# Лабораторная работа №5

Инфраструктура с открытыми ключами (PKI)

Инфраструктура с открытыми ключами (PKI) — это комплексная система, обеспечивающая все необходимые сервисы для использования технологии с открытыми ключами. Цель PKI состоит в управлении ключами и сертификатами, посредством которого корпорация может поддерживать надежную сетевую среду. PKI позволяет использовать сервисы шифрования и выработки цифровой подписи согласованно с широким кругом приложений, функционирующих в среде с открытыми ключами.

## Сервисы управления сертификатами

Сервисы управления сертификатами — это сервисы, образующие ядро инфраструктуры с открытыми ключами. К ним относятся:

**1. Выпуск сертификата.**

Сертификаты выпускаются для пользователей (физических и юридических лиц), для доверенных центров, находящихся на более низких уровнях иерархии доверия, а также для других доверенных центров в случае взаимной сертификации.

**2. Аннулирование сертификата.**

Если пользователь теряет свой секретный ключ, если ключ похищается или компрометируется, или есть вероятность наступления таких событий, действие сертификата должно быть прекращено. После получения подтверждения запроса пользователя об аннулировании сертификата ДЦ уведомляет об аннулировании все заинтересованные стороны, используя список аннулированных сертификатов (CAC). Аналогично аннулированию осуществляется приостановление действия сертификата. Оно заключается в однократной отмене сертификата на определенный период времени в течение срока его действия. После этого действие сертификата возобновляется автоматически или же сертификат аннулируется. Приостановление действия сертификата осуществляется в тех ситуациях, когда невозможно установить подлинность лица, обращающегося с запросом об аннулировании.

**3. Публикация сертификата.**

Выпущенный однократно сертификат включается в каталог (в соответствии со спецификациями стандарта X.500 или иными требованиями), чтобы третьи стороны могли иметь к нему доступ. В одних случаях каталог контролируется доверенным центром, в других — третьей стороной.

Доступ к каталогу может быть ограничен. Если необходимо соблюдение прав приватности абонентов, применяются профилактические меры для защиты от лиц, не имеющих полномочий доступа.

**4. Хранение сертификата в архиве.**

Выпускаемые сертификаты и списки аннулированных сертификатов хранятся в архиве длительное время. Это делается потому, что заверенный цифровой подписью документ

продолжает свое существование и по истечении срока действия сертификата, следовательно, сертификаты с истекшим сроком действия должны быть по-прежнему доступны.

**5. Выработка политики ДЦ.**

Для реализации операций сертификации формируется политика операционной работы ДЦ, работы с персоналом и оборудованием и политика выпуска сертификатов на основе критериев контроля за созданием сертификатов для пользователей и других доверенных центров.

# Вспомогательные сервисы

В инфраструктуре с открытыми ключами могут поддерживаться также различные дополнительные сервисы.

**1. Регистрация.**

Регистрационные сервисы обеспечивают регистрацию и контроль индивидуальной информации, а также аутентификацию, необходимую для выпуска или аннулирования сертификатов (от имени доверенного центра). Фактический выпуск сертификатов осуществляется ДЦ.

**2. Хранение информации в архиве.**

Сервисы хранения информации в архиве предназначены для долговременного хранения и управления цифровыми документами и другой информацией. Сервисы обеспечивают создание резервных копий и восстановление информации в случае уничтожения или старения среды хранения.

**3. Нотариальная аутентификация.**

Нотариальная аутентификация включает аутентификацию отправителя сообщения, подтверждение целостности и юридической силы цифровых документов.

**4. Создание резервных копий и восстановление ключей.**

ДЦ должен иметь возможность восстановить зашифрованную информацию в случае потери пользователями их ключей шифрования. Это означает, что доверенному центру, к которому относится пользователь, необходима система создания резервных копий и восстановления этих ключей. Этот процесс известен как коммерческое создание резервных копий и восстановление ключей, и он отличается от принудительного депонирования ключей третьей стороной (обычно правоохранительными органами), которая получает доступ к ключам для расшифровки необходимой информации. Коммерческие сервисы восстановления ключей обеспечивают заблаговременное засекречивание копии ключа на случай утери ключа пользователем, его ухода с работы, забывания пароля, необходимого для доступа к ключу, и восстановление ключа в ответ на запрос пользователя или его работодателя. В одних случаях ключ является секретным ключом из алгоритма с открытыми ключами, в других — это распределяемый ключ.

**5. Каталог.**

Сервисы каталога осуществляют всестороннее управление и обеспечение информацией, имеющей отношение к пользователю (атрибутами). К атрибутам относится не только сертификат, но и номер телефона, адрес электронной почты абонента и т.д.

**6. Поддержка невозможности отказа от цифровых подписей**

При бумажной технологии подписи лиц законно связывают их с документами, что не позволяет в дальнейшем отказаться от подписания документа. При электронных технологиях обычная подпись заменяется цифровой. Самое главное требование для невозможности отказа от цифровой подписи состоит в том, что ключ, используемый для выработки цифровых подписей — ключ подписи, должен генерироваться и безопасно храниться все время исключительно под контролем пользователя. Когда пользователи забывают свои пароли или теряют свои ключи подписи, на резервирование или восстановление предыдущей пары ключей подписи не накладывается никаких технических ограничений (в отличие от аналогичной ситуации с парами ключей шифрования сообщений). В таких случаях допускается генерация и дальнейшее использование пользователями новых пар ключей подписи.

Параллельное функционирование систем резервного копирования и восстановления ключей и системы поддержки невозможности отказа от цифровых подписей вызывает определенные проблемы. При резервном копировании и восстановлении ключей должны создаваться копии секретных ключей пользователя. Чтобы обеспечить невозможность отказа от цифровой подписи, не должны создаваться резервные копии секретных ключей пользователя, используемых для выработки цифровой подписи. Для соблюдения этих требований в инфраструктуре с открытыми ключами должны поддерживаться две пары ключей для каждого пользователя. В любой момент времени пользователь должен иметь одну пару ключей для шифрования и дешифрования, а другую пару — для выработки или проверки цифровой подписи.

**7. Корректировка ключей и управление историями ключей**

В ближайшем будущем пользователи будут иметь огромное количество пар ключей, которые должны будут поддерживаться как криптографические ключи, даже если никогда не будут использоваться. Ключи шифрования должны со временем обновляться и должна поддерживаться история всех ключей, использованных ранее. (Например, у пользователей появится необходимость расшифровать информацию многолетней давности и проверять цифровую подпись на контракте многие годы в дальнейшем).

