ЛАБОРАТОРНАЯ РАБОТА №1

УСТАНОВКА И НАСТРОЙКА ACTIVE DIRECTORY CERTIFICATE SERVICES

Цель работы

Целью данной лабораторной является ознакомление с процессом установки службы Active Directory Certificate Services (службы сертификации) и особенностями работы с сертификатами.

Ход работы

Данная лабораторная работа полностью выполняется на виртуальной машине с установленной операционной системой Windows Server 2008 R2.

Начнем с установки службы сертификации Active Directory (Active Directory Certificate Services). Организации могут использовать службы сертификации AD CS в инфраструктуре открытых ключей PKI (Public Key Infrastructure), чтобы создать центр сертификации для выдачи цифровых сертификатов, которые привязывают объект идентификации пользователя, устройства либо службы к соответствующему частному лицу.

Структура Active Directory включает пять технологий. Эти технологии полностью реализуют идентификацию и доступ «IDA»:

- Доменные службы Active Directory (Active Directory Domain Services) – Идентификация: проверяются подлинность и авторизация в сети, а так же поддерживается управление объектами с помощью групповой политики.
- Службы облегченного доступа к каталогам (Active Directory Lightweight Directory Services) – Приложения: поддерживает множество хранилищ данных в одной системе, чтобы каждое приложение можно было развернуть с собственным каталогом, схемой, назначенным облегченным протоколом доступа к каталогам LDAP (Lightweight Directory Access Protocol) , портами SSL и журналом событий приложений.
- Службы сертификации Active Directory (Active Directory Certificate Services) – Доверие: организации могут использовать службы сертификации AD CS в инфраструктуре открытых ключей PKI (Public Key Infrastructure) , чтобы создать центр сертификации для выдачи цифровых сертификатов, которые привязывают объект идентификации пользователя, устройства либо службы к соответствующему частному лицу.
- Службы управления правами Active Directory (Active Directory Rights Management Services) – Целостность: предоставляют технологию защиты информации, с помощью которой можно реализовать шаблоны устойчивых политик использования, задающих разрешенное и неавторизованное применение в сети, вне ее, а так же внутри и вне периметра брандмауэра
- Службы федерации Active Directory (Active Directory Federation Services) – Партнерские отношения: с помощью служб AD FS организация может расширить инфраструктуру «IDA» на множестве платформ, включая среды Windows и другие, а также обеспечить для доверенных партнеров защиту прав идентификации и доступа вне периметра безопасности.

Для начала запустите виртуальную машина, имеющую ОС Windows server 2008 R2 (Rus) с установленной службой активных каталогов Active Directory.

Рис.1 – Общий вид виртуальной машины

Далее производится авторизация под учетной записью администратора. После загрузки системы нажмите ПУСК-ВЫПОЛНИТЬ. В командной строке набрать команду servermanager.msc для вызова окна диспетчера задач.

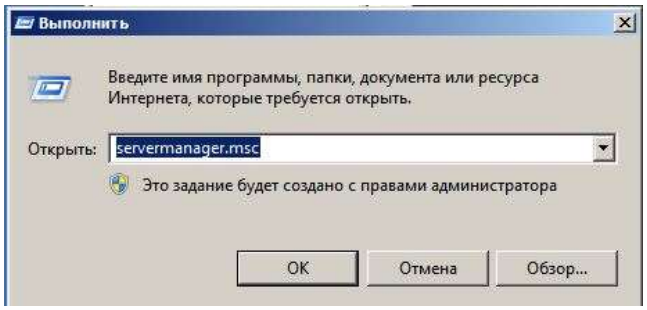


Рис.2 . Командная строка

Рис.3 . Диспетчер задач

Затем нажмите ДОБАВИТЬ РОЛИ. В открывшемся окне отметить пункт СЛУЖБЫ СЕРТИФИКАЦИИ ACTIVE DIRECTORY.

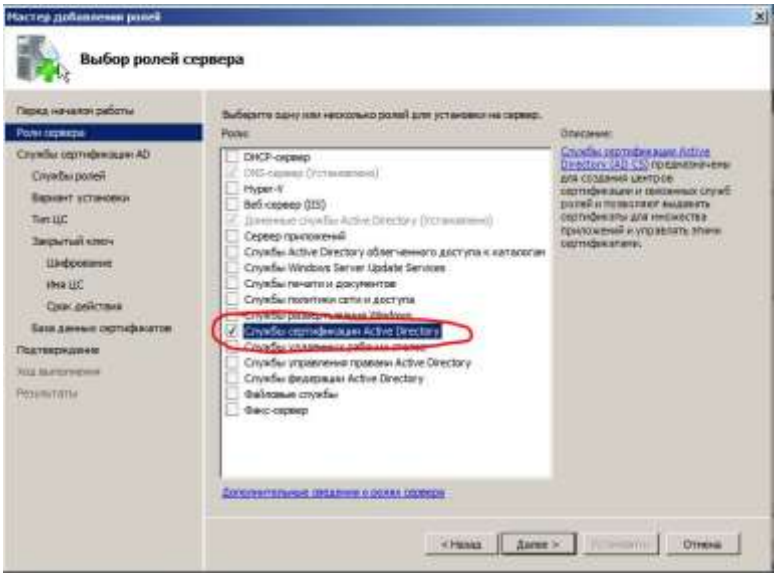


Рис.4 . Выбор роли для установки

Жмите ДАЛЕЕ-ДАЛЕЕ. Каждая роль имеет свои службы. Для дальнейшей работы со «службой сертификации «AD» поставим галочки напротив службы ЦЕНТР СЕРТИФИКАЦИИ СЛУЖБА РЕГИСТРАЦИИ В ЦЕНТРЕ СЕРТИФИКАЦИИ ЧЕРЕЗ ИНТЕРНЕТ.

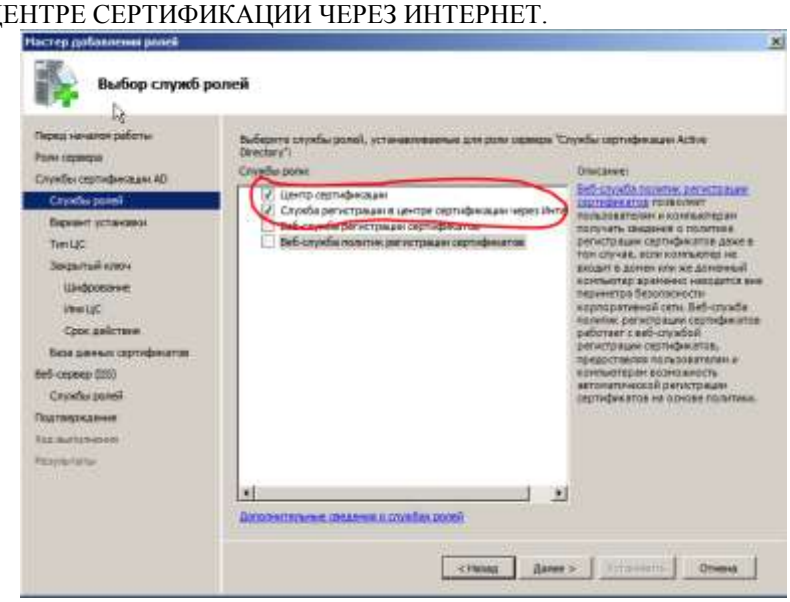


Рис.5 .Выбор службы ролей

ВЕБ-СЛУЖБА РЕГИСТРАЦИИ СЕРТИФИКАТОВ устанавливается после установки двух предыдущих служб.

Нажмем ДАЛЕЕ (Рис.5). В задании типа установки выберем ПРЕПРИЯТИЕ. Выбор УЦ предприятия обусловлен интеграцией с AD и дальнейшей простотой эксплуатации.

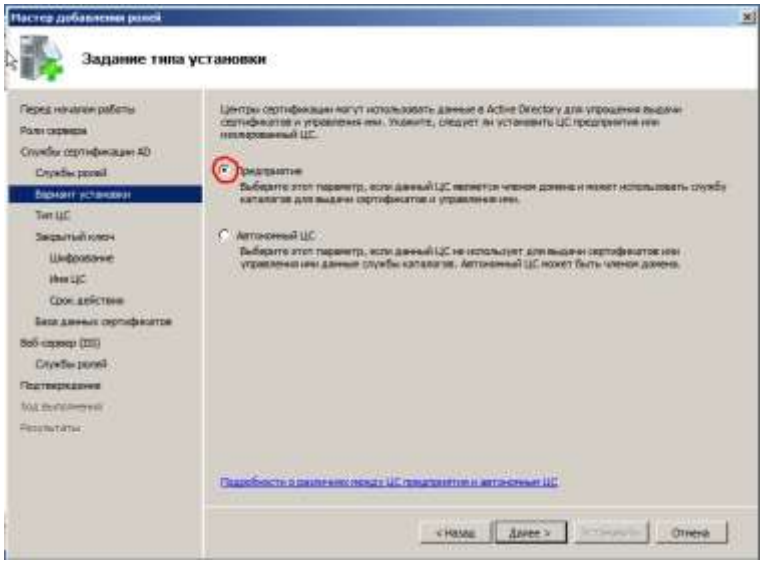


Рис.6. Задание типа установки

Нажмите ДАЛЕЕ. При задании типа ЦС выберем КОРНЕВОЙ ЦС, так как для дальнейшей работы необходим «самостоятельный» ЦС (корневой), который способен сам выдавать и подписывать сертификаты.

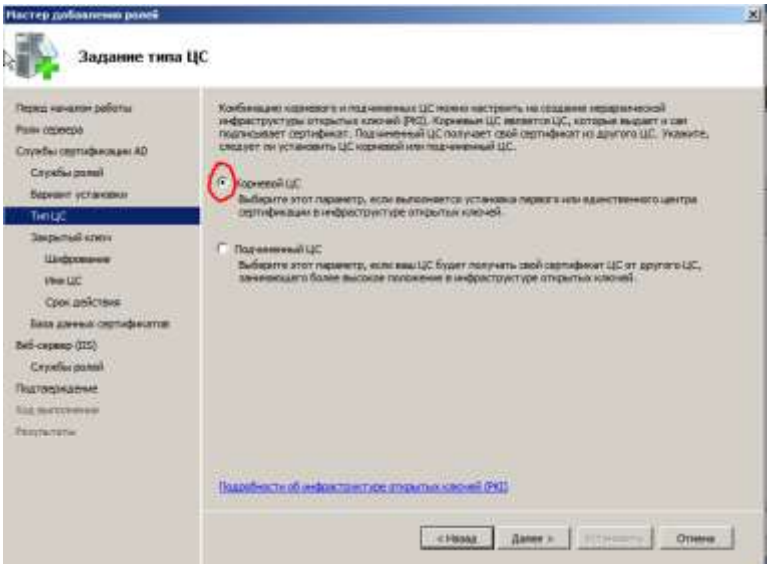


Рис.7 . Задание типа ЦС

Нажмем ДАЛЕЕ. Следующее окно позволяет выбрать тип закрытого ключа для работы будущего ЦС: уже готовый закрытый ключ или сделать новый закрытый ключ. Для выполнения данной лабораторной работы нам необходим новый ключ. Для этого выберем пункт СОЗДАТЬ НОВЫЙ ЗАКРЫТЫЙ КЛЮЧ (Рис.8).

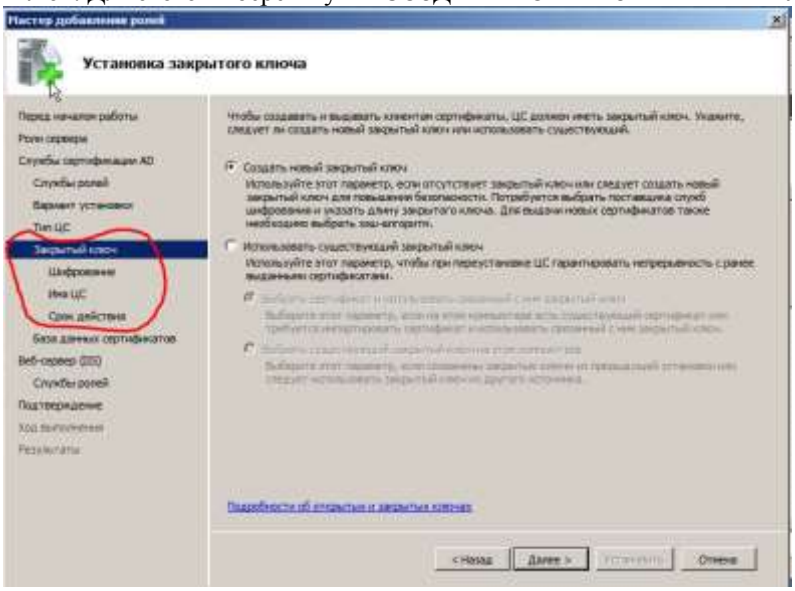


Рис.8 . Установка закрытого ключа

Нажмем ДАЛЕЕ. После шага с выбором установки закрытого ключа требуется произвести некоторые небольшие настройки шифрования будущего ЦС (рис.9). В данном окне, для начала, выберем поставщика служб шифрования (CSP, дословно, Cryptographic service provider). Компания Microsoft по умолчанию предалагает для выбора CSP собственной разработки, которые называется Microsoft Software Storage Provider. Но также предоставляется возможность работы с другими поставщиками. Недостатки посторонних CSP в том, что не всегда проявляется стабильности в их работе, а также если все-таки возникают проблемы в ходе работы, то, в отличии от «Майкрософтовского» поставщика, для получения руководства пользователя необходимо будет обращаться к разработчикам данного CSP. Данная лабораторная работа предусматривает работу с поставщиком по умолчанию. Выберите в строке ВЫБЕРИТЕ ПОСАВЩИКА СЛУЖБ ИНФОРМАЦИИ (CSP) - «RSA #Microsoft Software Storage Provider».

