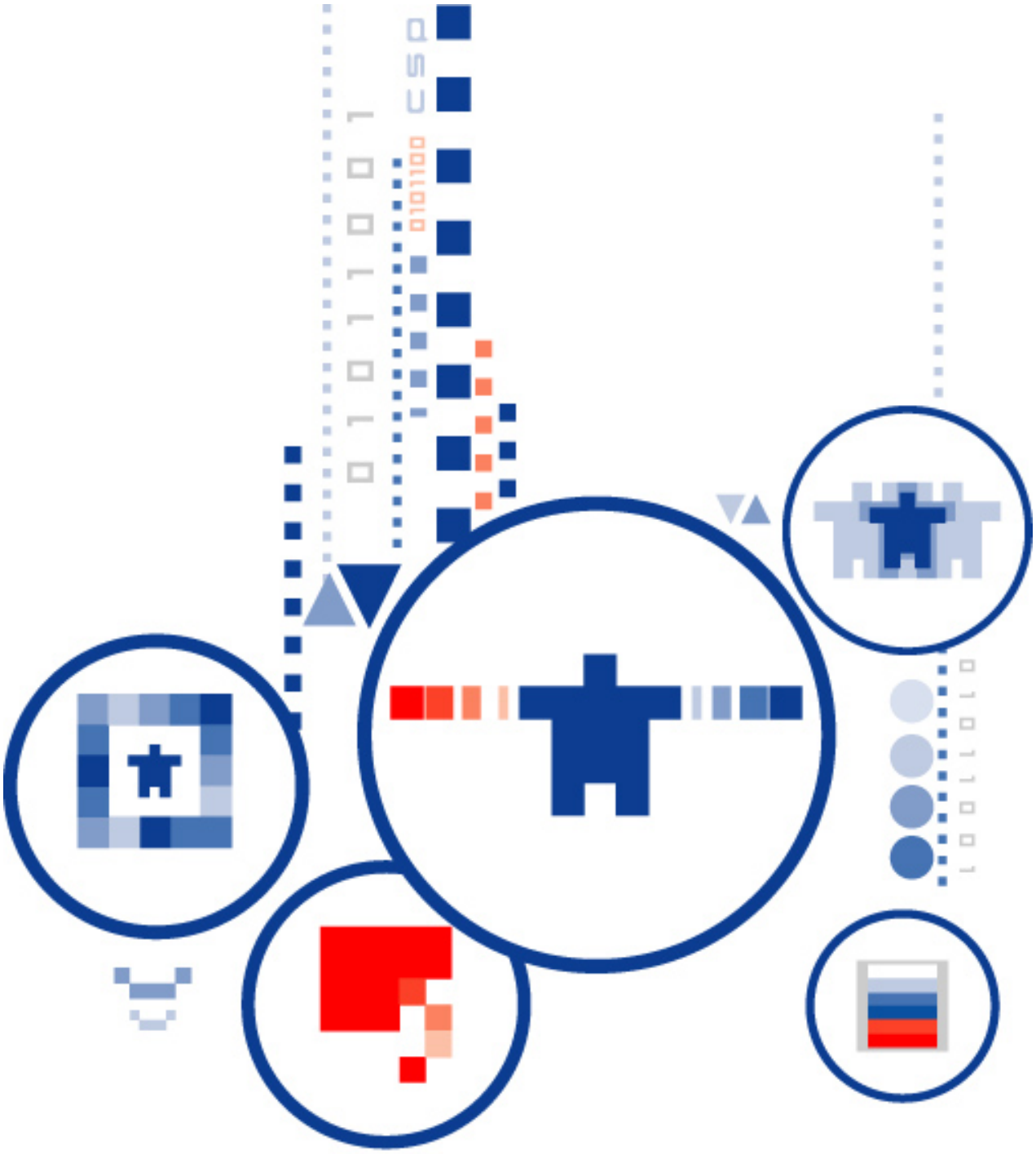
УТВЕРЖДЕН
ЖТЯИ.00035-01 90 17-ЛУ

ЖТЯИ.00035-01 90 17



КриптоПро УЦ

программно-аппаратный комплекс
удостоверяющий центр

Ошибки, возникающие при эксплуатации

АННОТАЦИЯ

Настоящий документ содержит список известных проблем, появление которых возможно при эксплуатации программно-аппаратного комплекса «Удостоверяющий Центр «КриптоПро УЦ», в документе указываются причины возникновения сбойных ситуаций, приводятся конкретные рекомендации по их устранению.

Настоящий документ призван оказать помощь администраторам Удостоверяющих центров в обеспечении эффективной и бесперебойной работы ПК «КриптоПро УЦ».

Информация о разработчике ПК «КриптоПро УЦ»:

ООО "Крипто-Про"

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

Телефон: (495) 780 4820

Факс: (495) 780 4820

http://www.CryptoPro.ru

E-mail: info@CryptoPro.ru

СОДЕРЖАНИЕ

1. Общие рекомендации по устранению возникших ошибок 4
2. Ошибки, возникающие на Центре Сертификации 7
3. Ошибки, возникающие на Центре Регистрации 9
4. Ошибки, возникающие на АРМ Администратора ЦР..... 13
5. Ошибки, вызванные аппаратно-программной несовместимостью устройств (в том числе устройств считывания ключевых носителей), установленных на ПЭВМ компонент ПК «КриптоПро УЦ»..... 33
6. Особенности эксплуатации разных типов ключевых носителей. 35

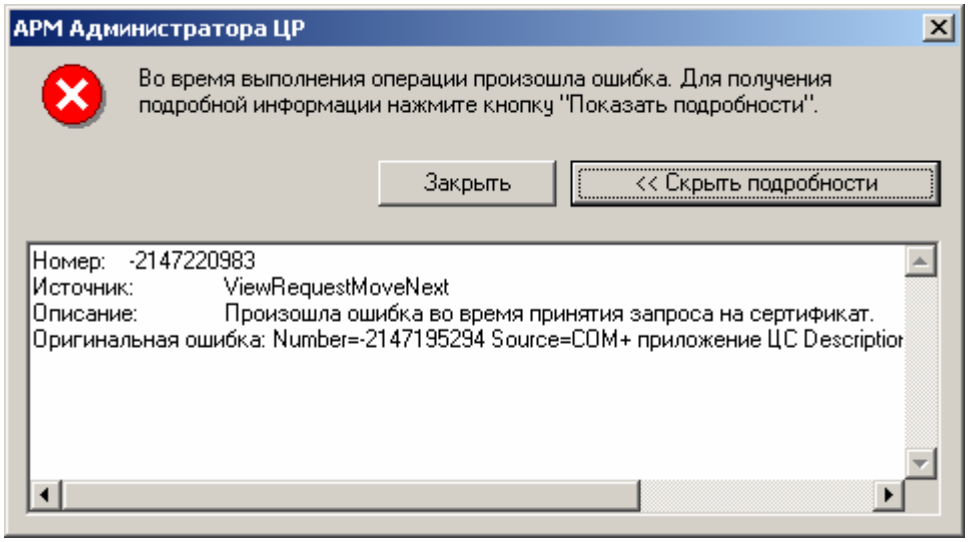
1. Общие рекомендации по устранению возникших ошибок

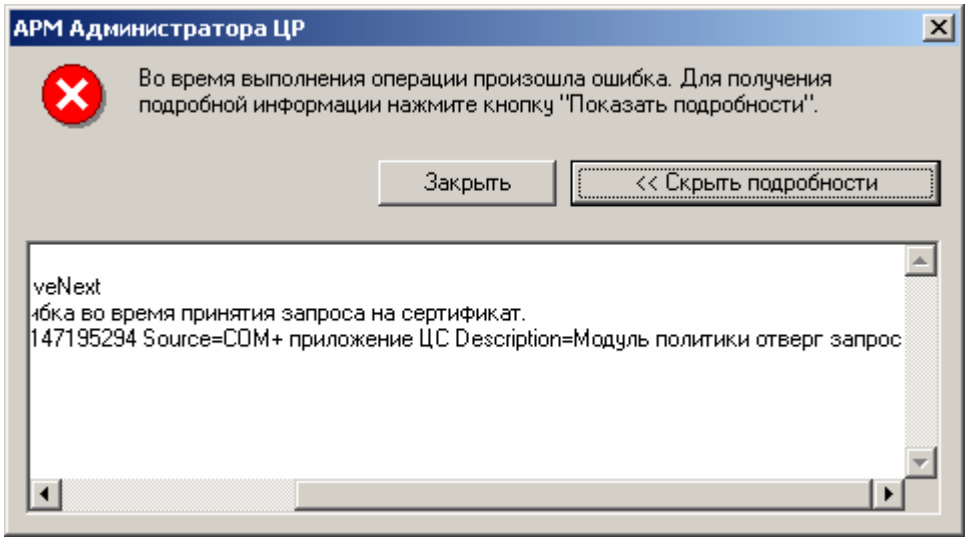
При возникновении ошибочных сообщений, возникающих во время эксплуатации программного комплекса «КриптоПро УЦ», внимательно ознакомьтесь с текстом появляющегося сообщения. Установите – на каком компоненте Удостоверяющего центра произошла ошибка (например, появление ошибки на АРМ администратора ЦР может быть причиной настройки Политик Центра Регистрации и Центра Сертификации, а следовательно, источником ошибки может быть ПЭВМ Центра Регистрации и Центра Сертификации).

Внимательно просмотрите журналы регистрации событий (журналы операционной системы – особо журнал Приложений) и постарайтесь уточнить причину возникновения сбойной ситуации и окончательно устранить возникновение данного события.

Порядок действий Администратора Удостоверяющего Центра по устранению ошибочных ситуаций удобно рассмотреть на конкретном примере.

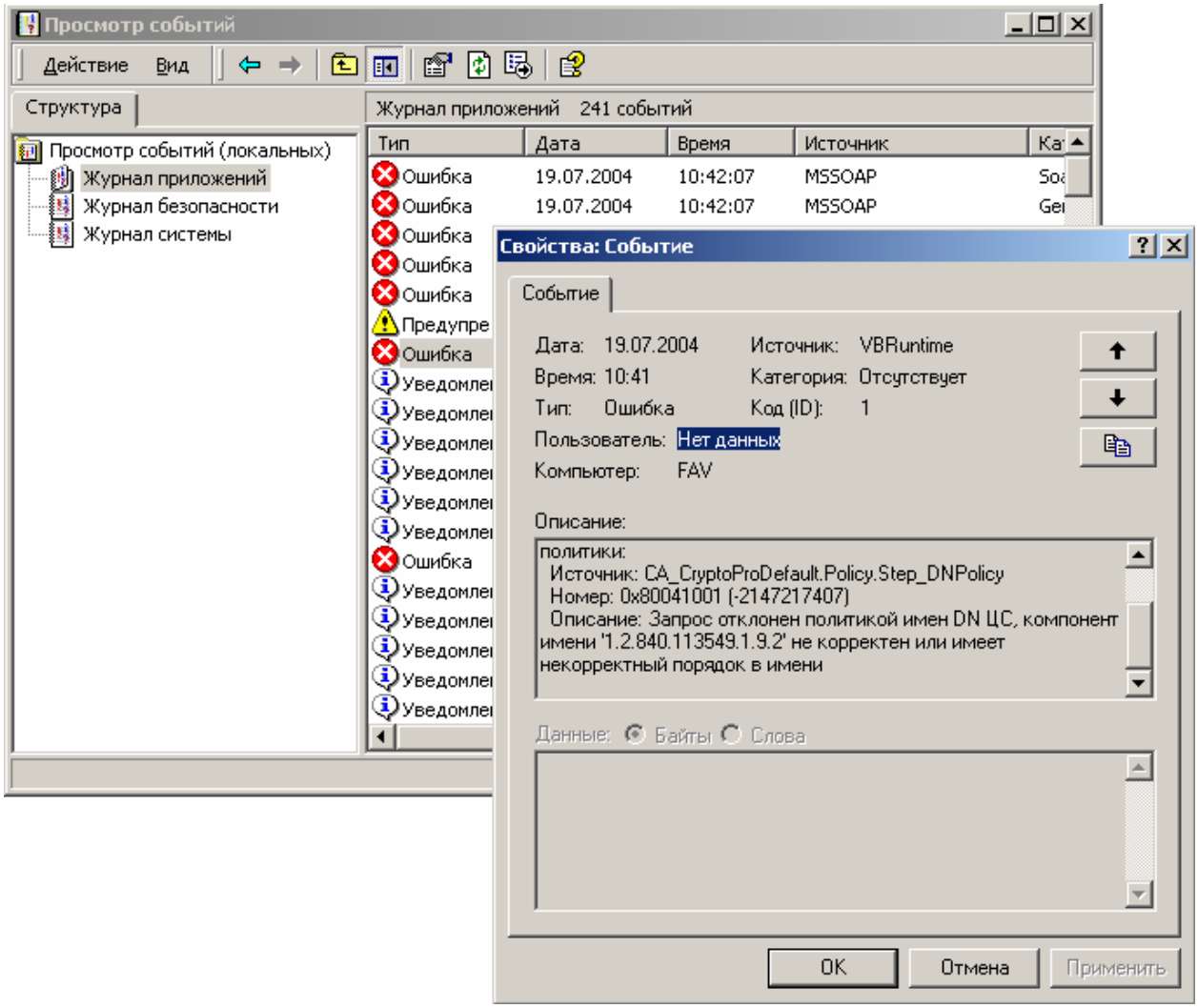
Например, появление на АРМ администратора ЦР сообщения (при изготовлении сертификата ключа подписи):





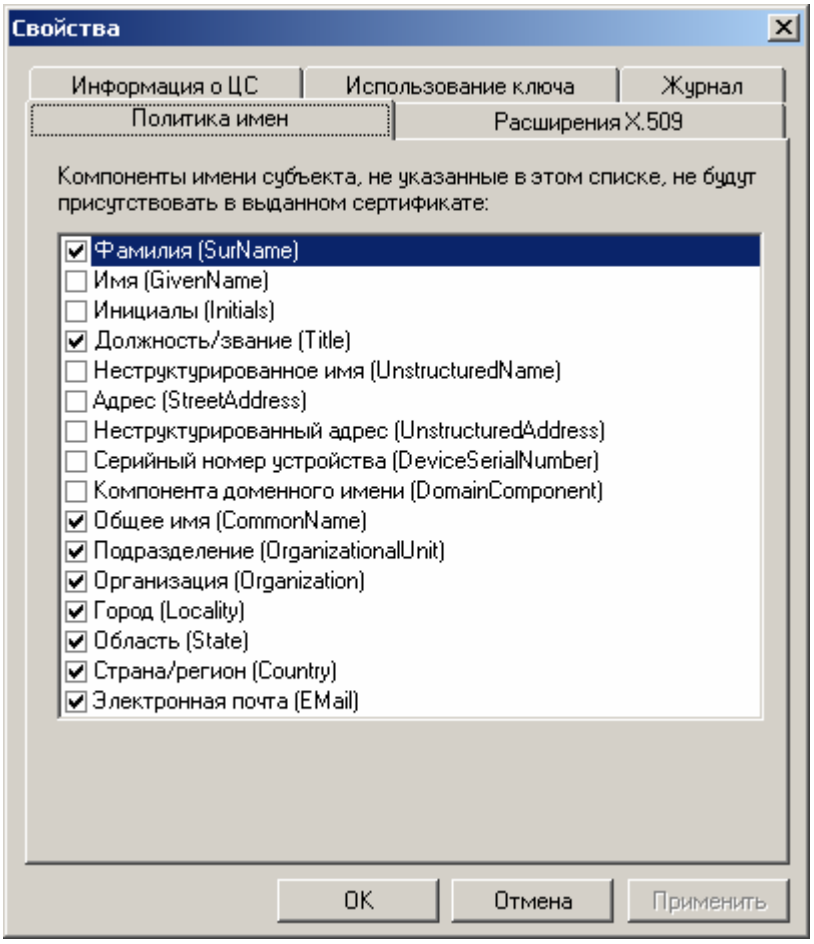
позволяет сделать вывод, что ошибка возникла на Центре Сертификации (Source - COM+ приложение ЦС) и была вызвана настройками Модуля политики Центра Сертификации (Description-Модуль политики отверг запрос).