Процесс корректировки пар ключей должен быть "прозрачен" для пользователя. Это означает, что пользователи не должны понимать, что осуществляется обновление ключей, и никогда не должны получать отказ сервиса из-за недействительности своих ключей. Для удовлетворения этого требования пары ключей пользователя должны автоматически обновляться до истечения срока их действия. При обновлении пары ключей подписи предыдущий ключ подписи безопасно уничтожается. Тем самым предотвращается получение несанкционированного доступа к ключу подписи и устраняется необходимость хранения предыдущих ключей подписи.

**8. Другие сервисы**

В ряде случаев необходимы и другие сервисы, например, сервисы генерации пар ключей и записи их на смарт-карты, если ключи хранятся на смарт-картах.

В Windows существует мощный инструмент — инфраструктура открытого ключа (public-key infrostructure, PKI). Эта инфраструктура представляет собой набор криптографических служб и инструментов, встроенных в операционную систему и существенно повышающих её безопасность. Криптографический метод, основанный на применении открытого ключа, позволяет решить проблему пересылки секретного ключа. И является, таким образом, очень удобным и применимым для пересылки секретной информации. С другой стороны тот же метод может применяться для аутентификации. Тоже очень важной с точки зрения безопасности функции.

Если рассмотреть поподробнее, как протокол открытого ключа работает, то это будет выглядеть так. Генерируются два взаимосвязанных ключа. Один — открытый — предназначается для всех, с его помощью шифруется сообщение. Другой требуется для расшифровки зашифрованного открытым ключом сообщения. Это прямое применение протокола. Существует и обратное. Можно зашифровать сообщение открытым ключом и послать его владельцу секретного ключа. Если тот сможет расшифровать, и пошлёт обратно расшифрованный текст, то это однозначно определяет его как владельца секретного ключа. На этом принципе строится простейшая процедура аутентификации. Более сложная позволяет сделать тоже самое с помощью открытого ключа и подписи, оставленной владельцем секретного ключа.

Таким образом, в основе инфраструктуры открытого ключа лежит работа с ключами. Для удобного обращения с ними был придуман сертификат. Сертификат является своеобразным документом, удостоверяющим личность человека, компьютера или другого устройства в цифровом мире.

Ещё один основополагающий принцип — доверие. В принципе, сертификаты могут удостоверить только один факт — что человек или устройство является владельцем секретного ключа. Но если вы состоите с кем-то в переписке и получили от него открытый ключ, то вы наверняка знаете, от кого он пришёл. Потому что вы доверяете тому человеку. Вы его знаете.

Вся инфраструктура строится на предположении, что секретный ключ принадлежит законному владельцу. Но это вполне может быть не так. Это самое слабое место всей системы безопасности. Для того, чтобы подобного не происходило, строится иерархическая система доверия. Существуют корневые центры сертификации, которым по умолчанию доверяет операционная система. Эти центры сертификации выдают сертификаты третьим лицам и подписывают их своей цифровой подписью, что позволяет убедиться в их подлинности. Доверие, предоставляемое корневым центрам, таким образом, распространяется и на выданные ими сертификаты.

Инфраструктура открытых ключей позволяет использовать цифровые сертификаты для подтверждения подлинности владельца и позволяет надежно и эффективно защищать трафик передаваемый по открытым сетям связи, а также осуществлять с их помощью аутентификацию пользователей. Основой инфраструктуры открытых ключей является центр сертификации, который осуществляет выдачу и отзыв сертификатов, а также обеспечивает проверку их подлинности.

Для чего это может быть нужно на практике? Цифровые сертификаты позволяют использовать шифрование на уровне приложений (SSL/TLS) для защиты веб-страниц, электронной почты, служб терминалов и т.п., регистрацию в домене при помощи смарт-карт, аутентификацию пользователей виртуальных частных сетей (VPN), шифрование

данных на жестком диске (EFS), а также в ряде случаев обойтись без использования паролей.

Для создания центра сертификации нам понадобится сервер, работающий под управлением Windows Server, который может быть как выделенным, так и совмещать роль центра сертификации с другими ролями. Однако следует помнить, что после развертывания центра сертификации вы не сможете поменять имя компьютера и его принадлежность к домену (рабочей группе).

Центр сертификации (ЦС) может быть двух типов: ЦС предприятия и изолированный (автономный) ЦС, рассмотрим их отличительные особенности:

**ЦС предприятия**

- Требует наличия ActiveDirectory
- Автоматическое подтверждение сертификатов
- Автоматическое развертывание сертификатов
- Возможность запроса сертификатов через Web-интерфейс, мастер запросов и автоматическое развертывание

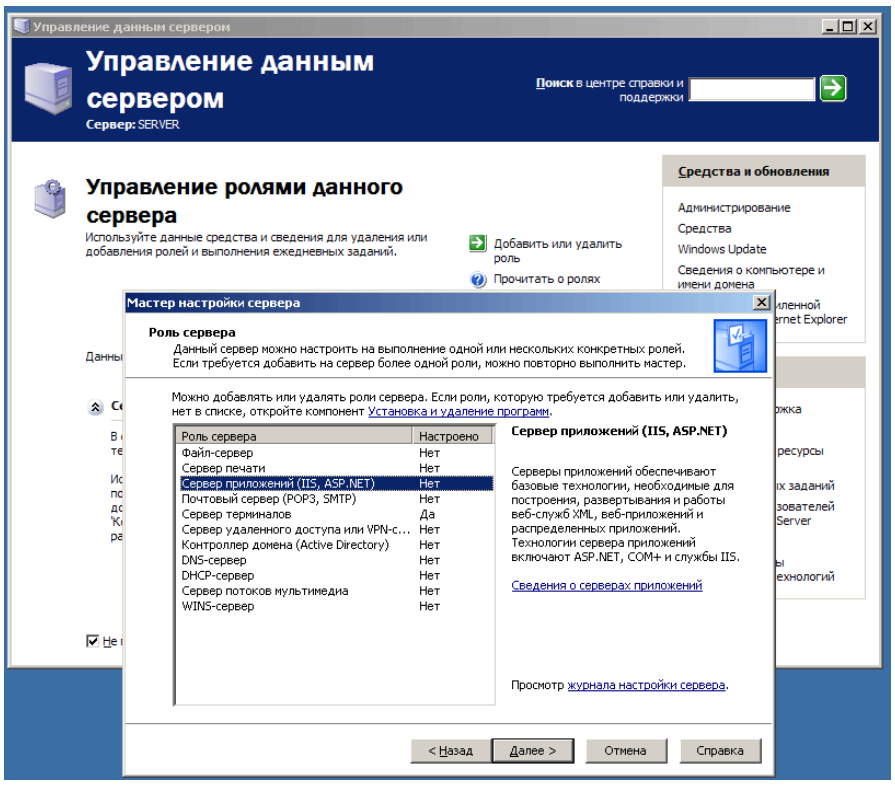
**Изолированный (автономный) ЦС**

- Не требует наличия ActiveDirectory
- Ручное подтверждение сертификатов
- Отсутствие возможности автоматического развертывания
- Запрос сертификатов только через Web-интерфейс

