МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
БУРЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

С.Г. Цыдыпов

Администрирование локально-вычислительных сетей под управлением MS Windows Server

Рекомендовано УМС БГУ в качестве учебного пособия для обучающихся по направлению подготовки 09.03.03 Прикладная информатика

Улан-Удэ
Издательство Бурятского госуниверситета
2019

УДК 004.451.9
ББК 32.972

Утверждено к печати
редакционно-издательским советом
Бурятского государственного университета

Рецензенты
С.В. Архипов
Директор ЦИТ и ДО доктор технических наук,
старший преподаватель кафедры информационных технологий
Бурятского государственного университета имени Доржи Банзарова
Р.Е. Патласов
Руководитель отдела информационных технологий ООО «Мегатехника»

Цыдыпов С.Г.
Администрирование локально-вычислительных сетей под управлением MS Windows Server: учебное пособие. — Улан-Удэ: Изд-во Бурятского госуниверситета, 2019. — 82 с.
ISBN

Пособие предназначено для обучающихся по направлению подготовки 09.03.03 "Прикладная информатика" в рамках дисциплины «Администрирование информационных систем»

ПРЕДИСЛОВИЕ

Настоящее учебное издание представляет собой учебное пособие для дисциплины «Администрирование информационных систем» в рамках реализации образовательной программы высшего образования по направлению подготовки 09.03.03 «Прикладная информатика» очной формы обучения и подготовлено в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования.

Дисциплина «Администрирование информационных систем» относится к обязательным дисциплинам базовой части Блока 1. Изучение дисциплины направлено на формирование общекультурных/ общепрофессиональных/ профессиональных компетенций:

ПК-1 (способность проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе)

В результате освоения дисциплины обучающийся должен:

Знать:

принципы построения компьютерных сетей; типовой круг задач, решаемых при настройке сетевого оборудования; типовой круг задач, решаемых при установке, настройке и использовании операционных систем;

Уметь:

Эффективно проектировать политику безопасности компьютерной сети, настраивать серверные операционные системы, использовать аппаратные и программные средства компьютера при решении практических задач

Владеть:

современными технологиями проектирования и реализации политики безопасности компьютерной сети

Основной задачей настоящего учебного пособия является изучение основ администрирования локально-вычислительных сетей на платформе MS Windows Server. В пособии подробно расписаны все этапы развертывания виртуальных машин и их конфигурирования для выполнения лабораторных заданий по предмету администрирование информационных систем.

Пособие состоит из предисловия, введения, 13 разделов, списка литературы и источников.

ВВЕДЕНИЕ

В данном учебном пособии рассматриваются возможности развертывания сервера на примере MS Windows Server 2008. Данная версия операционной системы была выбрана в виду меньших требований к объему оперативной памяти (512 Мб) и свободному дисковому пространству. Десктопная версия, к примеру, MS Windows Server 2016 требует наличия 2 Gb оперативной памяти, что в условиях развертывания в виртуальной среде может привести к нехватке памяти. В качестве основной задачи мы будем ставить овладение необходимыми базовыми навыками администрирования локально-вычислительной сети под управлением MS Windows Server.

Для реализации виртуальной среды будет использоваться бесплатным программным обеспечением Oracle VirtualBox. Последнюю версию можно скачать с сайта разработчика: https://www.virtualbox.org/wiki/Downloads

В этом учебном пособии показана модель построения локально-вычислительной сети с использованием доменной архитектуры под управлением одного сервера, который выполняет следующие функции:

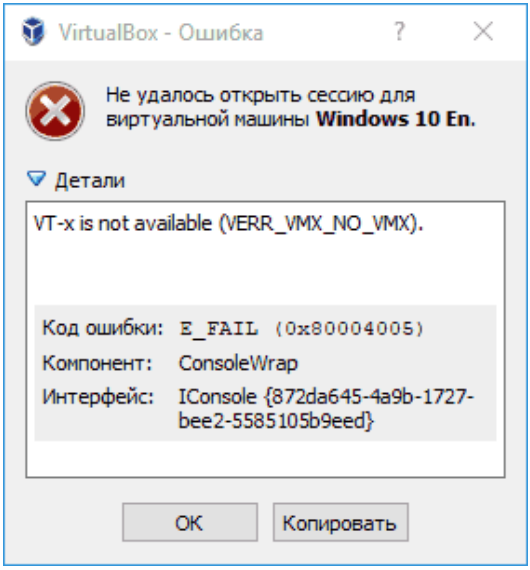
1. Контроллер домена
2. DNS сервер
3. DHCP сервер
4. Файловый сервер

Так же разобраны вопросы создания, настройки групповых политик на уровне домена и предоставления управляемого общего доступа в сеть интернет.

УСТАНОВКА И ЗНАКОМСТВО СО СРЕДОЙ VIRTUALBOX

Виртуальные машины представляют собой эмуляцию устройств на другом устройстве или, в контексте этого учебного пособия и упрощенно, позволяют запускать виртуальный компьютер (как обычную программу) с нужной операционной системой на вашем компьютере с той же или отличающейся ОС. Например, имея на своем компьютере Windows, вы можете запустить Linux или другую версию Windows в виртуальной машине и работать с ними как с обычным компьютером.

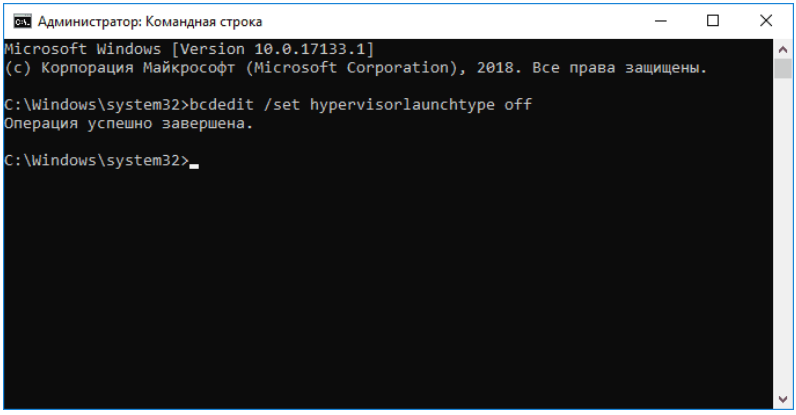
Здесь мы рассматриваем программную среду VirtualBox, которая является полностью бесплатной для работы с виртуальными машинами в Windows, MacOS и Linux. Здесь необходимо заметить, что в Windows 10 Pro и Enterprise есть встроенные средства для работы с виртуальными машинами. Если на компьютере установлены компоненты Hyper-V, то VirtualBox будет сообщать об ошибке «Не удалось открыть сессию для виртуальной машины».



Решить это можно, удалив компоненты Hyper-V в Windows (панель управления — программы и компоненты — установка и удаление компонентов). В случае, если виртуальные машины Hyper-V вам нужны, это может быть неудобно. Привожу инструкцию о том, как использовать на одном компьютере VirtualBox и Hyper-V с меньшими затратами времени:

Для того, чтобы иметь возможность запускать виртуальные машины VirtualBox и основанные на них эмуляторы Android при установленных компонентах Hyper-V, требуется выключить запуск гипервизора Hyper-V.

1. Запустите командную строку от имени администратора и введите следующую команду: *bcdedit /set hypervisorlaunchtype off*

2. 

3. После выполнения команды, перезагрузите компьютер.

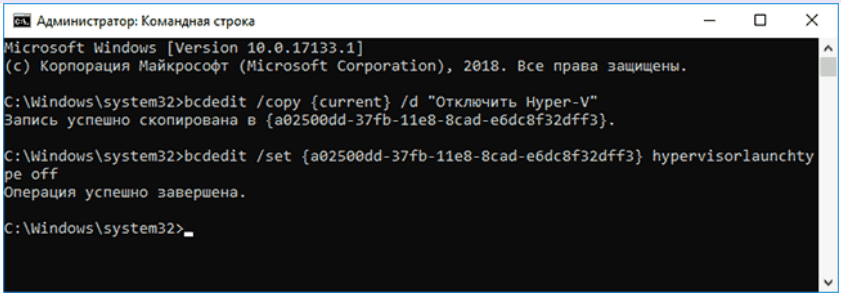
Теперь VirtualBox будет запускаться без ошибки «Не удалось открыть сессию для виртуальной машины» (однако Hyper-V запускаться не будет).

Чтобы вернуть всё в исходное состояние, используйте команду *bcdedit /set hypervisorlaunchtype auto* с последующей перезагрузкой компьютера.

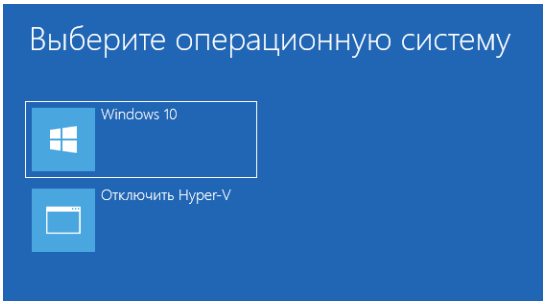
Этот способ можно модифицировать, добавив в меню загрузки Windows два пункта: один с включенным Hyper-V, другой — с отключенным. Путь примерно следующий (в командной строке от имени администратора):

1. bcdedit /copy {current} /d "Отключить Hyper-V"
2. Будет создан новый пункт меню загрузки Windows, также в командной строке отобразится GUID этого пункта.
3. Введите команду

bcdedit /set {отобразившийся GUID} hypervisorlaunchtype off



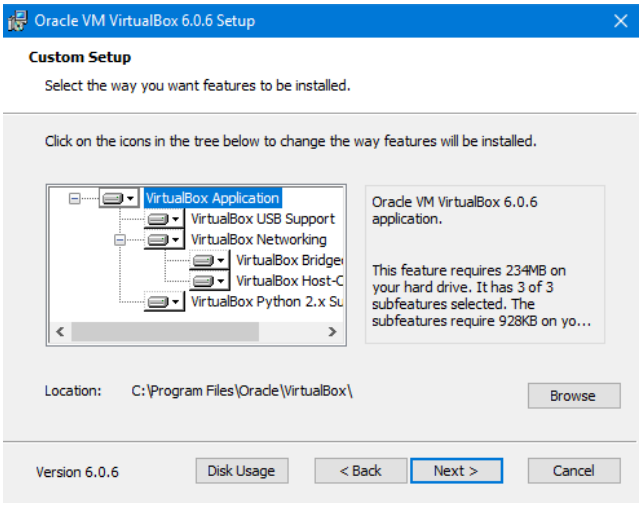
В результате, после перезагрузки Windows 10 или 8 (8.1) вы увидите два пункта меню загрузки ОС: загрузившись в один из них, получите рабочие ВМ Hyper-V, в другой — VirtualBox (в остальном это будет одна и та же система).