Внимательный просмотр журнала Приложений Центра Сертификации (**Пуск** -> **Программы** –> **Администрирование** –> **Просмотр Событий**) и зарегистрированных ошибочных событий, произошедших в установленный период времени, показал наличие сообщения:



свидетельствующего, что Запрос на сертификат был отклонен политикой имен DN **Центра Сертификации** и ошибку вызвал компонент имени **Неструктурированное имя** (**UnstructuredName**, 1.2.840.113549.1.9.2).

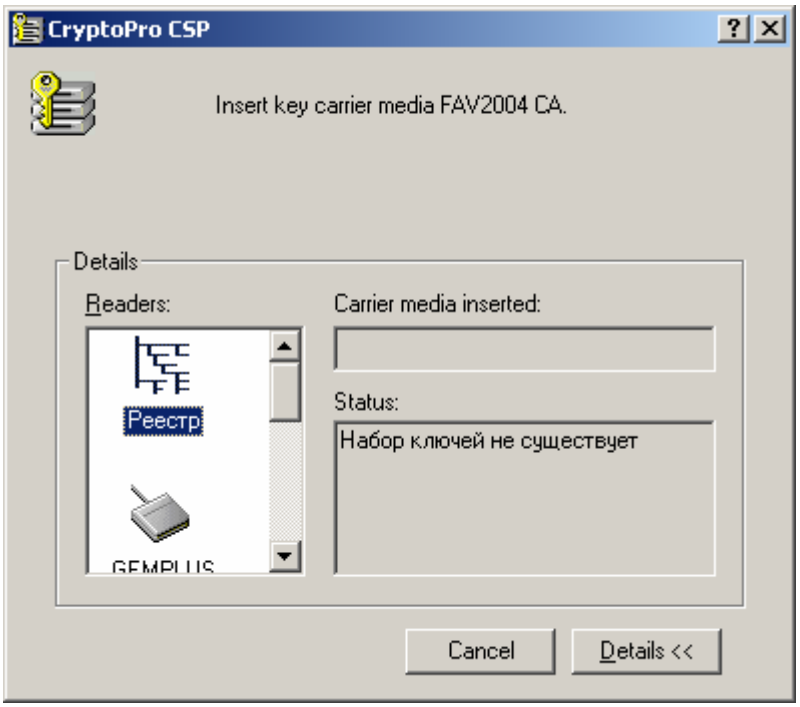
Дальнейший анализ описываемой ситуации показал, что в настройках политики имен Центра Сертификации (вкладка **Политика Имен** окна свойств **Модуля политики Центра Сертификации**) в списке разрешенных не был указан компонент имени **Неструктурированное имя**, а запрос на сертификат ключа подписи его содержал.



Для решения возникшей проблемы необходимо снова сформировать запрос на сертификат, но уже не содержащий компонент имени **Неструктурированное имя**, либо включить указанный компонент в список разрешенных для занесения в сертификаты ключей подписей.

2. Ошибки, возникающие на Центре Сертификации

2.1. Ошибка, возникающая после осуществления плановой смены ключей уполномоченного лица Удостоверяющего центра (Центра сертификации). При запуске службы сертификации (MS CA) появляется сообщение:

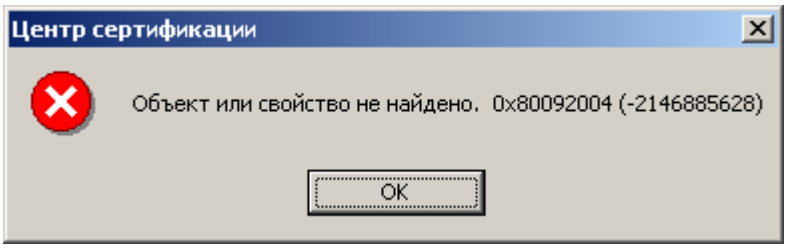


информирующее пользователя об отсутствии закрытого ключа, соответствующего старому сертификату уполномоченного лица Удостоверяющего центра, подвергшемуся плановой смене.

Возможная причина: Носитель старого закрытого ключа не установлен в считыватель или уничтожен

Рекомендуемое решение: После осуществления плановой смены ключей при запуске Службы сертификации (MS CA) требуется наличие всех закрытых ключей, соответствующих сертификатам уполномоченного лица Удостоверяющего центра (Центра сертификации), поэтому необходимо обеспечить их наличие при старте указанной службы (в частности, данные закрытые ключи используются для подписи списков отозванных сертификатов). При уничтожении старого закрытого ключа уполномоченного лица Удостоверяющего центра будет невозможен запуск службы сертификации, что потребует ее последующей переустановки.

2.2. Ошибка 0x80092004 (-2146885628). При запуске службы сертификации появляется сообщение об ошибке:

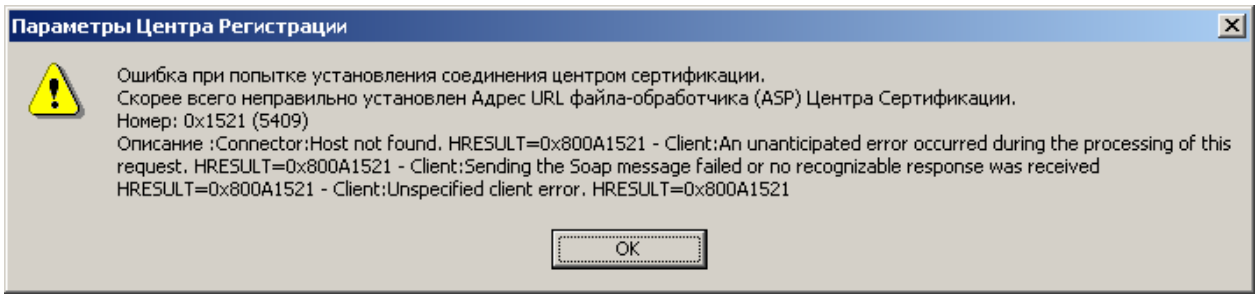


Возможная причина: После осуществления плановой смены ключей уполномоченного лица Удостоверяющего центра (Центра Сертификации) из хранилища **Локальный компьютер/Личные** был удален старый сертификат уполномоченного лица Удостоверяющего центра.

Рекомендуемое решение: Установить в хранилище **Локальный компьютер/Личные** старый сертификат уполномоченного лица Удостоверяющего центра со связкой с соответствующим закрытым ключом (данные действия осуществляются с использованием Сервисного интерфейса СКЗИ «КриптоПро CSP»).

3. Ошибки, возникающие на Центре Регистрации

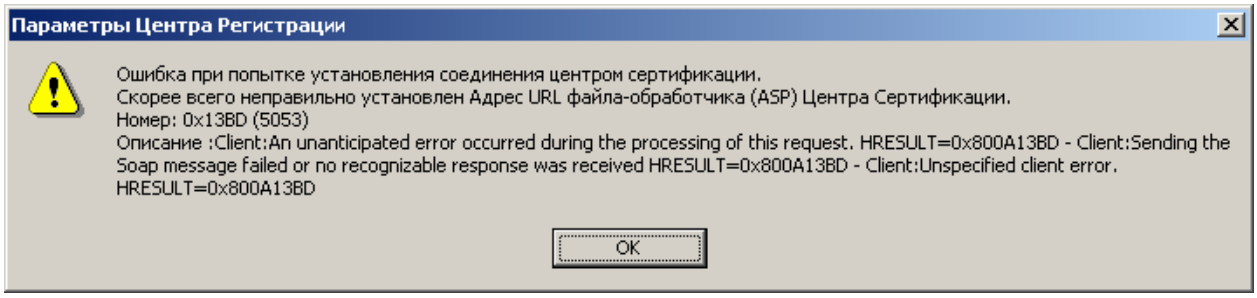
3.1. Ошибка 0x1521 (5409). При тестировании соединения между Центром регистрации и Центром Сертификации (кнопка **Протестировать соединение** окна **Свойства: ЦР**) появляется сообщение об ошибке:



Возможная причина: Наиболее вероятной причиной возникновения указанной ошибки является неверный ввод имени ПЭВМ Центра Сертификации (**Connector: Host not found**).

Рекомендуемое решение: Проверьте правильность указания имени ПЭВМ Центра Сертификации и внесите в него необходимые изменения.

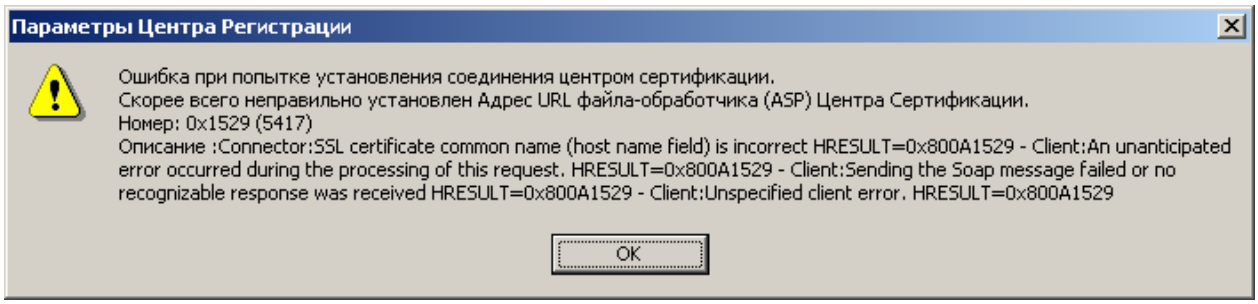
3.2. Ошибка 0x13BD (5053). При тестировании соединения между Центром регистрации и Центром Сертификации (кнопка **Протестировать соединение** окна **Свойства: ЦР**) появляется сообщение об ошибке:



Возможная причина: Наиболее вероятной причиной возникновения указанной ошибки является неверное указание пути к файлу **ca.asp** (**\ca\ca.asp**)

Рекомендуемое решение: Проверьте правильность указания пути к файлу **ca.asp** Центра Сертификации и внесите в него (путь) необходимые изменения

3.3. Ошибка 0x1529 (5417). При тестировании соединения между Центром регистрации и Центром Сертификации (кнопка **Протестировать соединение** окна **Свойства: ЦР**) появляется сообщение об ошибке:

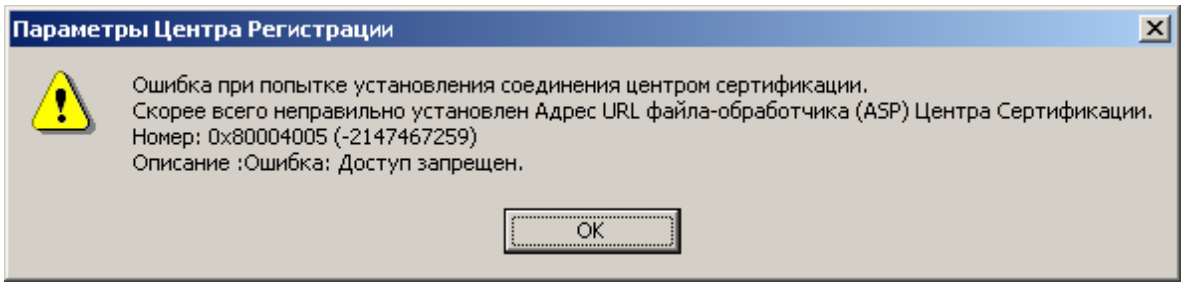


Возможная причина: В поле **Адрес URL файла – обработчика (ASP) Центра Сертификации** указано имя ПЭВМ Центра Сертификации, отличное от имени, указанного в сертификате web-сервера Центра сертификации (Connector: SSL certificate

common name (host name field) is incorrect). Например, сертификат выдан на полное доменное имя Центра Сертификации, а при подключении было указано короткое имя.