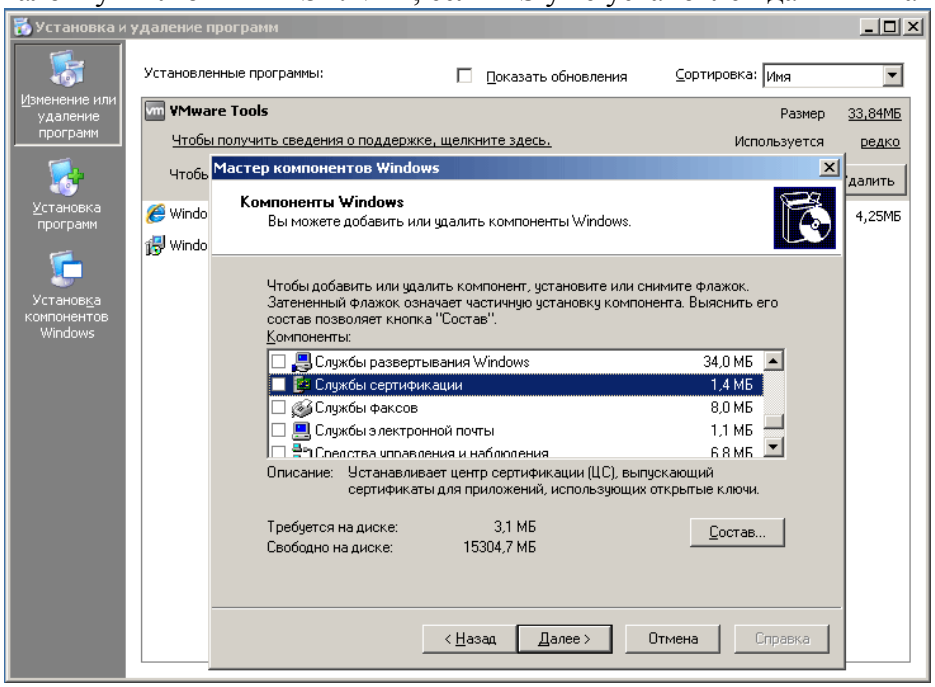
Методика развертывания ЦС для Windows Server 2003 и Windows Server 2008 несколько различаются, поэтому мы решили рассмотреть их в отдельности.

## Windows Server 2003

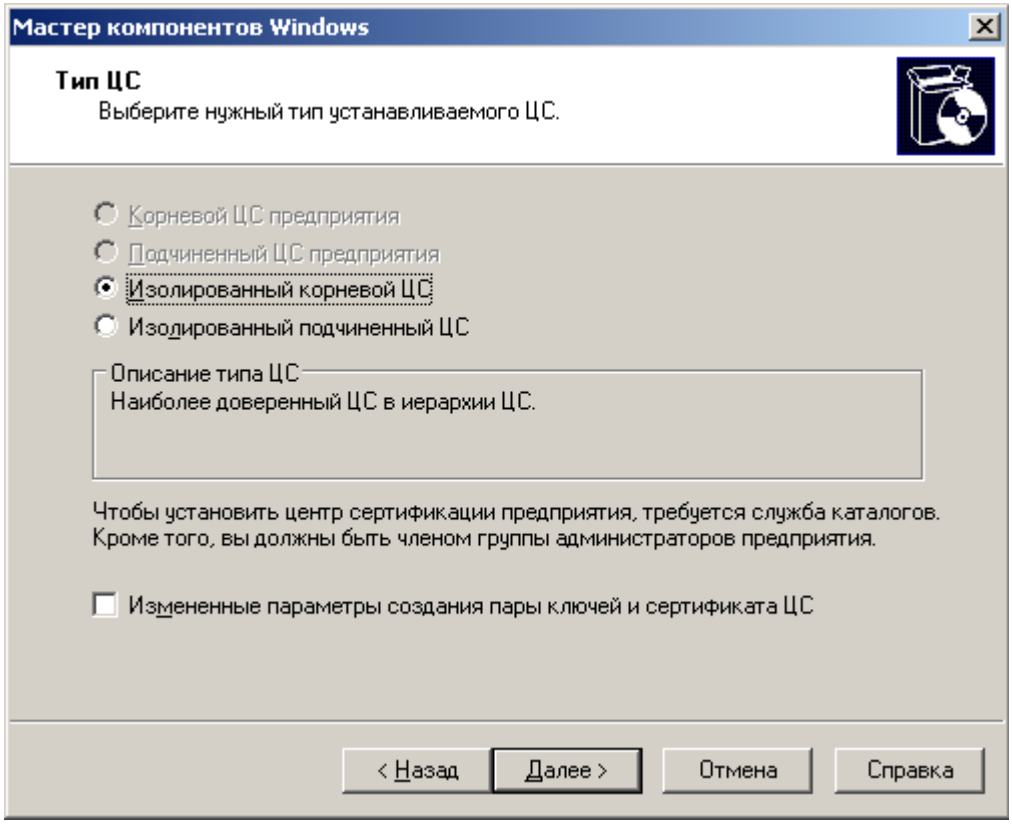
Для возможности использования Web-интерфейса для выдачи сертификатов нам понадобится установленный web-сервер IIS. Установим его через диспетчер сервера: **Пуск - Управление данным сервером - Добавить или удалить роль.**




В списке ролей выбираем роль **Сервера приложений**. В следующем окне устанавливаем галочку **Включить ASP.NET**, если IIS уже установлен данный шаг можно пропустить.




