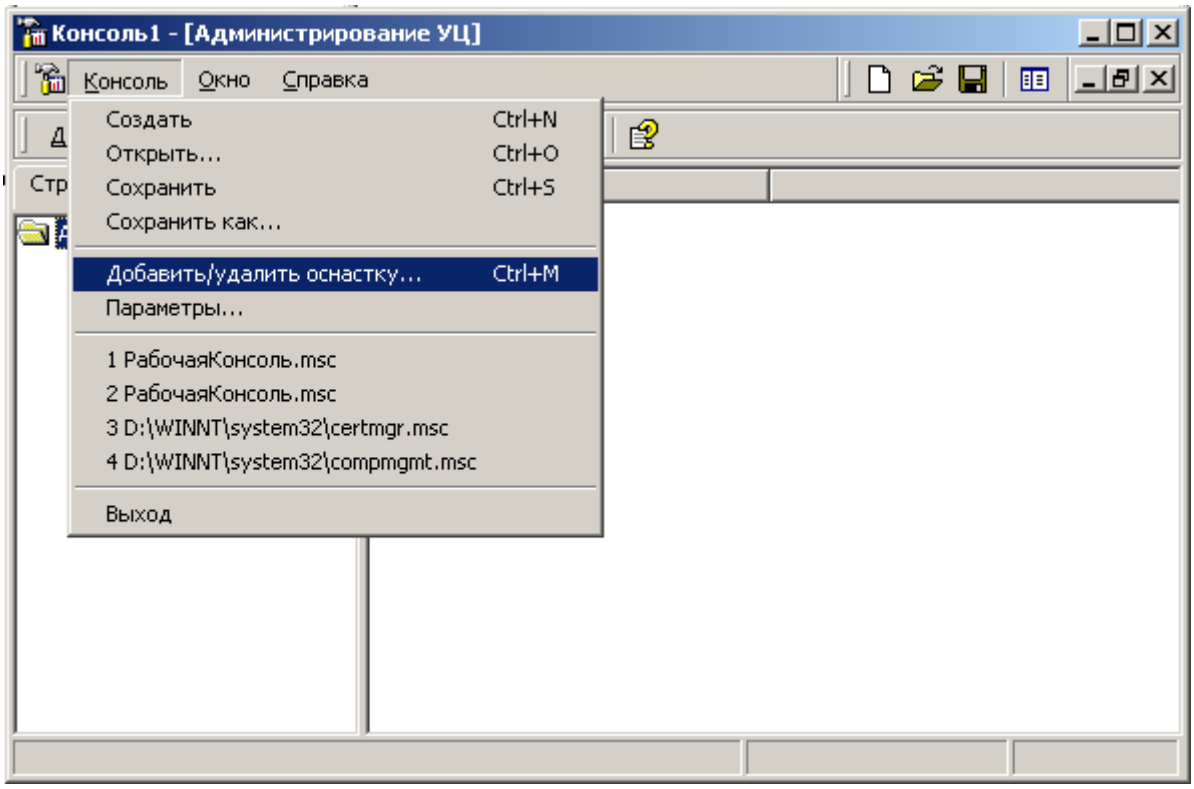
правой кнопкой мыши узел **Корень консоли,** в открывшемся контекстном меню нажмите **Переименовать** и введите новое название корневого узла консоли.

Рисунок 163. Переименование корневого узла созданной консоли



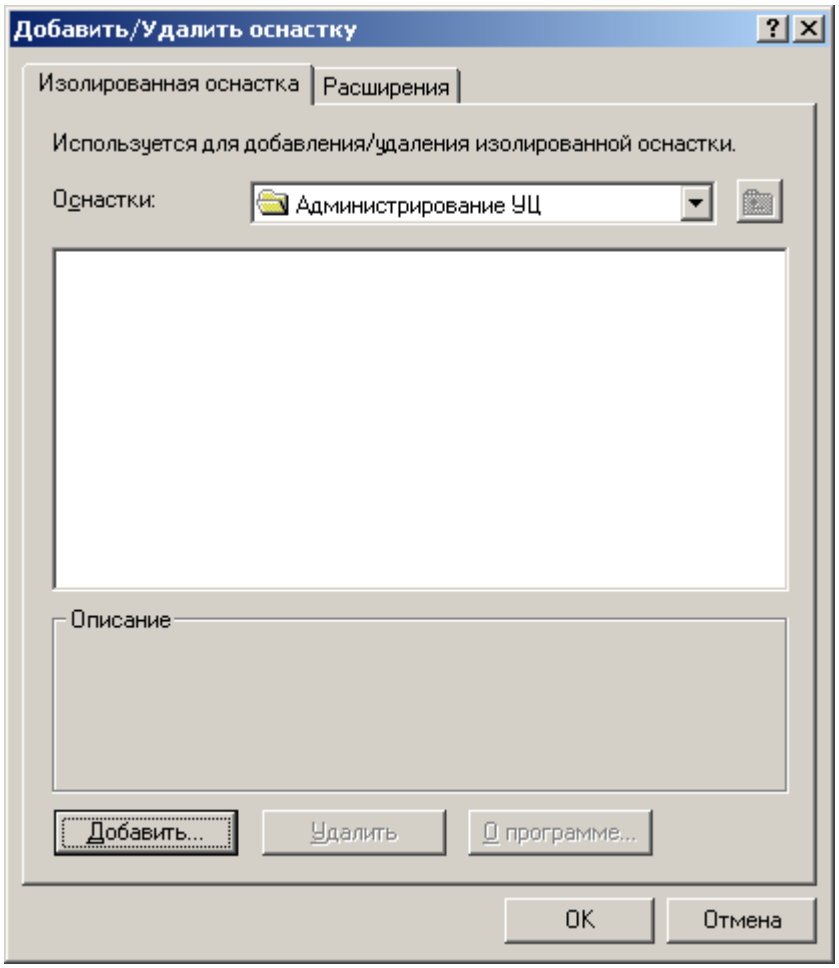
Для добавления оснастки **АРМ администратора ЦР** нажмите кнопку **Консоль**, затем в раскрывшемся меню выберите **Добавить/Удалить оснастку...**