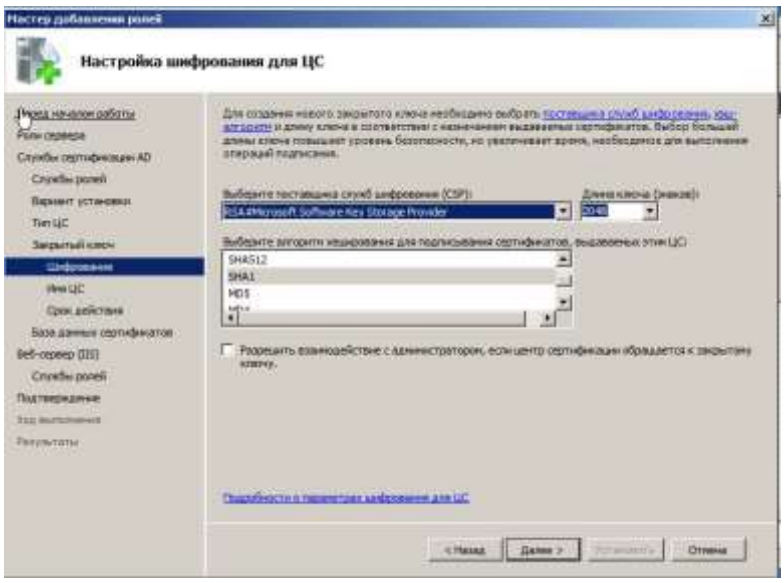


Рис.9 . Настройка шифрования для Центра сертификации

Следующим шагом необходимо задать имя будущего ЦС. (рис. 10).

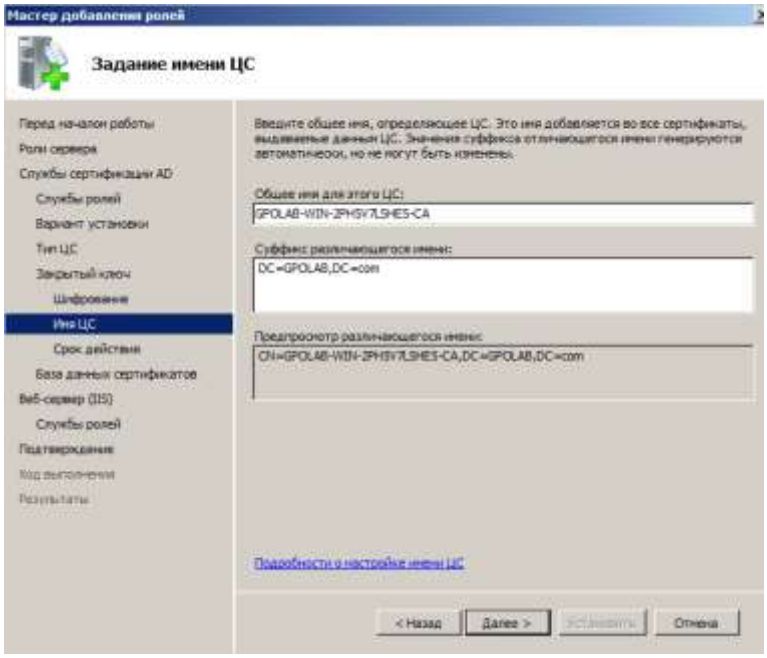


Рис.10. Задание имени ЦС

В следующем окне необходимо указать срок существования вашего будущего Центра сертификации. Стоит заметить, что срок действия сертификата зависит от срока действия его ЦС. По умолчанию предлагается пять лет. Рекомендуем так и отставить.

После нажатия кнопки ДАЛЕЕ появляется окно, где пользователю необходимо выбрать директорию для хранения всех сертификатов и журнал базы данных. То есть необходимо указать физическое место на вашем сервере, где будут хранится все сертификаты данного ЦС (рис.11).

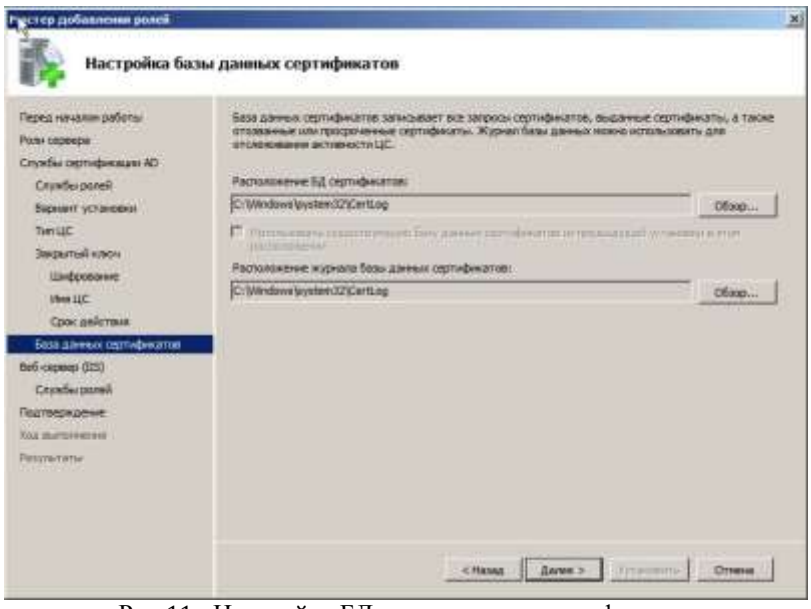


Рис.11 . Настройка БД для хранения сертификатов

Нажать кнопку ДАЛЕЕ. На данном этапе производится установка веб-сервера Internet Information Services (IIS). IIS уже интегрирован Windows Server 2008 R2. Веб-сервер это одна из служб IIS, которая позволяет организовывать совместный доступ к информации через Интернет. На данном этапе никаких действий от обучающегося не требуется. Просто внимательно прочитайте небольшой текст на странице и переходите к следующему шагу. Нажать ДАЛЕЕ.

Следующее окно отображает общую информацию о всех вами выбранных настройках для создаваемого ЦС. Просмотрите все пункты, нажмите кнопку ДАЛЕЕ. Начнется установка (рис.12).

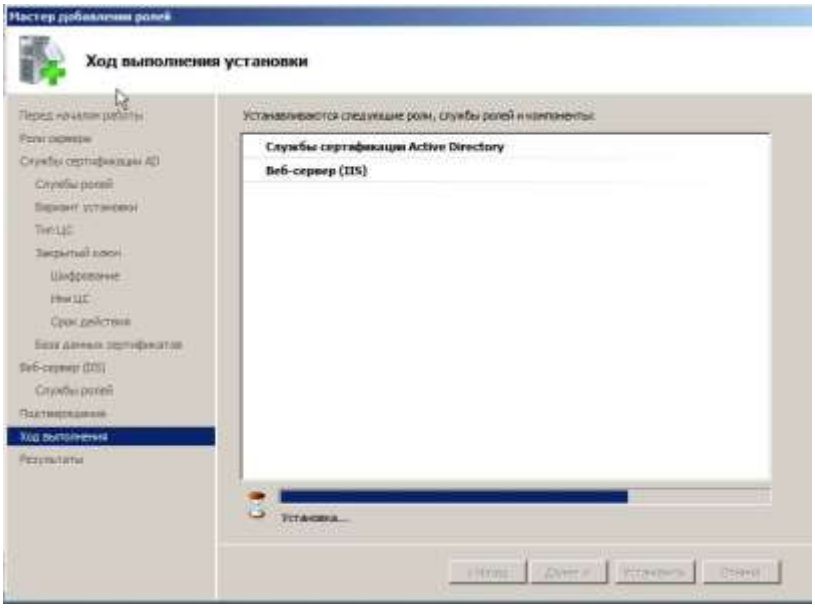


Рис.12 . Ход выполнения установки службы сертификации

Дождавшись окончания установки появится окно с результатами. На скриншоте (рис.13) выделены две строчки. Сравните своими результатами. Если все установилось успешно, поздравляю вас.

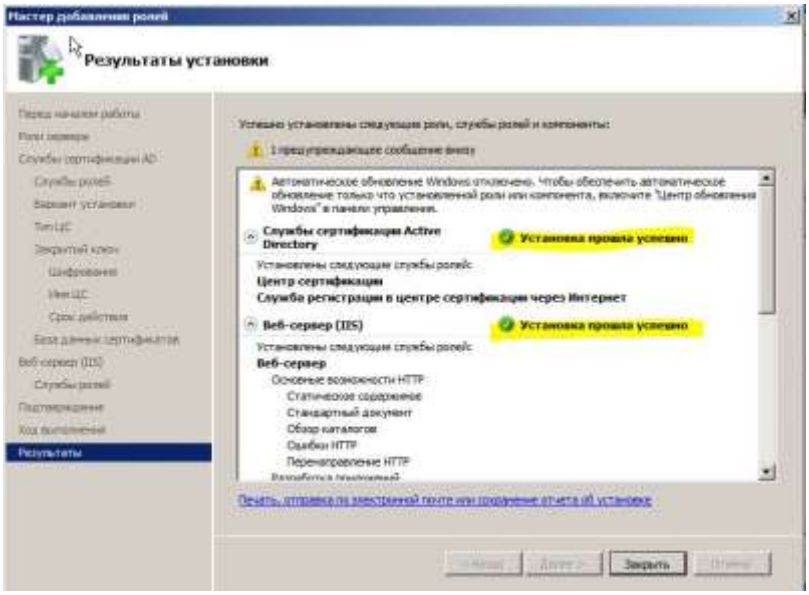


Рис.13 . Результаты установки

Теперь нужно добавить службу роли под название «ВЕБ-СЛУЖБА РЕГИСТРАЦИИ СЕРТИФИКАТОВ», которую мы пропустили в основной установке службы сертификации AD. Для этого перейдем на главное окно ДИСПЕТЧЕРА СЕРВЕРА. В правой его части выберем двойным кликом мыши пункт СЛУЖБЫ СЕРТИФИКАЦИИ AD. В правом появившемся окне найдите пункт СЛУЖБЫ РОЛЕЙ. И нажмите ДОБАВИТЬ СЛУЖБЫ РОЛЕЙ (рис.14).

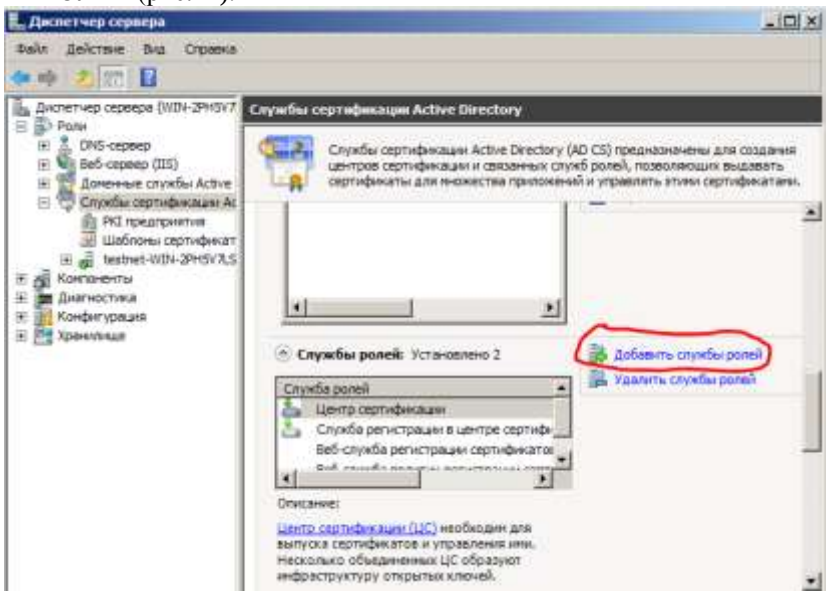


Рис.14 . Добавление службы ролей

В следующем окне выберите галочкой пункт ВЕБ-СЛУЖБА РЕГИСТРАЦИИ СЕРТИФИКАТОВ (рис.15).

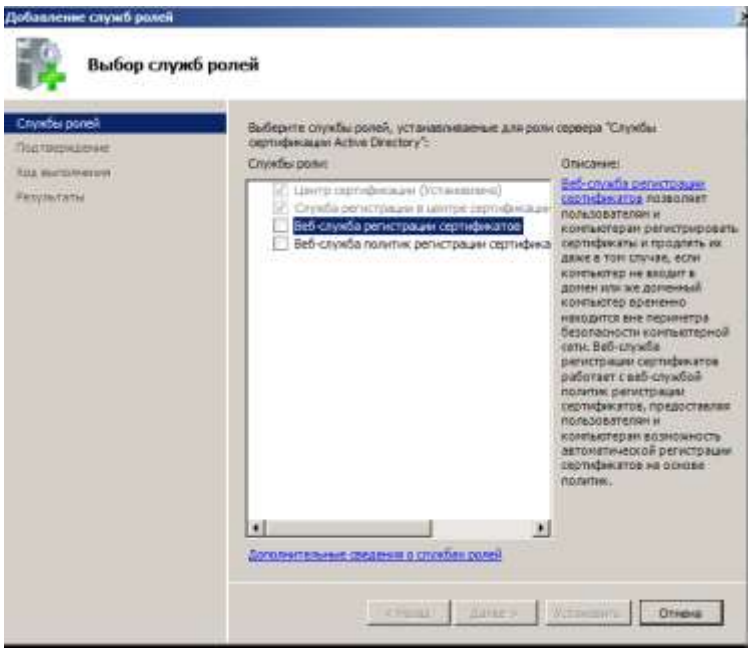


Рис.15 . Выбор служб ролей

При установки галочки открывается окно МАСТЕР ДОБАВЛЕНИЯ РОЛЕЙ (рис.16), где предлагается включить дополнительно некоторые службы, требуемые для корректной работы веб-служб для регистрации сертификатов. Нажмите ДОБАВИТЬ ТРЕБУЕМЫЕ СЛУЖБЫ РОЛИ.