После установки IIS приступим к развертыванию Центра сертификации, это делается через оснастку **Установка и удаление программ - Установка компонетнов Windows**, где выбираем **Службы сертификации**.

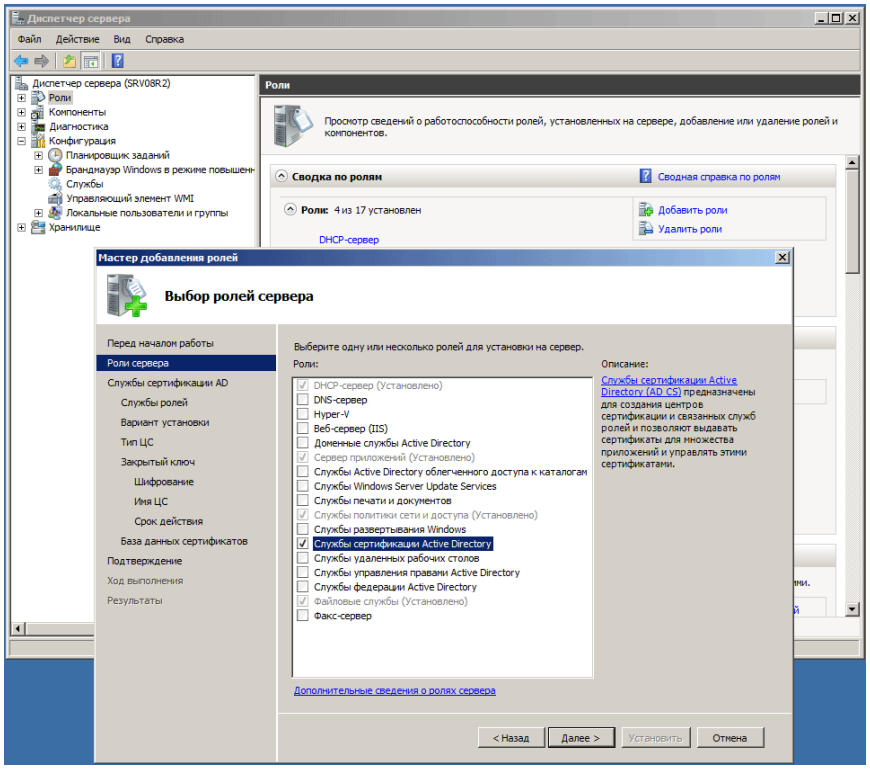



Следующим шагом выберите тип ЦС и его подчиненность. Так как в нашем случае сеть не имеет доменной структуры, то ЦС Предприятия недоступен для выбора. Поскольку это первый (и пока единственный ЦС) следует выбрать корневой сервер, подчиненный тип следует выбирать для развертывания следующих ЦС, например для филиалов.

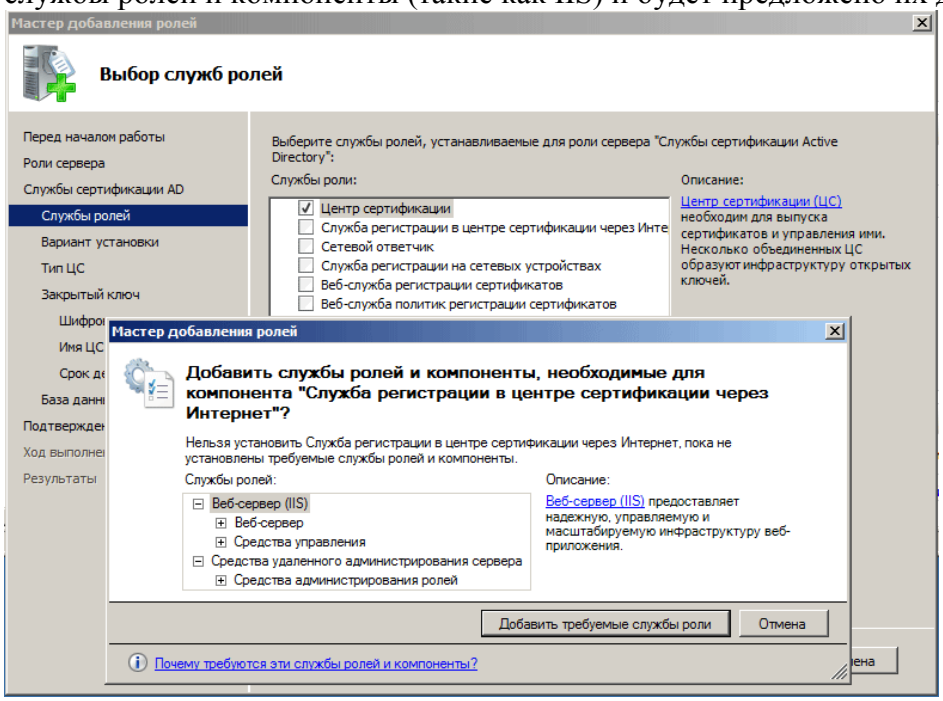
Далее вводим имя ЦС (должно совпадать с именем сервера) и пути размещения файлов. В процессе установки программа предложит перезапустить IIS и, если не была включена поддержка страниц ASP.NET, предложит ее включить, с чем следует согласиться.

## Windows Server 2008 R2

В Windows Server 2008 (2008 R2) все настройки консолидированы в одном месте, что делает установку ЦС более простой и удобной. Выбираем **Диспетчер сервера - Роли - Добавить роли**, в списке ролей выбираем **Службы сертификации Active Directory**.