Рисунок 164. Выбор пункта меню Добавить/Удалить оснастку...



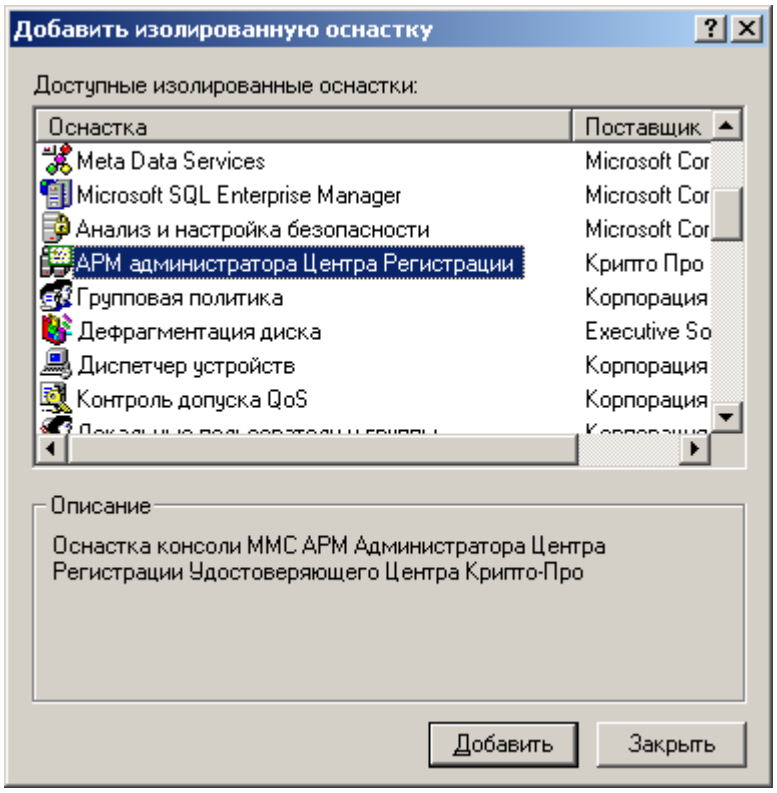
Откроется окно **Добавить/Удалить оснастку**, затем нажмите кнопку **Добавить...**

Рисунок 165. Окно Добавить/Удалить оснастку



В раскрывшемся списке доступных изолированных оснасток выберите оснастку **АРМ администратора Центра Регистрации** и нажмите кнопку **Добавить.**