Рекомендуемое решение: Укажите в поле **Адрес URL файла – обработчика (ASP) Центра Сертификации** имя ПЭВМ Центра Сертификации идентичное содержанию поля **Common Name** (Общее имя) сертификата web-сервера Центра сертификации

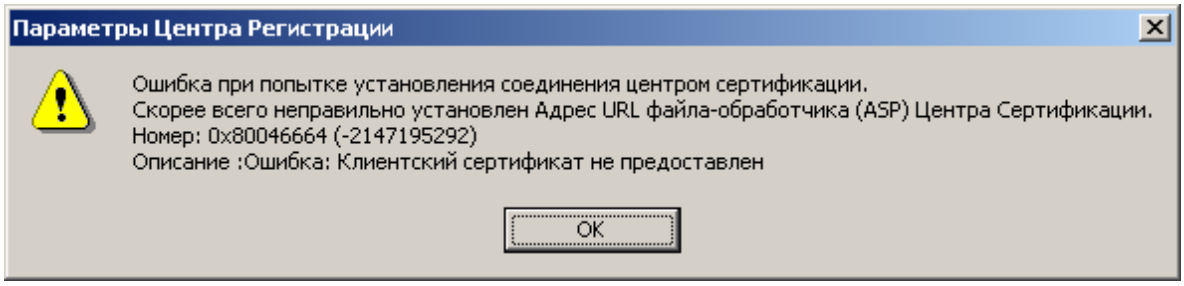
3.4. Ошибка 0x80004005 (-2147467259). При тестировании соединения между Центром регистрации и Центром Сертификации (кнопка **Протестировать соединение** окна **Свойства: ЦР**) появляется сообщение об ошибке:



Возможная причина: На Центре Сертификации в **Параметрах Центра сертификации** не указан клиентский сертификат Центра Регистрации (Окно **Средство настройки Центра Сертификации**, Вкладка **Центры Регистрации**)

Рекомендуемое решение: Добавить клиентский сертификат Центра Регистрации в список **Сертификаты Центров регистрации** окна **Средство настройки Центра Сертификации**, Вкладка **Центры Регистрации**.

3.5. Ошибка 0x80046664 (-2147195292). При тестировании соединения между Центром регистрации и Центром Сертификации (кнопка **Протестировать соединение** окна **Свойства: ЦР**) появляется сообщение об ошибке:



Возможная причина: Для файла **\ca\ca.asp** в окне настройки **Безопасных подключений** переключатель **Сертификаты клиентов** установлен в положение **Игнорировать сертификаты клиентов**. Указанная ошибка обычно возникает в случае плановой смены ключей web-сервера Центра Сертификации. Установленный сертификат web-сервера сначала удаляется (в окне **Мастер сертификатов IIS** выбран переключатель **Удалить текущий сертификат**), а затем устанавливается новый (в окне **Мастер сертификатов IIS** выбран переключатель **Назначение существующего сертификата**), что приводит к «сбросу» всех настроек **Безопасных подключений** к web-страницам Центра Сертификации

Рекомендуемое решение: Удалить ПО Центра сертификации, установить в IIS новый изданный сертификат web-сервера Центра Сертификации (в окне **Мастер сертификатов IIS** выбрать переключатель **Назначение существующего сертификата**), после чего снова установить ПО Центра Сертификации. При осуществлении последующих плановых смен ключей web-сервера Центра Сертификации в окне **Мастера сертификатов IIS** выбирать переключатель **Заменить текущий сертификат**

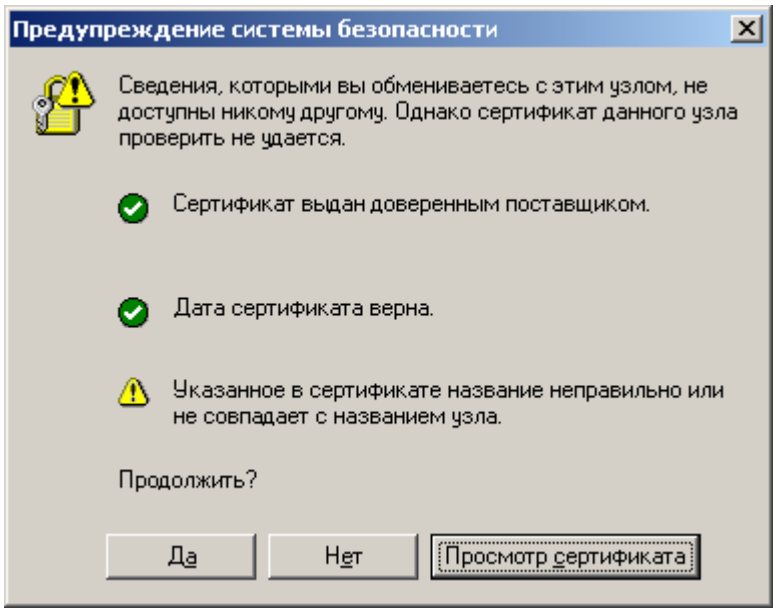
Довольно часто причиной возникновения ошибок при тестировании соединения между ЦР и ЦС являются ошибки соединения между указанными узлами, вызванные отсутствием физического подключения компонентов (ЦС и ЦР), ошибками DNS, неверной настройкой Internet-подключений, влиянием межсетевых экранов на http и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

Для определения описанных причин необходимо последовательно проделать следующие действия:

С ЦР выполните команду: **ping ИмяЦС**, где **ИмяЦС –** Имя Центра Сертификации (не IP-адрес, а именно имя), на которое выдан сертификат серверной аутентификации Центра Сертификации. 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 ЦР с использованием Internet Explorer по протоколу **http** откройте тестовую страницу (например, http://**ИмяЦС**/mmc.gif, где **ИмяЦС –** Имя Центра Сертификации, на которое выдан сертификат серверной аутентификации Центра Сертификации, но сначала обязательно убедитесь в ее наличии (тестовой страницы) на Центре Сертификации). Если при выполнении указанной команды страница не открывается, то на ЦР 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 Центром Сертификации и Центром Регистрации.

С Центра Регистрации по протоколу **https** откройте страницу https://ИмяЦС/ra/ra.wsdl, где **ИмяЦС –** Имя Центра Сертификации, на которое выдан сертификат серверной аутентификации Центра Сертификации. 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 Сертификации (см. рисунок ниже) необходимо установить их причину и устранить указанное несоответствие.

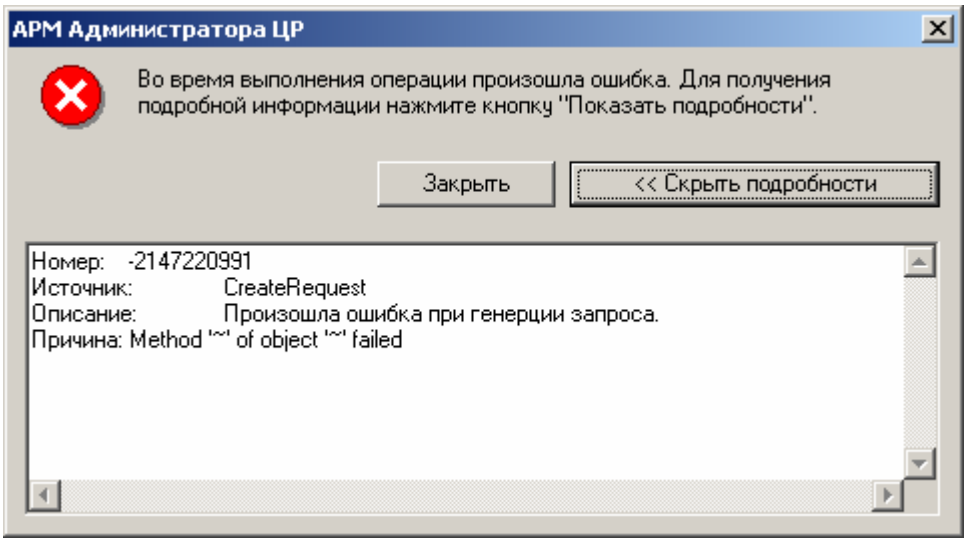


Невозможность открытия страницы по протоколу **https** также может быть вызвано некорректной работой модуля сетевой аутентификации «КриптоПро TLS» (или его отсутствием). В связи с этим на ЦР и ЦС проверьте отсутствие в журнале Приложений ошибочных сообщений вызванных этим модулем, а также службой инициализации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

удостоверьтесь, что на ЦС введен серийный номер серверной Лицензии на «КриптоПро TLS»

4. Ошибки, возникающие на АРМ Администратора ЦР

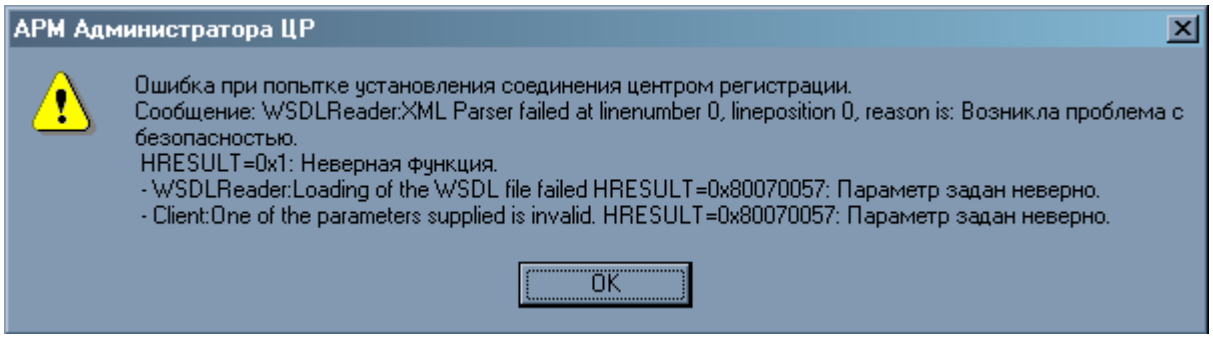
4.1. Ошибка -2147220991. CreateRequest. При формировании запроса на изготовление сертификата привилегированного пользователя появляется сообщение:



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.

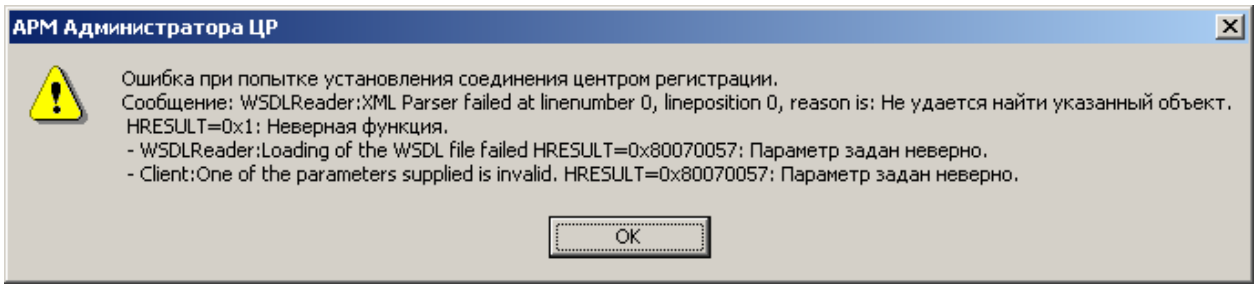
4.2. Ошибка при попытке установления соединения с ЦР (0x80070057). При инициализации подключения к ЦР (тестировании соединения между АРМ администратора и ЦР) появляется сообщение:



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).

4.3. 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)

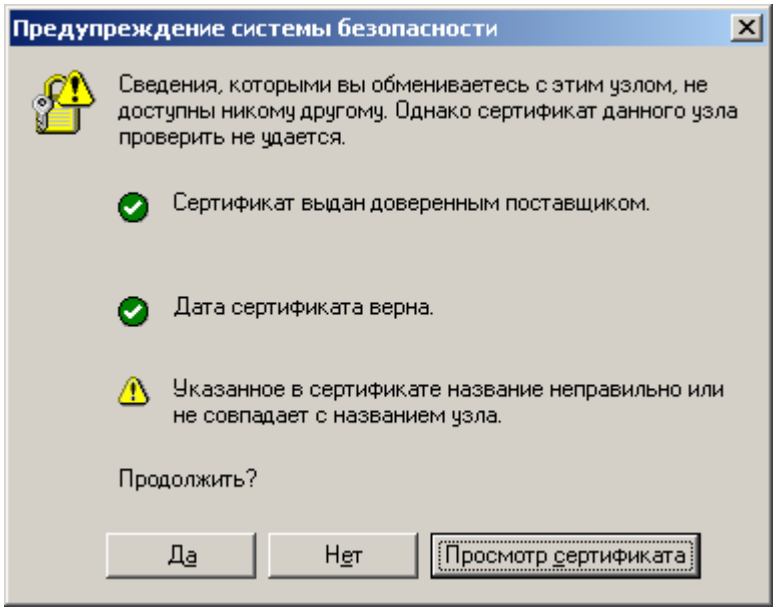
Довольно часто причиной возникновения ошибок при инициализации подключения к ЦР (при тестировании соединения между АРМ администратора и ЦР) являются ошибки соединения между указанными узлами, вызванные отсутствием физического подключения компонентов (АРМ администратора и ЦР), ошибками DNS, неверной настройкой 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 с использованием Internet Explorer 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 (тестовой страницы) 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.

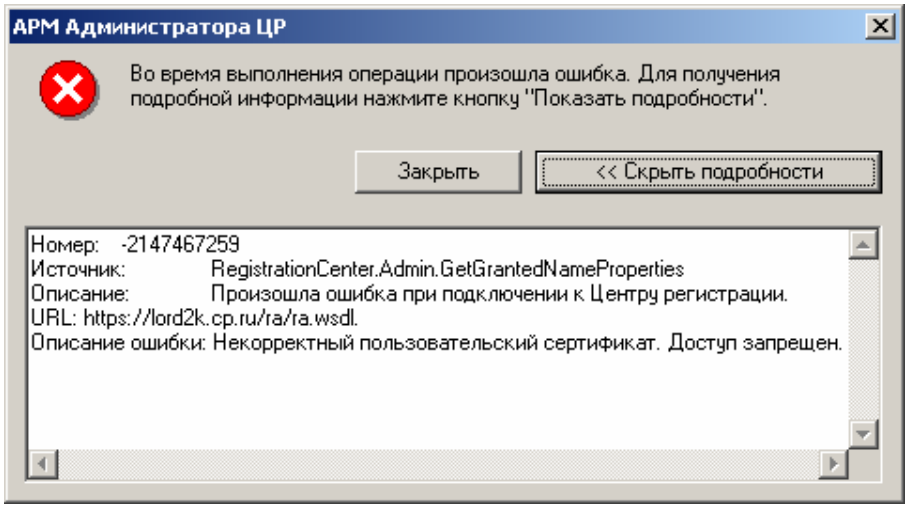
С АРМ администратора ЦР по протоколу **https** откройте страницу, указанную по адресу, содержащемуся в поле **Адрес URL файла описания WSDL Центра Регистрации** окна Свойств подключения к Центру регистрации - https://ИмяЦР/ra/ra.wsdl. Открытие указанной страницы должно сопровождаться только появлением 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.