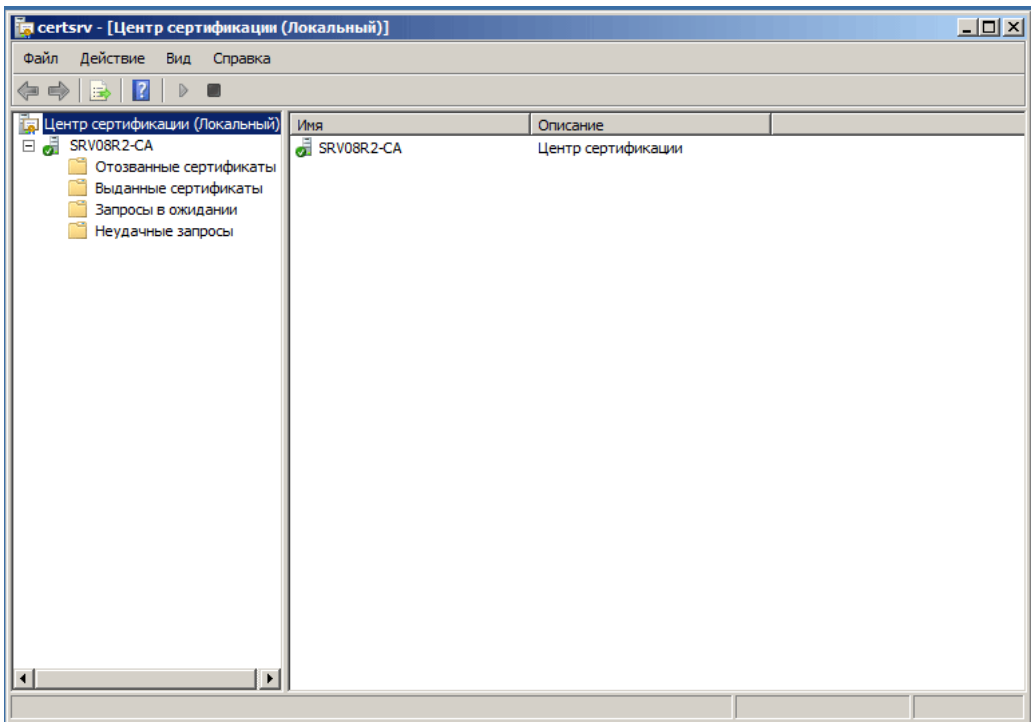

В следующем окне обязательно добавляем компонент **Служба регистрации в центре сертификации через интернет**. При этом будут автоматически определены необходимые службы ролей и компоненты (такие как IIS) и будет предложено их добавить.



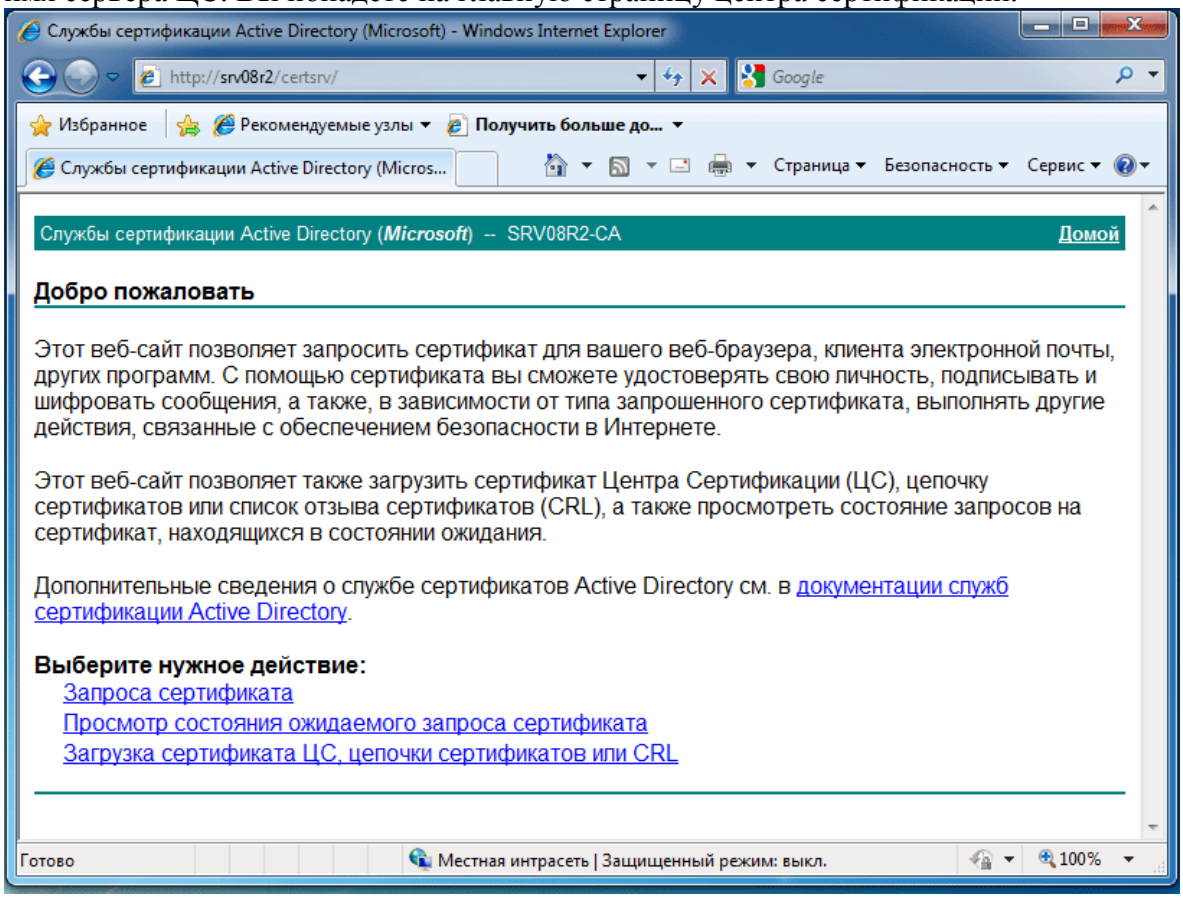

Дальнейшая настройка аналогична Windows Server 2003. Вводим тип ЦС, его имя и место хранения файлов, подтверждаем выбор компонент и завершаем установку.

## Проверка работы ЦС

Для первоначальной проверки работоспособности ЦС можете запустить оснастку **Центр сертификации** (Пуск - Администрирование - Центр Сертификации). Если все сделано правильно вы должны увидеть следующее окно:

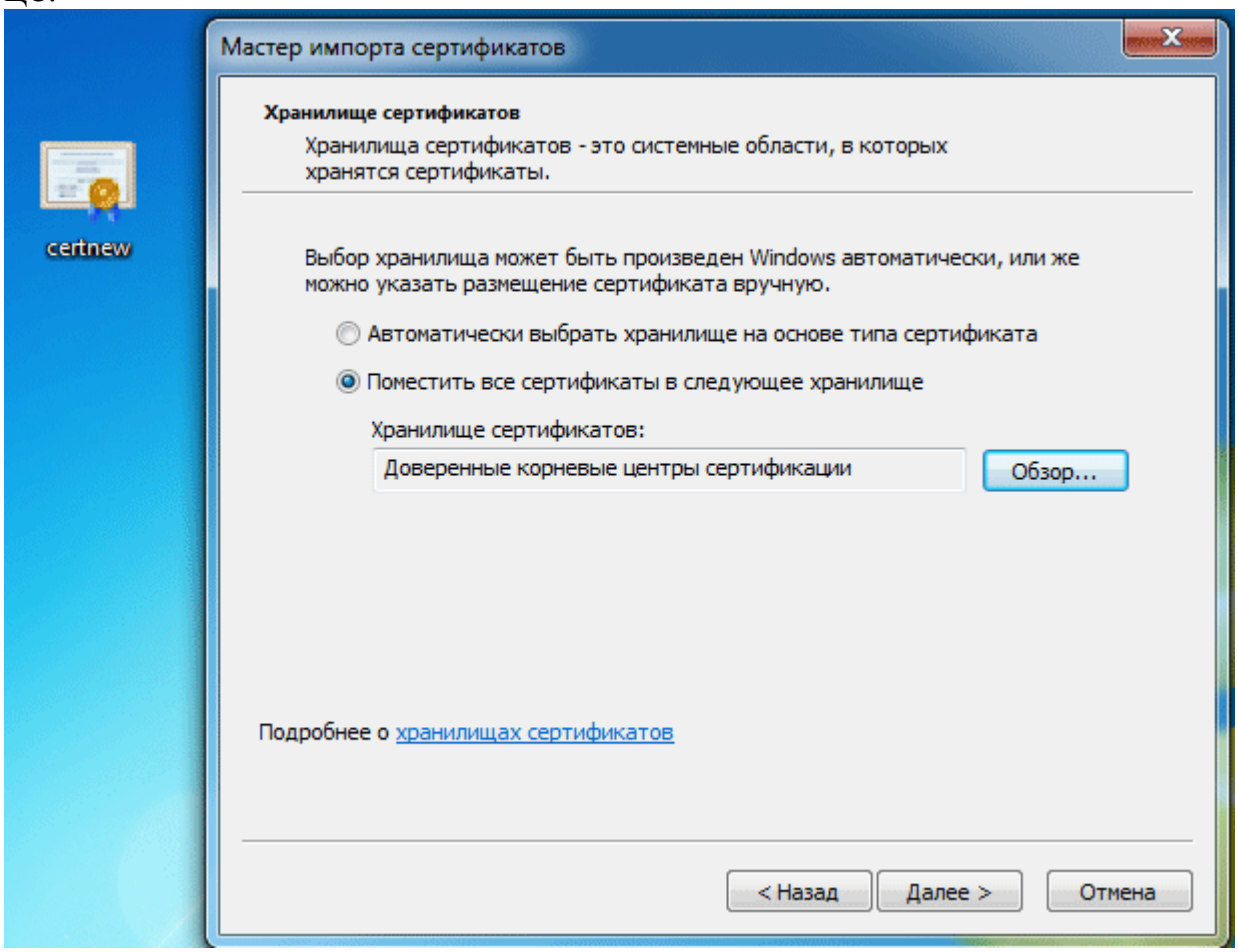



Попробуем теперь получить сертификат для клиентского ПК. Запустим браузер, в адресной строке которого укажем адрес **http://имя_сервера/certsrv**, где **имя_сервера** - имя сервера ЦС. Вы попадете на главную страницу центра сертификации.



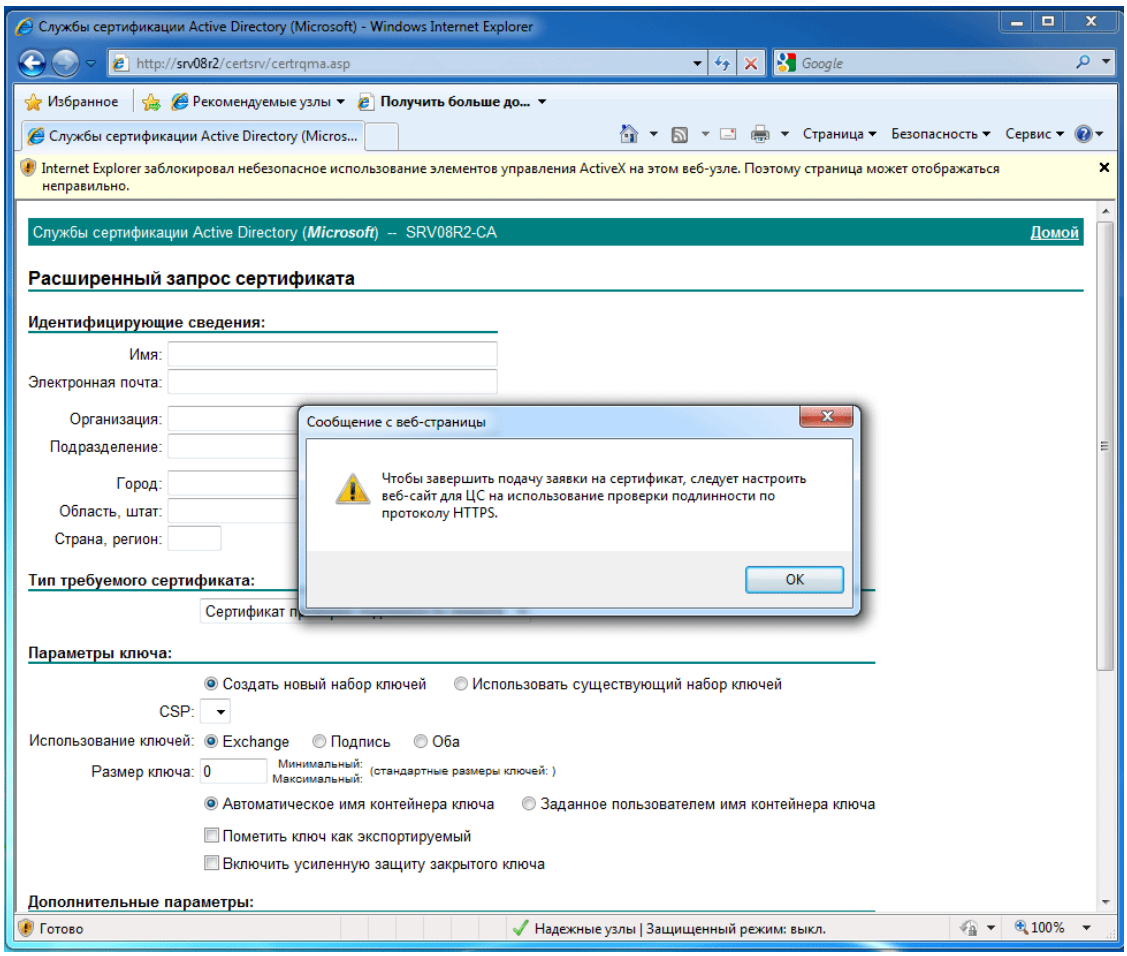

Прежде всего необходимо загрузить сертификат ЦС и поместить его в хранилище доверенных коренных центров сертификации. Если в вашей сети несколько ЦС следует загрузить и установить цепочку сертификатов. Для этого выбираем: **Загрузка сертификата ЦС, цепочки сертификатов или CRL**, затем **Загрузка сертификата ЦС** или **Загрузка сертификата ЦС** и сохраняем сертификат в любое удобное место.