Рисунок 166. Окно Добавить изолированную оснастку

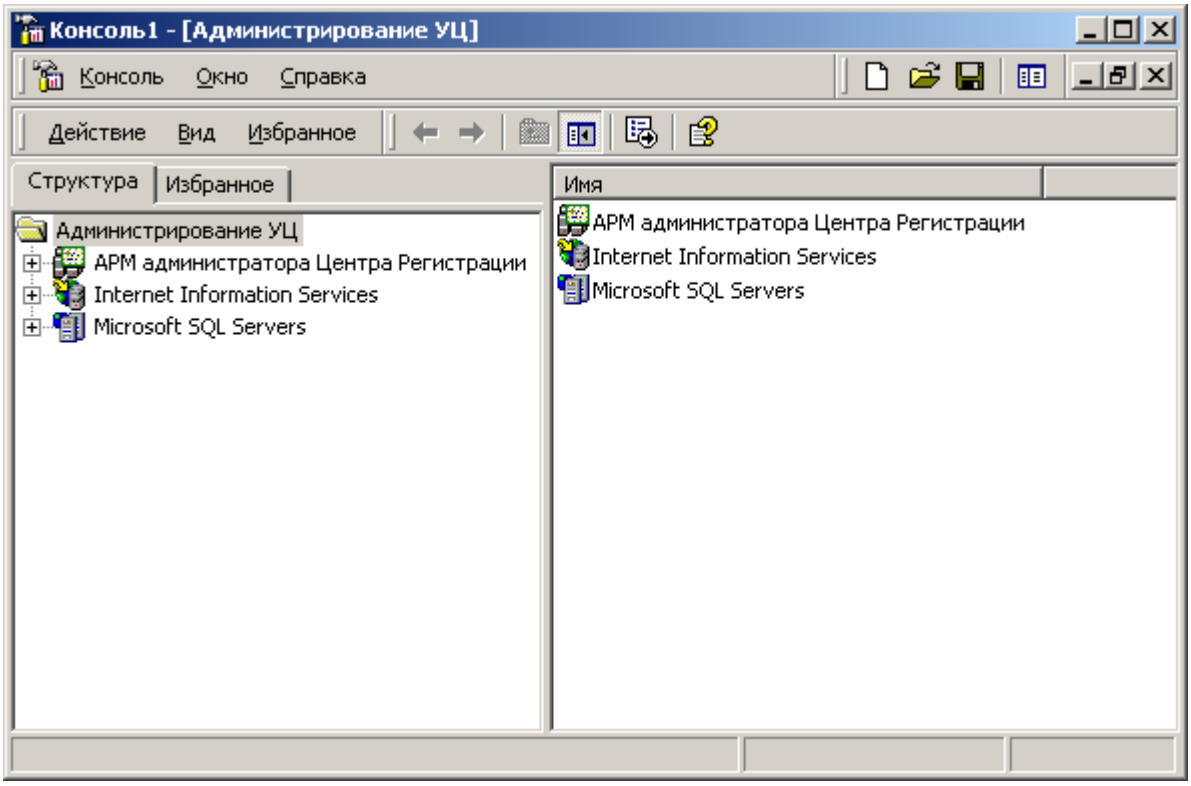


При необходимости, добавьте те оснастки, которые вам необходимы для администрирования компонентов Удостоверяющего Центра, например, **Internet Information Services** – для настройки Вэб-узла Центра Регистрации и **Microsoft SQL Enterprise Manager** – для организации резервного копирования Базы данных Центра Регистрации. Данные действия выполняются аналогично добавлению оснастки **АРМ администратора Центра Регистрации**.

После добавления всех необходимых оснасток в окне **Добавить изолированную оснастку** нажмите кнопку **Закрыть** и в окне **Добавить/Удалить оснастку** нажмите кнопку **ОК.**

Окно консоли управления примет следующий вид:

Рисунок 167. Окно консоли управления Консоль1 после добавления необходимых изолированных оснасток

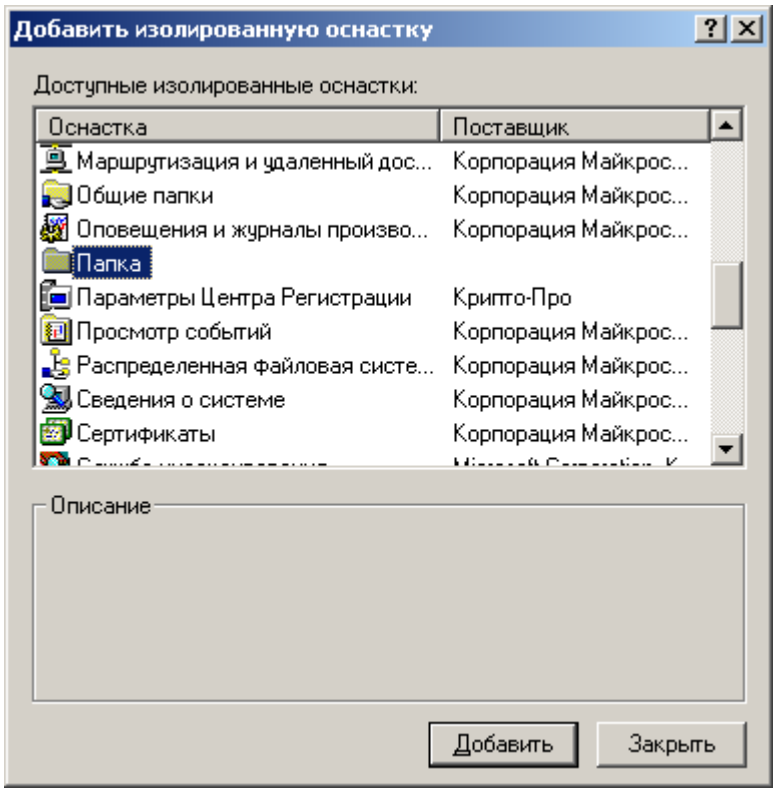


Интерфейс **Microsoft Management Console** позволяет объединять оснастки в отдельные папки и организовывать средства администрирования по иерархической модели. В приведенном выше примере три изолированные оснастки объединены в одном узле – корневом узле **Администрирование УЦ**.

Удобным средством управления сертификатами, установленными на компьютере, является оснастка **Сертификаты**. Создадим в приведенной консоли новый узел – папку **Сертификаты** и добавим в нее две оснастки, осуществляющие управление сертификатами, располагающимися в хранилищах **Текущего пользователя** и **Локального компьютера**.

