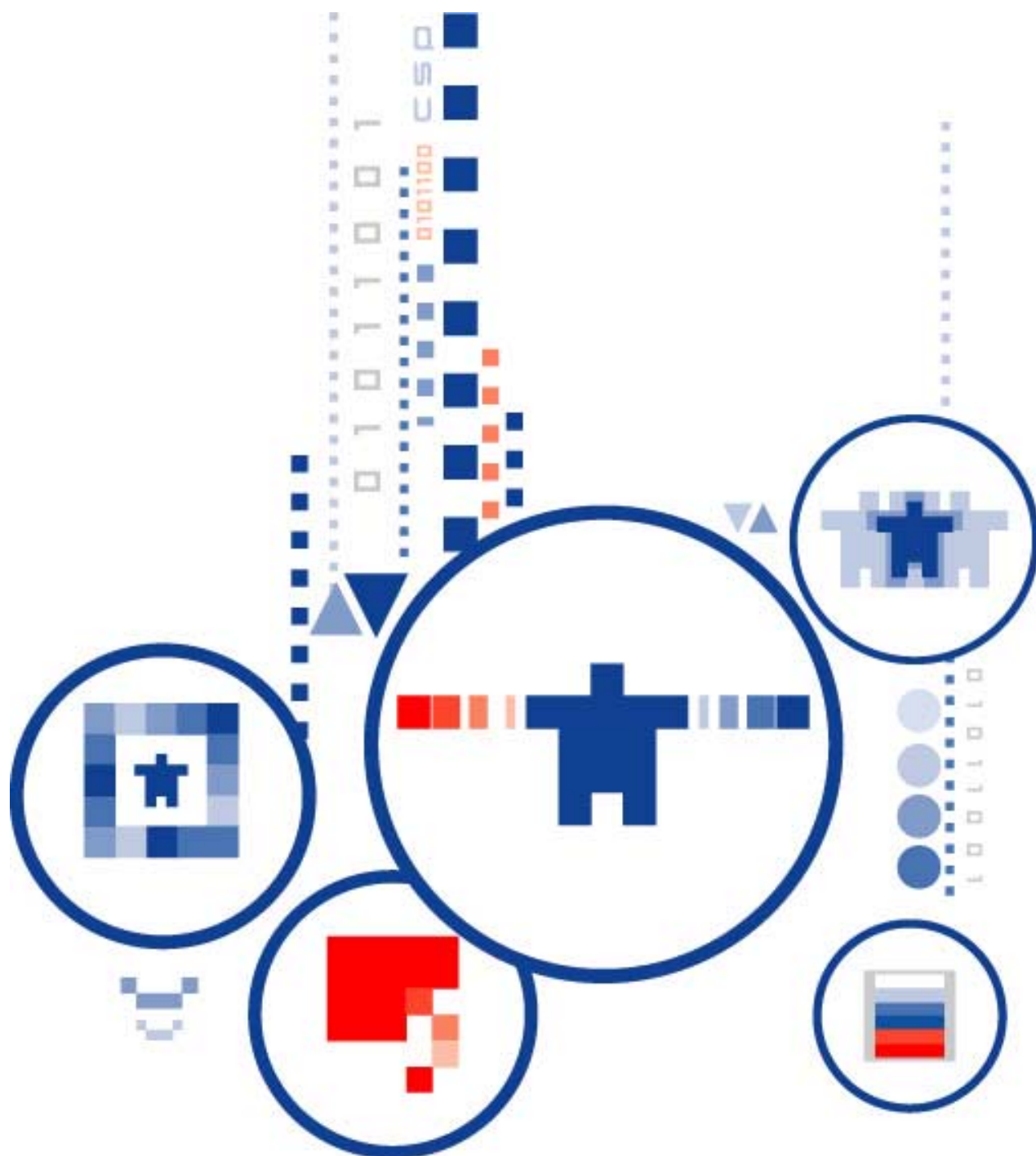




КриптоПро **УЦ**

программно-аппаратный комплекс
удостоверяющий центр

Руководство оператора Удостоверяющего центра
ООО «КРИПТО-ПРО» (срса.cryptopro.ru)

АННОТАЦИЯ

Настоящий документ содержит описание эксплуатации АРМ администратора Центра Регистрации программного комплекса «Удостоверяющий Центр «КриптоПро УЦ» (УЦ), устанавливаемого на рабочем месте Оператора Удостоверяющего Центра ООО «КРИПТО-ПРО»

АРМ администратора является инструментом управления Центром Регистрации, реализованным в виде Microsoft Management Console (MMC), и предназначен для выполнения организационно-технических мероприятий по управлению объектами Центра Регистрации, в соответствии с правами доступа, определенными ролью администратора или оператора.

Данное приложение предназначено для привилегированных пользователей Центра Регистрации (роли администратора и оператора), занимающихся регистрацией пользователей и управлением процессом выдачи сертификатов, и является руководством по эксплуатации программного обеспечения АРМ администратора.

Информация о разработчике ПК «КриптоПро УЦ»:

ООО "Крипто-Про"

127 018, Москва, Улица Образцова, 38

Телефон: (095) 933 1168

Факс: (095) 289 4367

<http://www.CryptoPro.ru>

E-mail: info@CryptoPro.ru

СОДЕРЖАНИЕ

1. Требования для установки и работы с приложением	5
2. Объекты управления	6
2.1. Пользователь.....	6
2.2. Сертификат открытого ключа.....	6
2.3. Запрос на регистрацию	6
2.4. Запрос на сертификат	7
2.5. Запрос на отзыв сертификата	7
3. Установка АРМ Администратора	8
4. Первый запуск и настройка АРМ администратора	13
4.1. Первый запуск приложения АРМ администратора.....	13
4.2. Настройка приложения АРМ администратора	14
4.2.1. Создание запроса на сертификат Оператора ЦР.....	14
4.2.2. Выпуск сертификата Оператора УЦ ООО «КРИПТО-ПРО»	16
4.2.3. Установка сертификата Оператора УЦ	17
4.2.4. Создание подключения ЦР.....	19
4.2.5. Настройка ПО АРМ администратора после подключения к ЦР.....	21
5. Конфигурация ПО АРМ администратора в процессе эксплуатации	25
6. Запуск и интерфейс приложения АРМ администратора	27
6.1. Запуск и активация подключения к ЦР	27
6.2. Просмотр содержимого активированного подключения.....	27
6.3. Контекстное меню папок и содержимого папок	28
6.4. Управление отображением списка в правой части консоли	29
6.5. Сортировка записей в списке консоли	30
6.6. Фильтрация записей в списке консоли	30
6.6.1. Отображение области описания фильтрации записей в списке консоли	30
6.6.2. Фильтрация по типам записей.....	31
6.6.3. Фильтрация по значениям полей записей	32
6.6.4. Фильтрация по подписи запросов на сертификат	33
6.7. Просмотр свойств элементов управления.....	34
6.8. Сохранение сертификата пользователя в файл	37
6.9. Групповые операции над объектами.....	38
7. Смена ключа и сертификата Оператора УЦ.....	40
8. Регистрация пользователей Центра Регистрации	42
8.1. Централизованный режим	42
8.2. Распределенный режим	42
8.3. Мастер регистрации пользователей.....	42
8.3.1. Работа Мастера регистрации пользователя при выборе опции	
генерации запроса на сертификат	43

8.3.2. Работа Мастера регистрации пользователя при выборе опции чтение запроса на сертификат из файла	47
9. Управление ключами и сертификатами пользователей	49
9.1. Генерация ключей и выпуск сертификатов открытых ключей пользователей	49
9.2. Отзыв (аннулирование) сертификатов открытых ключей пользователей.	52
9.3. Приостановление действия сертификатов открытых ключей пользователей	53
9.4. Возобновление действия сертификатов открытых ключей пользователей	54
10. Удаление зарегистрированных пользователей	56
11. Обработка запросов пользователей на Центр Регистрации	58
12. Печать сертификатов пользователей	59
13. Маркер временного доступа	60
13.1. Определение маркера временного доступа.....	60
13.2. Использование маркера временного доступа	60
13.3. Создание маркера временного доступа для зарегистрированного пользователя	60
14. Объекты Центра Сертификации	63
15. Протоколирование работы	65
16. Генерация ключей Центра Сертификации	67
17. Журнал регистрации событий Центра Регистрации	69
17.1. Описание событий, регистрирующихся в Журнале	71
17.2. Работа с Журналом регистрации событий	98
18. Экспорт объектов управления	111
18.1. Экспорт сертификатов открытых ключей подписей	111
18.2. Экспорт запросов на изготовление сертификатов открытых ключей...	115
18.3. Экспорт запросов на отзыв, приостановление и возобновление действия сертификатов открытых ключей подписей	119
19. Использование АРМ администратора ЦР в консоли управления ММС	124
20. Перечень сообщений об ошибках при работе с АРМ администратора	134
21. Перечень терминов	152
22. Перечень сокращений	155
23. Перечень рисунков	156
24. Перечень ссылочных документов	161

1. Требования для установки и работы с приложением

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

- Операционная система Microsoft Windows 2000 (Professional или Server);
- Пакеты обновлений:
 - Microsoft Windows 2000 Service Pack 4
- Программная библиотека CAPICOM.dll версии 2.0.0.1
(<http://www.microsoft.com/downloads/release.asp?ReleaseID=44155>)
- Microsoft MMC Console 1.2;
- Microsoft Internet Explorer 5.0 (и выше);
- Средство криптографической защиты (СКЗИ) КриптоПро CSP;
- Модуль аутентификации КриптоПро CSP (КриптоПро TLS).

Установка на АРМ администратора ЦР другого системного и прикладного программного обеспечения НЕ ДОПУСКАЕТСЯ !

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, соответствующие роли пользователя, запрашивающего методы.

Управление объектами ЦР обеспечиваются администратором и оператором АРМ ЦР с выполнением ими следующих функций:

Администратор АРМ ЦР

- генерация ключей пользователей;
- формирование сертификата открытых ключей пользователей;
- отзыв сертификатов открытых ключей пользователей;
- опубликование списка отозванных сертификатов;
- обработка запросов на сертификаты открытых ключей пользователей;
- обработка запросов на отзыв (приостановление/возобновление действия) сертификатов открытых ключей пользователей.

Оператор АРМ ЦР

- регистрация пользователей в Базе Данных Центра Регистрации;
- генерация служебных ключей пользователей в процессе выполнения процедуры регистрации пользователей;
- обработка запросов на регистрацию пользователей.

2.1. Пользователь

Пользователь — субъект прикладной системы, использующий УЦ. Пользователем УЦ является физическое лицо, которое может представлять юридическое лицо.

2.2. Сертификат открытого ключа

Сертификат — цифровой документ, который содержит открытый ключ пользователя и подписан электронной цифровой подписью его издателя, т.е. Удостоверяющего центра. 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.

Состояния объекта:

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

2.3. Запрос на регистрацию

Запрос на регистрацию — сообщение, содержащее необходимую информацию для регистрации пользователя в УЦ. Формируется при регистрации пользователя по сети. Передается по сети в Центр регистрации. Обработка осуществляется Администратором со своего рабочего места. Результатом обработки является формирование учетной записи пользователя в Базе Данных Центра регистрации или сообщение об ошибке.

Состояния объекта:

- поступивший – запрос поступил во входную очередь ЦР на обработку администратором;
- принятый – запрос из входной очереди ЦР обработан администратором и принят к обработке ЦР;
- отвергнутый – запрос из входной очереди ЦР обработан администратором и отклонен;
- обработанный – принятый запрос обработан ЦР.

2.4. Запрос на сертификат

Запрос на сертификат — сообщение, содержащее необходимую информацию для получения сертификата. Формируется в АРМ Пользователя или в АРМ Администратора, после чего передается через Центр регистрации в Центр сертификации УЦ, где и обрабатывается. Результатом обработки является выпущенный сертификат или сообщение об ошибке.

Состояния объекта:

- поступивший – запрос поступил во входную очередь ЦР на обработку администратором;
- принятый – запрос из входной очереди ЦР обработан администратором и поступил в выходную очередь ЦР на обработку в Центр Сертификации;
- отвергнутый – запрос из входной очереди ЦР обработан администратором и отклонен;
- удовлетворенный – запрос обработан Центром Сертификации, сертификат по запросу выпущен, но сертификат на рабочем месте пользователя не установлен;
- обработанный – запрос обработан Центром Сертификации, сертификат по запросу выпущен, сертификат на рабочем месте пользователя установлен (сертификат доставлен).

2.5. Запрос на отзыв сертификата

Запрос на отзыв сертификата — сообщение, содержащее необходимую информацию для выполнения процедуры отзыва, приостановления или возобновления действия сертификата пользователя из обращения в системе. Формируется на АРМ Пользователя или на АРМ Администратора, после чего передается через Центр регистрации Центру сертификации УЦ, где и обрабатывается. Результатом обработки является занесение сертификата в список отозванных сертификатов или сообщение об ошибке.

Состояния объекта:

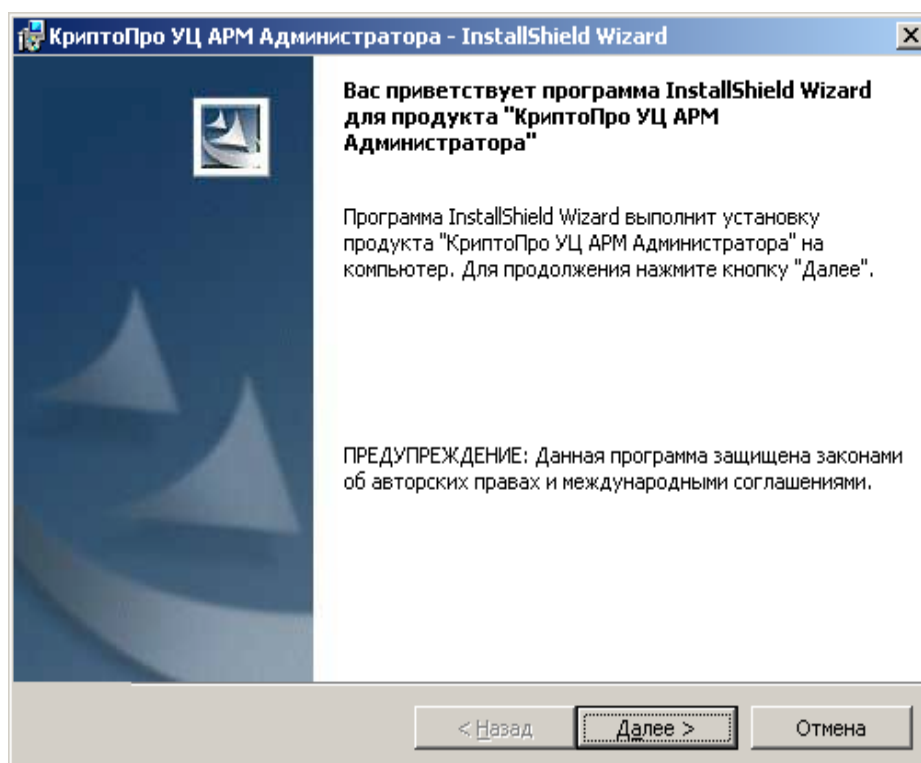
- поступивший – запрос поступил во входную очередь ЦР на обработку администратором;
- принятый – запрос из входной очереди ЦР обработан администратором и поступил в выходную очередь ЦР на обработку в Центр Сертификации;
- отклоненный – запрос из входной очереди ЦР обработан администратором и отклонен;
- обработанный – запрос обработан Центром Сертификации, сертификат по запросу отозван.

3. Установка АРМ Администратора

Для установки ПО АРМ Администратора необходимо выполнить программу установки **SETUP.EXE**, расположенную в каталоге носителя дистрибутива ПО АРМ Администратора.

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.

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

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

КриптоПро УЦ АРМ Администратора - InstallShield Wizard

Сведения о пользователе
Укажите сведения о себе.

Пользователь:
Администратор

Организация:
Крипто-Про

Серийный номер:
CR130 - 00010 - 00000 - -

InstallShield

< Назад Далее > Отмена

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

КриптоПро УЦ АРМ Администратора - InstallShield Wizard

Вид установки
Выбор наиболее подходящего вида установки.

Выберите вид установки.

☒ **Полная**
Будут установлены все компоненты программы. (Требуется больше всего места на диске.)

☐ **Выборочная**
Выбор необходимых компонентов программы и папки, в которой они будут установлены. Рассчитана на опытных пользователей.

InstallShield

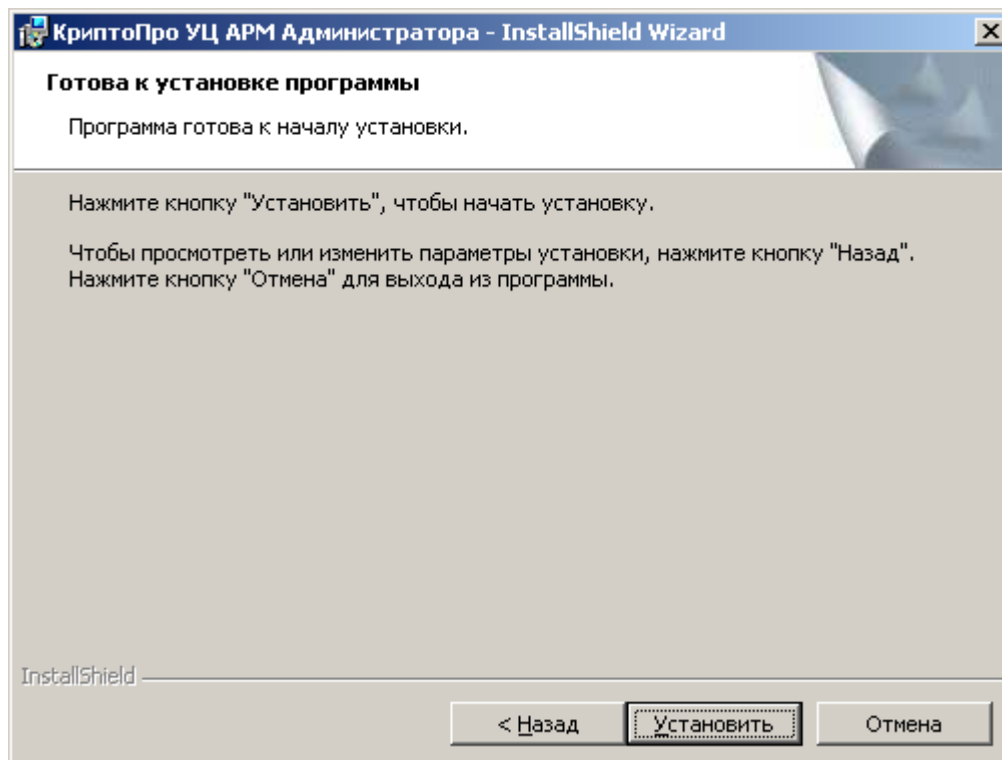
< Назад Далее > Отмена

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 иницируется собственно операция установки (см. Рисунок 4).

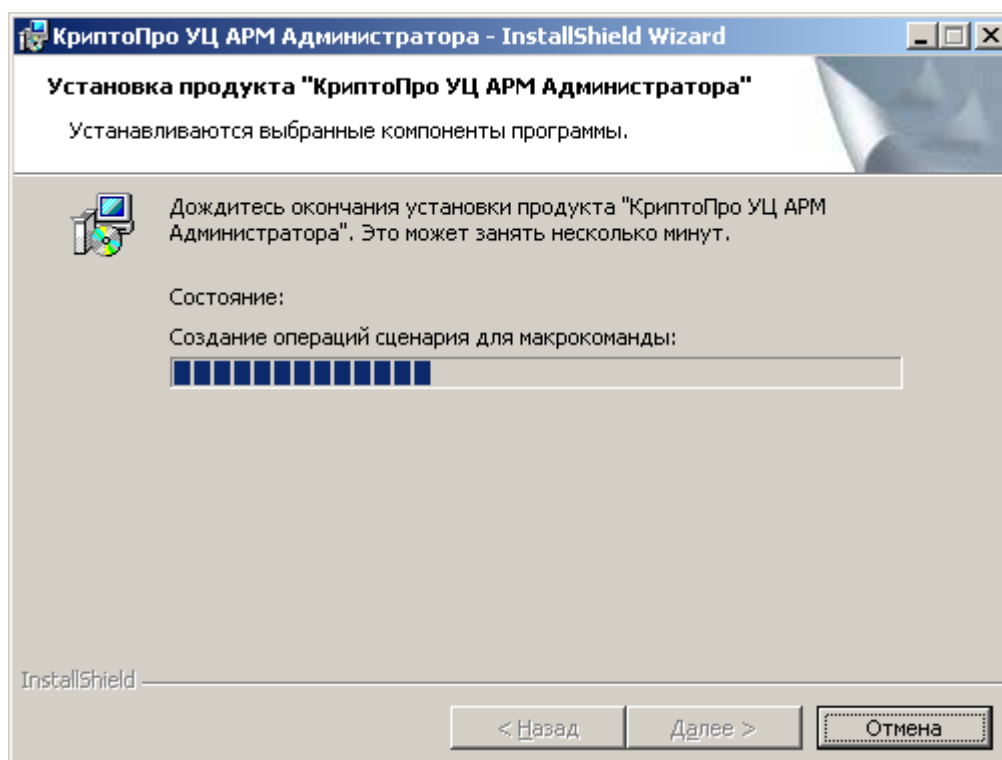
Рисунок 4. Окно подтверждения установки ПО Мастера установки АРМ администратора



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

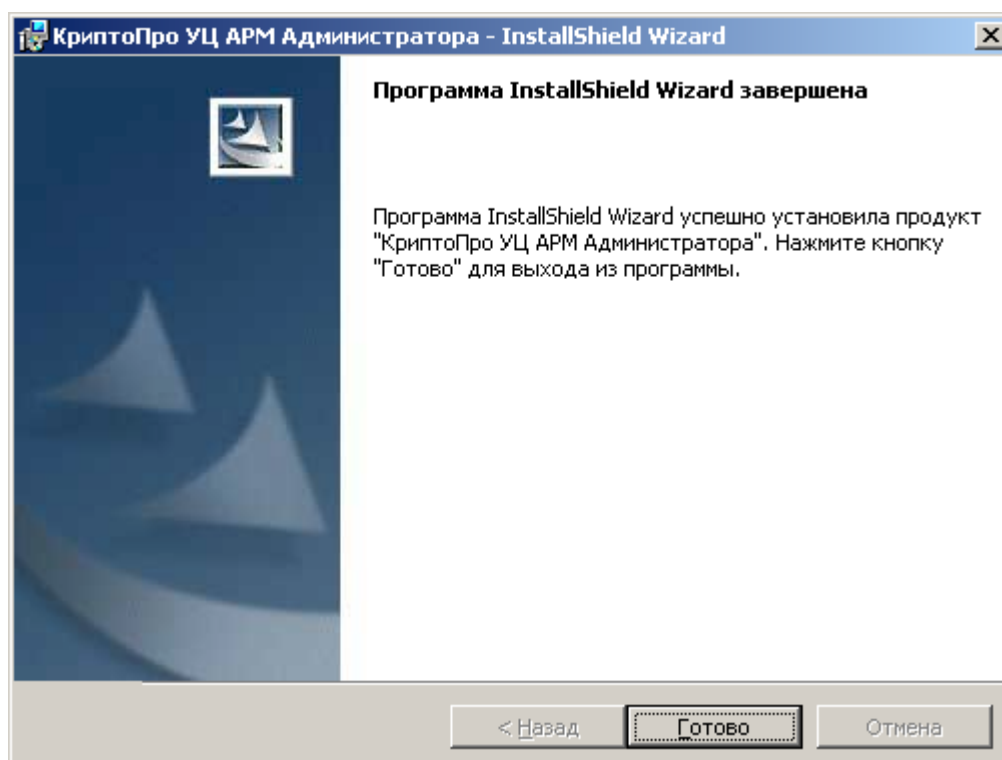
При выполнении операций установки, состояние процесса отображается в окне на экране.

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. В противном случае обратитесь в службу технической поддержки.

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

В ходе выполнения программы производится установка следующих компонент:

- Компоненты SOAP-интерфейса взаимодействия с ЦР.
- MMC консоль АРМ администратора в директорию **Program Files\Crypto Pro\CRAAdmin\CRAAdmin.msc.**
- Snap-in MMC консоли АРМ "АРМ Администратора ЦР" в директорию **Program Files\Crypto Pro\CRAAdmin\CRAAdmin.dll,**

4. Первый запуск и настройка АРМ администратора

4.1. Первый запуск приложения АРМ администратора

АРМ администратора является приложением, разработанным с использованием Microsoft Management Console и использует все основные средства управления, предлагаемые MMC.

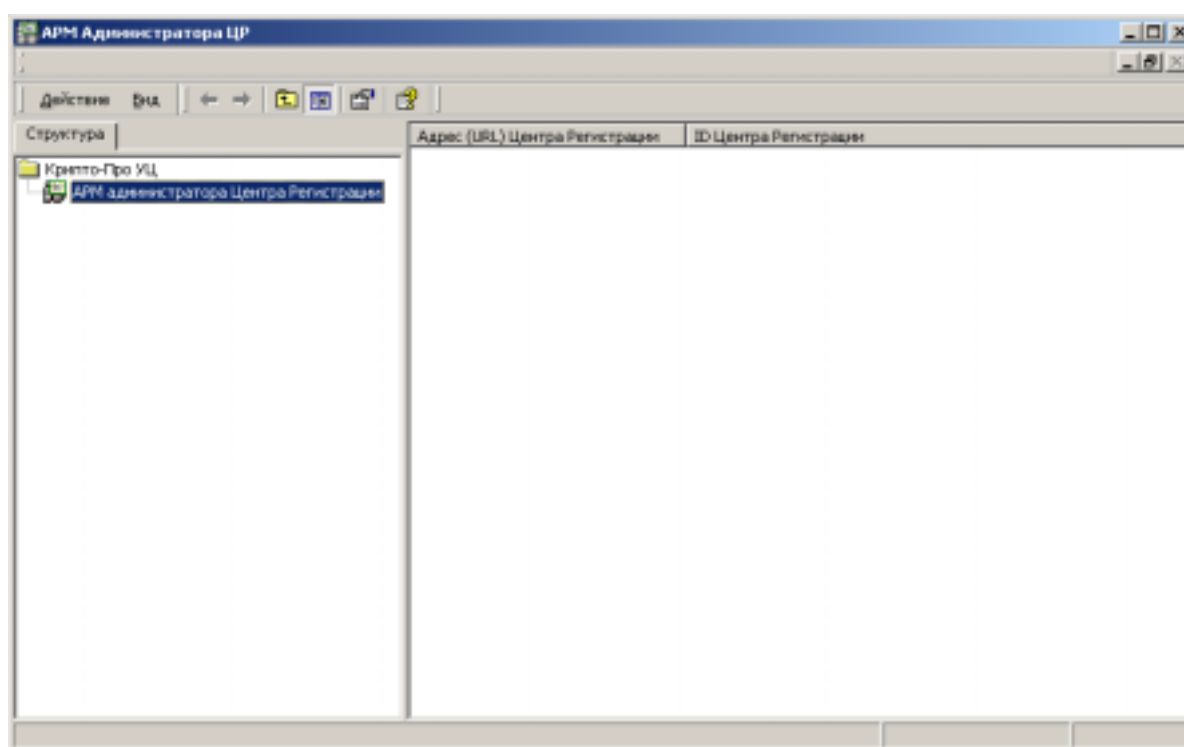
АРМ администратора может быть использован в интегрированной среде совместно с другими приложениями администрирования такими, как Microsoft SQL Server Enterprise Manager, Microsoft Internet Information Server Manager и пр.

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

Консоль MMC АРМ администратора при запуске и в процессе работы настраивается пользователем и сохраняет свои настройки при выполнении на следующих сеансах работы. Данное приложение доступно для запуска всем пользователям локального компьютера, но имеет разделение по настройкам. Т.е. при запуске его пользователем настройки консоли, сформированными другими пользователями, ему доступны не будут.

АРМ администратора имеет стандартный интерфейс приложения Windows (см. Рисунок 7).

Рисунок 7. Внешний вид приложения АРМ администратора .



Консоль **АРМ администратора** имеет две панели. На левой панели расположено дерево, определяющее иерархию объектов, с которыми работает АРМ. Правая панель отображает содержимое объекта, выделенного на левой панели. Все действия, которые можно выполнить над объектами, доступны через контекстные меню. Контекстные меню вызываются щелчком правой клавиши мыши на объекте, к которому применяется действие.

4.2. Настройка приложения АРМ администратора

АРМ администратора Центра Регистрации предназначено для работы привилегированных пользователей Удостоверяющего центра – Администратора и Оператора. Действия по настройке приложения АРМ администратора совпадают как для Администратора, так и для Оператора, поэтому дальнейшее описание процесса настройки будет осуществляться применительно к Администратору.

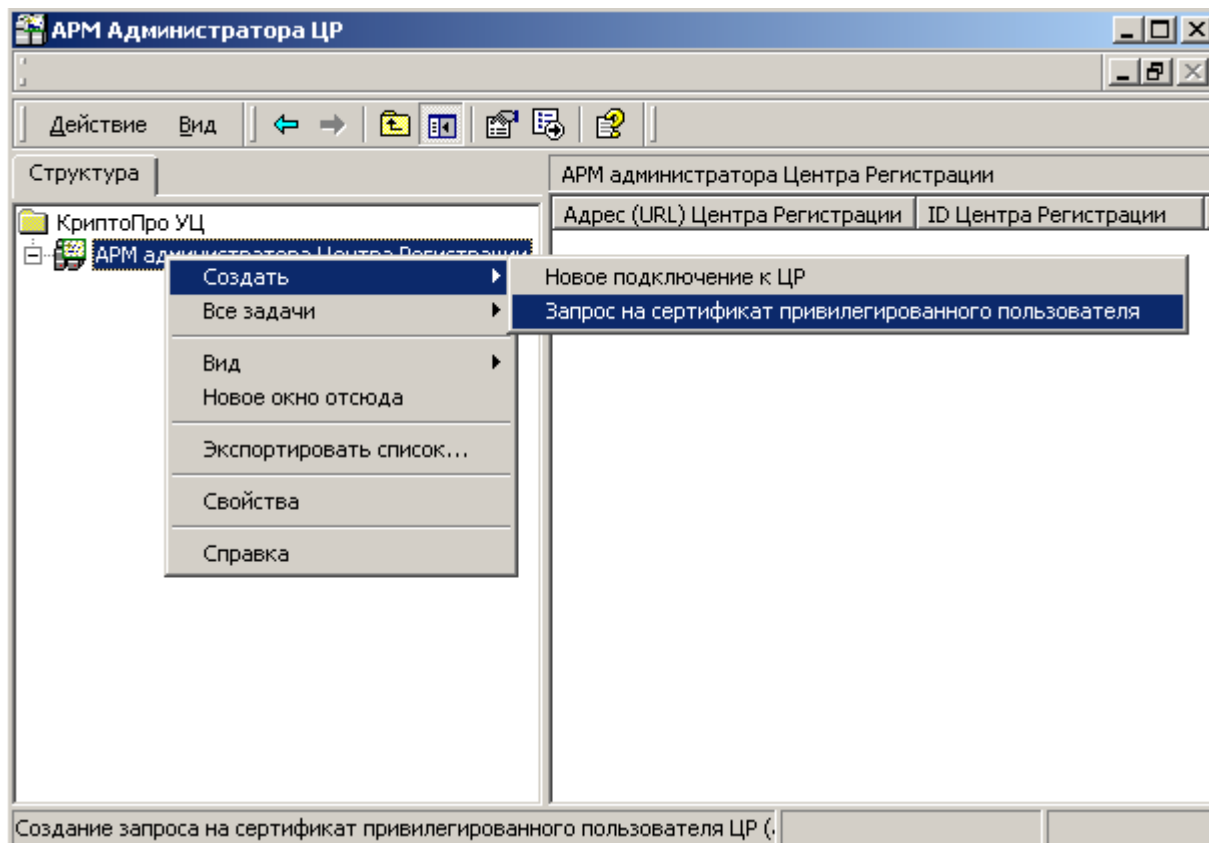
При первом запуске **АРМ администратора**, если у администратора не существует личного сертификата открытого ключа, необходимо выполнить следующие регламентные процедуры:

- создать запрос на сертификат администратора ЦР. Данное действие производится на рабочем месте администратора ЦР с использованием программного обеспечения АРМ.
- выпустить сертификат администратора ЦР. Данное действие производится на сервере ЦР в соответствии с документом КриптоПро УЦ ЦР. Руководство по эксплуатации.
- установить сертификат администратора ЦР. Установка сертификата выполняется на рабочем месте администратора ЦР с использованием программного обеспечения АРМ.
- создать подключение к ЦР. Создание подключения к ЦР выполняется на рабочем месте администратора ЦР с использованием программного обеспечения АРМ.

4.2.1. Создание запроса на сертификат Оператора ЦР

Создание запроса на сертификат Оператора ЦР осуществляется путем выполнения задачи **Создать/Запрос на сертификат привилегированного пользователя** (см. Рисунок 8).

Рисунок 8. Запуск задачи создания запроса на сертификат привилегированного пользователя



В диалоге **Мастера создания запроса на сертификат администратора** в первом окне ввода информации, отображаемого после окна приветствия Мастера, (см.

Рисунок 9) предоставляется возможность установки параметров генерируемых ключей. К этим параметрам относятся:

- Наименование криптопровайдера (CSP), определяющего алгоритм генерации ключей администратора;
- Размер ключа;
- Алгоритм хеширования;
- Режим усиленной защиты ключа (для криптопровайдеров, поддерживающих данный флаг). При установке данного режима каждая попытка обращения к закрытому ключу фиксируется системой, о чем пользователь будет получать соответствующее уведомление;
- Флаг (признак) возможности экспорта ключей (для криптопровайдеров, поддерживающих данный флаг). Флаг возможности экспорта ключей установится на создаваемый ключевой контейнер. При использовании СКЗИ КриптоПро CSP, установка данного флага обеспечит возможность копирования ключевого контейнера с помощью сервисных функций СКЗИ КриптоПро CSP. Установка данного флага рекомендуется.

Рисунок 9. Окно определения параметров ключа Мастера создания запроса на сертификат администратора

Мастер создания запроса на сертификат администратора

Параметры ключа
Установите параметры ключа

Выберите криптопровайдер из приведенного списка. Укажите требуемый размер ключа и алгоритм хеширования.

CSP
Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider

Размер ключа
512
Мин: 512
Макс: 512

Алгоритм хеширования
GOST R 34.11-94

☐ Включить усиленную защиту закрытого ключа
☒ Пометить ключи как экспортируемые

< Назад Далее > Отмена



Приведенное выше окно отображается только в том случае, если в окне свойств АРМ администратора Центра Регистрации (см. Рисунок 20) установлена опция **Разрешить выбор CSP**. Данная опция включена по умолчанию.

В следующем окне Мастера создания запроса на сертификат администратора необходимо ввести информацию о пользователе (см. Рисунок 10). Перечень полей, обязательных для заполнения, необходимо получить с Центра Регистрации. В противном случае запрос на сертификат при обработке на Центре Сертификации будет отвергнут.

Группа выбора **Роль** определяет, значение области определения, заносимую в сертификат открытого ключа, которая позволяет аутентифицироваться с соответствующей

Руководство оператора Удостоверяющего центра ООО «КРИПТО-ПРО» (срса.cryptopro.ru)
ролью: администратор или оператор. Установите переключатель **Роль** в положение **Оператор**.

Рисунок 10. Окно ввода информации об администраторе Мастера создания запроса на сертификат администратора.

The screenshot shows a window titled "Мастер создания запроса на сертификат администратора". The main heading is "Ввод информации о пользователе". Below it, a note says: "Введите информацию о пользователе системы. Необходимые для заполнения поля помечены красным цветом." The form contains several fields: "Фамилия Имя Отчество:" (highlighted in red), "Подразделение:", "E-Mail:", "Субъект федерации", "Организация:", "Город", and "Страна:" (with a dropdown menu showing "RU"). There is a "Роль" section with two radio buttons: "Администратор" and "Оператор" (which is selected). At the bottom, there is a note: "Введите информацию и нажмите кнопку 'Далее' для продолжения." and three buttons: "< Назад", "Далее >", and "Отмена".

В следующем окне Мастера необходимо выбрать имя файла, в который будет записан запрос на сертификат. Переключатель **Формат файла запроса** установите в положение **Файлы в Base64-кодировке PKCS#10 с заголовком**

Рисунок 11. Сохранение запроса на сертификат

The screenshot shows the same window, but the heading is "Файл запроса на сертификат". The note says: "Укажите имя файла, в котором будет сохранен запрос на сертификат." Below this, there is a text field with "f:\admin.p10" and a button "Обзор...". There is a section "Формат файла запроса" with three radio buttons: "Файлы в Base64-кодировке PKCS#10 с заголовком" (selected), "Файлы в Base64-кодировке PKCS#10 без заголовка", and "Файл в бинарном виде". At the bottom, there is a note: "При нажатии на кнопку 'Далее' будет сгенерирован запрос." and the same three navigation buttons: "< Назад", "Далее >", and "Отмена".

После формирования ключа и запроса на сертификат данный запрос будет сохранен в файл на диске с указанным именем и в указанном формате.

4.2.2. Выпуск сертификата Оператора УЦ ООО «КРИПТО-ПРО»

Для выпуска сертификата необходимо выполнить следующие действия:

- В адрес Администратора Удостоверяющего центра ООО «КРИПТО-ПРО» - срса@cryptopro.ru направить следующее почтовое сообщение: «Тема письма» - Запрос на изготовление сертификата Оператора УЦ; «Тело письма» - Прошу изготовить сертификат ключа подписи Оператора УЦ ООО «КРИПТО-ПРО» на основании прилагаемого в данном сообщении запроса на сертификат и направленного в адрес УЦ ООО «КРИПТО-ПРО» Заявления на изготовление сертификата ключа подписи в бумажном виде; «Вложение» - сформированный файл запроса на сертификат ключа подписи Оператора УЦ ООО «КРИПТО-ПРО».
- Оформить надлежащим образом в соответствии с Регламентом УЦ Доверенность Оператора УЦ, Заявление на регистрацию Оператора УЦ и Заявление на изготовление сертификата ключа подписи Оператора УЦ (с распечатанным файлом запроса на сертификат) и направить указанные документы в адрес Удостоверяющего центра ООО «КРИПТО-ПРО».

В целях ускорения процедуры регистрации и изготовления сертификата Оператора УЦ допускается предоставление копий указанных документов по факсу в Удостоверяющий центр ООО «КРИПТО-ПРО», с последующим обязательным предоставлением данных документов. Данная процедура производится исключительно по согласованию с Администратором Удостоверяющего центра.

В том случае, если оригиналы регистрационных документов не будут предоставлены в Удостоверяющий центр ООО «КРИПТО-ПРО» в течение 14 календарных дней с момента изготовления сертификата Оператора УЦ Удостоверяющий центр приостанавливает действие сертификата Оператора УЦ.

- После изготовления сертификата Оператора УЦ, получить от Удостоверяющего центра следующие данные:
 - о Файл с сертификатом Оператора УЦ;
 - о Файл с сертификатом Центра Сертификации (цепочкой сертификатов в случае иерархической модели Удостоверяющего Центра);

4.2.3. Установка сертификата Оператора УЦ

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

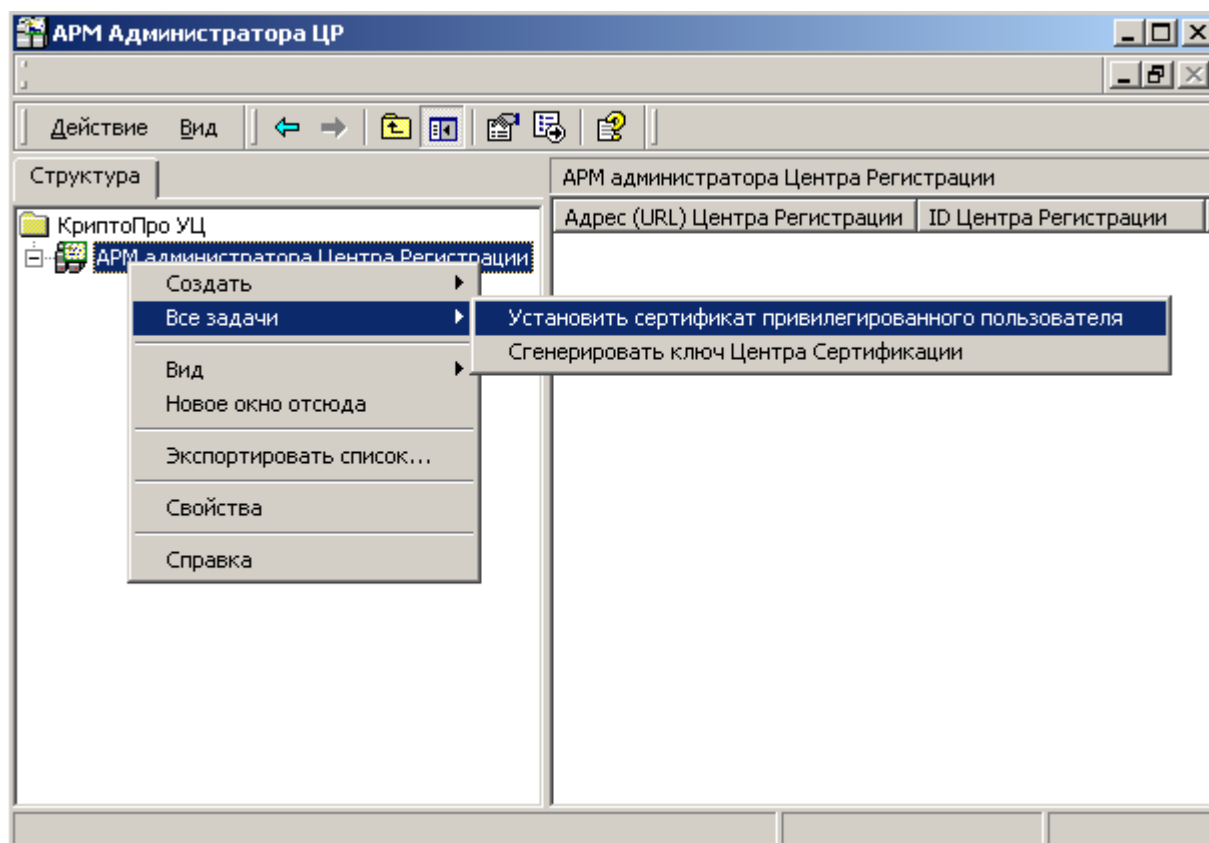
- Установить в список доверенных ЦС хранилища сертификатов текущего пользователя полученный сертификат Центра Сертификации.



В том случае, если изготовленный сертификат Оператора УЦ, сертификат центра Сертификации предоставляются Удостоверяющим центром в виде одного файла с расширением .p7b, программное обеспечение АРМ администратора автоматически произведет их установку на ПЭВМ.

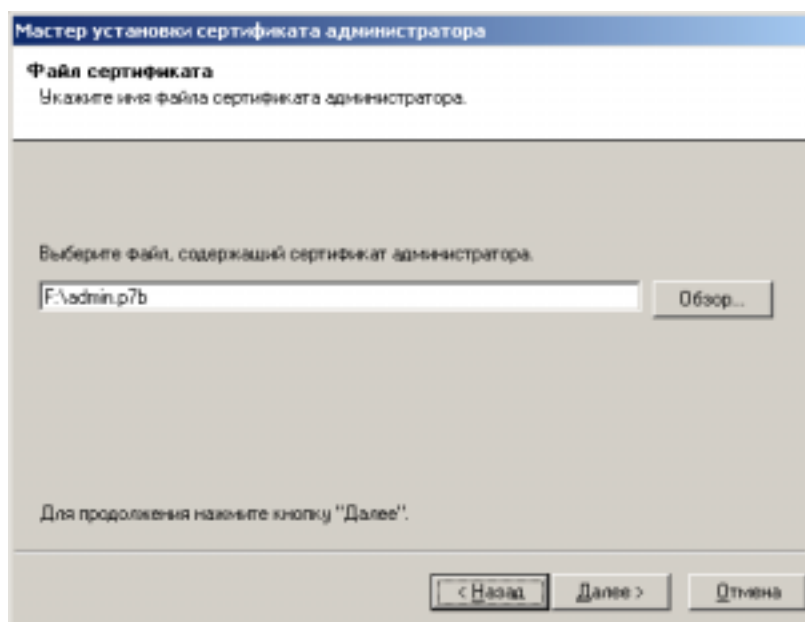
Для установки выпущенного сертификата на рабочем месте Администратора ЦР выполните задачу **Установить сертификат привилегированного пользователя** (см. Рисунок 12).

Рисунок 12. Запуск задачи установки сертификата привилегированного пользователя



В процессе установки, укажите файл, полученный с Удостоверяющего центра и содержащий сертификат Оператора УЦ (см. Рисунок 13).

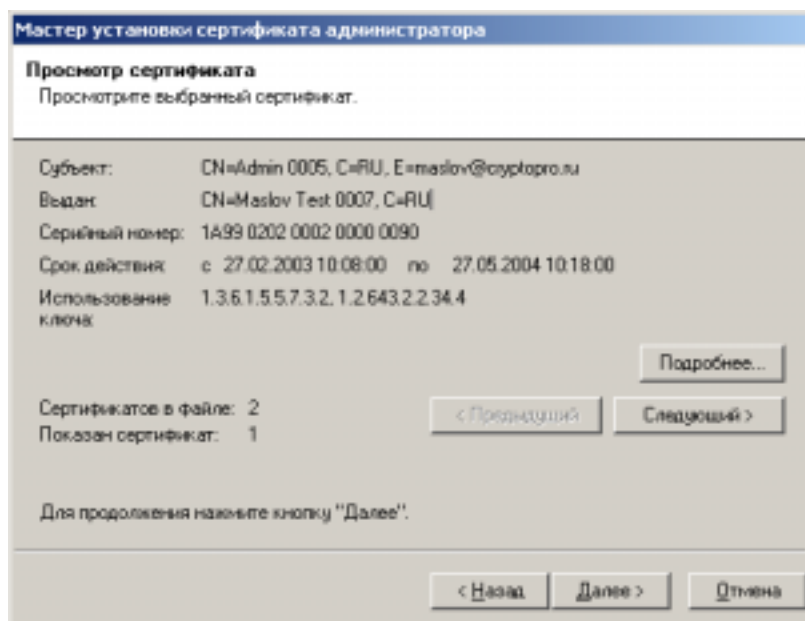
Рисунок 13. Окно выбора файла с сертификатом Мастера установки сертификата администратора



В следующем окне Мастера установки сертификата администратора убедитесь в том, что устанавливается сертификат, соответствующий запросу (см. Рисунок 14) Для просмотра сертификата(ов) издателя(ей) (сертификата(ов) Центра Сертификации) используются кнопки **Следующий >** и **< Предыдущий**, а также кнопка **Подробнее** для детализации информации о текущем сертификате в цепочке сертификатов.

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

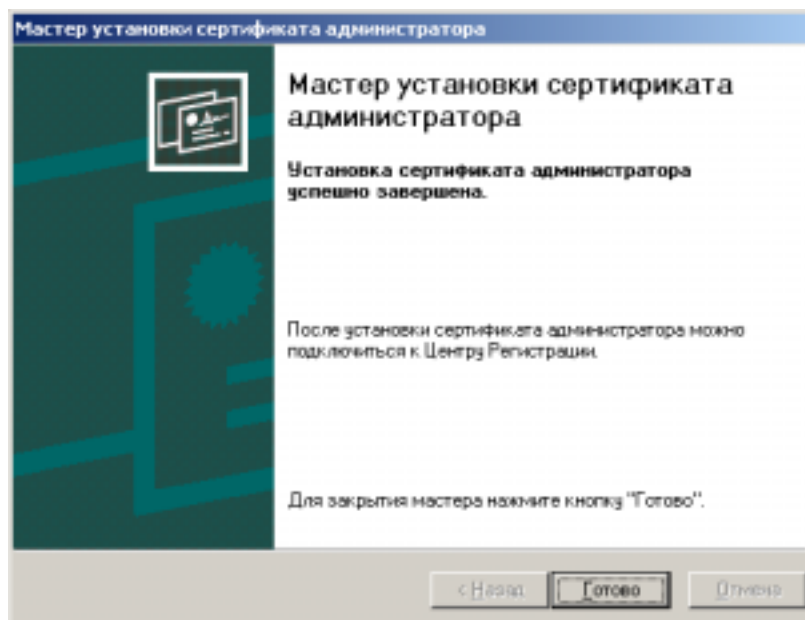
Рисунок 14. Окно просмотра сертификата Мастера установки сертификата администратора



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

Об успешном завершении записи сертификата на рабочее место свидетельствует появление окна Мастера (см. Рисунок 15).

Рисунок 15. Окно завершения установки сертификата администратора

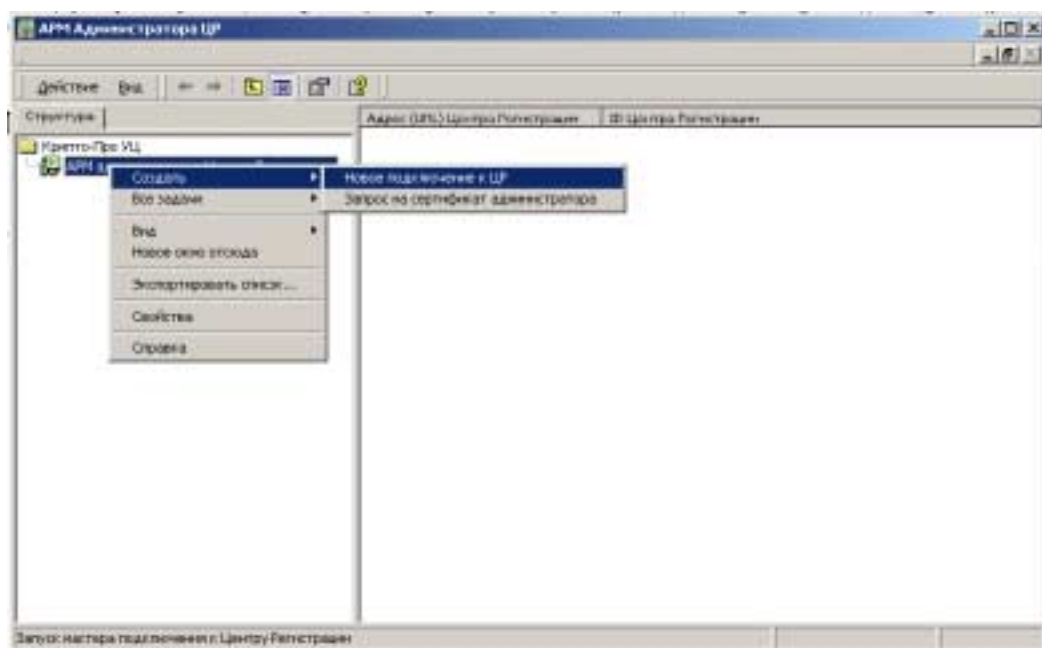


В противном случае, будет выдано соответствующее диагностическое окно Мастера с сообщением об ошибке.

4.2.4. Создание подключения ЦР

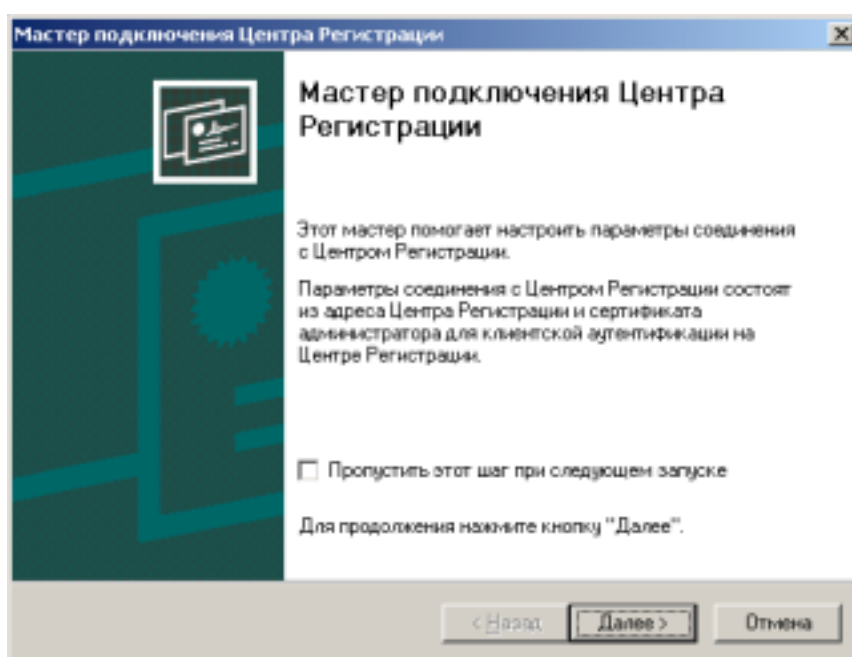
После выполнения установки сертификата необходимо перейти к созданию подключения к ЦР. Для этого необходимо запустить на выполнение задачу **Новое подключение к ЦР** (см. Рисунок 16).

Рисунок 16. Запуск задачи создания подключения к ЦР



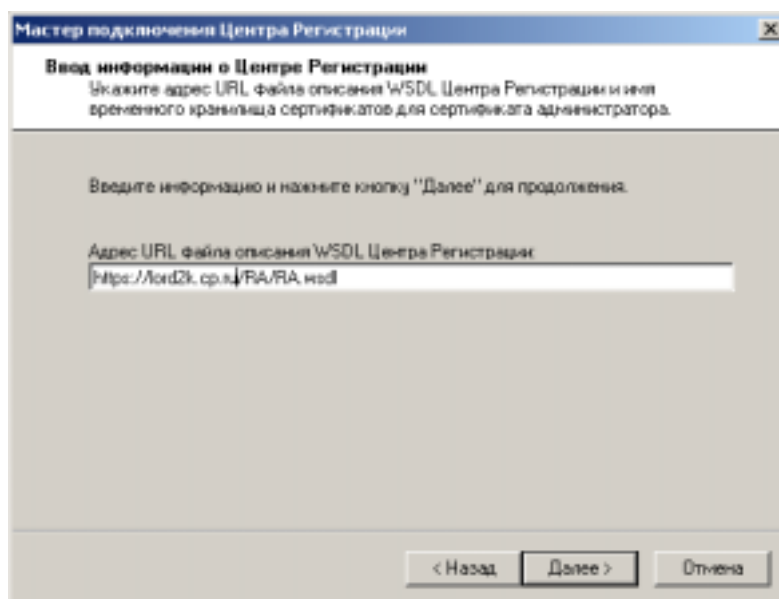
Создание подключения осуществляется с помощью Мастера подключения к ЦР (см. Рисунок 17).

Рисунок 17. Мастер подключения к ЦР



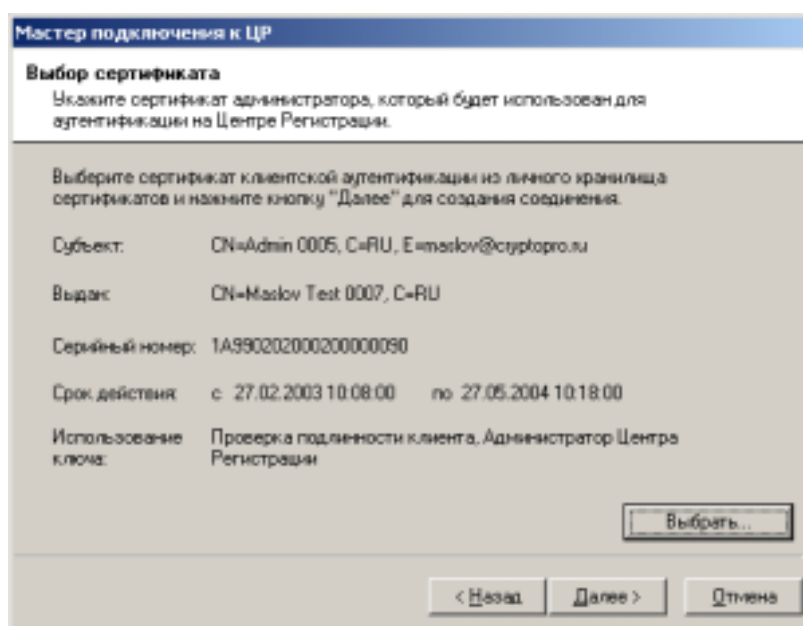
В ходе подключения необходимо ввести URL Web-сервиса Центра регистрации (файла RA.WSDL), с которым будет работать APM - данный URL указывается в Регламенте УЦ (см. Рисунок 18).