Теперь перейдем к установке, для этого щелкнем правой кнопкой на файле сертификата и выберем **Установить сертификат**, откроется мастер импорта, в котором откажемся от автоматического выбора хранилища вручную выбрав **Доверенные корневые центры сертификации**, теперь данный ПК будет доверять всем сертификатам выданным данным ЦС.

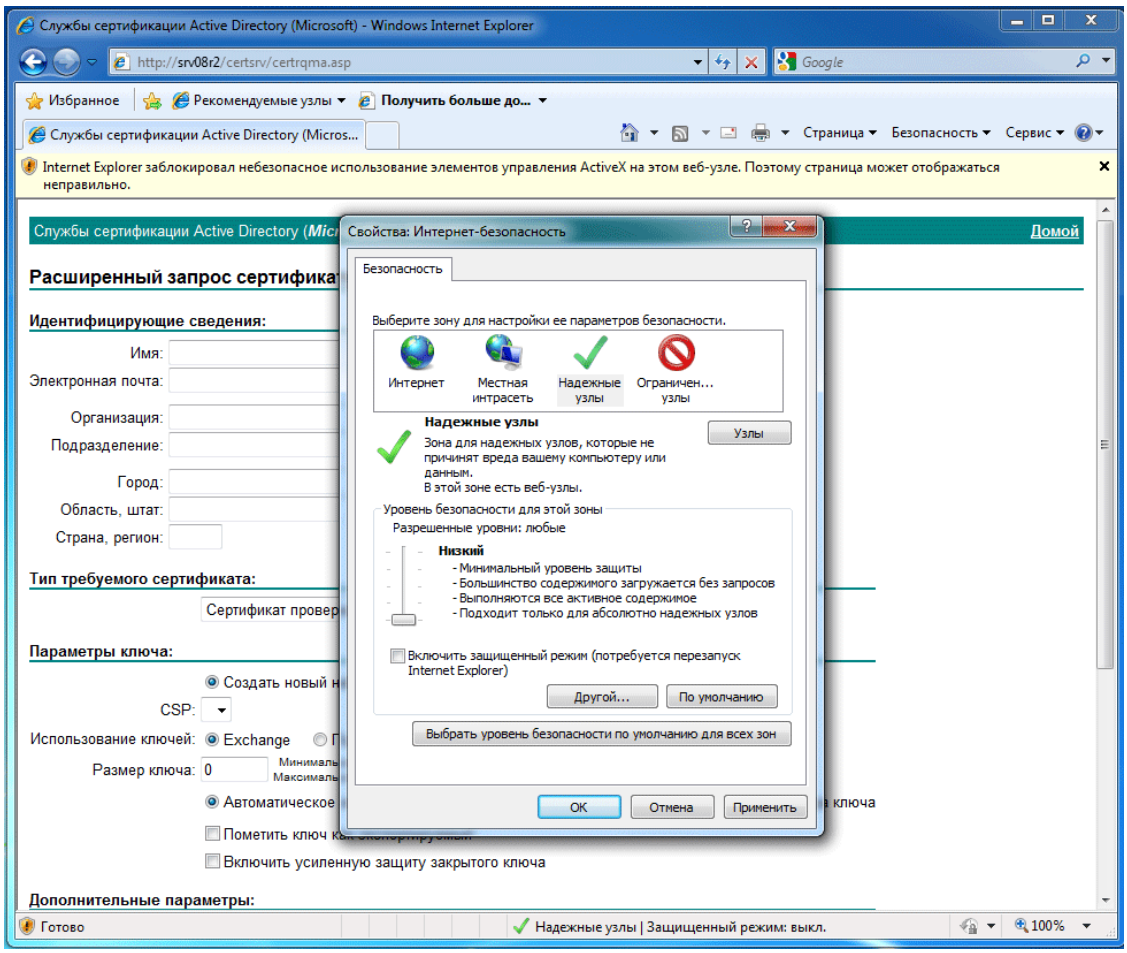



Для получения клиентского сертификата снова откроем сайт ЦС и выберем **Запрос сертификата - расширенный запрос сертификата - Создать и выдать запрос к этому ЦС**. Заполняем форму запроса, в качестве имени указываем имя ПК или пользователя, в качестве типа сертификата указываем Сертификат проверки подлинности клиента и жмем кнопку **Выдать**.