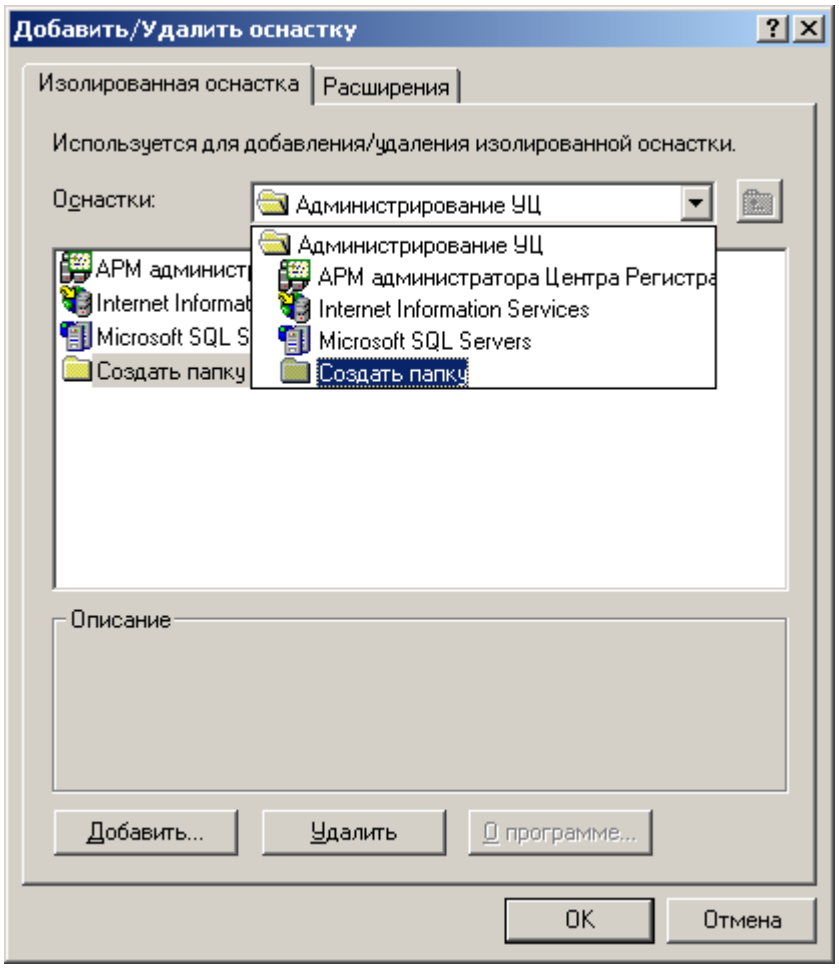
Для этого нажмите кнопку **Консоль** и в раскрывшемся меню выберите **Добавить/Удалить оснастку...** В появившемся окне нажмите кнопку **Добавить...**, из списка выберите оснастку **Папка** и в окне **Добавить изолированную оснастку** последовательно нажмите **Добавить** и **Закрыть.**

Рисунок 168. Создание нового узла консоли управления



Затем в окне **Добавить/Удалить оснастку** в раскрывающемся списке **Оснастки** выберите созданный новый узел с именем **Создать папку**, либо нажмите на этот узел двойным щелчком левой кнопки «мыши».

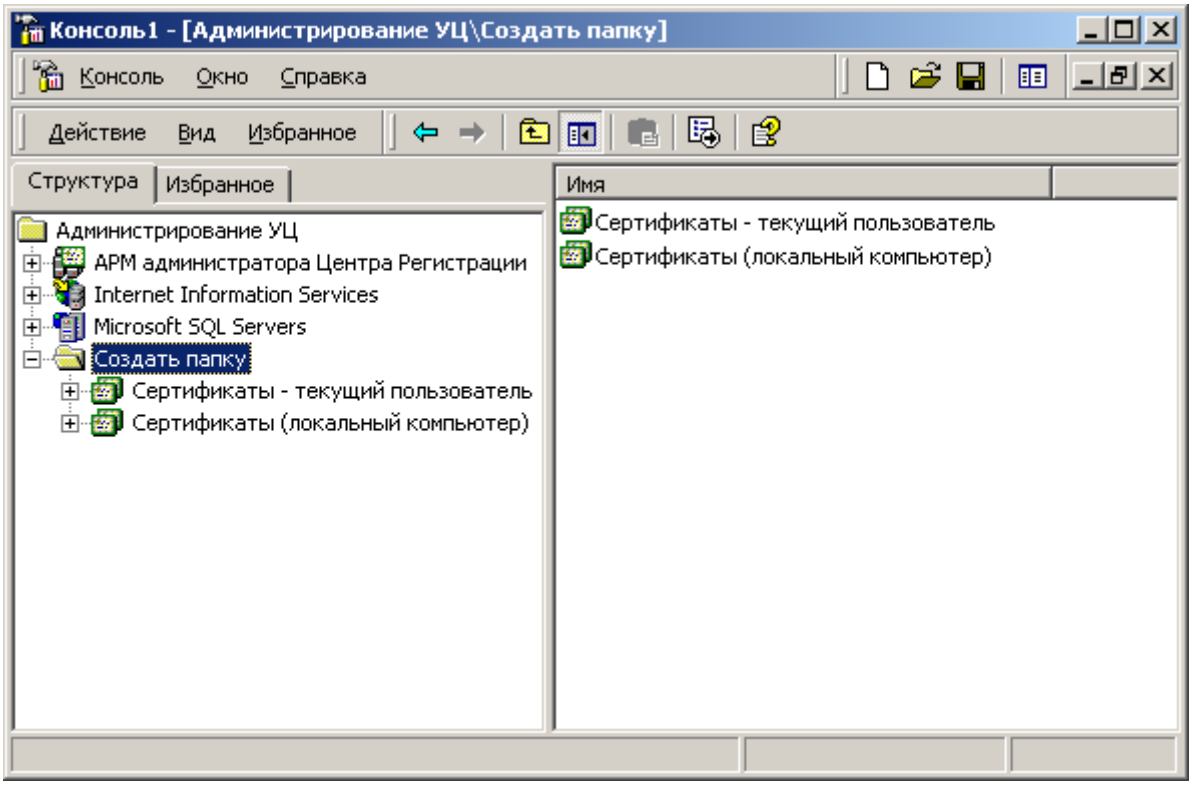
Рисунок 169. Выбор нового узла для добавления оснасток