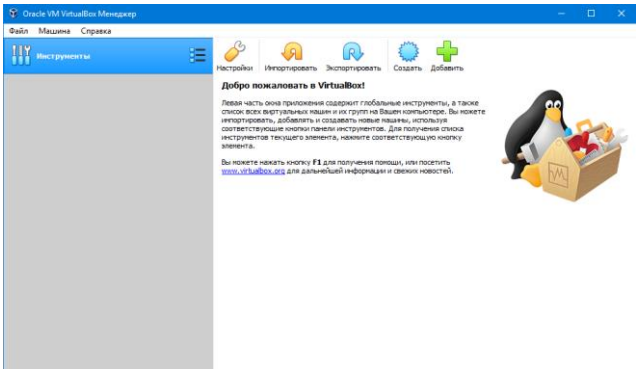
Как итог, добиться работы, пусть и не одновременной, двух виртуальных машин на одном компьютере возможно.

Для чего нужны виртуальные машины? Чаще всего, виртуальные машины используют для запуска серверов или для тестирования работы программ в различных ОС. Для начинающего пользователя такая возможность может быть полезна как для того, чтобы попробовать в работе незнакомую систему или, например, для запуска сомнительных программ без опасности получить вирусы на своем компьютере.

Где скачать VirtualBox? Вы можете бесплатно скачать ПО для работы с виртуальными машинами VirtualBox с официального сайта https://www.virtualbox.org/wiki/Downloads где представлены версии для Windows, Mac OS X и Linux. Несмотря на то, что сайт на английском, сама программа будет на русском языке. Запустите загруженный файл и пройдите простой процесс установки (в большинстве случаев достаточно оставить все параметры по умолчанию).

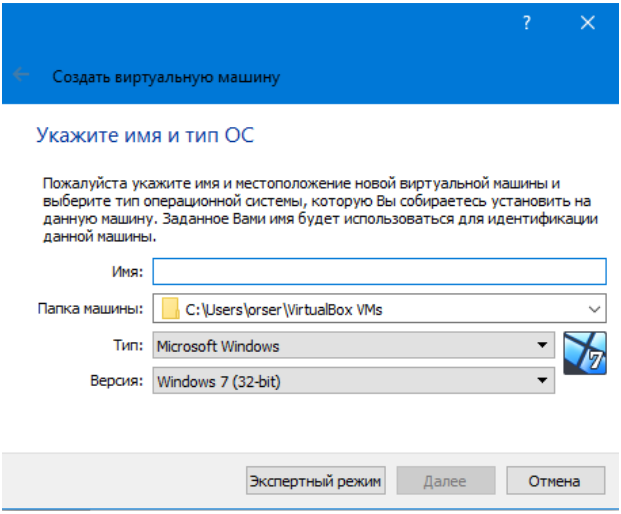


Рабочее окно программы при первом запуске:



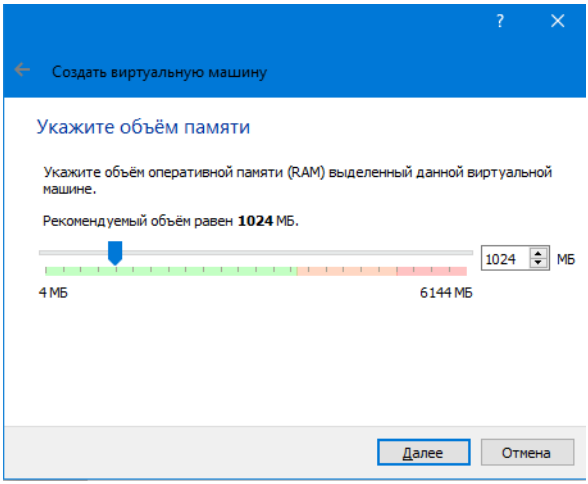
Создание новой виртуальной машины:

Нажимаем кнопку «Создать» и тем самым запускаем мастер создания новой виртуальной машины:

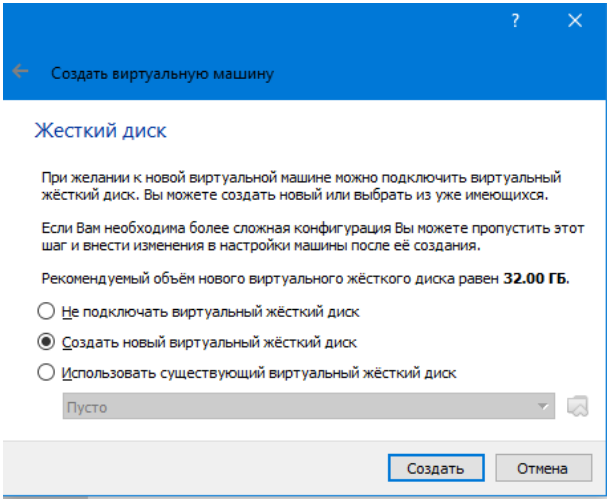


Указываем имя машины, путь, где будет храниться машина, тип и версию операционной системы (которую мы будем в итоге устанавливать на виртуальную машину).

В следующем окне нам будет необходимо установить объем оперативной памяти, выделяемой для виртуальной машины. В идеале – достаточный, чтобы виртуальная машина работала без торможений, но не слишком большой – необходимо помнить, что выделяемая оперативная память «отнимается» от основной системы в момент запуска виртуальной машины.



В этом окне мы выберем необходимый объем оперативной памяти (512 Мб) и переходим к следующему окну.

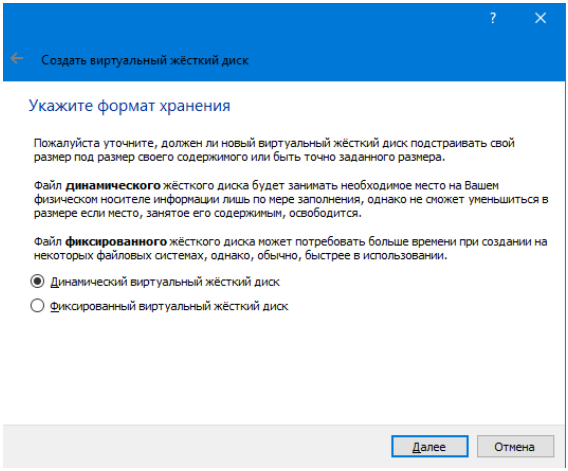


Здесь мы можем подключить к нашей машине виртуальный жесткий диск. Если он у вас уже есть, то выбирайте «использовать существующий виртуальный жесткий диск» с указанием пути, где он находится. Обычно эта схема используется, если необходимо

создать новую виртуальную машину, используя заранее подготовленный жесткий диск. Например, там уже установлена операционная система.

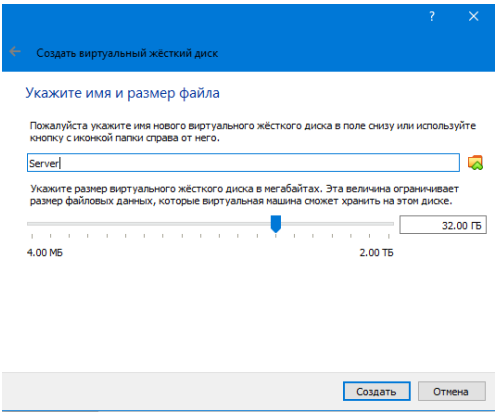
В большинстве случаев выбирается опция «Создать новый виртуальный жесткий диск».

В следующем окне необходимо выбрать тип виртуального жесткого диска. Выбираем **VDI** (VirtualBox Disk Image), так как не планируем использовать виртуальную машину вне среды VirtualBox.



Здесь необходимо выбрать формат хранения. Если ваша виртуальная машина планируется эксплуатироваться в течение достаточно долгого периода, то логично выбрать фиксированный размер.

Для учебных целей достаточно выбрать динамический – можно сэкономить на занимаемом дисковом пространстве. В этом случае образ виртуального жесткого диска будет занимать на физическом носителе ровно столько места, сколько будет занято файлами.



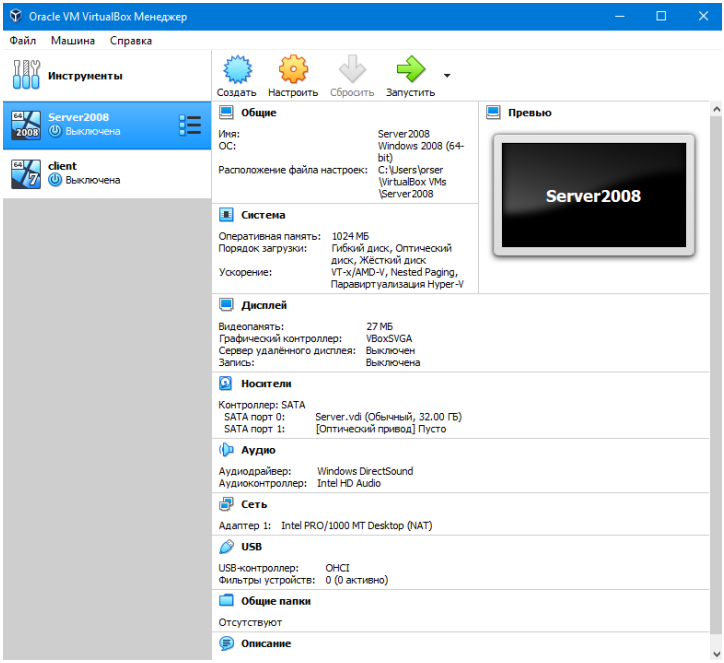
Здесь необходимо указать имя компьютера и размер виртуального жесткого диска. Это финальный этап настройки и после нажатия кнопки «Создать» виртуальная машина будет создана.

Согласно приведенного алгоритма необходимо создать две виртуальные машины: на одной будет развернута операционная система Windows Server 2008, вторая будет работать в составе домена как рядовая рабочая станция.

Настройку и конфигурирование операционных систем мы будем проводить в изолированной среде, не связанной никак с внешним миром, поэтому тяжеловесные антивирусные продукты использовать не будем. За счет этого можно существенно сэкономить на объеме планируемой оперативной памяти для виртуальных машин – и на сервер и на клиент будет достаточно по 512 Мб ОЗУ.

Эти параметры также можно изменить в дальнейшем. Для изменения объема оперативной памяти, выделенной на конкретную виртуальную машину, необходимо зайти в настройки этой машины в раздел «система». Для того, чтобы изменить данный параметр, виртуальная машина, с которой необходимо произвести действия, в этот момент должна быть выключена.