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

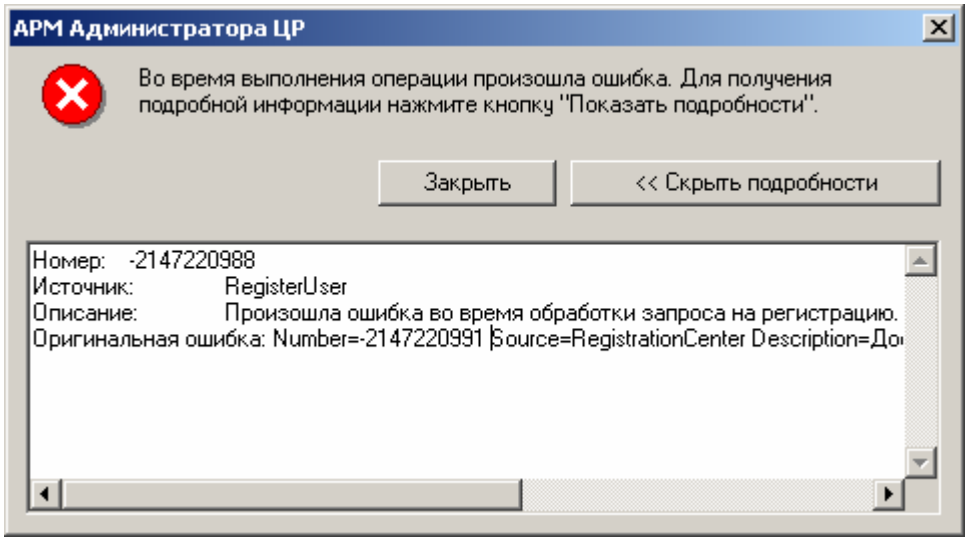


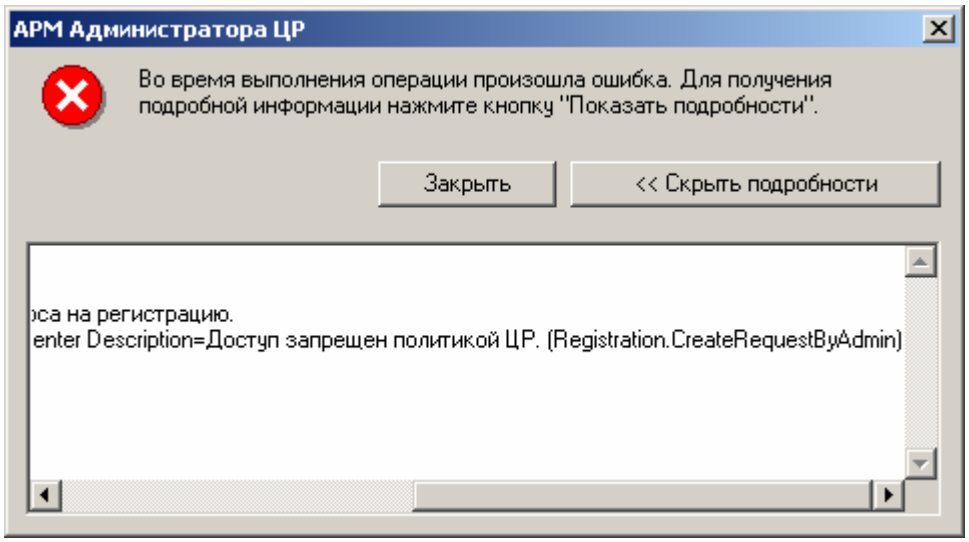
Возможная причина: Сертификат, на котором осуществляется подключение к Центру Регистрации, недействителен (аннулирован (отозван), действие его

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 привилегированного пользователя

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

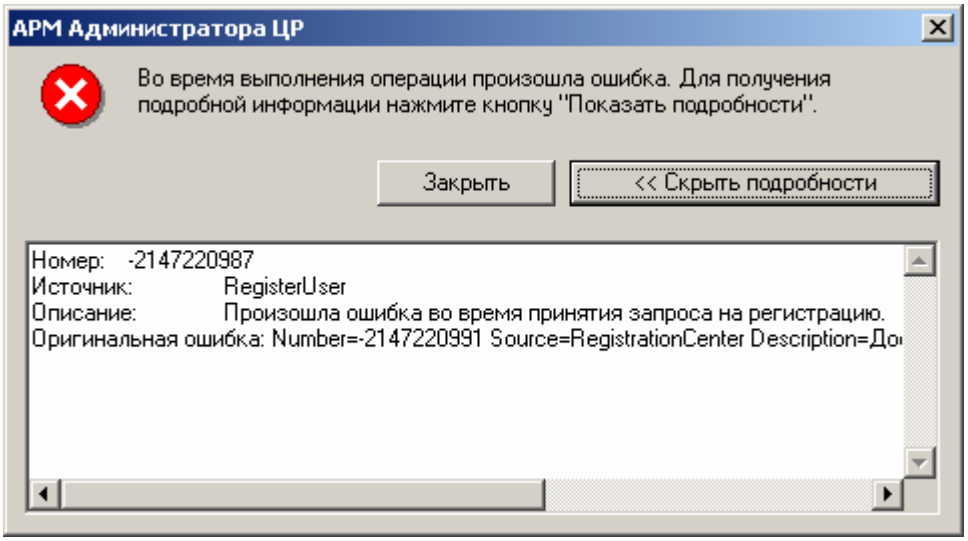


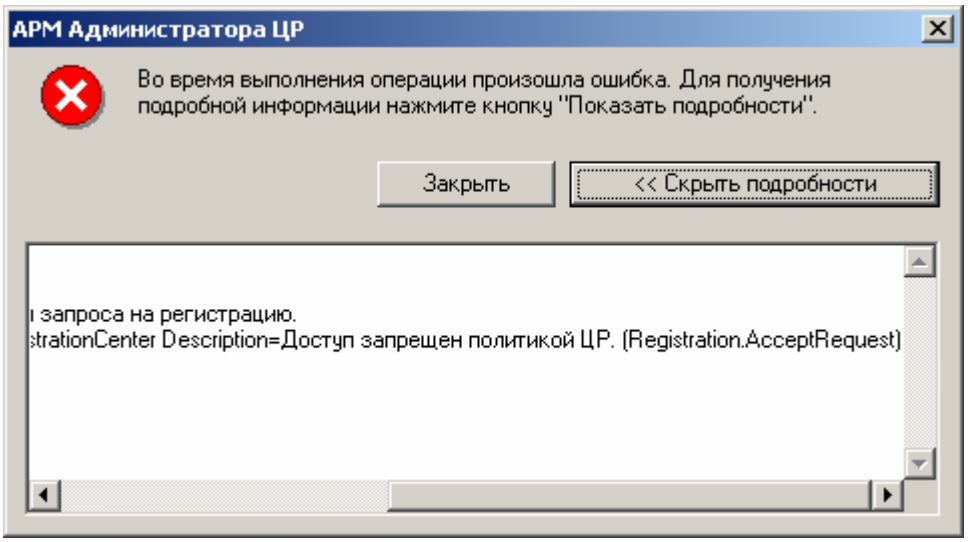


Возможная причина: У привилегированного пользователя, производящего регистрацию пользователя в Удостоверяющем центре не достаточно прав на выполнение метода **Registration.CreateRequestByAdmin**

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**)

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

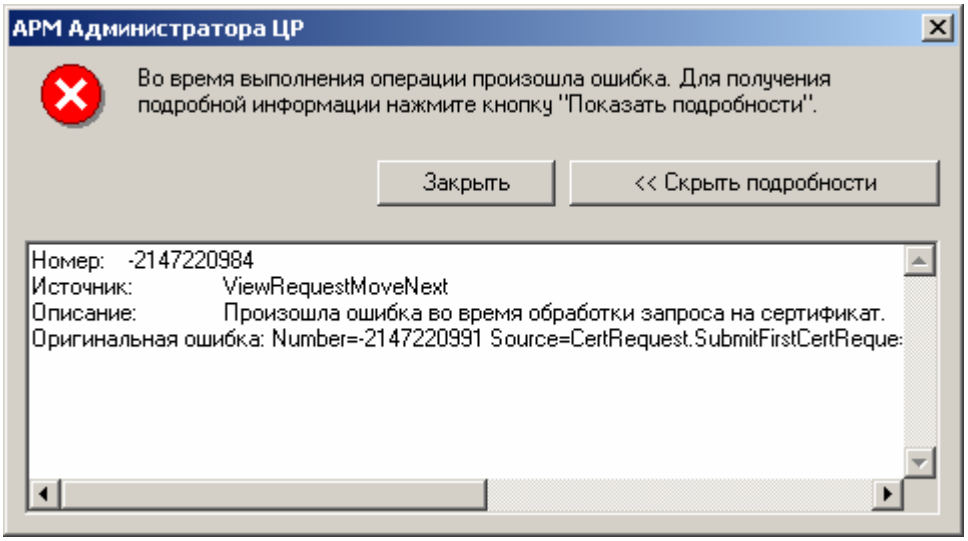


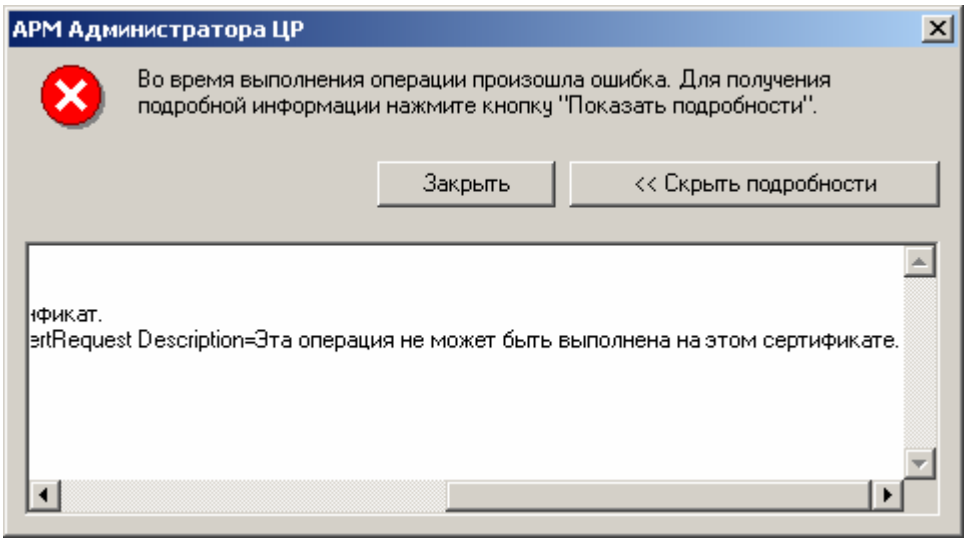


Возможная причина: У привилегированного пользователя, производящего регистрацию пользователя в Удостоверяющем центре не достаточно прав на выполнение метода **Registration.AcceptRequest**.

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**).

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

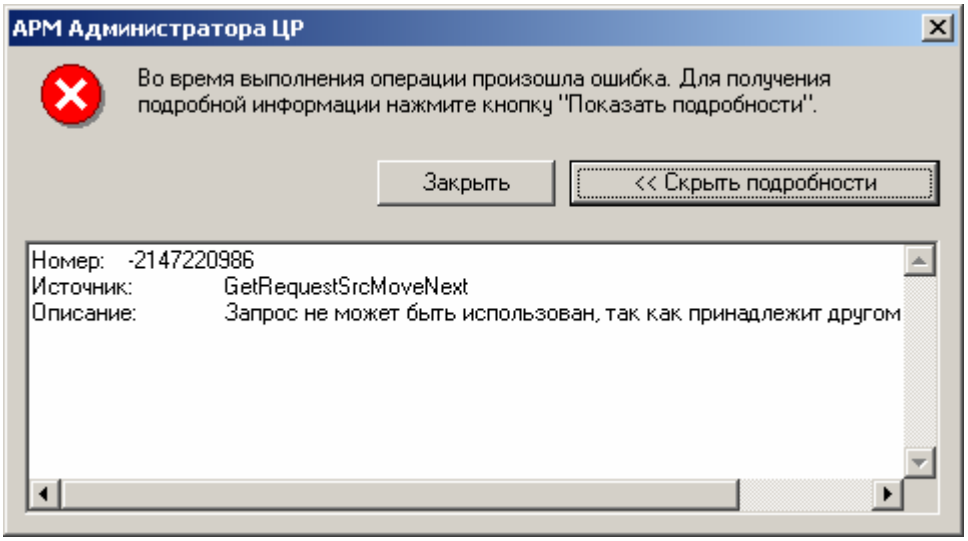


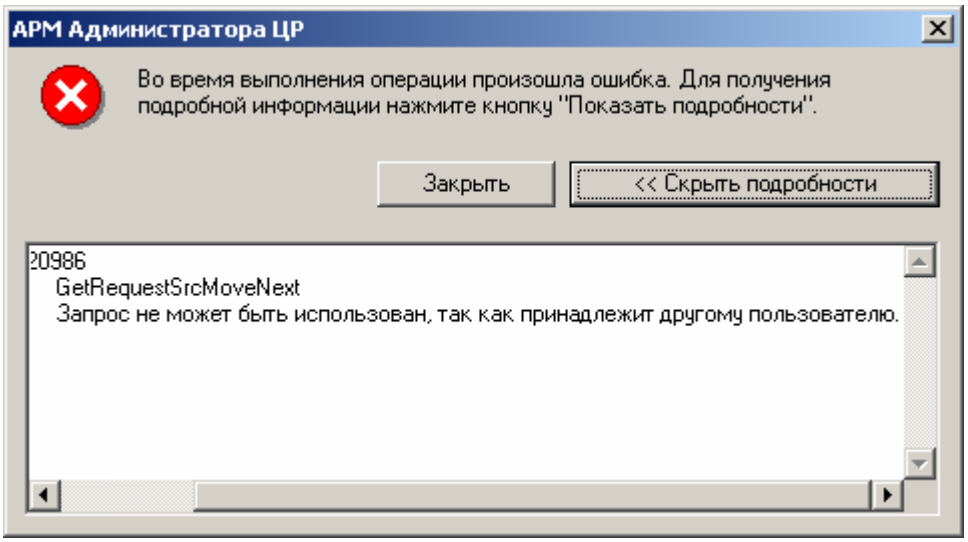


Возможная причина: Привилегированный пользователь не имеет прав на изготовление сертификата, содержащего области использования, указанные в запросе (шаблоне) на сертификат.