Рисунок 18. Задание адреса ЦР в Мастере подключения к ЦР



В следующем окне Мастера необходимо выбрать сертификат Оператора УЦ (см. Рисунок 19). Для выбора сертификата Оператора нажмите кнопку **Выбрать**.

Рисунок 19. Выбор сертификата администратора в Мастере подключения к ЦР



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

4.2.5. Настройка ПО АРМ администратора после подключения к ЦР

После завершения создания подключения необходимо произвести настройку ПО АРМ администратора.

Настройка ПО АРМ администратора заключается в определении следующих параметров:

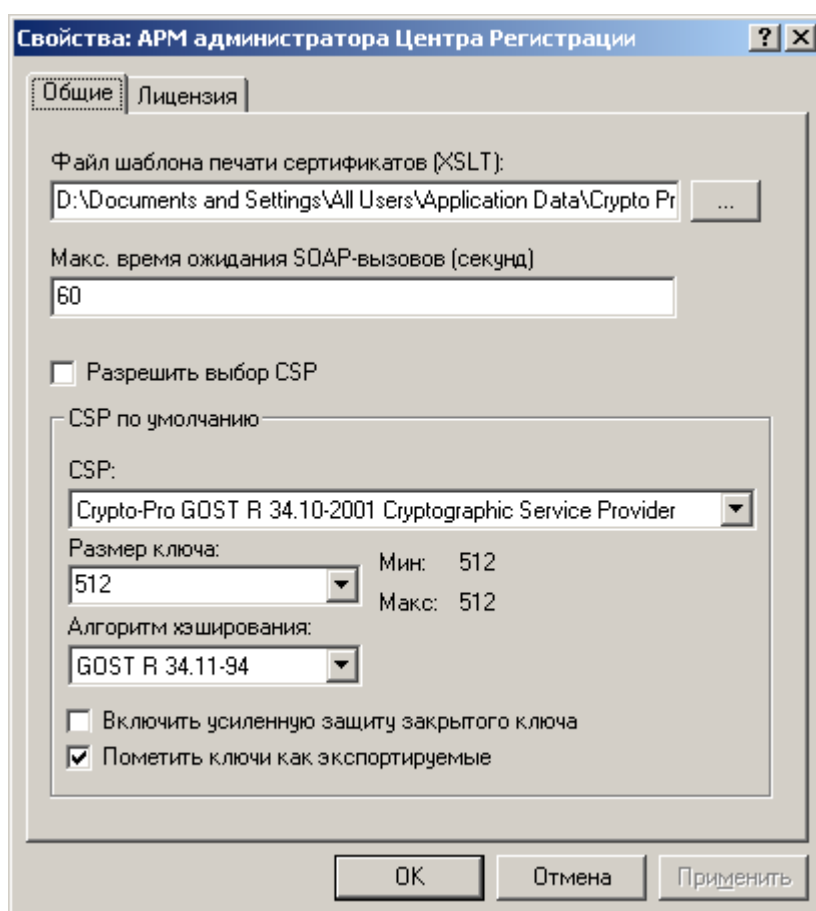
- Имя и расположение XSL-файла, содержащего шаблон для печати сертификата;
- Максимальное время ожидания SOAP-вызовов (устанавливается в секундах)
- Разрешить выбор CSP. При установке данного флага при генерации ключей привилегированный пользователь сможет изменить настроенный по умолчанию криптопровайдер и использовать любой другой, установленный на ПЭВМ АРМ Администратора ЦР. При снятии данного флага будет использоваться криптопровайдер, настроенный по умолчанию.
- Настройка CSP по умолчанию. При генерации ключей в соответствующих диалоговых окнах АРМ Администратора ЦР по умолчанию будет устанавливаться указанный в настоящей настройке криптопровайдер.

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.

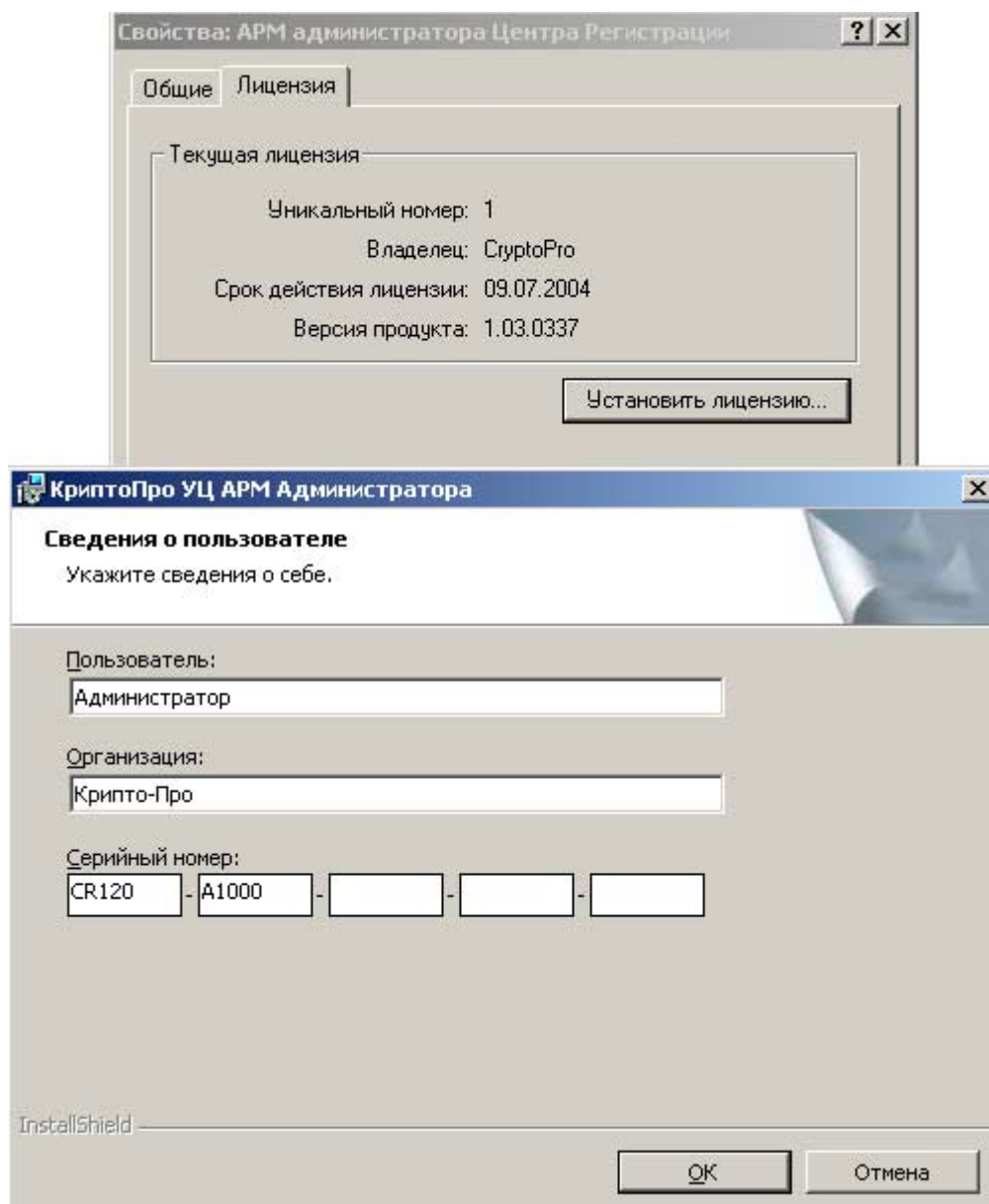
Изменение параметров осуществляется в окне свойств АРМ администратора (вкладка Общие), доступного из выпадающего контекстного меню при щелчке правой кнопки мыши на узле **АРМ администратора Центра Регистрации** (см. Рисунок 20).

Рисунок 20. Окно свойств АРМ администратора



В том случае, если при установке ПО АРМ Администратора ЦР процедура ввода серийного номера лицензии была опущена, или требуется замены 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 20а)

Рисунок 20а. Ввод наименования организации и серийного номера лицензии



5. Конфигурация ПО АРМ администратора в процессе эксплуатации

В процессе эксплуатации программного обеспечения АРМ администратора доступно изменение настроек АРМ Администратора.

Процедура конфигурации параметров настроек АРМ администратора необходима в следующих случаях:

- смена ключей и сертификата администратора, с помощью которого будет аутентифицироваться администратор;
- смена файла-шаблона печати сертификата или изменения его местонахождения;
- смена доменного имени или расположения в сети сервера Центра Регистрации.
- изменение параметров настройки кэша (количество страниц КЭШа и размер страницы КЭШа в записях)

Конфигурация АРМ администратора осуществляется в двух точках:

- конфигурация собственно АРМ администратора в окне свойств (см. Рисунок 20);
- конфигурация подключения (или одного из подключений) к Центру Регистрации в окне свойств подключения (см. Рисунок 21).

Процедура открытия окна свойств АРМ администратора и набор параметров конфигурации описаны в разделе 4.2.5 настоящего Руководства.

Для открытия окна свойств подключения к ЦР щелкните правой кнопкой мыши по объекту (или нужному объекту) левой панели, обозначенному в дереве консоли как **Центр регистрации**. Затем выберите из контекстного меню пункт **Свойства**.

В окне свойств подключения к ЦР доступны для конфигурации следующие параметры:

Центра Регистрации (закладка **Центр Регистрации**)

- URL Web-сервиса Центра регистрации, с которым будет работать АРМ;
- Сертификат аутентификации администратора;

Настройки кэша (закладка **Настройки кэша**)

- Количество страниц кэша;
- Размер страницы кэша в записях



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

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.

Рисунок 21. Окно свойств подключений к ЦР в АРМ администратора ЦР.

The image shows a Windows-style dialog box titled "Свойства: Центр Регистрации - fav.cr.ru". It has two tabs: "Центр регистрации" (selected) and "Настройки кэша". The "Центр регистрации" tab contains the following fields and information:

- Адрес URL файла описания WSDL Центра Регистрации:
- Макс. время ожидания SOAP-вызовов (секунд):
- Сертификат администратора:
 - Субъект: CN=Оператор ЦР, O=Крипто-Про, L=Москва, S=Москва, C=RU, E=fav@cryptopro.ru
 - Выдан: CN=FAV2004 CA, O=CryptoPro, L=Moscow, S=Moscow, C=RU, E=fav@cryptopro.ru
 - Серийный номер: 6133 BFA4 0000 0000 0005
 - Срок действия: с 09.06.2004 15:03:00 по 09.06.2010 15:12:00
 - Использование ключа: 1.3.6.1.5.5.7.3.2, 1.2.643.2.2.34.5

At the bottom of the "Центр регистрации" tab are three buttons: "Выбрать...", "Просмотр...", and "Протестировать соединение".

The "Настройки кэша" sub-tab is currently selected and shows:

- Количество страниц кэша:
- Размер страницы кэша (в записях):

At the bottom of the "Настройки кэша" sub-tab are three buttons: "ОК", "Отмена", and "Применить".

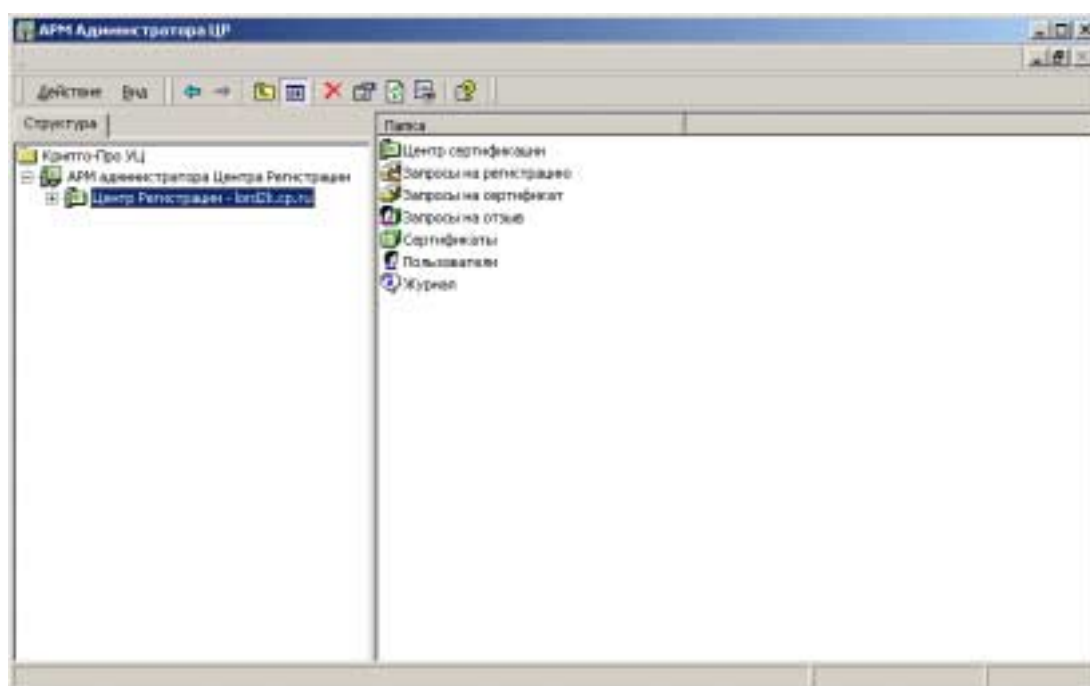
6. Запуск и интерфейс приложения АРМ администратора

6.1. 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 АРМа администратора 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 22).

Рисунок 22. 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 АРМ 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 появится крестик и список папок в правой части окна (см. Рисунок 22).

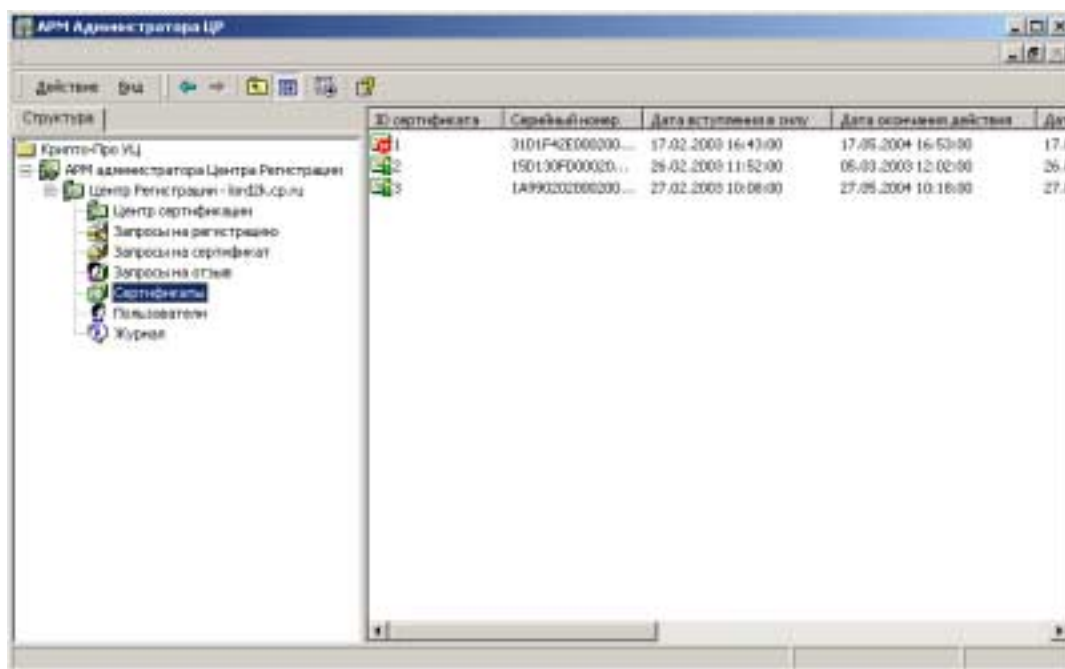
Открытие активированного подключения осуществляется путем нажатия на крестик слева от строки подключения к ЦР.

В случае, если на консоли администратора создано несколько подключений, активирована может быть только одна из них. Активизация другого подключения приводит к закрытию (деактивации) предыдущего подключения к ЦР.

6.2. 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 23).

Рисунок 23. Окно консоли администратора с активированными элементами дерева подключения

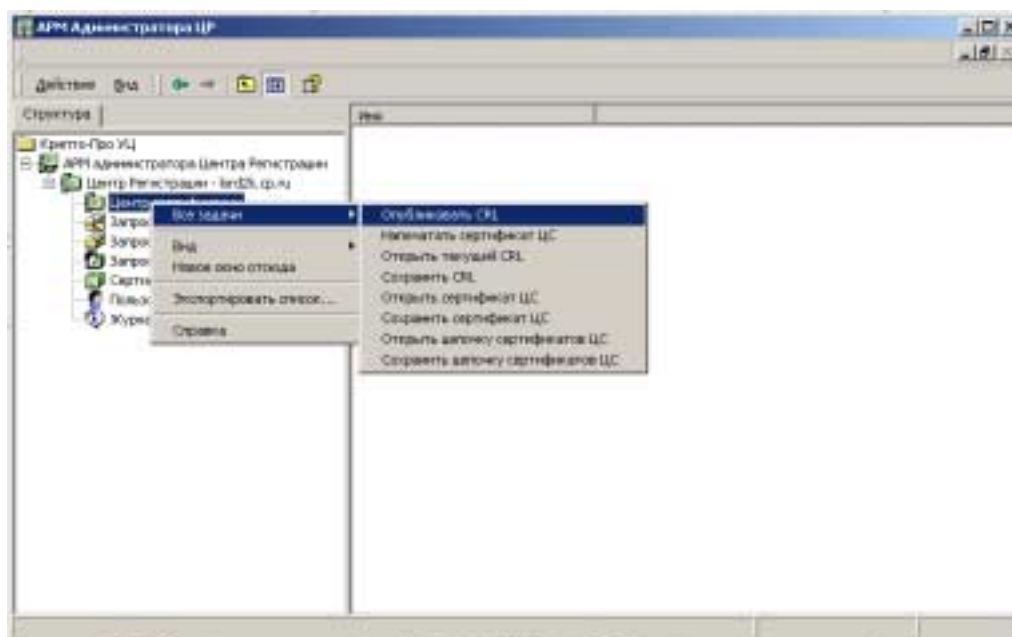


6.3. Контекстное меню папок и содержимого папок

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 24.

Рисунок 24. Пример контекстного меню в консоли администратора



Дополнительно, доступ к задачам доступен по пункту меню **Действие** консоли администратора.

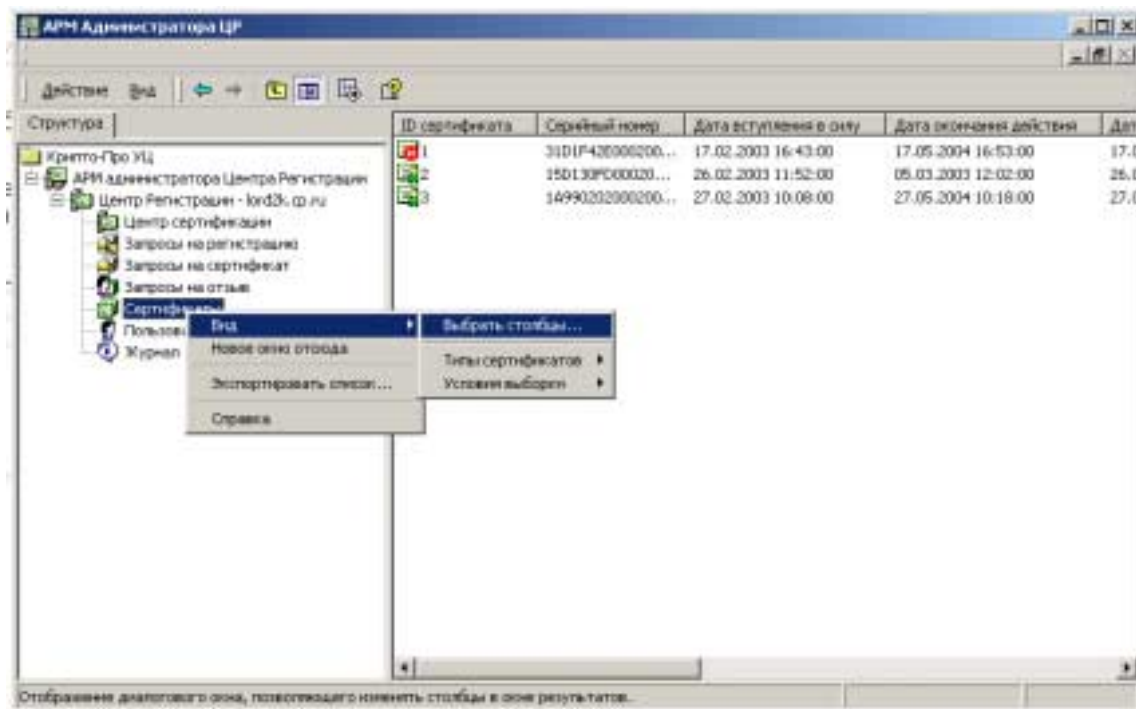
6.4. Управление отображением списка в правой части консоли

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 позволяет настраивать состав отображаемых полей для каждой папки. Для этого необходимо выбрать пункт **Вид/Выбрать столбцы** из контекстного меню элемента дерева (см. Рисунок 25).

Рисунок 25. Пункт меню настройки состава полей списка

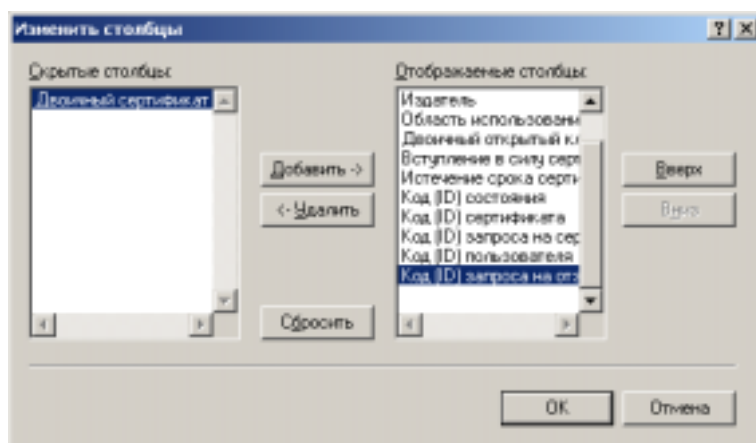


При выполнении данного пункта меню будет отображено диалоговое окно изменения состава полей, отображаемых для выбранной папки (см. Рисунок 26).

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 столба 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 26. 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**.

6.5. Сортировка записей в списке консоли

Программное обеспечение АРМ администратора 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.

6.6. Фильтрация записей в списке консоли

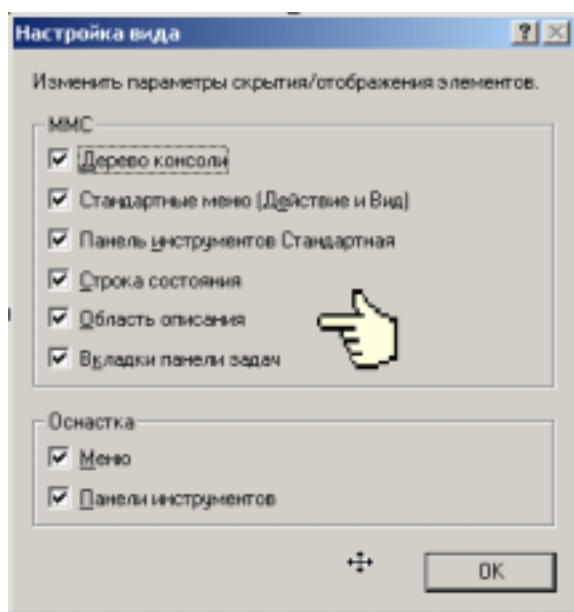
Программное обеспечение АРМ администратора позволяет работать не только со всем списком записей по содержимому папки в правой части консоли, но и с его подмножеством, построенному по разнообразным условиям (фильтрация записей).

6.6.1. 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 27).

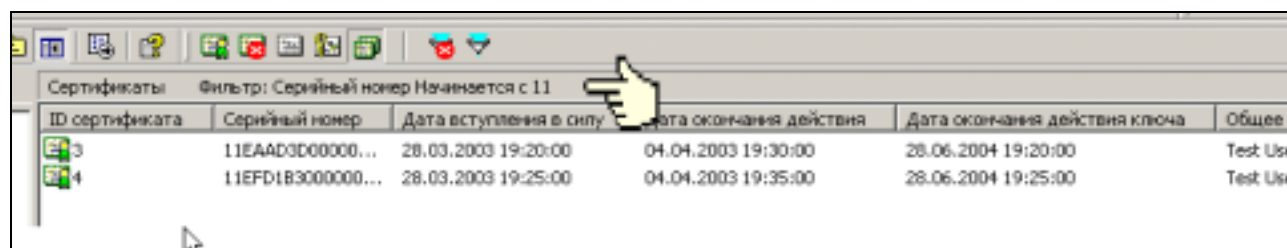
Рисунок 27. Настройка отображения области описания фильтрации записей



Закройте окно настройки.

После этого условие выборки будет отображаться в области отображения, расположенной над списком консоли (см. Рисунок 28).

Рисунок 28. Область отображения условий фильтрации



Действия для отображения области описания фильтрации записей в списке консоли выполнять не надо (они выполнены при установке ПО АРМ администратора ЦР) если используется консоль администратора, сформированная при установке. Если Вы создали собственную консоль и добавили в нее оснастку **АРМ администратора Центра Регистрации** то для отображения значения фильтра выполните действия данного раздела Руководства.

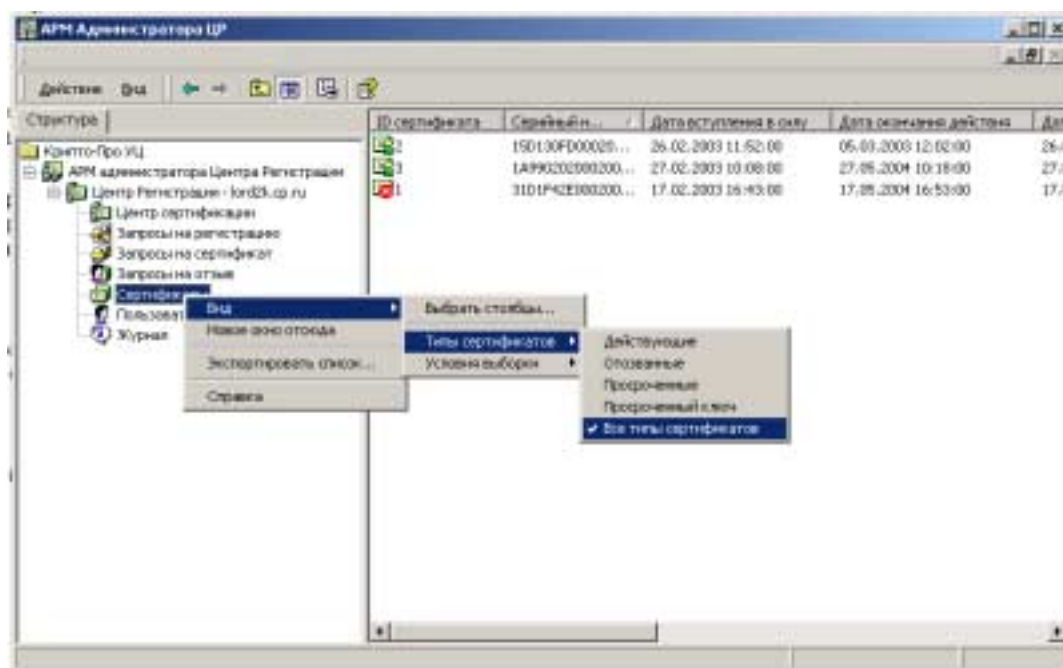
6.6.2. Фильтрация по типам записей

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...** (см. Рисунок 29).

Рисунок 29. 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 актуальные при следующем сеансе работы с АРМ администратора.

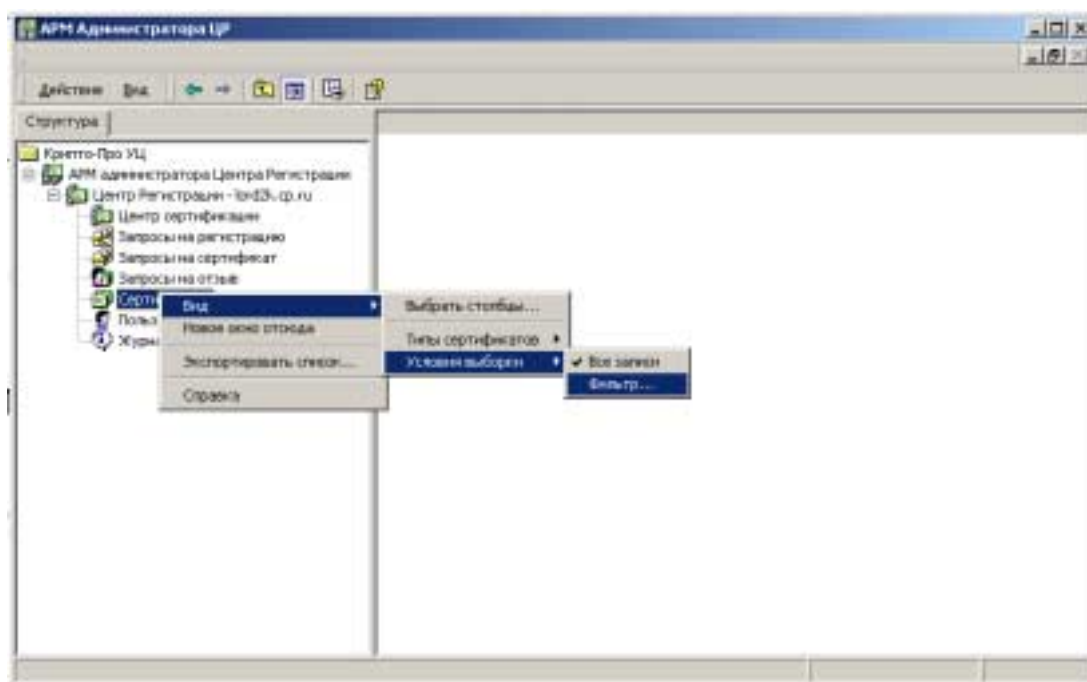
6.6.3. Фильтрация по значениям полей записей

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

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

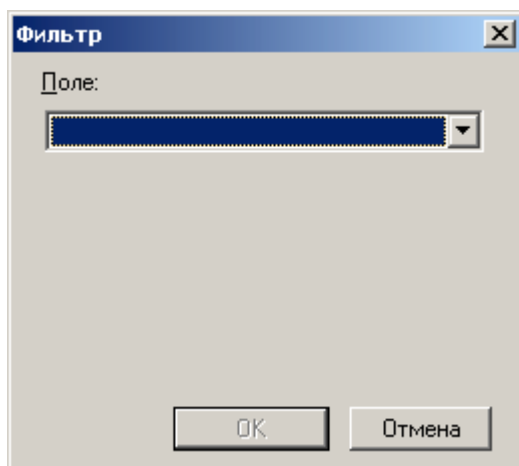
Для установления фильтра по типам записей необходимо из контекстного меню соответствующей папки выбрать пункт **Вид**, пункт **Условия выборки** и следующий пункт **Фильтр** (см. Рисунок 30).

Рисунок 30. Окно выбора фильтрации записей по значениям полей



После выполнения данного пункта контекстного меню будет отображено диалоговое окно определения поля записи для фильтрации (см. Рисунок 31).

Рисунок 31. 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.

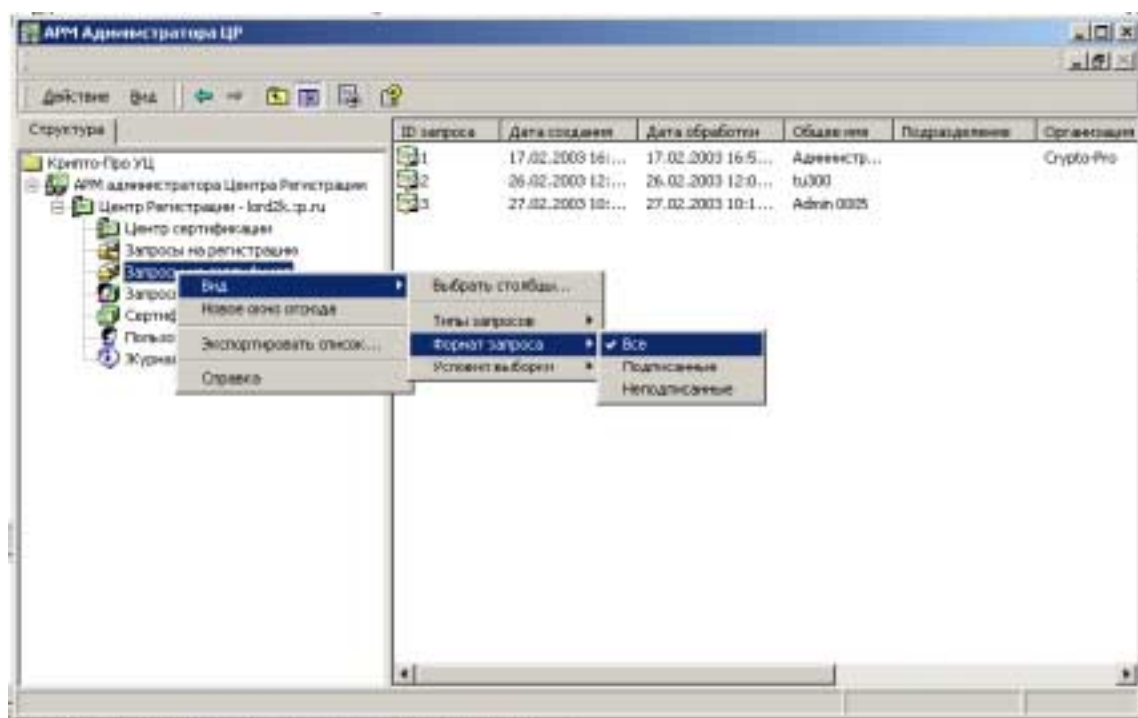
Данный режим фильтрации удобен к применению при большом количестве записей в папке. Его применение значительно сократит время получения и отображения информации по объектам управления Центра Регистрации.

6.6.4. 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 32).

Рисунок 32. Окно выбора фильтрации запросов на сертификат по признаку подписания



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

6.7. Просмотр свойств элементов управления

Объекты управления Центра Регистрации (см. раздел 2) 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 окна свойств:

Рисунок 33. Окно свойств запроса на сертификат

Запрос на сертификат

Информация о запросе

Состояние: Подтвержден

Субъект: CN=User 1, E=maslov@cryptopro.ru

Использование ключа: Пользователь Центра Регистрации (1.2.643.2.2.34.6)

Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)

Дата запроса: 17.09.2003 18:34:00

Дата рассмотрения: 17.09.2003 18:34:00

Открытый ключ: ГОСТ Р 34.10-94

0481 8028 AC66 C0B7 ED6A 88D4 6B16 93D4 235B
5A9C 5973 DC67 BA6C 54D4 FD11 539D 94A6 4743
4C9F C3BA 4A59 AB86 2A0C 4BF9 751B 3F89 6FEE

Комментарий пользователя:

Комментарий администратора:

Сертификат подписавшего Сертификат одобрявшего

OK Отмена Применить

Рисунок 34. Окно свойств запроса на регистрацию

Запрос на регистрацию

Информация о запросе

Состояние: Завершен

Субъект: 1.2.840.113549.1.9.1=maslov@cryptopro.ru, 2.5.4.6=RU, 2.5.4.3=Admin 0005

Дата запроса: 27.02.2003 10:17:54

Дата рассмотрения: 27.02.2003 10:17:54

Комментарий пользователя:

Комментарий администратора:

OK Отмена Применить

Рисунок 35. Окно свойств запроса на отзыв сертификата

Запрос на отзыв

Информация о запросе

Состояние: Завершен

Дата запроса: 17.09.2003 19:01:00

Дата рассмотрения: 17.09.2003 19:01:00

Серийный номер сертификата: 615EB68B00000000003C

Причина отзыва: Компрометация ключа

Комментарий администратора:

Сертификат подписавшего Сертификат одобряющего

OK Отмена Применить

Рисунок 36. Окно свойств запроса на приостановление действия сертификата

Запрос на отзыв

Информация о запросе

Состояние: Завершен

Дата запроса: 17.09.2003 19:01:00

Дата рассмотрения: 17.09.2003 19:01:00

Серийный номер сертификата: 615CD82200000000003B

Причина отзыва: Приостановка действия

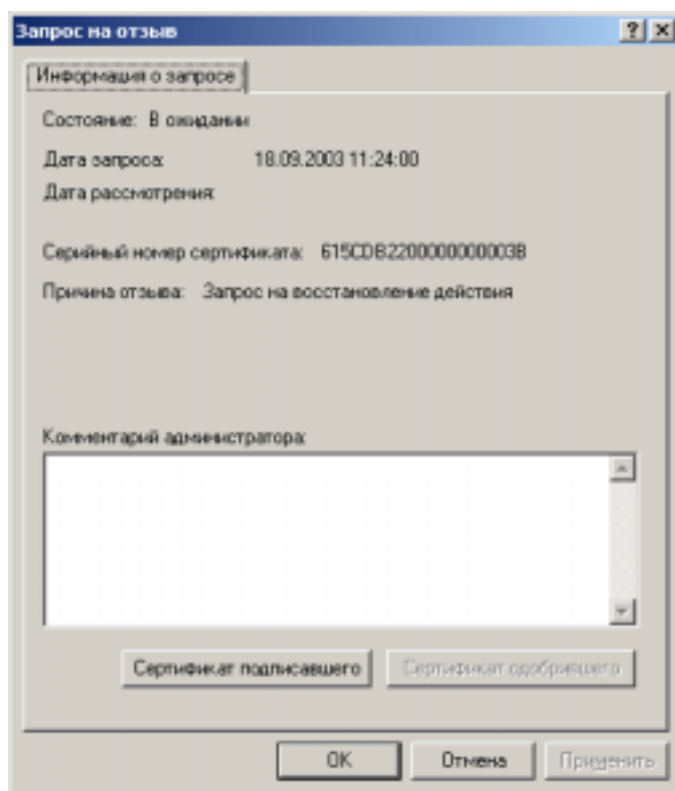
Дата возобновления действия: 17.10.2003 19:01:00

Комментарий администратора:

Сертификат подписавшего Сертификат одобряющего

OK Отмена Применить

Рисунок 37. Окно свойств запроса на возобновление действия сертификата



6.8. Сохранение сертификата пользователя в файл

Для сохранения сертификата или группы сертификатов (см. раздел 6.9) в файл используется задача **Экспортировать** для списка сертификатов папки **Сертификаты**.

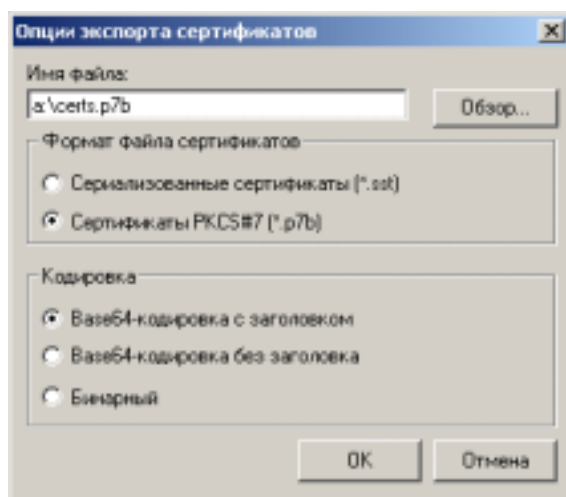
Поддерживаются следующие форматы файла экспорта сертификата(ов):

- сериализованные сертификаты (.sst)
- сертификаты PKCS#7 (.p7b)

При экспорте сертификатов поддерживаются следующие кодировки содержимого файла:

- Base-64 с заголовками или без заголовков
- Бинарный

Выбор формата файла для экспорта сертификата(ов) и кодировки файла осуществляется в окне выбора опций экспорта сертификатов (см. Рисунок 38).

Рисунок 38. Окно опций экспорта сертификатов

6.9. Групповые операции над объектами

Программное обеспечение АРМ администратора 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 папки, поддерживающие выполнение групповых операций
Запросы на регистрацию	Запросы поступившие	Принять Отклонить
Запросы на сертификат	Запросы поступившие	Принять Отклонить
Запросы на отзыв	Запросы поступившие	Принять Отклонить
Сертификаты	Все типы	Экспортировать
	Действующие	Отозвать Приостановить действие Экспортировать
	Отозванные	Возобновить действие (отозванные с кодом 6) Экспортировать

Для выполнения групповой операции над объектами (записями) необходимо с помощью мыши или удерживая клавишу Shift 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.

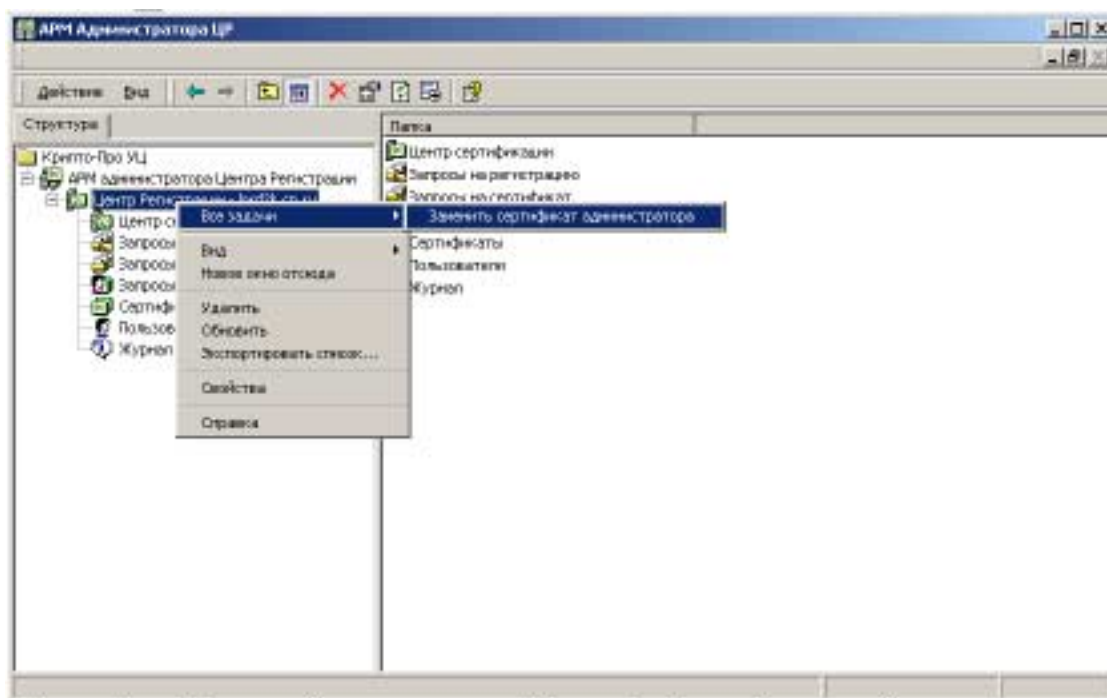
7. Смена ключа и сертификата Оператора УЦ

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

Смена ключей Оператора УЦ (плановая и внеплановая смена) производится в соответствии с регламентом, определенном в руководящих документах организации.

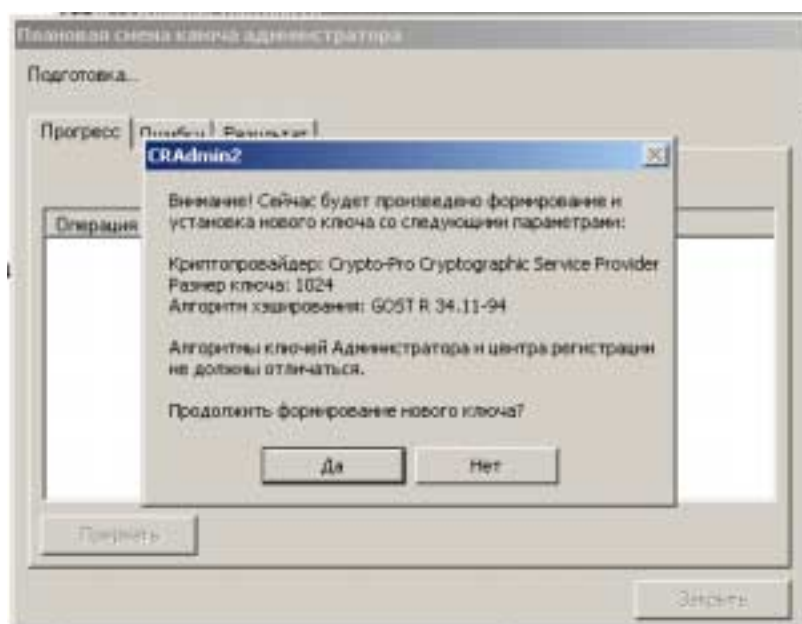
Плановая смена ключа Оператора УЦ производится с использованием задачи **Заменить сертификат администратора**, доступной в контекстном меню ветки (подключения) **Центр регистрации** консоли администратора (см. Рисунок 39).

Рисунок 39. 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 40).

Рисунок 40. Окно приглашения задачи плановой смены ключа администратора

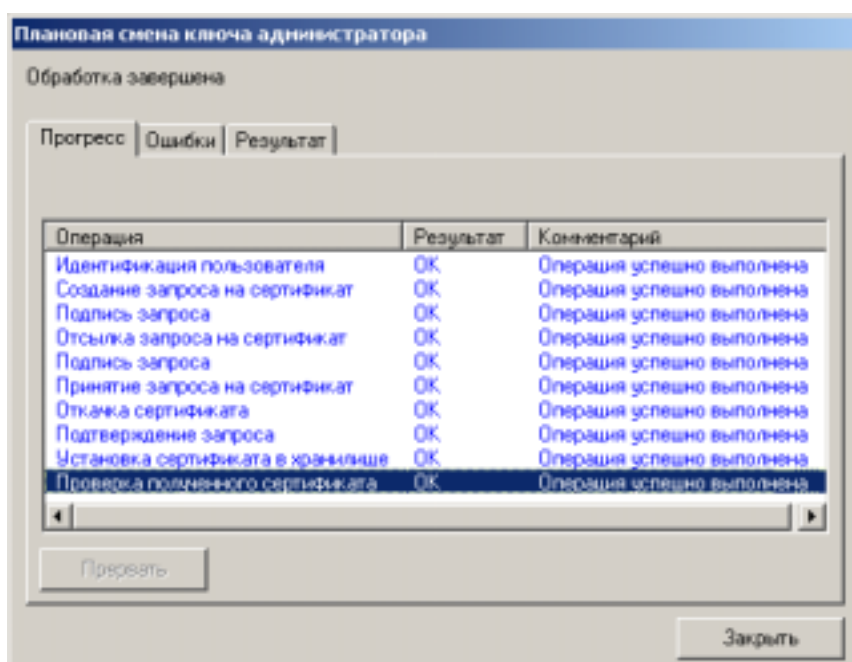


После нажатия кнопки **Да** происходит:

- генерация ключей;
- запись ключей на ключевой носитель;
- формирование запроса на новый сертификат администратора;
- получение выпущенного сертификата и установка на компьютера 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 41).

Рисунок 41. Окно завершения задачи плановой смены ключа администратора



Внеплановая смена ключей Оператора УЦ выполняется в соответствии с порядком, определенном Регламентом Удостоверяющего Центра.

8. 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.

8.1. Централизованный режим

АРМ администратора обеспечивает технические мероприятия процедуры регистрации пользователей с выдачей служебных ключей и сертификатов, заключающиеся в выполнении следующих процедур:

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

8.2. 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 служебный сертификат открытого ключа регистрируемого пользователя.

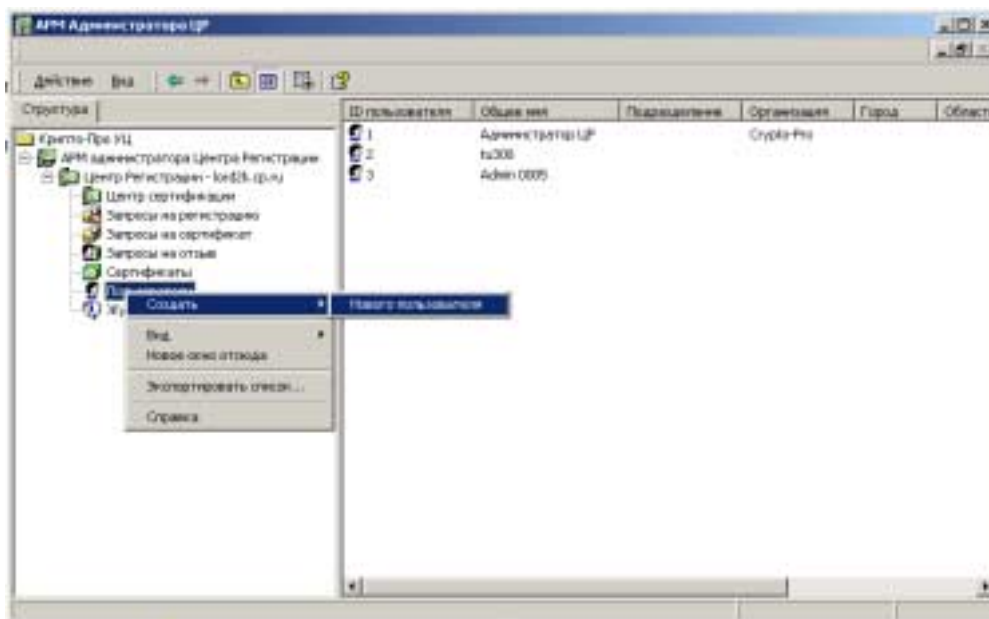
При регистрации пользователя в распределенном режиме используются организационные мероприятия, связанные с пересылкой пользователем по почте нотариально заверенных документов. Подробнее см. КриптоПро УЦ. Регламент.

8.3. Мастер регистрации пользователей

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

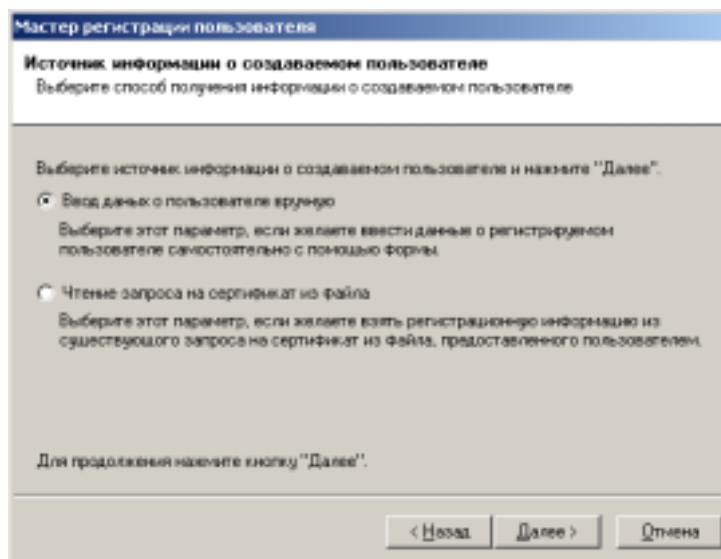
Запуск Мастера осуществляется путем выполнения задачи **Создать/Нового пользователя** в контекстном меню папки **Пользователи** (см. Рисунок 42).

Рисунок 42. Запуск задачи создания нового пользователя



После запуска Мастера регистрации пользователя на экране отобразится окно выбора источника информации о создаваемом пользователе (см. Рисунок 43).

Рисунок 43. 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 ключа УЦ.

8.3.1. Работа Мастера регистрации пользователя при выборе опции генерации запроса на сертификат

В случае выбора пункта **Генерация нового запроса на сертификат** отображается окно определения имени владельца сертификата открытого ключа (см. Рисунок 44).

Рисунок 44. Окно ввода информации о пользователе Мастера регистрации пользователя

The screenshot shows a window titled 'Мастер регистрации пользователя' (User Registration Wizard) with a tab 'Информация о пользователе' (User Information). Below the tab is a text box with the instruction: 'Укажите данные о пользователе системы. Необходимые для заполнения поля помечены значком (*)' (Specify system user data. Fields to be filled are marked with an asterisk). Below this is a table with the following fields: 'Общее имя(*)', 'Подразделение', 'Организация', 'Город', 'Область', 'Страна/регион', and 'Электронная почта'. The 'Общее имя(*)' field is currently selected. At the bottom of the window, there is a text box with the instruction: 'Для продолжения нажмите кнопку "Далее".' (To continue, click the "Next" button.) and three buttons: '< Назад' (Back), 'Далее >' (Next), and 'Отмена' (Cancel).

Состав полей, определяющих владельца сертификата, зависит от настроек ПО Центра Регистрации. Значения данных полей будут занесены в учетную запись пользователя и будут заноситься во все последующие сертификаты пользователя в качестве имени владельца сертификата. Данная информация для зарегистрированного пользователя является не изменяемой в дальнейшем.

В следующем окне Мастера регистрации пользователя введите Ключевую фразу пользователя и, при необходимости, комментарий администратора к запросу на регистрацию. После чего появится завершающее окно Мастера регистрации пользователя. Установите в нем переключатель – **Запустить мастер создания сертификата**.

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

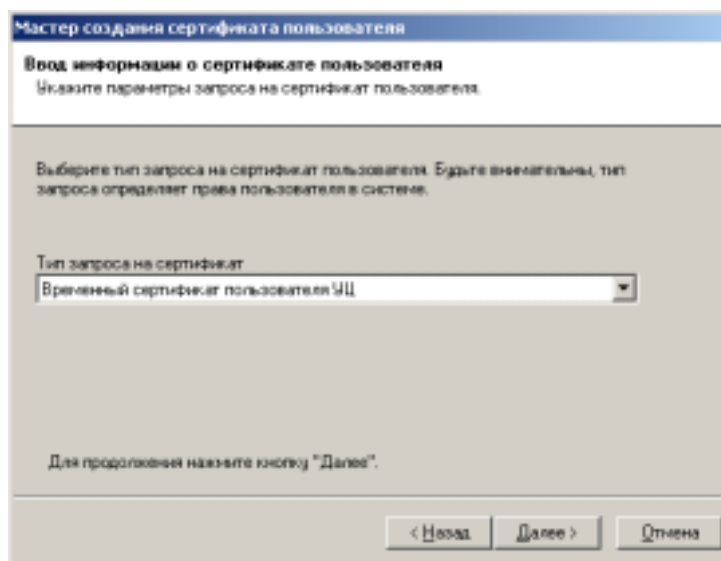
В зависимости от настройки АРМ администратора в части выбора криптопровайдера, следующим окном может быть диалоговое окно настройки параметров ключа (см. Рисунок 45).

Рисунок 45. Окно установки параметров ключа Мастера создания сертификата

The screenshot shows a window titled 'Мастер создания сертификата пользователя' (User Certificate Creation Wizard) with a tab 'Параметры ключа' (Key Parameters). Below the tab is a text box with the instruction: 'Установите параметры ключа' (Set key parameters). Below this is a text box with the instruction: 'Выберите криптопровайдер из приведенного списка. Укажите требуемый размер ключа и алгоритм хеширования.' (Select a cryptographic provider from the list. Specify the required key size and hashing algorithm). Below this is a dropdown menu for 'CSP' with the value 'Crypto Pro GOST R 34.10-94 Cryptographic Service Provider'. Below this is a text box for 'Размер ключа' (Key size) with the value '1024'. To the right of this text box are two labels: 'Мин: 1024' and 'Макс: 1024'. Below this is a dropdown menu for 'Алгоритм хеширования' (Hashing algorithm) with the value 'GOST R 34.11-94'. Below this are two checkboxes: 'Включить усиленную защиту закрытого ключа' (Enable enhanced protection of the private key) and 'Пометить ключи как экспортируемые' (Mark keys as exportable). The second checkbox is checked. At the bottom of the window, there is a text box with the instruction: 'Для продолжения нажмите кнопку "Далее".' (To continue, click the "Next" button.) and three buttons: '< Назад' (Back), 'Далее >' (Next), and 'Отмена' (Cancel).