На следующем скриншоте представлено главное окно VM VirtualBox. В левом столбце можно наблюдать список виртуальных машин, созданных в этой программе:



Здесь видно, что мы создали две виртуальные машины. Вторую можно создать абсолютно аналогично, просто повторив тот же алгоритм действий, как и при создании первой машины.

НАСТРОЙКА СЕТИ В VIRTUALBOX

Виртуальные машины VirtualBox очень часто используются для тестирования различного программного обеспечения и его взаимодействия между собой. Обычно, таким программам необходим доступ к интернету. Время от времени возникает необходимость протестировать работу программ по сети или даже создать небольшую тестовую лабораторию из виртуальных машин.

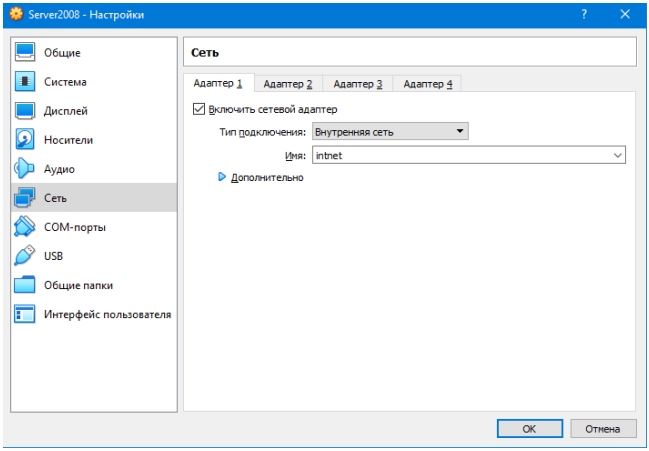
Существует несколько способов как настроить сеть в virtualbox, и каждый из них подходит для лучше для решения одной задачи и меньше для другой. Рассмотрим основные:

- **NAT** - этот способ используется по умолчанию. Для каждой машины создается отдельная внутренняя локальная сеть, в которой машина получает ip 10.10.0.1. Машина может связаться с интернетом, используя технологию NAT, и вы можете обратиться к машине, используя проброс портов VirtualBox, но если у вас будет две виртуальные машины, то вы уже не сможете между ними так взаимодействовать. И если из основной системы к гостевой можно обратиться, то к основной ни гостевой уже никак не получится;
- **Виртуальный адаптер хоста** - создается виртуальный сетевой адаптер, к которому можно подключить несколько виртуальных машин, тем самым объединив их в локальную сеть. Доступа к интернету нет, но зато машины находятся в одной сети и каждая имеет свой ip адрес, теперь они могут взаимодействовать между собой. Основная система тоже доступна по ip 192.168.56.1. Машины доступны не только между собой, но и из основной системы;
- **Сетевой мост** - при таком подключении виртуальная машина становится полноценным членом локальной сети, к которой подключена основная система. Машина использует сетевой интерфейс чтобы получить адрес у роутера и становится доступна для других устройств, как и основной компьютер по своему ip адресу.

- **Внутренняя сеть** - почти то же самое, что и виртуальный адаптер хоста, только без возможности доступа к виртуальной сети из основной системы, доступа к интернету нет.
- **Универсальный драйвер** - позволяет использовать драйвер из расширений VirtualBox для связи между машинами, расположенными на разных физических хостах.

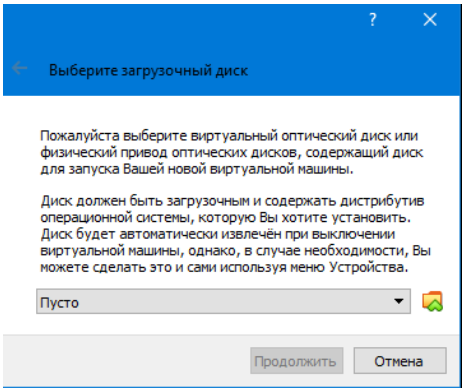
Для связи между нашими виртуальными компьютерами мы будем использовать тип подключения «**внутренняя сеть**».

Для этого выбираем виртуальную машину, нажимаем кнопку «Настроить», дальше «Сеть», выбираем тип соединения – внутренняя сеть. Для того, чтобы ваши виртуальные машины «видели» друг друга, необходимо, чтобы имя сети на обеих машинах было одинаковым.



УСТАНОВКА ОПЕРАЦИОННОЙ СИСТЕМЫ НА ВИРТУАЛЬНУЮ МАШИНУ

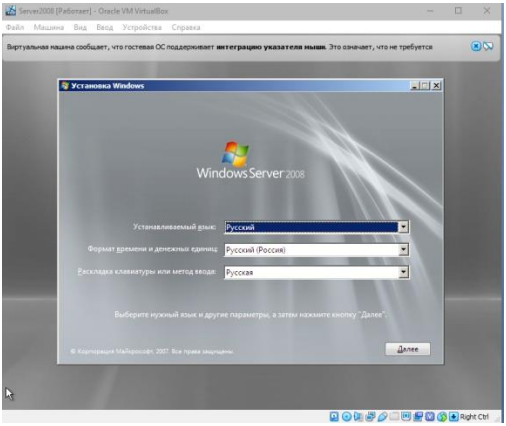
При первом включении виртуальной машины VirtualBox запросит загрузочный диск:



Здесь можно в физический привод оптических дисков вложить диск с файлами установки операционной системы, либо указать на образ установочного диска, хранящегося на каком либо физическом носителе. После этого необходимо нажать кнопку «продолжить» и начнется творческий процесс установки операционной системы.

Стартовое окно установки Windows 7:

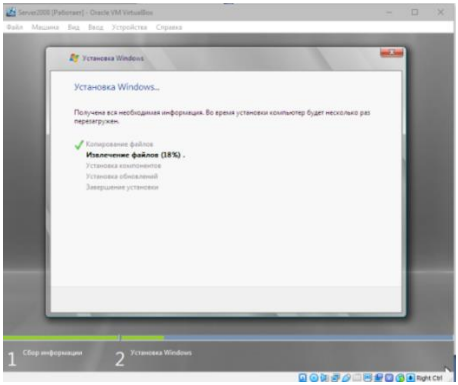
Стартовое окно установки Windows Server 2008:



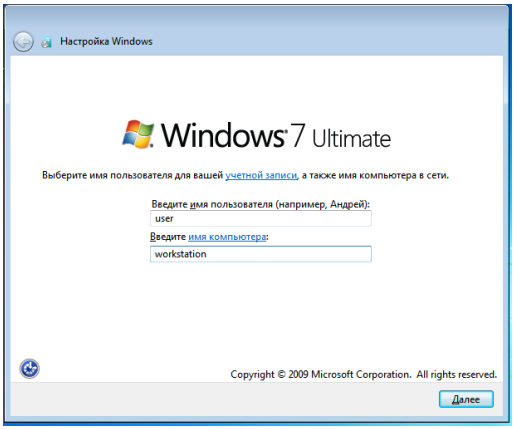
Процесс установки операционных систем на виртуальные машины ничем не отличается от обычного. Для наших целей подойдет редакция Windows Server 2008 Standart. Весь необходимый функционал для наших задач там уже присутствует.

Для клиентской версии необходимо, чтобы компьютер в дальнейшем мог работать в составе домена. Для Windows 7 это редакции Proffessional, Enterprise и Ultimate.

Процесс установки Windows Server 2008 R2:

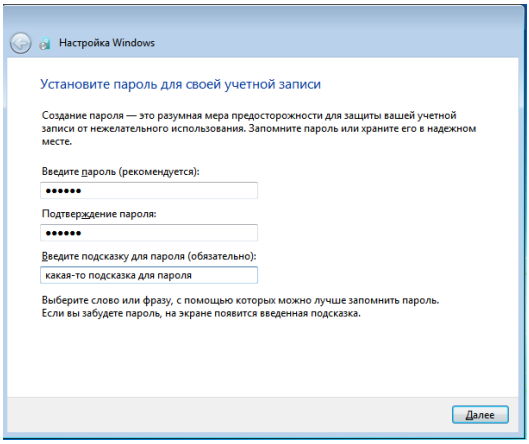


По завершению установки Windows 7 на клиентскую машину необходимо будет ввести имя пользователя и имя компьютера. В данном случае вводим имя пользователя **user** и в качестве имени компьютера **workstation**:



В вашем случае имена компьютера и пользователя могут быть другими. Следует заметить, что в больших сетях имеет смысл давать компьютерам имена, характеризующие их местоположение в локально-вычислительной сети. Это бывает необходимо для более быстрой локализации места аварии и сокращения времени реагирования на сетевые неисправности. В данном случае рабочая станция будет только одна и поэтому не имеет большого значения, как ее называть.

На следующем этапе система предложит вам установить пароль для учетной записи. Можно оставить поле пустым, но это может повлечь за собой существенное снижение безопасности вашего компьютера. Заданный пароль ограничивает число лиц, имеющих доступ к компьютеру. Так же не следует забывать о сложности паролей. Пароли типа «123», «12345», «123456», «qwerty» и т.д. могут быть легко подобраны! Злоумышленник в этом случае может получить доступ к вашим файлам и настройкам компьютера.



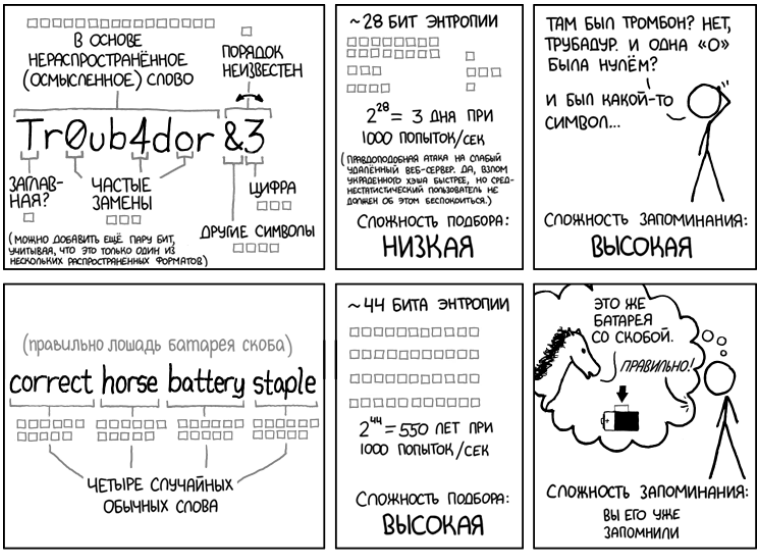
Согласно NIST Special Publication 800-63B (набор инструкций по выбору и управлению паролей) рекомендуется чередовать цифры, специальные символы, строчные и прописные буквы, а также периодически менять пароли. Этот стандарт широко применяется во многих организациях по всему миру.