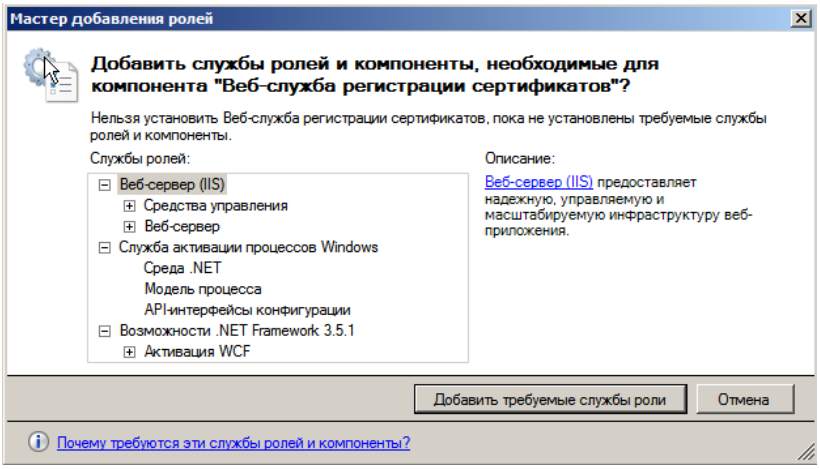


Рис.16. Мастер добавления ролей

На следующем окне необходимо выбрать ЦС, к которому будет прикреплена данная служба. Так как ранее уже был создан ЦС. Выберем ПРОСМОТР ПО ИМЯ ЦС и убедимся что в строке нижеуказанное верное имя (как на скриншоте рисунка 17).

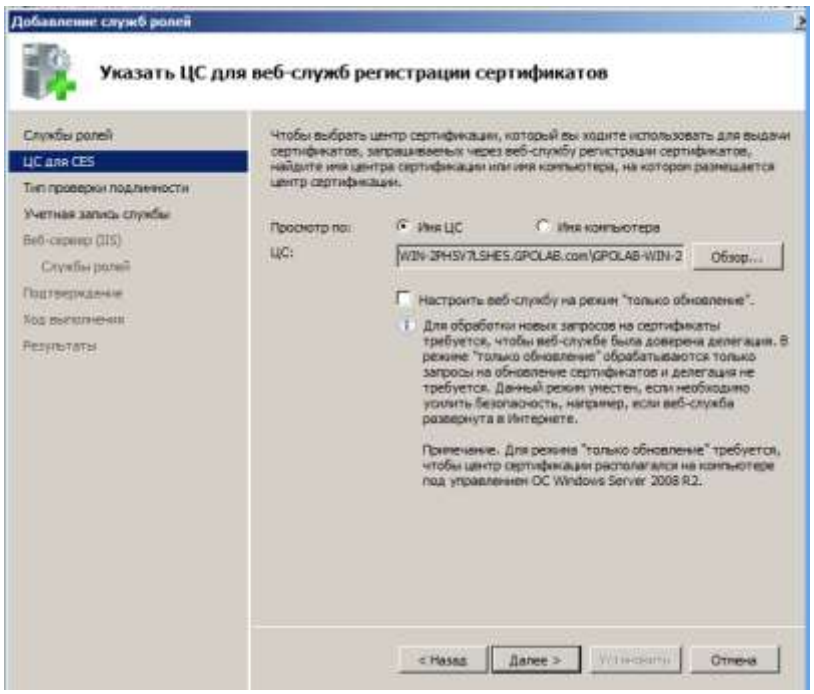


Рис.17 . Выбор ЦС для службы

Нажмите ДАЛЕЕ. В следующем окне выберите пункт ИМЯ ПОЛЬЗОВАТЕЛЯ И ПАРОЛЬ. Прочитайте описание про этот пункт (рис.18).

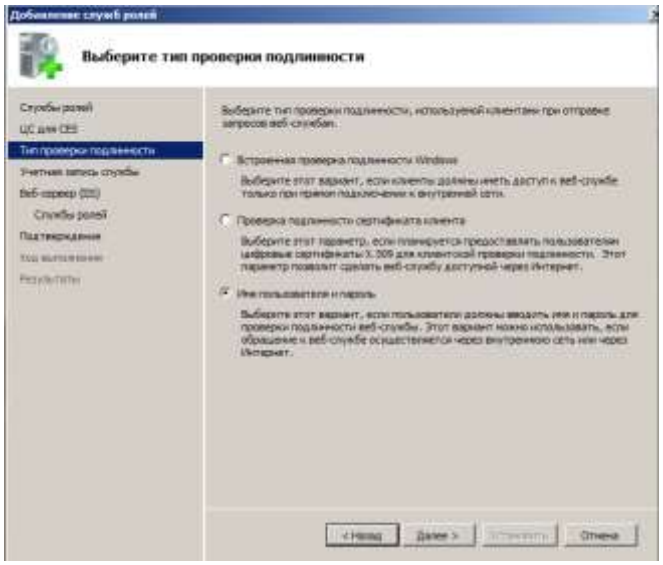


Рис.18 . Тип проверки подлинности

Нажмите ДАЛЕЕ. Укажите ИСПОЛЬЗОВАТЬ ВСТРОЕННЫЙ ИНДЕНТИФИКАТОР ПУЛА ПРИЛОЖЕНИЙ.

Нажмите ДАЛЕЕ. На следующем окне внимательно прочитайте всю информацию о Веб-серверах (рис.19).

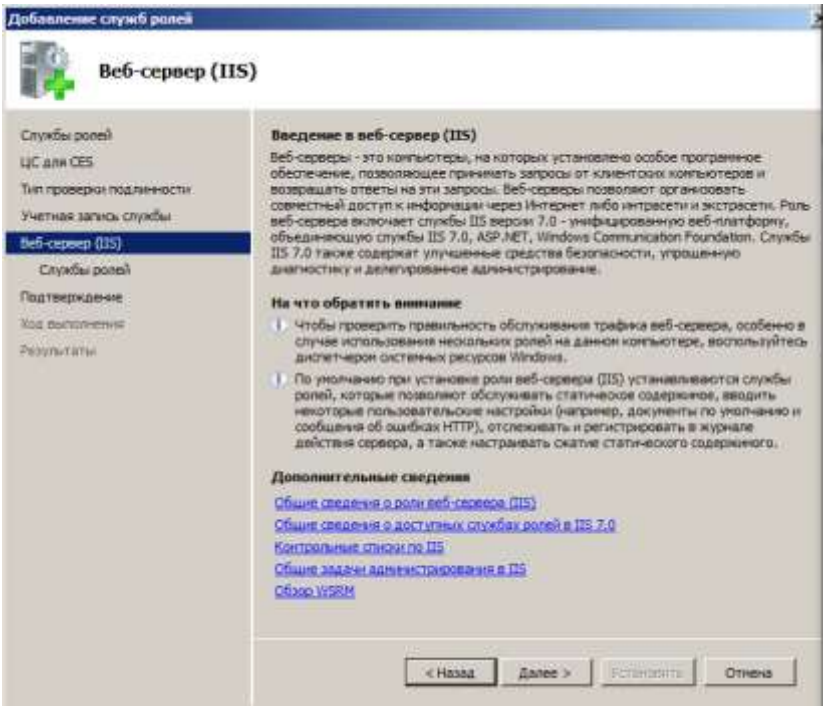


Рис.19 . IIS

Нажмите ДАЛЕЕ, в следующем окне от студента не требуется никаких действий (рис.20).

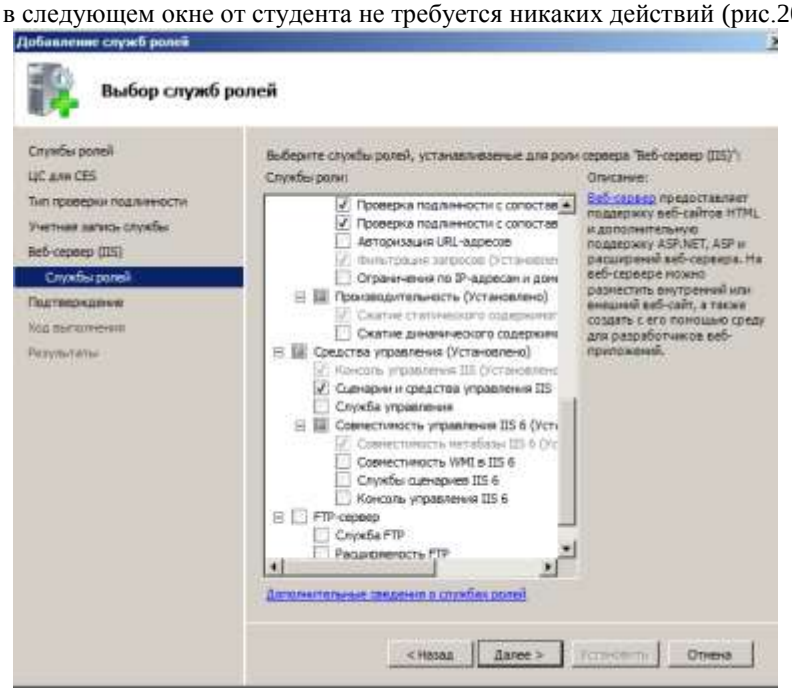


Рис.20 . Выбор служб ролей

Снова нажмите ДАЛЕЕ. На данном этапе нужно проверить все настройки, которые были сделаны. Если все верно нажмите кнопку УСТАНОВИТЬ. Появится окно установки (рис.21).

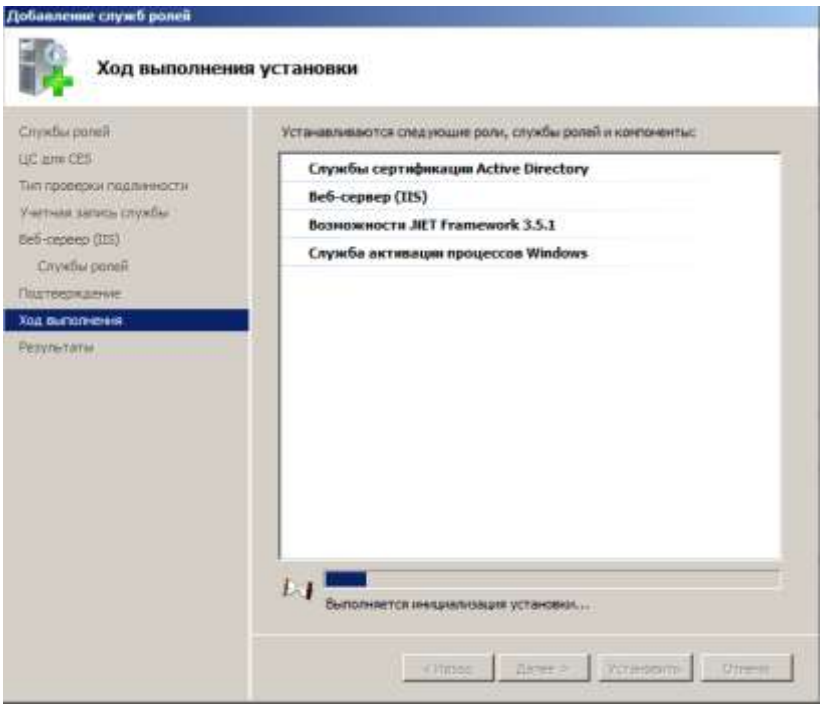


Рис.21. Ход выполнения установки

ПЕРЕЗАГРУЗИТЕ СЕРВЕР (в вашем случае это просто виртуальная машина).

ЛАБОРАТОРНАЯ РАБОТА №3

УСТАНОВКА И НАСТРОЙКА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Цель работы

Целью данной лабораторной является ознакомление с процессом установки и настройки УЦ.

Ход работы

Приступим к получению сертификата для УЦ и веб-сервера.

Вызовем консоль управления Microsoft. Для этого запустим командную строку ПУСК - ВЫПОЛНИТЬ. Далее набрать команду «mmc». Появится окно консоли (рис.1).

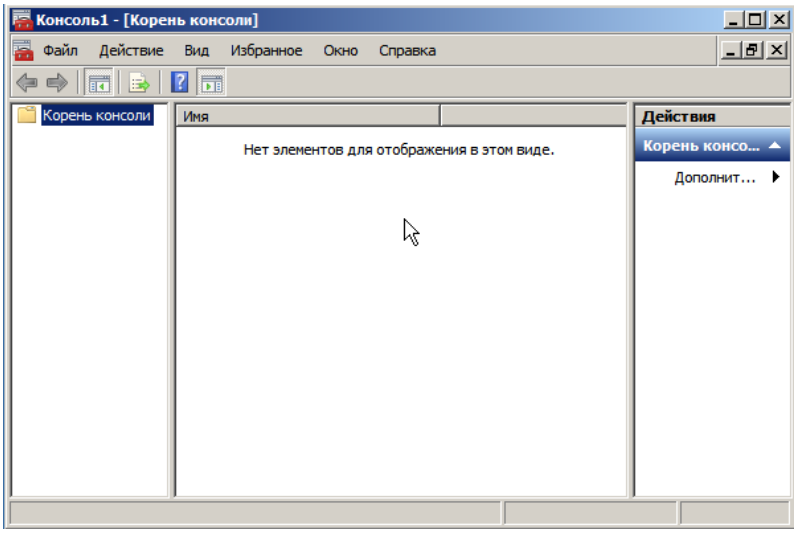


Рис.1 . Консоль управления Microsoft

Далее, для работы с сертификатами в данной консоли нам необходимо добавить соответствующую оснастку. Нажать сочетание клавиш на клавиатуре CNRL+ M. В появившемся окне в левом поле выбрать строку «СЕРТИФИКАТЫ» и нажать кнопку ДОБАВИТЬ (рис. 2).

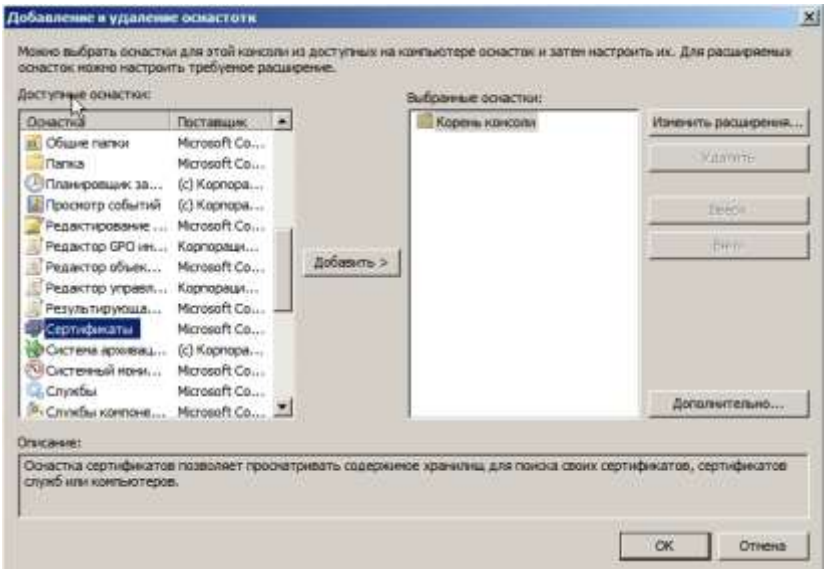


Рис.2. Окно добавления и удаления оснастки

После кнопки ДОБАВИТЬ появится окно как на скриншоте ниже (рис.3). Нужно выбрать строку «учетной записи компьютера». Нажать ДАЛЕЕ.