Следующим окном Мастера является окно определения типа сертификата (см. Рисунок 46).

Рисунок 46. 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.

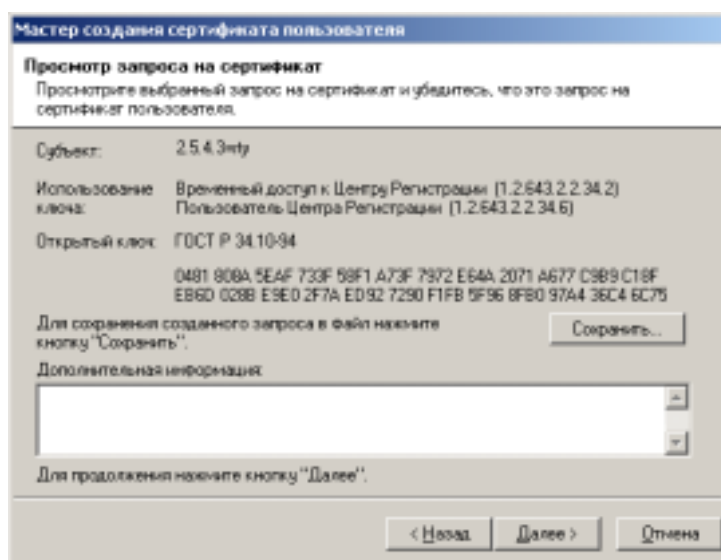
При регистрации пользователя с выдачей служебных ключей и служебного сертификата открытого ключа, необходимо выбрать шаблон сертификата, соответствующий служебному сертификату.

При регистрации пользователя с выдачей рабочих ключей и рабочего сертификата открытого ключа, необходимо выбрать шаблон сертификата, соответствующий рабочему сертификату.

После определения типа сертификата выполняется генерация ключей и формирование ключевого носителя.

В следующем окне Мастера (см. Рисунок 47) необходимо определить дополнительную информацию в учетных данных регистрируемого пользователя. Данная информация сохраняется в базе данных Центра Регистрации, но не включается в выпускаемые сертификаты пользователя.

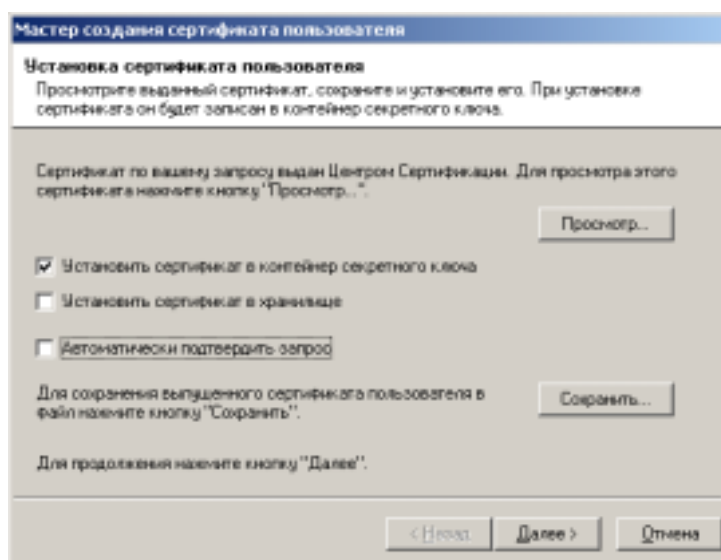
Рисунок 47. Окно запроса на сертификат Мастера создания сертификата



Установка выпущенного сертификата в контейнер закрытого ключа выполняется для технического обеспечения процедуры записи сертификата внутрь ключевого контейнера, расположенном 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. Определение наименования раздела хранилища сертификатов, в который производится установка выпущенного сертификата, задается в окне установки сертификата Мастера (см. Рисунок 48).

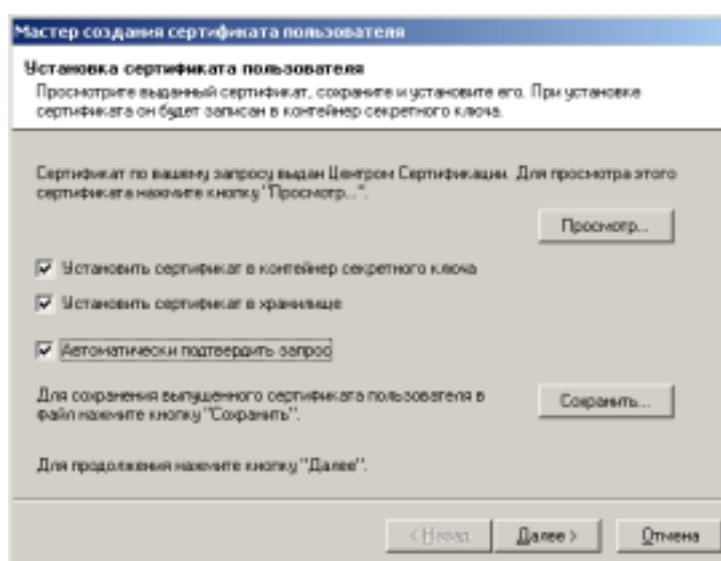
Также в данном окне возможно задать имя и расположение файла, в который будет сохранен выпущенный сертификат регистрируемого пользователя. Выбор имени файла осуществляется путем нажатия кнопки **Сохранить**.

Рисунок 48. Окно установки выпущенного сертификата Мастера создания сертификата



После нажатия кнопки **Далее** в окне установки сертификата Мастера происходит передача сформированного запроса на сертификат регистрируемого пользователя в Центр Регистрации для последующей обработки и выпуска сертификата Центром Сертификации.

Рисунок 49. Установка переключателей Установить сертификат в хранилище и Автоматически подтвердить запрос



В следующем окне Мастера возможно определить (выбрать) возможность сохранения цепочки сертификатов на магнитном носителе (см. Рисунок 50).

Рисунок 50. Окно сохранения цепочки сертификатов Мастера создания сертификата

The screenshot shows a window titled "Мастер создания сертификата пользователя". The main heading is "Сохранение цепочки сертификатов Центра Сертификации". Below it, text says: "Укажите расположение файла для сохранения цепочки сертификатов Центра Сертификации." There is a paragraph explaining that the master has an option to save the chain for user transfer, with an example of saving to a disk. Below this is a checked checkbox "Сохранить цепочку сертификатов Центра Сертификации". Underneath is a text field "Имя файла:" containing "a:\caser.p7b" and a button "Обзор...". A group box "Формат файла запроса" contains two radio buttons: "Файлы в Base64-кодировке PKCS#10 с заголовком" (selected) and "Файлы в Base64-кодировке PKCS#10 без заголовка". Below this is another checked checkbox "Включать в результат соответствующие СОС". At the bottom, text says "Для продолжения нажмите кнопку 'Далее'." and there are three buttons: "< Назад", "Далее >", and "Отмена".

Подтверждение успешной регистрации пользователя сопровождается соответствующим окном Мастера (см. Рисунок 51).

Рисунок 51. Окно окончания работы Мастера создания сертификата

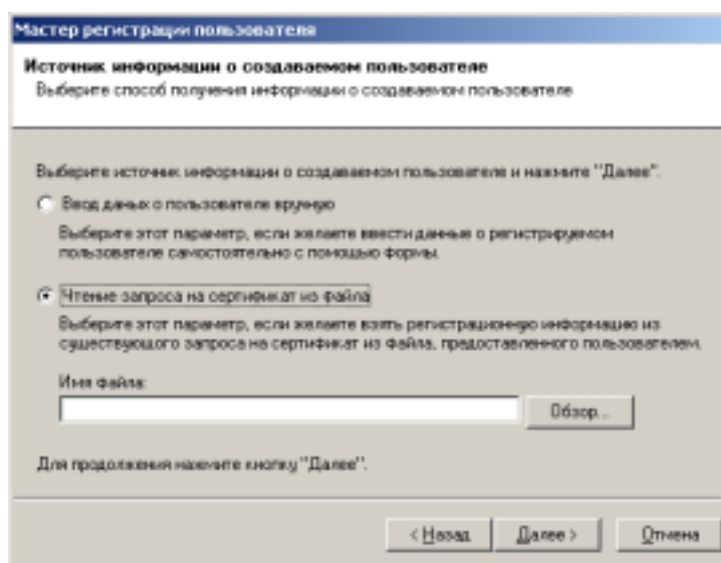
The screenshot shows the same window title "Мастер создания сертификата пользователя". On the left is a graphic with the text "Мастер создания сертификата" and an image of a certificate and a coin. On the right, the text says "Мастер создания сертификата пользователя" and "Создание сертификата успешно завершено." Below this, it says "Для закрытия мастера нажмите кнопку 'Готово'." At the bottom are three buttons: "< Назад", "Готово", and "Отмена".

8.3.2. Работа Мастера регистрации пользователя при выборе опции **чтение запроса на сертификат из файла**

В случае выбора пункта **Чтения запроса на сертификат из файла** окно расширяется полем ввода имени и расположения файла, содержащим запрос на сертификат регистрируемого пользователя (см. Рисунок 52).

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

Рисунок 52. 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.

В следующем окне Мастера (см. Рисунок 44) отображается идентификационная информация об учетных данных регистрируемого пользователя, содержащаяся в файле запроса на сертификат.

Нажмите кнопку **Далее** - откроется окно ввода секретной ключевой фразы пользователя и комментария администратора. После чего появится завершающее окно Мастера регистрации пользователя. Установите в нем переключатель – **Запустить мастер создания сертификата**.

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

В окне Просмотра запроса на сертификат **Мастера создания сертификата** (Рисунок 47) укажите необходимую дополнительную справочную информацию. Данная информация не будет заноситься в сертификат. Также в данном окне возможно задать имя и расположение файла, в который будет сохранен выпущенный сертификат регистрируемого пользователя. Выбор имени файла осуществляется путем нажатия кнопки **Сохранить**.

В окне установки сертификата Мастера (см. Рисунок 48,49) происходит передача сформированного запроса на сертификат регистрируемого пользователя в Центр Регистрации для последующей обработки и выпуска сертификата Центром Сертификации.

В следующем окне Мастера возможно определить (выбрать) возможность сохранения цепочки сертификатов и списка отозванных сертификатов на магнитном носителе (см. Рисунок 50).

Подтверждение успешного изготовления сертификата сопровождается соответствующим окном Мастера (см. Рисунок 51).

9. 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.

Порядок выполнения данных процедур определяется регламентом Удостоверяющего Центра.

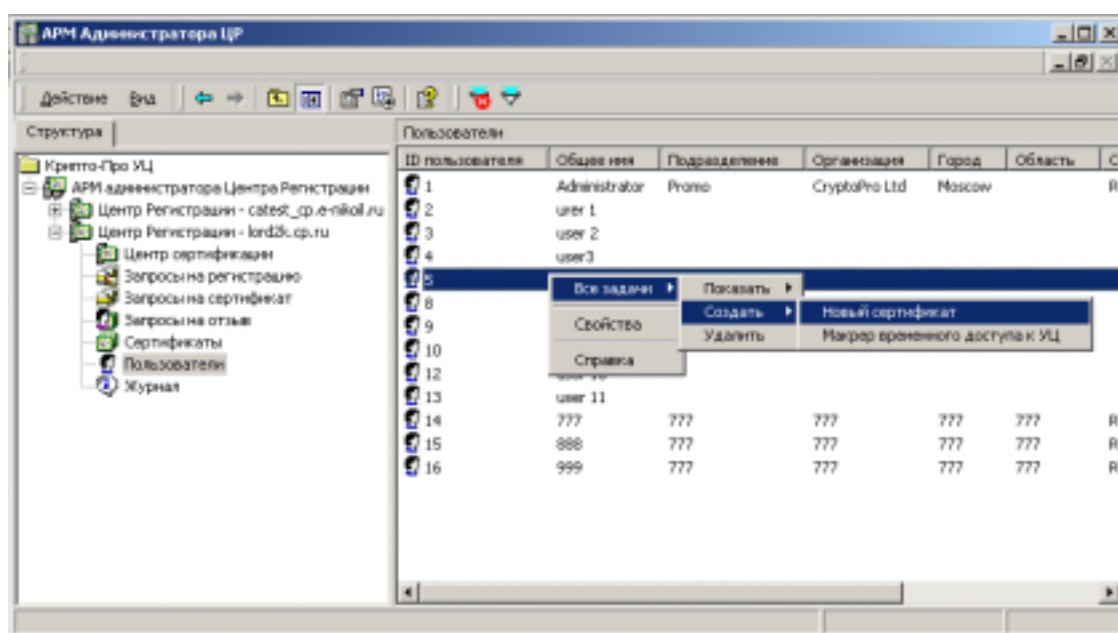
АРМ администратора обеспечивает выполнение следующих задач:

- генерация ключей и выпуск сертификатов открытых ключей пользователей;
- отзыв (аннулирование) сертификатов открытых ключей пользователей.

9.1. 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 53).

Рисунок 53. Запуск задачи выпуска нового сертификата пользователя



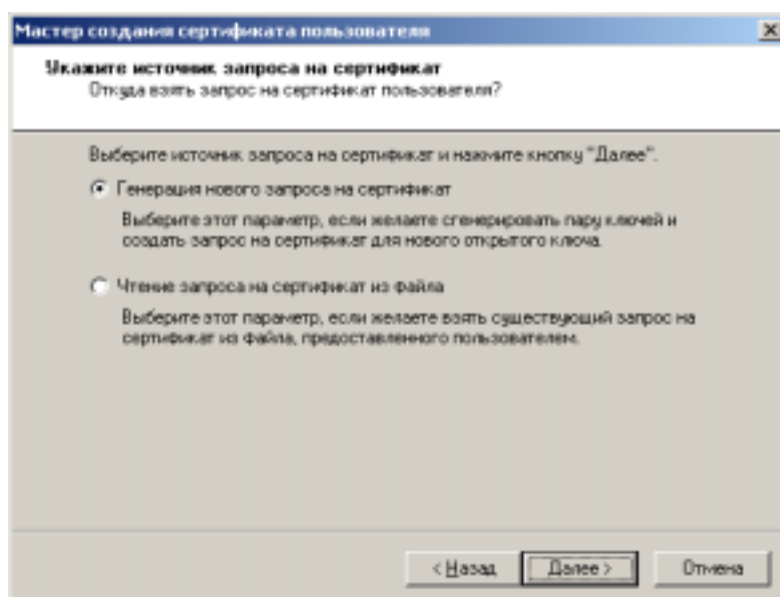
Создание нового сертификата пользователя выполняется с помощью Мастера создания сертификата пользователя.

В окне Мастера необходимо определить источник запроса на сертификат (см. Рисунок 54). 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 54. Окно определения источника запроса на сертификат в Мастере создания сертификата пользователя

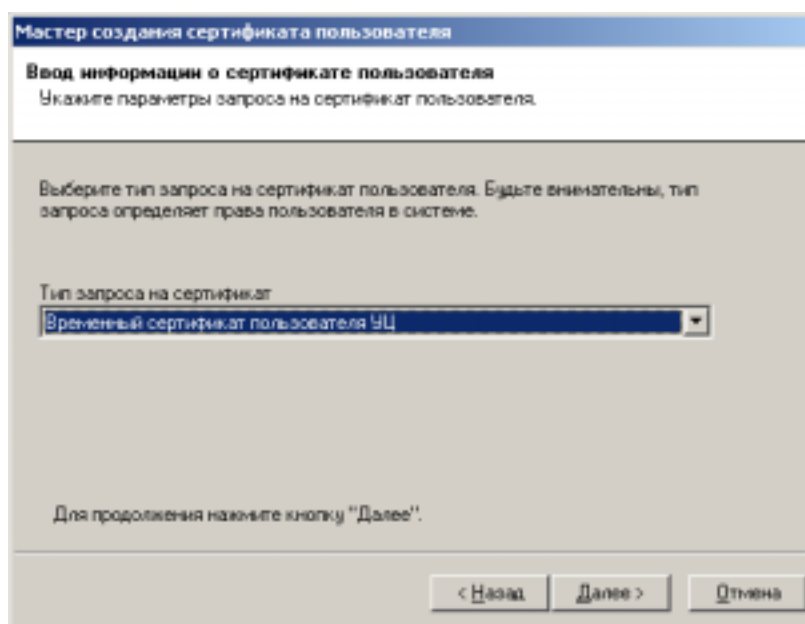


Последовательность дальнейших окон Мастера зависит от выбранного в окне определения источника запроса на сертификат пункта.

При выборе пункта **Генерация нового запроса на сертификат** в следующем окне необходимо выбрать шаблон сертификата для создаваемого сертификата (см. Рисунок 55).

В зависимости от настройки АРМ администратора в части выбора криптопровайдера, перед окном выбора шаблона на сертификат может быть диалоговое окно настройки параметров ключа (см. Рисунок 45).

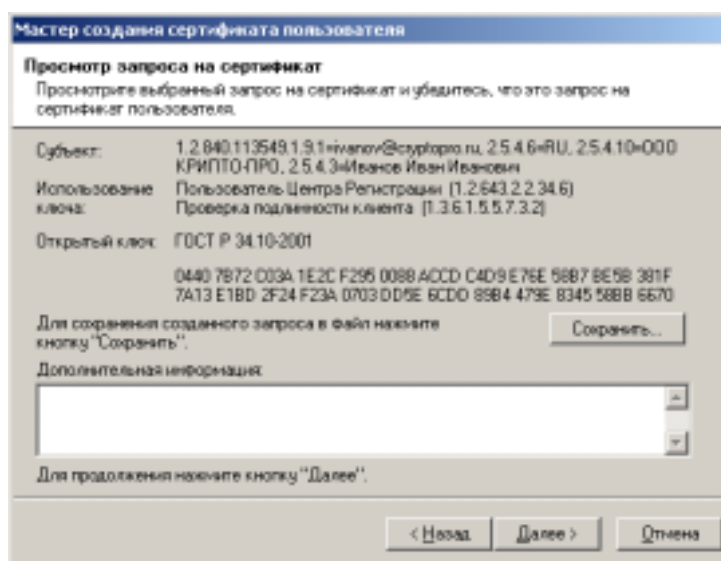
Рисунок 55. Окно выбора шаблона сертификата Мастера создания сертификата пользователя



При выборе пункта **Чтение запроса на сертификат из файла** окно выбора шаблона будет пропущено.

Следующим окном Мастера будет окно просмотра запроса на сертификат (см. Рисунок 56). В нем отображается информация о владельце сертификата и области применения сертификата.

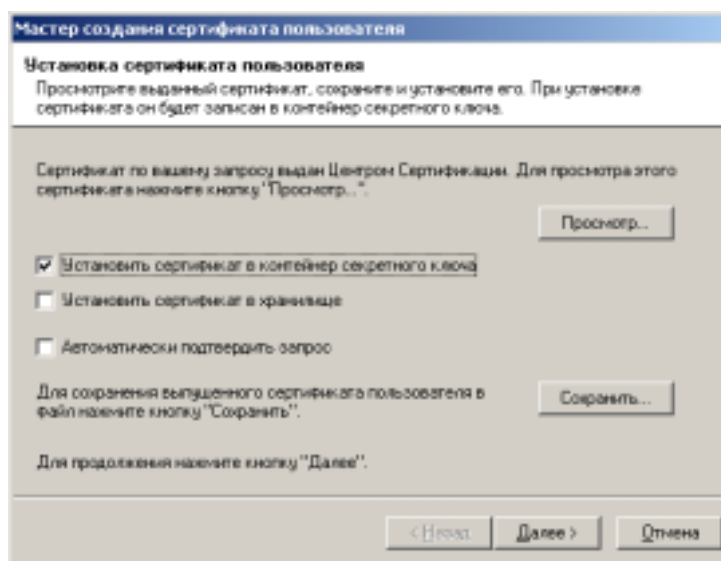
Рисунок 56. Окно просмотра запроса на сертификат Мастера создания сертификата пользователя



Установка выпущенного сертификата на компьютере администратора выполняется для технического обеспечения процедуры записи сертификата в ключевой контейнер на ключевом носителе. Данная опция возможна только для криптопровайдеров (CSP), поддерживаемых ее реализацию. К таким CSP относится СКЗИ КриптоПро CSP. Определение наименования раздела хранилища сертификатов, в который производится установка выпущенного сертификата, задается в окне установки сертификата Мастера (см. Рисунок 57).

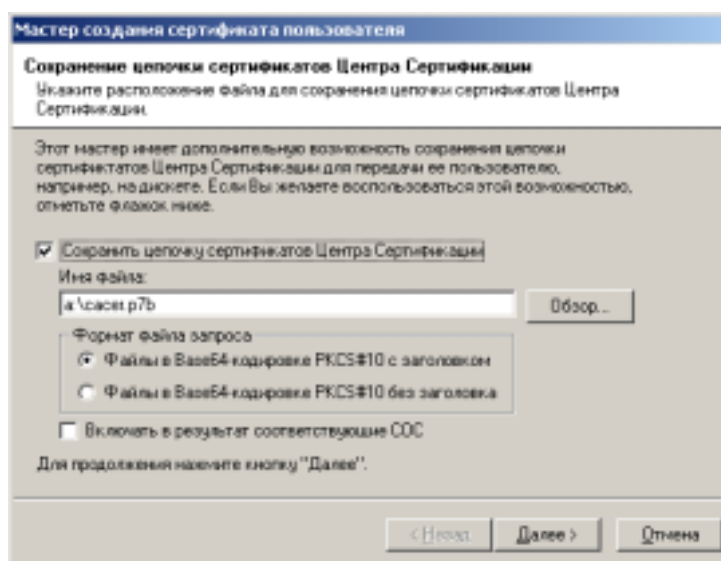
Также в данном окне возможно задать имя и расположение файла, в который будет сохранен выпущенный сертификат пользователя. Выбор имени файла осуществляется путем нажатия кнопки **Сохранить**.

Рисунок 57. Окно установки сертификата Мастера создания сертификата пользователя



В следующем окне Мастера возможно определить (выбрать) возможность сохранения цепочки сертификатов и списка отозванных сертификатов на магнитный носитель (см. Рисунок 58).

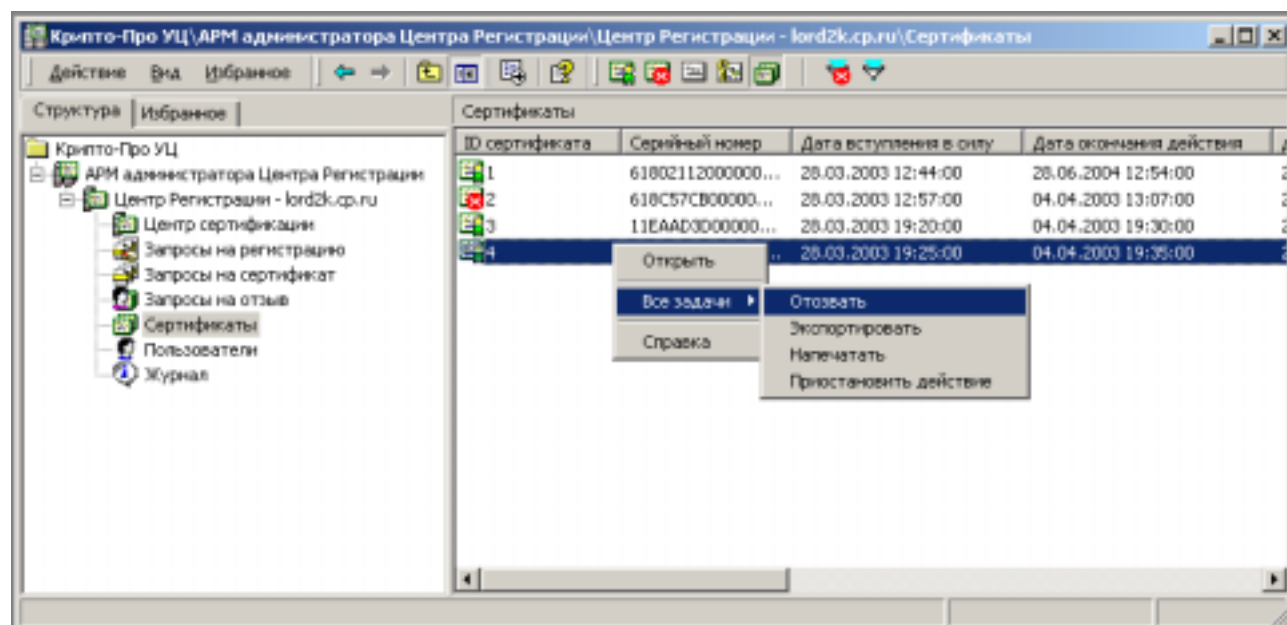
Рисунок 58. Окно сохранения цепочки сертификатов Мастера создания сертификата пользователя



9.2. Отзыв (аннулирование) сертификатов открытых ключей пользователей

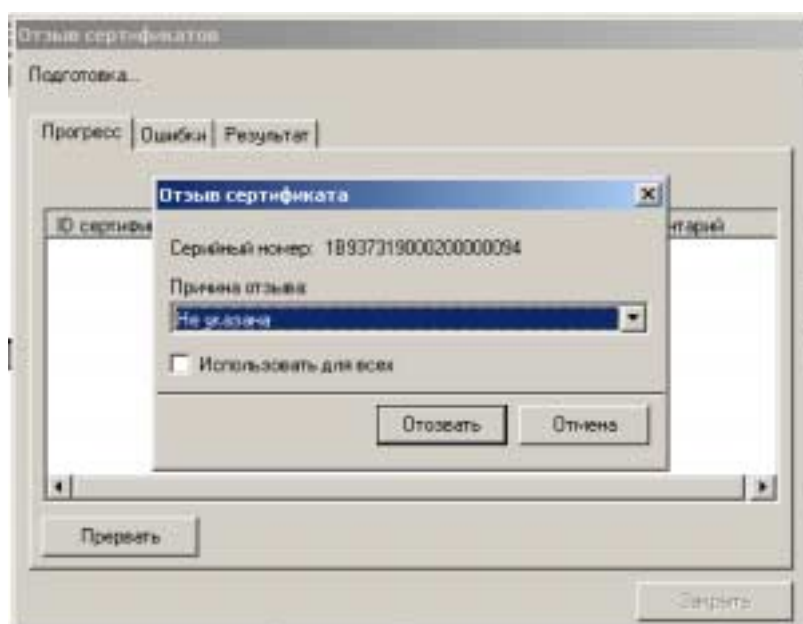
Отзыв сертификата открытого ключа для зарегистрированного пользователя выполняется с помощью задачи **Отозвать** из контекстного меню записи папки **Сертификаты** (см. Рисунок 59).

Рисунок 59. Запуск задачи отзыва сертификата пользователя



При запуске данной задачи, администратору будет выведено окно для указания причины отзыва сертификата (см. Рисунок 60).

Рисунок 60. Окно указания причины отзыва в задаче отзыва сертификата пользователя

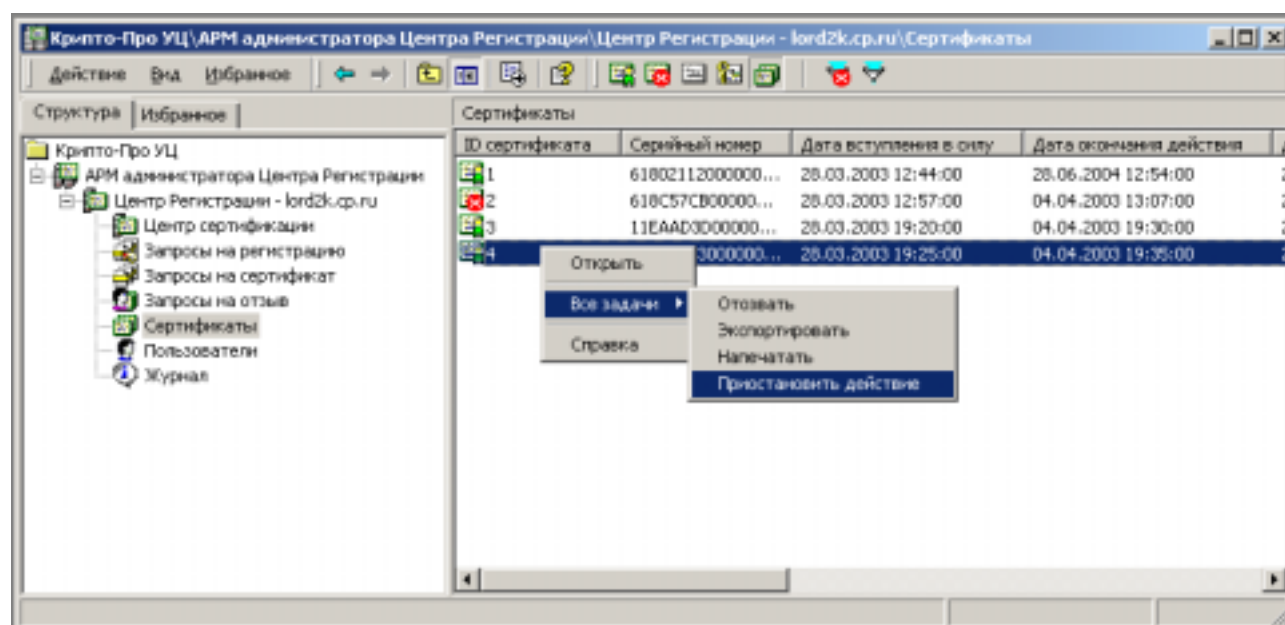


При выполнении групповой операции над несколькими сертификатами, можно указать одну причину отзыва для всех сертификатов. Для этого нужно выбрать пункт **Использовать для всех** в окне указания причины отзыва.

9.3. 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.

Рисунок 61. Запуск задачи приостановления действия сертификата пользователя



После начала выполнения задачи приостановления действия сертификата, администратору будет отображено окно (см. Рисунок 62), в котором необходимо указать

Руководство оператора Удостоверяющего центра ООО «КРИПТО-ПРО» (срса.cryptopro.ru)
период, на который приостанавливается действие сертификата открытого ключа пользователя.

Рисунок 62. Окно указания периода приостановления действия сертификата пользователя

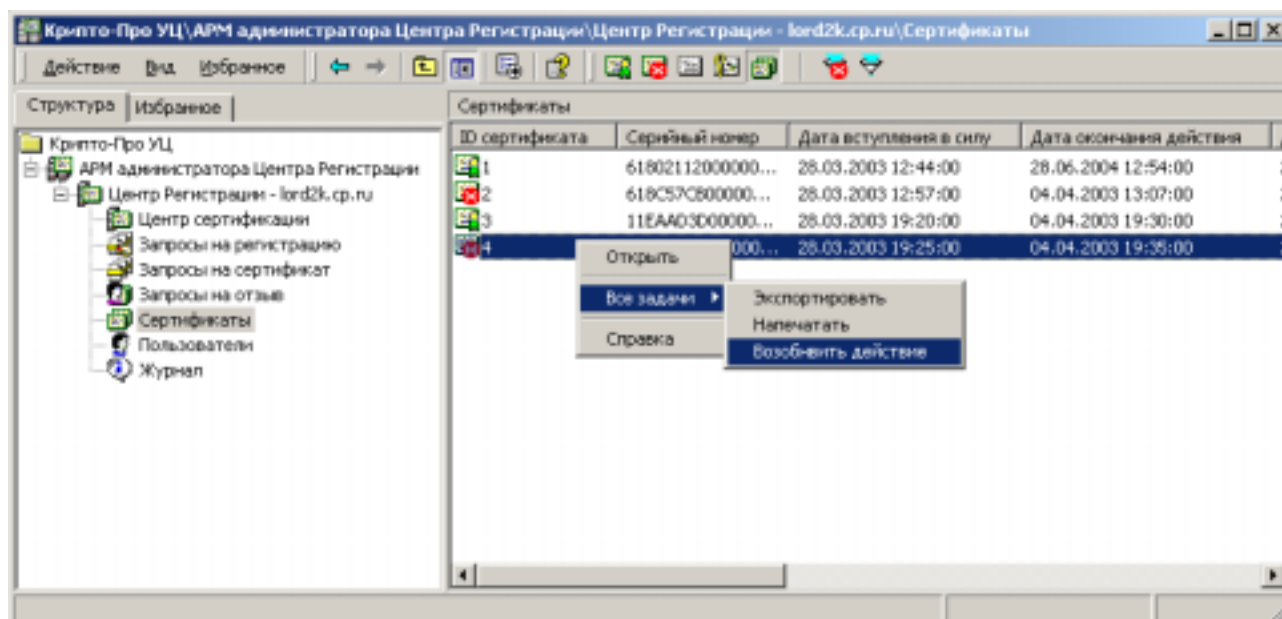
The image shows a screenshot of a software application window titled 'Form1'. In the foreground, a smaller dialog box titled 'Выбор интервала времени' (Time Interval Selection) is open. This dialog box contains a label 'Введите интервал времени:' (Enter time interval:) followed by six input fields with spinners: 'Число лет' (Number of years) with the value 1, 'Число месяцев' (Number of months) with 0, 'Число недель' (Number of weeks) with 0, 'Число дней' (Number of days) with 0, 'Число часов' (Number of hours) with 0, and 'Число минут' (Number of minutes) with 0. At the bottom of the dialog are 'OK' and 'Отмена' (Cancel) buttons. The background window 'Form1' has a tabbed interface with tabs labeled 'Подготовка...' (Preparation), 'Прогресс' (Progress), and 'Ошибки' (Errors). Below the tabs is a list box labeled 'ID запроса' (Request ID) and a text area labeled 'Комментарий' (Comment). At the bottom of the window are buttons for 'Прервать' (Interrupt) and 'Закреть' (Close).

Запрос на приостановление действия сертификата будет отправлен на Центр Сертификации и сертификат будет помещен в список отозванных сертификатов (CRL) при его формировании. Код причины отзыва сертификата в CRL будет установлен **Приостановка действия(6)**.

9.4. 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.

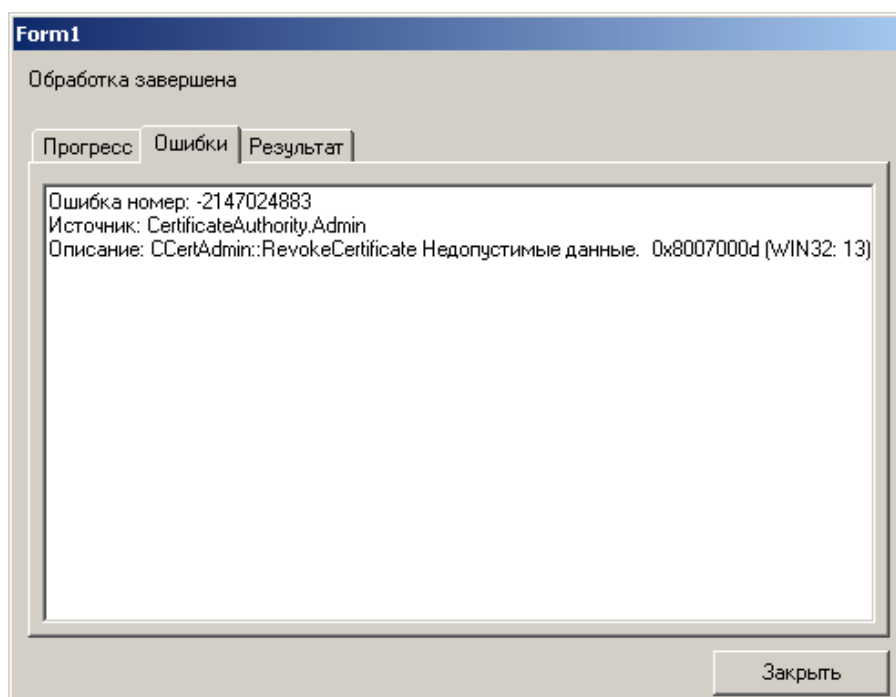
Рисунок 63. Запуск задачи возобновления действия сертификата пользователя



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

В противном случае будет диагностирована ошибка:

Рисунок 64. Сообщение об ошибке при попытке возобновления действия отозванного сертификата



После выполнения задачи возобновления действия сертификату будет установлен статус *Действующий* и он будет выведен из списка отозванных сертификатов (CRL) после его формирования.

10. Удаление зарегистрированных пользователей

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

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 не обработанного запроса на сертификат открытого ключа, стоящего в очереди.

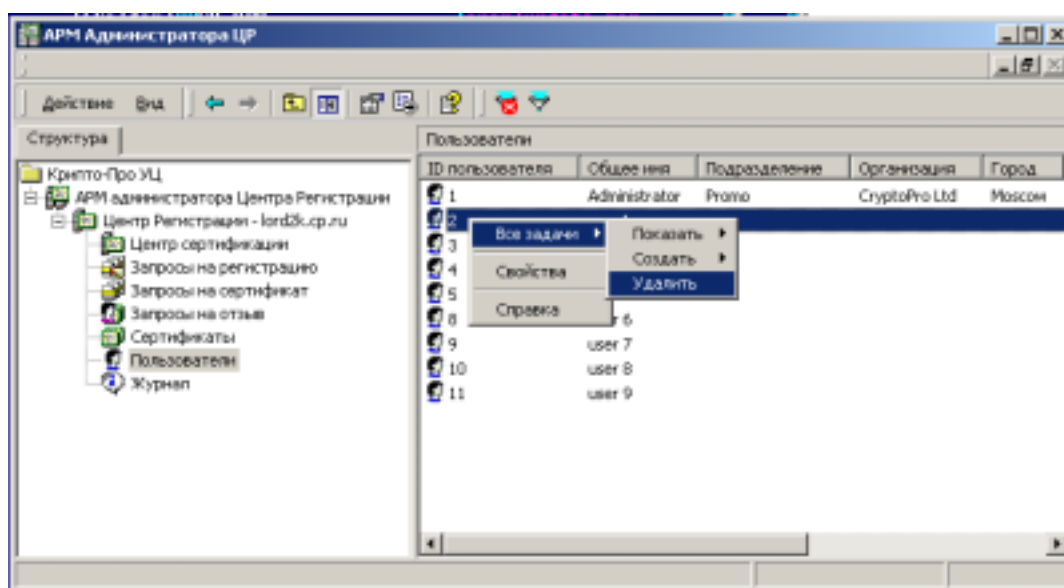
При удалении пользователя удаляется вся информация по пользователю из базы данных Центра Регистрации.



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

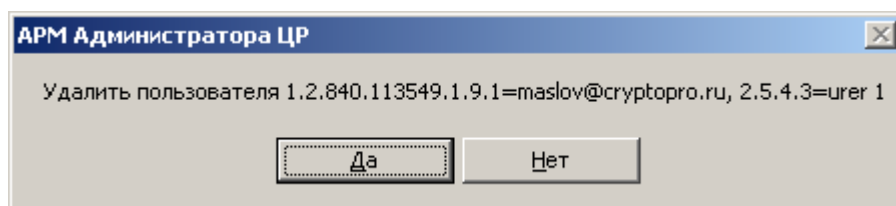
Для запуска задачи удаления пользователя необходимо выбрать пользователя из списка и выполнить задачу **Удалить** из контекстного меню (см. Рисунок 65).

Рисунок 65. Запуск задачи удаления зарегистрированного пользователя



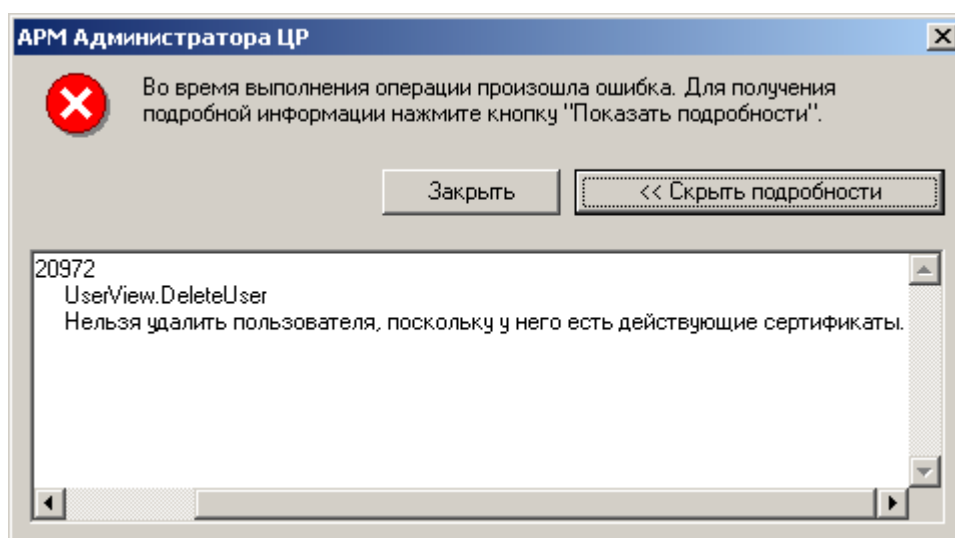
В следующем окне отображается информация по значениям атрибута имени пользователя (см. Рисунок 66). Администратору необходимо убедиться в правильном выборе удаляемого пользователя.

Рисунок 66. Окно предупреждения при удалении пользователя



В случае, если выбранный пользователь не удовлетворяет критериям для удаления, отображается окно с соответствующим диагностическим сообщением (см. Рисунок 67).

Рисунок 67. Окно сообщения о невозможности удаления пользователя



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

11. Обработка запросов пользователей на Центр 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 Центр Регистрации сконфигурирован для поддержки регистрации пользователей в распределенном режиме);
- запросы на сертификат открытого ключа (если Центр Регистрации сконфигурирован для поддержки режима распределенного управления ключами и сертификатами пользователями посредством АРМ зарегистрированного пользователя);
- запросы на отзыв сертификата открытого ключа, приостановление, возобновление его действия (если Центр Регистрации сконфигурирован для поддержки режима распределенного управления ключами и сертификатами пользователями посредством АРМ зарегистрированного пользователя).

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

Под обработкой понимается регламентная процедура изменения типа объекта управления (запроса) из типа **Поступившие**, в тип **Принятые** или **Отвергнутые/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.

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:
 - а. открыть окно свойств запроса и проанализировать информацию в нем (см. примеры окон свойств в разделе 6.6);
 - б. 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.

12. Печать сертификатов пользователей

Программное обеспечение АРМ администратора 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.

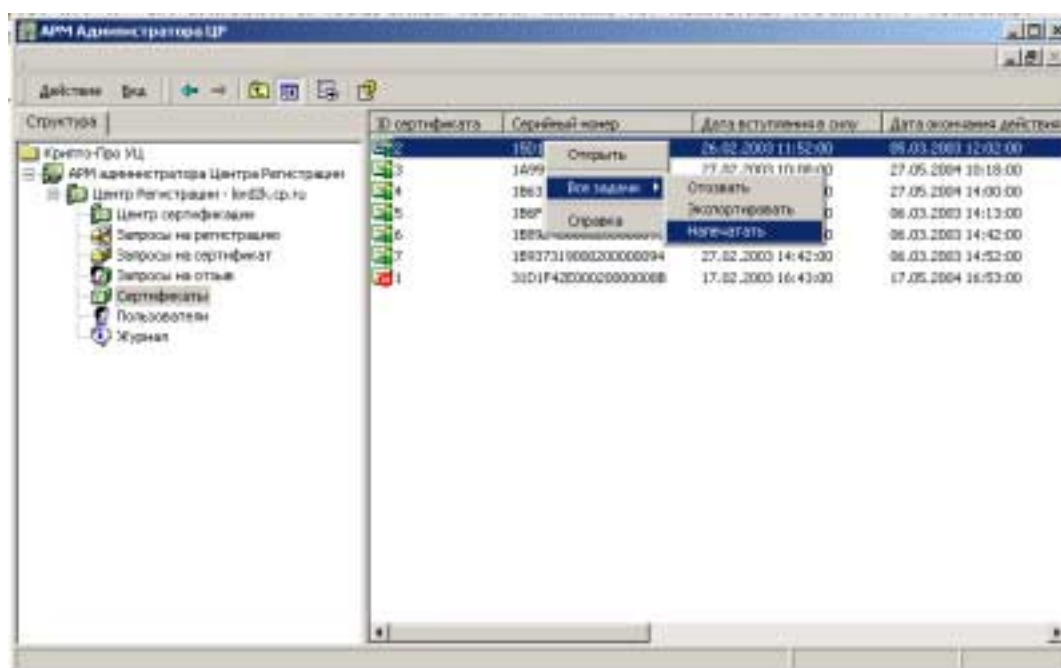
Данный файл может корректироваться для приведения в соответствия формы бланку сертификата Удостоверяющего Центра предприятия.

Имя и размещение файла с шаблоном формы сертификата задается в окне свойств оснастки АРМ администратора (см. Рисунок 20).

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.

Формирование формы для печати сертификата происходит при выполнении задачи **Печать** из контекстного меню для записи папки **Сертификаты** (см. Рисунок 68).

Рисунок 68. Запуск задачи печати сертификата пользователя



13. Маркер временного доступа

13.1. 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 ограниченное по времени действие. Маркер временного доступа становится неактивным после подтверждения получения сертификата открытого ключа, поступающего от пользователя на Центр Регистрации в момент установки сертификата на рабочем месте пользователя.

13.2. 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:
 - о Сформировать ключи;
 - о Сформировать запрос на сертификат открытого ключа и поставить его в очередь Центра Регистрации на обработку;
 - о Сформировать бланк запроса на сертификат открытого ключа для печати его на бумажном носителе;
 - о 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.

13.3. Создание маркера временного доступа для зарегистрированного пользователя

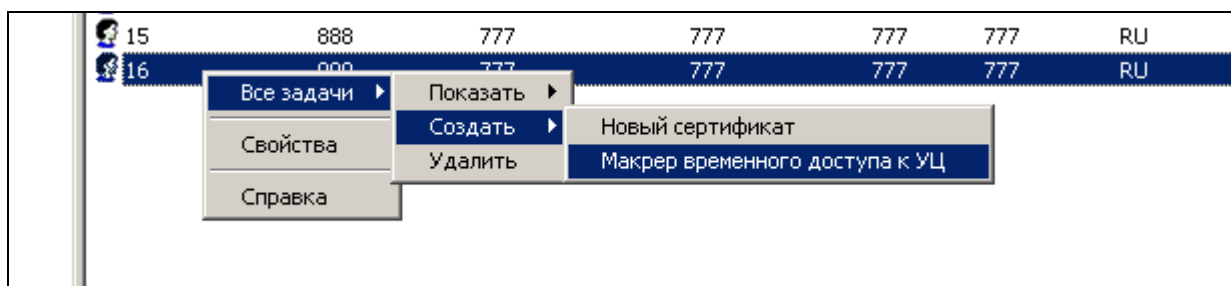


Маркер временного доступа может быть создан только зарегистрированному пользователю, у которого:

- нет ни одного действующего сертификата;
- нет ни одного запроса на сертификат, стоящего в очереди на обработку.

Для создания маркера временного доступа зарегистрированному пользователю необходимо выполнить задачу **Создать Маркер временного доступа** в приложении **АРМ администратора Центра Регистрации** (см. Рисунок 69).

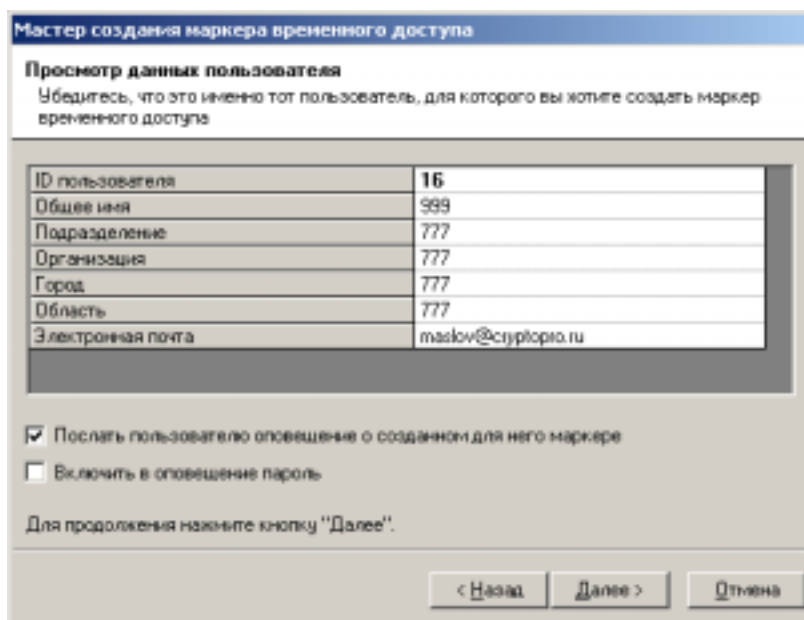
Рисунок 69. Запуск задачи создания маркера временного доступа



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

В следствии того, что создание маркера временного доступа понижает надежность системы в части аутентификации зарегистрированных пользователей, убедитесь, что выбран необходимый пользователь для данной операции (см. Рисунок 70).

Рисунок 70. Просмотр данных пользователя Мастера создания маркера временного доступа

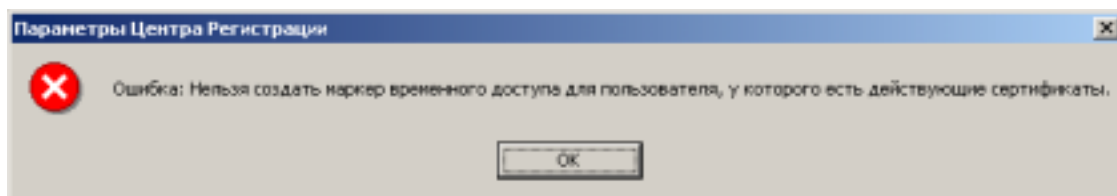


Установка опции **Послать пользователю оповещение о созданном для него маркере** обеспечивает отправку почтового сообщения в адрес пользователя с уведомлением о создании маркера доступа.

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

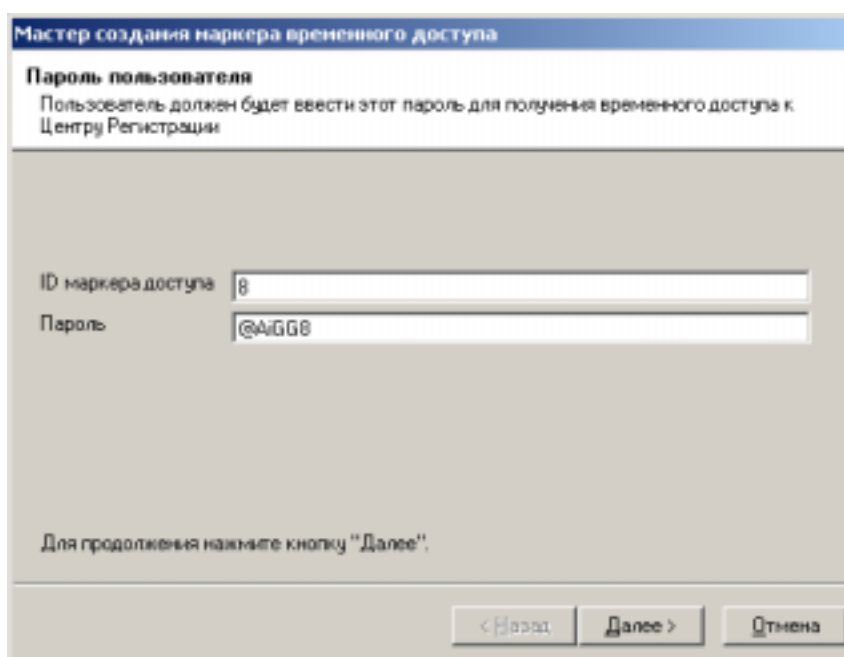
Если выбранный пользователь не удовлетворяет критериям, по которым ему может быть изготовлен маркер временного доступа, то выводится окно с сообщением об ошибке. Пример окна отображен ниже (см. Рисунок 71).

Рисунок 71. Окно ошибки о невозможности создания маркера временного доступа пользователю Мастера создания маркера временного доступа



После создания маркера временного доступа, Мастер отображает его в диалоговом окне (см. Рисунок 72).

Рисунок 72. 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**.

14. Объекты Центра Сертификации

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

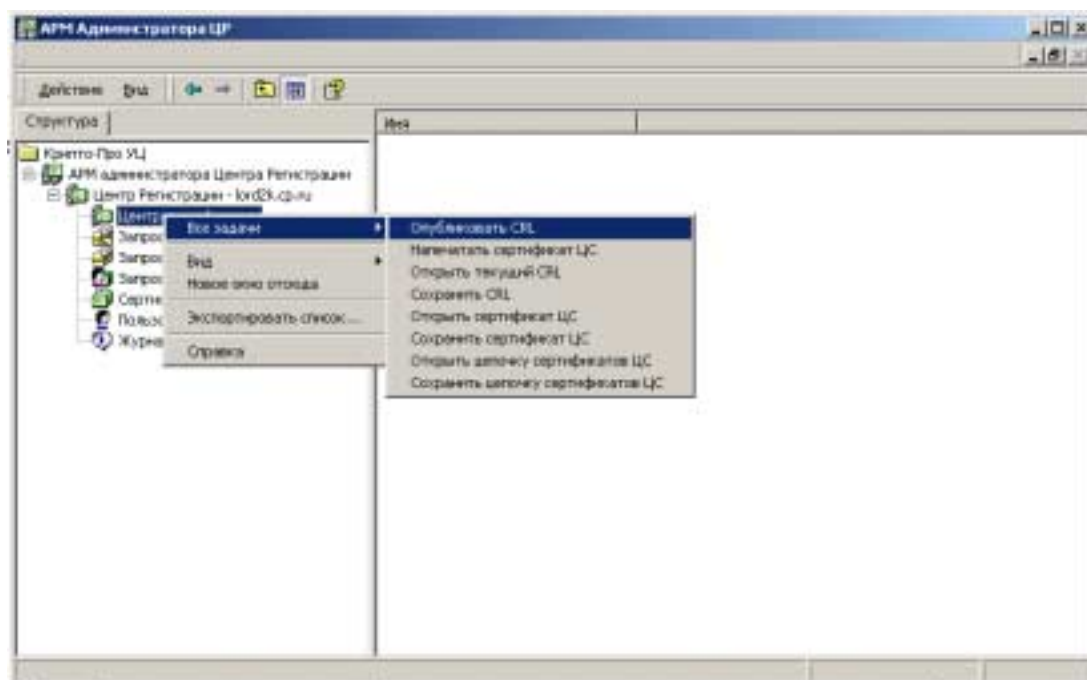
- сертификат Центра Сертификации. Данный объект представляет собой сертификат Центра Сертификации, к которому подключен Центр Регистрации из активного подключения к ЦР;
- цепочка сертификатов Центра Сертификации. Данный объект представляет собой последовательность (цепочку) сертификатов, начиная с сертификата корневого Центра Сертификации, промежуточных Центров Сертификации в иерархии и заканчивая Центром Сертификации, к которому подключен Центр Регистрации из активного подключения к ЦР;
- список отозванных (аннулированных) 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;
 - o печать – формирование формы для печати;
 - o открыть – отображение сертификата в окне свойств сертификата;
 - o сохранить – сохранение сертификата в виде файла на магнитном носителе в формате Base-64.
- цепочка сертификатов Центра Сертификации;
 - o открыть – отображение цепочки сертификатов в окне свойств цепочки сертификатов;
 - o сохранить – сохранение цепочки сертификатов в виде файла (p7b) на магнитный носитель в формате Base-64.
- список отозванных (аннулированных) сертификатов Центра Сертификации (CRL)
 - o опубликовать – создание запроса на выпуск CRL с текущей датой актуальности;
 - o открыть – отображение CRL в окне свойств списка отозванных сертификатов;
 - o 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 73).

Рисунок 73. Окно задач элемента Центр Сертификации текущего активного подключения к ЦР



15. Протоколирование работы

Программным обеспечением Центра регистрации ведется протоколирование работы УЦ в базу данных Центра регистрации.