Но со временем проявилась одна проблема. Выяснилось, что эти рекомендации неправильные, они вовсе не способствуют повышению компьютерной безопасности.

Во-первых, такие пароли гораздо труднее запомнить. Попробуйте запомнить беспорядочный набор символов в верхнем и нижнем регистрах, перемешанные с цифрами.

Во-вторых, особенно неправильной оказалась рекомендация менять пароли каждые 90 дней. Если хотя бы один сложный пароль из букв с цифрами пользователь может запомнить, то как ему изменить его через 90 дней и запомнить новый пароль? Как показала практика, большинство людей решают эту проблему самым логичным способом: они делают минимальные изменения в пароле. Например, просто меняют последнюю цифру, прибавляя единицу: Pa55word!1, Pa55word!2, Pa55word!3 и так далее. Это совершенно не способствует повышению безопасности.

Сейчас более правильным считается использовать длинные парольные фразы, легкие для запоминания, но трудные для брутфорса.

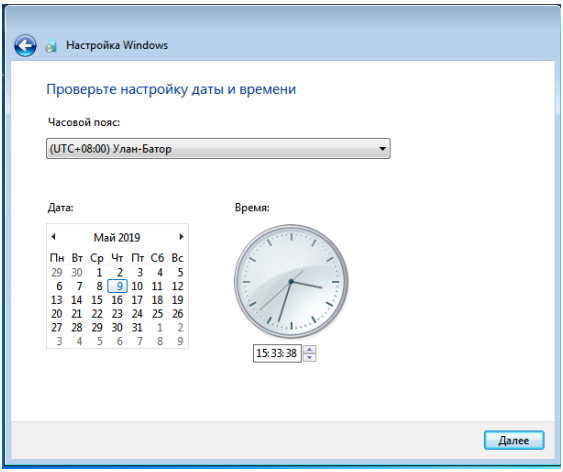


ЗА 20 ЛЕТ СТАРАНИЙ МЫ НАУЧИЛИ ВСЕХ ИСПОЛЬЗОВАТЬ ПАРОЛИ, КОТОРЫЕ ЧЕЛОВЕКУ ЗАПОМНИТЬ СЛОЖНО, А КОМПЬЮТЕРУ ПОДОБРАТЬ ЛЕГКО.

Это могут быть строчки из стихотворения или произвольные предложения. Чтобы брутфорсить 40-символьные фразы, хакерам придётся применять новые словари с графами сочетаемости слов. Это более сложно, чем сбрутить восьмисимвольный пароль с произвольными символами.

Исследователи говорят, что даже фраза из четырёх произвольных слов обеспечивает достаточно высокий уровень безопасности, чтобы надёжно защититься от брутфорса.

Продолжаем настройку клиентской машины.

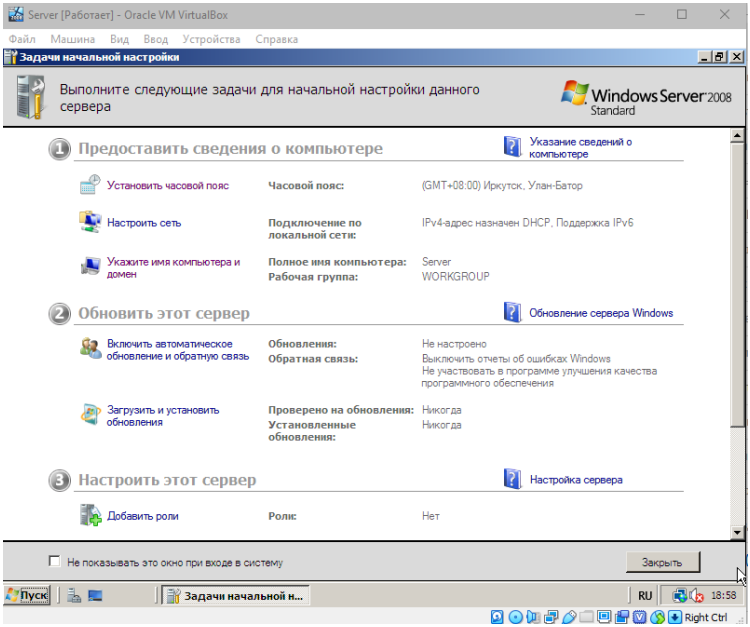


В этом окне нужно выбрать правильный часовой пояс (а в нашем случае это +8 от Гринвича) и проверить корректность установки даты и времени.

В следующем окне при выборе типа сети выбираем рабочую сеть. На этом первоначальная настройка рабочей станции завершена.

ПЕРВИЧНАЯ НАСТРОЙКА MS SERVER 2008

Устанавливаем правильные настройки часового пояса, времени и даты.



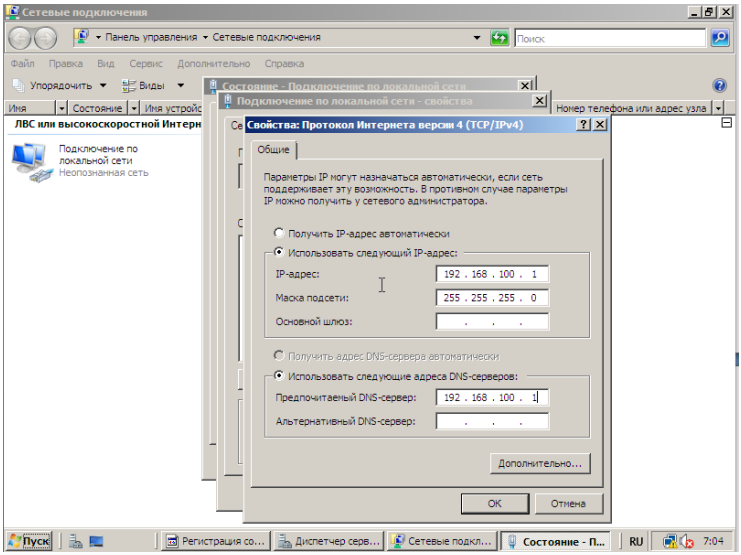
Перед настройкой DNS-сервера, переименовываем его в server (или какое-либо другое осмысленное имя), чтобы назначение компьютера в сети было понятно:

Мой компьютер \ ПКМ \ Свойства \ Имя компьютера \ Изменить параметры \ Изменить \ server \ ОК \ Перезагрузка (Здесь и далее ПКМ – правая клавиша мыши)

Теперь назначаем сетевой карте статический IP-адрес, так как у сервера IP-адрес меняться не должен:

Центр управления сетями и общим доступом \ Подключение по локальной сети \ Свойства \ Протокол интернета версии 4

Устанавливаем значения:



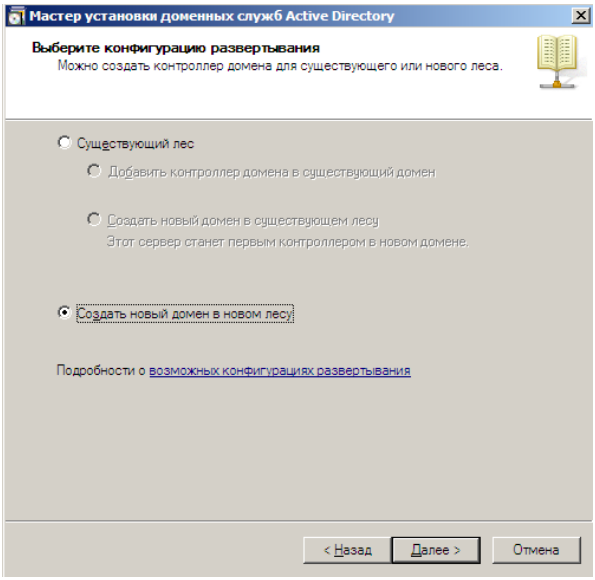
РАЗВЕРТЫВАНИЕ КОНТРОЛЛЕРА ДОМЕНА ПОД УПРАВЛЕНИЕМ MS SERVER 2008

Пуск \ Администрирование \ Диспетчер сервера \ Роли \ Добавить роли \ Далее \Доменные службы Active Directory\ Далее \ Далее \Установить\ Закрыть

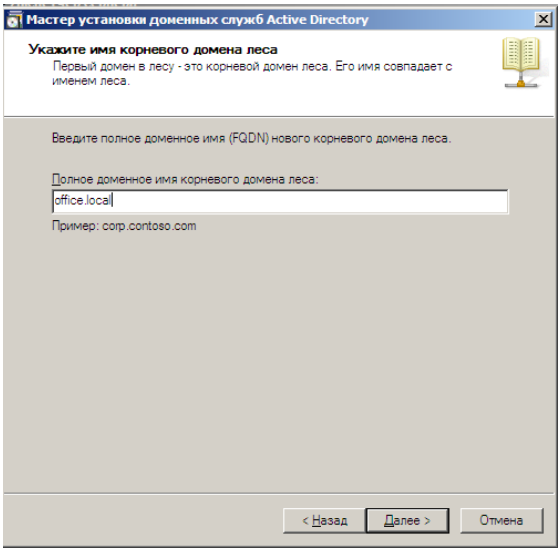
Затем следует запустить мастер установки доменных служб Active Directoty: для этого можно использовать комбинацию клавиш Win-R и в появившемся окошке напечатать **dcpromo.exe,** затем нажать кноку **ОК.**

В ходе установки при выборе конфигурации развертывания необходимо выбрать **Создать новый домен в новом лесу.**

В нашей учебной сети еще нет доменов, поэтому выбор тут очевиден.



Затем вводим имя вашего домена:



Режим работы леса выбираем Windows Server 2008. В нашей сети нет серверов под управлением предыдущих редакций Windows Server (2000 или 2003).

Так как мы еще не разворачивали DNS сервер, то мастер на определенном этапе предложит его установить. Ответим на это нашим решительным согласием.

Остальные настройки оставляем по умолчанию. Необходимо задать надежный пароль для администратора режима восстановления служб каталогов.

В финальном окне можно просмотреть заданные настройки, проверить их корректность. Если настройки правильны, то можно нажать кнопку **Далее**

После завершения установки необходимо перезагрузить компьютер.

СОЗДАНИЕ УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ В ACTIVE DIRECTORY

Основополагающим компонентом доменных служб в каждой организации являются принципалы безопасности (оригинальное название - Security Principal), которые предоставляют пользователей, группы или компьютеры, которым требуется доступ к определенным ресурсам в сети. Именно таким объектам, как принципалам безопасности можно предоставлять разрешения доступа к ресурсам в сети, причем каждому принципалу во время создания объекта присваивается уникальный идентификатор безопасности (SID), который состоит из двух частей.