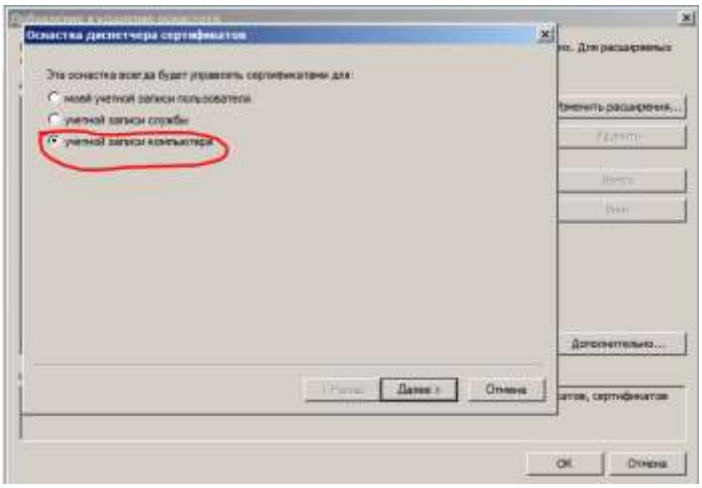


Рис.3 . Вид управляющего оснасткой

На следующем окне выбора компьютера ничего изменять не нужно, все остается по умолчанию. Нажмите ГОТОВО (рис.4).

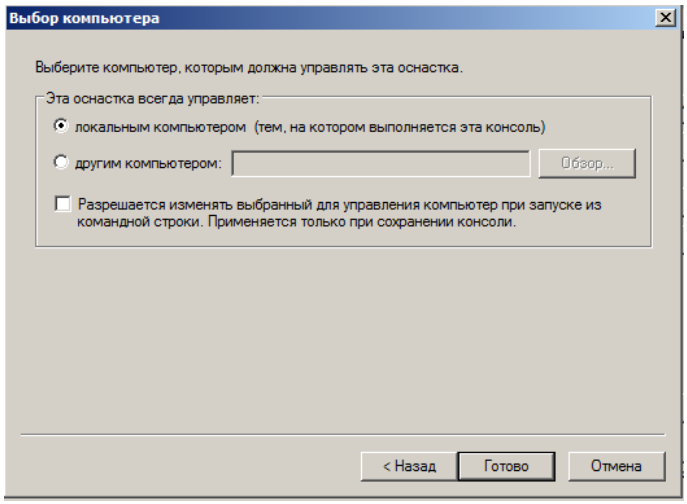


Рис.4. Выбор компьютера

Нажать кнопку ОК. Далее вы перейдете на главное окно консоли (рис.5).

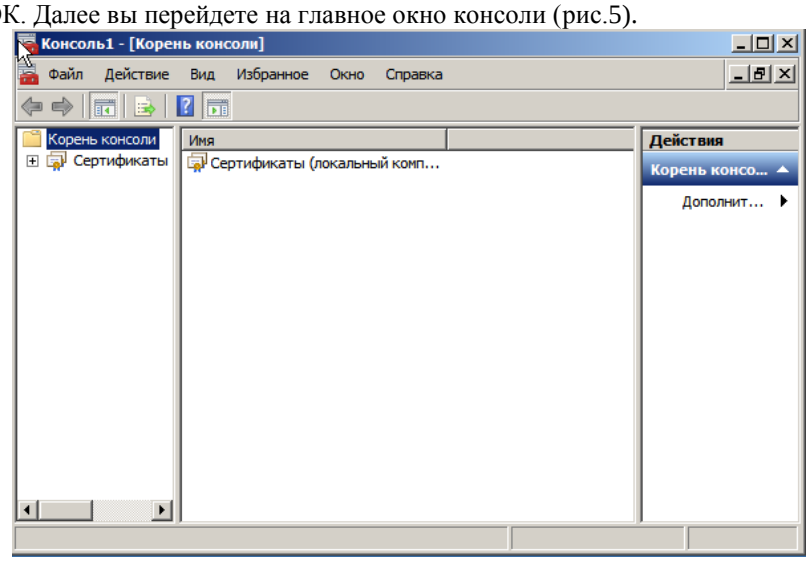


Рис.5 . Окно консоли после добавления новой оснастки

Если нажать в левом окне на вкладку сертификаты то далее в выпадающем списке можно увидеть 11 папок, каждая из которых имеет физическое место хранения на жестком диске и свое имя, характеризующее типы сертификатов, которые она содержит. Нажмите на папке с именем «Личное». Вы можете увидеть в центральном поле сертификат уже существующий сертификат. После активации роли Active Directory Certificate Services ‑ в списке сертификатов уже есть сертификат с коротким именем, совпадающим с именем ЦС (именно тот, в столбце НАЗНАЧЕНИЕ которого указано ПРОВЕРКА ПОДЛИННОСТИ). Но этот сертификат непригоден для доступа к веб-серверу по защищенному каналу, то есть необходимому протоколу HTTPS. Получим сертификат для веб-сервера с новым ключом.

Нажмите правой кнопкой мыши на данной сертификате, далее ВСЕ ЗАДАЧИ – ЗАПРОСИТЬ СЕРТИФИКАТ С НОВЫМ КЛЮЧОМ. Появится окно как на рисунке ниже (рис.6).

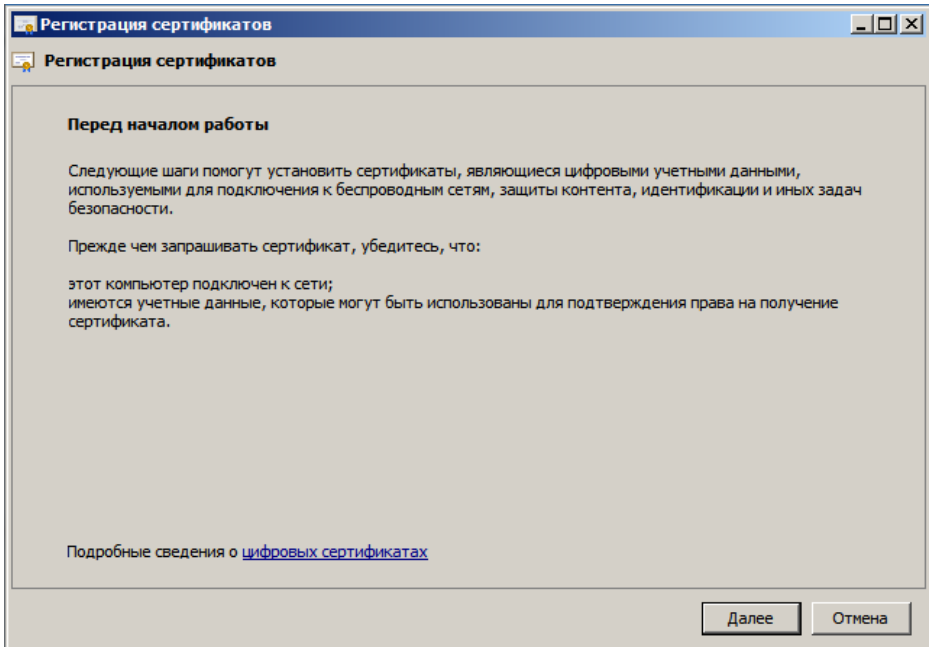


Рис.6 . Помощник по регистрации сертификатов

Ознакомьтесь внимательно с представленной информацией и нажмите ДАЛЕЕ. В следующем окне необходимо выбрать типы сертификатов. Ранее существующий сервер был сделан контроллером домена, поэтому в списке по умолчанию уже доступен сертификат типа контроллера домена. На данном этапе вмешательств от обучаемого не требуется (рис.7). Нажмите ЗАЯВКА.

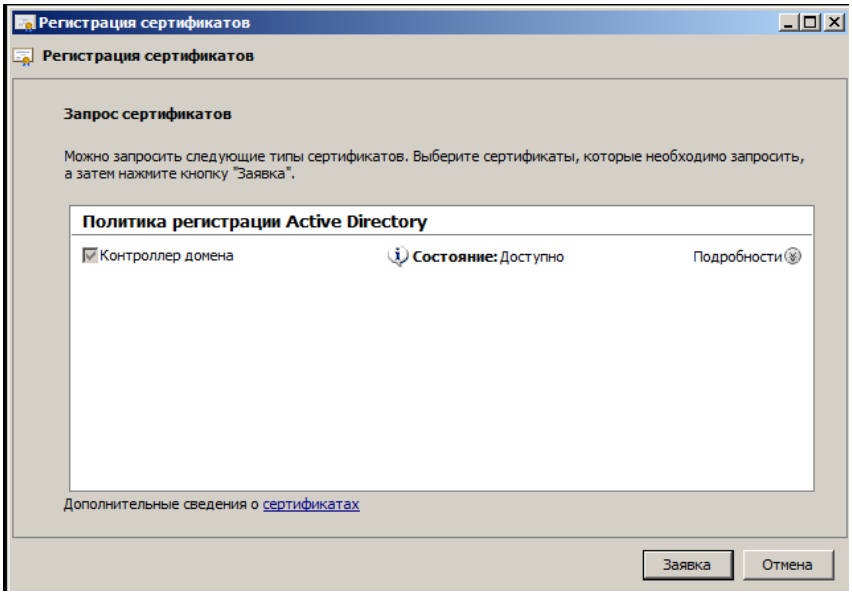


Рис.7. Запрос сертификата

Далее будет выполнена установка сертификата. После успешной установки появится окно. Сравните свой результат с результатом на скриншоте ниже. Если все сходится и не никаких ошибок, нажмите ГОТОВО.

Приступим к связыванию сертификата с веб-сервером. Нажмите ПУСК- ВЫПОЛНИТЬ. Наберите команду «InetMgr». Или (без командной строки) ПУСК – АДМИНИСТРИРОВАНИЕ – ДИСТПЕЧЕР ЗАДАЧ IIS (рис.8). В левом окне нажать название сервера, затем САЙТ- DEFAULT WEB SITE (правой кнопкой мыши) – ИЗМЕНЕНИТЬ ПРИВЯЗОКИ. Далее откроется окно как на скриншоте ниже (рис.9).

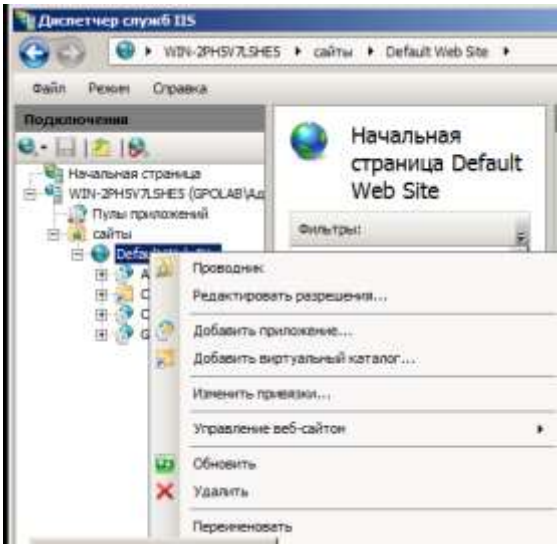


Рис.8 . Диспетчер устройств IIS

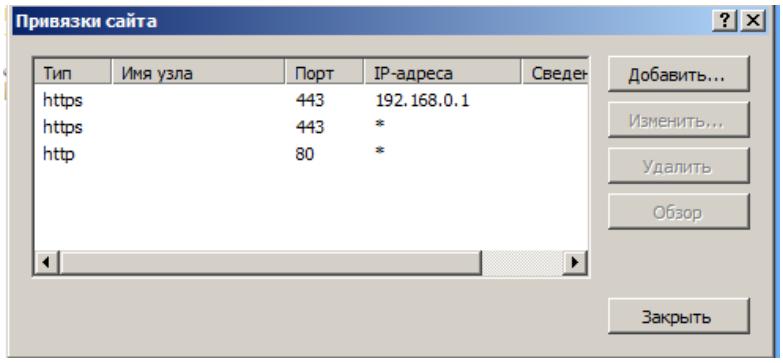


Рис.9 . Привязки сайта

Данным шагом можно задать адрес, по которому с помощью браузера можно просто и беспрепятственно работать уже с веб-оболочкой ЦС. В данной случае задан IP адрес «192.168.0.1» и порт 443 и еще два порта, которые в данной работе не нужны. Выберите первую строку с ip-адресом 192.168.0.1 и портом 443. Нажмите кнопку ИЗМЕНИТЬ. Откроется окно как на скриншоте ниже (рис.10).

Выберите из списка сертификатов SSL - WIN-2PH5V7LSHE5.GPOLAB.COM. Нажмите OK.

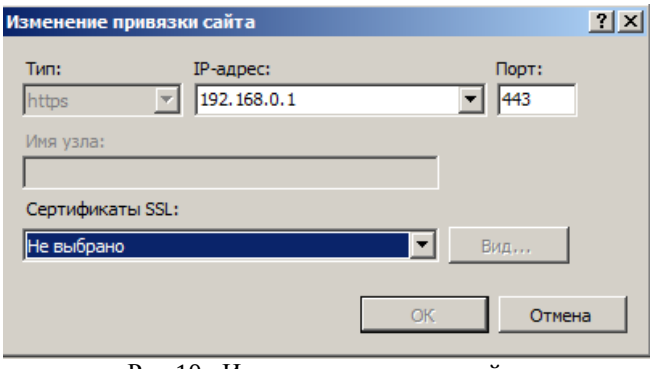


Рис.10 . Изменение привязки сайта

Для проверки работоспособности Центра сертификации запустите браузер Internet Explorer и в строке навигации наберите адрес «https://192.168.0.1/certsrv/»

(рис.12). Либо можно перейти на сайт через обзор веб-сайта диспетчера службы IIS (рис.11).