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

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

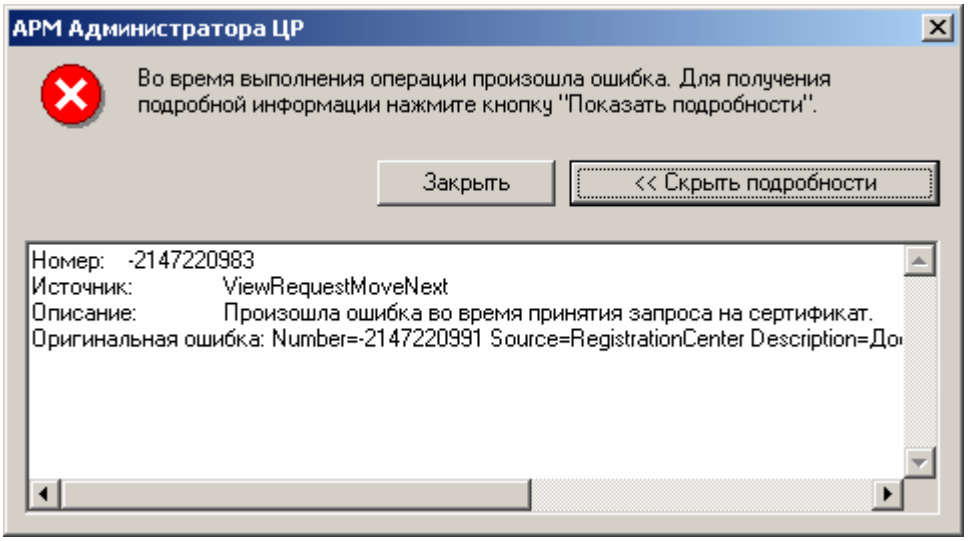


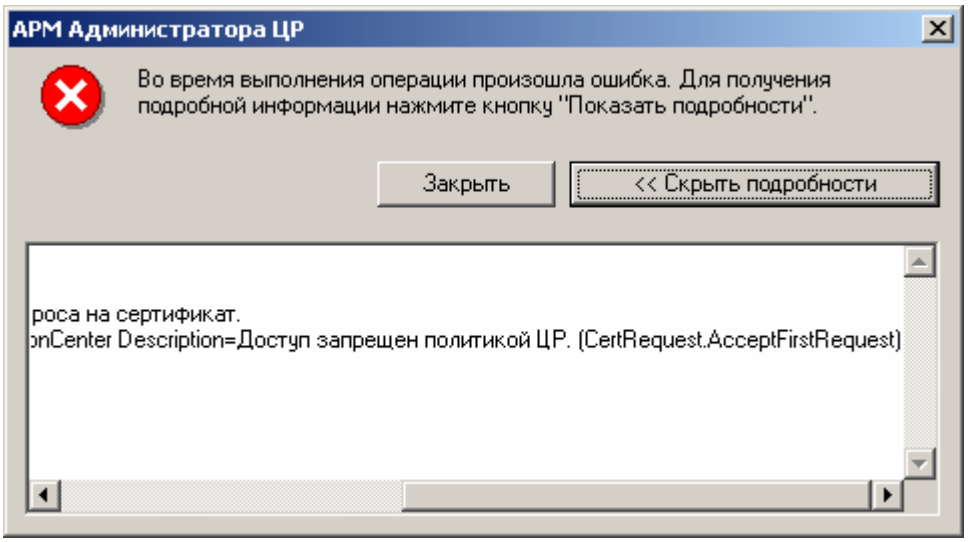


Возможная причина: Идентификационные данные пользователя, содержащиеся в запросе на сертификат отличны от идентификационных данных зарегистрированного пользователя, на имя которого требуется изготовить сертификат (например, выбран файл, содержащий запрос на сертификат другого пользователя), либо при 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, исключающий обнаруженные ошибки.

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

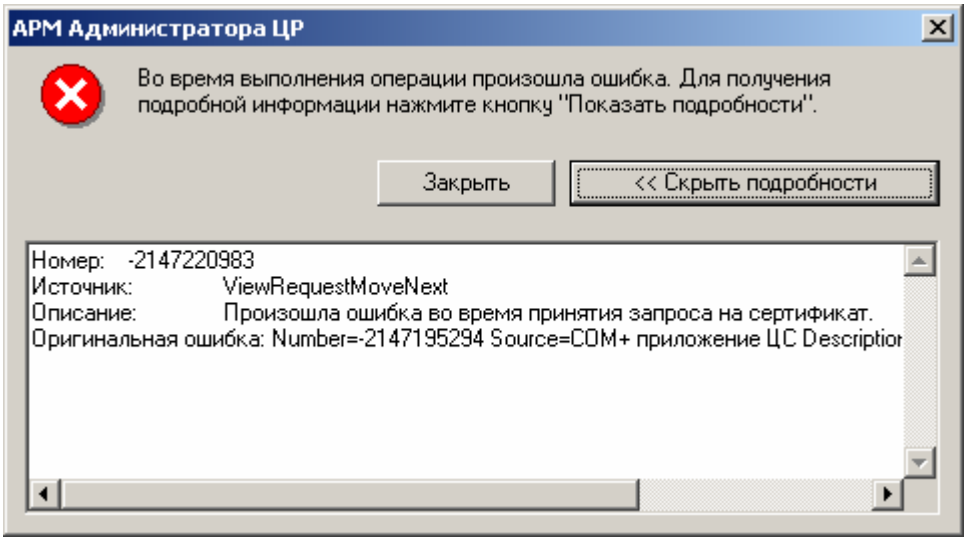


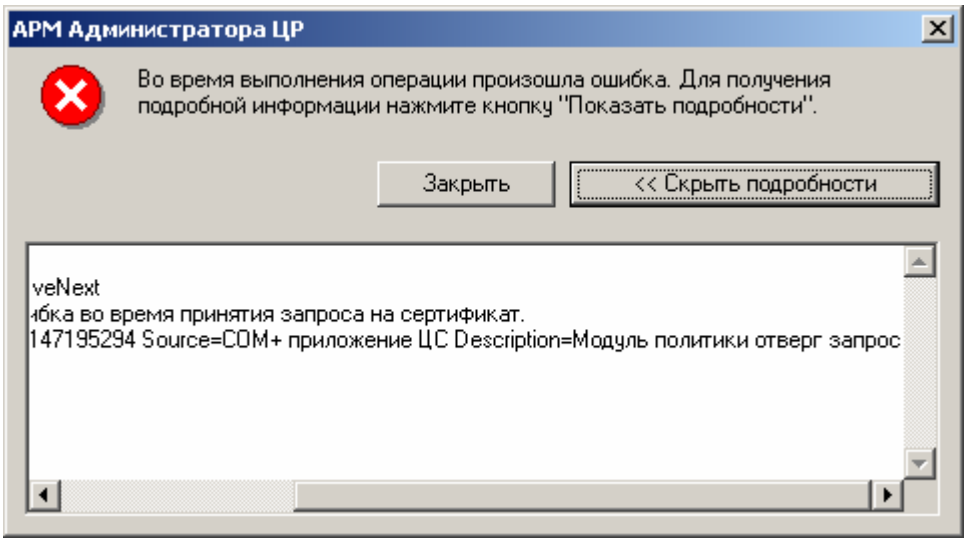


Возможная причина: У привилегированного пользователя, производящего изготовление сертификата пользователя в Удостоверяющем центре не достаточно прав на выполнение метода **CertRequest.AcceptFirstRequest.**

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**).

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

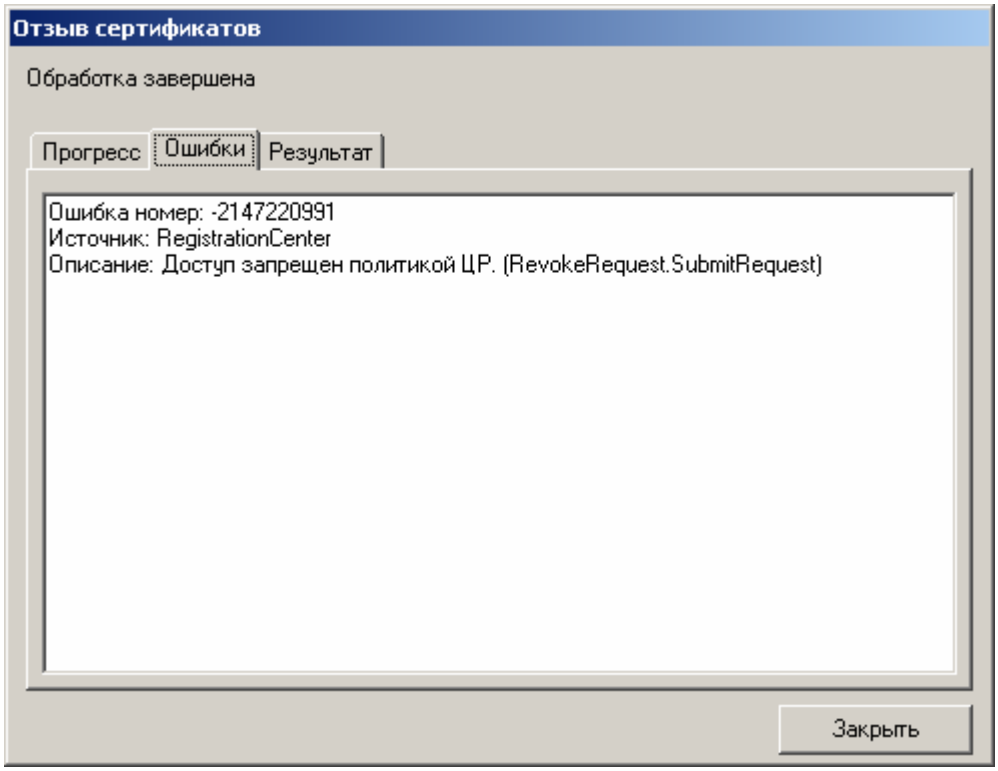




Возможная причина: Модуль политики Центра сертификации отверг запрос – наиболее вероятная причина – на вкладке **Использование ключа** окна **Свойства Модуля политики Центра Сертификации** в списке разрешенных областей использования сертификата отсутствует хотя бы одна область, содержащаяся в запросе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

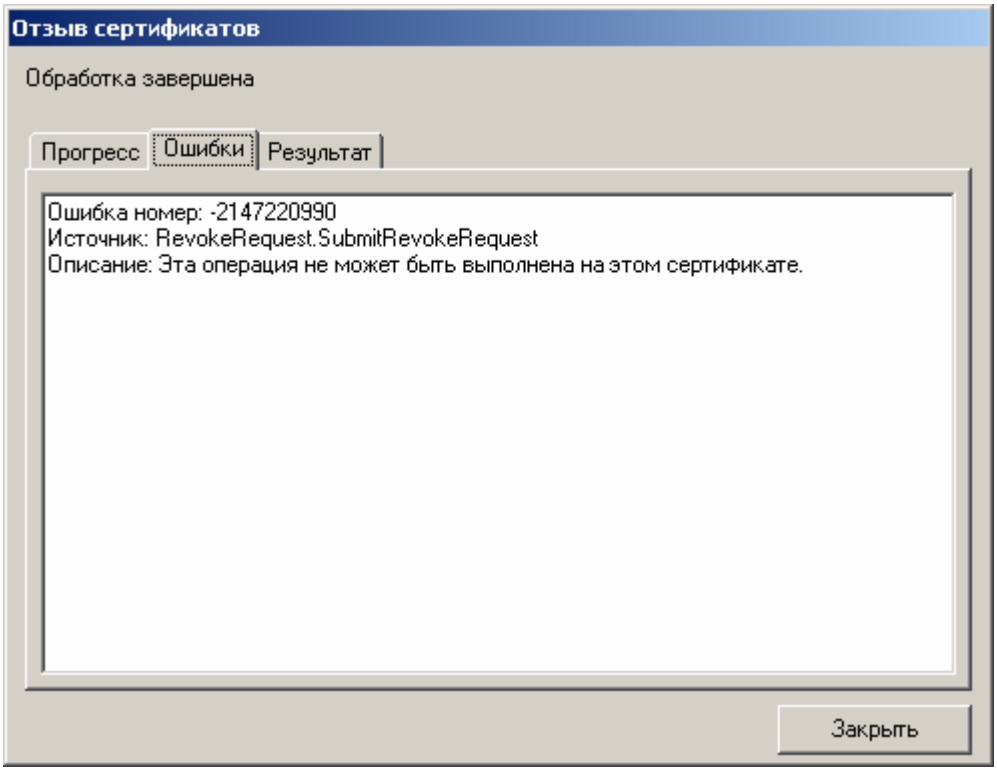
4.11. Ошибка -2147220991. RevokeRequest.SubmitRequest (RevokeRequest.SubmitHoldrequest/RevokeRequest.SubmitUnHoldRequest). При отзыве (приостановлении/возобновлении действия) сертификата привилегированным пользователем в окне **Отзыв сертификатов - Обработка завершена** возникает ошибка:



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)**)