Идентификатором безопасности SID называется числовое представление, которое уникально идентифицирует принципал безопасности. Первая часть такого идентификатора представляет собой **идентификатор домена**. Ввиду того, что принципалы безопасности расположены в одном домене, всем таким объектам присваивается один и тот же идентификатор домена. Второй частью SID является **относительный идентификатор (RID)**, который используется для уникальной идентификации принципала безопасности по отношению к ведомству, которое выдает SID.

Несмотря на то, что планирование и развертывание инфраструктуры доменных служб в большинстве организаций выполняется лишь один раз и в большинство объектов изменения вносятся очень редко, к важному исключению из этого правила можно отнести принципалы безопасности, которые необходимо периодически добавлять, изменять, а также удалять. Одним из основополагающих компонента идентификации являются учетные записи пользователей.

По сути, учетные записи пользователей представляют собой физические объекты, в основном людей, которые являются сотрудниками вашей организации, но бывают исключения, когда учетные записи пользователей создаются для некоторых приложений в качестве служб. Учетные записи пользователей играют важнейшую роль в администрировании предприятии. К таким ролям можно отнести:

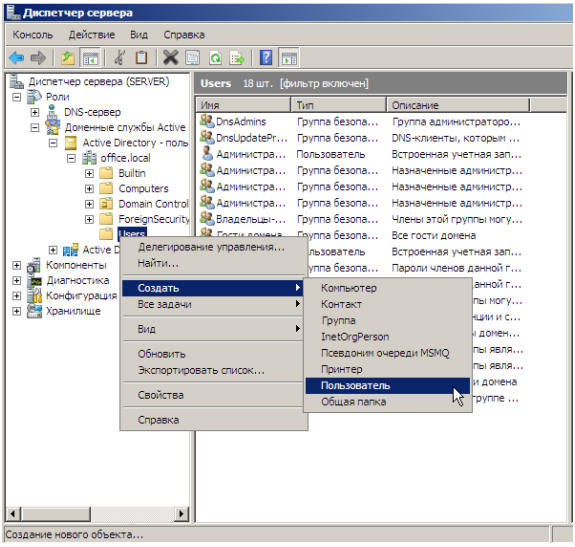
- **Удостоверение личности пользователей**, так как созданная учетная запись позволяет входить на компьютеры и в домены именно с теми данными, подлинность которых проверяет домен;
- **Разрешения доступа к ресурсам домена**, которые назначаются пользователю для предоставления доступа к доменным ресурсам на основании явных разрешений.

Объекты учетных записей пользователей можно отнести к самым распространенным объектам в Active Directory. Именно пользовательским учетным записям администраторы обязаны уделять особое внимание, так как пользователям свойственно приходить работать в организацию, перемещаться между отделами и офисами, жениться, выходить замуж, разводиться и даже увольняться из компании. Такие объекты представляют собой набор атрибутов, причем только одна пользовательская учетная запись может содержать свыше 250 различных атрибутов, что в несколько раз превышает количество атрибутов на рабочих станциях и компьютеров, работающих под операционной системой Linux. Во время создания учетной записи пользователя создается ограниченный набор атрибутов, а уже потом вы можете добавлять такие пользовательские учетные данные как организационные сведения, адреса проживания пользователей, телефонные номера и многое другое. Поэтому важно обратить внимание на то, что одни атрибуты являются **обязательными**, а остальные – **опциональными**.

В подавляющем большинстве случаев системные администраторы для создания основных принципалов безопасности предпочитают использовать оснастку **«Active Directory – пользователи и компьютеры»**, которая добавляется в папку **«Администрирование»** сразу после установки роли **«Доменные службы Active Directory»** и повышения сервера до контролера домена. Этот метод является наиболее удобным, так как для создания принципалов безопасности используется графический пользовательский интерфейс и мастер создания учетных записей пользователя очень прост в применении. К недостатку данного метода можно отнести тот момент, что при создании учетной записи пользователя вы не можете сразу задать большинство атрибутов, и вам придется добавлять необходимые атрибуты путем редактирования учетной записи.

Для того чтобы создать пользовательскую учетную запись, выполните следующие действия:

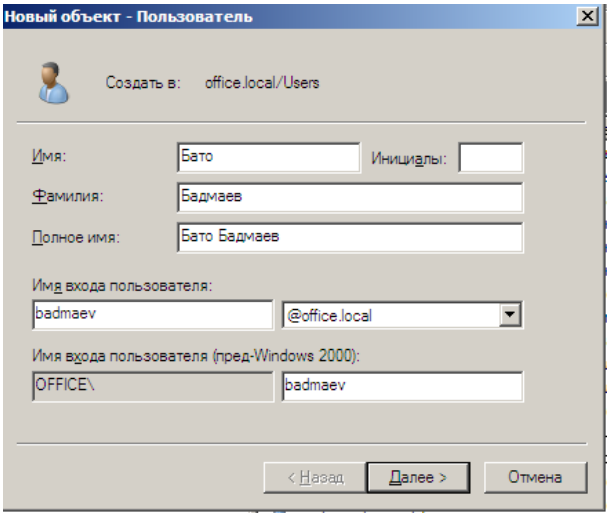
1. Откройте оснастку **«Active Directory – пользователи и компьютеры»**. Для этого вам нужно открыть панель управления, в ней открыть раздел **«Система и безопасность»**, затем **«Администрирование»** и в появившемся окне открыть оснастку **«Active Directory – пользователи и компьютеры»**.
2. В дереве оснастки, разверните узел своего домена и перейдите к подразделению, в котором будет создаваться пользовательская учетная запись. Для создания пользовательских учетных записей рекомендуется создавать дополнительные подразделения, после чего добавлять учетные записи пользователей в подразделения, отличающиеся от стандартного подразделения Users. Щелкните на этом подразделении правой кнопкой мыши и из контекстного меню выберите команду **«Создать»**, а затем **«Пользователь»**, как показано на следующей иллюстрации:



3. В появившемся диалоговом окне **«Новый объект - Пользователь»** введите следующую информацию:

1. В поле **«Имя»** введите имя пользователя;
2. В поле **«Инициалы»** введите его инициалы (чаще всего инициалы не используются);
3. В поле **«Фамилия»** введите фамилию создаваемого пользователя;
4. Поле **«Полное имя»** используется для создания таких атрибутов создаваемого объекта, как основное имя (Common Name) **CN** и отображения свойств имени. Это поле должно быть уникальным во всем домене, и заполняется автоматически, а изменять его стоит лишь в случае необходимости;
5. Поле **«Имя входа пользователя»** является обязательным и предназначено для имени входа пользователя в домен. Здесь вам нужно ввести имя пользователя и из раскрывающегося списка выбрать суффикс UPN, который будет расположен после символа @;
6. Поле **«Имя входа пользователя (Пред-Windows 2000)»** предназначено для имени входа для систем предшествующих операционной системе Windows 2000. В последние годы в организациях все реже встречаются обладатели таких систем, но поле обязательно, так как некоторое программное обеспечение для идентификации пользователей использует именно этот атрибут;

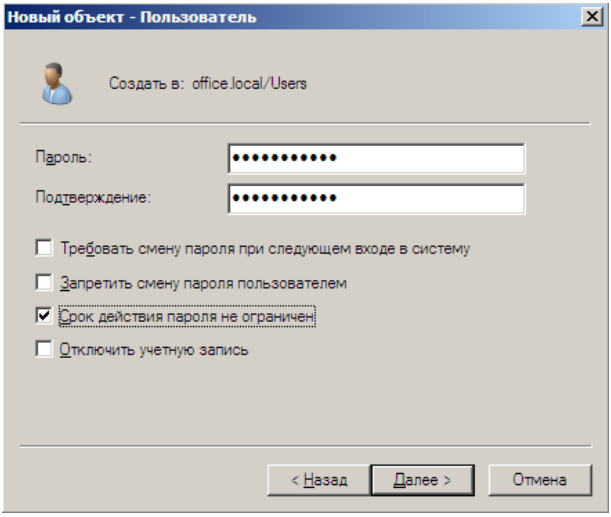
После того как заполните все требуемые поля, нажмите на кнопку **«Далее»**:



На следующей странице мастера создания пользовательской учетной записи вам предстоит ввести начальный пароль пользователя в поле **«Пароль»** и подтвердить его в поле **«Подтверждение»**. Помимо этого, вы можете выбрать атрибут, указывающий на то, что при первом входе пользователя в систему пользователь должен самостоятельно изменить пароль для своей учетной записи.

Лучше всего использовать эту опцию в связке с локальными политиками безопасности **«Политика паролей»**, что позволит создавать надежные пароли для ваших пользователей. Также, установив флажок на опции **«Запретить смену пароля пользователем»** вы предоставляете пользователю свой пароль и запрещаете его изменять. При выборе опции **«Срок действия пароля не ограничен»** у пароля учетной записи пользователя срок действия пароля никогда не истечет и не будет необходимости в его периодическом изменении. Если вы установите флажок **«Отключить учетную запись»**, то данная учетная запись будет не предназначена для дальнейшей работы и пользователь с такой учетной записью не

сможет выполнить вход до ее включения. После выбора всех атрибутов, нажмите на кнопку **«Далее»**. Эта страница мастера изображена на следующей иллюстрации:



Создание учетных записей пользователей с помощью командной строки

Как и в большинстве случаев, в операционной системе Windows есть утилиты командной строки с аналогичными функциями графического пользовательского интерфейса оснастки **«Active Directory – пользователи и компьютеры»**. Такие команды называются командами DS, так как они начинаются с букв DS. Для создания принципалов безопасности используется команда **Dsadd**. После самой команды указываются модификаторы, которые определяют тип и имя DN объекта. В случае с созданием учетных записей пользователей вам нужно указать модификатор **user**, который является типом объекта. После типа объекта необходимо ввести DN имя самого объекта. DN (Distinguished Name) объекта является результирующим набором, который содержит отличительное имя. Следом за DN обычно указывают имя пользователя UPN или имя

входа предыдущих версий Windows. Если в имени DN присутствуют пробелы, то такое имя нужно заключить в кавычки. Синтаксис команды следующий:

```
Dsadd user DN имя –samid имя учетной записи –UPN имя –pwd пароль –дополнительные параметры
```