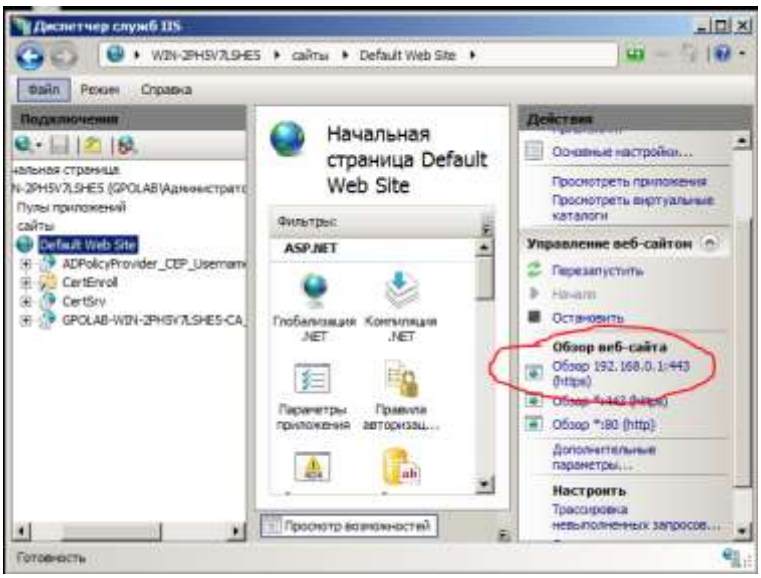


Рис.11 . Обзор веб-сайта

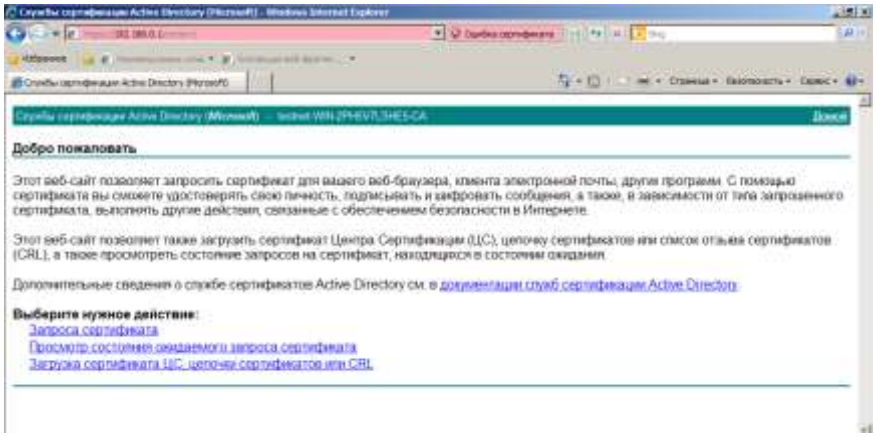


Рис.12 .Проверка работоспособности

Примечание: при переходе на сайт может появится (зависит от настроек браузера) сообщение такого типа как на скриншоте ниже (рис.13).

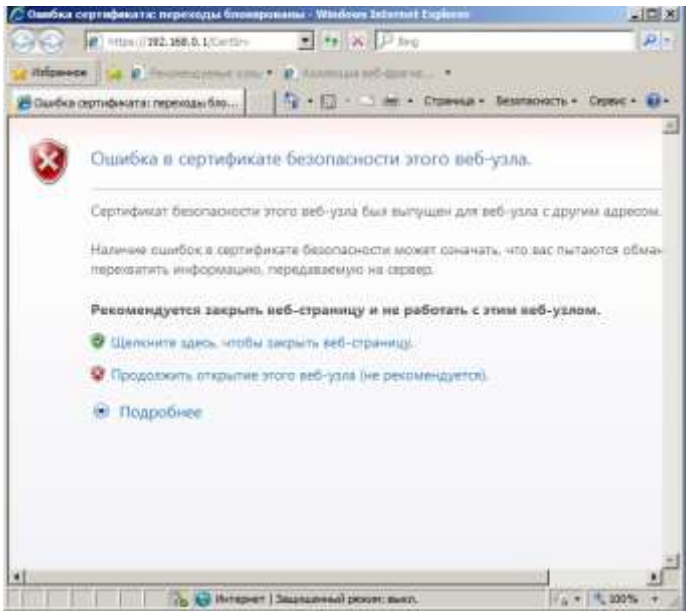


Рис.13 . Ошибка в сертификате безопасности этого веб-узла

Нажмите ПРОДОЛЖИТЬ ОТКРЫТИЕ ЭТОГО ВЕБ-УЗЛА (или иную фразу, зависящую от браузера). Появится окно с вводом имени пользователя и пароля. Введите «Администратор» и текущий пароль от учетной записи администратора. Нажмите ОК.

3. Последняя часть данной лабораторной работе заключается в особенностях выдачи сертификатов с помощью готовой (пункт 1 и 2) веб-оболочки Центра сертификации.

Перед вами главная веб-страница ЦС (рис.14).

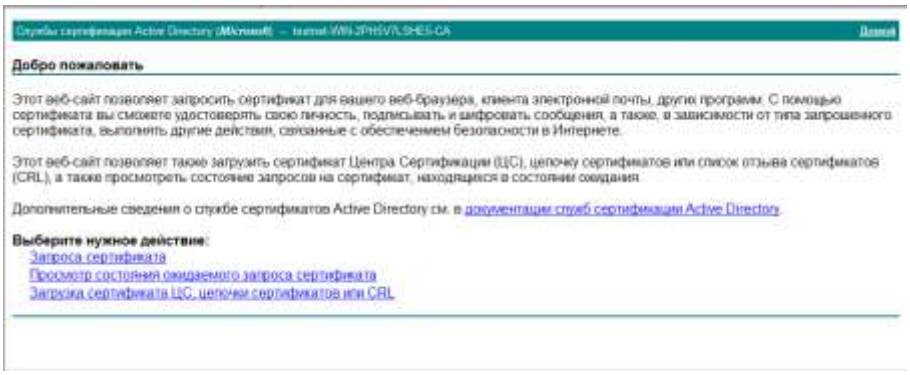


Рис.14 . Главная веб-страница ЦС

Прочитайте внимательно все написано на странице. Также рекомендуется прочитать раздел ДОКУМЕНТАЦИЯ СЛУЖБ СЕРТИФИКАЦИИ AD.

Для того чтобы выдать сертификат данного ЦС необходимо нажать ЗАПРОС СЕРТИФИКАТА. На следующей странице (рис.15) можно выбрать уже готовый сертификат пользователя, либо воспользоваться расширенными настройками запроса сертификата. Разберем второй вариант.

Рис.15 . Страница запроса сертификата

На следующей странице (рис.16) необходимо выбрать тип генерирования сертификата: либо полностью с первого шага создать сертификат, либо по имеющемуся запросу сертификата создать этот сертификат. Для начала, разберем первый вариант. Нажать СОЗДАТЬ И ВЫДАТЬ ЗАПРОС К ЭТОМУ ЦС.

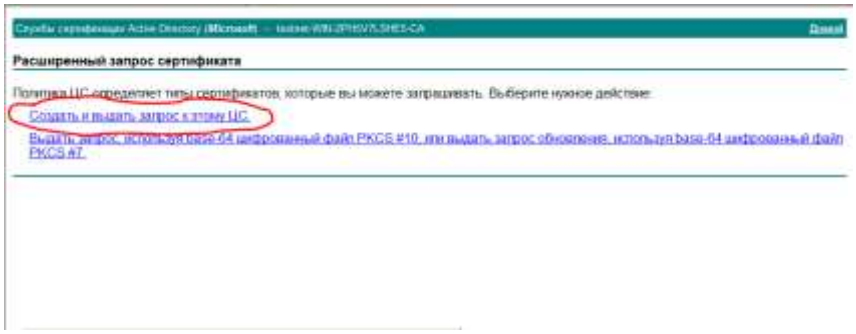


Рис.16 . Расширенный запрос сертификата

На следующей странице (рис.17) появится множество полей, которые необходимо заполнить. Тем самым пополняется информация о запрашиваемом сертификате: его назначение, кем он выдан и т.п. Разберем каждое из полей подробно.

Рис.17. Расширенный запрос сертификата

Первый пункт это ШАБЛОНЫ СЕРТИФИКАТОВ. При создании сертификата можно выбрать его готовый шаблон. В AD доступно всего шесть шаблонов сертификатов. В таблице (таблица 1) представлено описание и возможности каждого из сертификатов.

Таблица 1 . Шаблоны сертификата

Имя	Описание	Использование ключа	Тип субъекта
Пользователь	Используется пользователями для проверки подлинности электронной почты, EFS и клиента.	Подпись и шифрование	Пользователь
Базовое шифрование EFS	Используется шифрованной файловой системой (EFS) для шифрования данных.	Шифрование	Пользователь
Администратор	Разрешает подписывание списка доверия и проверку подлинности пользователя	Подпись и шифрование	Пользователь
Агент восстановления EFS	Позволяет субъекту расшифровать файлы, ранее зашифрованные с помощью EFS.	Шифрование	Пользователь
Веб-сервер	Удостоверяет подлинность веб-сервера.	Подпись и шифрование	Компьютер
Подчиненный центр сертификации	Используется для доказательства подлинности корневого ЦС. Выдается родительским или корневым ЦС.	Подпись	ЦС

Выберите, для упрощенного варианта создания сертификата, ПОЛЬЗОВАТЕЛЬ или МНОЮ СОЗДАННЫЙ СЕРТИФИКАТ, но в последнем варианте необходимо заполнить поля самостоятельно: имя, электронная почта, организация, подразделение, город, область, регион (рис.18).

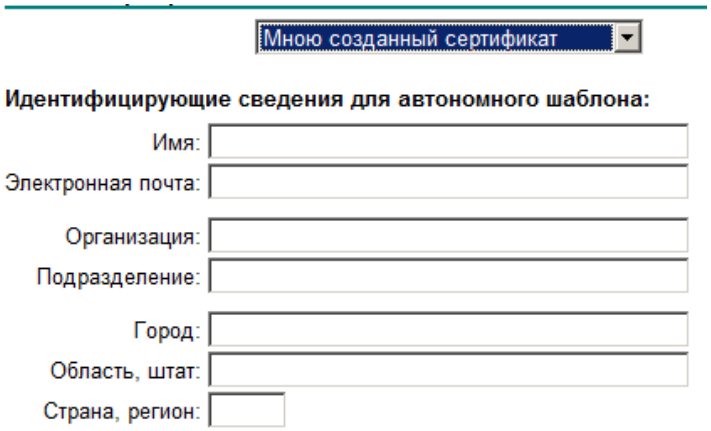


Рис.18 . Идентифицирующие сведения

Далее переходим к следующему пункту это ПАРАМЕТРЫ КЛЮЧА. Для начала необходимо выбрать: создать новый набор ключей или использовать существующие. По плану данной лабораторной работы будем всегда для каждого сертификата создавать свой набор ключей. Выберите пункт СОЗДАТЬ НОВЫЙ НАБОР КЛЮЧЕЙ.

Далее, в пункте (CSP - Cryptography Service Provider - криптопровайдер) по умолчанию выбран «Microsoft RSA SChannel Cryptographic Provider». Поставщик службы шифрования (CSP) отвечает за создание, уничтожение и использование ключей в различных криптографических операциях. Одни поставщики предоставляют криптографические алгоритмы повышенной надежности, другие используют аппаратные компоненты, такие как смарт-карты. Существует несколько версии данного криптопровайдера от компании Microsoft. У каждого свое назначение. Что касается Microsoft RSA SChannel Cryptographic Provider, он

предоставляет функциональность для реализации ЭЦП.

Далее, размер ключ, то по умолчанию установлено 2048 бит. Для улучшения безопасности можно выбрать больший размер, но вместе с тем в геометрической прогрессии будет расти и время генерации ключа. Выберите 2048. Это хорошее соотношение безопасность/время генерации.

Переходим к двум «галочкам»: «Пометить ключ как экспортируемый» и «Включить усиленную защиту закрытого ключа». Что касается первой, Если ключи помечены как экспортируемые, открытый и закрытый ключи можно сохранить в файле PKCS #12. Это может быть полезно при смене компьютера и перенесении пары ключей или при удалении пары ключей и сохранении ее в безопасном месте. Что касается второй, Если усиленная защита закрытого ключа включена, пароль будет запрашиваться при каждом использовании закрытого ключа. Данные пункты не являются ключевыми в выдаче сертификата, поэтому обучаемый сам может выбрать изменять или нет данные пункты.

Теперь переходим к пункту ФОРМАТ ЗАПРОСА. При работе с данным ЦС можно воспользоваться двумя типами форматов запросов: CMC и PKCS#10. Запрос на новый сертификат создается в формате PKCS#10, а запрос на обновление действующего сертификата — в формате CMC (RFC 5272).

Далее, о пункте АЛГОРИТМЫ ХЭШИРОВАНИЯ. Его настройка влияет только на подписание запроса. Хороший алгоритм хэширования не позволяет создать два независимых набора входных данных, имеющих одинаковые хэш-коды. Примерами алгоритмов хеширования являются MD2, MD4, MD5 и SHA-1.

Если требуется отправить запрос позже, можно также выбрать Сохранить запрос. Данный запрос сохранится на вашем жестком диске в виде текстового файла.