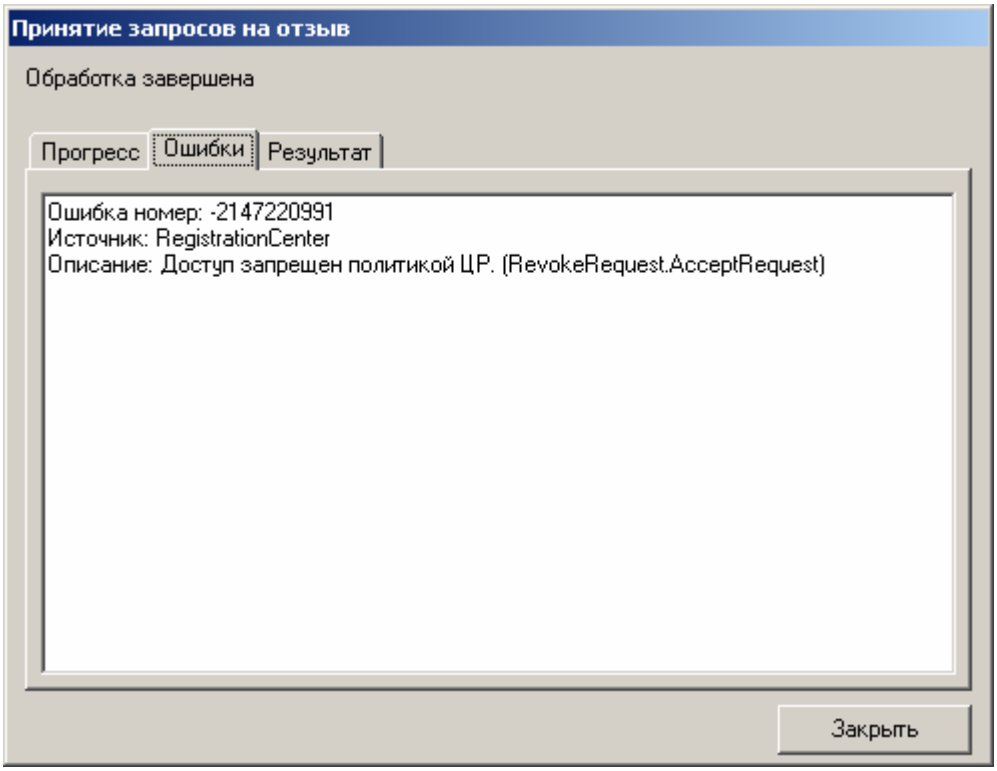
4.12. Ошибка -2147220990. RevokeRequest.SubmitRequest. При отзыве (простановлении/возобновлении действия) сертификата привилегированным пользователем в окне **Отзыв сертификатов - обработка завершена** возникает ошибка



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

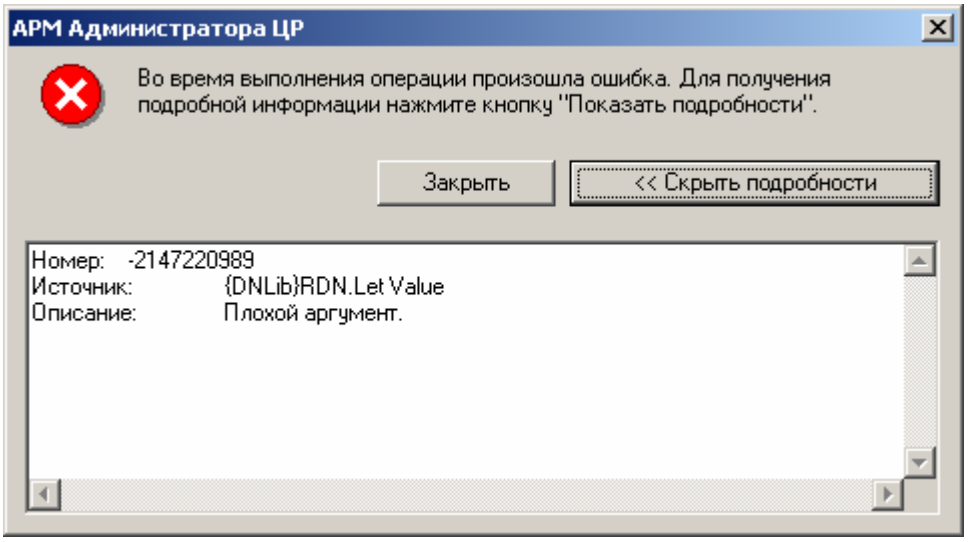
4.13. Ошибка -2147220991. RevokeRequest.AcceptRequest. При принятии запроса на отзыв (приостановление/возобновление действия) сертификата привилегированным пользователем в окне **Отзыв сертификатов - обработка завершена** возникает ошибка



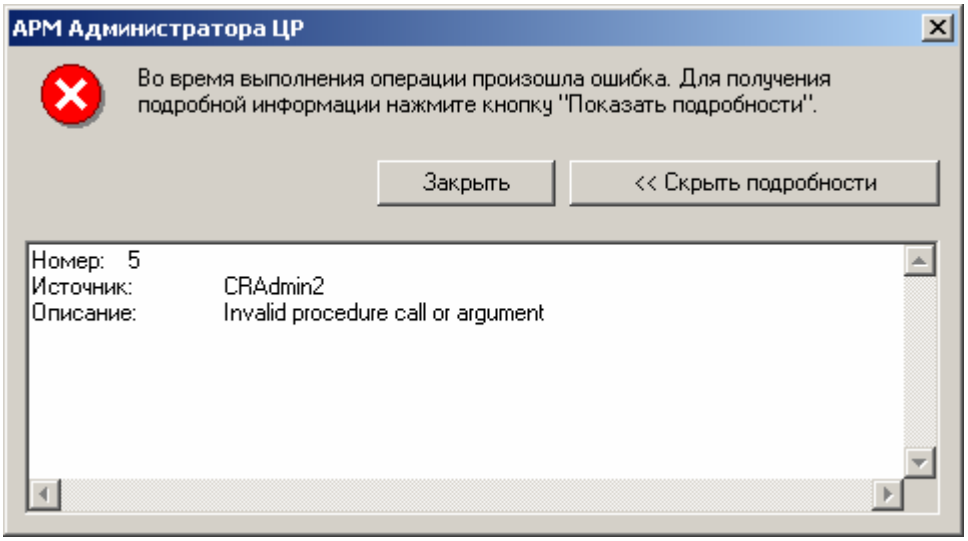
Возможная причина: У привилегированного пользователя, производящего принятие запроса на отзыв (приостановление/возобновление действия) сертификата не достаточно прав на выполнение метода **RevokeRequest.AcceptRequest**

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**)

4.14. Ошибка -2147220989 (Ошибка 5). При генерации ключей подписей и изготовлении сертификата ключа подписи появляется сообщение:



либо



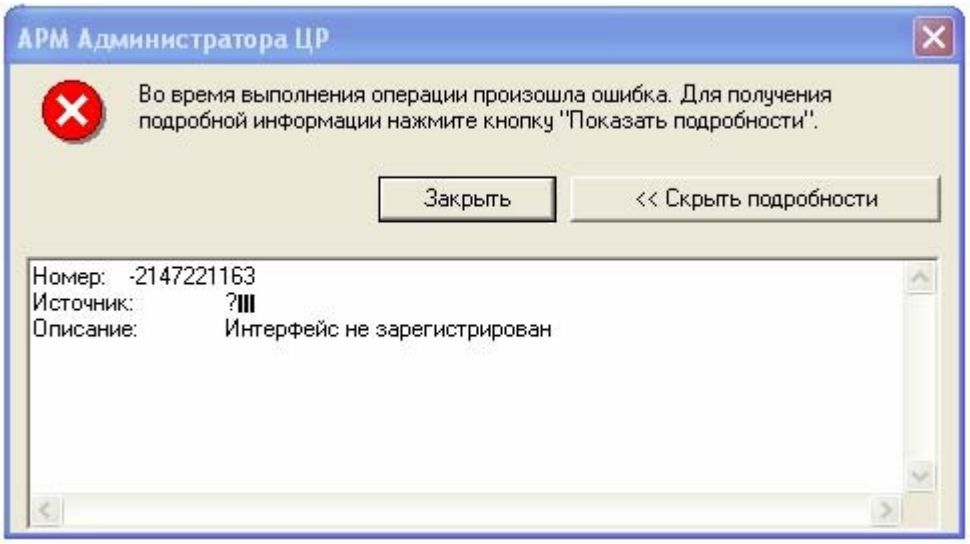
Возможная причина:

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

4.15. 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:

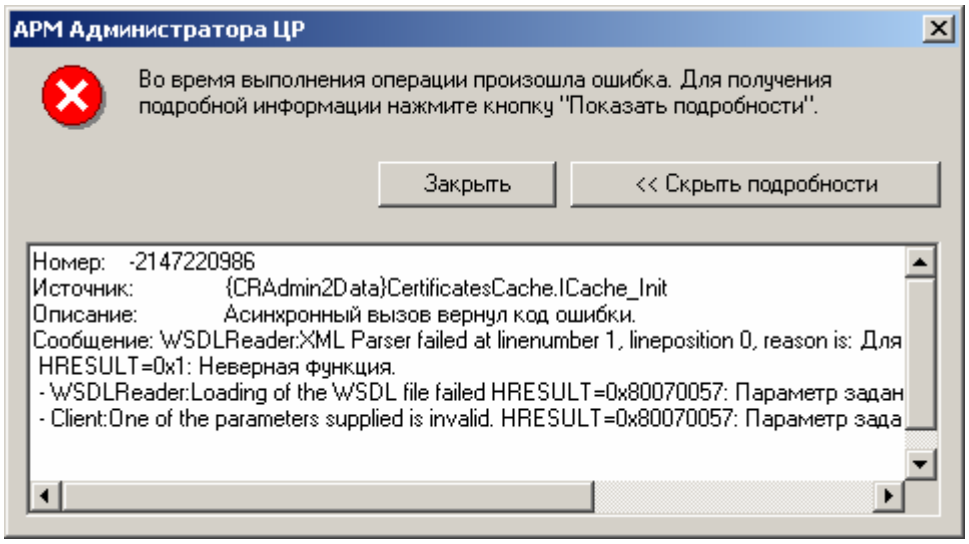
Для установки и эксплуатации АРМ администратора ЦР необходимо следующее программное обеспечение:

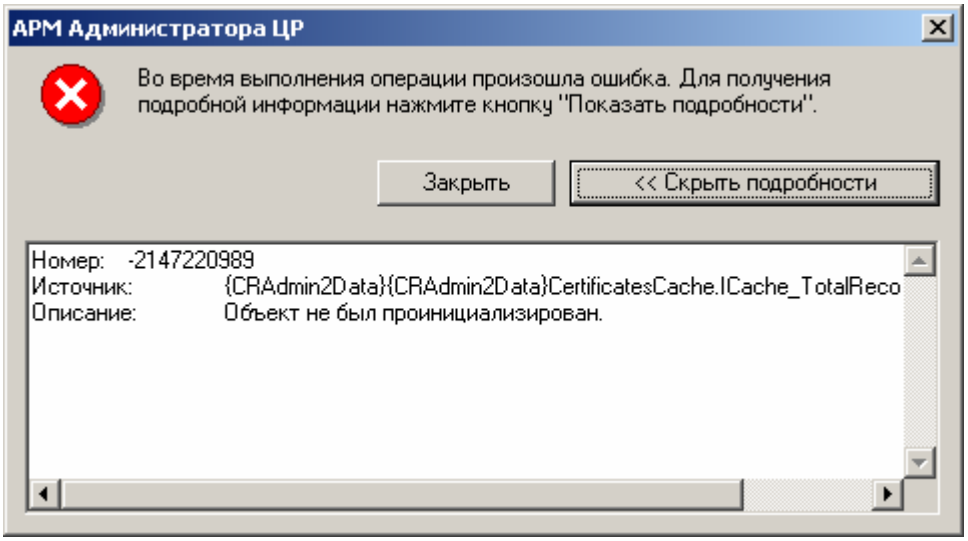
- Операционная система Microsoft Windows 2000 (Professional или Server);
- Пакеты обновлений:
  - Microsoft Windows 2000 Service Pack 4
- Программная библиотека CAPICOM.dll версии 2.1.0.1 (http://www.microsoft.com/downloads/details.aspx?FamilyID=860ee43a-a843-462f-abb5-ff88ea5896f6&DisplayLang=en)
- 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

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



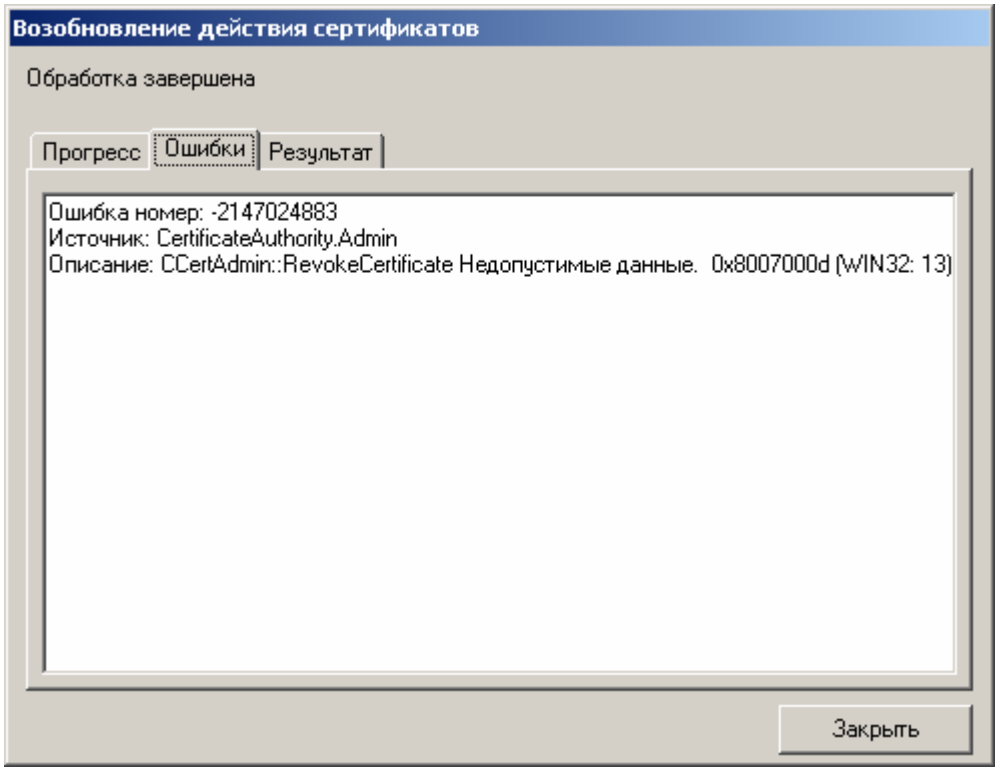


Возможная причина:

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.).