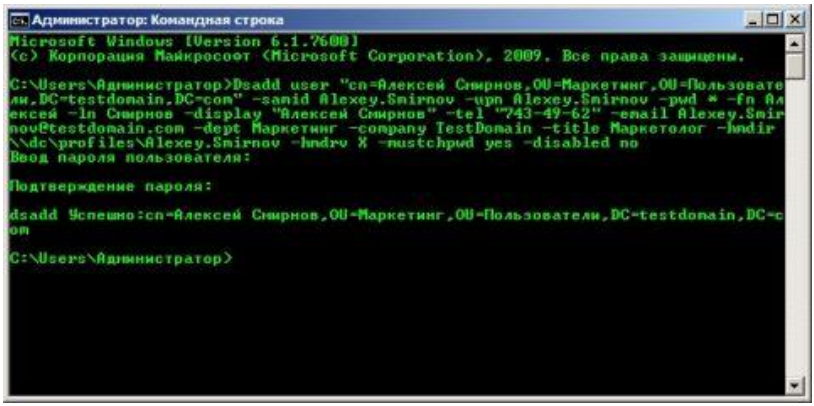
С данной командой можно использовать 41 параметр. Рассмотрим самые распространенные из них:
-samid – имя учетной записи пользователя;
-upn – имя входа пользователя пред-Windows 2000;
-fn – имя пользователя, которое в графическом интерфейсе заполняется в поле **«Имя»**;
-mi – инициал пользователя;
-ln – фамилия пользователя, указываемая в поле «Фамилия» мастера создания пользовательской учетной записи;
-display – указывает полное имя пользователя, которое автоматически генерируется в пользовательском интерфейсе;
-empid – код сотрудника, который создается для пользователя;
-pwd – параметр, определяющий пользовательский пароль. В том случае, если вы укажете символ звездочки (*), вам будет предложено ввести пароль пользователя в защищенном от просмотра режиме;
-desc – краткое описание для пользовательской учетной записи;
-memberof – параметр, определяющий членство пользователя в одной или нескольких группах;
-office – местонахождения офиса, где работает пользователь. В свойствах учетной записи этот параметр можно найти во вкладке **«Организация»**;
-tel – номер контактного телефона текущего пользователя;
-email – адрес электронной почты пользователя, который можно найти во вкладке **«Общие»**;
-hometel – параметр, указывающий номер домашнего телефона пользователя;
-mobile – телефонный номер мобильного пользователя;
-fax – номер факсимильного аппарата, который использует текущий пользователь;
-title – должность пользователя в данной организации;

-dept – этот параметр позволяет указать наименование отдела, в котором работает данный пользователь;
-company – название компании, в которой работает создаваемый пользователь;
-hmdir – основной каталог пользователя, в котором будут расположены его документы;
-hmdrv – путь к сетевому диску, на котором будет размещена домашняя папка учетной записи
-profile – путь профиля пользователя;
-mustchpwd – данный параметр указывает на то, что при последующем входе в систему пользователь обязан изменить свой пароль;
-canchpwd – параметр, определяющий, должен ли пользователь изменять свой пароль. Если значением параметра указано **«yes»**, то у пользователя будет возможность изменения пароля;
-reversiblepwd – текущий параметр определяет хранение пароля пользователя с применением обратного шифрования;
-pwdneverexpires – параметр, указывающий на то, что срок действия пароля никогда не истечет. Во всех этих четырех параметрах, значениями могут выступать только **«yes»** или **«no»**;
-acctexpires – параметр, определяющий, через сколько дней срок действия учетной записи истечет. Положительное значение представляет собой количество дней, через которое учетная запись истечет, а отрицательное означает, что срок действия уже закончен;
-disabled – указывает, что учетная запись уже отключена. Значениями для этого параметра также выступают **«yes»** или **«no»**;
-q – указание тихого режима для обработки команды.
Пример использования:

```
Dsadd user “cn=Алексей Смирнов,OU=Маркетинг,OU=Пользователи,DC=testdomain,DC=com” -samid Alexey.Smirnov -upn Alexey.Smirnov

-pwd * -fn Алексей -ln Смирнов -display “Алексей Смирнов” -tel “743-49-62” -email Alexey.Smirnov@testdomain.com -dept Маркетинг

-company TestDomain -title Маркетолог -hmdir \\dc\profiles\Alexey.Smirnov -hmdrv X -mustchpwd yes -disabled no
```


Администратор: Командная строка
Microsoft Windows [Version 6.1.7600]
(c) Корпорация Майкрософт (Microsoft Corporation), 2009. Все права защищены.
C:\Users\Администратор>Dsadd user "cn=Алексей Смирнов,OU=Маркетинг,OU=Пользовате
ли,DC=testdomain,DC=com" -samid Alexey.Smirnov -upn Alexey.Smirnov -pwd * -fn Ал
ексей -ln Смирнов -display "Алексей Смирнов" -tel "743-49-62" -email Alexey.Smir
nov@testdomain.com -dept Маркетинг -company TestDomain -title Маркетолог -hmdir
\\dc\profiles\Alexey.Smirnov -hmdrv X -mustchpwd yes -disabled no
Ввод пароля пользователя:
Подтверждение пароля:
dsadd Успешно:cn=Алексей Смирнов,OU=Маркетинг,OU=Пользователи,DC=testdomain,DC=c
om
C:\Users\Администратор>

СОЗДАНИЕ ГРУПП ПОЛЬЗОВАТЕЛЕЙ

К одному из ключевых моментов концепции доменных служб Active Directory можно отнести обеспечение авторизации принципалов безопасности для получения доступа к имеющимся сетевым ресурсам. Несмотря на то, что весь доступ к сетевым ресурсам основан на учетных записях отдельных пользователей, компьютеров или служб, со временем они могут меняться. В средних и крупных компаниях управление существующими пользователями требует большой административной нагрузки. Стоит учесть, что пользователи, выполняющие в компании конкретную роль, могут меняться, но сама роль должна оставаться без каких-либо изменений. Если назначать доступ к сетевым ресурсами индивидуально для каждого отдельного пользователя, то списки контроля доступа ACL вскоре станут неуправляемыми и при изменении отдела пользователем вам нужно будет учесть все возможные разрешения доступа. Так как этот процесс может легко выйти из-под контроля, задачи, связанные с управлением должны быть привязаны к объектам групп. Чаще всего группы используются для идентификации ролей пользователей и компьютеров, фильтрации групповой политики, назначения уникальных политик паролей, прав, разрешений доступа, приложений электронной почты и многое другое.

Сами по себе, группы представляют собой принципалы безопасности с уникальными SID, которые могут содержать в атрибуте member такие принципалы безопасности, как пользователи, компьютеры, группы и контакты.

Перед тем как создавать группы следует знать, какие существуют разновидности групп. Так как структура доменных служб предназначена для поддержки сложных и крупных распределительных сред, Active Directory включает в себя два типа групп домена с тремя областями действия в каждой из них, а также локальную группу безопасности. Типы групп, а также их область действия подробно рассмотрены в следующих подразделах.

В доменных службах Active Directory Windows Server 2008 можно отметить два типа групп: безопасности и распространения. При создании новой группы в диалоговом окне **«Новый объект - группа»** оснастки **«Active Directory – пользователи и**

компьютеры» вы можете выбрать одну из этих двух групп. Группы безопасности относятся к принципалам безопасности с SID-идентификаторами. В связи с этим данный тип группы считается самым распространенным и группы такого типа можно использовать для управления безопасностью и назначения разрешений доступа к сетевым ресурсам в списках ACL. В общем, группу безопасности стоит использовать в том случае, если они будут использоваться для управления безопасностью.

В свою очередь, группа распространения изначально используется приложениями электронной почты, и она не может быть принципалом безопасности. Другими словами, этот тип группы не является субъектом безопасности. Так как эту группу нельзя использовать для назначения доступа к ресурсам, она чаще всего используется при установке Microsoft Exchange Server в том случае, когда пользователей необходимо объединить в группу с целью отправки электронной почты сразу всей группе.

Ввиду того, что именно группы безопасности вы можете использовать как с целью назначения доступа к ресурсам, так и с целью распространения электронной почты, многие организации используют только этот тип группы. В домене с функциональным уровнем не ниже Windows 2000 вы можете преобразовывать группы безопасности в группы распространения и наоборот.

Область действия группы определяет диапазон, в котором применяется группа внутри домена. Помимо того, что группы могут содержать пользователей и компьютеры, они могут быть членами других групп, ссылаться на списки ACL, фильтры объектов и групповых политик и пр. Граница диапазона области действия группы может определяться заданием режима работы домена. К основным характеристикам области действия групп можно отнести членство (определение принципалов безопасности, которые может содержать группа), репликация (определение области репликации группы), а также доступность (определение местонахождения группы, возможности включения этой группы в членство другой, добавление группы в список ACL). Существует четыре области действия групп: локальная, локальная в домене, глобальная и универсальная. Рассмотрим подробнее каждую из них:

- **Локальная группа в домене**. Группы с областью локальные группы в домене предназначены для управления разрешениями доступа к ресурсам и функционируют в том случае, если домен работает на функциональном уровне не ниже Windows 2000. В том случае, если домен работает на уровне Windows NT или в смешанном уровне, то эти группы будут использоваться лишь как локальные группы. Такая группа определяется в контексте именования домена. Локальную группу в домене можно добавлять в списки ACL любого ресурса на любом рядовом компьютере домена. В локальную группу в домене могут входить пользователи, компьютеры, глобальные и локальные группы в текущем домене, любом другом домене леса, а также универсальные группы в любом домене леса. Другими словами, репликация и доступность такой группы позволяет ее использовать в пределах всего домена. В связи с этим, локальные группы в домене обычно используют для предоставления правил доступа во всем домене, а также для членов доверительных доменов. Чаще всего, с локальными группами в домене связаны сценарии, подобные следующему: вам нужно предоставить доступ к папке с секретной документацией восьми пользователям из разных отделов. Вы должны учесть, что кто-либо из этих пользователей может перейти в другой отдел или уволиться и позже вам придется изменять разрешения доступа на принтере. А если доступ нужно предоставить не восьми, а восьмидесяти пользователям из разных подразделений и доменов? Поэтому, чтобы упростить такую рутинную работу вы можете создать группу с локальной областью безопасности в домене и разрешить доступ к папке именно этой группе. После этого вы можете добавлять, любых пользователей из этой группы и все пользователи, входящие в состав этой группы автоматически получат доступ к папке;
- **Глобальная группа**. Основной целью глобальных групп безопасности является определение коллекции объектов доменов на основании бизнес-правил и управление объектами, которые требуют ежедневного использования. Чаще

всего, членами таких групп выступают пользователи и компьютеры. Группы безопасности удобно использовать для фильтрации области действия групповых политик, так как область действия таких групп не реплицируется за пределы своего домена, при этом не вызывая дополнительного трафика к глобальному каталогу. Глобальная группа может содержать пользователей, компьютеры и другие глобальные группы только из одного домена. Несмотря на это, глобальные группы могут быть членами любых универсальных и локальных групп как в своем домене, так и доверяющем домене. Помимо этого, глобальные группы можно добавлять в списки ACL в домене, лесу и в доверяющем домене, что делает управление группами более простым и рациональным;

- **Универсальная группа**. Универсальные группы целесообразно задействовать только в лесах, состоящих из множества доменов для их объединения. Эти группы позволяют управлять ресурсами, распределенными на нескольких доменах, поэтому универсальные группы считаются самыми гибкими. Универсальные группы определяются в одном домене, но реплицируются в глобальный каталог. Например, для того чтобы получить пользователям из домена B доступ к ресурсам, расположенным в домене A, добавьте учетные записи пользователей домена B в глобальные группы безопасности, а затем эти группы вложите в универсальную группу. Универсальная группа может быть членом другой универсальной или локальной группы домена в лесу, а также может использоваться для управления ресурсами;
- **Локальная группа**. Локальная группа считается самой примитивной, так как она доступна только на одном компьютере. Такая группа создается в базе данных диспетчера безопасности учетных записей рядового компьютера и поэтому в домене управление локальными группами не нужно. В списках ACL можно использовать такие группы только на локальном компьютере. В другие системы такие группы не реплицируются, но эта группа содержит пользо-

вателей, компьютеры, глобальные и локальные группы в домене в своем домене, пользователей, компьютеры и глобальные и универсальные группы в любом домене леса.