В заключении, нажмите кнопку ВЫДАТЬ. Появится страница ожидания (рис.19)

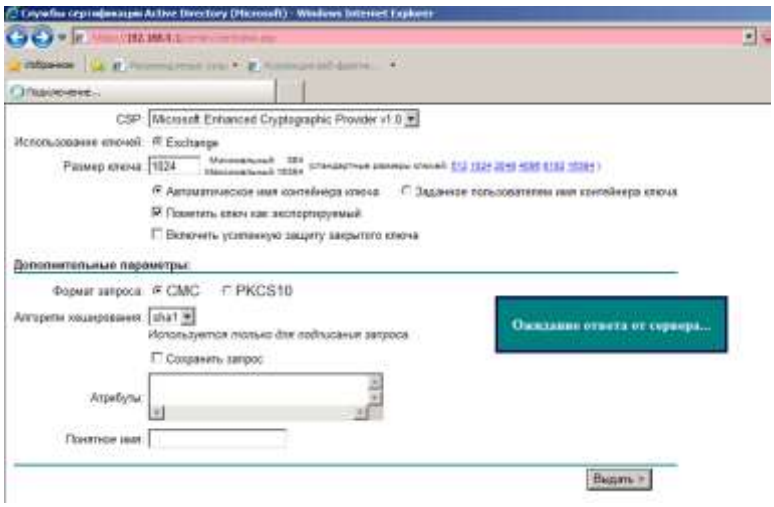


Рис.19 . Ожидание чуда

Если все прошло успешно то появится окно как на скриншоте ниже (рис.20). Нажмите УСТАНОВИТЬ ЭТОТ СЕТРИФИКАТ

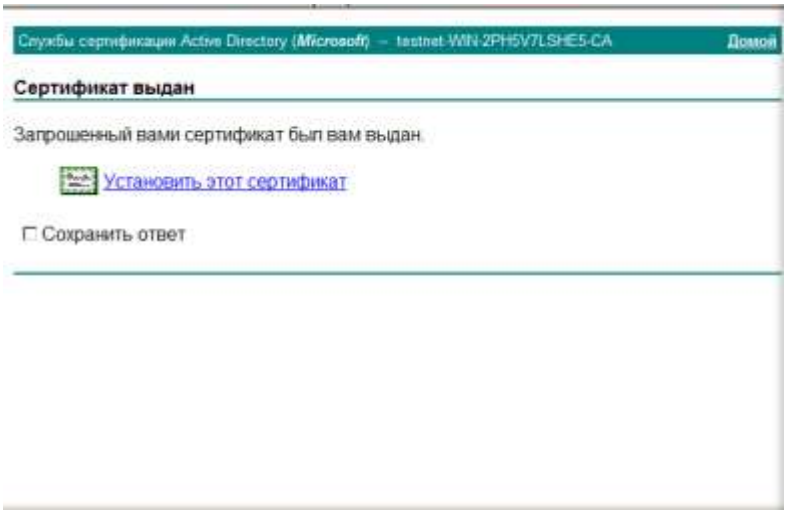


Рис.20 . Сертификат выдан

ЛАБОРАТОРНАЯ РАБОТА №3

УПРАВЛЕНИЕ ШАБЛОНАМИ СЕРТИФИКАТА

Цель работы

Целью данной лабораторной является ознакомление с процессом управления шаблонами сертификата.

Ход работы

Данная лабораторная работа полностью выполняется на виртуальной машине с установленной операционной системой Windows Server 2008 R2.

Для начала запустите виртуальную машина (рисунок 1), имеющую ОС Windows server 2008 R2 (Rus) с установленной службой активных каталогов Active Directory и службой сертификации Active Directory Certificate Services. А также полностью налаженной системой выдачи сертификатов через веб-интерфейс. Полное описание всего вышесказанного с подробной пошаговой инструкцией вы можете найти в предыдущих лабораторных работах 1 и 2.

Рис. 1. Вход в систему

Пароль для входа в систему под пользователем АДМИНИСТРАТОР является «Urbann91». Через некоторый промежуток времени в целях повышения уровня защиты ОС Windows Server 2008 требует менять пароль. Если при входе в систему вас просят ввести новые пароль, то введите старый пароль и новый. Запишите новый пароль, чтобы не забыть.

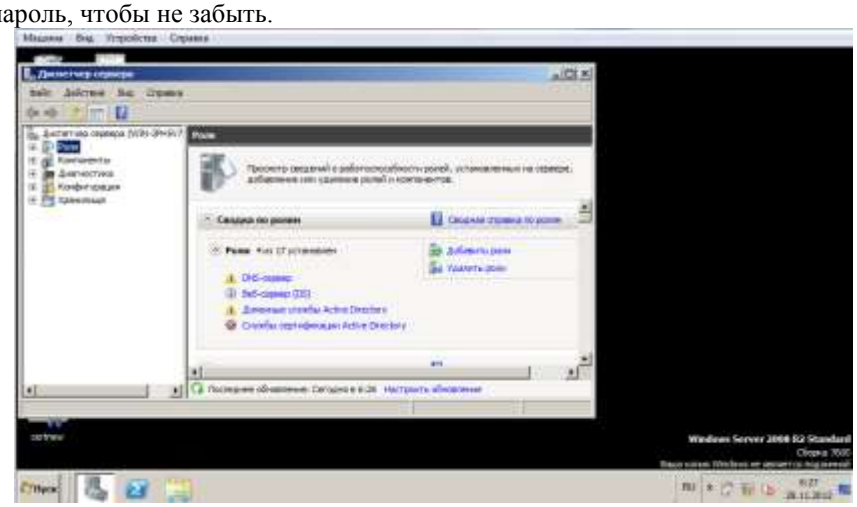


Рис. 2 . Запущенная ОС Windows Server 2008 R2

В лабораторной работе №2 вы ознакомились со стандартными шаблонами сертификата, которые уже встроены в AD.

Данный же лабораторный практикум направлен на углубленную работу с шаблонами сертификата, точнее на получение навыков управления шаблонами сертификата. Понятие «управление шаблонами сертификата» можно разделить на:

- Создание новых шаблонов сертификата;
- Обновление уже существующих шаблонов;
- Настройка шаблонов;
- Удаление шаблонов сертификата.

1. Установка оснастки «Шаблонов сертификата»

Для того чтобы начать работать с шаблонами необходимо открыть оснастку шаблонов сертификатов. Для этого с помощью командной строки запустите консоль управления Windows с помощью команды mmc. (рисунок 3).

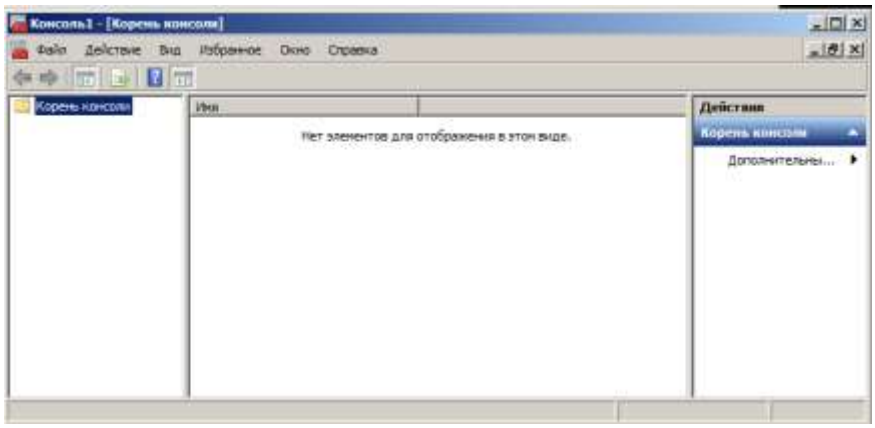


Рис. 3 . Консоль управления Windows

Затем выберите ФАЙЛ – ДОБАВИТЬ ИЛИ УДАЛИТЬ ОСНАСТКУ. В появившемся окне в правой части выбрать строку ШАБЛОНЫ СЕРТИФИКАТА и нажать кнопку ДОБАВИТЬ (рисунок 4).

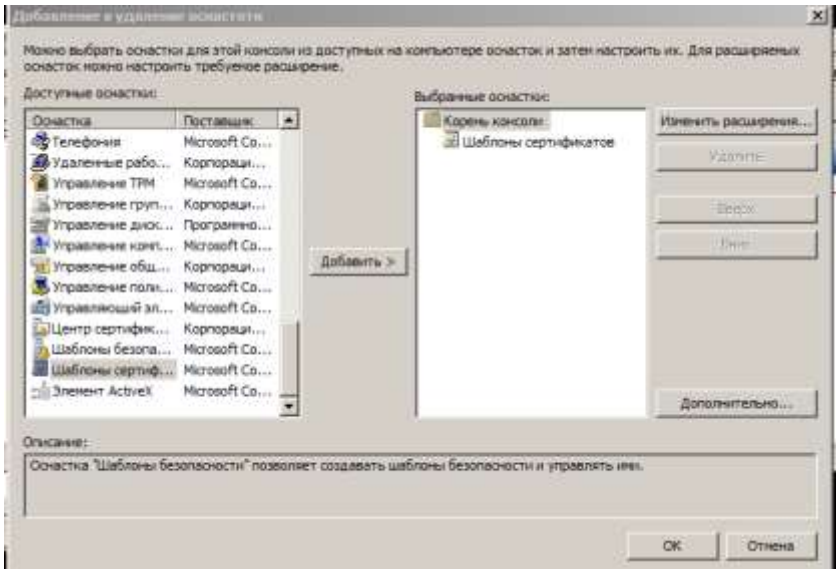
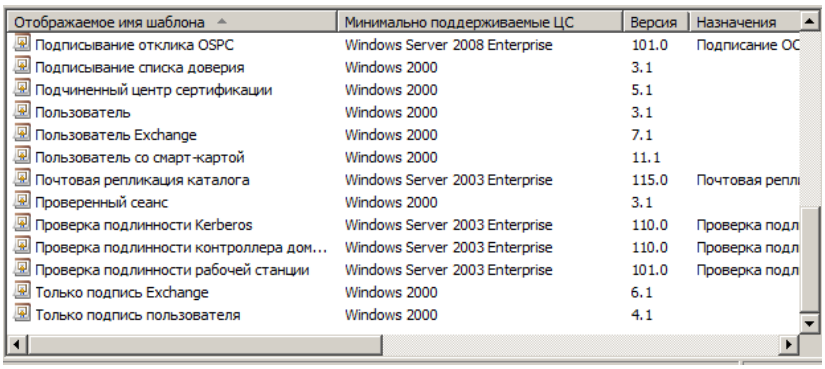


Рис. 4 . Добавление оснастки

Нажмите ОК. Новая оснастка добавлена. Нажмите двойным кликом мыши на Шаблоны сертификата (имя сервера) в поле ИМЯ на главном окне КОНСОЛИ. В этом же поле откроется полный список всевозможным шаблонов; минимальное ОС, которая поддерживает данный шаблон; назначение каждого из шаблонов; версия (рис. 5).



Отображаемое имя шаблона	Минимально поддерживаемые ЦС	Версия	Назначения
Подписывание отклика OSPC	Windows Server 2008 Enterprise	101.0	Подписание ОС
Подписывание списка доверия	Windows 2000	3.1	
Подчиненный центр сертификации	Windows 2000	5.1	
Пользователь	Windows 2000	3.1	
Пользователь Exchange	Windows 2000	7.1	
Пользователь со смарт-картой	Windows 2000	11.1	
Почтовая репликация каталога	Windows Server 2003 Enterprise	115.0	Почтовая репл
Проверенный сеанс	Windows 2000	3.1	
Проверка подлинности Kerberos	Windows Server 2003 Enterprise	110.0	Проверка подл
Проверка подлинности контроллера дом...	Windows Server 2003 Enterprise	110.0	Проверка подл
Проверка подлинности рабочей станции	Windows Server 2003 Enterprise	101.0	Проверка подл
Только подпись Exchange	Windows 2000	6.1	
Только подпись пользователя	Windows 2000	4.1	

Рис. 5 . Полный список шаблонов

В итоге данной лабораторной работы получим новый собственный шаблон.

2. Создание новых шаблонов сертификата

Новый шаблон сертификата можно создать дублированием существующего шаблона с использованием свойств существующего шаблона в качестве значений по умолчанию для нового шаблона. Разные применения и типы ЦС поддерживают разные шаблоны сертификатов. Например, некоторые шаблоны сертификатов могут выдаваться и управляться только ЦС предприятия, работающими под управлением Windows Server 2003, а для некоторых может потребоваться, чтобы ЦС работал под управлением Windows Server 2008.

В поле сертификатов на панели ВХОД СО СМАРТ-КАРТОЙ щелкните правой кнопкой мыши копируемый шаблон сертификата, а затем выберите команду СКОПИРОВАТЬ ШАБЛОН (рисунок 6).

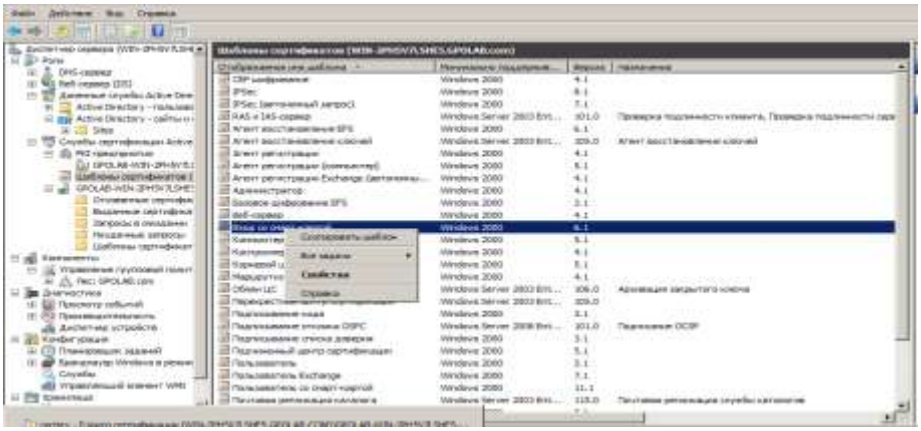


Рис. 6 . Копирование шаблона

Далее, выберите минимальную версию ЦС, которую нужно поддерживать. Поэтому выберите Windows Server 2003 Enterprise (Рис. 7). Нажмите ОК.