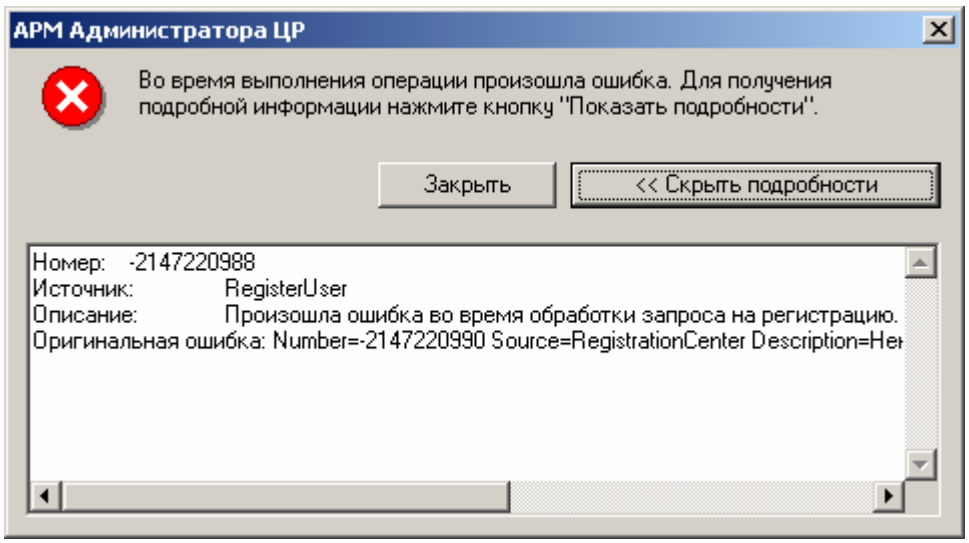
4.17. Ошибка -2147024883. При возобновлении/приостановлении действия сертификата появляется сообщение

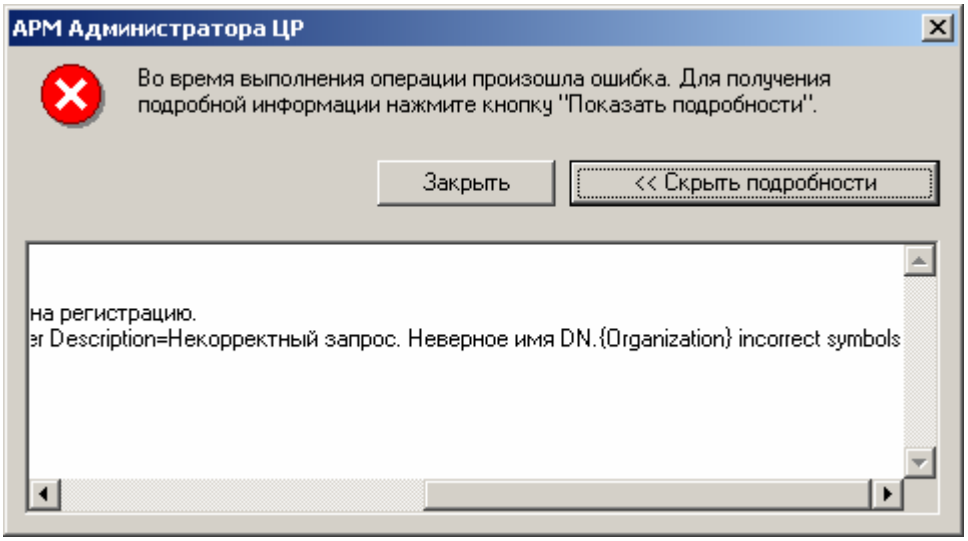


Возможная причина: Сертификат, действие которого администратор пытается приостановить/возобновить, уже отозван

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

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

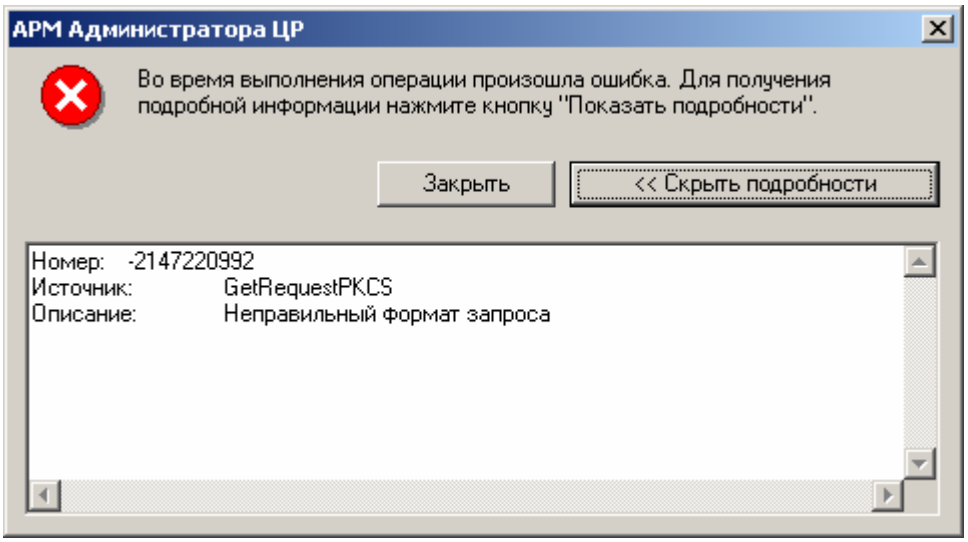




Возможная причина: Значения поля (в описываемом случае поля Organization) не соответствует формату имен X.500

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)

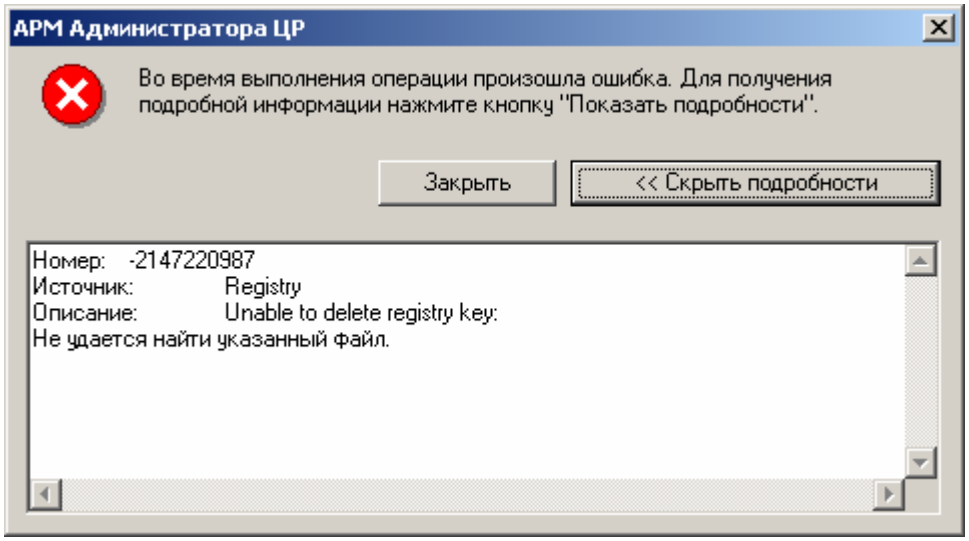
4.19. Ошибка -2147220992. GetRequestPKCS. При регистрации пользователя на основании идентификационных данных, содержащихся в файле запроса на сертификат появляется сообщение:



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.

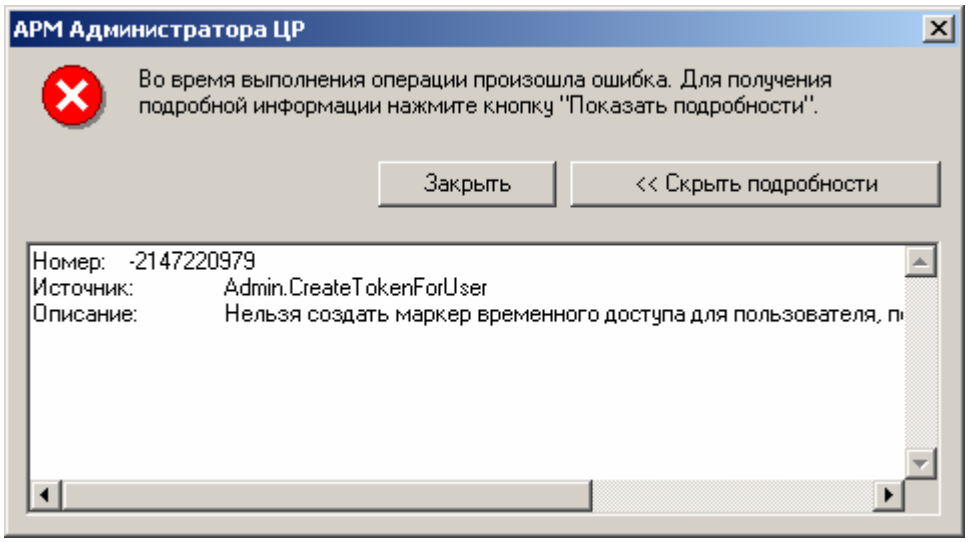
4.20. Ошибка 2147220987. Unable to delete registry key. После нажатия на кнопку **Далее** в окне **Установка сертификата** АРМ администратора ЦР (флаг **Автоматически подтвердить запрос** установлен) появляется сообщение:

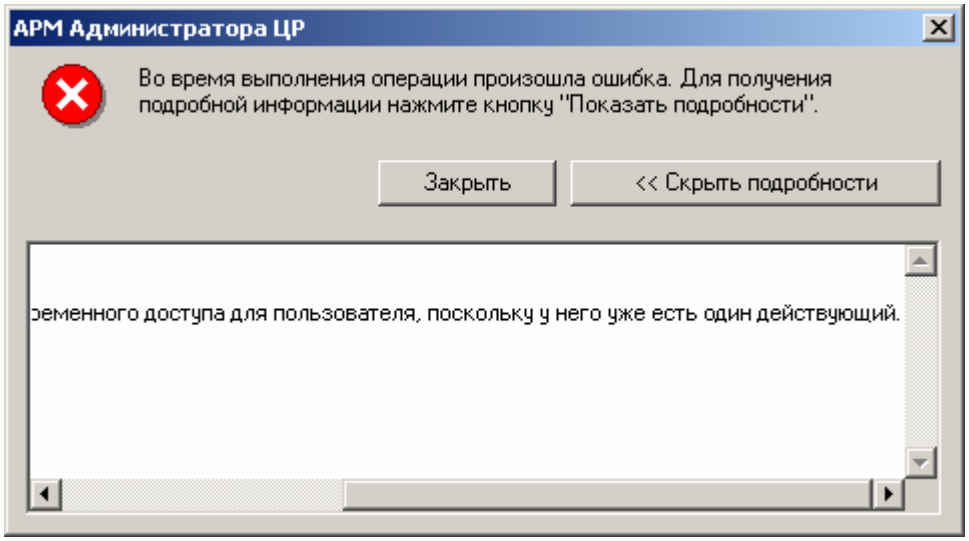


Возможная причина: У привилегированного пользователя, осуществившего изготовление сертификата ключа подписи не достаточно прав на выполнение метода **CertRequest.ConfirmRequest**. В журнале Приложений ОС должны быть зарегистрированы соответствующие события, содержащие информацию об ошибочном выполнении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

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



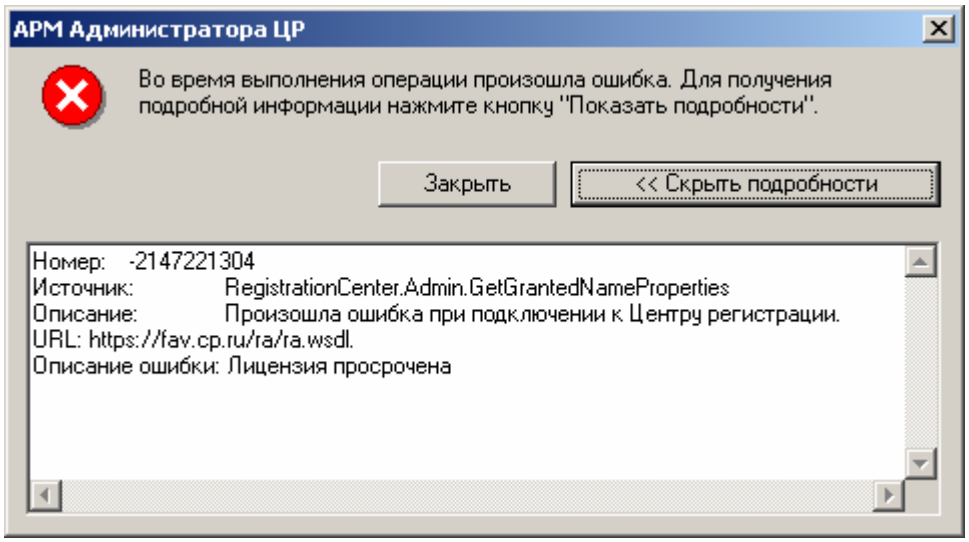


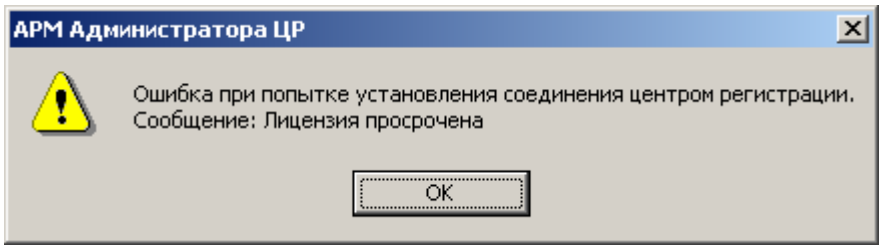
Возможная причина: Пользователь, для которого создается маркер временного доступа, уже имеет действующий маркер

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

4.22. Ошибка -2147221304. При инициализации подключения к Центру регистрации (тестировании соединения) появляется сообщение:





Возможная причина: На Центре регистрации и на АРМ администратора ЦР просрочена лицензия

Рекомендуемое решение: Установить (при необходимости приобрести) новую действующую лицензию Центра регистрации и/или АРМ администратора ЦР

5. Ошибки, вызванные аппаратно-программной несовместимостью устройств (в том числе устройств считывания ключевых носителей), установленных на ПЭВМ компонент ПК «КриптоПро УЦ»

5.1. Ошибки, возникающие при использовании в качестве носителя закрытого ключа уполномоченного лица УЦ (ЦС) и web-сервера электронного ключа eToken R2 (eToken Pro).