В обновленном окне область выбранных оснасток пуста. Далее нажмите кнопку **Добавить...** и аналогично предыдущим пунктам выберите из списка оснастку **Сертификаты** для управления сертификатами **Моей учетной записи**, а затем снова выберите эту же оснастку, но для управления сертификатами **Учетной записи компьютера**.

После проделанных действий окно консоли управления **Консоль1** примет следующий вид:

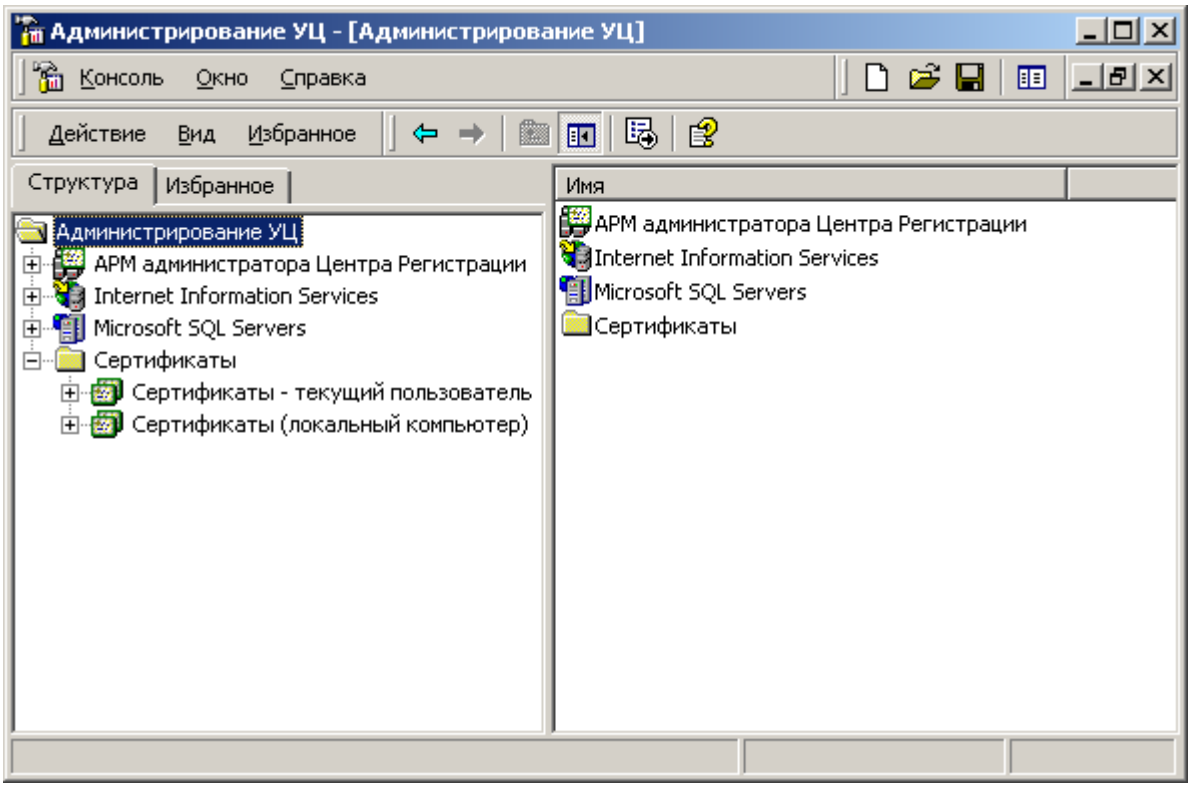
Рисунок 170. Окно консоли управления Консоль1 после добавления нового узла