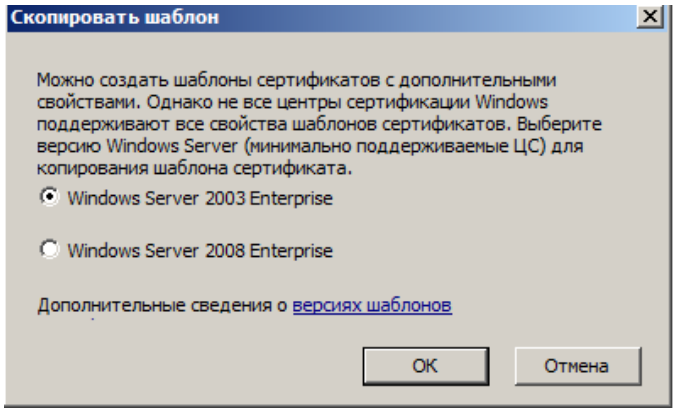


Рис. 7 . Тип ЦС

Далее появится следующее окно (рисунок 8).

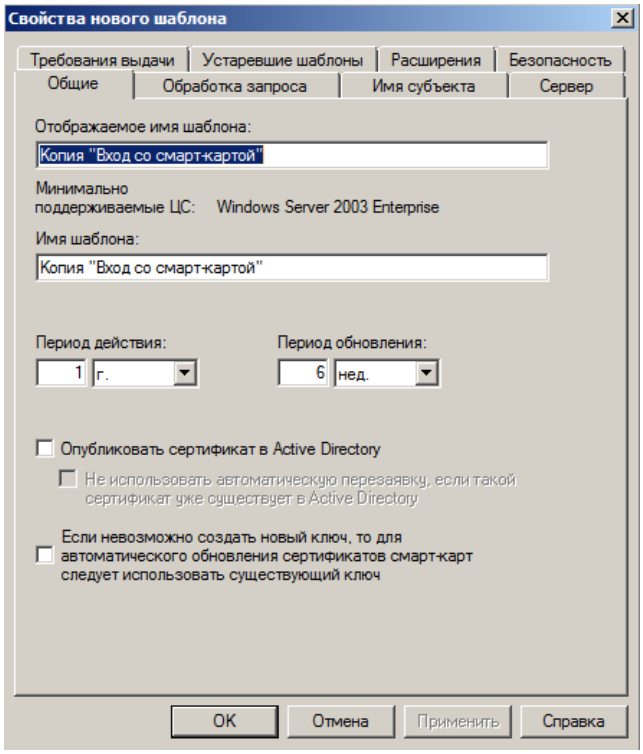


Рис. 8 . Свойства нового шаблона

Теперь переходим к подпункту настройка шаблона сертификата.

3. Настройка шаблона сертификата

Рассмотрим каждую из вкладок по отдельности.

Текущее положение это вкладка ОБЩЕЕ как на рисунке 8. Поле ОТОБРАЖАЕМОЕ ИМЯ вводится имя для шаблона. Можно применить имя, предложенное по умолчанию. Строка ИМЯ ШАБЛОНА будет тоже самое что и ОТОБРАЖАЕМОЕ ИМЯ, только без пробелов.Параметры достоверности по умолчанию и периода обновления для сертификатов, выдаваемых службами сертификатов Active Directory (AD CS), предназначены удовлетворить большинство требований безопасности. Однако для сертификатов, используемых определенными группами пользователей, может потребоваться указать другие параметры достоверности и обновления, такие как более короткие срок действия или периоды обновления. За это два параметра отвечают для поля ПЕРИОД ДЕЙСТВИЯ и ПЕРИОД ОБНОВЛЕНИЯ.Параметр ОПУБЛИКОВАТЬ СЕРТИФИКАТ В ACTIVE DIRECTORY определяет, будут ли сведения о шаблоне сертификата доступными по всему предприятию. Параметр НЕ ИСПОЛЬЗОВАТЬ АВТОМАТИЧЕСКУЮ ПЕРЕЗАЯВКУ, ЕСЛИ ТАКОЙ СЕРТИФИКАТ УЖЕ СУЩЕСТВУЕТ В ACTIVE DIRECTORY. С помощью этого параметра автоматическая подача заявки на сертификат не подаст запрос повторной заявки, если в доменных службах Active Directory (AD DS) существует дубликат сертификата. Это дает возможность обновлять сертификаты, но предотвращает выдачу нескольких дубликатов сертификатов (рис. 9).

Запишем в поле:

ОТОБРАЖАЕМОЕ ИМЯ ШАБЛОНА - GPO2012;

ПЕРИОД ДЕЙСТВИЯ и ПЕРИОД ОБНОВЛЕНИЯ – по-умолчанию;

ОПУБЛИКОВАТЬ СЕРТИФИКАТ В ACTIVE DIRECTORY – отметить.

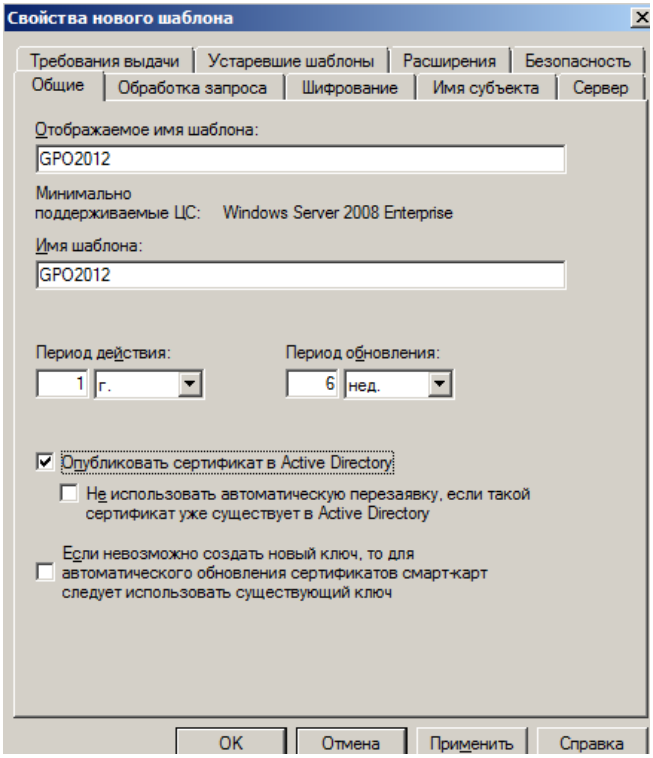


Рис. 9 . Свойство шаблона

Далее перейдите на следующую вкладку ОБРАБОТКА ЗАПРОСА. В строке ЦЕЛЬ указывается назначение сертификата определяет предполагаемое основное использование сертификата и может быть одним из четырех параметров, описанных в следующей таблице.

Таблица 1 . Назначения сертификатов

Параметр	Назначение
Шифрование	Содержит шифровальные ключи для шифрования и дешифрования.
Подпись	Содержит шифровальные ключи только для подписи данных.
Подпись и шифрование	Охватывает все основные применения шифровального ключа сертификата, включая шифрование данных, дешифрование данных, первоначальный вход в систему и цифровое подписывание данных.
Подпись и вход со смарт-картой	Разрешает первоначальный вход в систему с помощью смарт-карты и цифровую подпись данных. Нельзя использовать для шифрования данных.

Параметр ВКЛЮЧИТЬ СИММЕТРИЧНЫЕ АЛГОРИТМЫ, РАЗРЕШЕННЫЕ СУБЪЕКТОМ параметр позволяет администратору выбрать алгоритм стандарта AES для шифрования закрытых ключей, когда они передаются в ЦС для архивации ключа. Если установлен этот параметр, клиент будет использовать симметричное шифрование AES-256 (наряду с сертификатом обмена ЦС для асимметричного шифрования), чтобы отправить закрытый ключ в ЦС для архивации. Если этот параметр не установлен, используется симметричный алгоритм 3DES. Поскольку архивация ключа предназначена для ключей шифрования (а не для ключей подписывания), этот параметр задействован, только если назначение сертификата установлено в **Шифрование.**

Параметр АВТОРИЗАЦИЯ ДОПОЛНИТЕЛЬНЫХ УЧЕТНЫХ ЗАПИСЕЙ СЛУЖБ ДЛЯ ДОСТУПА К ЗАКРЫТОМУ КЛЮЧУ позволяет задать настраиваемый список управления доступом (ACL) к закрытым ключам сертификатов компьютеров на основе любых шаблонов сертификатов компьютера версии 3 за исключением корневого ЦС, подчиненного ЦС и перекрестных шаблонов ЦС. Настраиваемый список управления доступом необходим в случае, если учетная запись службы, которой требуется доступ к закрытому ключу, не включена в разрешения по умолчанию. Разрешения по умолчанию, применяемые к закрытому ключу клиентом регистрации сертификатов Майкрософт и поставщиком хранилища программных ключей, включают разрешение «Полный доступ» для группы «Администраторы» и учетной записи «Local System». Сторонние поставщики могут применять различные разрешения по умолчанию и могут не поддерживать настраиваемые списки управления доступом, заданные с помощью этого параметра. Дополнительные сведения см. в документации поставщика.

Установите значение следующих полей (Рис. 10):

ЦЕЛЬ – Подпись и шифрование;

ВКЛЮЧИТЬ СИММЕТРИЧНЫЕ АЛГОРИТМЫ, РАЗРЕШЕННЫЕ СУБЪЕКТОМ – установить галочку;

АРХИВИРОВАТЬ ЗАКРТЫЙ КЛЮЧ – установить галочку.

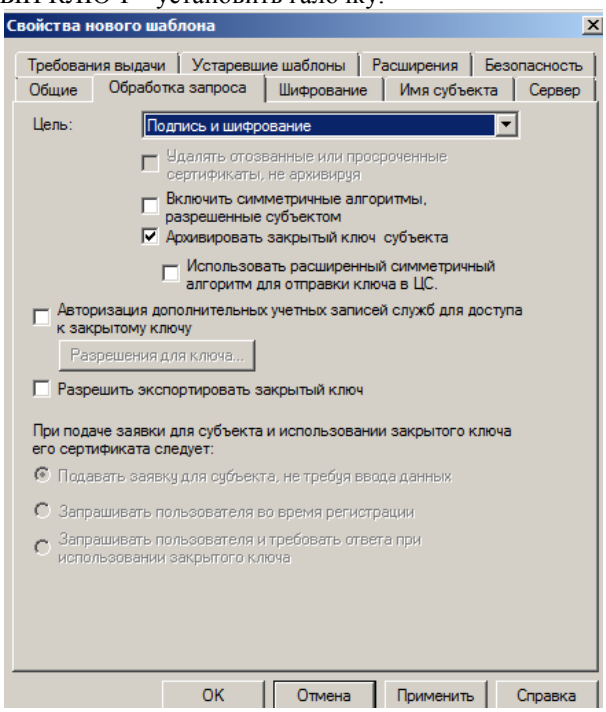


Рис. 10.Обработка запроса

Перейдем на вкладку ШИФРОВАНИЕ (Рис. 11).

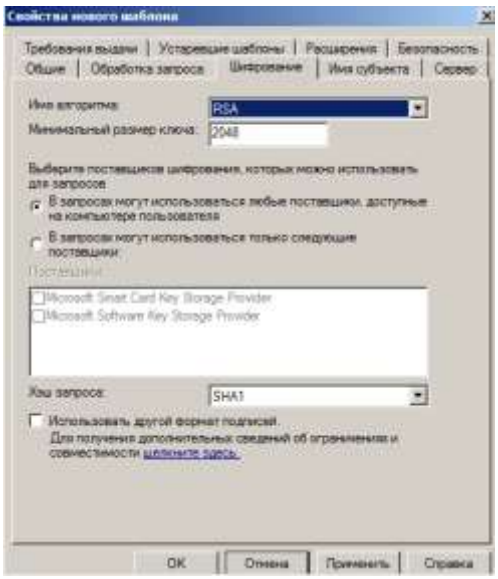


Рис. 11 - Шифрование

В поле МИНИМАЛЬНЫЙ РАЗМЕР КЛЮЧА определите количество символов в ключе, наиболее подходящее для развернутой системы. Большая длина ключа обеспечивает оптимальную безопасность, но может негативно повлиять на производительность сервера. Рекомендуется сохранить значение по умолчанию, равное 2048, или, если это подходит для развернутой системы, уменьшить МИНИМАЛЬНЫЙ РАЗМЕР КЛЮЧА до 1024.

Перейдите на вкладку БЕЗОПАСНОСТЬ (Рис. 12).

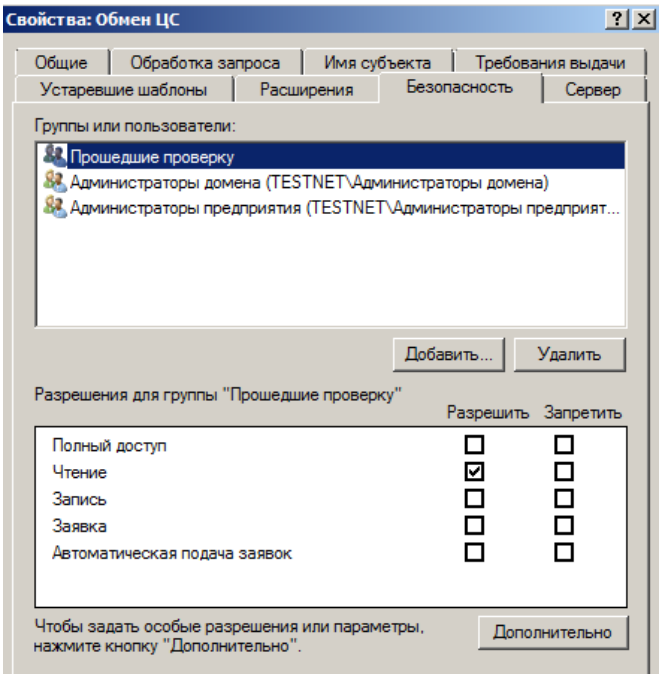


Рис. 12 . Вкладка БЕЗОПАСНОСТЬ

Вкладку РАСШИРЕНИЕ пропустим. Подробнее о работе с этим разделом познакомимся в пункте 3.1 данной лабораторной работы.

Нажмите кнопку ОК. В результате получается собственно созданный новый шаблон сертификата «GPO2012» (рисунок 13).