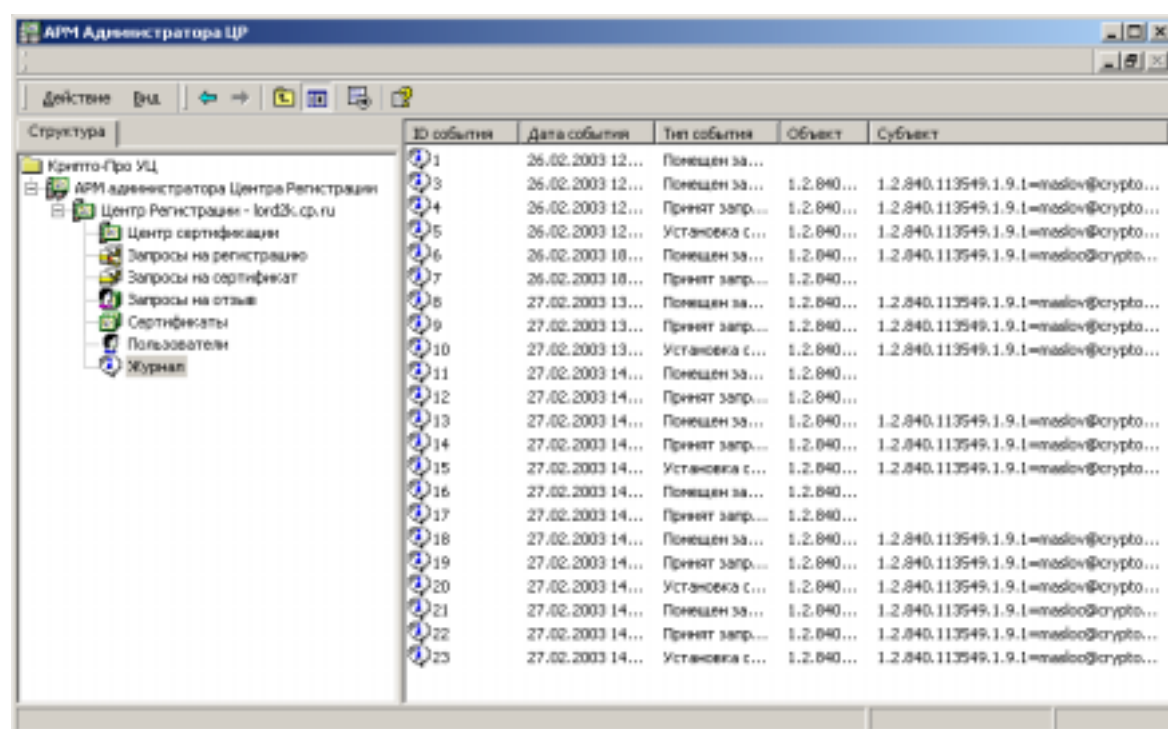
Протоколирование работы включает в себя фиксацию следующих событий:

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

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 74. 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.

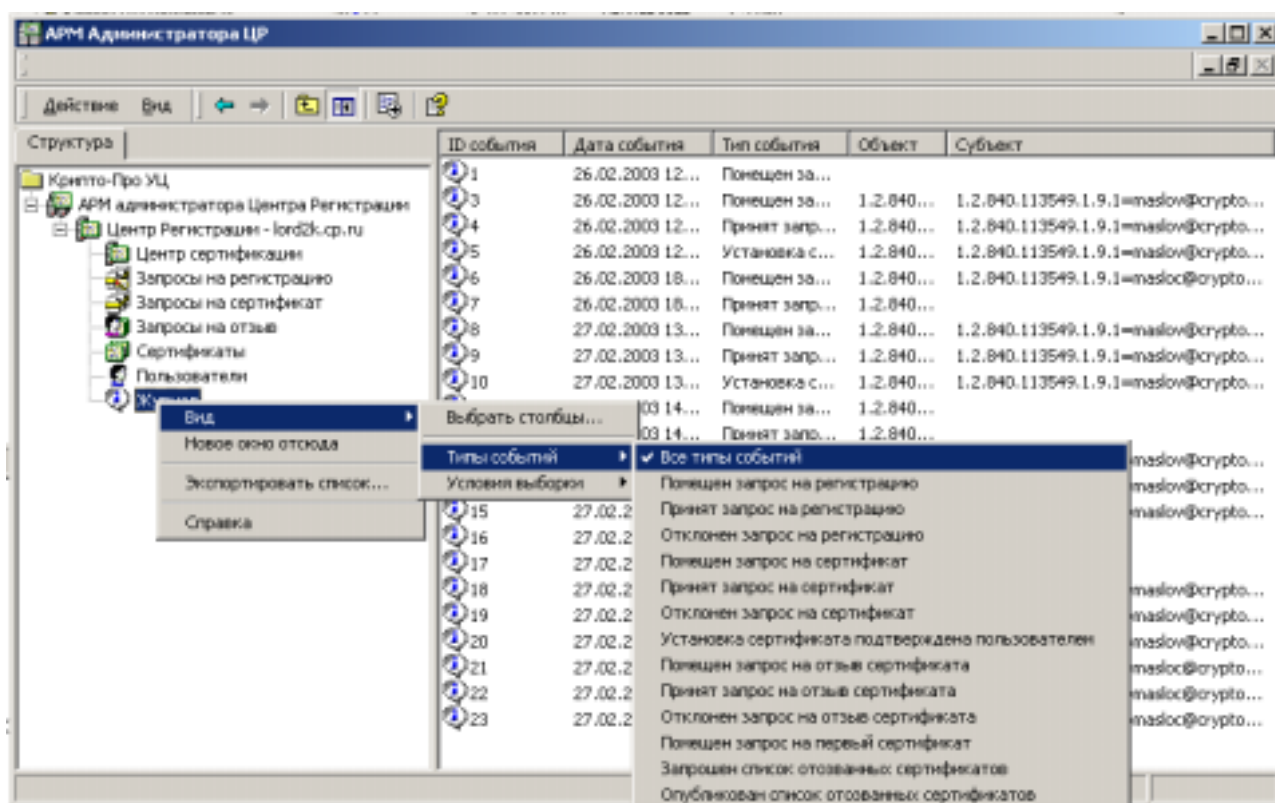
Для анализа журнала событий Центра Регистрации может использоваться фильтрация журнала, выполняемая через контекстное меню папки **Журнал** (см. Рисунок 75).

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 75. Окно задач папки Журнал



Работа с журналом регистрации событий подробно рассматривается в Разделе 18 настоящего руководства «Журнал регистрации событий Центра Регистрации»

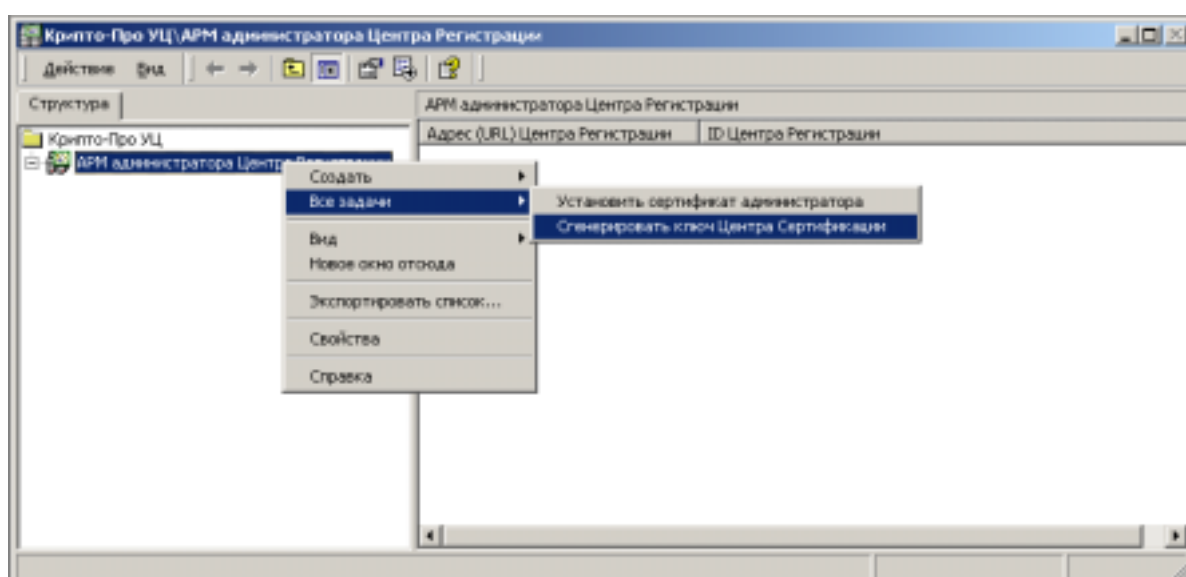
16. Генерация ключей Центра Сертификации

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 76).

Рисунок 76. Запуск задачи генерации ключей Центра Сертификации



Далее необходимо следовать указаниям Мастера создания ключа Центра Сертификации.

В окне определения параметров ключа Мастера (см. Рисунок 77) выберите алгоритм формирования ключа (список CSP). Появление данного окна зависит от параметра **Разрешить выбор CSP** окна свойств АРМ (см. Рисунок 20).

Рисунок 77. Окно определения параметров ключа Мастера создания ключа ЦС

The screenshot shows a window titled "Мастер создания ключа Центра Сертификации". The main heading is "Параметры ключа" with the instruction "Установите параметры ключа". Below this, a text box says "Выберите криптопровайдер из приведенного списка. Укажите требуемый размер ключа и алгоритм хеширования." There are three dropdown menus: "CSP" set to "Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider", "Размер ключа" set to "512" (with "Мин: 512" and "Макс: 512" labels), and "Алгоритм хеширования" set to "GOST R 34.11-94". At the bottom, there are two checkboxes: "Включить усиленную защиту закрытого ключа" (unchecked) and "Пометить ключи как экспортируемые" (checked). Navigation buttons at the bottom right are "< Назад", "Далее >", and "Отмена".

В следующем окне Мастера необходимо задать имя создаваемого ключевого контейнера для ключей ЦС (см. Рисунок 78).

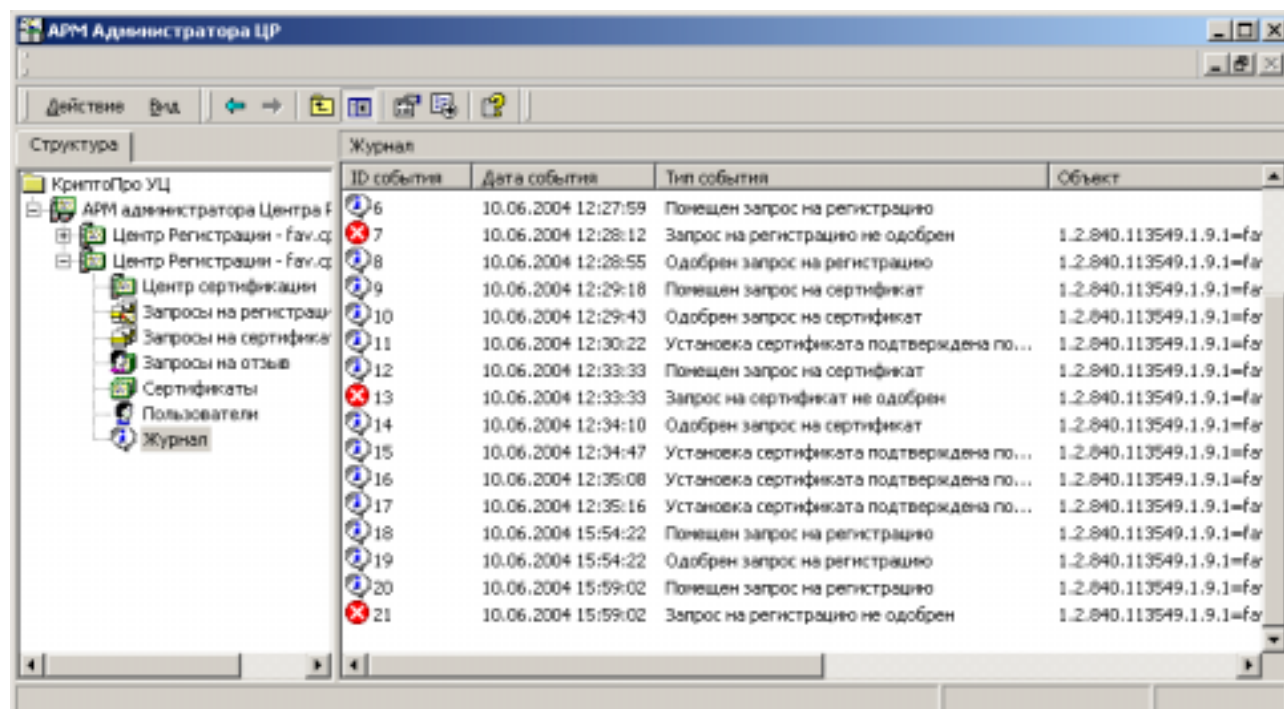
Рисунок 78. Окно определения имени ключевого контейнера Мастера создания ключа ЦС

The screenshot shows a window titled "Мастер создания ключа Центра Сертификации". The main heading is "Имя ключевого контейнера" with the instruction "Задайте имя ключевого контейнера". Below this, a text box labeled "Имя контейнера" contains the text "Test CA". At the bottom right, there are navigation buttons: "< Назад", "Далее >", and "Отмена".

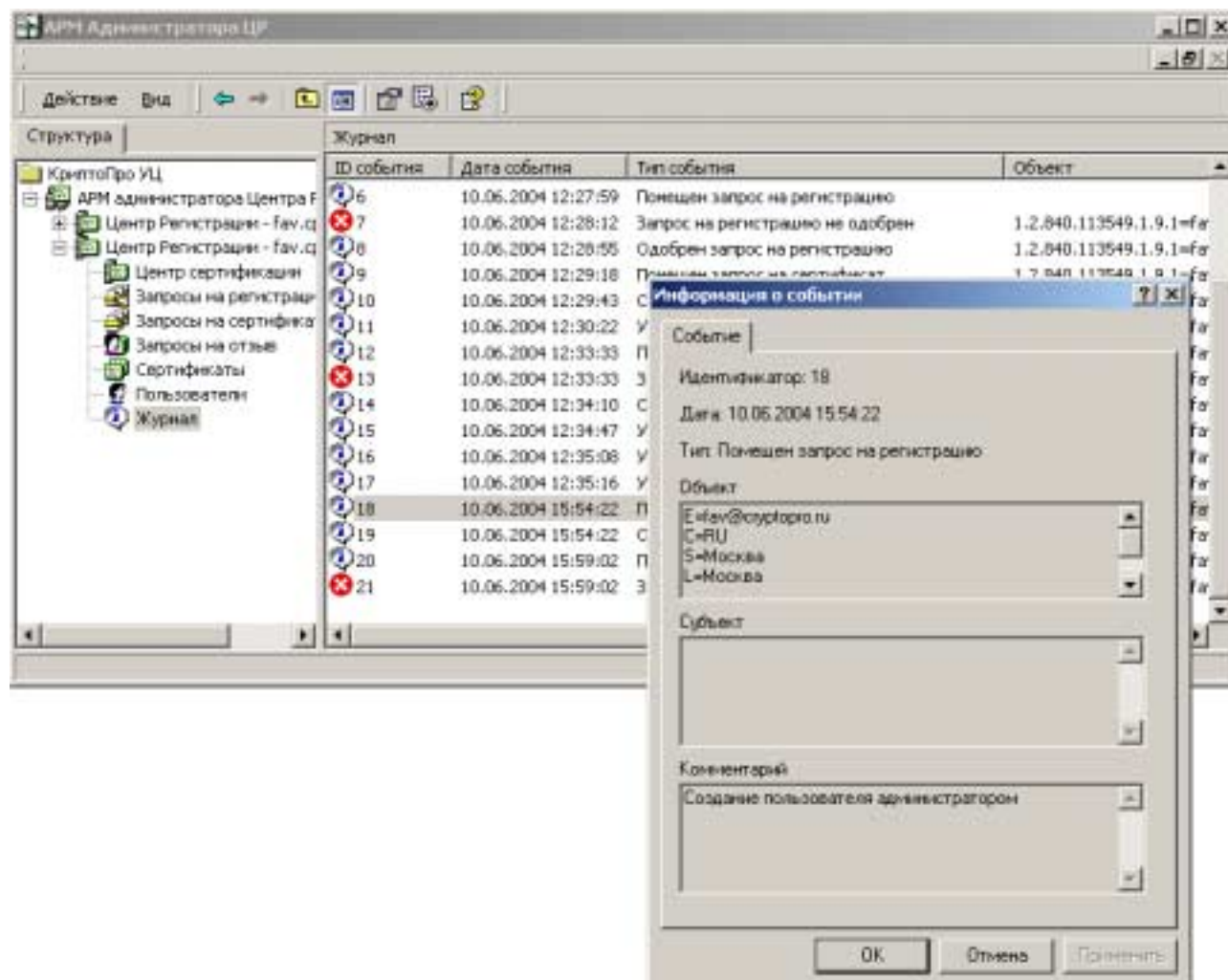
17. Журнал регистрации событий Центра Регистрации

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 79. 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 80. 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,

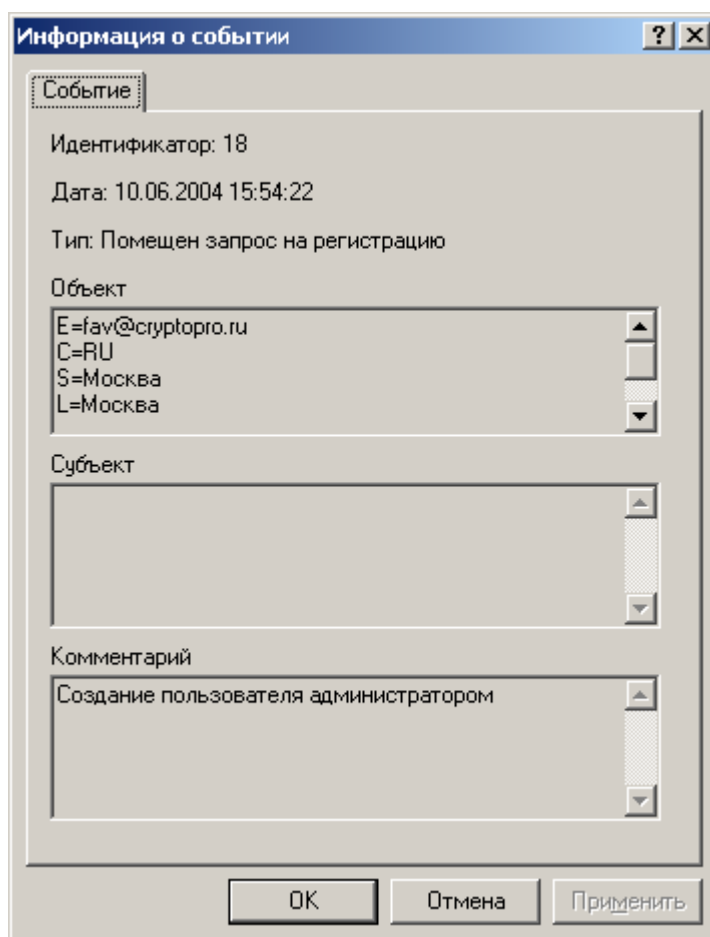
либо при выполнении Администратором задачи Центра Сертификации «Опубликовать текущий CRL» событие «Опубликован список отозванных сертификатов» не содержит значения поля Субъект, поскольку список отозванных сертификатов не принадлежит к объекту управления какого-либо зарегистрированного пользователя.

17.1. 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 регистрирующим 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 81. Событие Помещен запрос на регистрацию



- **Одобен 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 82. Событие Одобрен запрос на регистрацию

Информация о событии

Событие

Идентификатор: 19

Дата: 10.06.2004 15:54:22

Тип: Одобрен запрос на регистрацию

Объект

S=Москва
L=Москва
O=Крипто-Про
CN=Оператор ЦР

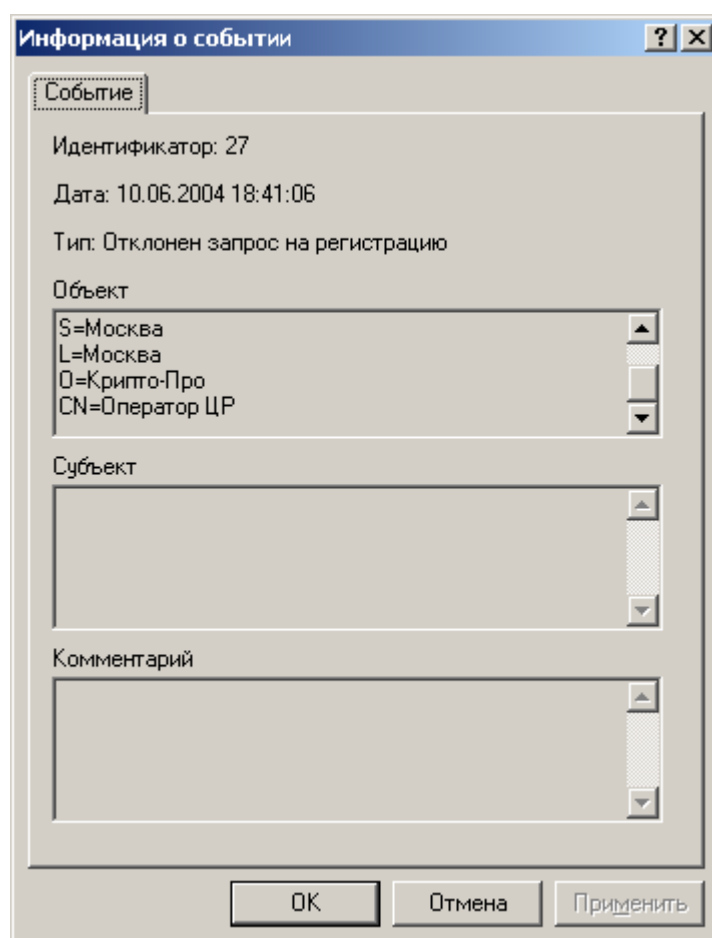
Субъект

Комментарий

OK Отмена Применить

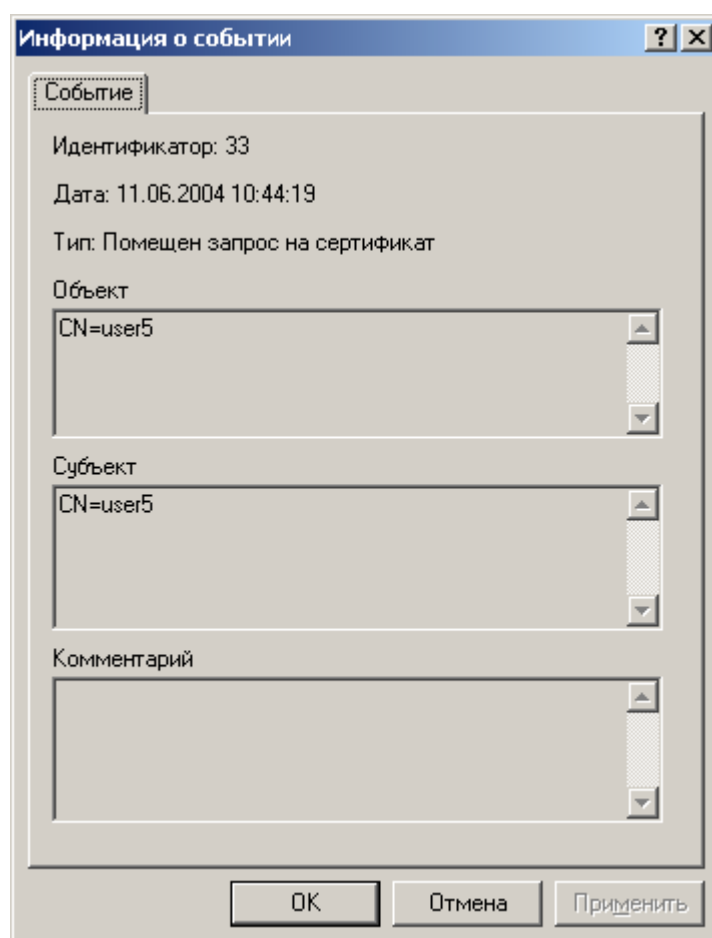
- **Отклонен запрос на регистрацию** – данное событие возникает при успешном выполнении метода `Registration.DenyRequest` (важность события – предупреждение). Поле Объект данного события содержит идентификационные данные пользователя выполнившего указанный метод.

Рисунок 83. 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 84. Событие Помещен запрос на сертификат



Информация о событии

Событие

Идентификатор: 33

Дата: 11.06.2004 10:44:19

Тип: Помещен запрос на сертификат

Объект

CN=user5

Субъект

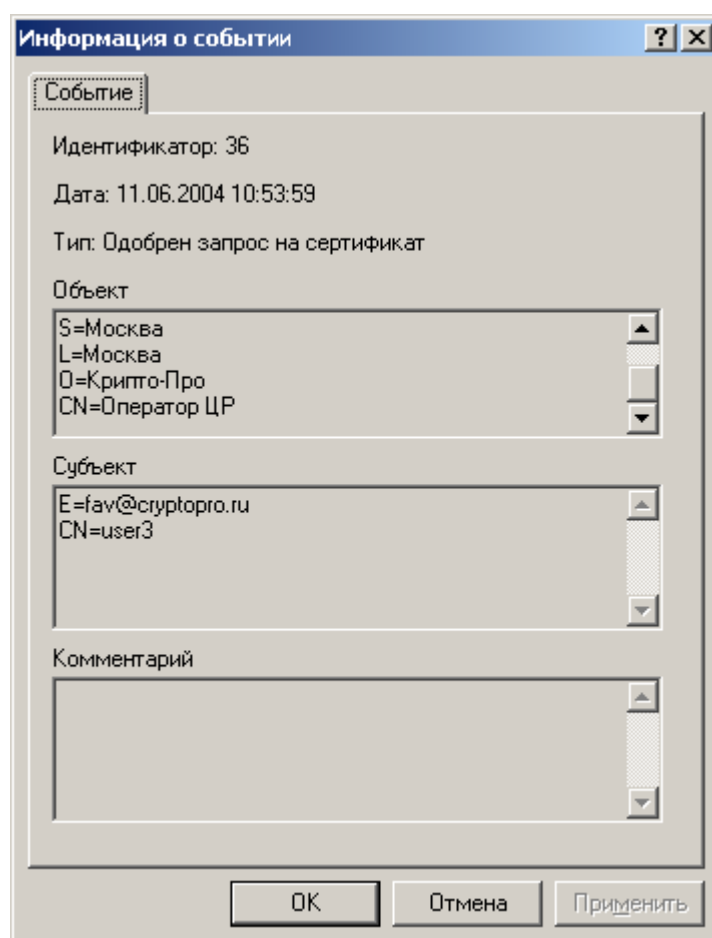
CN=user5

Комментарий

OK Отмена Применить

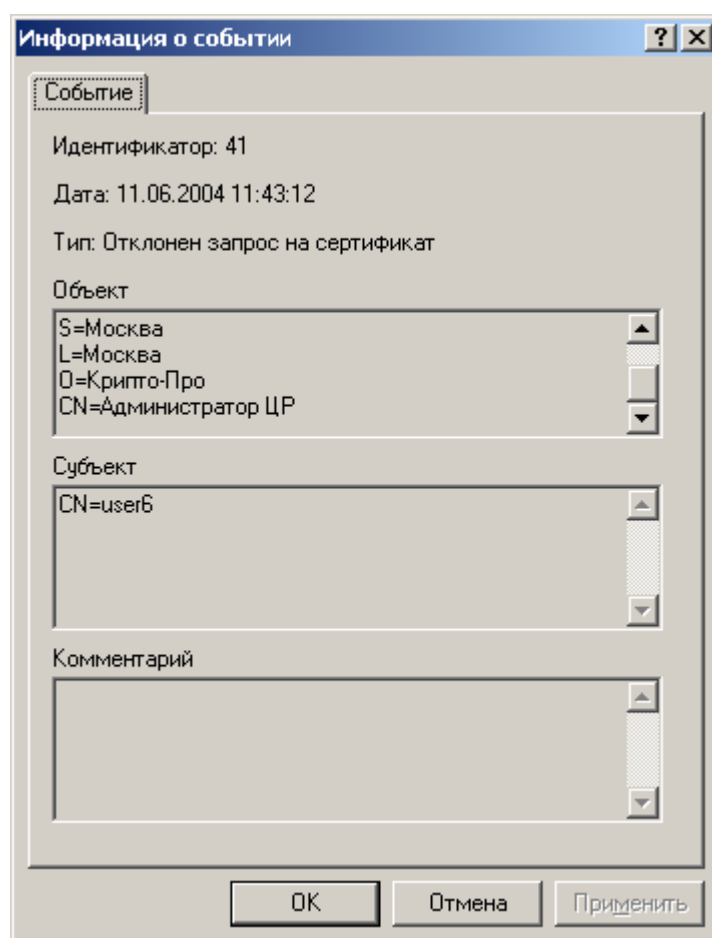
- **Одобен запрос на сертификат** - данное событие возникает при успешном выполнении метода CertRequest.AcceptRequest и CertRequest.AcceptFirstRequest (важность события – обычная). Поле Объект данного события содержит идентификационные данные пользователя, выполнившего указанный метод, поле Субъект –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

Рисунок 85. 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 86. Событие Отклонен запрос на сертификат



Информация о событии

Событие

Идентификатор: 41

Дата: 11.06.2004 11:43:12

Тип: Отклонен запрос на сертификат

Объект

S=Москва
L=Москва
O=Крипто-Про
CN=Администратор ЦР

Субъект

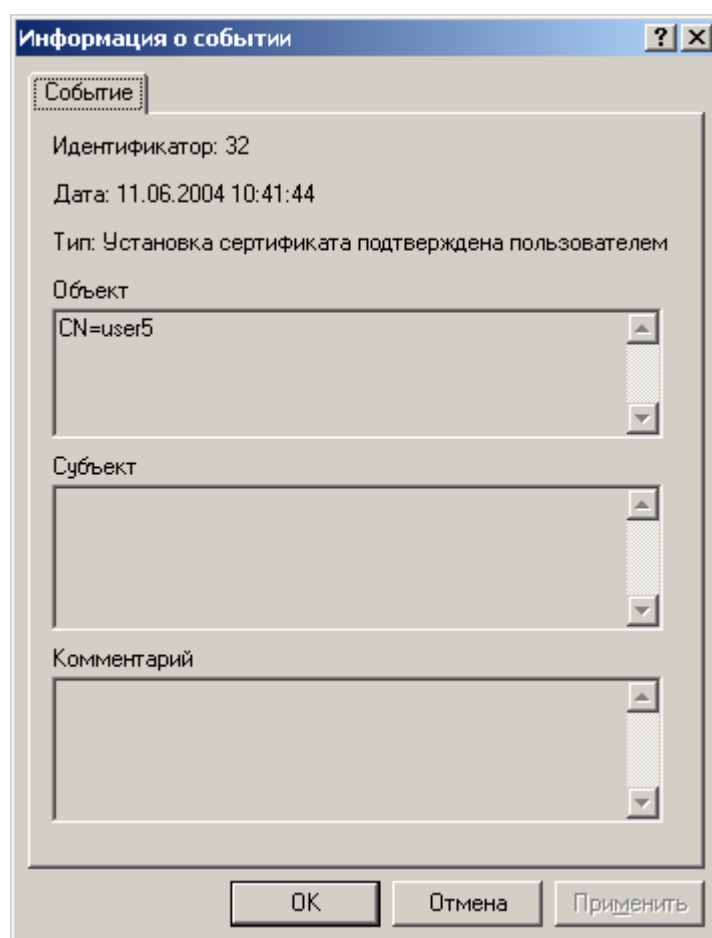
CN=user6

Комментарий

OK Отмена Применить

- **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 87. 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 88. Событие Помещен запрос на отзыв сертификата

Информация о событии

Событие

Идентификатор: 44

Дата: 11.06.2004 12:55:57

Тип: Помещен запрос на отзыв сертификата

Объект

S=Москва
L=Москва
O=Крипто-Про
CN=Оператор ЦР

Субъект

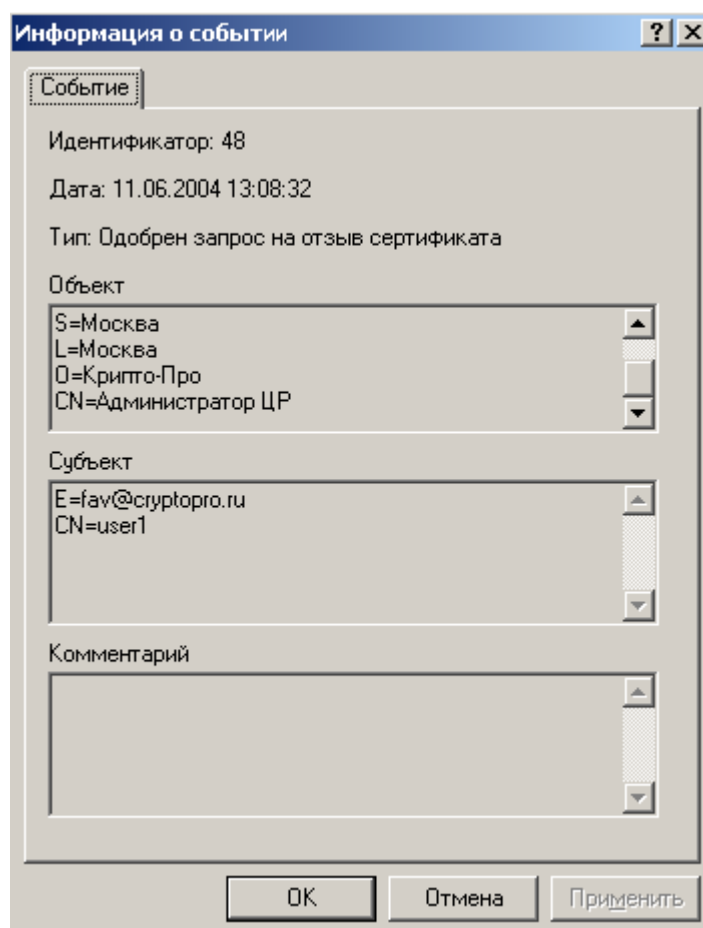
E=fav@cryptopro.ru
CN=user1

Комментарий

OK Отмена Применить

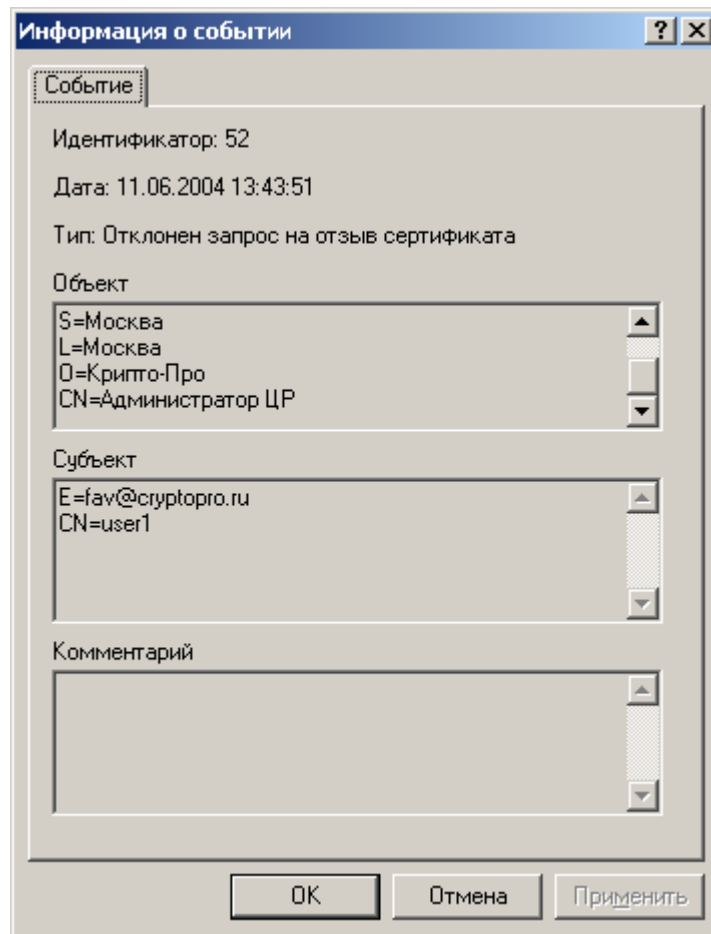
- **Одобен запрос на отзыв сертификата** - данное событие возникает при успешном выполнении метода `RevokeRequest.AcceptRequest` (важность события – обычная). Поле Объект данного события содержит идентификационные данные пользователя, выполнившего указанный метод, поле Субъект – идентификационные данные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

Рисунок 89. 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;

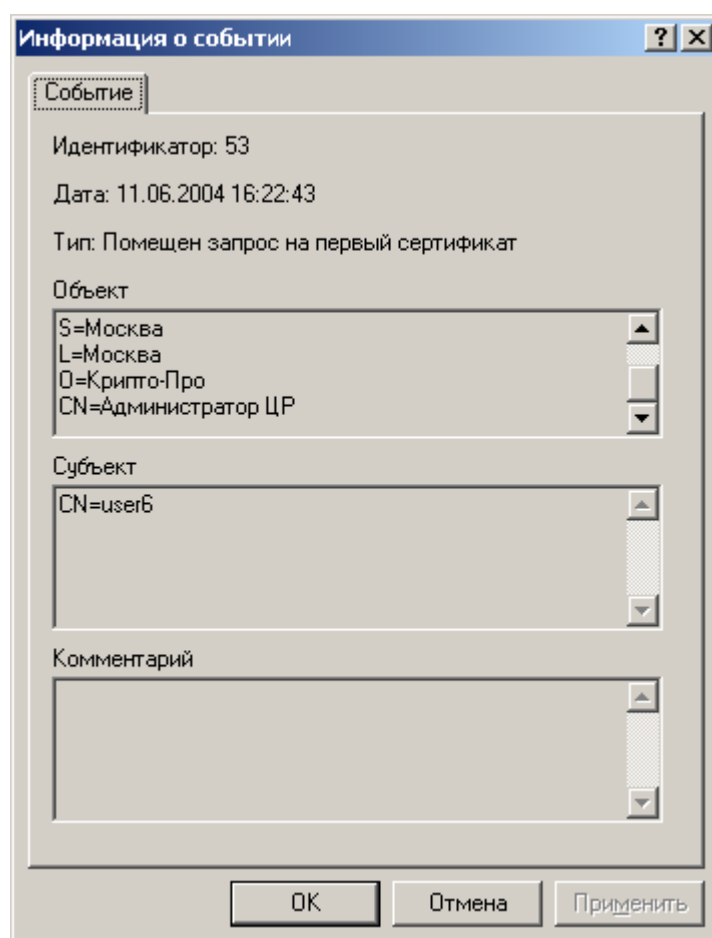
Рисунок 90. Событие Отклонен запрос на отзыв сертификата



Описанные события «Помещен запрос на отзыв сертификата», «Одобен 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

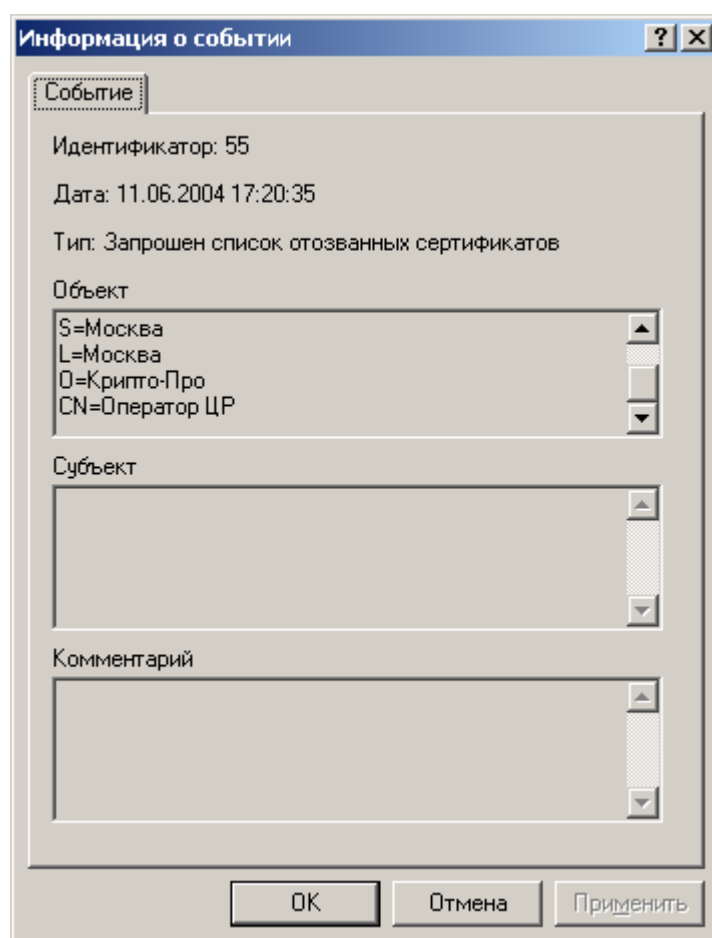
- **Помещен запрос на первый сертификат** - данное событие возникает при успешном выполнении метода CertRequest.SubmitFirstRequest (важность события – обычная). Обработка метода CertRequest.SubmitFirstRequest осуществляется в соответствии с политикой «Обработка неподписанных запросов». В связи с этим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

Рисунок 91. Событие Помещен запрос на первый сертификат



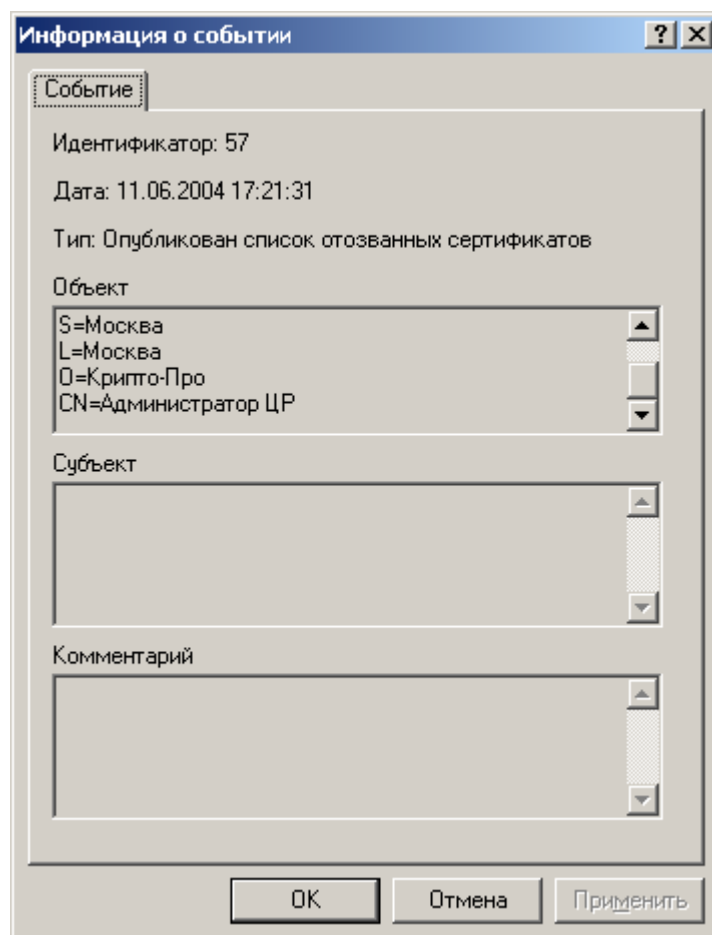
- **Запрошен список отозванных сертификатов** - данное событие возникает при успешном выполнении метода CertView.GetCRL (важность события – обычная). Поле Объект данного события содержит идентификационные данные пользователя, запросившего список отозванных сертификатов;

Рисунок 92. 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 93. Событие Опубликован список отозванных сертификатов



Информация о событии

Событие

Идентификатор: 57

Дата: 11.06.2004 17:21:31

Тип: Опубликован список отозванных сертификатов

Объект

S=Москва
L=Москва
O=Крипто-Про
CN=Администратор ЦР

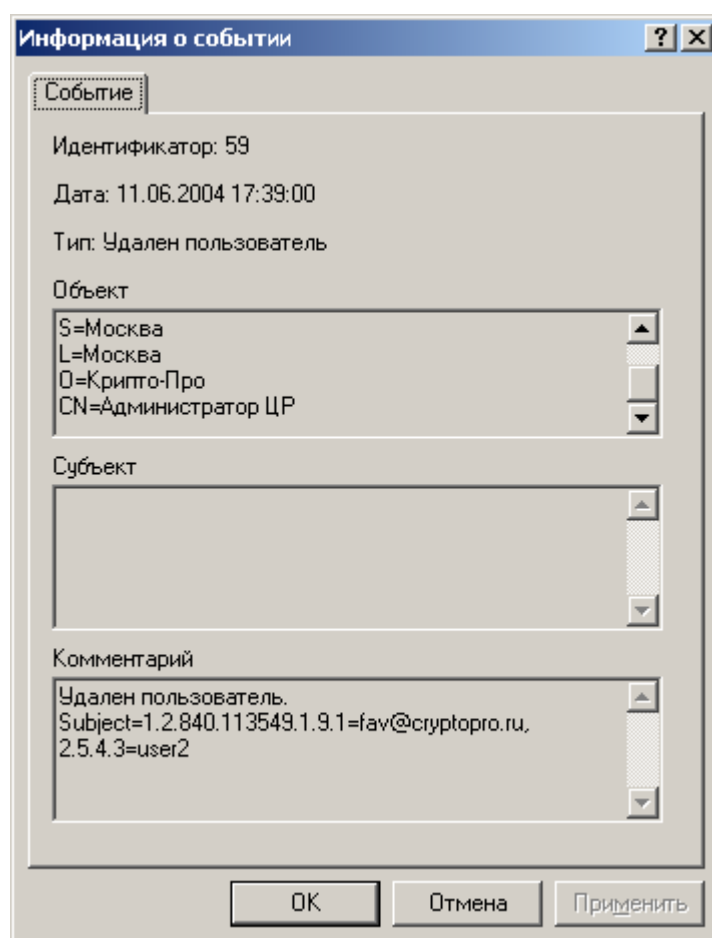
Субъект

Комментарий

OK Отмена Применить

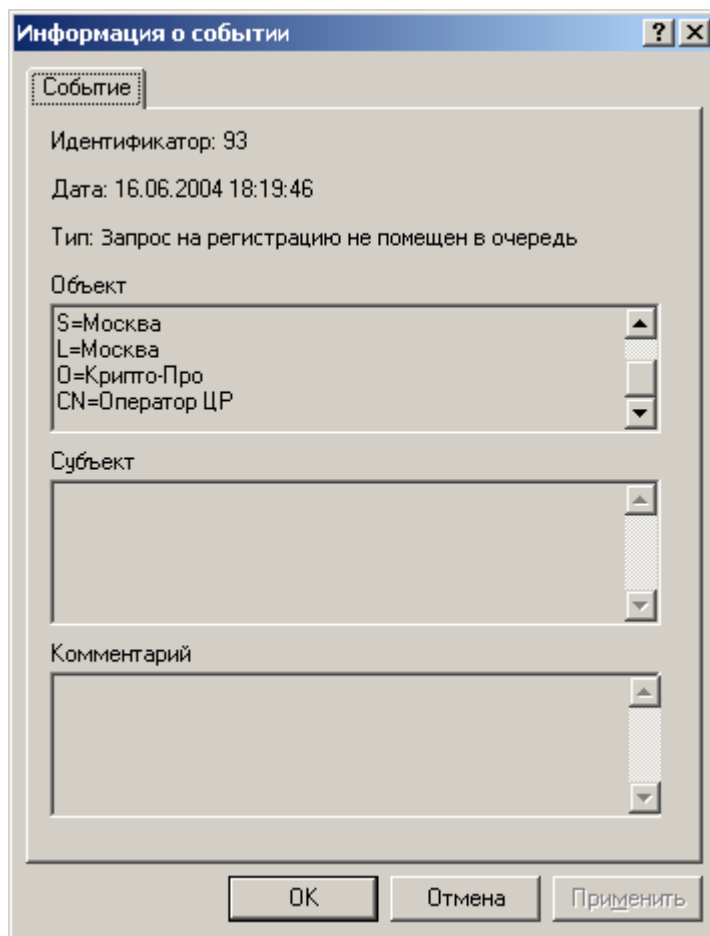
- **Удален пользователь** - данное событие возникает при успешном выполнении метода UserView.DeleteUser (важность события – обычная). Поле Объект данного события содержит идентификационные данные пользователя, выполнившего удаление учетной записи пользователя, поле Комментарий – идентификационные данные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

Рисунок 94. 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 95. Событие Запрос на регистрацию не помещен в очередь



Информация о событии

Событие

Идентификатор: 93

Дата: 16.06.2004 18:19:46

Тип: Запрос на регистрацию не помещен в очередь

Объект

S=Москва
L=Москва
O=Крипто-Про
CN=Оператор ЦР

Субъект

Комментарий

OK Отмена Применить

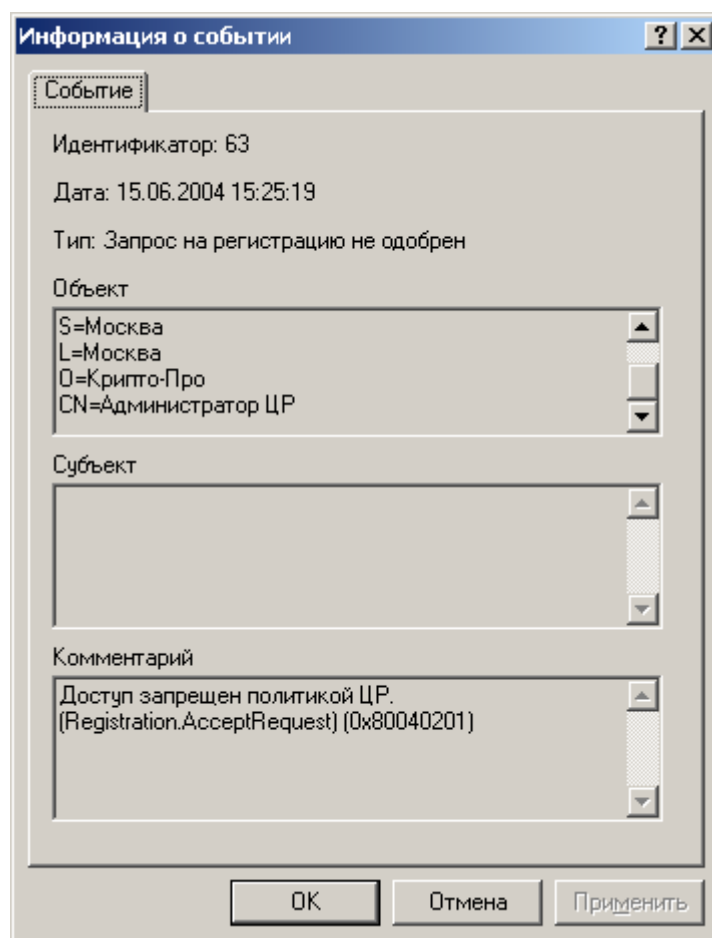


Здесь и далее использование выражения «важность события – ошибка» не означает регистрацию в системе ошибки при работе АРМ Администратора ЦР (такого рода сообщения отображаются в журнале приложений операционной системы). Возникновение таких событий происходит по причине настроек политик Центра Регистрации.