В некоторых случаях перед вами может встать необходимость преобразования одной области действия в другую. Например, в связи с тем, что по умолчанию при создании группы фокус установлен на глобальной группе безопасности, по невнимательности можно оставить все без изменений и создать группу. После создания группы, ее область действия можно изменить на вкладке **«Общие»** диалогового окна свойств группы, одним из следующих доступных способов:

- Глобальную группу в универсальную в том случае, если изменяемая группа не является членом другой глобальной группы;
- Локальную группу в домене в универсальную в том случае, если эта группа не содержит другую локальную группу в домене в качестве члена;
- Универсальную группу в глобальную в том случае, если эта группа не содержит в качестве члена другую универсальную группу;
- Универсальную группу в локальную группу в домене.

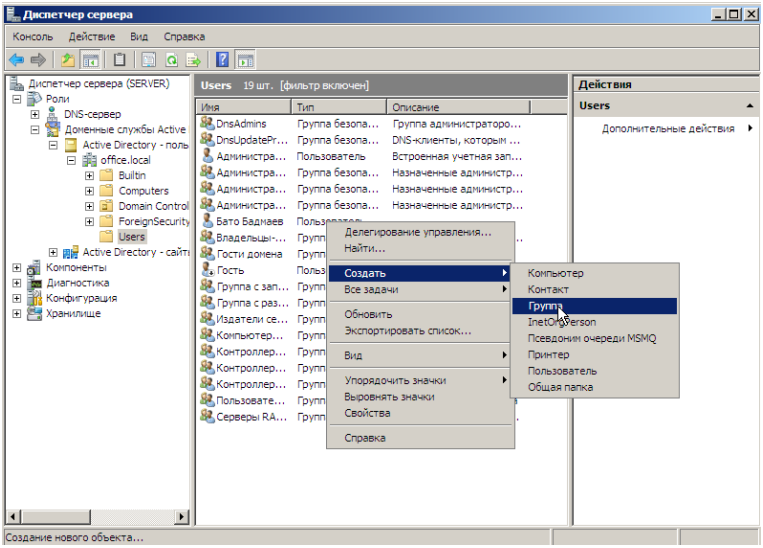
Как вы заметили, глобальную группу просто так невозможно модифицировать в локальную группу в домене. Несмотря на это, вы можете сначала глобальную группу преобразовать в универсальную, а затем уже получившуюся универсальную группу – в локальную группу в домене.

На первый взгляд все эти области групп могут показаться одинаковыми, но для наилучшего понимания их использования можно рассмотреть простой пример. Допустим, есть два домена. На первом домене (домен **A**) есть папка, для которой должен быть предоставлен доступ сотрудникам отдела продаж обоих доменов. В домене **A**, доступ к этой папке могут получить любые пользователи, но для более рационального использования пользователей, которым должен предоставляться доступ можно поместить их в глобальную группу безопасности. Но глобальная группа «Продажи»

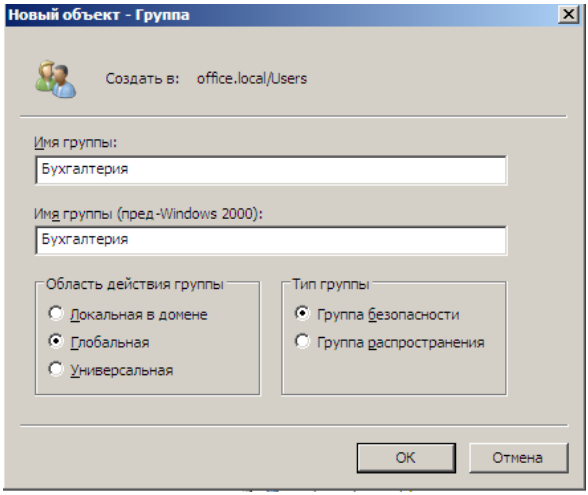
домена **B** не может получать доступ к папке в домене **A**. Поэтому глобальную группу «Продажи» из домена B нужно включить в универсальную группу, скажем «Доступ к ресурсам домена A». Затем, в домене **A** нужно создать локальную группу в домене (например, «Доступ к секретным материалам»), так как универсальная группа не может быть членом глобальной группы. Теперь нужно включить в группу «Доступ к секретным материалам» глобальную группу «Продажи» из домена **A** и универсальную группу «Доступ к ресурсам домена A» домена **B**. Только после этого, члены групп «Продажи» из обоих доменов будут иметь разрешения на использование секретных документов, расположенных в домене **A**.

Создание групп пользователей через оснастку «Active Directory – пользователи и компьютеры»

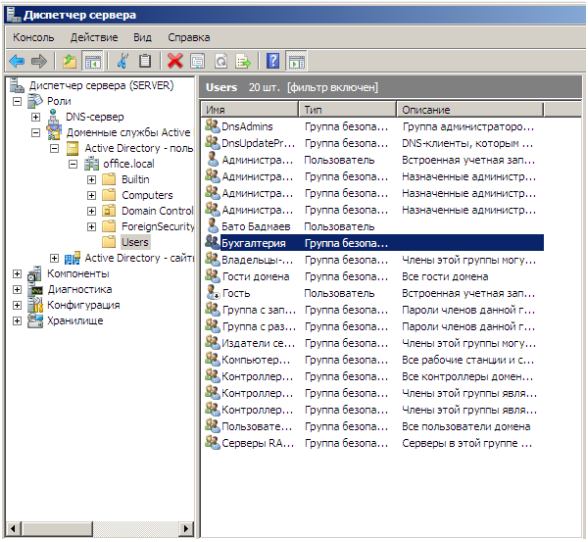
Используя данную оснастку, создавать пользователей и группы пользователей очень легко:



Диалоговое окно «Новый объект – группа»:

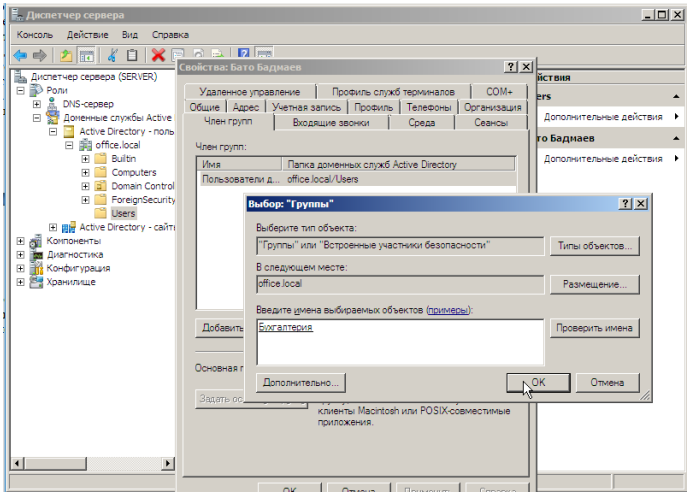


При нажатии кнопки **ОК** будет создана новая группа - Бухгалтерия:



ДОБАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯ В ГРУППУ

Пользователя в группу можно добавить разными способами. Можно открыть свойства пользователя, перейти в закладку «Член групп», нажать кнопку «Добавить» и в открывшемся окне выбора групп ввести имя нужной группы.



После нажатия на кнопку «ОК» пользователь Бато Бадмаев будет успешно добавлен в группу пользователей Бухгалтерия.

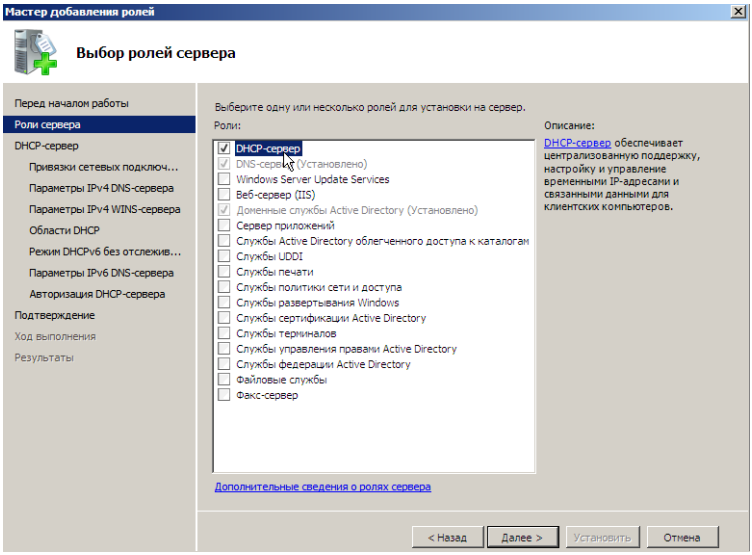
Так же можно пользователя добавить в группу через свойства этой группы. Открываем группу Бухгалтерия, переходим в закладку «Члены группы». Здесь мы видим список пользователей, входящих в группу. Можно добавить новых пользователей, либо, при необходимости, удалить каких-нибудь пользователей. Таким образом, вы можете создавать новых пользователей и группы, управлять составом групп пользователей. Следует заметить, что пользователь может являться членом нескольких групп.