Исходные данные: Носителем закрытого ключа уполномоченного лица удостоверяющего центра, web-серверов ЦС и ЦР должен являться электронный ключ eToken R2. На ПЭВМ установлены драйверы RTE_3.0.116 и eTok2.0.0.50 (драйвер eToken для КриптоПро CSP)

После установки службы сертификации и изготовления сертификата web-сервера (все закрытые ключи были сгенерированы на один носитель eToken R2, КриптоПро CSP функционирует в режиме **В службе хранения ключей**) ПЭВМ была полностью работоспособна. После установки ПО Центра Сертификации ПК «КриптоПро УЦ» и последующей перезагрузки контейнеры закрытых ключей, располагающиеся на eToken R2, становились недоступны (система их «не видела» и предлагала вставить носитель, содержащий указанные контейнеры). В результате Службы сертификации (MS CA) не запускались, и доступ к Центру Сертификации по ssl/tls был невозможен.

Анализ журнала Приложений ОС выявил наличие в нем сообщения об ошибке инициализации, возникшей при запуске **Службы хранения ключей** СКЗИ «КриптоПро CSP».

Установка СКЗИ «КриптоПро CSP» в режим работы **В памяти приложений** приводило к восстановлению работоспособности Центра Сертификации.

Аналогичная ситуация была выявлена и при установке ПО Центра регистрации.

Возможная причина: Входящие в состав ПО Центра Сертификации и ПО Центра Регистрации программные модули вызывали конфликт с драйвером eToken для «КриптоПро CSP», не позволявший работать СКЗИ «КриптоПро CSP» в режиме **Службы хранения ключей**.

Рекомендуемое решение:

1. Эксплуатацию Центра Сертификации и Центра Регистрации осуществлять исключительно при настройке СКЗИ «КриптоПро TLS» в режиме **В памяти приложений**. Данное решение является неудобным в том случае, если АРМ Администратора ЦР и Центр Регистрации физически расположены на одной ПЭВМ – при работе привилегированного пользователя на АРМ администратора ЦР при каждом обращении к узлам АРМ Администратора (Запросы на регистрацию, Запросы на сертификат и т.д.) будет осуществляться обращение к закрытому ключу, что потребует ввода пароля (если он установлен и не сохранен на данной ПЭВМ).
2. Отказаться от использования драйвера eToken для «КриптоПро CSP», и использовать только стандартный драйвер для eToken (RTE_3.0.116 и выше)

Ознакомиться с описанием драйвера eToken для «КриптоПро CSP» можно на сайте ООО «КРИПТО-ПРО» (www.cryptopro.ru) в разделе **КриптоПро CSP/Использование/Модули поддержки устройств хранения ключевой информации**

5.2. Ошибки, возникающие при использовании в качестве носителя закрытого ключа уполномоченного лица УЦ (ЦС) USB Flash Drive

Исходные данные: ПЭВМ Центра сертификации – Compaq, носителем закрытого ключа уполномоченного лица удостоверяющего центра должен являться USB Flash Drive. В описываемом случае производителем Flash Drive была компания из юго-восточной Азии – «дочка» Sumsung (точное наименование модели и фирмы-производителя неизвестно).

После установки Службы сертификации, а также после установки ПО Центра Сертификации и последующей перезагрузки контейнер закрытого ключа, располагающийся на FlashDrive (уполномоченного лица УЦ), становился недоступен (система его «не видела» и предлагала вставить носитель, содержащий указанный контейнер). В результате Службы сертификации (MS CA) не запускались, хотя после полной загрузки системы и запуска MS CA «в ручную» работоспособность Центра Сертификации восстанавливалась.

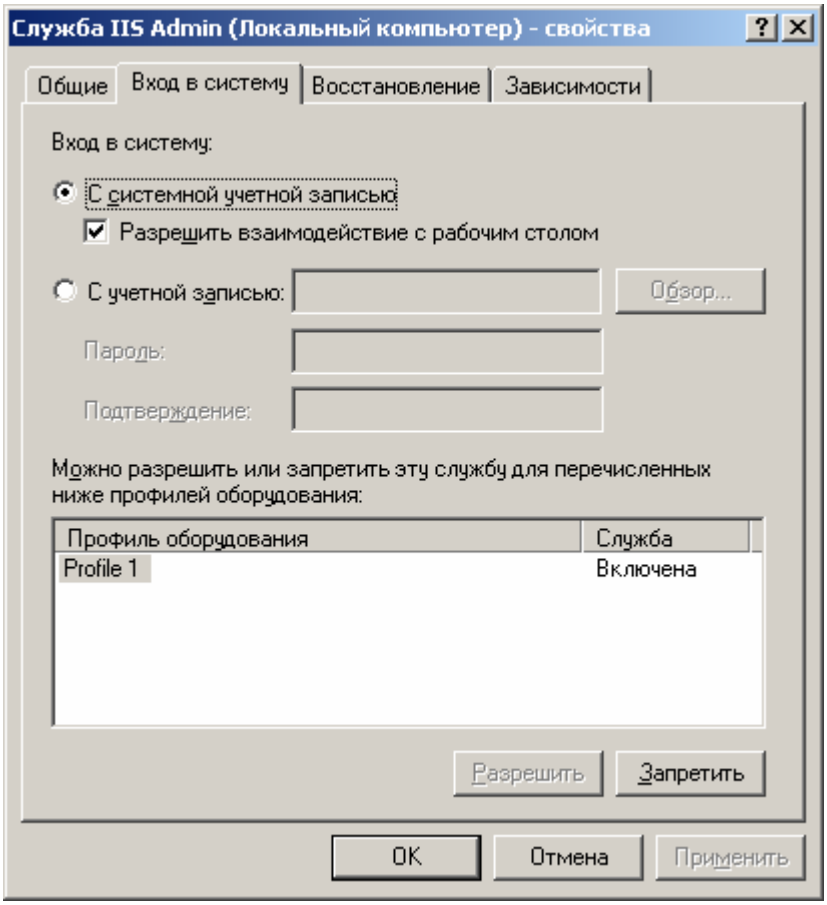
Возможная причина: Порядок загрузки служб операционной системы и драйвера указанного носителя не позволял автоматически осуществлять запуск Службы сертификации (MS CA)

Рекомендуемое решение: Использование носителей Flash Drive успешно зарекомендовавших себя на рынке указанных изделий (например, компании Transcend). Использование в качестве носителя Transcend JetFlash не выявило указанных в описываемом случае ошибок – служба MS CA успешно запускалась и функционировала.

6. Особенности эксплуатации разных типов ключевых носителей.

6.1. Особенности использования ключевых носителей закрытых ключей, соответствующих сертификатам, установленным в хранилище Локальный Компьютер\Личные (сертификатов серверной аутентификации)

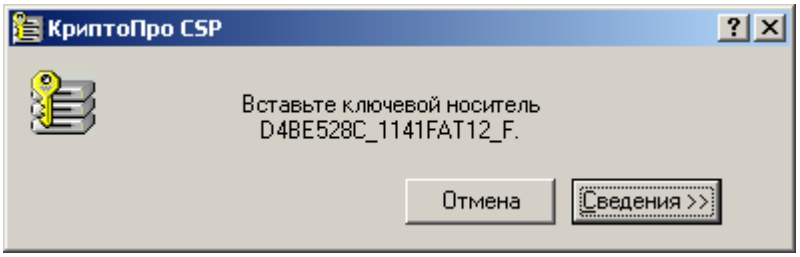
При использовании ключевых носителей, отличных от жесткого диска (Реестр), и использовании паролей на доступ к закрытому ключу для служб, использующих сертификаты серверной аутентификации – IIS Admin и MSSQL, обязательно должен быть установлен переключатель **Разрешить взаимодействие с рабочим столом (Управление компьютером\Службы\Сдужба IIS Admin** и **Управление компьютером\Службы\MSSQL$CPCC** (при использовании экземпляра MSDE), **Управление компьютером\Службы\MSSQLSERVER)**

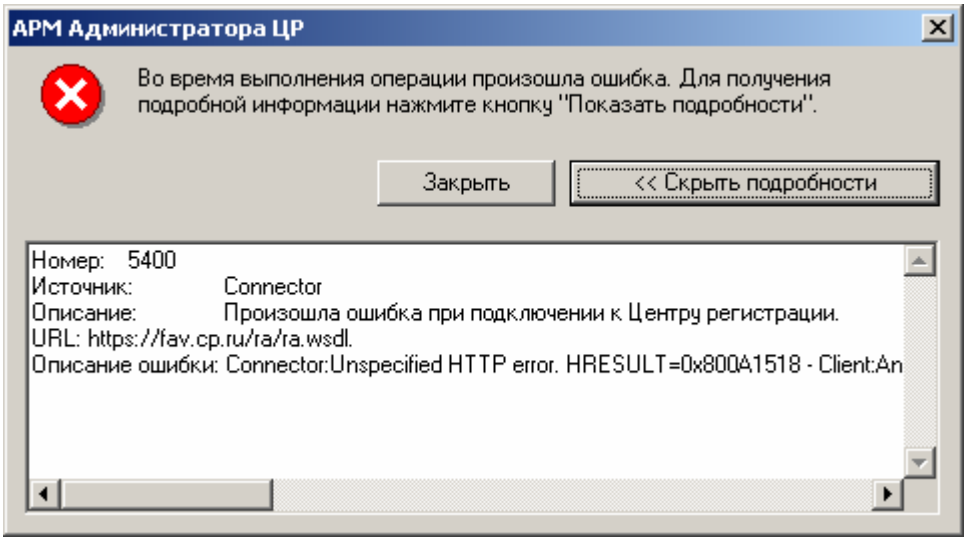


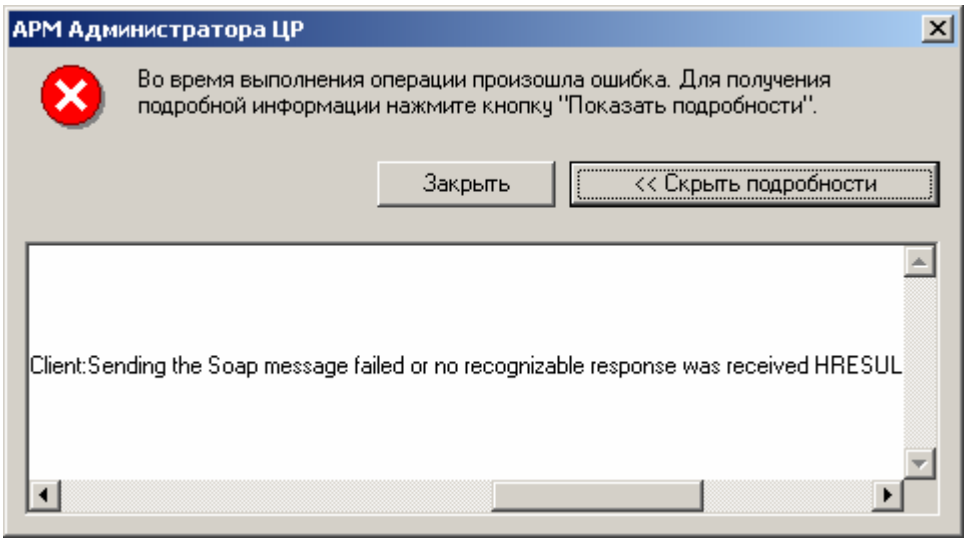
При отсутствии указанной настройки запуск службы MSSQL и доступ к web-страницам по протоколу TLS будут невозможны.

6.2. Особенности использования носителей типа FlashDrive.

Одной из часто встречающихся ошибочных ситуаций, возникающих при использовании в качестве носителя закрытого ключа привилегированного пользователя (Администратора или Оператора) устройства типа FlashDrive, является появление сообщения об отсутствии устройства хранения закрытого ключа и невозможности подключения к Центру Регистрации Удостоверяющего Центра:







Возможная причина: Устройство FlashDrive было добавлено в качестве носителя закрытого ключа (**Свойства: КриптоПро CSP**/**Оборудование**/**Настроить считыватели**) и этому устройству была поставлена в соответствие буква, например, «E». Во время отключения указанного устройства от ПЭВМ АРМ администратора был создан новый логический диск (например, подмонтирована сетевая папка, которой было также присвоено имя «E»). Последующее подключение устройства FlashDrive привело к назначению ему новой буквы – «F», что и привело к невозможности доступа к закрытому ключу.

Рекомендуемое решение: Обеспечить соответствие устройства типа FlashDrive ранее назначенной букве, в частности вновь подключаемым сетевым папкам стараться ставить в соответствие буквы, находящиеся в конце алфавита. Добавление в качестве нового считывателя закрытых ключей (**Свойства: КриптоПро CSP**/**Оборудование**/**Настроить считыватели**) новой буквы, соответствующей устройству FlashDrive, описываемую проблему не решит, поскольку при генерации пары ключей и установке сертификата привилегированного пользователя в реестре ОС

сохраняется указатель, содержащий именно старую букву – в контексте приведенного примера – букву «Е».