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 96. Событие Запрос на регистрацию не одобрен



Информация о событии ? X

Событие

Идентификатор: 63

Дата: 15.06.2004 15:25:19

Тип: Запрос на регистрацию не одобрен

Объект

S=Москва
L=Москва
O=Крипто-Про
CN=Администратор ЦР

Субъект

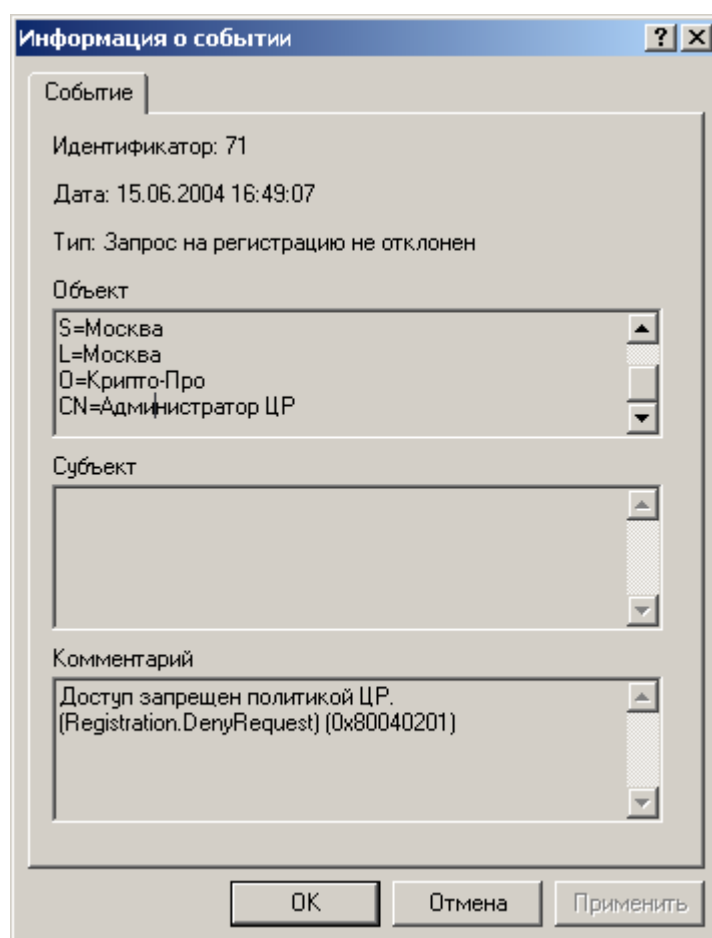
Комментарий

Доступ запрещен политикой ЦР.
(Registration.AcceptRequest) (0x80040201)

OK Отмена Применить

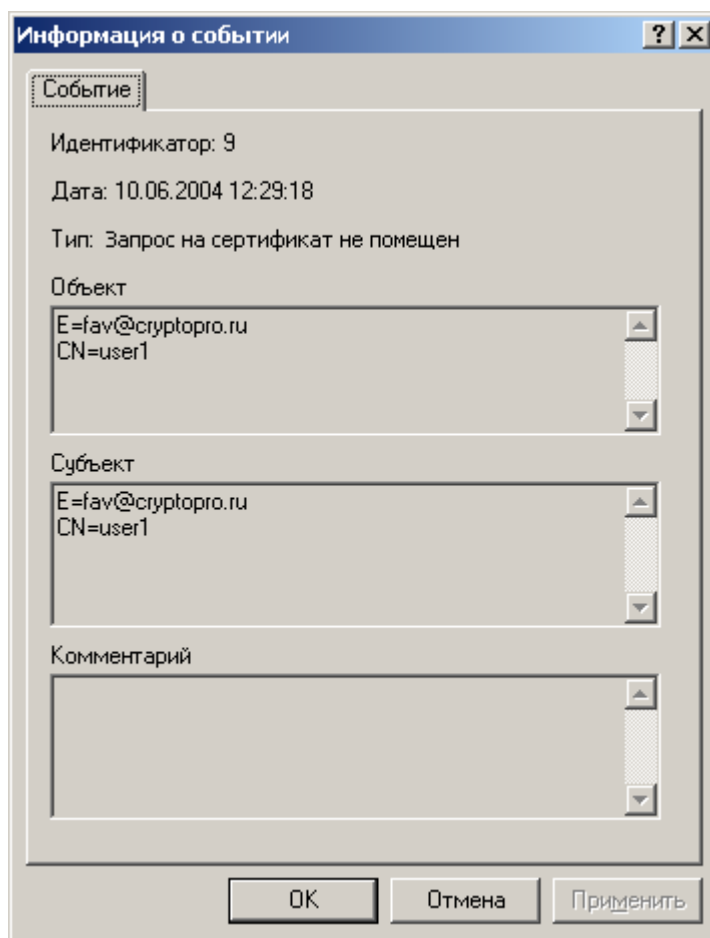
- **Запрос на регистрацию не отклонен** - данное событие возникает при выполнении метода `Registration.DenyRequest` в том случае, если успешное выполнение указанного метода противоречит настройкам политик Центра Регистрации (важность события – ошибка). Поле Объект данного события содержит идентификационные 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 97. 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 98. Событие Запрос на сертификат не помещен



Информация о событии

Событие

Идентификатор: 9

Дата: 10.06.2004 12:29:18

Тип: Запрос на сертификат не помещен

Объект

E=fav@cryptopro.ru
CN=user1

Субъект

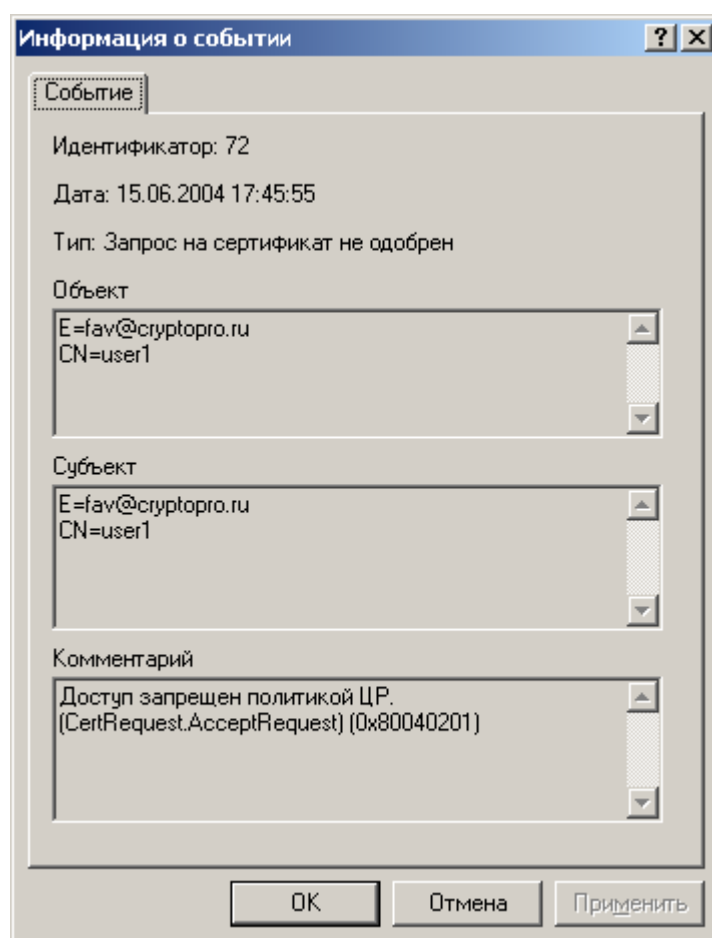
E=fav@cryptopro.ru
CN=user1

Комментарий

OK Отмена Применить

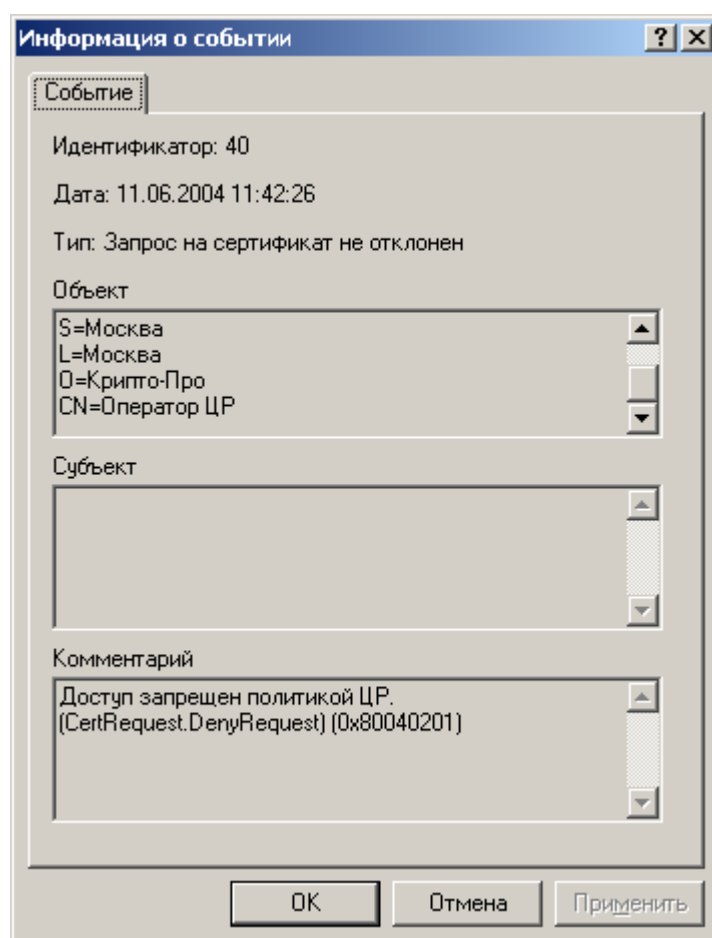
- **Запрос на сертификат не одобрен** - данное событие возникает при выполнении методов CertRequest.AcceptRequest и CertRequest.AcceptFirstRequest в том случае, если успешное выполнение пользователем одного из указанных методов противоречит настройкам политик Центра Регистрации (важность события – ошибка). 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 99. Событие Запрос на сертификат не одобрен



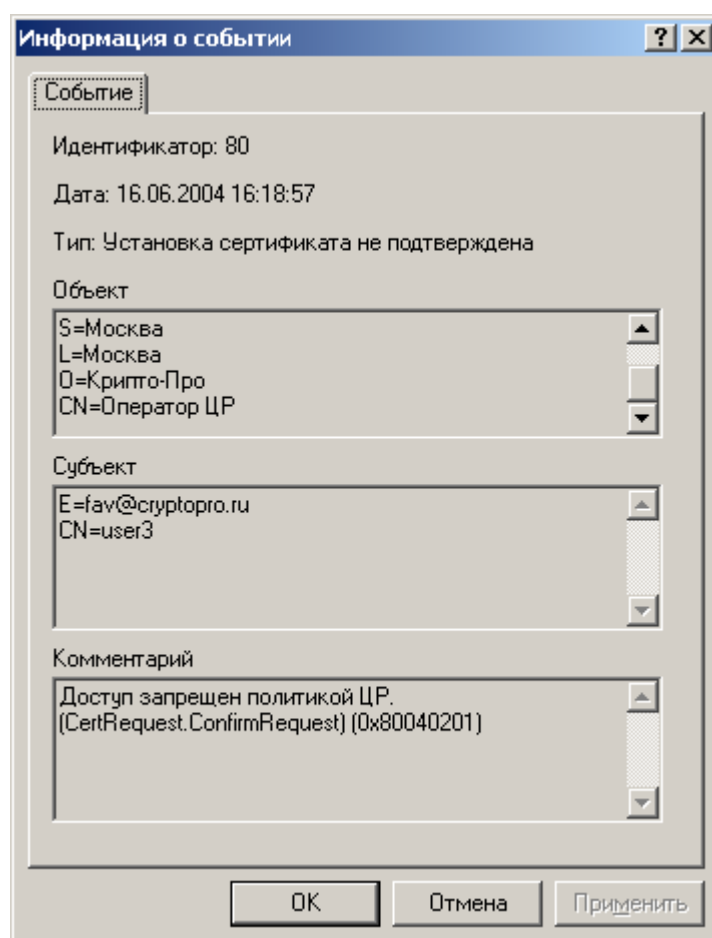
- **Запрос на сертификат не отклонен** - данное событие возникает при выполнении метода `CertRequest.DenyRequest` в том случае, если успешное выполнение пользователем данного метода противоречит настройкам политик Центра Регистрации (важность события – ошибка). Поле Объект данного события содержит идентификационные 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 100. 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 101. 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 102. Событие Запрос на отзыв сертификата не помещен

Информация о событии

Событие

Идентификатор: 84

Дата: 16.06.2004 16:30:00

Тип: Запрос на отзыв сертификата не помещен

Объект

S=Москва
L=Москва
O=Крипто-Про
CN=Оператор ЦР

Субъект

E=fav@cryptopro.ru
CN=user1

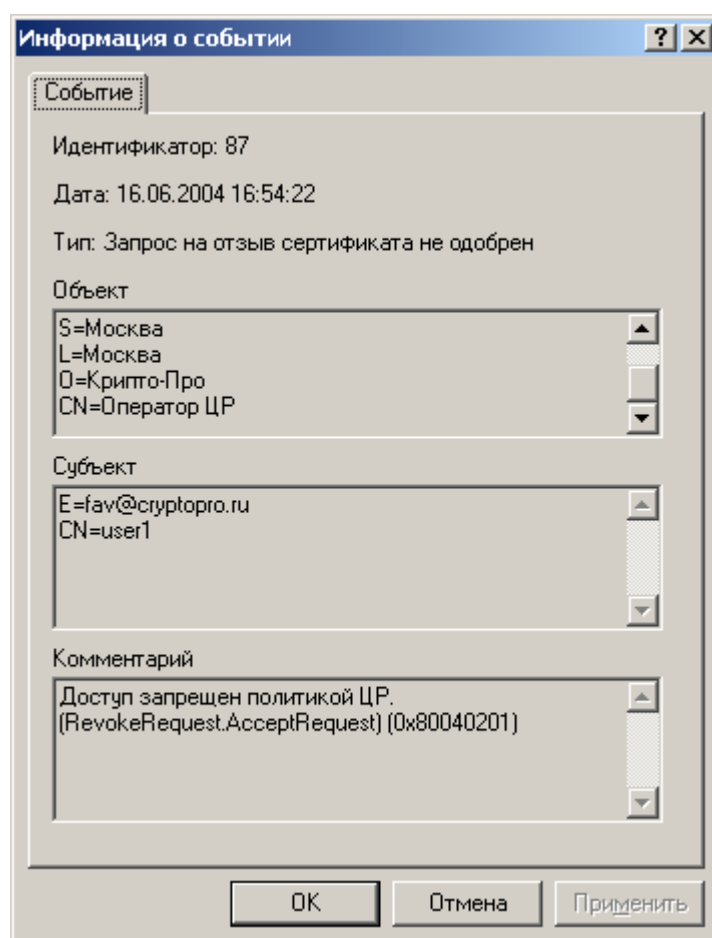
Комментарий

Доступ запрещен политикой ЦР.
(RevokeRequest.SubmitRequest) (0x80040201)

OK Отмена Применить

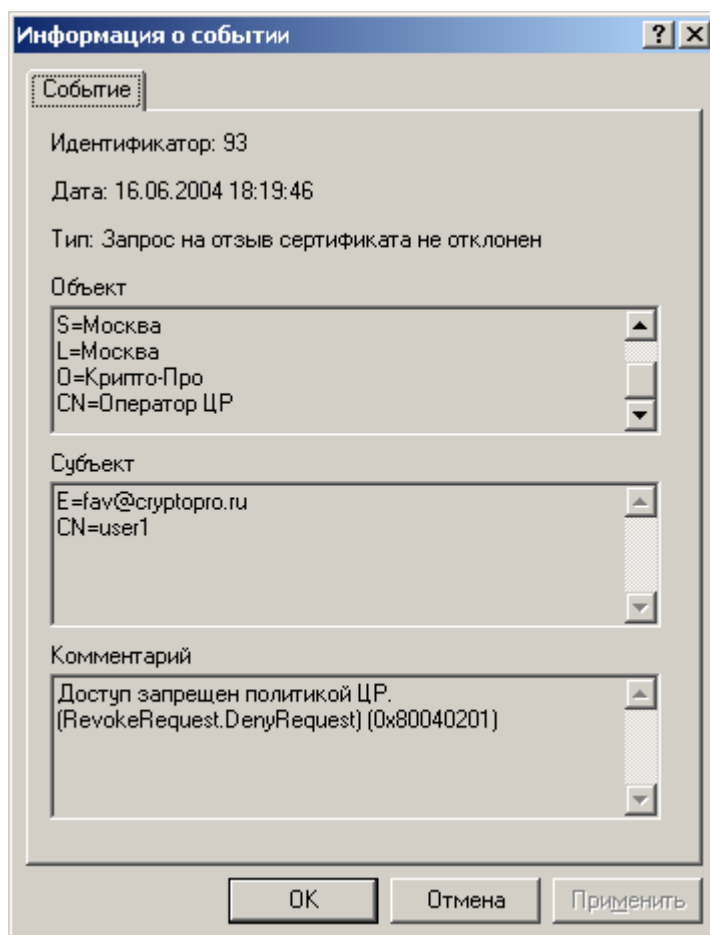
- **Запрос на отзыв сертификата не одобрен** - данное событие возникает при выполнении метода `RevokeRequest.AcceptRequest` в том случае, если успешное выполнение пользователем данного метода противоречит настройкам политик Центра Регистрации (важность события – ошибка). Поле Объект данного события содержит 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 103. 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;

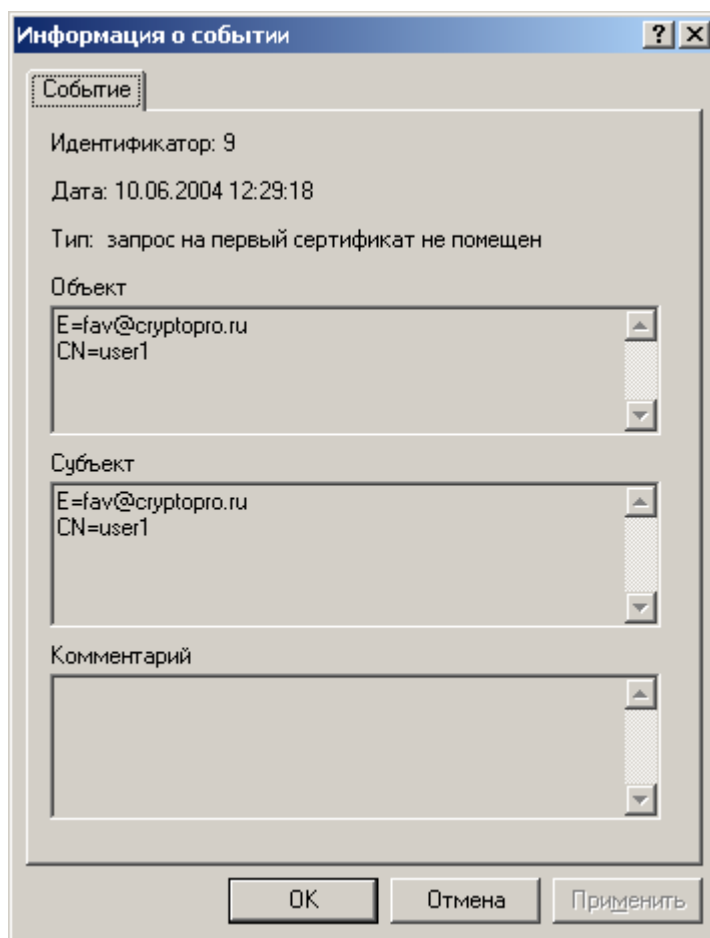
Рисунок 104. Событие Запрос на отзыв сертификата не отклонен



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

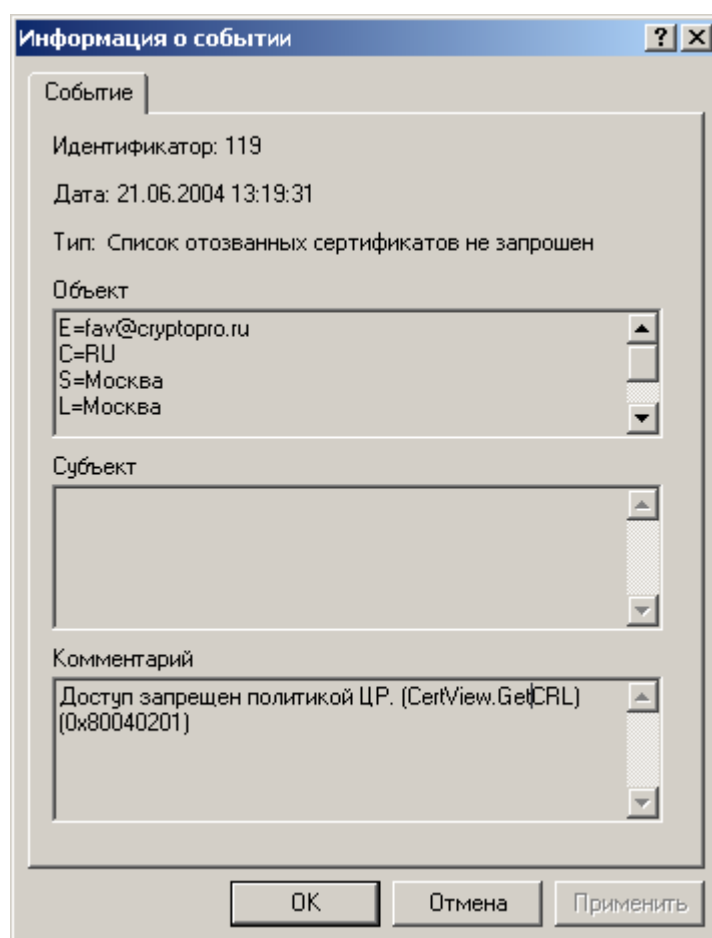
- **Запрос на первый сертификат не помещен** - данное событие возникает при выполнении метода CertRequest.SubmitFirstRequest в том случае, если успешное выполнение указанного метода противоречит настройкам политик Центра Регистрации (важность события – ошибка). Обработка метода CertRequest.SubmitFirstRequest 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 105. Событие Запрос на первый сертификат не помещен



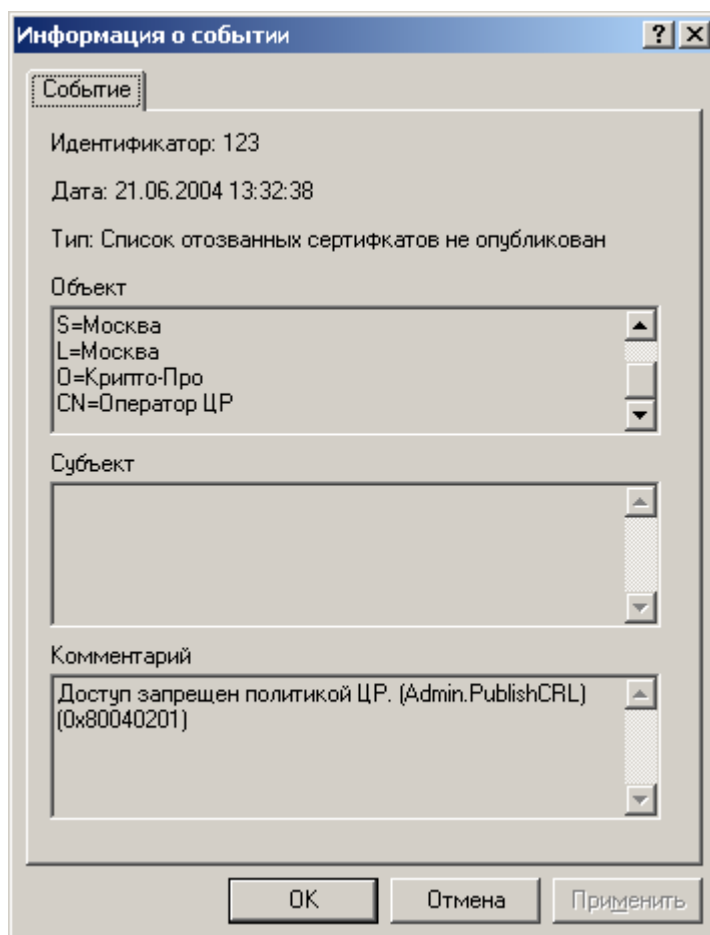
- **Список отозванных сертификатов не запрошен** - данное событие возникает при выполнении метода CertView.GetCRL в том случае, если успешное выполнение указанного метода противоречит настройкам политик Центра Регистрации (важность события – ошибка). Поле Объект данного события содержит идентификационные 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 106. Событие Список отозванных сертификатов не запрошен



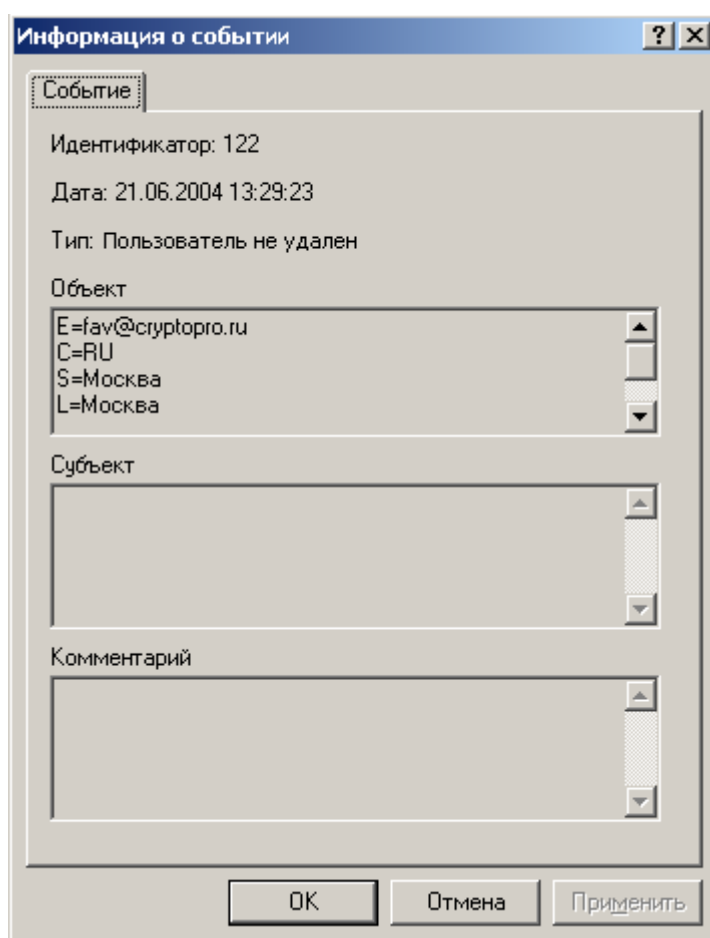
- **Список отозванных сертификатов не опубликован** - данное событие возникает при выполнении метода Admin.PublishCRL в том случае, если успешное выполнение указанного метода противоречит настройкам политик Центра Регистрации (важность события – ошибка). Поле Объект данного события содержит идентификационные 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 107. Событие Список отозванных сертификатов не опубликован



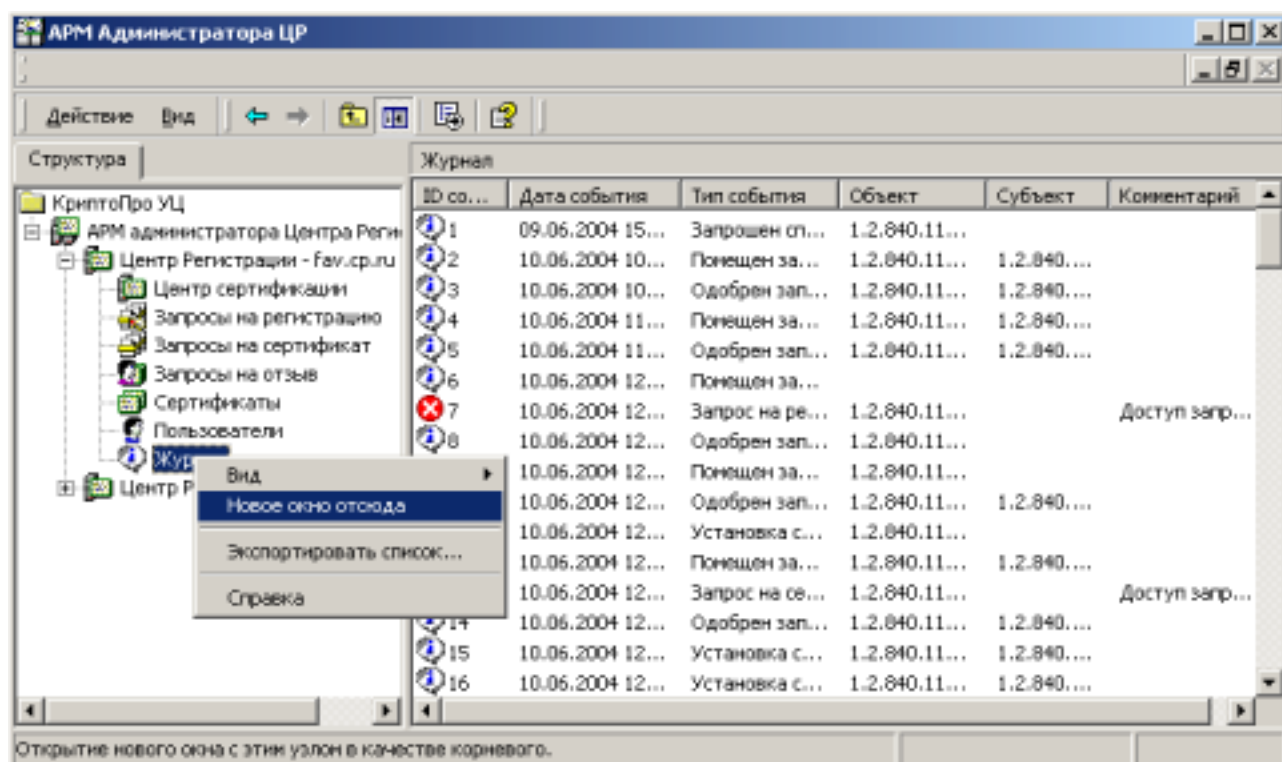
- **Пользователь не удален** - данное событие возникает при выполнении метода UserView.DeleteUser в том случае, если успешное выполнение указанного метода противоречит настройкам политик Центра Регистрации (важность события – ошибка). Поле Объект данного события содержит идентификационные данные пользователя,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

Рисунок 108. Событие Пользователь не удален

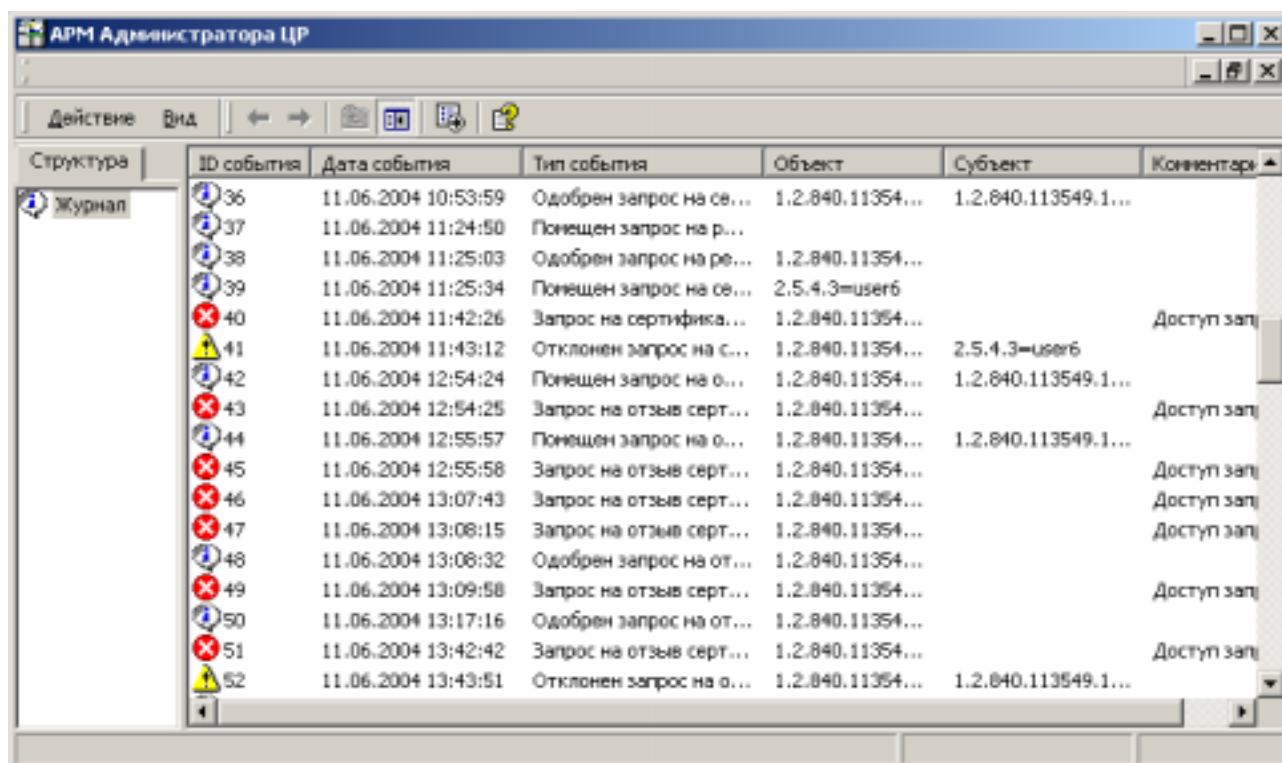


17.2. Работа с Журналом регистрации событий

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 109. Выбор режима просмотра записей Журнала в новом окне

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

Рисунок 110. Просмотр Журнала регистрации событий в отдельном окне

Каждое событие **Журнала** регистрации событий представляет из себя 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 111. Вызов окна "Изменить столбцы"

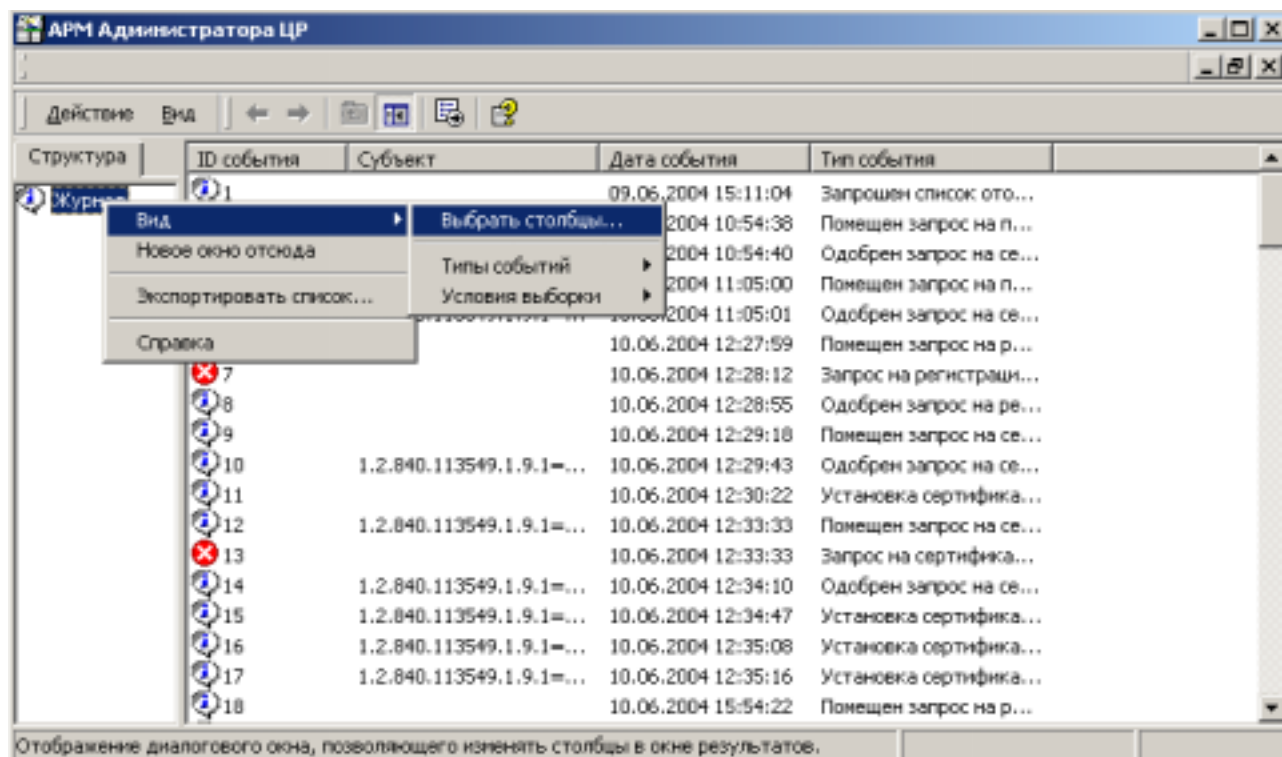
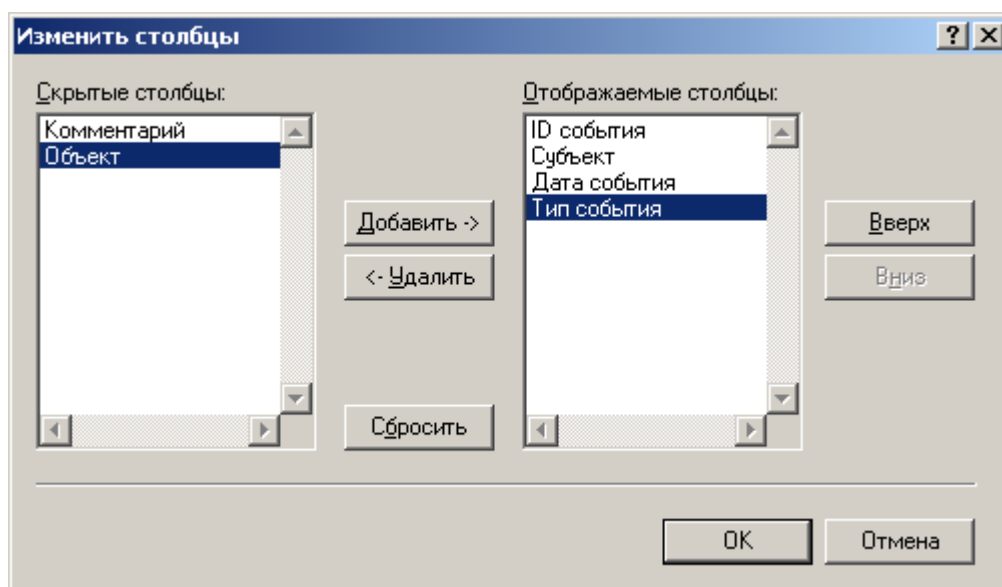


Рисунок 112. Окно Изменить столбцы



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».

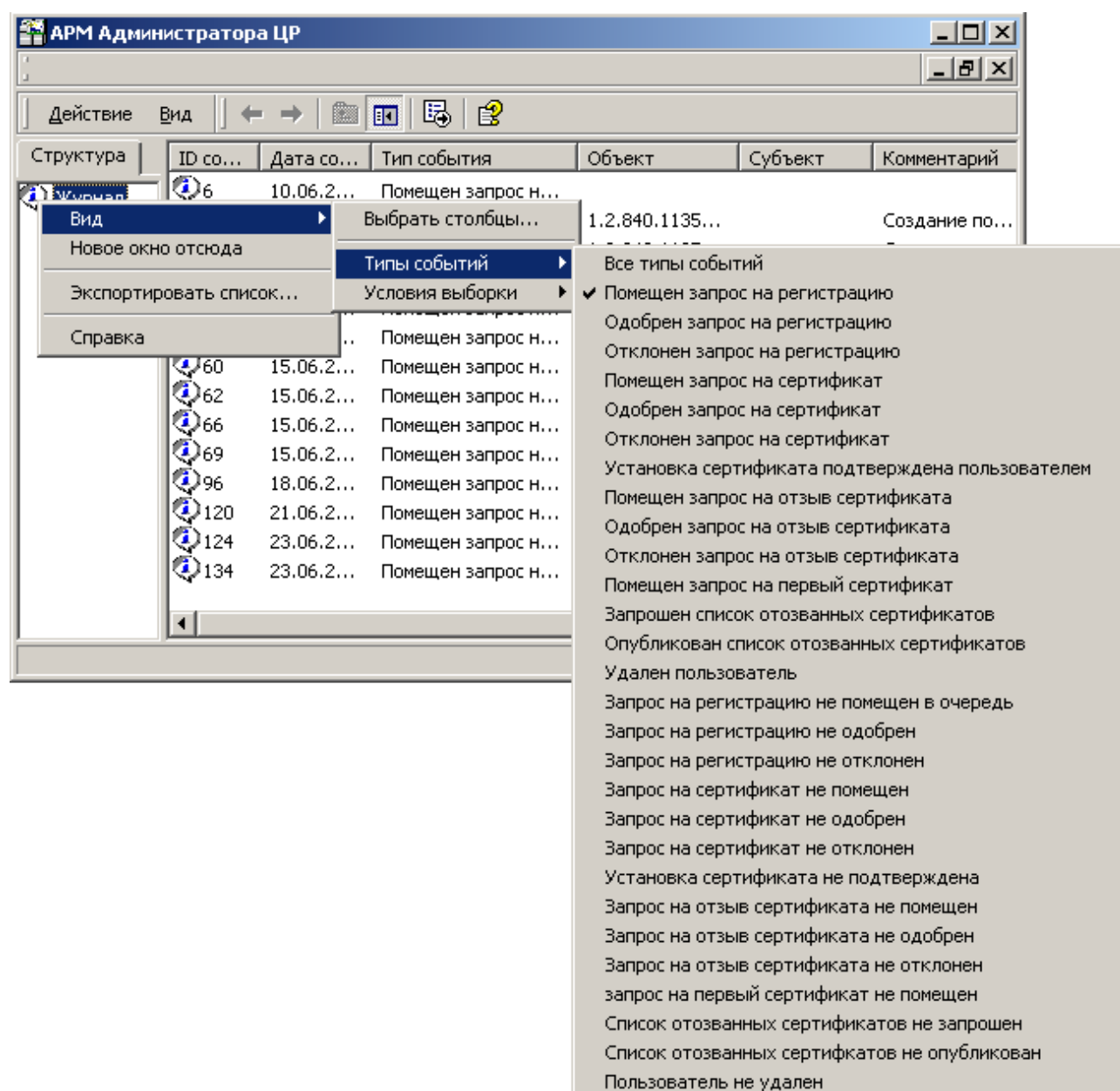
При нажатии на кнопку «Удалить» выделенное в списке «Отображаемые столбцы» наименование столбца будет удалено из указанного списка и добавлено в список «скрытые столбцы».



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

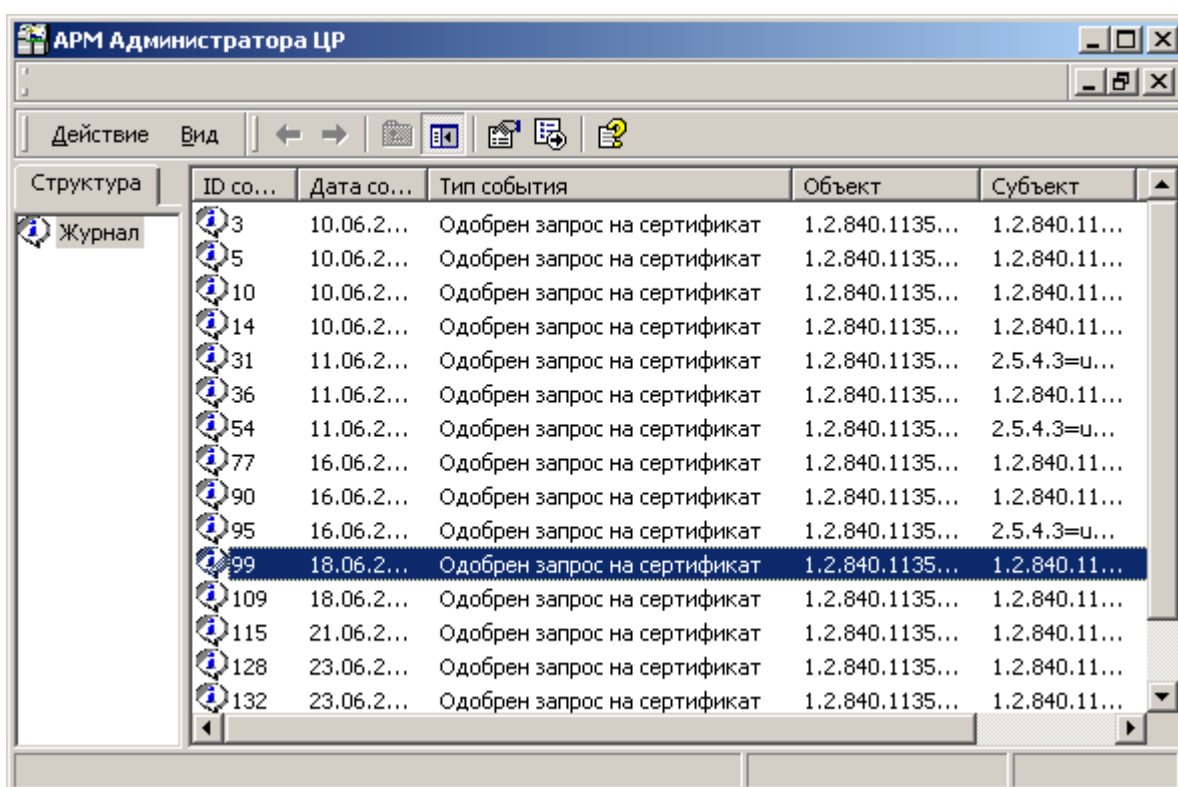
Нажатие на кнопку «Сбросить» приводит к восстановлению отображения столбцов по умолчанию, т.е. к отображению всех столбцов в следующем порядке: «ID события», «Дата события», «Тип события», «Объект», «Субъект», «Комментарий».

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 113. Выбор необходимого типа события

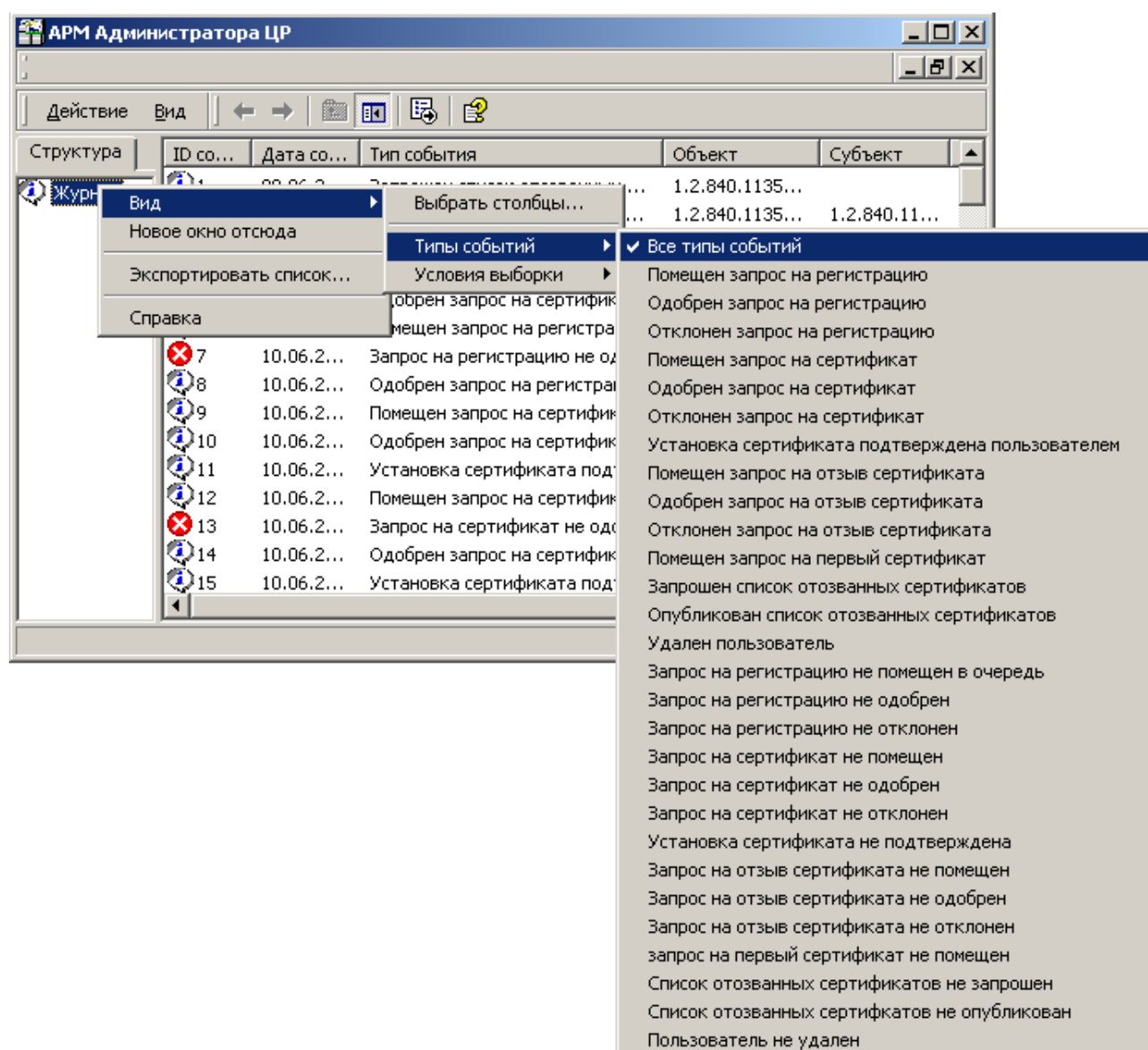
Например, для выбора всех событий типа **Одобрен запрос на сертификат** необходимо правой кнопкой мыши выделить узел **Журнал**, затем в открывшемся контекстном меню выбрать **Вид -> Типы событий -> Одобрен запрос на сертификат**. Окно просмотра зарегистрированных событий будет содержать только события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

Рисунок 114. Пример отображения событий одного типа



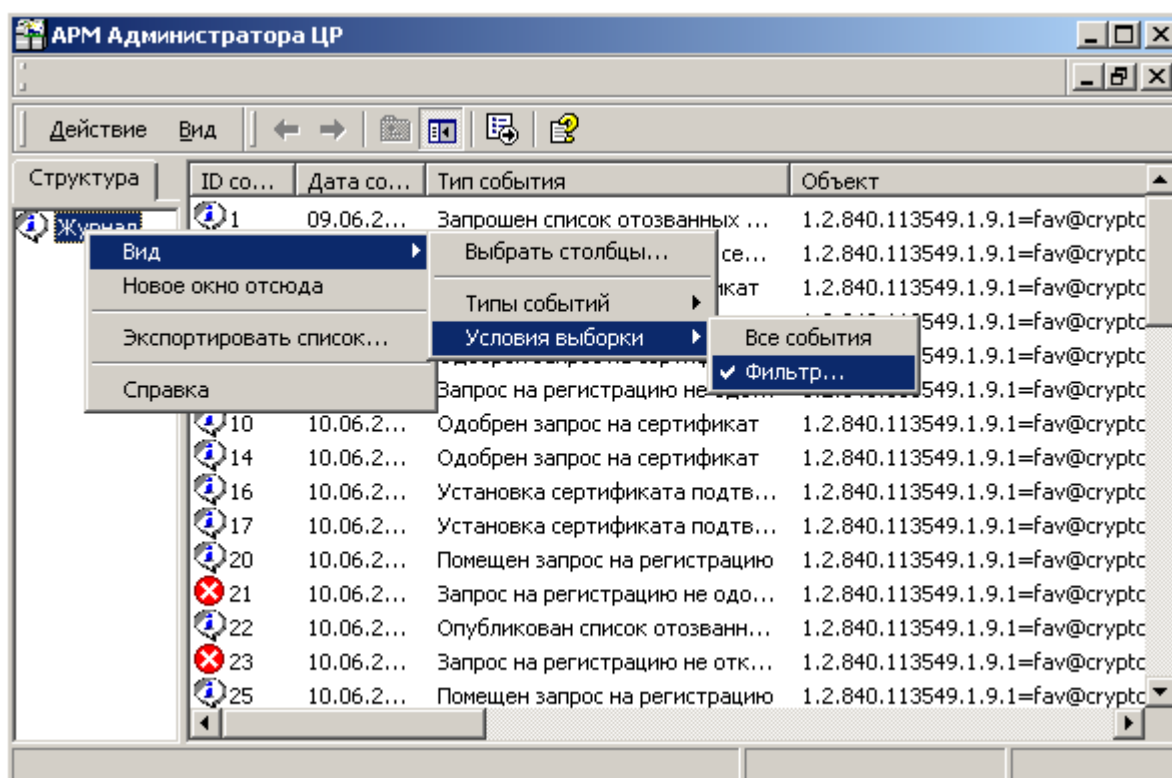
ID со...	Дата со...	Тип события	Объект	Субъект
3	10.06.2...	Одобен запрос на сертификат	1.2.840.1135...	1.2.840.11...
5	10.06.2...	Одобен запрос на сертификат	1.2.840.1135...	1.2.840.11...
10	10.06.2...	Одобен запрос на сертификат	1.2.840.1135...	1.2.840.11...
14	10.06.2...	Одобен запрос на сертификат	1.2.840.1135...	1.2.840.11...
31	11.06.2...	Одобен запрос на сертификат	1.2.840.1135...	2.5.4.3=u...
36	11.06.2...	Одобен запрос на сертификат	1.2.840.1135...	1.2.840.11...
54	11.06.2...	Одобен запрос на сертификат	1.2.840.1135...	2.5.4.3=u...
77	16.06.2...	Одобен запрос на сертификат	1.2.840.1135...	1.2.840.11...
90	16.06.2...	Одобен запрос на сертификат	1.2.840.1135...	1.2.840.11...
95	16.06.2...	Одобен запрос на сертификат	1.2.840.1135...	2.5.4.3=u...
99	18.06.2...	Одобен запрос на сертификат	1.2.840.1135...	1.2.840.11...
109	18.06.2...	Одобен запрос на сертификат	1.2.840.1135...	1.2.840.11...
115	21.06.2...	Одобен запрос на сертификат	1.2.840.1135...	1.2.840.11...
128	23.06.2...	Одобен запрос на сертификат	1.2.840.1135...	1.2.840.11...
132	23.06.2...	Одобен запрос на сертификат	1.2.840.1135...	1.2.840.11...

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

Рисунок 115. Выбор всех зарегистрированных типов событий

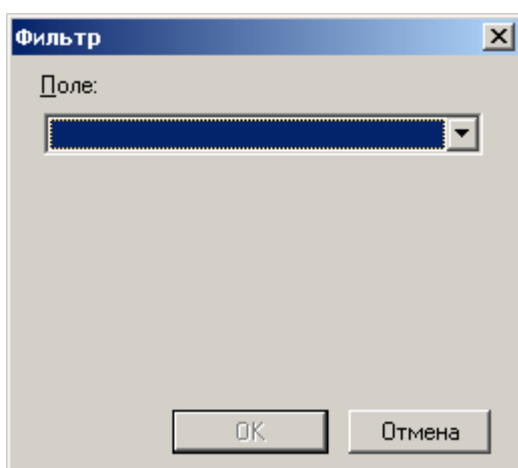
АРМ Администратора Центра Регистрации позволяет производить фильтрацию зарегистрированных в **Журнале** событий по содержанию полей. Для этого необходимо выделить правой кнопкой мыши узел **Журнал**, в открывшемся контекстном меню выбрать **Вид -> Условия выборки -> Фильтр...**

Рисунок 116. Задание фильтра просмотра зарегистрированных событий



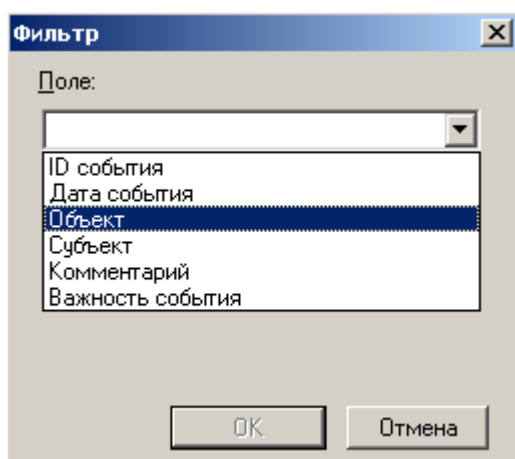
Откроется окно настройки **Фильтра**

Рисунок 117. 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**

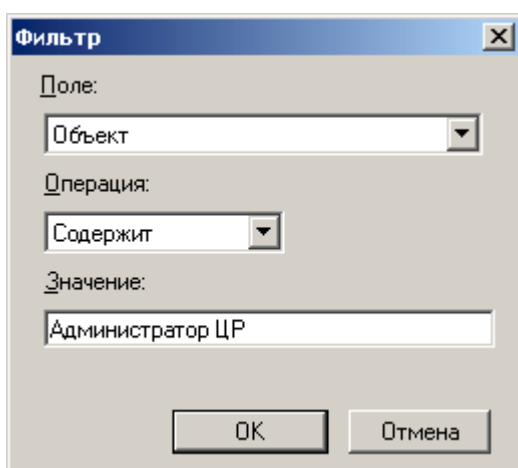
Рисунок 118. Выбор поля фильтрации



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

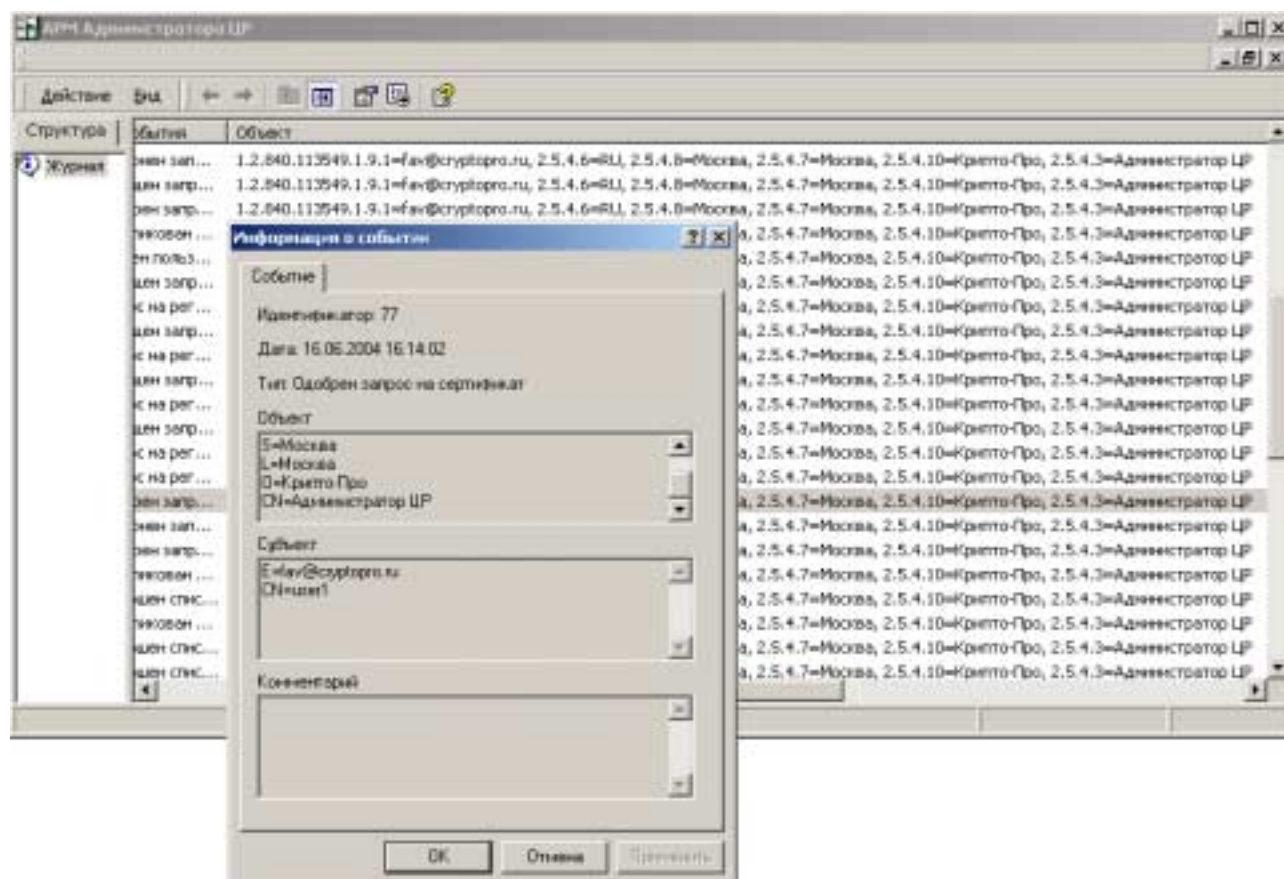
Например, для просмотра событий, выполнение которых осуществлял Администратор (в данном примере это привилегированный пользователь с псевдонимом Администратор ЦР) необходимо осуществить следующие действия: Выделить правой кнопкой мыши узел **Журнал**, в открывшемся контекстном меню выбрать **Вид -> Условия 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 119. Задание параметров Фильтра



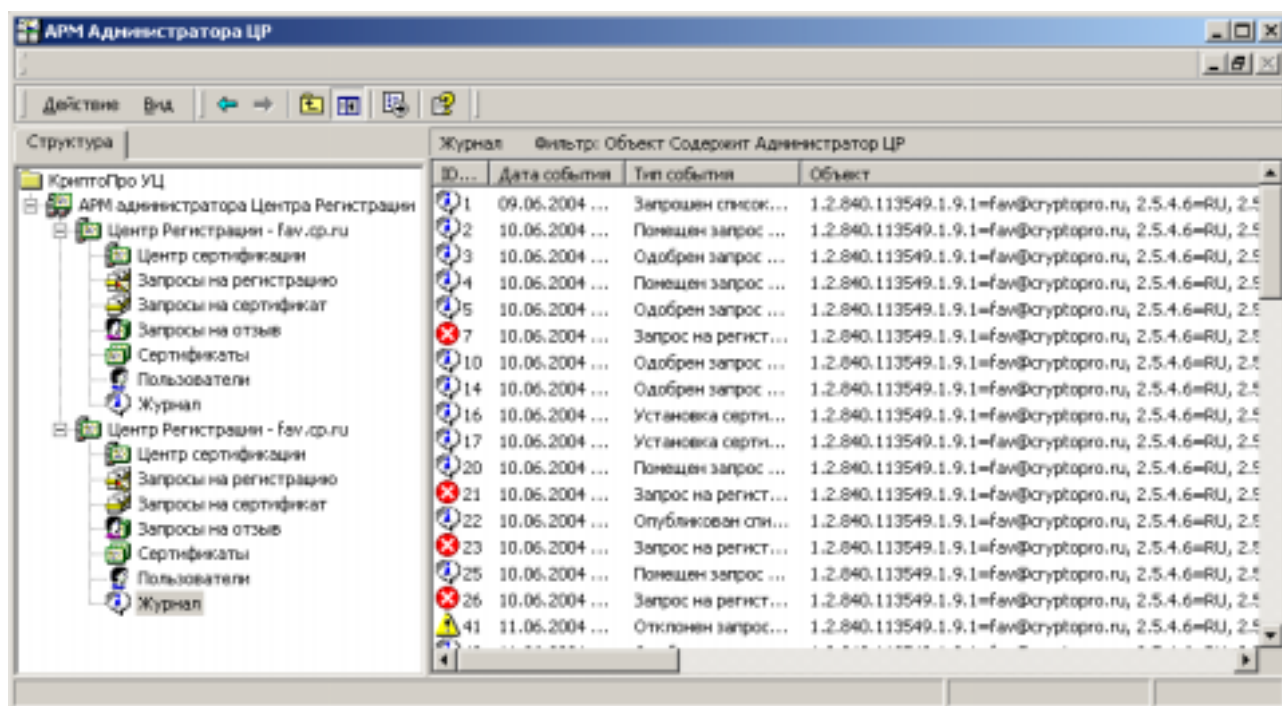
Нажатие кнопки **ОК** в окне настроек фильтра осуществит фильтрацию зарегистрированных событий журнала в соответствии с установленными условиями.