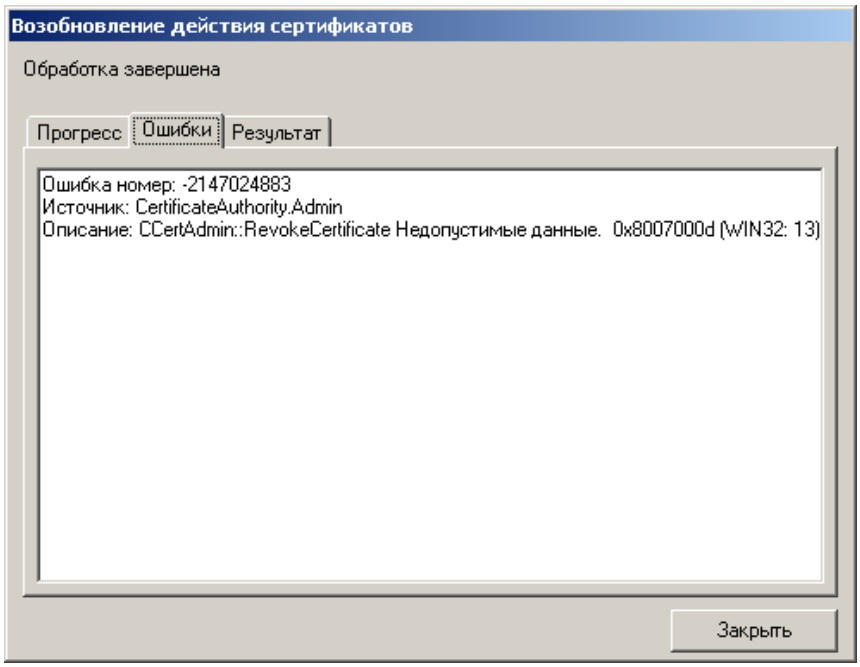
Переименуйте созданный узел с именем **Создать папку** в более удобное и отражающее функциональность наименование **Сертификаты** нажатием правой кнопки мыши и выбором в открывшемся контекстном меню пункта **Переименовать**. Затем сохраните созданную консоль управления в файл **Администрирование УЦ.msc** (например, на рабочем столе своего компьютера).

Теперь созданный файл содержит все необходимые для пользователя компоненты администрирования, организованные и упорядоченные определенным образом, и которые при желании могут быть удалены, либо дополнены новыми административными средствами.

Рисунок 171. Окно консоли Администрирование УЦ



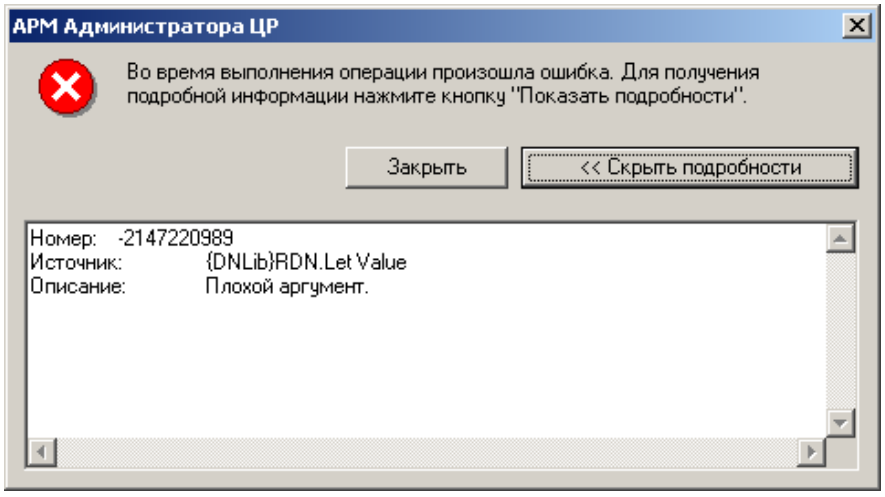
19. Перечень сообщений об ошибках при работе с АРМ администратора



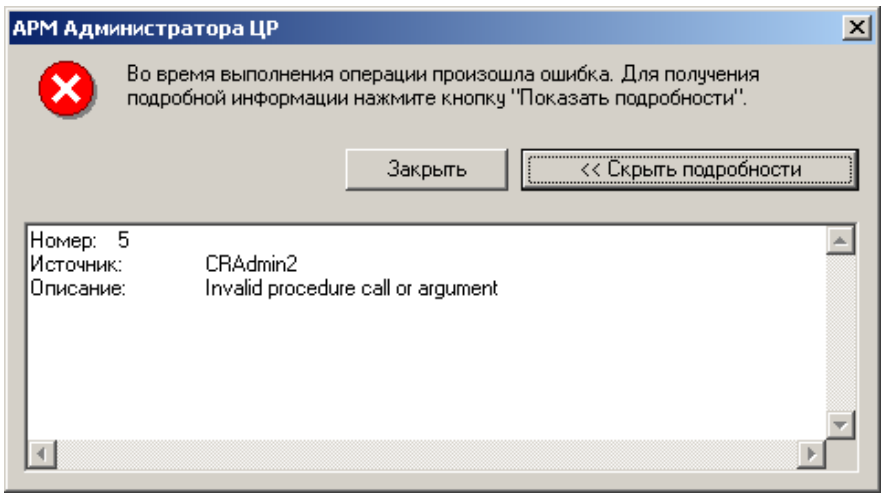
Причина:

а) Возобновление действия сертификата, который уже был отозван;