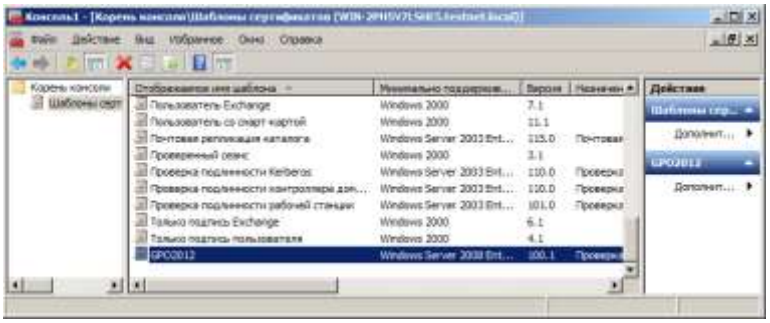


Рис. 13 . Созданный сертификат «GPO2012»

3.1 Изменение политики применения шаблона сертификата

В предыдущих пунктах было описание того как создавать новый шаблон. Но как можно заметить, в столбце НАЗНАЧЕНИЕ оснастки ШАБЛОНОВ СЕРТИФИКАТА (рисунок 13) у созданного шаблона значение исходного шаблона, который был продублирован: «Вход со смарт-картой, проверка подлинности клиента, Проверка подлинности сервера, Проверка подлинности центра распространения ключей». Это все является расширением (или политика применения) шаблона «Проверка подлинности Kerberos».

Политика применения шаблонов строится на основании так называемых объектных идентификаторов или иначе «деревьев - OID»

Объектный идентификатор (OID) — это уникальный набор чисел, разделенных точками. OID имеет уникальное значение, которое связано с объектом и однозначно идентифицирует его в мировом адресном пространстве объектов. Объектные идентификаторы распределяются иерархически. Как правило, рекомендуется назначать объектные идентификаторы политикам сертификатов, разрабатываемым организацией, и включать ссылки на них, а так же ссылки на регламент удостоверяющего центра в сертификаты открытых ключей, издаваемые в соответствии с этими политиками сертификатов. Так же можно назначать OID сертификатам центров сертификации, спискам отозванных сертификатов, регламентам и любым другим объектам, используемым при организации работы удостоверяющего центра.

Следует определить правила построения дерева объектных идентификаторов. Российский корень дерева идентификаторов объектов имеет следующий вид: {iso(1) member-body(2) ru(643)}.

Суффиксы следующего уровня:

{Операторы связи (1)} — регистрирующая организация REG1;

{Производители ПО (2)} — регистрирующая организация REG2;

{Удостоверяющие центры (3)} — регистрирующая организация REG3;

{Банки (4)} — регистрирующая организация REG4;

Соответственно, какая–либо организация, предоставляющая услуги удостоверяющего центра в России, может иметь OID 1.2.643.3.XXX. Зарегистрировавшись, организация получает статус организации–эмитента и может инициировать создание новых объектных идентификаторов. Порядок инициирования нового OID определяется организацией–эмитентом. То есть, организация разрабатывает свой порядок и принципы инициализации объектных идентификаторов. Можно при этом воспользоваться понятиями объектный класс и подкласс. Например, введем объектный класс документ. Уточним его подклассом тип документа. В этом контексте типами документов могут являться политики сертификатов, регламенты и т. п. Теперь мы можем определить конкретный объект — регламент корневого удостоверяющего центра, принадлежащий классу документов и подклассу регламентов.

Существует такой ресурс http://oid-info.com (рисунок 14), располагающий достаточной обширной базой данных существующих объектных идентификаторов. Также позволяющий самостоятельно сформировать свой OID.

Объектные идентификаторы OID шаблонов, уже по умолчанию хранящихся в УЦ, можно посмотреть. Для этого в консоли нажать правой клавишей на оснастке ШАБЛОНЫ СЕРТИФИКАТА (рис. 15) и выбрать ПРОСМОТР ИДЕНТИФИКАТОРОВ ОБЪЕКТОВ. Появится новое окно, содержащие три поля ИМЯ ПОЛИТИКИ, ИДЕНТИФИКАТОР ОБЪЕКТОВ, ТИП ПОЛИТИКИ (рисунок 16). Проанализируете несколько идентификаторов.

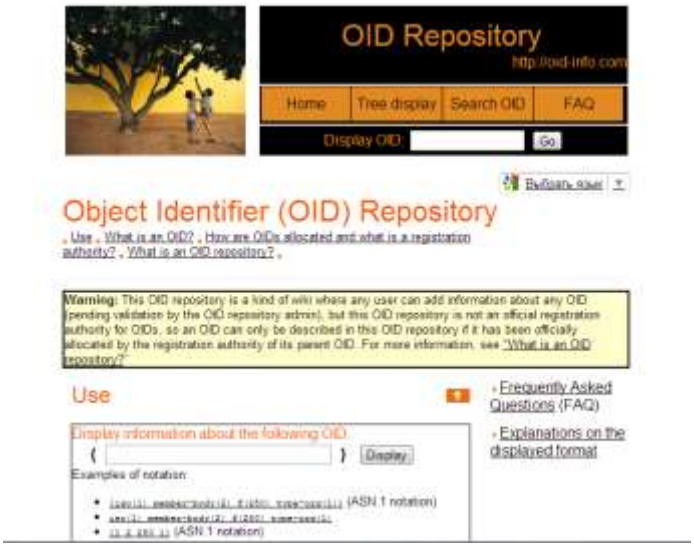


Рис. 14 . Ресурс http://oid-info.com

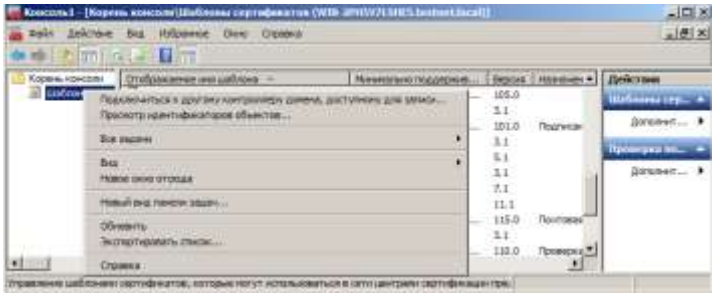


Рис. 15. Консоль

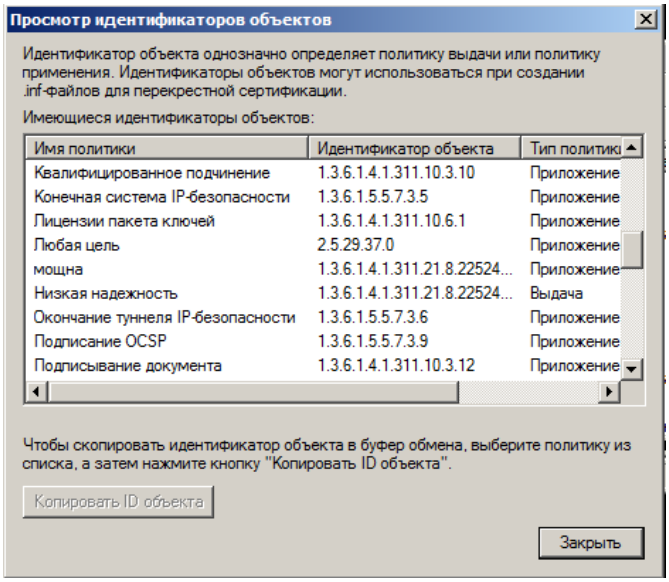


Рис. 16. Просмотр идентификаторов объектов

Теперь для нами созданного шаблона пропишем свой OID. Для этого перейдите на окно оснастки ШАБЛОНЫ СЕРТИФИКАТА, нажмите правой кнопкой на шаблоне «GPO2012» и выберите СВОЙСТВА. Далее выберите вкладку РАШИРЕНИЕ (рисунок 17).

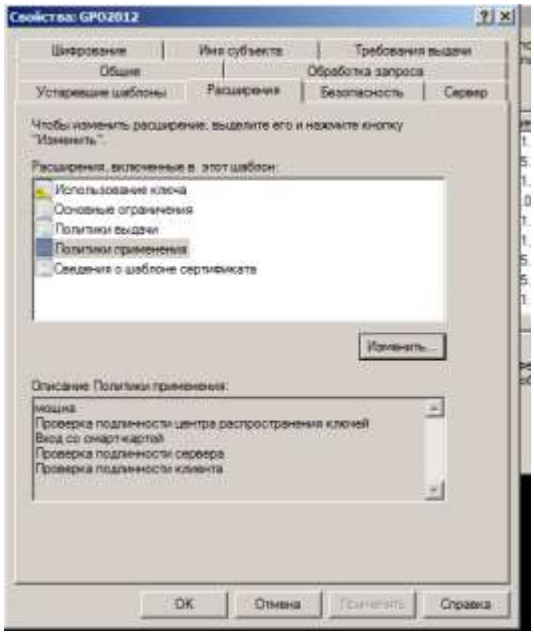


Рис. 17. Свойства шаблона

Затем выберите расширение ПОЛИТИКИ ПРИМЕНЕНИЯ и нажмите кнопку ИЗМЕНИТЬ. В новом окне удалите все существующие политики (рисунок 18)

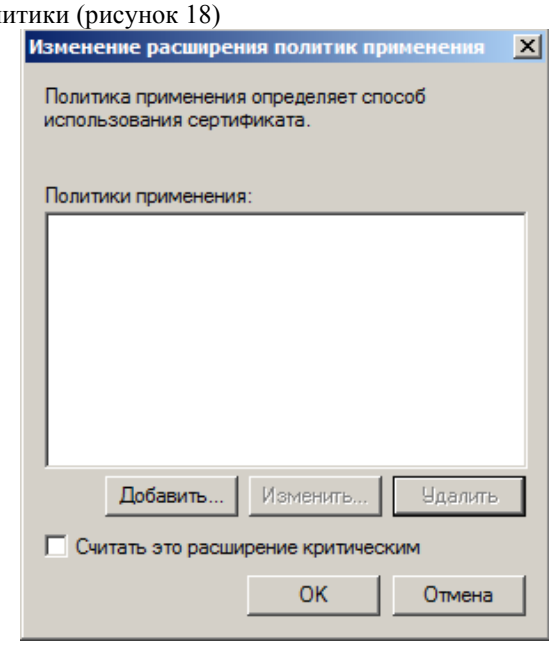


Рис. 18 . Удаленные политики

Следующим шагом добавим уже новый объектный идентификатор. Для этого нажмите кнопку ДОБАВИТЬ. В появившемся окне можно выбрать уже готовую политику, но для наглядности создайте свою собственную. Нажмите СОЗДАТЬ (рис.19).

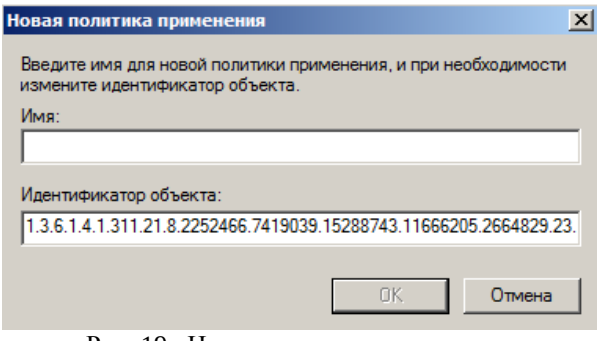


Рис. 19 . Новая политика применения

Воспользуемся идентификатором OID компании «КРИПТО-ПРО» для подписи ЦП 1.2.643.2.2.32. Очистите поле ИДЕНТИФИКАТОР ОБЪЕКТА и запишите туда это OID. В поле ИМЯ запиши «ключи ЭЦП» (рисунок 20).

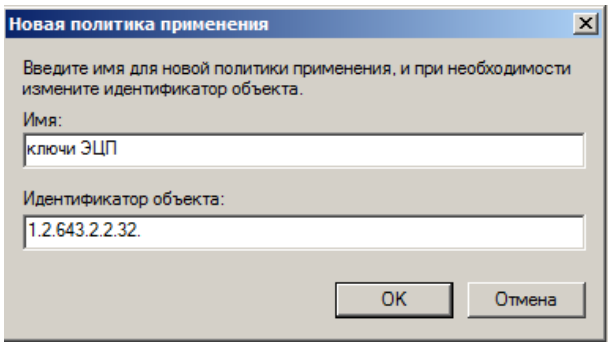


Рис. 20 . Новая политика

Нажмите ОК.

4. Добавление созданного шаблона в Веб-интерфейс УЦ

Для добавления нами созданного шаблона в Веб-интерфейс УЦ необходимо в консоли (ВЫПОЛНИТЬ – «ммс») добавить оснастку ЦЕНТР СЕРТИФИКАЦИИ (рисунок 21) по такому же принципу как добавлялась оснастка ШАБЛОНЫ СЕРТИФИКАТА ранее в данной лабораторной работе.

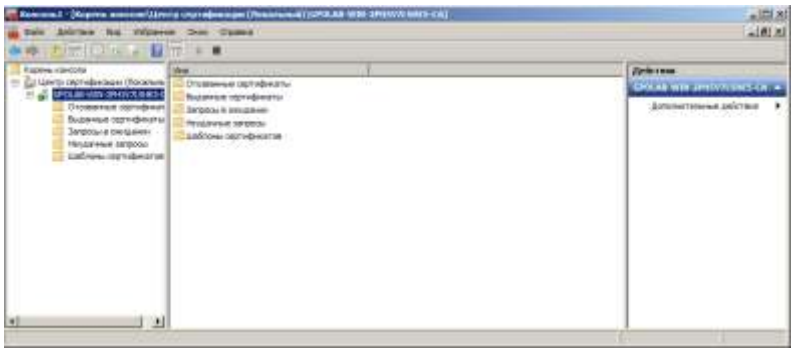


Рис. 21. Консоль Windows

Затем нажмите правой кнопкой на подразделе ШАБЛОНЫ СЕРТИФИКАТОВ – СОЗАДАТЬ-ВЫДАВАЕМЫЙ ШАБЛОН СЕРТИФИКАТА. И выберите созданный шаблон «GPO2012». Нажмите ОК. Теперь при работе с сертификатами через Веб-интерфейс можно выбрать созданный вами шаблон с уже прописанными объектным идентификатором.