Рисунок 120. Просмотр событий журнала с использованием фильтра



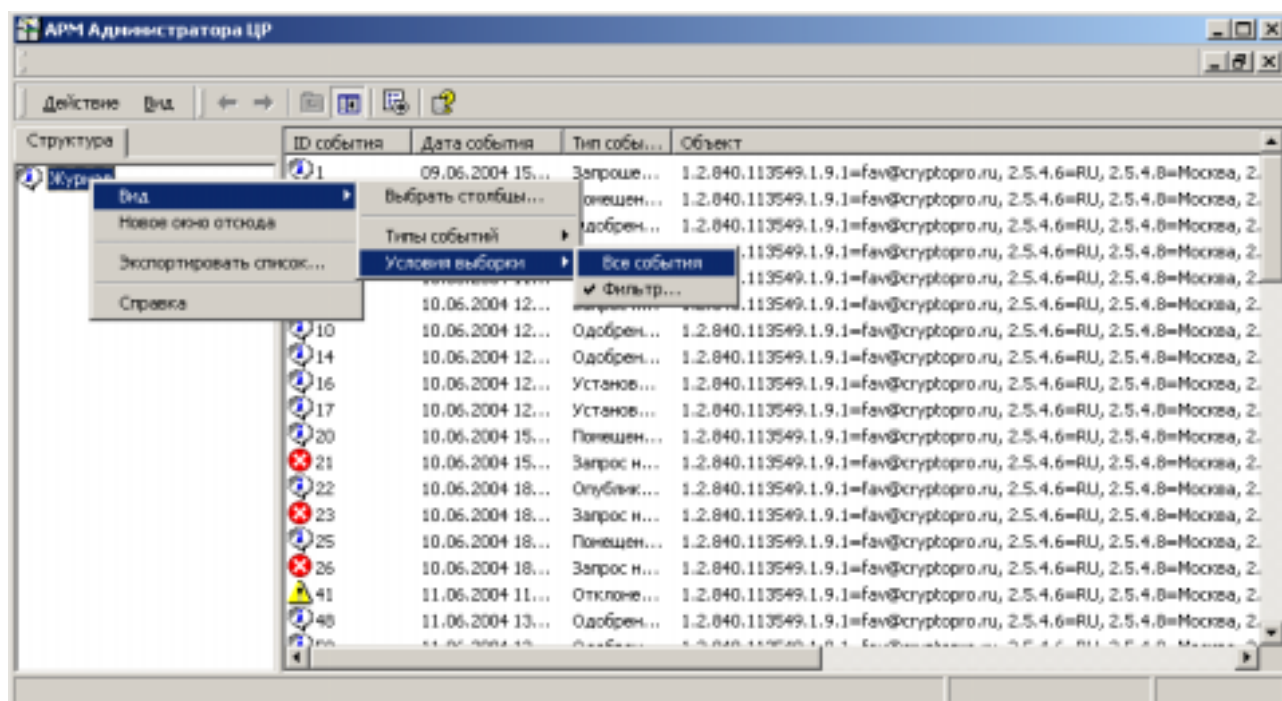
При просмотре **Журнала** посредством выбора одноименного узла в списке объектов управления Центра Регистрации в верхней строке области просмотра событий выводится информация о параметрах используемого фильтра (если фильтр не используется, то поле содержит только запись Журнал).

Рисунок 121. Отображение параметров фильтрации событий Журнала



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

Рисунок 122. Отмена использования фильтрации событий Журнала



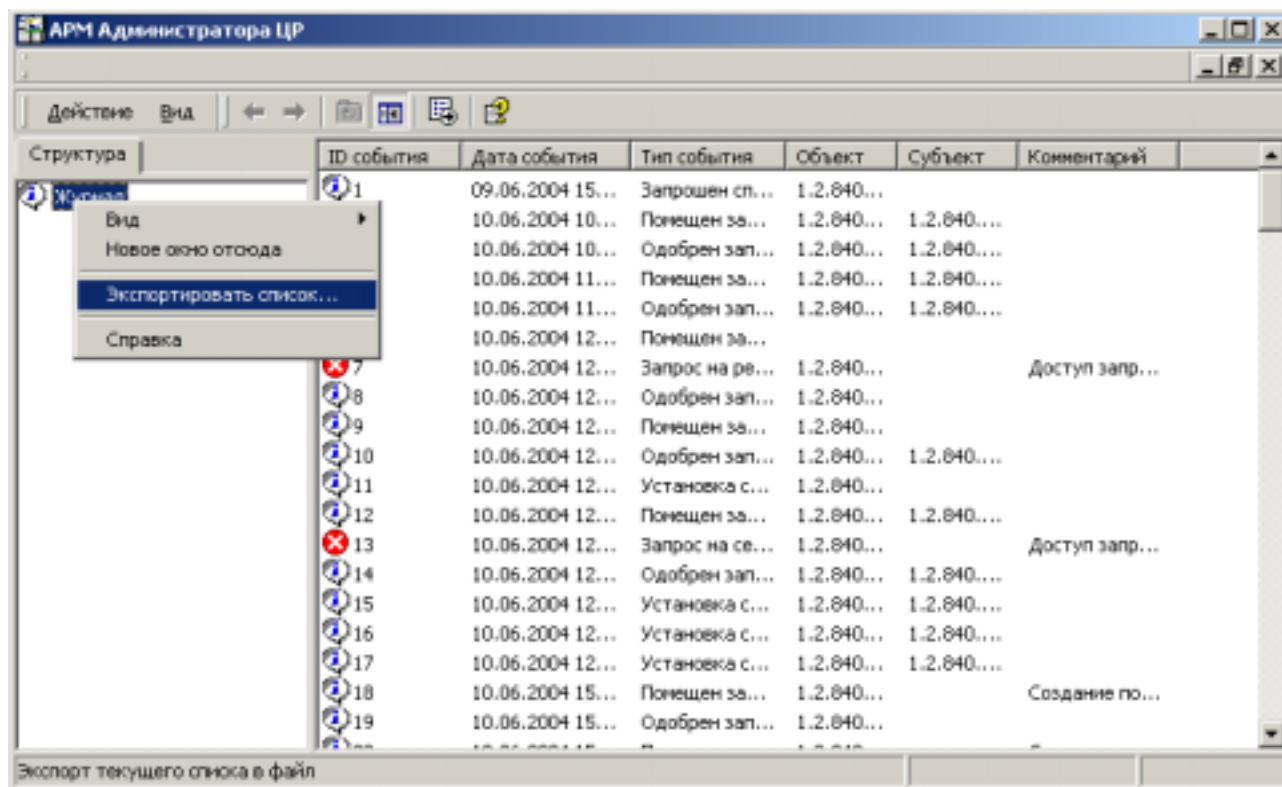
Журнал зарегистрированных событий может быть экспортирован во внешний файл и представлен в виде следующих форматов:

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

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

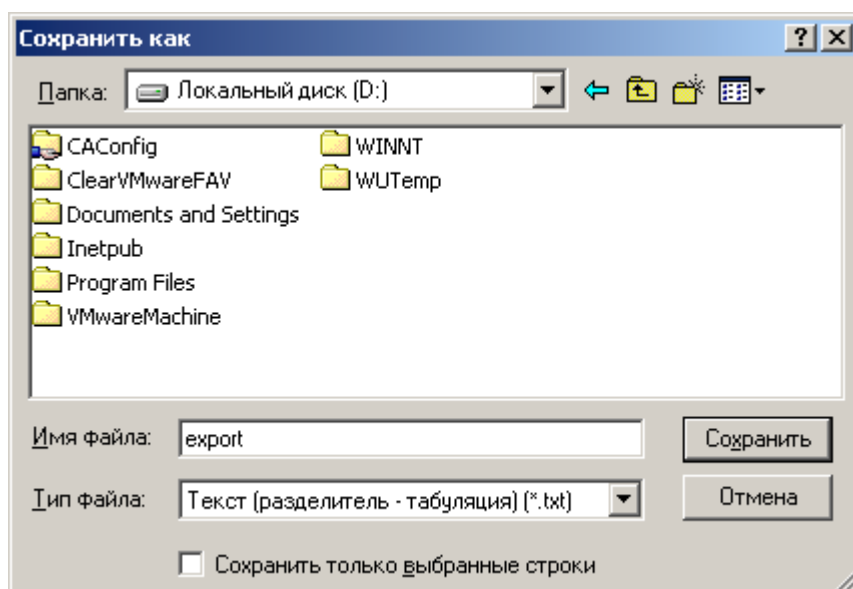
Для осуществления экспорта отображаемых событий выделите правой кнопкой мыши узел **Журнал**, в открывшемся контекстном меню выберите **Экспортировать список**.

Рисунок 123. 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 124. 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

18. 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.

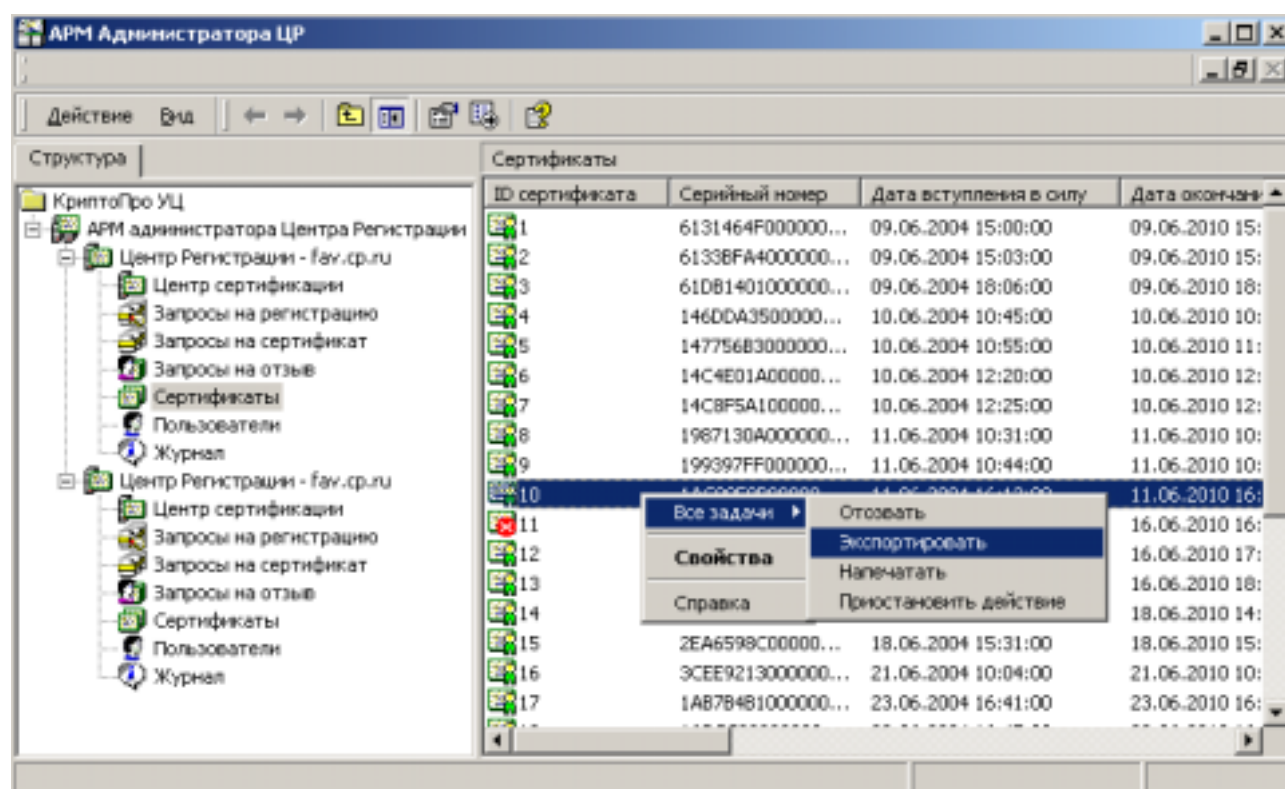
Экспорту могут быть подвергнуты следующие объекты управления:

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

18.1. Экспорт сертификатов открытых ключей подписей

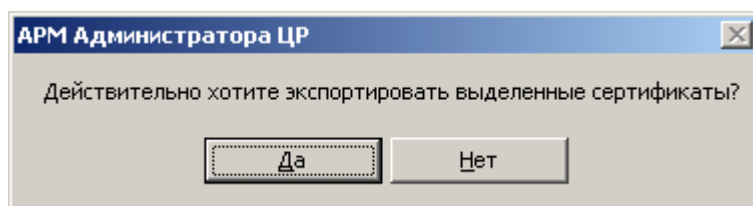
Для осуществления экспорта сертификата открытого ключа в окне просмотра изготовленных сертификатов узла **Сертификаты** выделите правой кнопкой мыши сертификат, который требуется экспортировать, в открывшемся контекстном меню выберите **Все задачи** -> **Экспортировать**

Рисунок 125. Экспорт сертификата ключа подписи



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

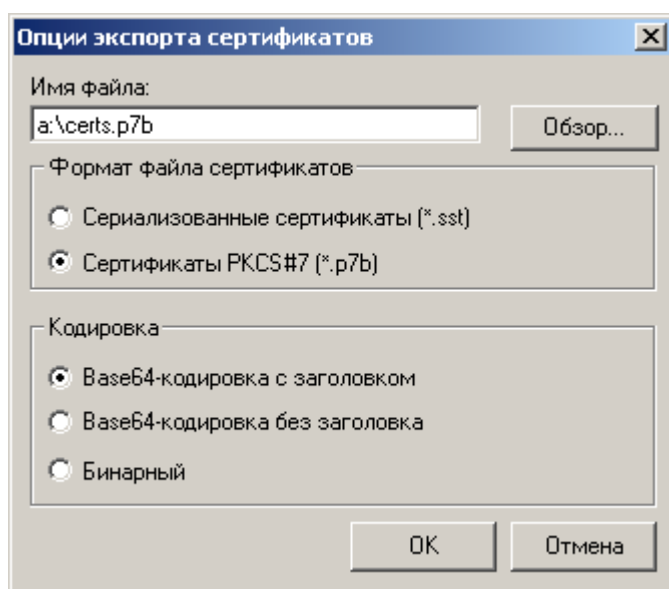
Рисунок 126. Подтверждение экспорта сертификата



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

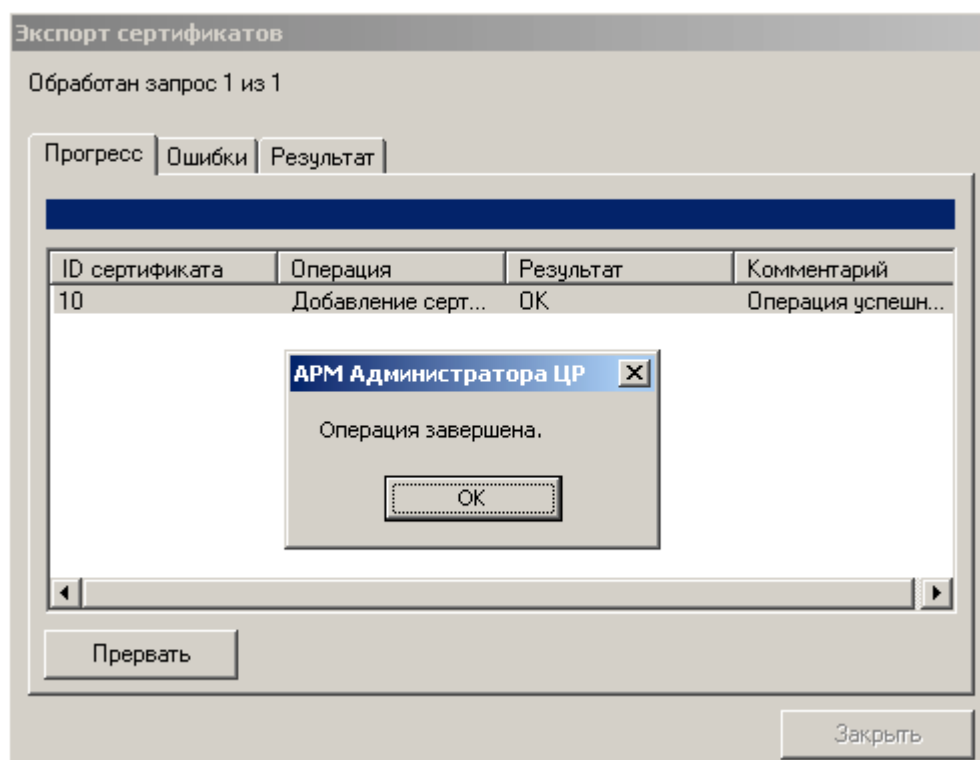
- размещение и имя выходного файла - поле **Имя файла** (для указания папки размещения выходного файла рекомендуется воспользоваться кнопкой **Обзор** данного окна)
- формат выходного файла – переключатель **Формат файла сертификатов**, позволяющий указать формат выходного файла - **PKCS#7 (.p7b)** или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

Рисунок 127. Задание опций экспорта сертификатов



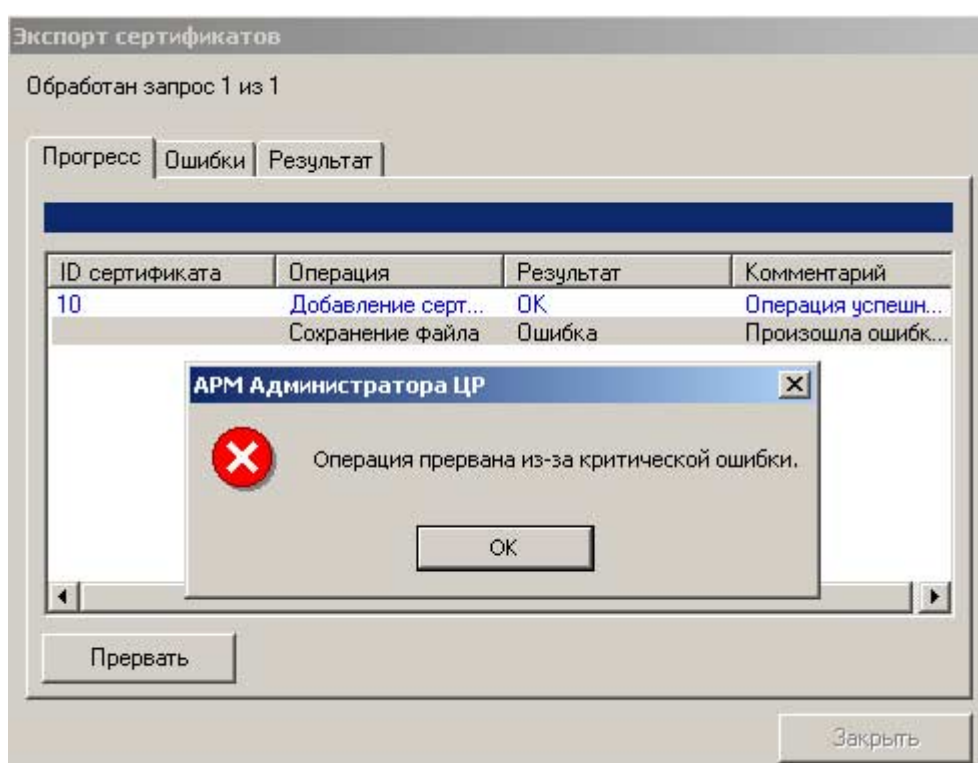
После задания необходимых параметров нажмите кнопку **ОК**. Успешное выполнение экспорта сертификата вызовет появление сообщения **Операция завершена** и в окне экспорт сертификатов будет отображена запись с результатом выполнения данного действия.

Рисунок 128. Успешное завершение процедуры экспорта сертификата



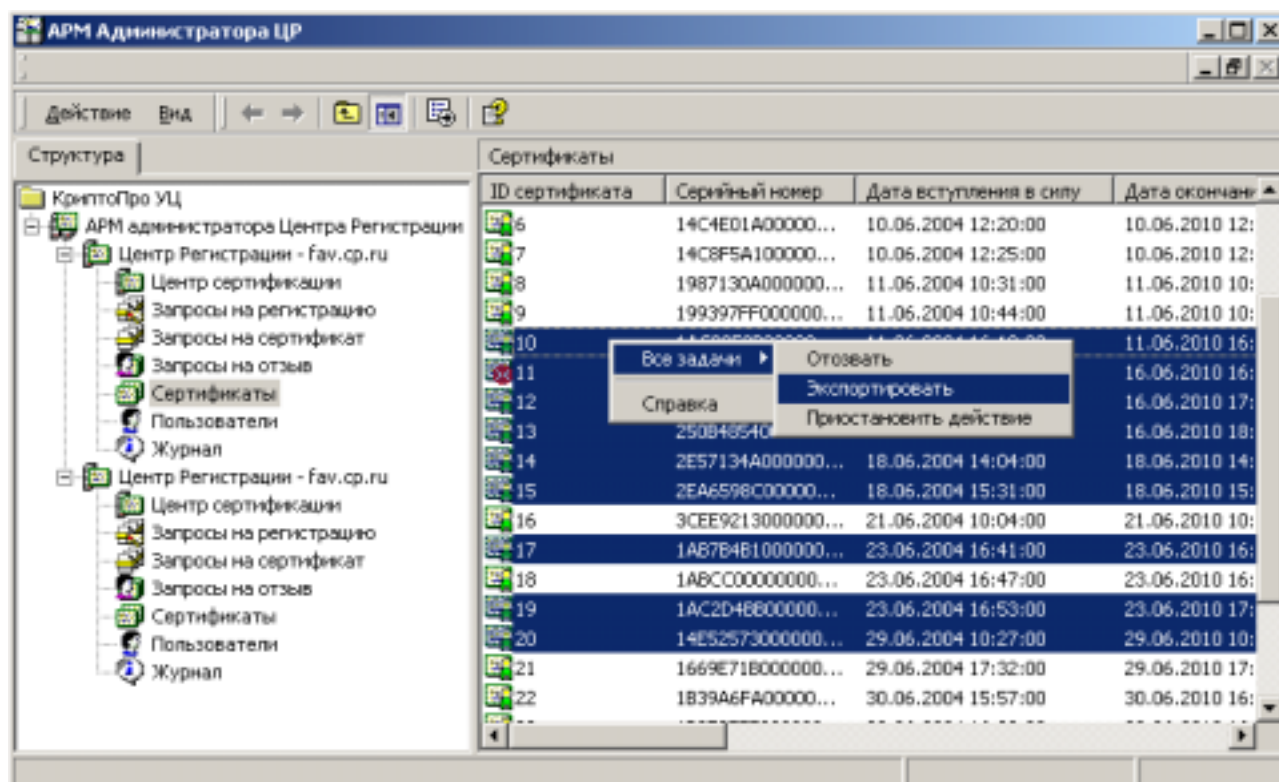
При появлении ошибки в процессе экспорта сертификата ключа подписи отображается соответствующее сообщение, а в окне **Экспорт сертификатов** указывается подробная причина ее возникновения. Наиболее часто встречающейся ошибкой является событие, вызванное отсутствием внешнего носителя либо его защитой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

Рисунок 129. 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 130. Экспорт группы сертификатов в один файл



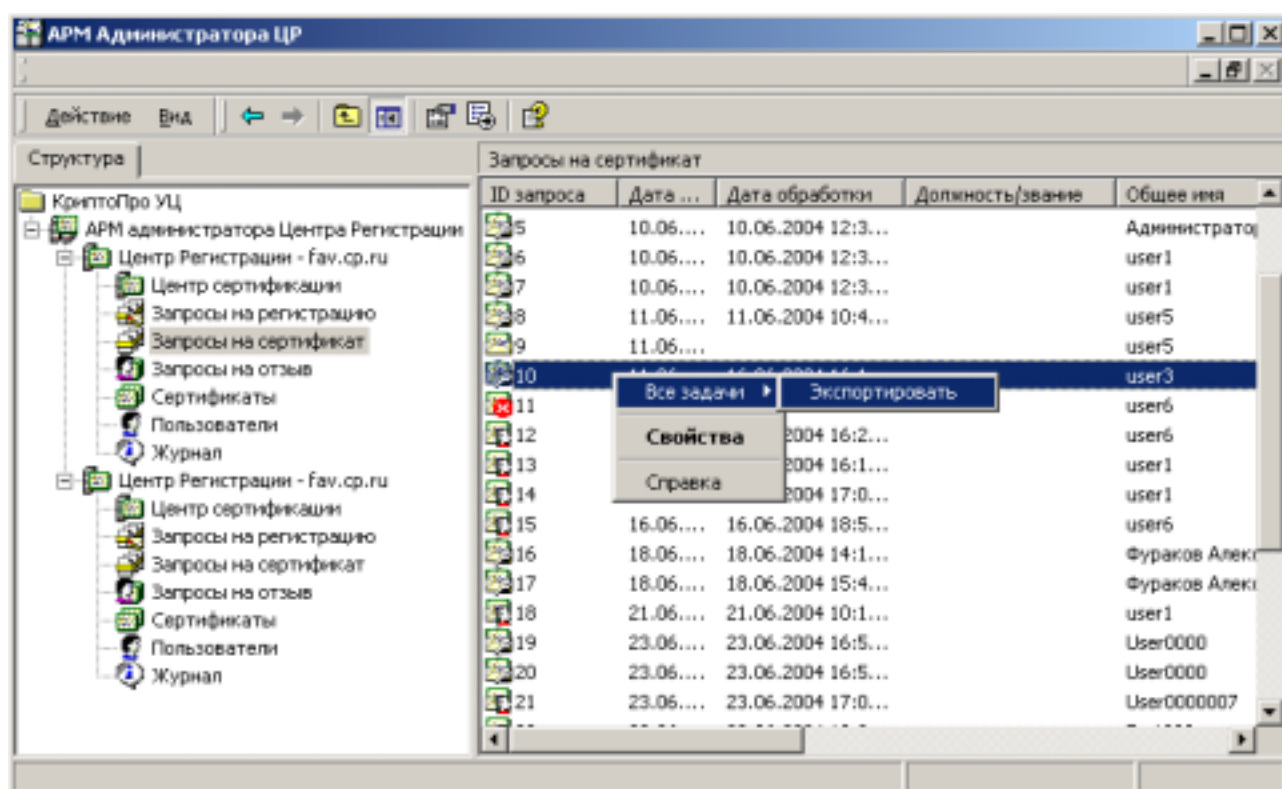


Экспорт сертификата (сертификатов) ключа подписи также может быть осуществлен в окне просмотра сертификатов конкретного пользователя. Порядок выполнения указанной процедуры аналогичен описанному в п. 19.1.

18.2. Экспорт запросов на изготовление сертификатов открытых ключей

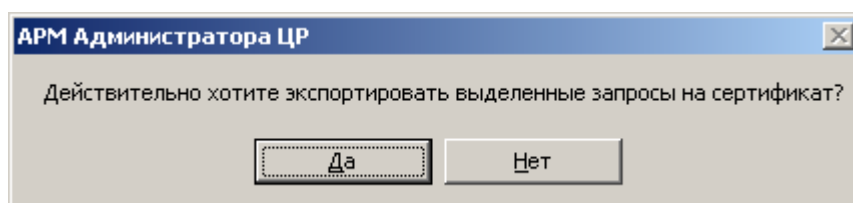
Для осуществления экспорта запроса на сертификат открытого ключа в окне просмотра запросов узла **Запросы на сертификат** выделите правой кнопкой мыши запрос на сертификат, который требуется экспортировать, в открывшемся контекстном меню выберите **Все задачи** -> **Экспортировать**

Рисунок 131. Экспорт запроса на сертификат ключа подписи



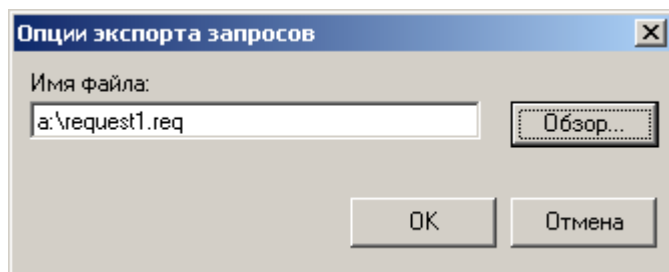
Откроется предупреждающее сообщение, требующее подтвердить выбор указанного действия, нажмите кнопку **Да**

Рисунок 132. Подтверждение экспорта запроса на сертификат



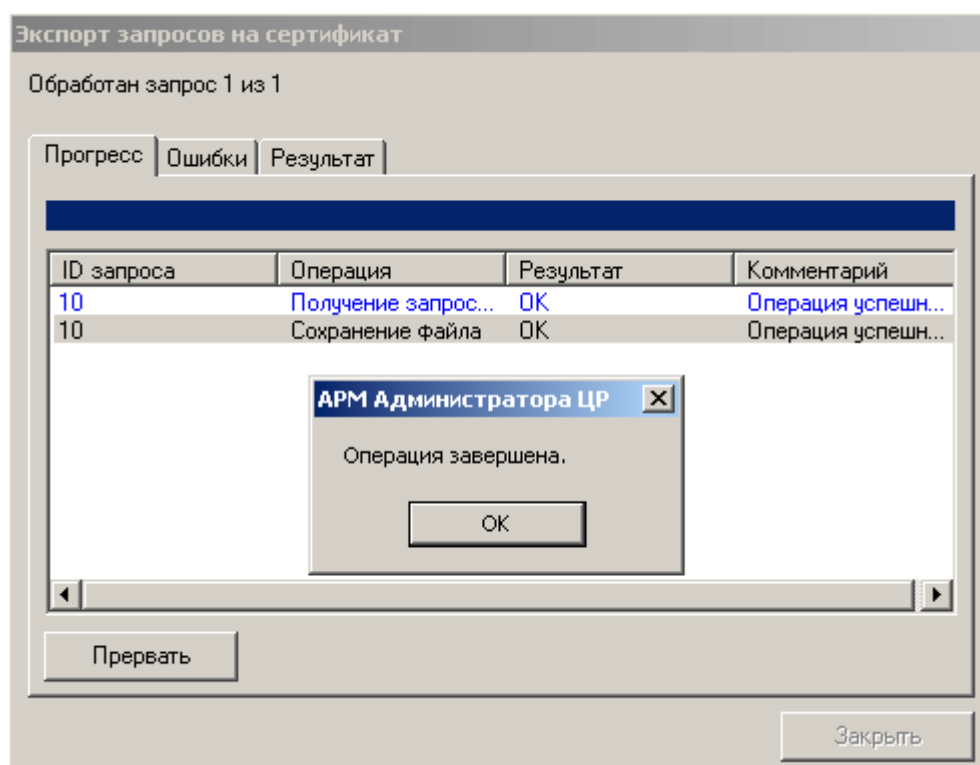
Откроется окно **Опции экспорта запросов**, в котором установите путь размещения и имя выходного файла запроса на сертификат (для указания папки размещения выходного файла рекомендуется воспользоваться кнопкой **Обзор** данного окна) после чего нажмите кнопку **ОК**

Рисунок 133. Задание опций экспорта запроса на сертификат



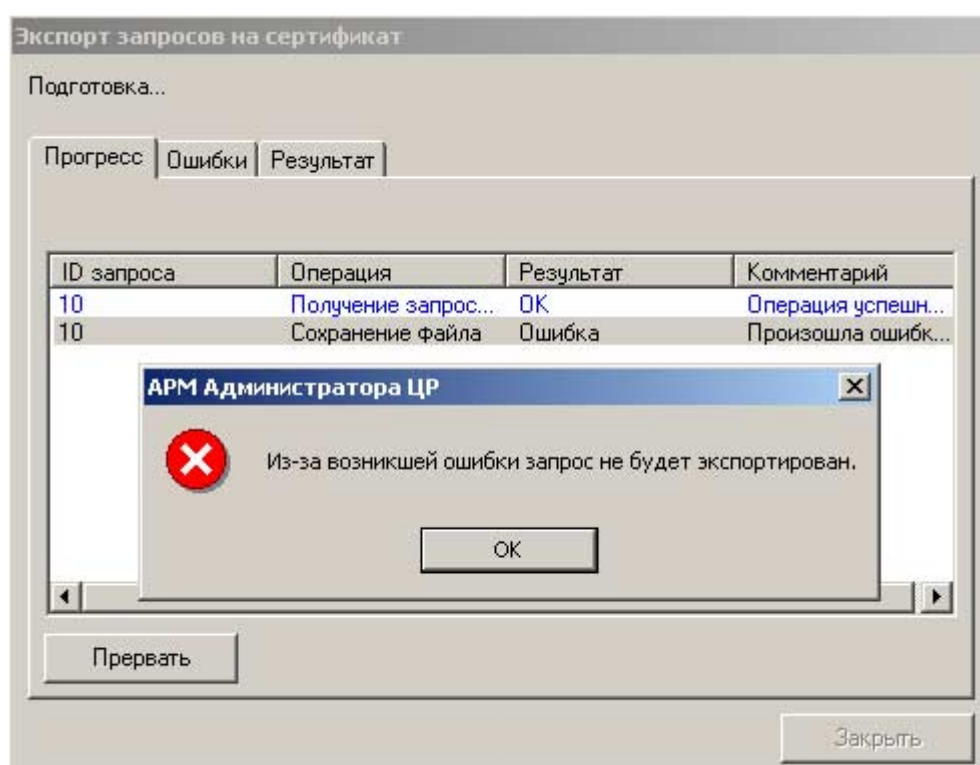
Успешное выполнение экспорта запроса на сертификат вызовет появление сообщения **Операция завершена** и в окне **Экспорт запросов на сертификат** будет отображена запись с результатом выполнения данного действия.

Рисунок 134. 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 135. Сообщение об ошибке при экспорте запроса на сертификат



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

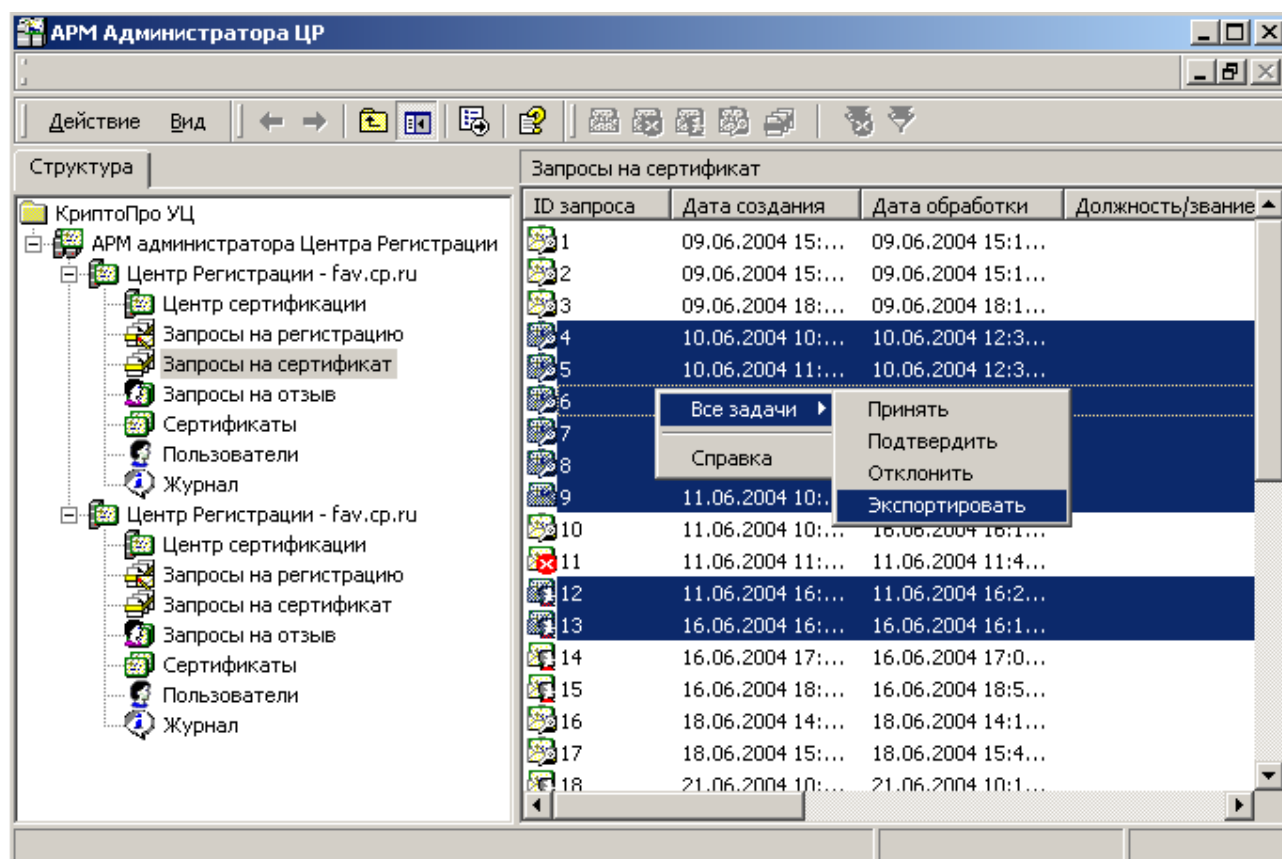
- в формате PKCS#10 в кодировке Base64 (собственно запрос на сертификат определенный стандартом PKCS#10). В данном формате представлены следующие запросы (данные запросы в окне просмотра свойств запроса на сертификат позиционируются, как неподписанные):
 - о поступившие на Центр Регистрации от пользователя, обладающего маркером временного доступа (посредством АРМ пользователя), и еще не одобренные привилегированным пользователем УЦ
 - о 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:
 - о поступившие на Центр Регистрации от пользователя с использованием подключения на действующем сертификате (посредством АРМ пользователя), и еще не одобренные привилегированным пользователем УЦ
 - о поступившие на Центр Регистрации от пользователя, обладающего маркером временного доступа (посредством АРМ пользователя), и уже одобренные привилегированным пользователем УЦ
 - о 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
 - о 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 пункте 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 136. Экспорт группы запросов на сертификат



Экспорт запроса на сертификат (запросов) также может быть осуществлен в окне просмотра запросов на сертификат конкретного пользователя. Порядок выполнения указанной процедуры аналогичен описанному в п. 19.2.

18.3. 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**

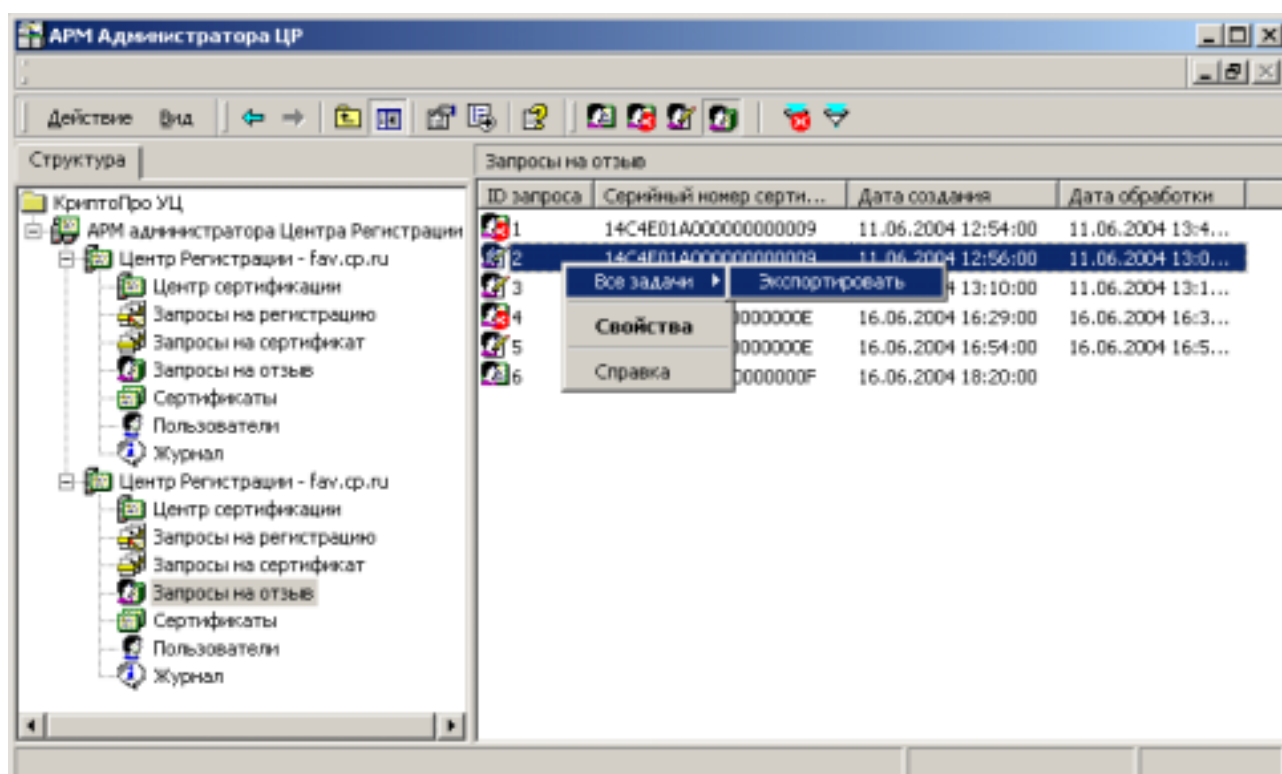


В окне просмотра запросов узла **Запросы на отзыв** помимо запросов на отзыв размещаются запросы на приостановление и возобновление действия сертификатов. Определение типа запроса осуществляется в окне просмотра его Свойств (для этого необходимо дважды кликнуть левой кнопкой мыши необходимый запрос, 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.



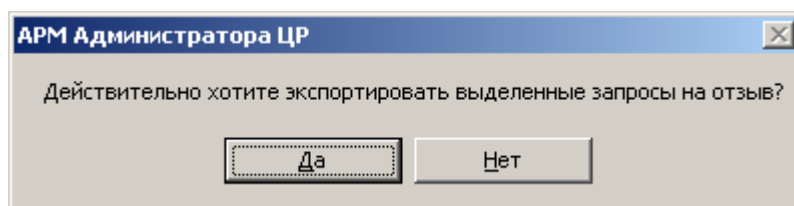
В данном разделе экспорт указанных запросов будет рассмотрен на примере экспорта запроса на отзыв сертификата. Процедуры экспорта запросов на приостановление и возобновление действия сертификата осуществляется аналогично экспорту запроса на отзыв сертификата

Рисунок 137. Экспорт запроса на отзыв сертификата



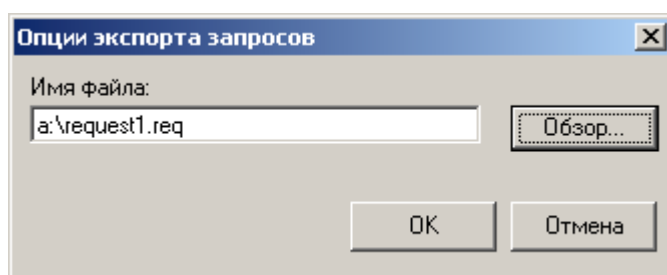
Откроется предупреждающее сообщение, требующее подтвердить выбор указанного действия, нажмите кнопку **Да**

Рисунок 138. Подтверждение экспорта запроса на отзыв сертификата



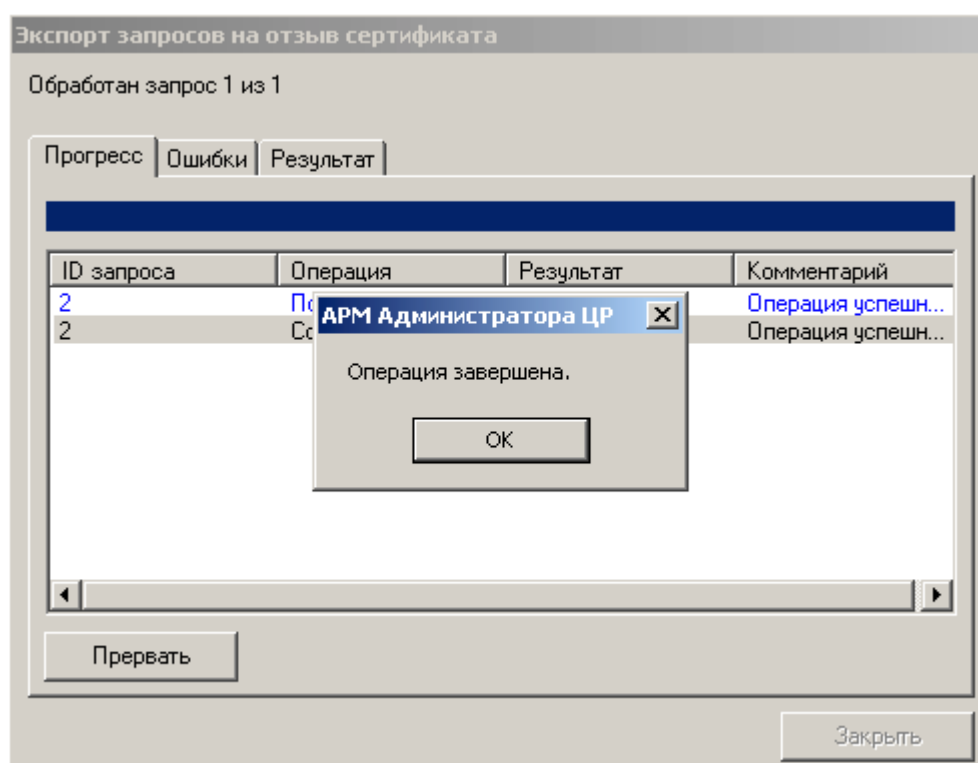
Откроется окно **Опции экспорта запросов**, в котором установите путь размещения и имя выходного файла запроса на сертификат (для указания папки размещения выходного файла рекомендуется воспользоваться кнопкой **Обзор** данного окна) после чего нажмите кнопку **ОК**

Рисунок 139. Задание опций экспорта запроса на отзыв сертификата



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.

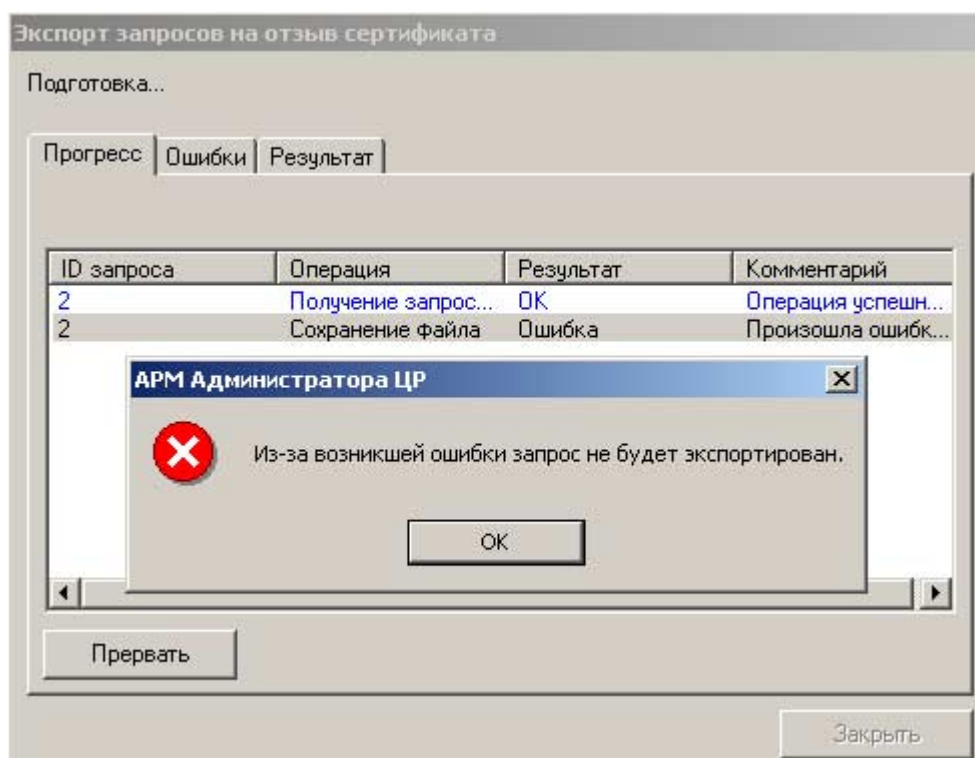
Рисунок 140. Успешное завершение процедуры экспорта запроса на отзыв сертификата





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 141. 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 (а1). 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:

- о 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
- о 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
 - о 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:

- о 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
- о 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

- о 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:

- о 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
- о 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
 - о 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



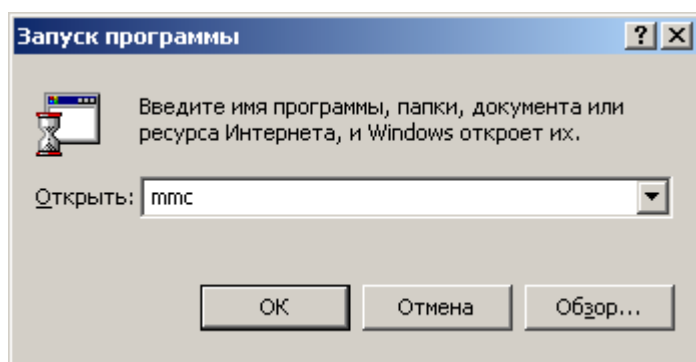
Экспорт запросов на отзыв, приостановление и возобновление действия сертификата также может быть осуществлен в окне просмотра **Запросов на отзыв** конкретного пользователя. Порядок выполнения указанной процедуры аналогичен описанному в п. 19.3.

19. 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.