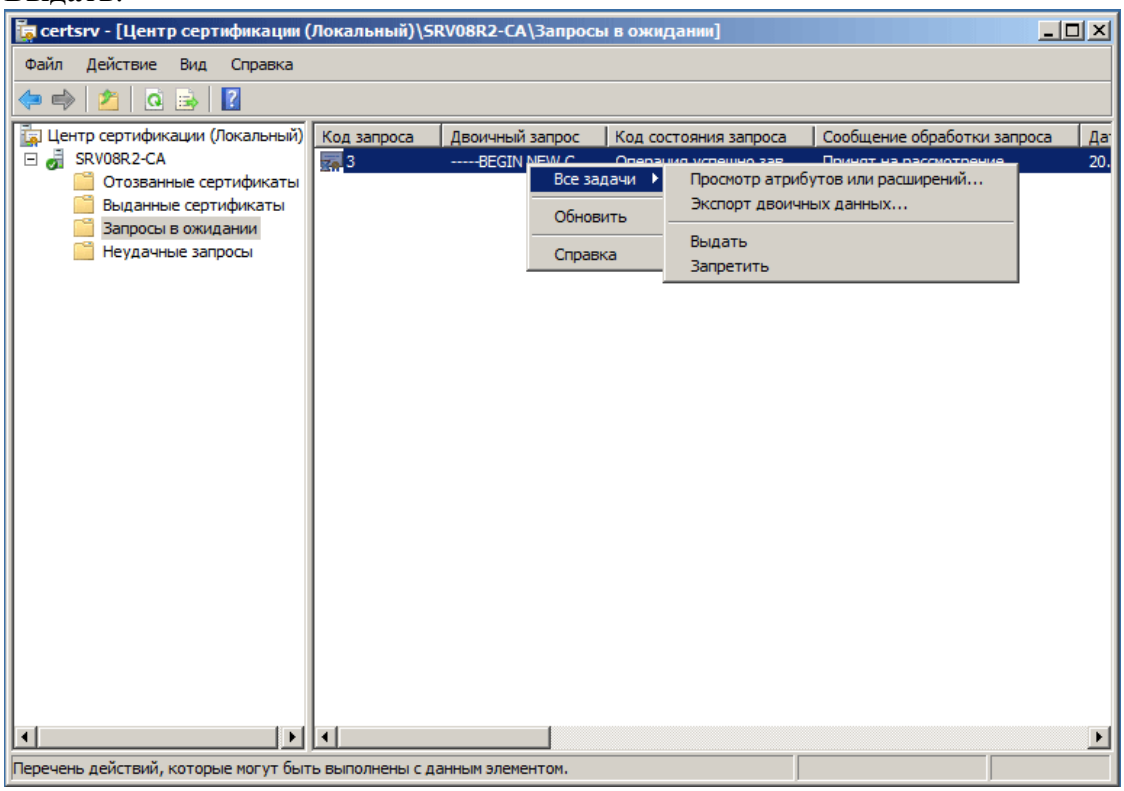
При попытке создать запрос сертификата вы можете получить следующее предупреждение:




В этом случае можно добавить данный узел в зону Надежные узлы и установить низкий уровень безопасности для этой зоны. В Windows Server понадобится также разрешить загрузку неподписанных ActiveX.



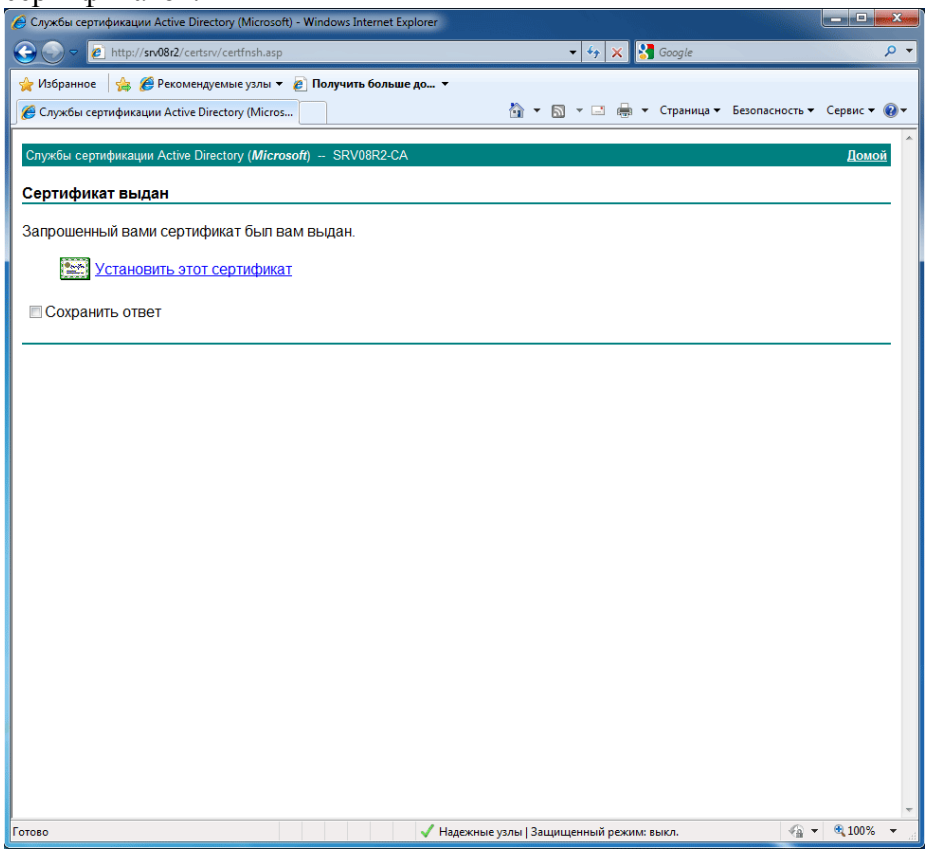

Теперь на сервере откроем оснастку **Центр сертификации** и в разделе **Запросы на ожидание** найдем наш запрос и щелкнув на него правой кнопкой выберем **Все задачи - Выдать.**




Теперь вернемся на клиентский ПК и еще раз откроем сайт ЦС. На этот раз выберем **Просмотр состояния ожидаемого запроса сертификата**, вы увидите свой запрос, щелкнув на которой вы попадете на страницу **Сертификат выдан** и сможете сразу его

установить.

Если все сделано правильно, то сертификат успешно установится в хранилище личных сертификатов.




По окончании проверки не забудьте удалить ненужные сертификаты с клиентского ПК и отозвать их в центре сертификации на сервере.

**Практическое задание:**

1. **Развернуть структуру PKI на базе сервера Windows;**
2. **Произвести настройку центра сертификации;**
3. **Установить сгенерированный корневой сертификат в хранилище сертификатов;**
4. **Сгенерировать новый сертификат для локального ПК, либо виртуальной клиентской машины;**
5. **Сгенерировать различные сертификаты для клиентских приложений.**

**Контрольные вопросы**

**1. Как выглядит процедура получения сертификата при использовании web-страницы формирования запроса?**

**2. Каким образом используется сертификат пользователя при шифровании в EFS? Каким требованиям он должен удовлетворять?**

**3. Какой формат позволяет экспортировать сертификат вместе с путем сертфиикации?**

**4. По каким причинам необходимо разделение ключевых пар, используемых для подписи и шифрования?**

**5. Используется ли в S/MIME технология «цифрового конверта»?**

**6. В чем отличие расширений сертификата Key Usage и Extended Key Usage? Для чего они используются?**

**7. Каким образом осуществляется проверка статуса сертификатов? Каким образом пользователи могут узнать источник информации о статусе данного сертификата?**