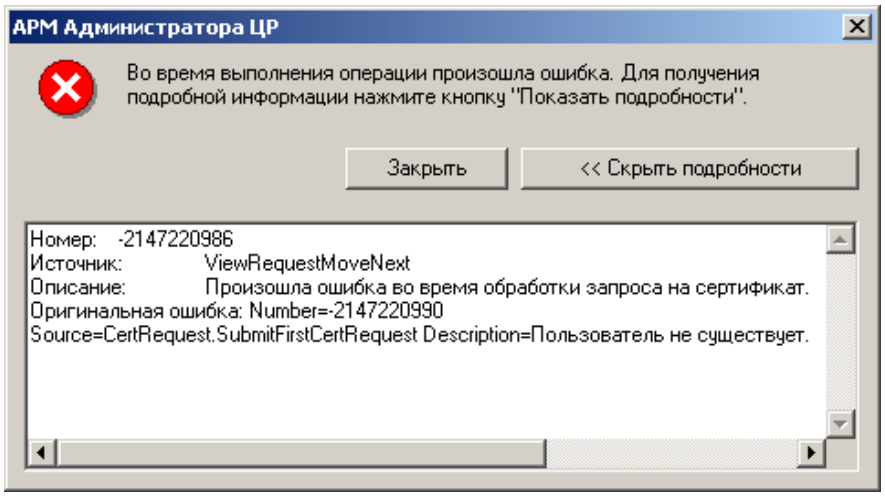
б) Приостановление действие уже отозванного сертификата;



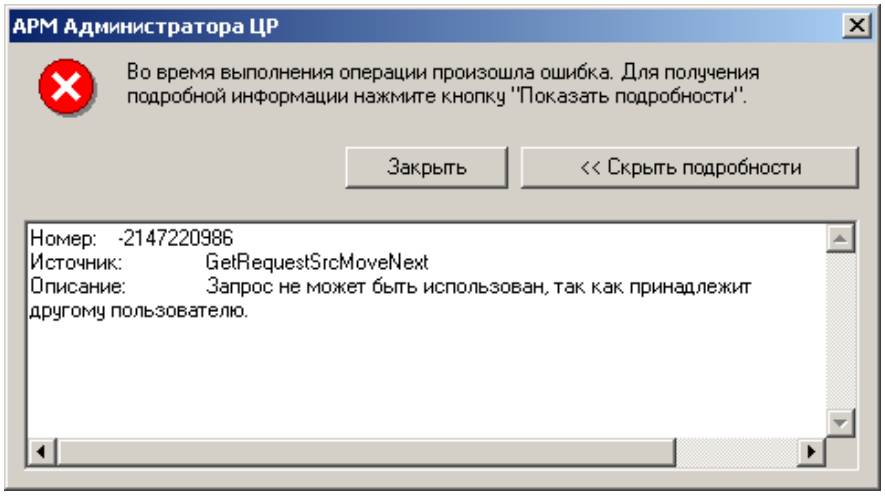
Причина: Недопустимое значение одного из заполненных полей при вводе информации о пользователе.



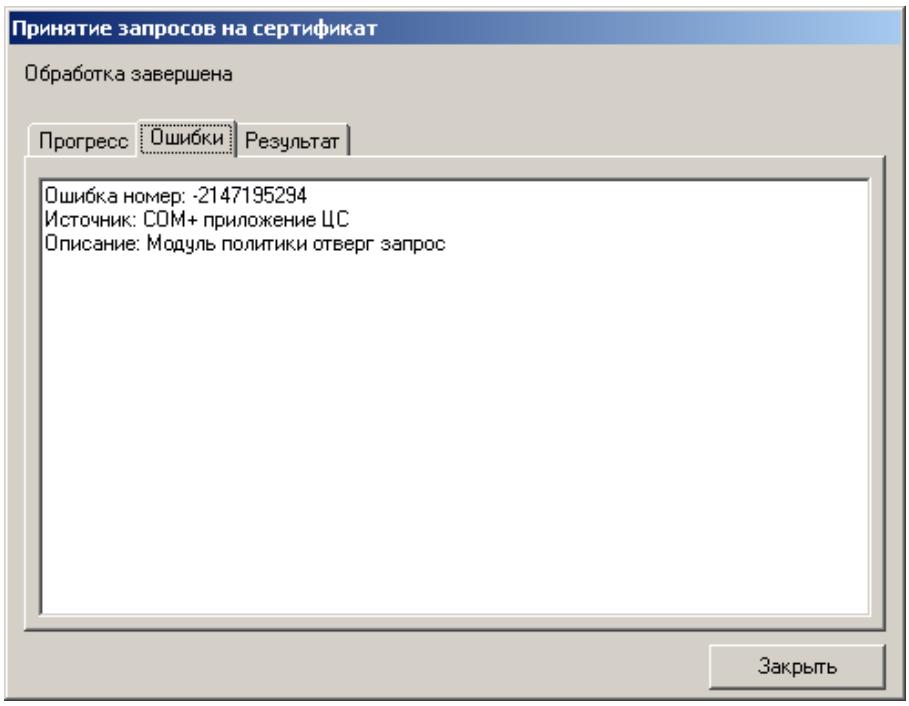
Причина: Недопустимое значение одного из заполненных полей при вводе информации о пользователе.