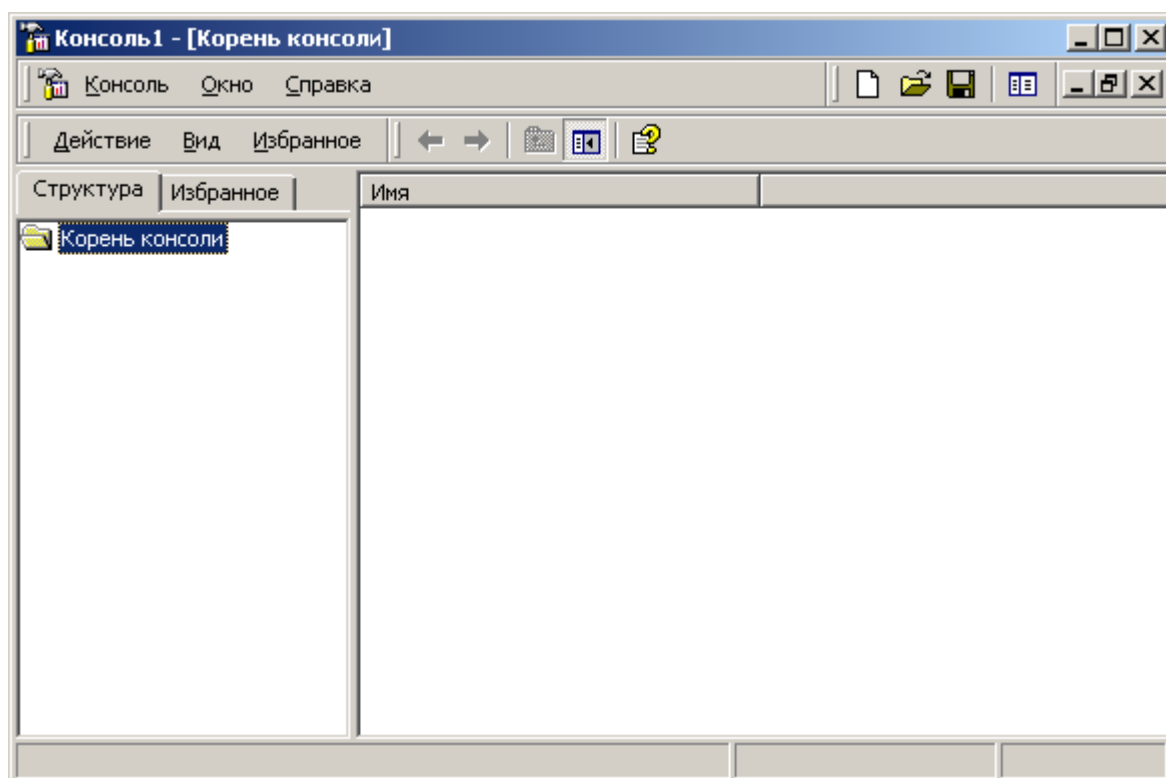
Для создания новой консоли управления нажмите **Пуск\Выполнить**, в окне **Запуск программы** введите **mmc** и нажмите кнопку **ОК**

Рисунок 142. Запуск консоли mmc



Откроется окно консоли **Консоль1**

Рисунок 143. Окно консоли Консоль1

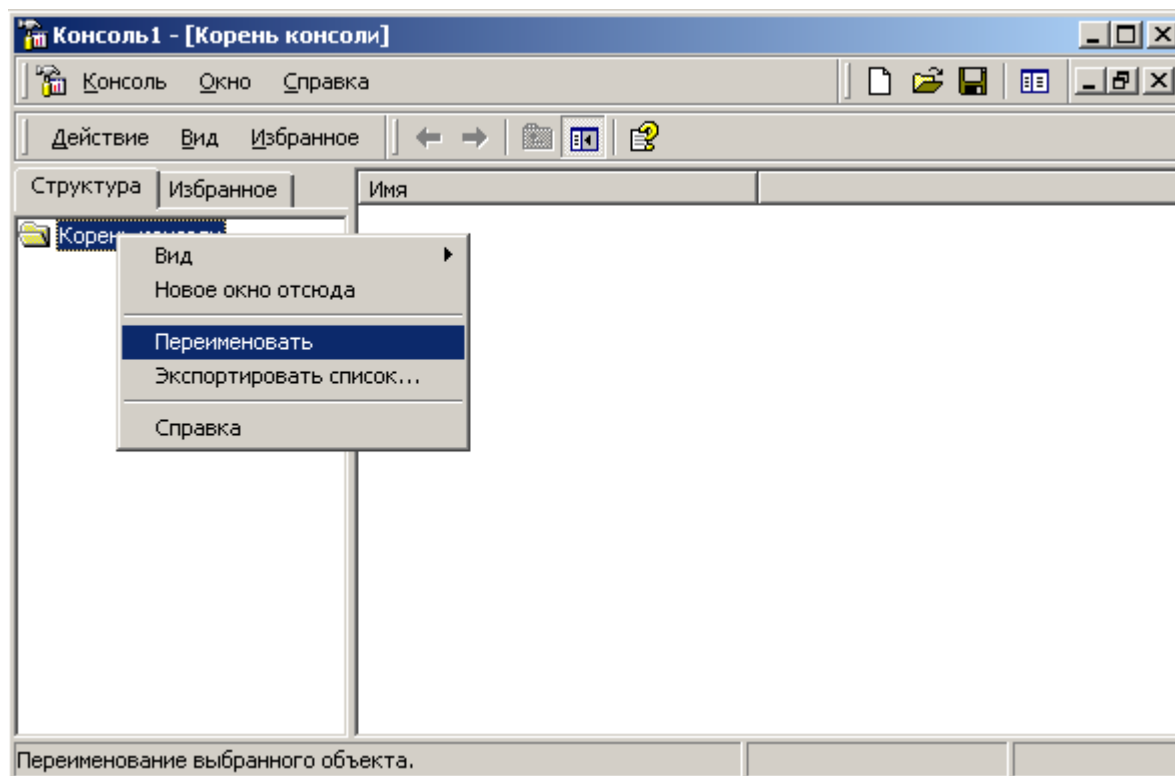


Для удобства и отражения функциональности созданной консоли управления переименуйте узел **Корень консоли** в **Администрирование УЦ**. Для этого выберите

Руководство оператора Удостоверяющего центра ООО «КРИПТО-ПРО» (срса.cryptopro.ru)

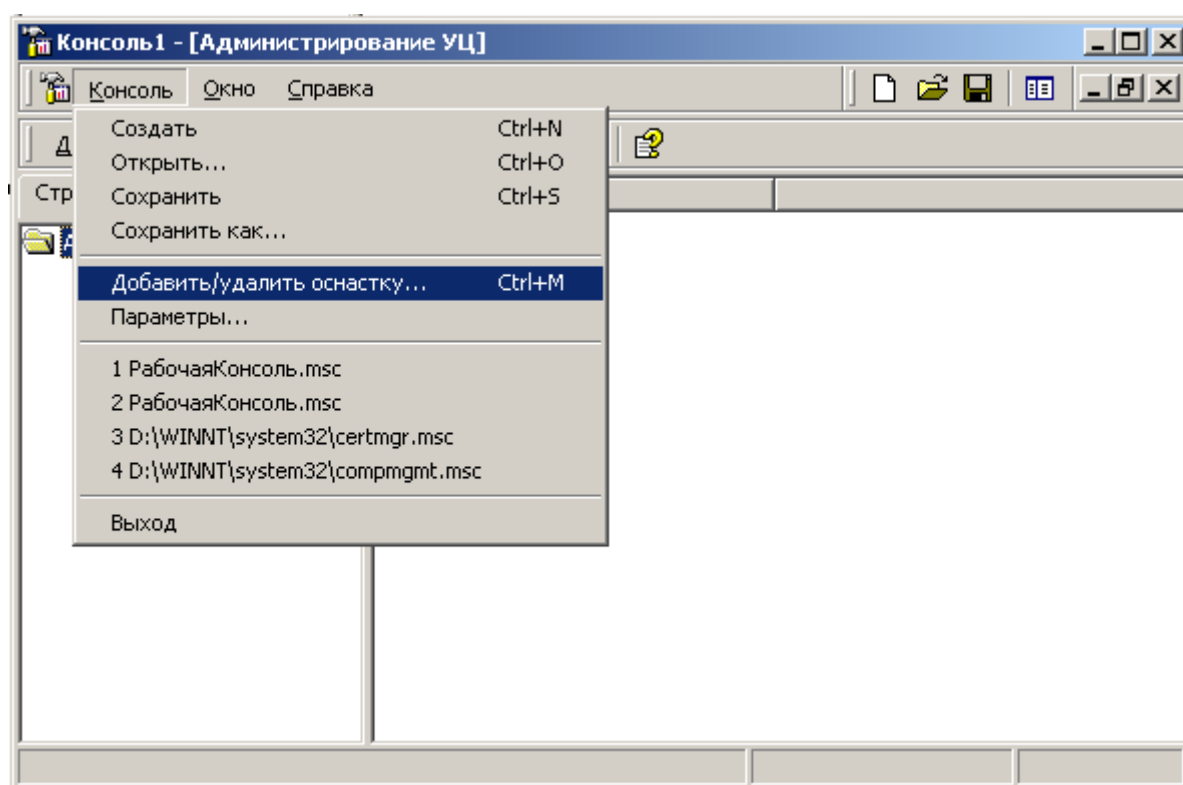
правой кнопкой мыши узел **Корень консоли** и в открывшемся контекстном меню нажмите **Переименовать** и введите новое название корневого узла консоли.

Рисунок 144. Переименование корневого узла созданной консоли



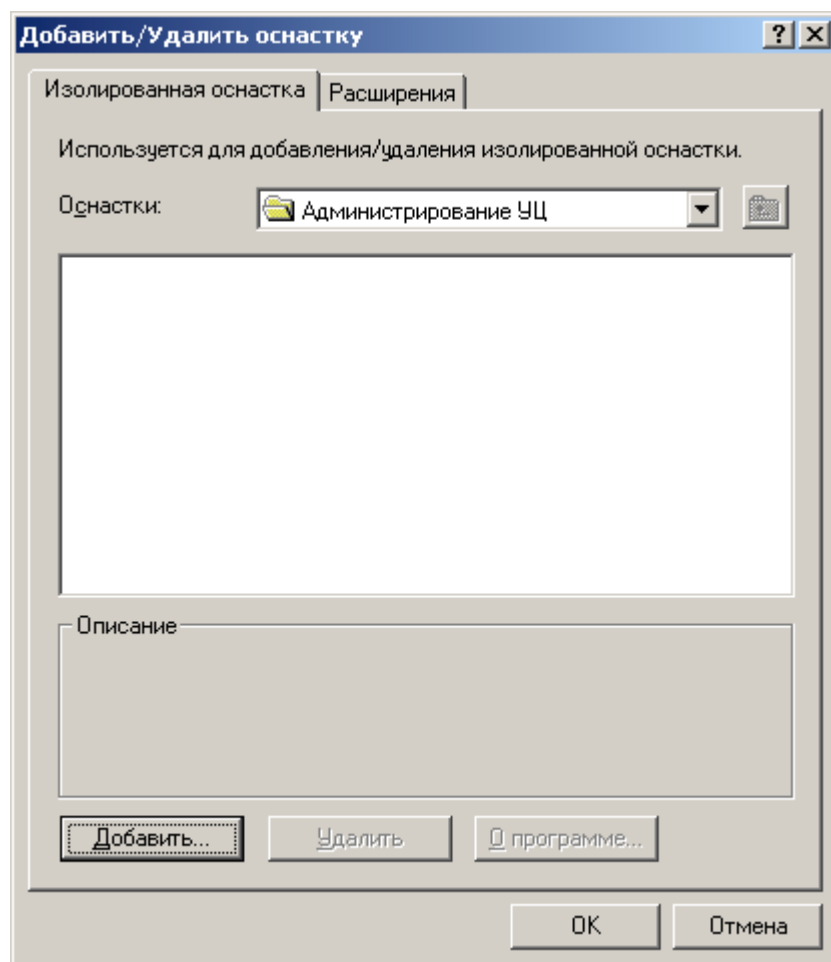
Для добавления оснастки **АРМ администратора ЦР** нажмите кнопку **Консоль**, затем в раскрывшемся меню выберите **Добавить/Удалить оснастку...**

Рисунок 145. Выбор пункта меню Добавить/Удалить оснастку...



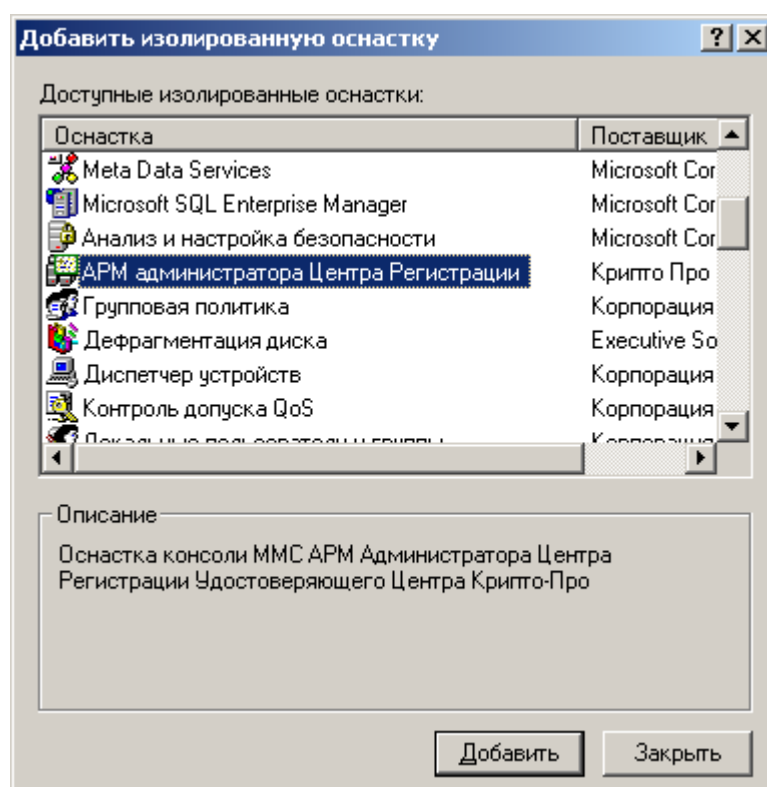
Откроется окно **Добавить/Удалить оснастку**, затем нажмите кнопку **Добавить...**

Рисунок 146. Окно Добавить/Удалить оснастку



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

Рисунок 147. Окно Добавить изолированную оснастку

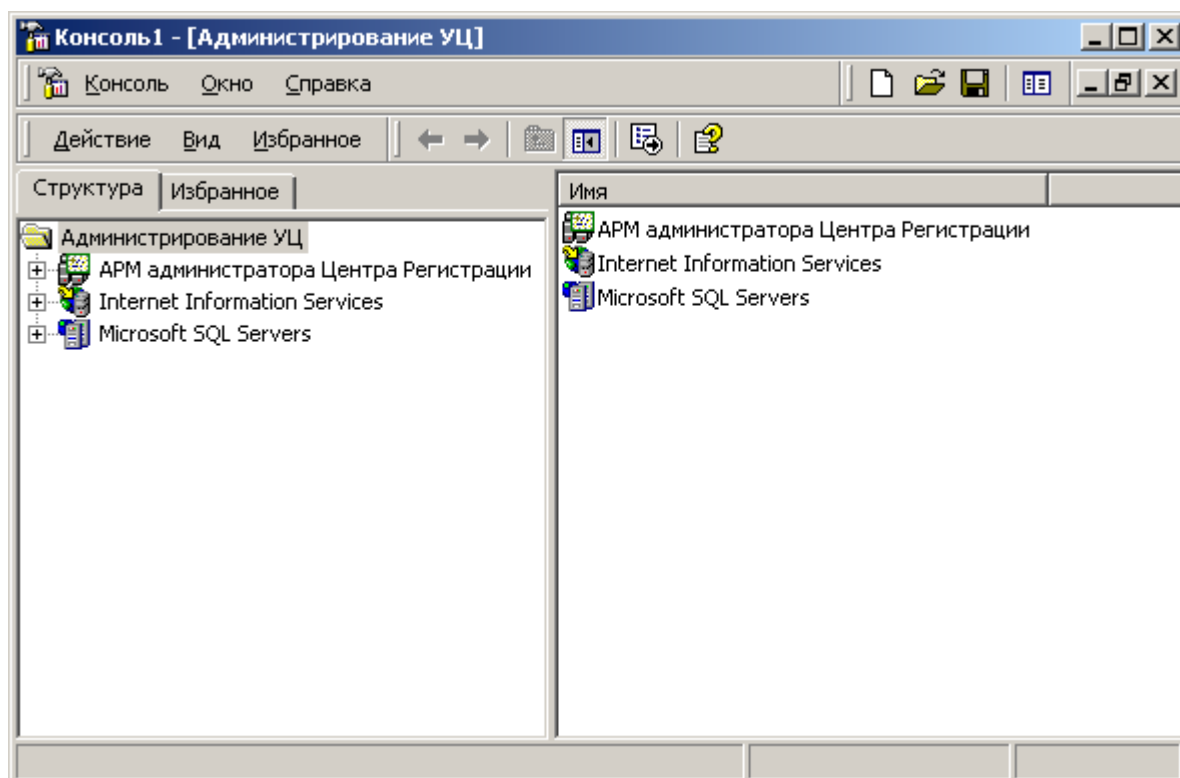


При необходимости, добавьте те оснастки, которые вам необходимы для администрирования компонент Удостоверяющего центра, например, **Internet Information Services** – для настройки Вэб-узла Центра регистрации и **Microsoft SQL Enterprise Manager** – для организации резервного копирования Базы данных Центра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

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

Окно консоли управления примет следующий вид:

Рисунок 148. Окно консоли управления Консоль1 после добавления необходимых изолированных оснасток

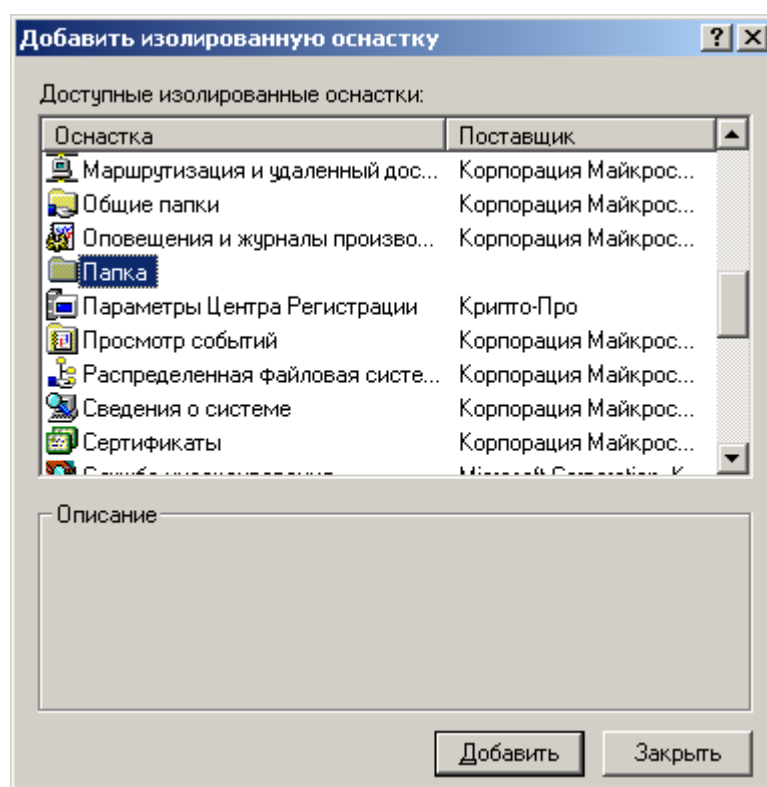


Интерфейс **Microsoft Management Console** позволяет объединять оснастки в отдельные папки и организовывать средства администрирования по иерархической модели. В приведенном выше примере три изолированные оснастки объединены в одном узле – корневом узле **Администрирование УЦ**.

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**.

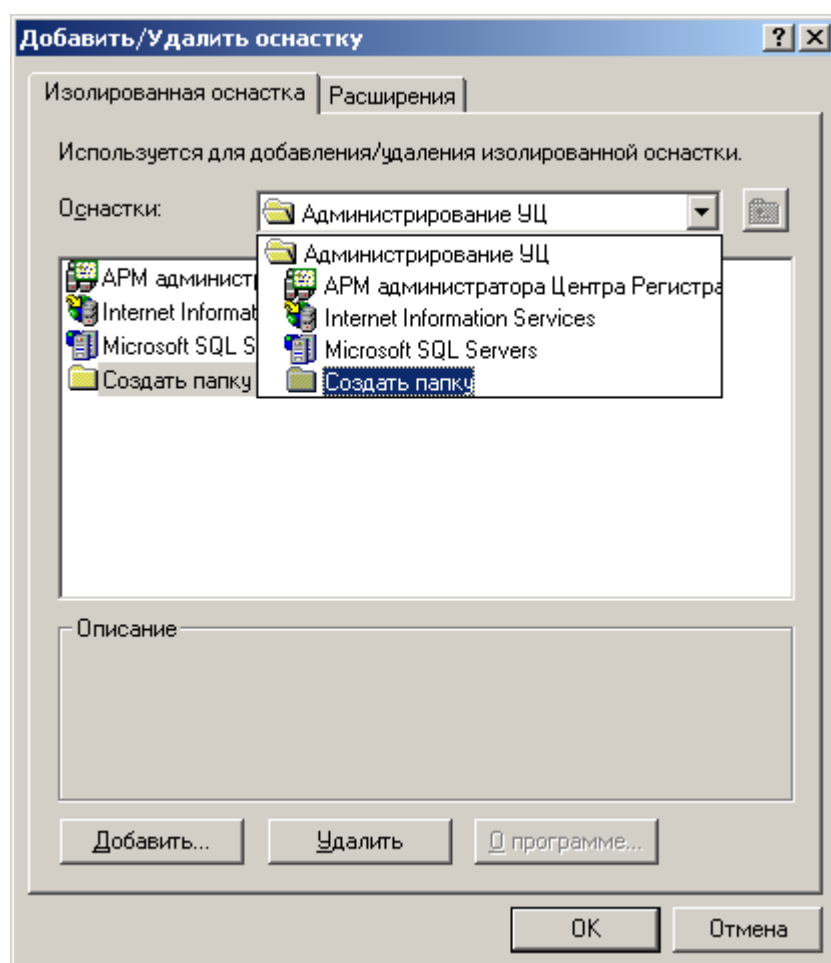
Для этого нажмите кнопку **Консоль** и в раскрывшемся меню выберите **Добавить/Удалить оснастку...** В появившемся окне нажмите кнопку **Добавить...**, из списка выберите оснастку **Папка** и в окне **Добавить изолированную оснастку** последовательно нажмите **Добавить** и **Заккрыть**

Рисунок 149. 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»

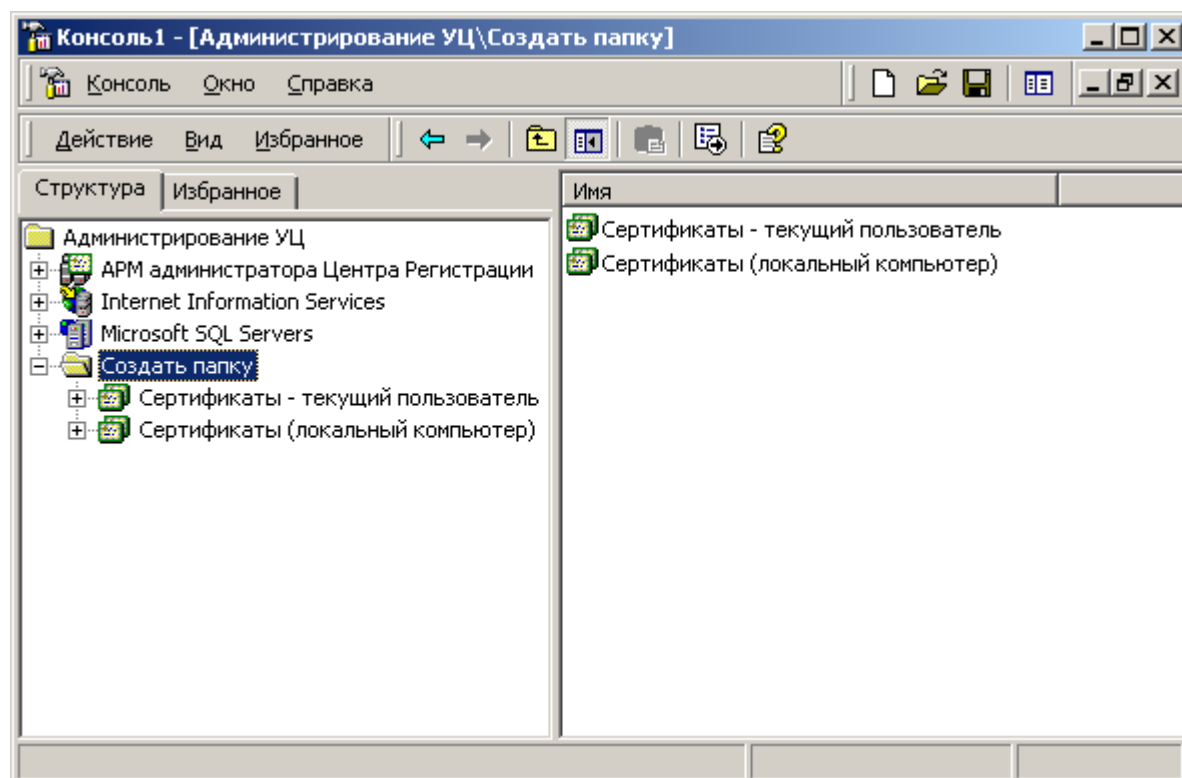
Рисунок 150. Выбор нового узла для добавления оснасток



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 **Консоли1** примет следующий вид

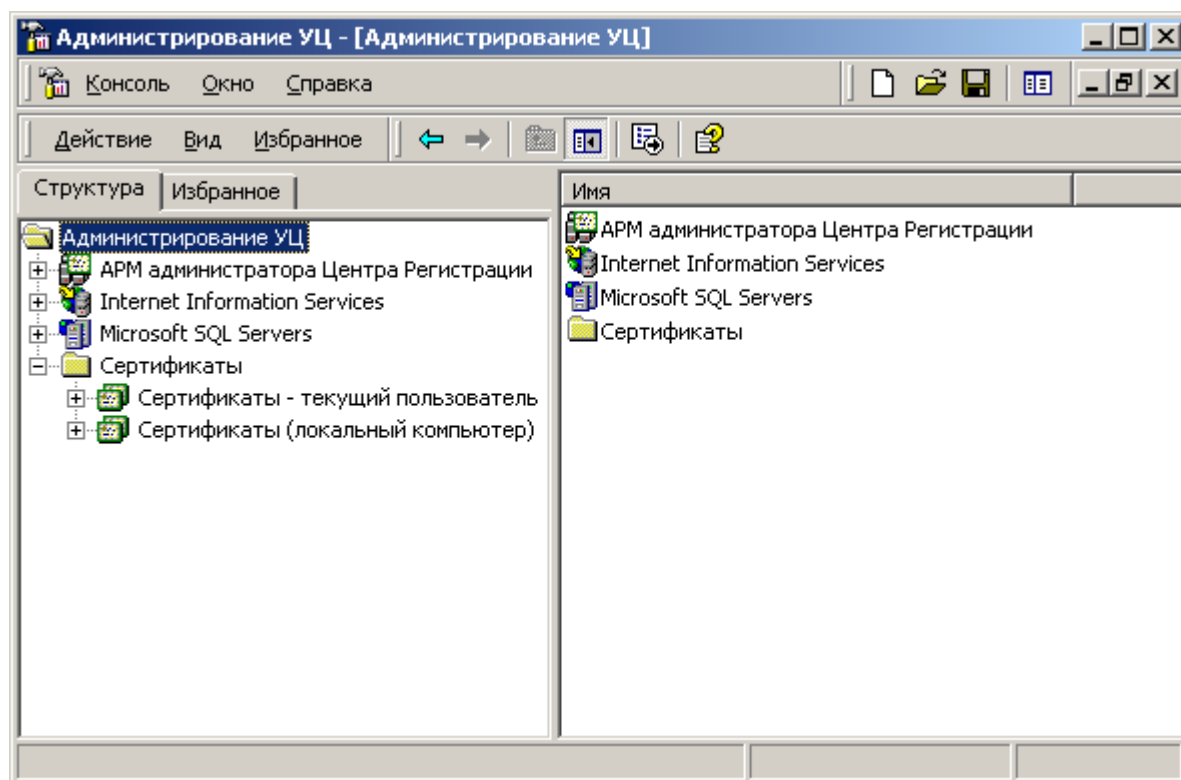
Рисунок 151. Окно консоли управления Консоль1 после добавления нового узла



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).

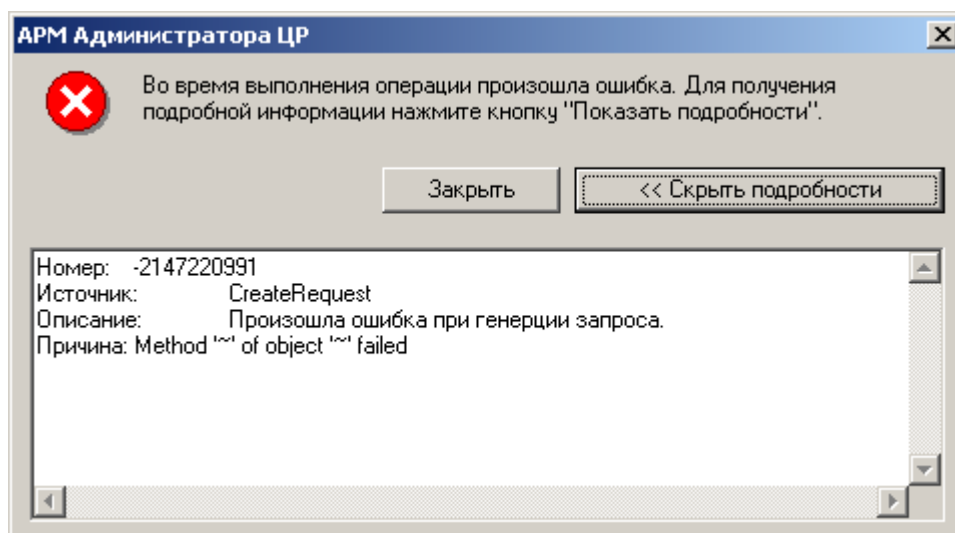
Теперь созданный файл содержит все необходимые для пользователя компоненты администрирования, организованные и упорядоченные определенным образом, и которые при желании могут быть удалены, либо дополнены новыми административными средствами

Рисунок 152. Окно консоли Администрирование УЦ



20. Перечень сообщений об ошибках при работе с АРМ администратора

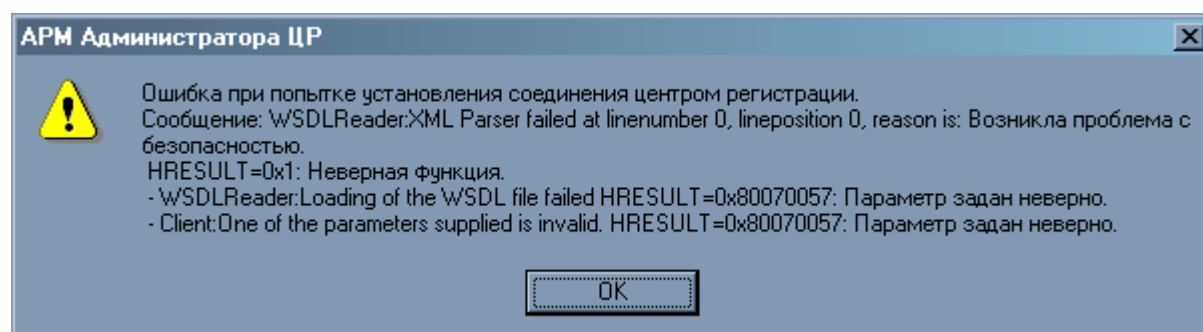
Ошибка -2147220991. CreateRequest. При формировании запроса на изготовление сертификата привилегированного пользователя появляется сообщение:



Возможная причина: Значения полей идентификационных данных привилегированного пользователя не соответствуют формату имен X.500

Рекомендуемое решение: Проверьте правильность заполнения полей на соответствие формату X.500. Данные поля не должны содержать служебных символов - кавычек, слешей и т.д.

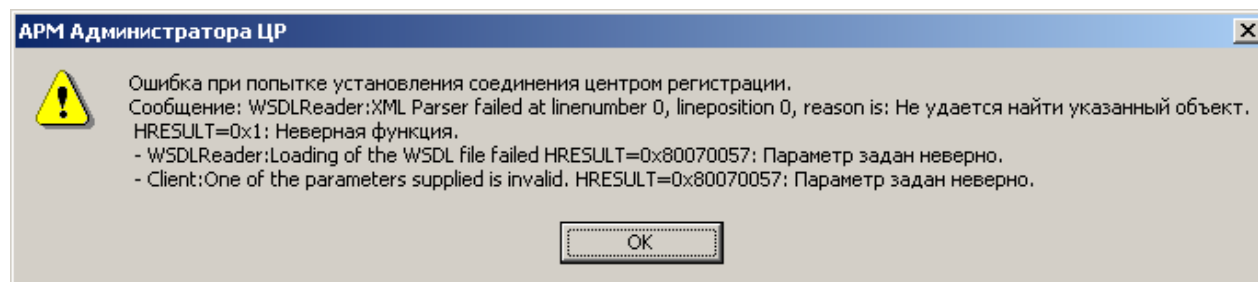
Ошибка при попытке установления соединения с ЦР (0x80070057). При инициализации подключения к ЦР (тестировании соединения между АРМ администратора и ЦР) появляется сообщение:



Возможная причина: На АРМ администратора и Центре Регистрации не удается проверить статус сертификатов или сертификаты недействительны - привилегированного пользователя, на котором осуществляется подключение к ЦР и сертификата web-сервера Центра Регистрации. В стандартном окне просмотра сертификата ОС Windows указанные сертификаты отображаются как недействительные (с красным крестом).

Рекомендуемое решение: Установите на ПЭВМ АРМ администратора все сертификаты уполномоченного лица Удостоверяющего центра – издателя сертификата привилегированного пользователя и все сертификаты уполномоченных лиц Удостоверяющих центров цепочки включая самоподписанный сертификат уполномоченного лица корневого Удостоверяющего центра, а также соответствующие списки отозванных сертификатов (CRL).

Ошибка при попытке установления соединения с ЦР (0x80070057). При инициализации подключения к ЦР (тестировании соединения между АРМ администратора и ЦР) появляется сообщение:



Возможная причина: В окне просмотра параметров подключения к ЦР неправильно установлен Адрес URL файла описания WSDL Центра Регистрации.

Рекомендуемое решение: Проверьте правильность задания указанного URL и внесите в него необходимые изменения (<https://ВнешнееИмяЦР/ra/ra.wsdl>)



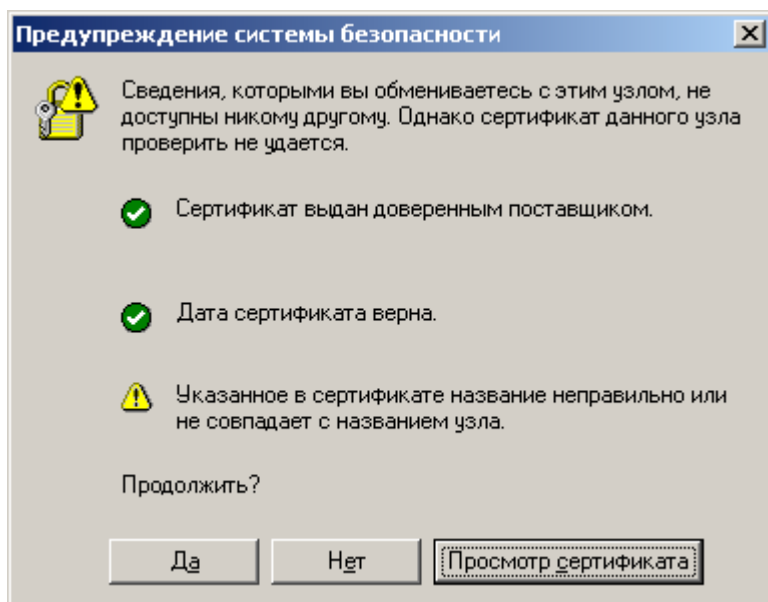
Довольно часто причиной возникновения ошибок при инициализации подключения к ЦР (при тестировании соединения между АРМ администратора и ЦР) являются ошибки соединения между указанными узлами, вызванные отсутствием физического подключения компонентов (АРМ администратора и ЦР), ошибками DNS, неверной настройкой Internet-подключений, влиянием межсетевых экранов на http и https трафик.

Для определения описанных причин необходимо последовательно проделать следующие действия:

С АРМ администратора ЦР выполните команду: **ping ИмяЦР**, где **ИмяЦР** – Имя Центра Регистрации (не IP-адрес, а именно имя), на которое выдан сертификат серверной аутентификации Центра Регистрации. Если при выполнении указанной команды появляется сообщение о превышении интервала ожидания для запроса, то необходимо проверить физическое подключение компонент к сети передачи данных и настройки DNS (при необходимости указать соответствие IP-адресов именам ПЭВМ в файле %systemroot%\system32\drivers\etc\hosts)

С АРМ администратора ЦР по протоколу **http** откройте тестовую страницу (например, <http://ИмяЦР/mmc.gif>, где **ИмяЦР** – Имя Центра Регистрации, на которое выдан сертификат серверной аутентификации Центра Регистрации, но сначала обязательно убедитесь в ее наличии на Центре Регистрации). Если при выполнении указанной команды страница не открывается, то на АРМ администратора проверьте настройки Internet Explorer (особое внимание уделите правильности настроек прокси-сервера, если такое используется), а также настройки межсетевых экранов, в том числе персональных, через которые проходит соединение между АРМ администратора ЦР и Центром Регистрации.

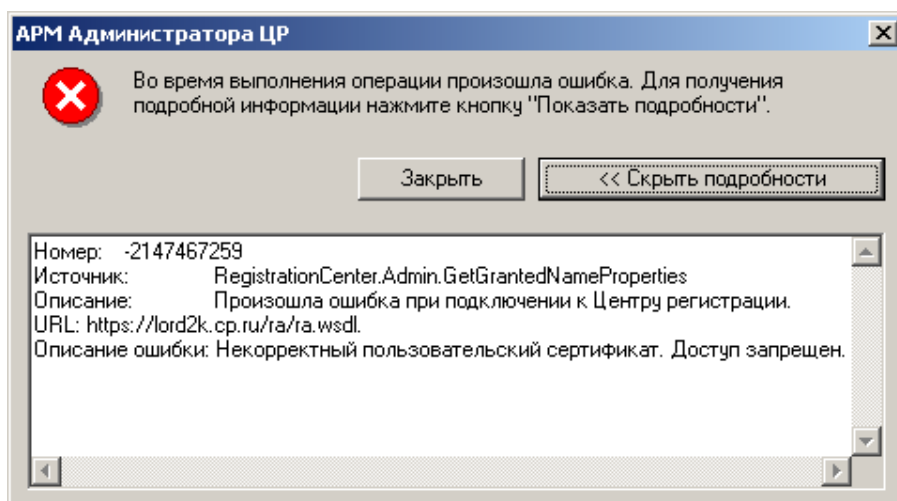
С АРМ администратора ЦР по протоколу **https** откройте страницу, указанную по адресу, содержащемуся в поле **Адрес URL файла описания WSDL Центра Регистрации** окна Свойств подключения к Центру регистрации - <https://ИмяЦР/ra/ra.wsdl>. Открытие указанной страницы должно сопровождаться только появлением сообщения о начале просмотра страниц через безопасное соединение. При появлении иных сообщений, связанных с проверкой сертификата серверной аутентификации Центра Регистрации (см. рисунок ниже) необходимо установить их причину и устранить указанное несоответствие.



Невозможность открытия страницы по протоколу **https** также может быть вызвана некорректной работой модуля сетевой аутентификации «КриптоПро TLS» (или его отсутствием). В связи с этим на ЦР и АРМ администратора ЦР проверьте отсутствие в журнале Приложений ошибочных сообщений вызванных этим модулем, а также службой инициализации «КриптоПро CSP» и службой хранения ключей «КриптоПро CSP». Дополнительно удостоверьтесь, что на ЦР введен серийный номер серверной Лицензии на «КриптоПро TLS»

С АРМ администратора ЦР по протоколу **https** откройте страницу <https://ИмяЦР/ra/ra.asp>. Должно появиться окно выбора сертификата подключения, после чего укажите необходимый сертификат привилегированного пользователя. Ошибка при открытии указанной страницы может быть вызвана отсутствием на Центре регистрации в хранилище Локальный компьютер/Промежуточные центры сертификации актуального списка отозванных сертификатов (CRL) либо недоступности списка отозванных сертификатов по точке распределения списков отозванных сертификатов (CDP), указанной в выбранном сертификате привилегированного пользователя. Для обеспечения автоматического и своевременного переноса списков отозванных сертификатов настройте параметры публикации CRL на Центре Сертификации и параметры задач, отвечающих за перенос CRL.

Ошибка -2147467259. При инициализации подключении к Центру регистрации появилось сообщение об ошибке

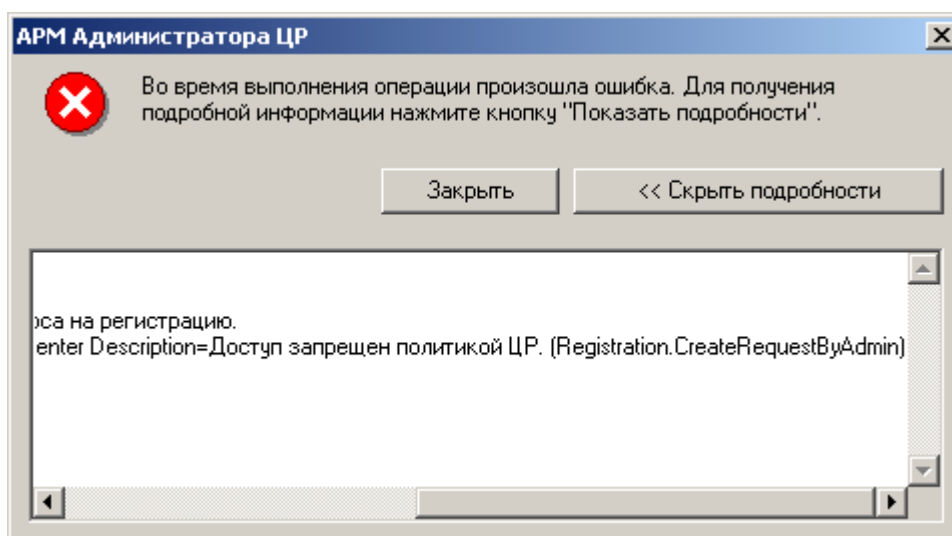
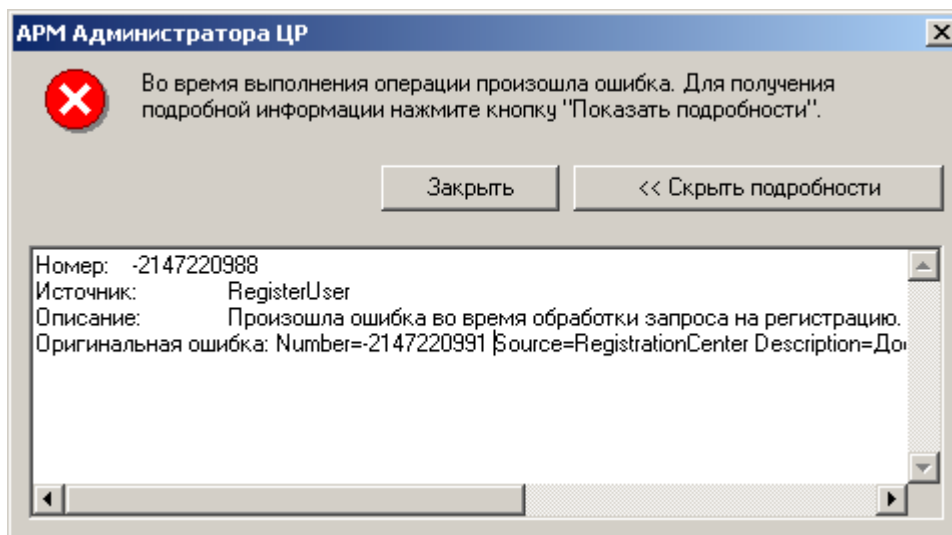


Возможная причина: Сертификат, на котором осуществляется подключение к Центру Регистрации недействителен (аннулирован (отозван), действие его

Руководство оператора Удостоверяющего центра ООО «КРИПТО-ПРО» (срса.cryptopro.ru)
приостановлено, срок его действия истек или не наступил) либо не содержит
необходимых областей использования ключа (Оператор УЦ, Администратор УЦ)

Рекомендуемое решение: Проверьте статус указанного сертификата

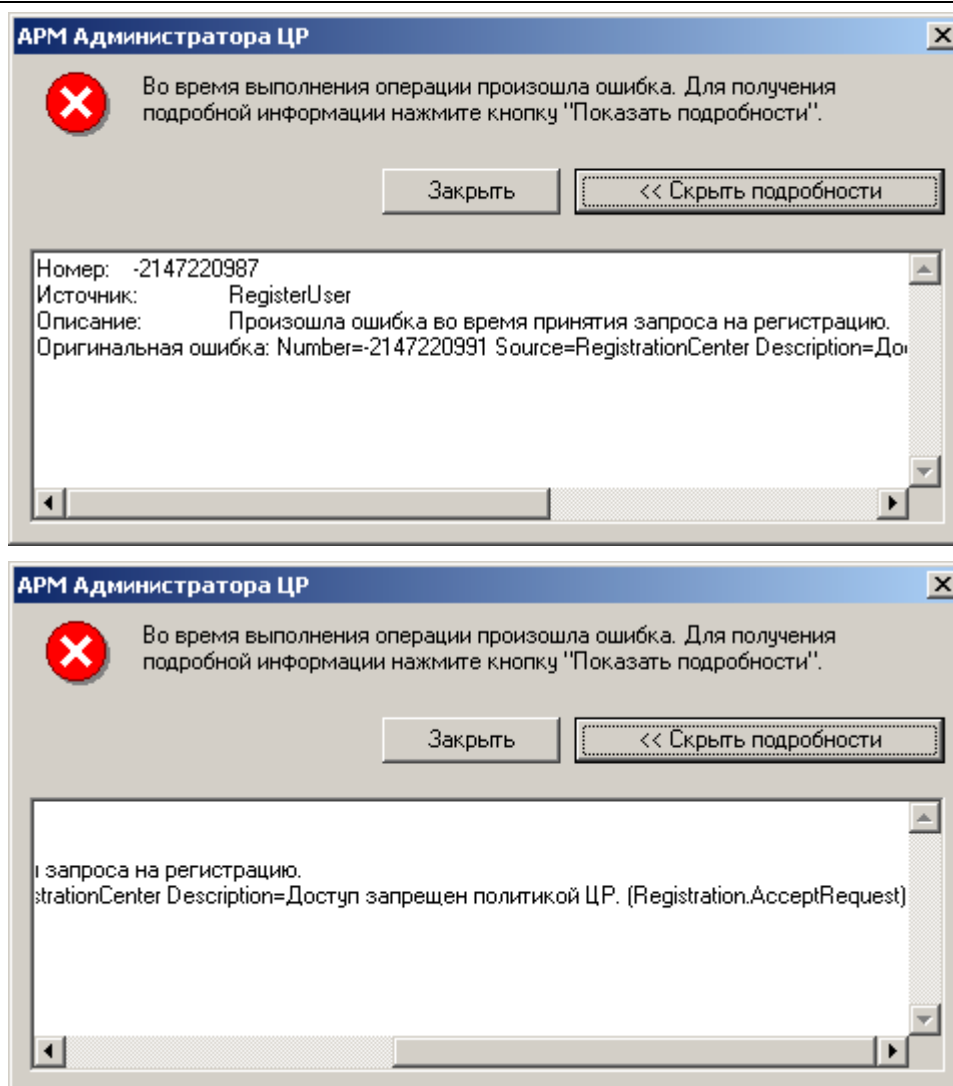
Ошибка -2147220988. Оригинальная ошибка -2147220991. В окне **Окончание регистрации пользователя** после нажатия на кнопку **Далее** появляется сообщение:



Возможная причина: У привилегированного пользователя, производящего регистрацию пользователя в Удостоверяющем центре не достаточно прав на выполнение метода **Registration.CreateRequestByAdmin**

Рекомендуемое решение: На Центре Регистрации необходимо осуществить настройку политики безопасности, позволяющую осуществлять выполнение указанного метода (Окно **Свойства: ЦР** на '**веб-узел**', вкладка **Безопасность**, метод **Registration.CreateRequestByAdmin**)

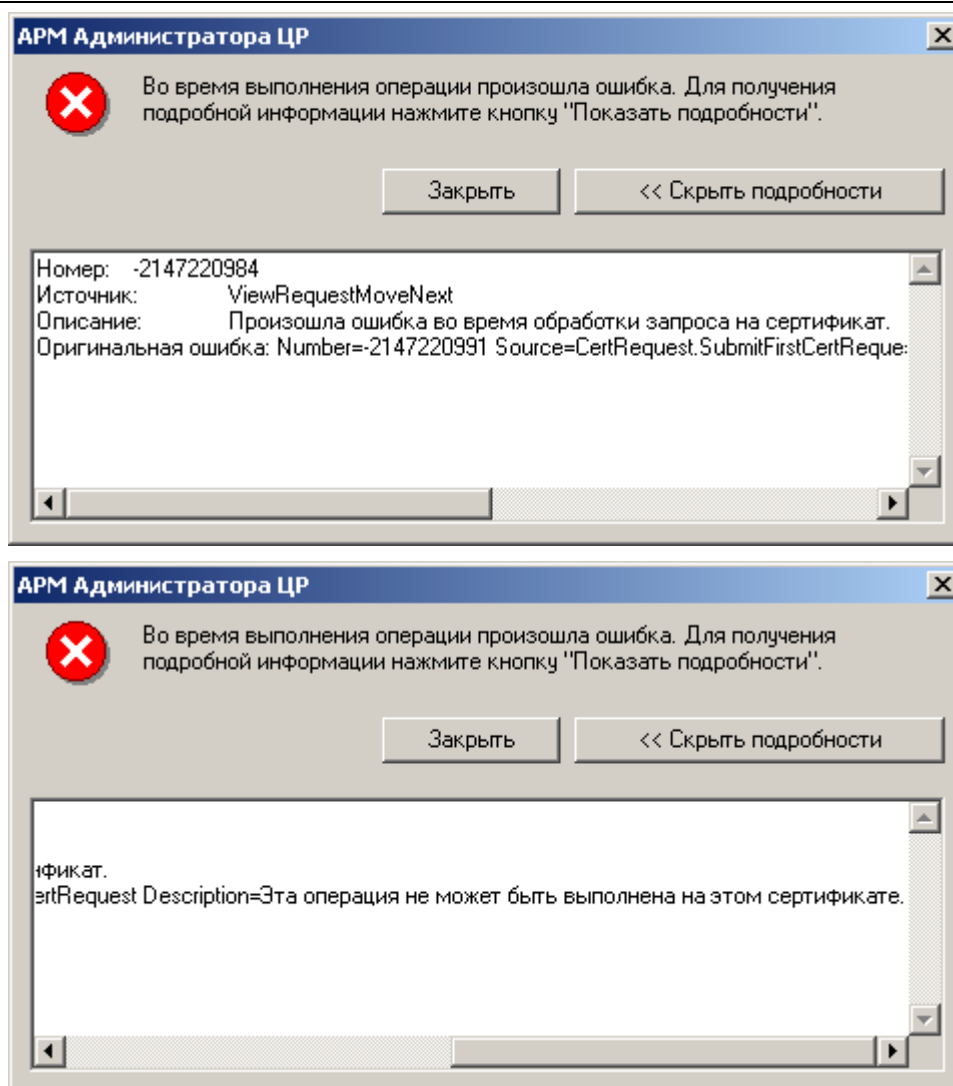
Ошибка -2147220987. Оригинальная ошибка -2147220991. В окне **Окончание регистрации пользователя** после нажатия на кнопку **Далее** (либо при принятии запроса на регистрацию) появляется сообщение:



Возможная причина: У привилегированного пользователя, производящего регистрацию пользователя в Удостоверяющем центре не достаточно прав на выполнение метода **Registration.AcceptRequest**.

Рекомендуемое решение: На Центре Регистрации необходимо осуществить настройку политики безопасности, позволяющую осуществлять выполнение указанного метода (Окно **Свойства: ЦР** на 'веб-узел', вкладка **Безопасность**, метод **Registration.AcceptRequest**).

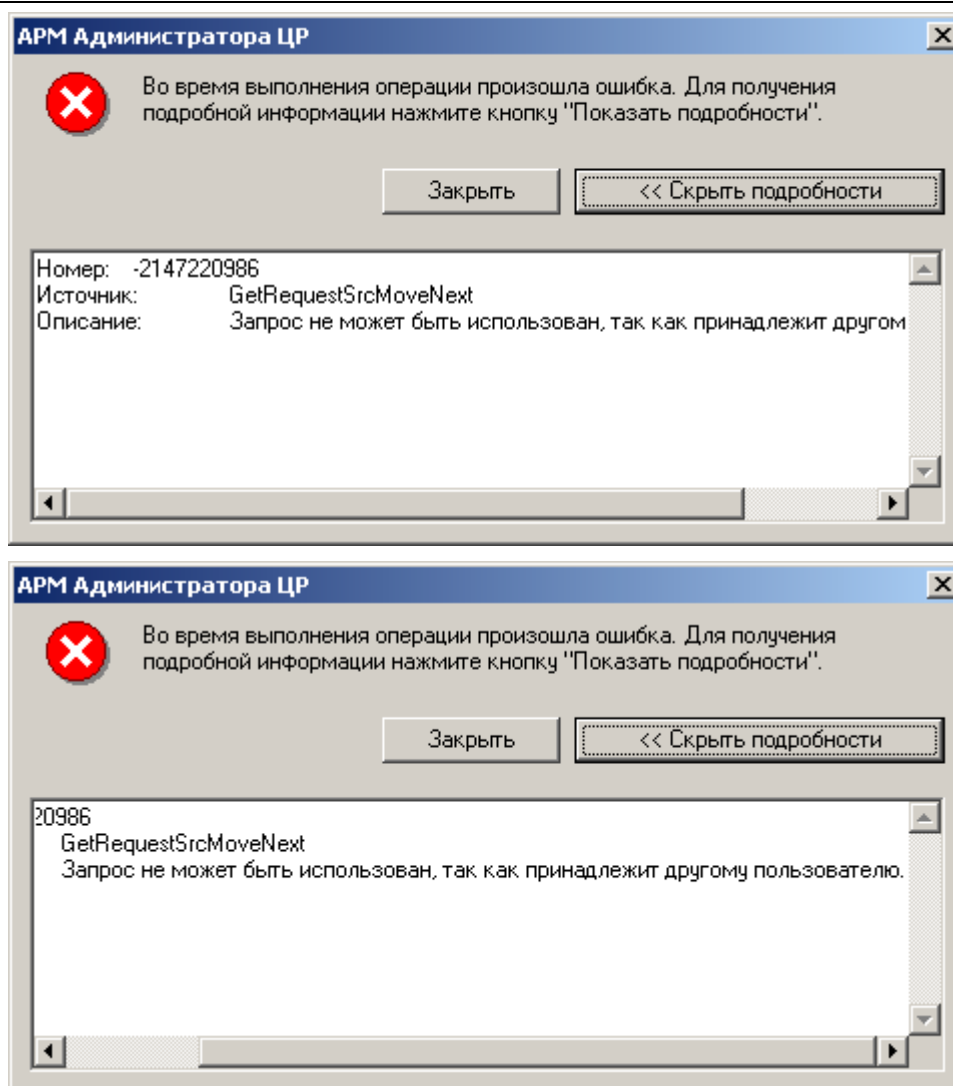
Ошибка -2147220984. Оригинальная ошибка -2147220991. После нажатия на кнопку **Далее** в окне **Просмотр запроса на сертификат** появляется сообщение



Возможная причина: Привилегированный пользователь не имеет прав на изготовление сертификата, содержащего области использования, указанные в запросе (шаблоне) на сертификат.

Рекомендуемое решение: На центре Регистрации осуществите настройку **Политики обработки неподписанных запросов** и добавьте необходимые области использования сертификата для роли привилегированного пользователя.

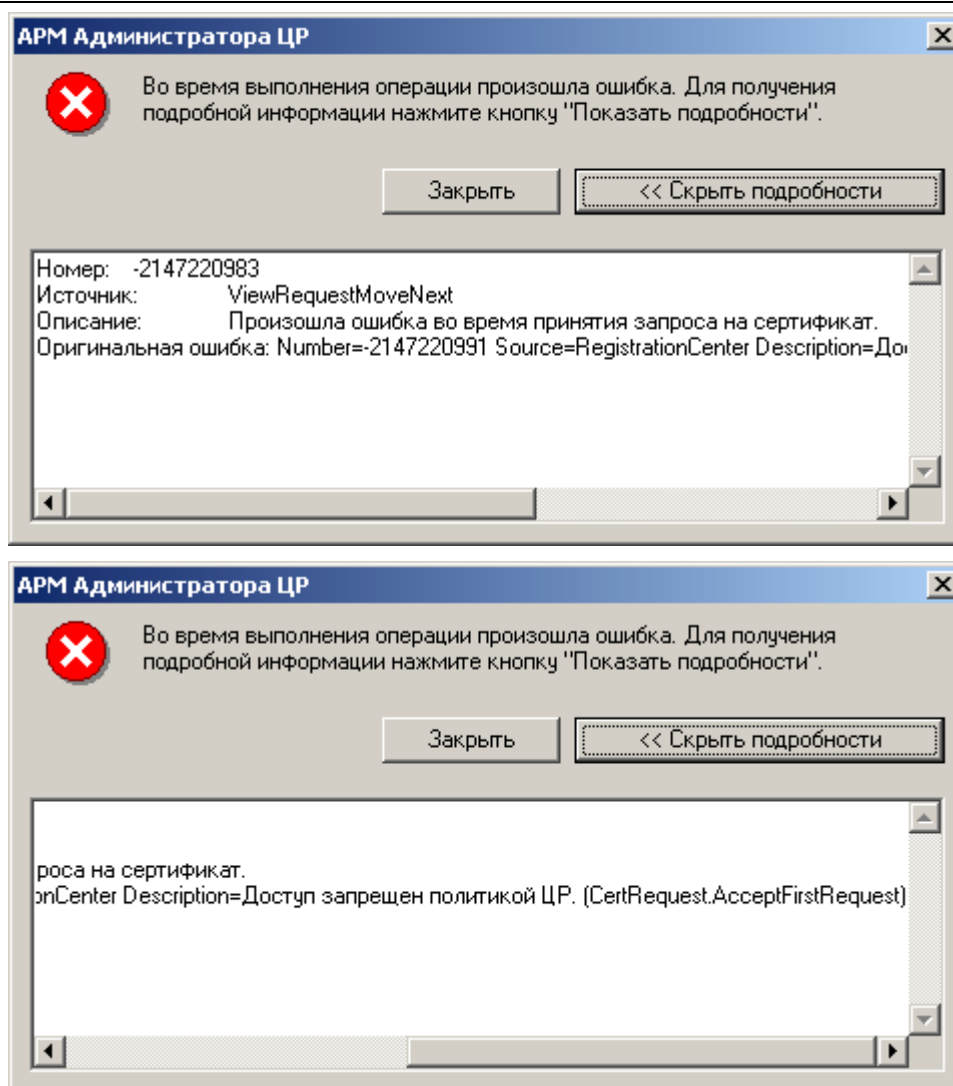
Ошибка -2147220986. После нажатия кнопку **Далее** в окне **Источник запроса на сертификат**, в случае выбора переключателя **Чтение запроса на сертификат из файла** появляется сообщение:



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

Рекомендуемое решение: Проверьте правильность формирования запроса на сертификат и соответствие идентификационных данных, содержащихся в запросе, идентификационным данным зарегистрированного пользователя. При необходимости снова сформируйте запрос на сертификат, исключая обнаруженные ошибки.

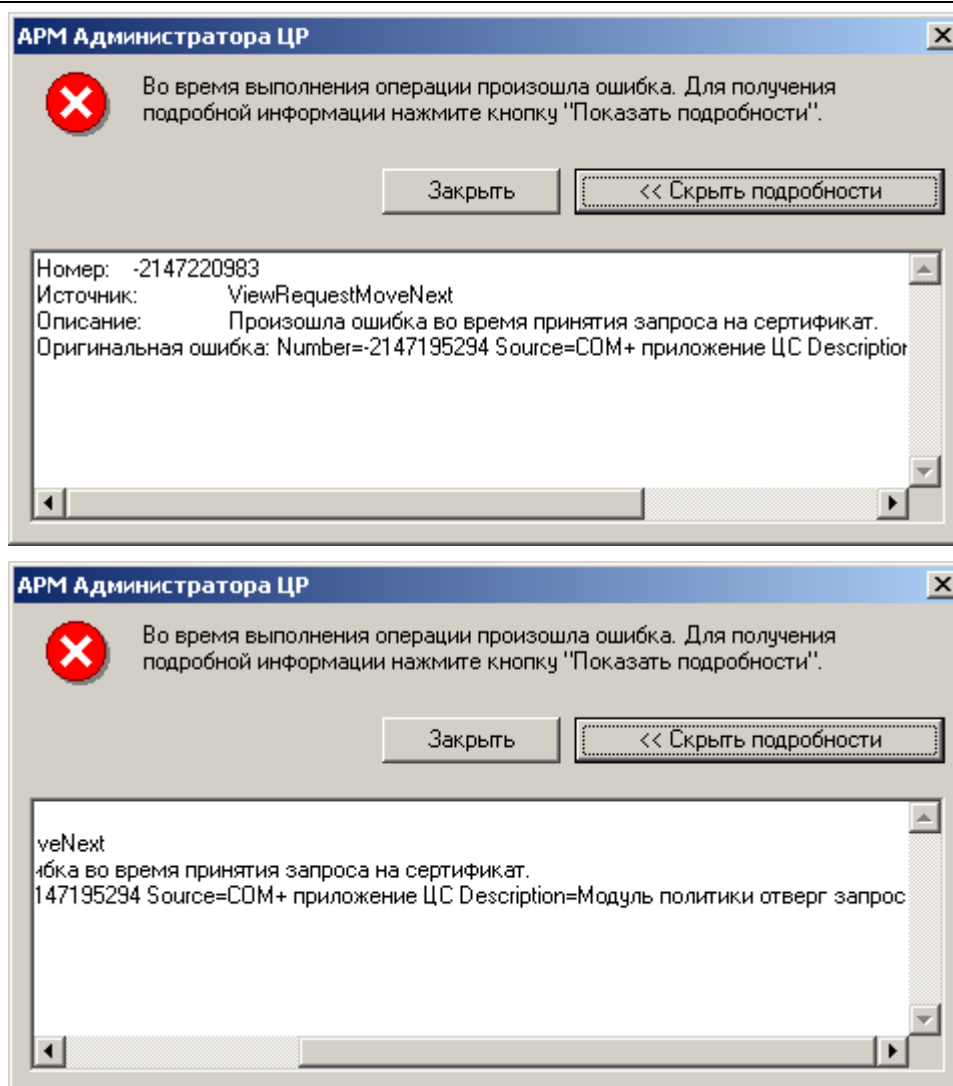
Ошибка -2147220983. Оригинальная ошибка -2147220991. После нажатия на кнопку **Далее** в окне **Просмотр запроса на сертификат** (либо при принятии запроса на сертификат) появляется сообщение



Возможная причина: У привилегированного пользователя, производящего изготовление сертификата пользователя в Удостоверяющем центре не достаточно прав на выполнение метода **CertRequest.AcceptFirstRequest**.

Рекомендуемое решение: На Центре Регистрации необходимо осуществить настройку политики безопасности, позволяющую осуществлять выполнение указанного метода (Окно **Свойства: ЦР** на 'веб-узел', вкладка **Безопасность**, метод **CertRequest.AcceptFirstRequest**).

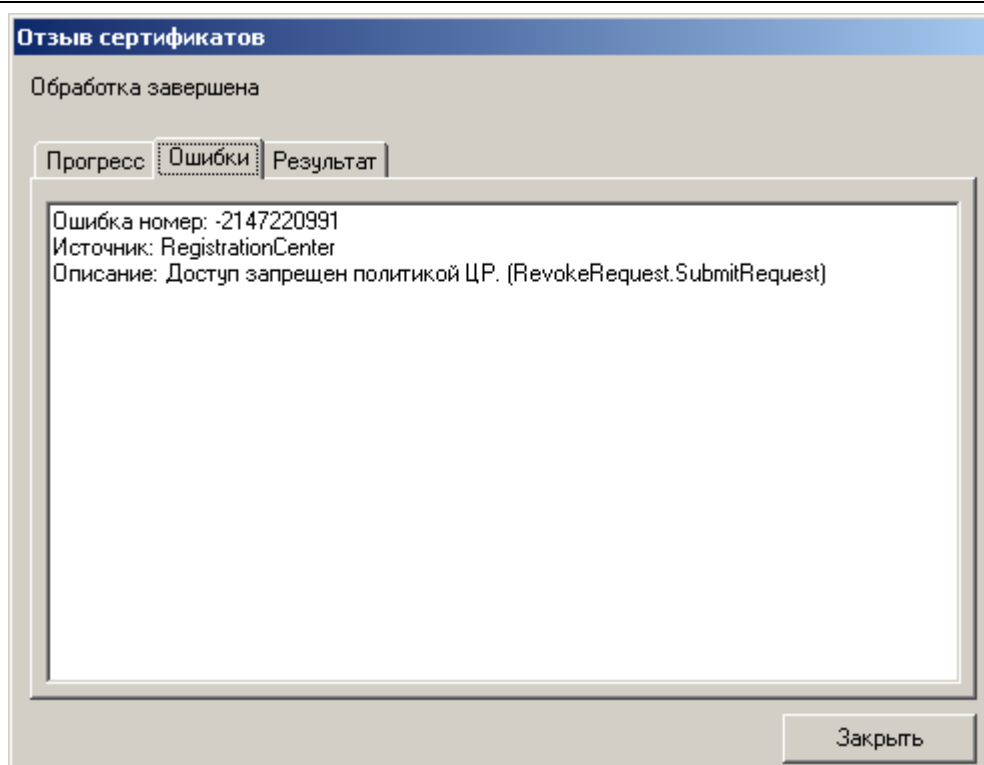
Ошибка -2147220983. После нажатия на кнопку **Далее** в окне **Просмотр запроса на сертификат** (при принятии запроса на сертификат) появляется сообщение



Возможная причина: Модуль политики Центра сертификации отверг запрос – наиболее вероятная причина – на вкладке **Использование ключа** окна **Свойства Модуля политики Центра Сертификации** в списке разрешенных областей использования сертификата отсутствует хотя бы одна область, содержащаяся в запросе на сертификат, либо поступивший запрос на сертификат не удовлетворяет настройкам **Политики имен** Модуля политики Центра Сертификации

Рекомендуемое решение: Просмотрите журнал Приложений ПЭВМ Центра Сертификации и установите конкретную причину возникшей ситуации, после чего внесите изменения в настройки Модуля политики Центра Сертификации, либо снова сформируйте запрос на сертификат, удовлетворяющий указанным политикам.

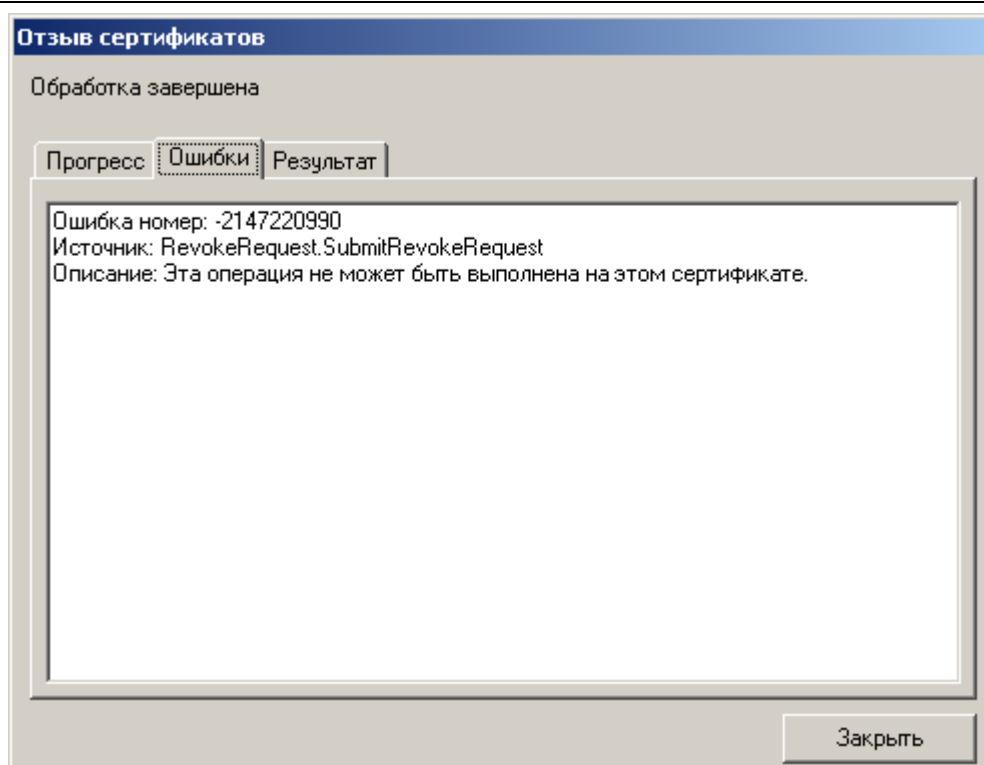
Ошибка -2147220991. RevokeRequest.SubmitRequest (RevokeRequest.SubmitHoldrequest/RevokeRequest.SubmitUnHoldRequest). При отзыве (приостановлении/возобновлении действия) сертификата привилегированным пользователем в окне **Отзыв сертификатов - Обработка завершена** возникает ошибка:



Возможная причина: У привилегированного пользователя, производящего отзыв (приостановление/возобновление действия) сертификата не достаточно прав на выполнение метода **RevokeRequest.SubmitRequest (RevokeRequest.SubmitHoldrequest/RevokeRequest.SubmitUnHoldRequest)**

Рекомендуемое решение: На Центре Регистрации необходимо осуществить настройку политики безопасности, позволяющую осуществлять выполнение указанного метода (Окно **Свойства: ЦР** на 'веб-узел', вкладка **Безопасность**, метод **RevokeRequest.SubmitRequest (RevokeRequest.SubmitHoldrequest/RevokeRequest.SubmitUnHoldRequest)**)

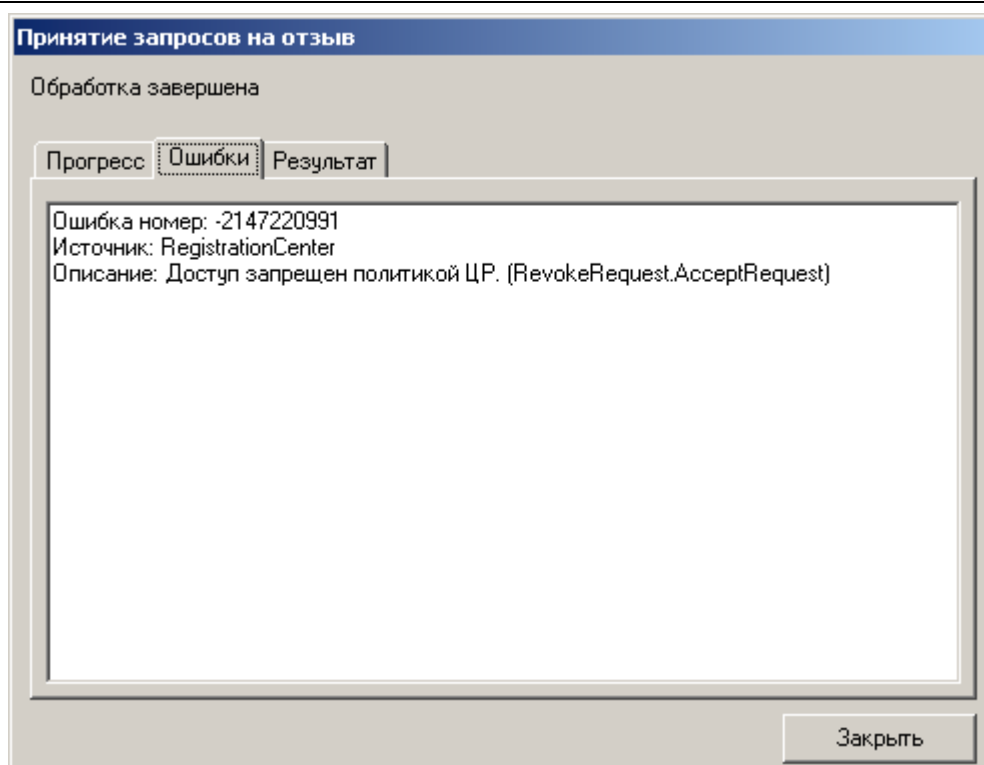
Ошибка -2147220990. RevokeRequest.SubmitRequest. При отзыве (приостановлении/возобновлении действия) сертификата привилегированным пользователем в окне **Отзыв сертификатов - обработка завершена** возникает ошибка



Возможная причина: Отзываемый сертификат содержит хотя бы одну область использования (поле **Extended Key Usage**), присутствие которой в сертификате не позволяет привилегированному пользователю отозвать (приостановить/возобновить действие) указанный сертификат (данная область использования отсутствует в списке разрешенных для указанного привилегированного пользователя)

Рекомендуемое решение: На Центре Регистрации осуществите настройку **Политики обработки запросов на отзыв** и для привилегированного пользователя, осуществляющего отзыв (приостановление/возобновление действия) сертификатов, добавьте необходимые области использования

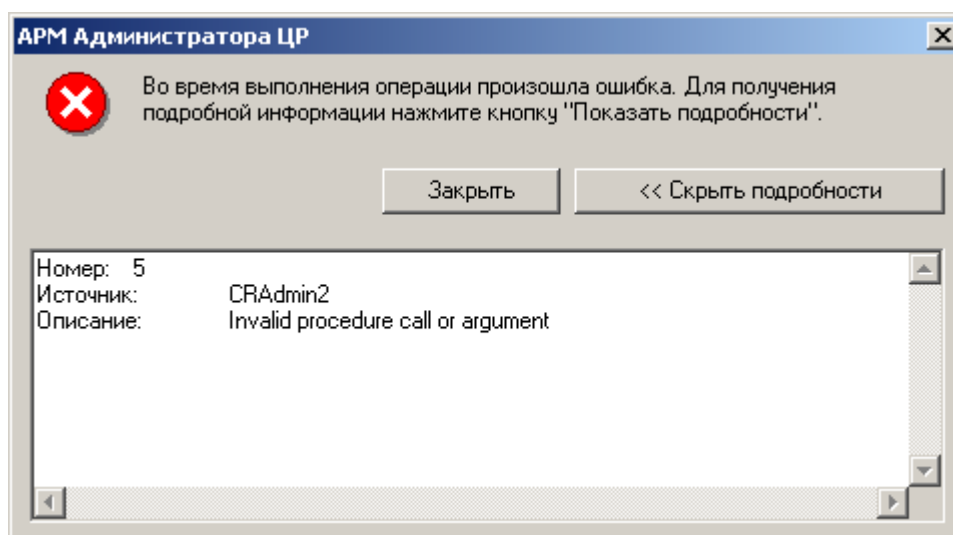
Ошибка -2147220991. RevokeRequest.AcceptRequest. При принятии запроса на отзыв (приостановление/возобновление действия) сертификата привилегированным пользователем в окне **Отзыв сертификатов - обработка завершена** возникает ошибка



Возможная причина: У привилегированного пользователя, производящего принятие запроса на отзыв (приостановление/возобновление действия) сертификата не достаточно прав на выполнение метода **RevokeRequest.AcceptRequest**

Рекомендуемое решение: На Центре Регистрации необходимо осуществить настройку политики безопасности, позволяющую осуществлять выполнение указанного метода (Окно **Свойства: ЦР** на 'веб-узел', вкладка **Безопасность**, метод **RevokeRequest.AcceptRequest**)

Ошибка 5. При генерации ключей подписей и изготовлении сертификата ключа подписи появляется сообщение:



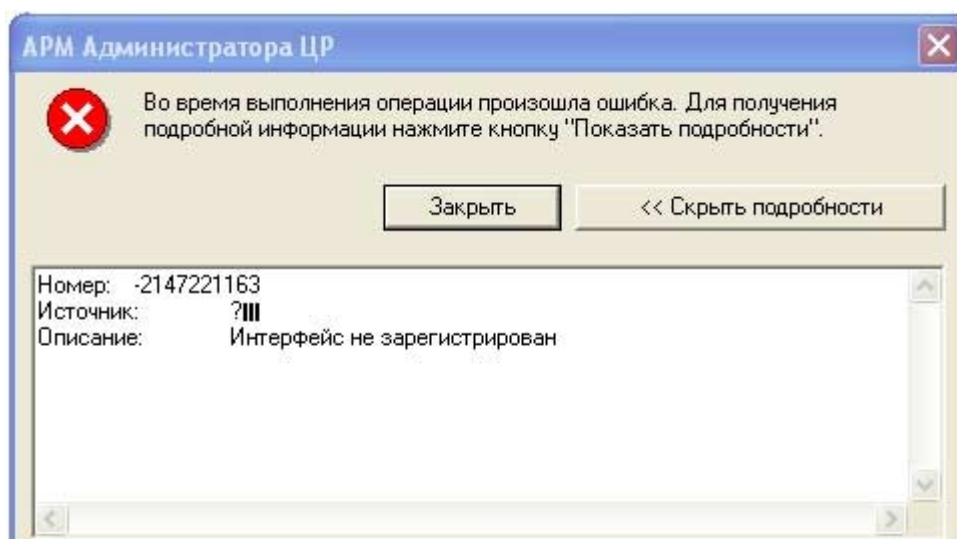
Возможная причина:

1. На ключевом носителе нет свободного места для записи закрытого ключа подписи (контейнера закрытого ключа), либо нет места для сохранения изготовленного сертификата ключа подписи в контейнер закрытого ключа
2. Во время генерации ключей (в окне выбора считывателя ключевого носителя, при отказе в установке пароля) была нажата кнопка **Отмена**

Рекомендуемое решение:

1. Убедитесь в наличии достаточного свободного места на ключевом носителе, в случае его отсутствия произведите его очистку либо используйте другой носитель. Дополнительно протестируйте носитель на наличие аппаратных ошибок.
2. Снова осуществите процедуру генерации ключей без нажатия на кнопки **Отмена** окон приложения

Ошибка -2147221163. При выборе пункта контекстного меню **Свойства** узла АРМ администратора ЦР возникает сообщение об ошибке



Возможная причина: Одна или несколько библиотек ПО АРМ администратора были разрегистрированы по причине возможного сбоя работы ОС или установки нового программного обеспечения.



Раздел 1. «Требования для установки и работы с приложением» документа «ЖТЯИ.00016-01 90 04-ЛУ. КриптоПро УЦ. Руководство администратора» определяет:

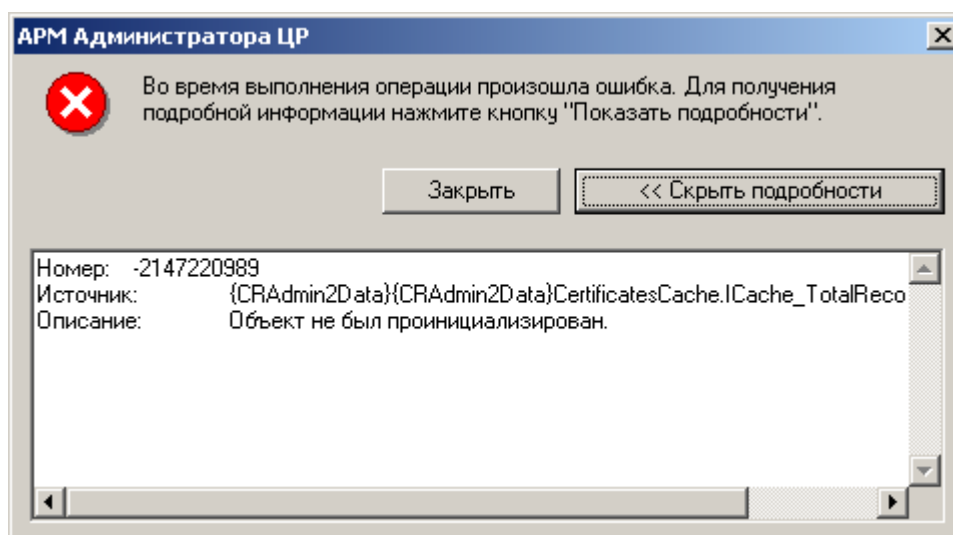
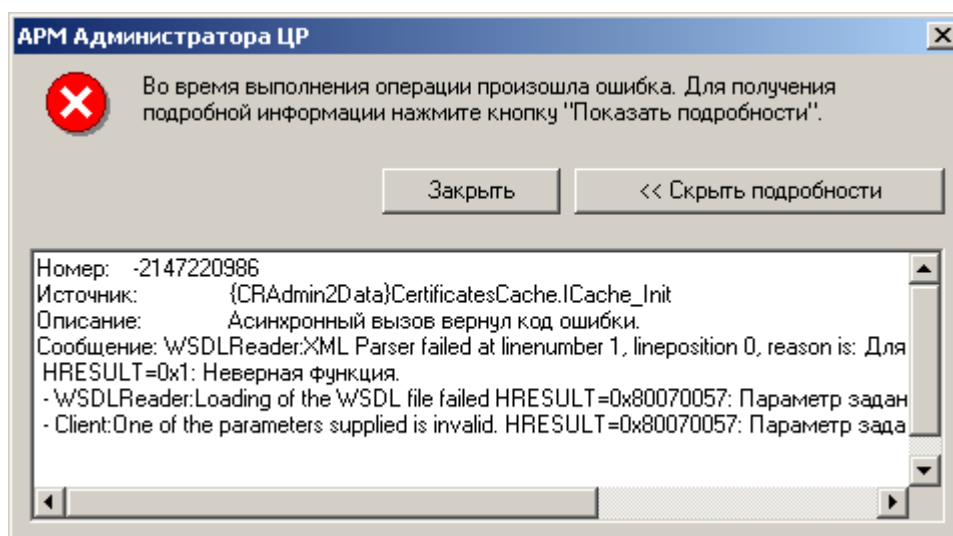
Для установки и эксплуатации АРМ администратора ЦР необходимо следующее программное обеспечение:

- Операционная система Microsoft Windows 2000 (Professional или Server);
- Пакеты обновлений:
 - Microsoft Windows 2000 Service Pack 4
- Программная библиотека CAPICOM.dll версии 2.0.0.1 (<http://www.microsoft.com/downloads/release.asp?ReleaseID=44155>)
- Microsoft MMC Console 1.2;
- Microsoft Internet Explorer 5.0 (и выше);
- Средство криптографической защиты (СКЗИ) КриптоПро CSP;
- Модуль аутентификации СКЗИ КриптоПро CSP (КриптоПро TLS).

Установка на АРМ администратора ЦР другого системного и прикладного программного обеспечения НЕ ДОПУСКАЕТСЯ!

Рекомендуемое решение: Удалить с ПЭВМ АРМ администратора ЦР «лишнее» ПО и переустановить ПО АРМ администратора ЦР

Ошибка -2147220986. При переходе между узлами (например, Сертификаты и Пользователи) окна АРМ администратора ЦР, либо при инициализации подключения появляется сообщение

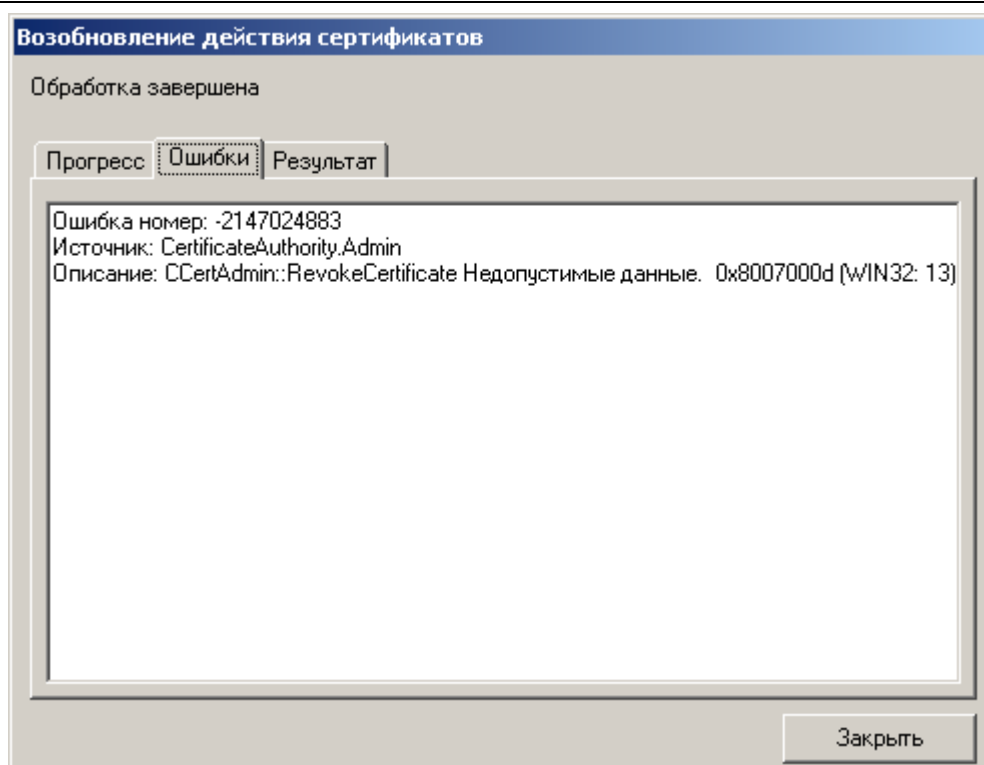


Возможная причина:

1. Переход между узлами осуществлялся достаточно быстро (например, администратор выбрал левой кнопкой мыши узел Сертификаты, а затем, не дождавшись отображения списка изданных сертификатов, выбрал узел Запросы на сертификат), что вызвало сбой при загрузке данных с Центра Регистрации
2. При инициализации подключения администратор сразу после открытия списка подчиненных узлов выбрал один из них. Окончательно не завершилась инициализация подключения, что вызвало невозможность просмотра содержимого выбранного узла и появление данного сообщения

Рекомендуемое решение: Закрыть приложение АРМ администратора ЦР, после чего загрузить его снова. В работе с ПО АРМ администратора не торопиться, поскольку простой клик левой кнопкой мыши на одном из узлов АРМ администратора ЦР вызывает выполнение большого количества операций (создание сессии, ее инициализации, передача данных с Центра Регистрации, формирование/проверка ЭЦП передающихся данных, а также их шифрование/расшифрование и т.д.).

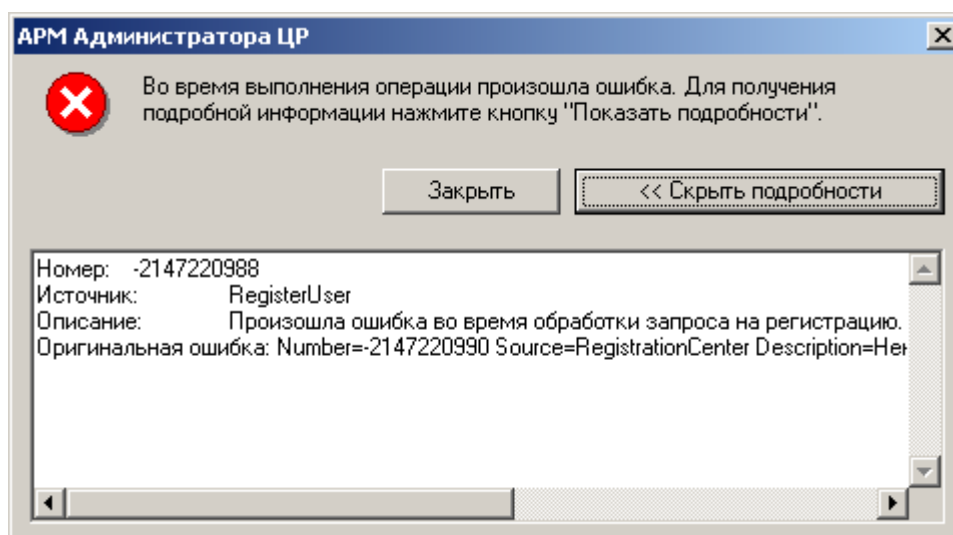
Ошибка -2147024883. При возобновлении/приостановлении действия сертификата появляется сообщение

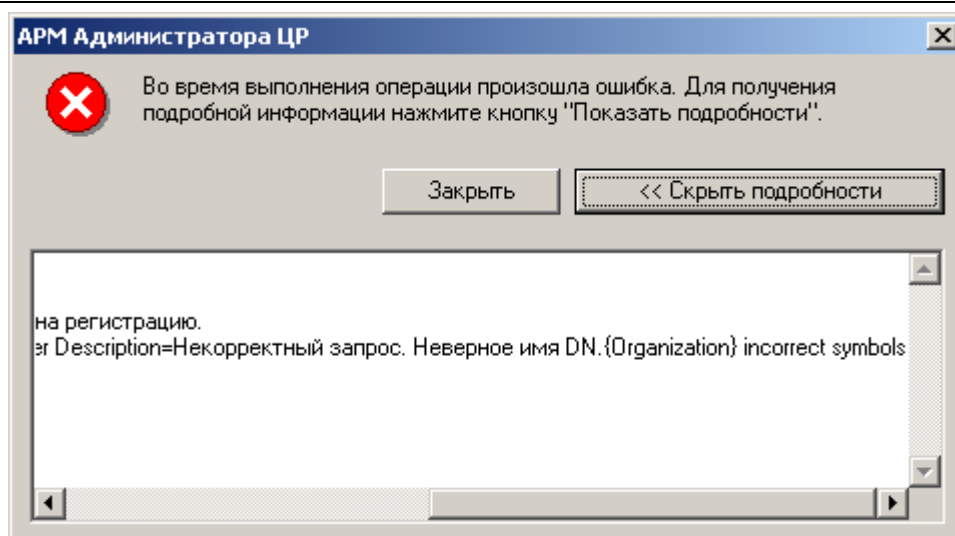


Возможная причина: Сертификат, действие которого администратор пытается приостановить/возобновить, уже отозван

Рекомендуемое решение: Действие сертификата, который ранее был уже отозван, нельзя приостановить или возобновить

Ошибка -2147220988. Оригинальная ошибка -2147220990. При регистрации пользователя появляется сообщение

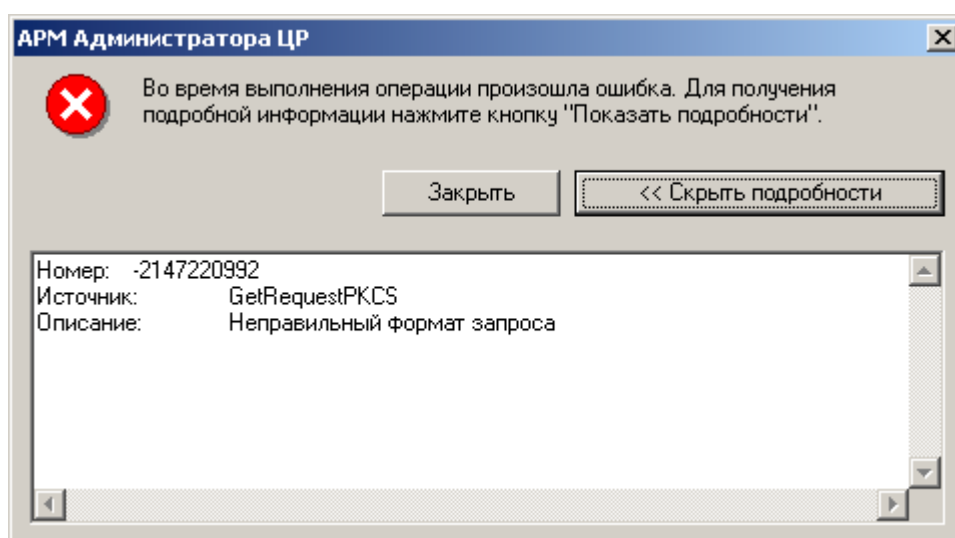




Возможная причина: Значения поля (в описываемом случае поля Organization) не соответствует формату имен X.500

Рекомендуемое решение: Проверьте правильность заполнения полей на соответствие формату X.500. Данные поля не должны содержать служебных символов - кавычек, слешей и т.д., поле Страна/Регион (Country) должно соответствовать формату двухсимвольного кода Страны/Региона согласно X.500 (например, RU)

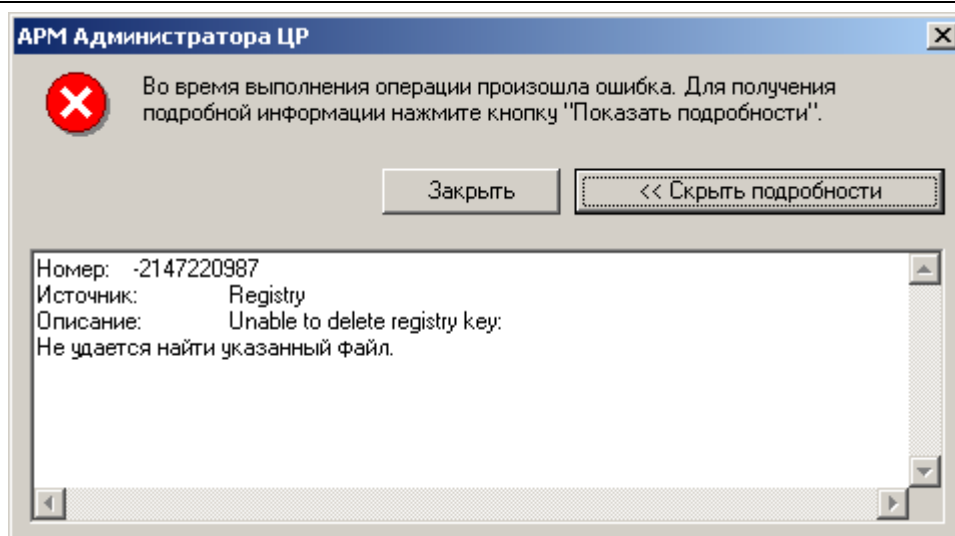
Ошибка -2147220992. GetRequestPKCS. При регистрации пользователя на основании идентификационных данных, содержащихся в файле запроса на сертификат появляется сообщение:



Возможная причина: Формат файла запроса на сертификат не соответствует PKCS#10

Рекомендуемое решение: Снова сформировать файл запроса на сертификат ключа подписи, удовлетворяющий формату PKCS#10. Типичной ошибкой формирования запроса на сертификат ключа подписи является добавление в конец файла дополнительных символов – 0D, 0A.

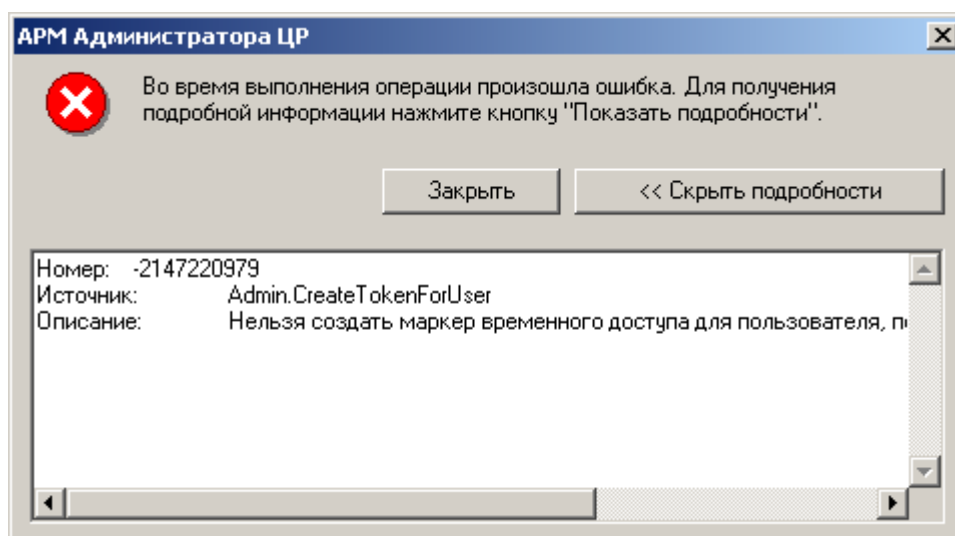
Ошибка 2147220987. Unable to delete registry key. После нажатия на кнопку **Далее** в окне **Установка сертификата** АРМ администратора ЦР (флаг **Автоматически подтвердить запрос** установлен) появляется сообщение:

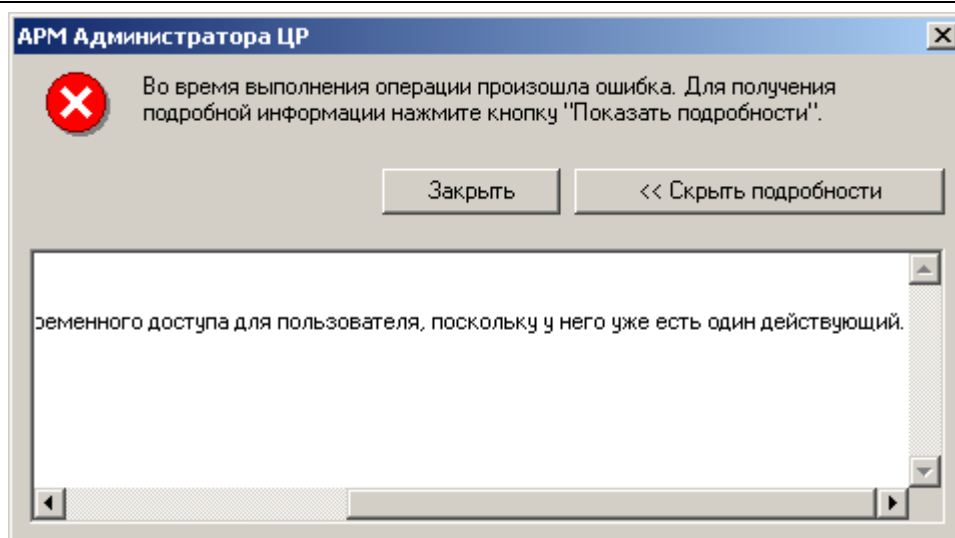


Возможная причина: У привилегированного пользователя, осуществившего изготовление сертификата ключа подписи не достаточно прав на выполнение метода **CertRequest.ConfirmRequest**. В журнале Приложений ОС должны быть зарегистрированы соответствующие события, содержащие информацию об ошибочном выполнении указанного метода

Рекомендуемое решение: На Центре Регистрации необходимо осуществить настройку политики безопасности, позволяющую осуществлять выполнение указанного метода (Окно **Свойства: ЦР** на 'веб-узел', вкладка **Безопасность**, метод **CertRequest.ConfirmRequest**)

Ошибка -2147220979 в методе AdminCreateTokenForUser. При создании маркера временного доступа появляется сообщение:





Возможная причина: Пользователь, для которого создается маркер временного доступа, уже имеет действующий маркер

Рекомендуемое решение: Нет необходимости создавать новый маркер временного доступа – пользователь должен использовать предоставленный ранее маркер



Аналогичная ошибка возникает в том случае, если у пользователя, для которого необходимо создать маркер временного доступа, отсутствует ключевая фраза, данный пользователь является владельцем хотя бы одного действующего сертификата, в очереди для обработки находится хотя бы один запрос на изготовление сертификата, направленный данным пользователем

21. Перечень терминов

Аутентификация

Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Закрытый ключ

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

Запрос на сертификат

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

Запрос на отзыв сертификата

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

Идентификация

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

Ключ (криптографический ключ)

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

Ключевая пара

Открытый и закрытый ключи.

Ключевой носитель

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

Компрометация ключа

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

1. Потеря ключевых носителей.
2. Потеря ключевых носителей с их последующим обнаружением.
3. Увольнение сотрудников, имевших доступ к ключевой информации.
4. Нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа.
5. Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.

6. Нарушение печати на сейфе с ключевыми носителями.
7. Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника)

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

Открытый ключ

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

Плановая смена ключей

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

Проверка электронной подписи документа

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

Сертификат

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

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

Список отзыва

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

Центр Сертификации (Удостоверяющий центр)

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

Центр регистрации

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

Шифрование

Процесс зашифрования или расшифрования.

Шифрование информации – взаимнооднозначное математическое (криптографическое) преобразование, зависящее от ключа (секретный параметр преобразования), которое ставит в соответствие блоку открытой информации, представленной в некоторой цифровой кодировке, блок шифрованной информации, также

представленной в цифровой кодировке. Термин шифрование объединяет в себе два процесса: зашифрование и расшифрование информации.

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

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

Электронная цифровая подпись (ЭЦП)

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

Проверка электронной цифровой подписи под блоком открытой информации производится с помощью криптографического преобразования и открытого ключа, соответствующего секретному ключу, участвовавшего 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.

22. Перечень сокращений

<i>CRL</i>	Список отозванных сертификатов (Certificate Revocation List)
<i>DN</i>	Отличительное имя (Distinguished Name)
<i>ITU-T</i>	Международный комитет по телекоммуникациям (International Telecommunication Union)
<i>IETF</i>	Internet Engineering Task Force
<i>LDAP</i>	Lightweight Directory Access Protocol. Упрощенный протокол доступа к справочнику
<i>TM</i>	Устройство хранения информации на таблетке touch-memory
<i>PKI</i>	Public Key Infrastructure. Аналог ИОК.
<i>RDN</i>	Относительное отличительное имя (Relative Distinguished Name)
<i>URI</i>	Единый идентификатор ресурса (Uniform Resource Identifier)
<i>URL</i>	Единый локатор ресурса (Uniform Resource Locator)
<i>АС</i>	Автоматизированная система
<i>АРМ</i>	Автоматизированное рабочее место
<i>ДСЧ</i>	Датчик случайных чисел
<i>ИОК</i>	Инфраструктура Открытых Ключей
<i>КП</i>	Конечный пользователь
<i>НСД</i>	Несанкционированный доступ
<i>ОС</i>	Операционная система
<i>ПАК</i>	Программно-аппаратный комплекс
<i>ПО</i>	Программное обеспечение
<i>СОР</i>	Список отозванных сертификатов (Certificate Revocation List)
<i>СС</i>	Справочник сертификатов открытых ключей. Сетевой справочник
<i>ЦР</i>	Центр Регистрации
<i>ЦС</i>	Центр Сертификации
<i>УЦ</i>	Удостоверяющий центр
<i>ЭЦП</i>	Электронная цифровая подпись

23. Перечень рисунков

Рисунок 1. Окно Мастера установки ПО АРМ администратора	8
Рисунок 2. Окно ввода информации о пользователе, организации и серийного номера лицензии Мастера установки АРМ администратора	9
Рисунок 3. Окно определения типа установки Мастера установки АРМ администратора	9
Рисунок 4. Окно подтверждения установки ПО Мастера установки АРМ администратора	10
Рисунок 5. Окно состояния установки Мастера установки АРМ администратора	11
Рисунок 6. Окно окончания работы Мастера установки АРМ администратора	11
Рисунок 7. Внешний вид приложения АРМ администратора	13
Рисунок 8. Запуск задачи создания запроса на сертификат привилегированного пользователя	14
Рисунок 9. Окно определения параметров ключа Мастера создания запроса на сертификат администратора	15
Рисунок 10. Окно ввода информации об администраторе Мастера создания запроса на сертификат администратора.	16
Рисунок 11. Сохранение запроса на сертификат	16
Рисунок 12. Запуск задачи установки сертификата привилегированного пользователя	18
Рисунок 13. Окно выбора файла с сертификатом Мастера установки сертификата администратора	18
Рисунок 14. Окно просмотра сертификата Мастера установки сертификата администратора	19
Рисунок 15. Окно завершения установки сертификата администратора	19
Рисунок 16. Запуск задачи создания подключения к ЦР	20
Рисунок 17. Мастер подключения к ЦР	20
Рисунок 18. Задание адреса ЦР в Мастере подключения к ЦР	21
Рисунок 19. Выбор сертификата администратора в Мастере подключения к ЦР	21
Рисунок 20. Окно свойств АРМ администратора	23
Рисунок 21. Окно свойств подключений к ЦР в АРМ администратора ЦР	26
Рисунок 22. Активизация подключения к ЦР в окне консоли АРМ администратора	27
Рисунок 23. Окно консоли администратора с активированными элементами дерева подключения	28
Рисунок 24. Пример контекстного меню в консоли администратора	28
Рисунок 25. Пункт меню настройки состава полей списка	29
Рисунок 26. Окно изменения состава полей списка содержимого папки	30
Рисунок 27. Настройка отображения области описания фильтрации записей	31
Рисунок 28. Область отображения условий фильтрации	31
Рисунок 29. Окно выбора фильтрации записей по типу	32
Рисунок 30. Окно выбора фильтрации записей по значениям полей	33
Рисунок 31. Окно выбора поля для фильтрации по значению полей записей	33

Рисунок 32. Окно выбора фильтрации запросов на сертификат по признаку подписания.....	34
Рисунок 33. Окно свойств запроса на сертификат.....	35
Рисунок 34. Окно свойств запроса на регистрацию.....	35
Рисунок 35. Окно свойств запроса на отзыв сертификата.....	36
Рисунок 36. Окно свойств запроса на приостановление действия сертификата.....	36
Рисунок 37. Окно свойств запроса на возобновление действия сертификата	37
Рисунок 38. Окно опций экспорта сертификатов.....	38
Рисунок 39. Задача плановой смены ключа администратора	40
Рисунок 40. Окно приглашения задачи плановой смены ключа администратора ...	41
Рисунок 41. Окно завершения задачи плановой смены ключа администратора	41
Рисунок 42. Запуск задачи создания нового пользователя	43
Рисунок 43. Окно определения источника запроса на сертификат в Мастере регистрации пользователя	43
Рисунок 44. Окно ввода информации о пользователе Мастера регистрации пользователя	44
Рисунок 45. Окно установки параметров ключа Мастера создания сертификата ...	44
Рисунок 46. Окно определения типа сертификата Мастера создания сертификата	45
Рисунок 47. Окно запроса на сертификат Мастера создания сертификата	45
Рисунок 48. Окно установки выпущенного сертификата Мастера создания сертификата	46
Рисунок 49. Установка переключателей Установить сертификат в хранилище и Автоматически подтвердить запрос	46
Рисунок 50. Окно сохранения цепочки сертификатов Мастера создания сертификата	47
Рисунок 51. Окно окончания работы Мастера создания сертификата	47
Рисунок 52. Окно выбора файла с запросом на сертификат Мастера регистрации пользователя	48
Рисунок 53. Запуск задачи выпуска нового сертификата пользователя.....	49
Рисунок 54. Окно определения источника запроса на сертификат в Мастере создания сертификата пользователя	50
Рисунок 55. Окно выбора шаблона сертификата Мастера создания сертификата пользователя	50
Рисунок 56. Окно просмотра запроса на сертификат Мастера создания сертификата пользователя	51
Рисунок 57. Окно установки сертификата Мастера создания сертификата пользователя	51
Рисунок 58. Окно сохранения цепочки сертификатов Мастера создания сертификата пользователя.....	52
Рисунок 59. Запуск задачи отзыва сертификата пользователя.....	52
Рисунок 60. Окно указания причины отзыва в задаче отзыва сертификата пользователя	53
Рисунок 61. Запуск задачи приостановления действия сертификата пользователя	53
Рисунок 62. Окно указания периода приостановления действия сертификата пользователя	54

Рисунок 63. Запуск задачи возобновления действия сертификата пользователя...	55
Рисунок 64. Сообщение об ошибке при попытке возобновления действия отозванного сертификата.....	55
Рисунок 65. Запуск задачи удаления зарегистрированного пользователя.....	56
Рисунок 66. Окно предупреждения при удалении пользователя	57
Рисунок 67. Окно сообщения о невозможности удаления пользователя	57
Рисунок 68. Запуск задачи печати сертификата пользователя.....	59
Рисунок 69. Запуск задачи создания маркера временного доступа	61
Рисунок 70. Просмотр данных пользователя Мастера создания маркера временного доступа	61
Рисунок 71. Окно ошибки о невозможности создания маркера временного доступа пользователю Мастера создания маркера временного доступа	62
Рисунок 72. Окно отображения созданного маркера временного доступа Мастера создания маркера временного доступа	62
Рисунок 73. Окно задач элемента Центр Сертификации текущего активного подключения к ЦР	64
Рисунок 74. Папка Журнал.....	65
Рисунок 75. Окно задач папки Журнал	66
Рисунок 76. Запуск задачи генерации ключей Центра Сертификации	67
Рисунок 77. Окно определения параметров ключа Мастера создания ключа ЦС....	68
Рисунок 78. Окно определения имени ключевого контейнера Мастера создания ключа ЦС.....	68
Рисунок 79. Журнал регистрации событий Центра Регистрации	69
Рисунок 80. Окно просмотра информации о событии	70
Рисунок 81. Событие Помещен запрос на регистрацию	71
Рисунок 82. Событие Одобрен запрос на регистрацию	72
Рисунок 83. Событие Отклонен запрос на регистрацию.....	73
Рисунок 84. Событие Помещен запрос на сертификат	74
Рисунок 85. Событие Одобрен запрос на сертификат.....	75
Рисунок 86. Событие Отклонен запрос на сертификат.....	76
Рисунок 87. Установка сертификата подтверждена пользователем	77
Рисунок 88. Событие Помещен запрос на отзыв сертификата	78
Рисунок 89. Одобрен запрос на отзыв сертификата	79
Рисунок 90. Событие Отклонен запрос на отзыв сертификата	80
Рисунок 91. Событие Помещен запрос на первый сертификат	81
Рисунок 92. Событие Запрошен список отозванных сертификатов	82
Рисунок 93. Событие Опубликован список отозванных сертификатов	83
Рисунок 94. Событие Удален пользователь.....	84
Рисунок 95. Событие Запрос на регистрацию не помещен в очередь.....	85
Рисунок 96. Событие Запрос на регистрацию не одобрен	86
Рисунок 97. Событие Запрос на регистрацию не отклонен.....	87
Рисунок 98. Событие Запрос на сертификат не помещен.....	88

Рисунок 99. Событие Запрос на сертификат не одобрен.....	89
Рисунок 100. Событие Запрос на сертификат не отклонен.....	90
Рисунок 101. Событие Установка сертификата не подтверждена	91
Рисунок 102. Событие Запрос на отзыв сертификата не помещен.....	92
Рисунок 103. Событие Запрос на отзыв сертификата не одобрен	93
Рисунок 104. Событие Запрос на отзыв сертификата не отклонен.....	94
Рисунок 105. Событие Запрос на первый сертификат не помещен	95
Рисунок 106. Событие Список отозванных сертификатов не запрошен.....	96
Рисунок 107. Событие Список отозванных сертификатов не опубликован	97
Рисунок 108. Событие Пользователь не удален	98
Рисунок 109. Выбор режима просмотра записей Журнала в новом окне	99
Рисунок 110. Просмотр Журнала регистрации событий в отдельном окне.....	99
Рисунок 111. Вызов окна "Изменить столбцы"	100
Рисунок 112. Окно Изменить столбцы	100
Рисунок 113. Выбор необходимого типа события	102
Рисунок 114. Пример отображения событий одного типа.....	103
Рисунок 115. Выбор всех зарегистрированных типов событий	104
Рисунок 116. Задание фильтра просмотра зарегистрированных событий.....	105
Рисунок 117. Настройка фильтра Журнала регистрации событий.....	105
Рисунок 118. Выбор поля фильтрации	106
Рисунок 119. Задание параметров Фильтра	106
Рисунок 120. Просмотр событий журнала с использованием фильтра.....	107
Рисунок 121. Отображение параметров фильтрации событий Журнала	108
Рисунок 122. Отмена использования фильтрации событий Журнала	108
Рисунок 123. Экспорт списка событий Журнала.....	109
Рисунок 124. Окно определения имени, расположения и формата выходного файла	109
Рисунок 125. Экспорт сертификата ключа подписи	111
Рисунок 126. Подтверждение экспорта сертификата	112
Рисунок 127. Задание опций экспорта сертификатов	112
Рисунок 128. Успешное завершение процедуры экспорта сертификата	113
Рисунок 129. Сообщение об ошибке при экспорте сертификата	114
Рисунок 130. Экспорт группы сертификатов в один файл.....	114
Рисунок 131. Экспорт запроса на сертификат ключа подписи.....	115
Рисунок 132. Подтверждение экспорта запроса на сертификат.....	115
Рисунок 133. Задание опций экспорта запроса на сертификат.....	116
Рисунок 134. Успешное завершение процедуры экспорта запроса на сертификат	116
Рисунок 135. Сообщение об ошибке при экспорте запроса на сертификат.....	117
Рисунок 136. Экспорт группы запросов на сертификат	118
Рисунок 137. Экспорт запроса на отзыв сертификата.....	119
Рисунок 138. Подтверждение экспорта запроса на отзыв сертификата.....	120

Рисунок 139. Задание опций экспорта запроса на отзыв сертификата.....	120
Рисунок 140. Успешное завершение процедуры экспорта запроса на отзыв сертификата	120
Рисунок 141. Сообщение об ошибке при экспорте запроса на отзыв сертификата.....	121
Рисунок 142. Запуск консоли mms	124
Рисунок 143. Окно консоли Консоль1	124
Рисунок 144. Переименование корневого узла созданной консоли	125
Рисунок 145. Выбор пункта меню Добавить/Удалить оснастку... ..	126
Рисунок 146. Окно Добавить/Удалить оснастку.....	127
Рисунок 147. Окно Добавить изолированную оснастку.....	128
Рисунок 148. Окно консоли управления Консоль1 после добавления необходимых изолированных оснасток	129
Рисунок 149. Создание нового узла консоли управления	130
Рисунок 150. Выбор нового узла для добавления оснасток.....	131
Рисунок 151. Окно консоли управления Консоль1 после добавления нового узла.....	132
Рисунок 152. Окно консоли Администрирование УЦ.....	133

24. 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. <i>PKCS #7: Cryptographic Message Syntax Standard</i> . Version 1.5, November 1993. |
| [PKCS-10] | RSA Laboratories. <i>PKCS #10: Certification Request Syntax Standard</i> . |