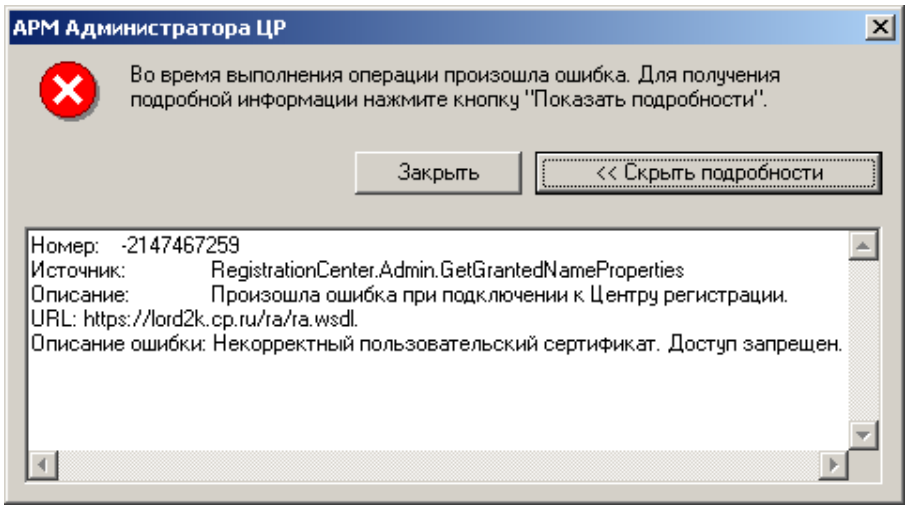
Причина: Недопустимый порядок следования атрибутов DN в запросе на сертификат.



Причина: Несоответствие запроса зарегистрированному пользователю.



Причина: Центр Сертификации отверг запрос на сертификат, как не удовлетворяющий параметрам модуля политики КриптоПро УЦ службы сертификации ЦС. Более подробную информацию смотрите в журнале приложений системного журнала сервера Центра Сертификации, источник CertSvc.



Причина:

а) Владелец сертификата, на котором устанавливается соединение, не зарегистрирован на Центре Регистрации

б) Область применения сертификата, на котором устанавливается соединение, не содержит роль, удовлетворяющую настройкам прав доступа к методам Центра Регистрации.

20. Обеспечение целостности программных средств АРМ администратора ЦР

Система контроля целостности программных компонентов АРМ администратора ЦР основывается на аппаратном контроле целостности программных модулей АРМ администратора ЦР и общесистемного программного обеспечения до загрузки операционной системы.

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

Периодичность контроля целостности программных компонентов АРМ администратора ЦР – ежесуточно. Выполняется путем перезапуска операционной системы компьютера АРМ администратора ЦР.

В состав программных модулей АРМ администратора ЦР, подвергающихся контролю целостности входят:

Для 32-битных ОС:

Наименование модуля	**Расположение (по умолчанию)**
Все файлы каталога	..:\Program Files\Crypto Pro\CRAdmin2
Все файлы каталога	..:\Program Files\Crypto Pro\CRAdmin2\Template
Все файлы *.dll каталога	..:\Program Files\Common Files\Crypto Pro\Shared

Для 64-битных ОС:

Наименование модуля	**Расположение (по умолчанию)**
Все файлы каталога	..:\Program Files (x86)\Crypto Pro\CRAdmin2
Все файлы каталога	..:\Program Files (x86)\Crypto Pro\CRAdmin2\Template
Все файлы *.dll каталога	..:\Program Files (x86)\Common Files\Crypto Pro\Shared

Контроль целостности программных компонентов средств СКЗИ, используемых на АРМ администратора ЦР, осуществляется средствами самого СКЗИ.

21. Удаление программного обеспечения АРМ администратора ЦР

Удаление программного обеспечения АРМ администратора ЦР осуществляется в следующем порядке:

1. Удаление компоненты «КриптоПро УЦ – АРМ администратора ЦР»;
2. Удаление сертификата привилегированного пользователя и соответствующего этому сертификату закрытого ключа - выполняется в том случае, если в дальнейшем нет необходимости их применения, либо срок действия данного закрытого ключа истек;
3. Удаление сертификата Центра Сертификации (уполномоченного лица Удостоверяющего Центра) из соответствующего хранилища доверенных сертификатов Центров Сертификации – выполняется в том случае, если в дальнейшем нет необходимости применения данного сертификата для построения цепочки сертификатов пользователей Удостоверяющего Центра на компьютере АРМ администратора ЦР;
4. Удаление СКЗИ КриптоПро CSP – выполняется в том случае, если в дальнейшем на компьютере АРМ администратора ЦР отсутствует необходимость использования СКЗИ.

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

Удаление сертификата привилегированного пользователя из хранилища сертификатов **Пользователь/Личные** осуществляется с использованием интерфейса консоли **mmc** и изолированной оснастки **Сертификаты**. Удаление закрытого ключа, соответствующего данному сертификату, осуществляется штатными средствами используемого СКЗИ.

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

22. 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 всех возможных 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 также 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.

23. 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

24. Перечень рисунков

25. Перечень ссылочных документов

[X.509]	ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework, June 1997.
[RFC 2459]	RFC 2459. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", January 1999.
[PKCS-7]	RSA Laboratories. *PKCS #7: Cryptographic Message Syntax Standard.* Version 1.5, November 1993.
[PKCS-10]	RSA Laboratories. *PKCS #10:* Certification Request Syntax Standard.

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					