РАЗВЕРТЫВАНИЕ DHCP-СЕРВЕРА

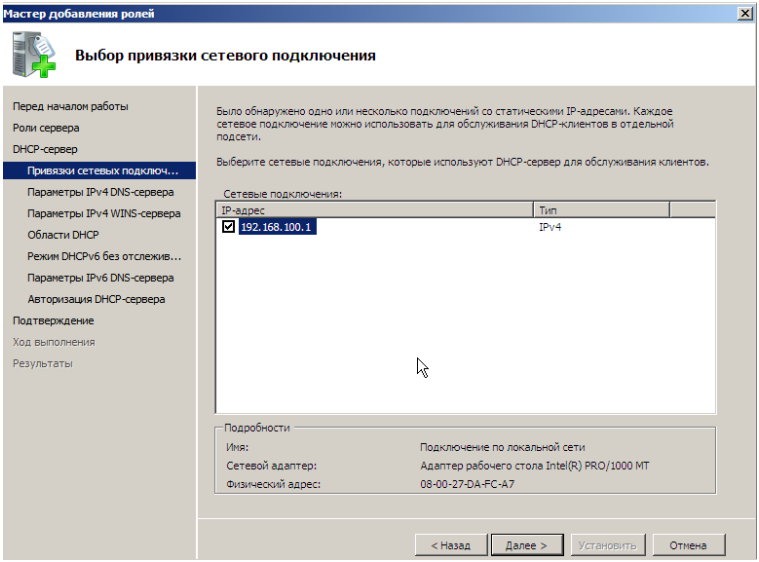
Для чего нужен DHCP-сервер? Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста) – сетевой протокол, используемый для того, чтобы компьютеры в сети смогли автоматически получить правильный IP-адрес и другие параметры для работы в сети TCP/IP.

Заметим, что IP адреса можно прописать на каждом компьютере сети вручную, но в больших сетях это не самый лучший вариант. Когда новый компьютер подключается к сети, обслуживаемой сервером DHCP, он запрашивает уникальный IP-адрес, а сервер DHCP назначает его из пула доступных адресов.

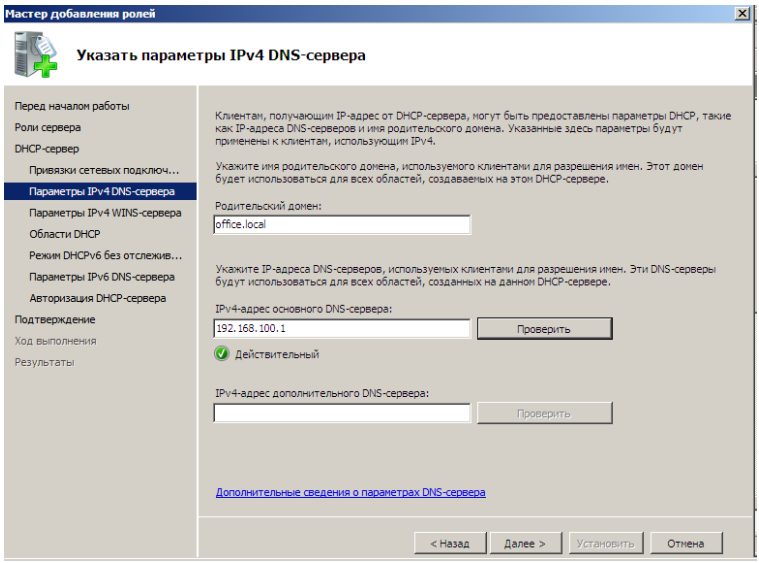
Установка DHCP сервера происходит через мастер добавления ролей:



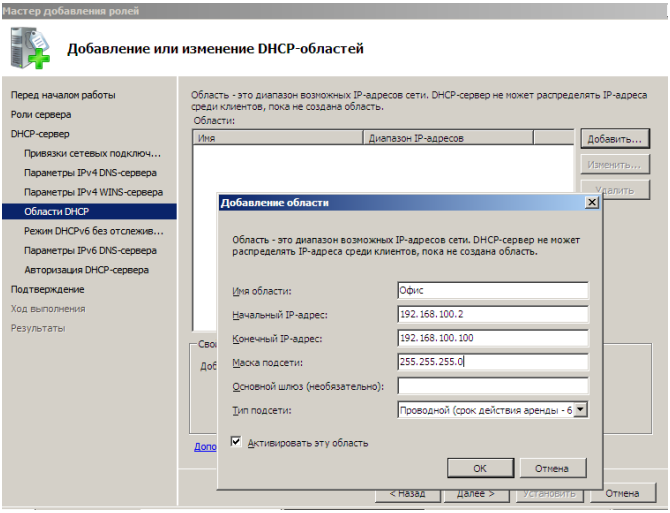
Важно, чтобы на сервере был статический IP адрес. Мы помним, что этот шаг проделали на этапе первоначальной настройки сервера. Мы присвоили сетевому адаптеру сервера IP адрес 192.168.100.1



Выбираем наше подключение с данным IP адресом и нажимаем «Далее».

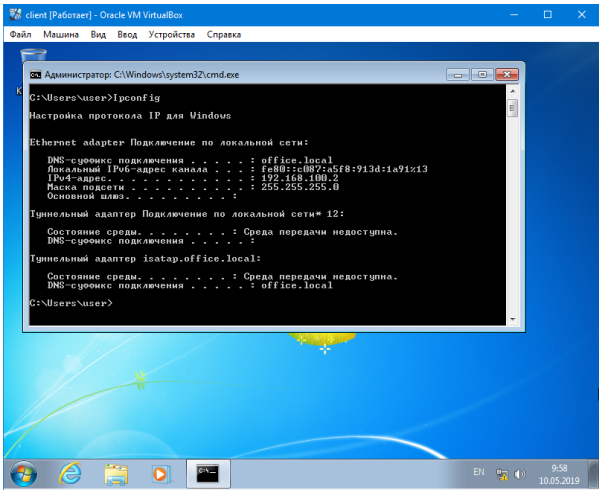


Использование WINS серверов при наличии DNS сервера является необязательным, поэтому мы этот пункт при настройке пропустим. Более интересным будет следующее окно, где необходимо будет добавить DHCP-области. Это диапазон раздаваемых IP адресов.



Здесь выбран диапазон от 192.168.100.2 до 192.168.100.100. Вы можете выбрать свои значения начального и конечного IP адреса.

Затем нажимаем «Далее» несколько раз и кнопку «Установить». Если вы все сделали правильно, то буквально через несколько минут мастер вам сообщит об успешной установке DHCP-сервера. Для проверки работоспособности можно запустить клиентскую машину под управлением Windows 7, которую мы уже сконфигурировали ранее. В командной строке запустим **ipconfig**

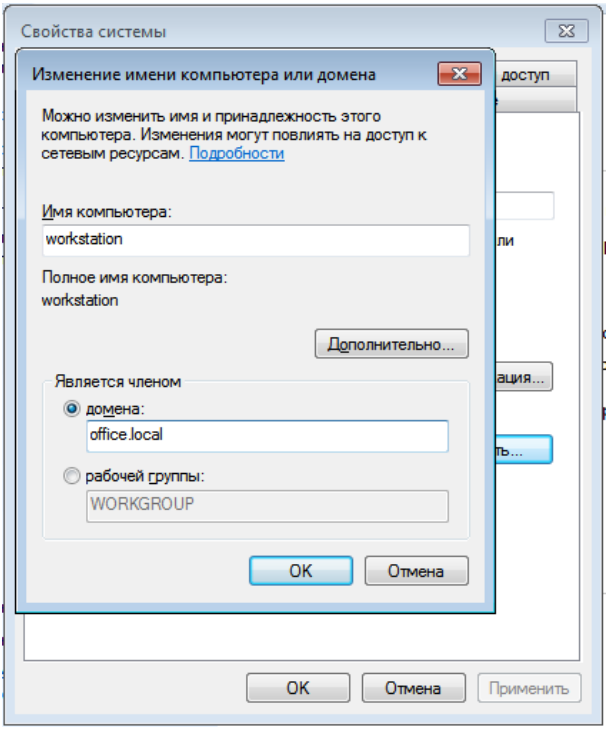


Здесь видим значение IPv4 адреса: 192.168.100.2 – это первый из пула адресов DHCP сервера. IP адрес получен верный, значит DHCP сервер работает корректно.

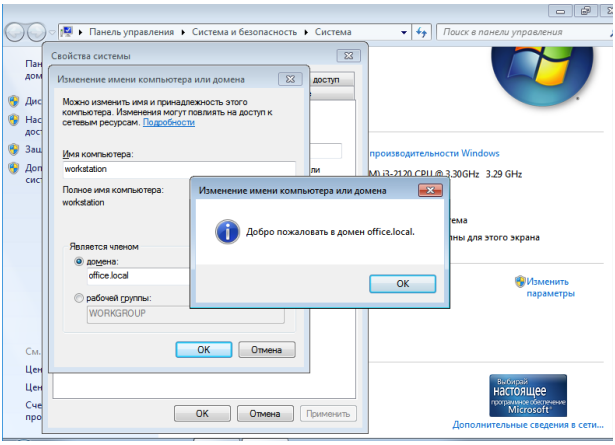
ДОБАВЛЕНИЕ КЛИЕНТСКОЙ МАШИНЫ В ДОМЕН

Клиентская машина у нас пока еще работает в рабочей группе. Необходимо ее добавить в домен. Существует несколько способов добавления рабочей станции в домен. Рассмотрим самый простейший для начинающих сисадминов – с использованием графического интерфейса.

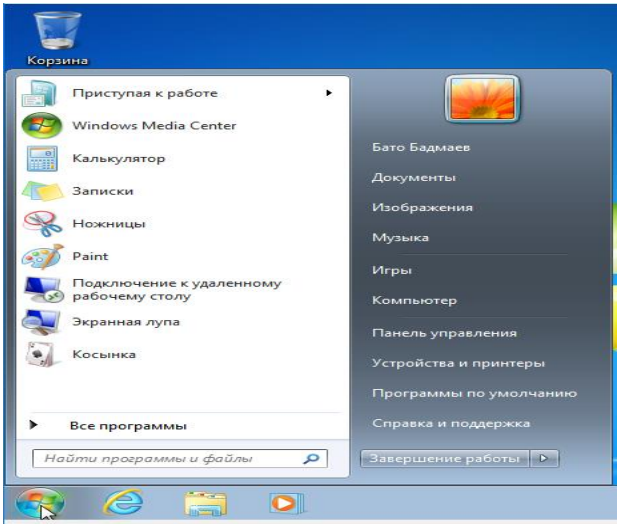
Мой компьютер / ПКМ / Свойства / Изменить параметры / Изменить



Здесь нужно прописать имя нашего домена и нажать кнопку ОК. В следующем окне нужно будет ввести логин и пароль администратора домена.



Компьютер теперь в домене и для входа в него мы можем использовать учетные записи пользователей домена. На следующей иллюстрации можно увидеть, что был осуществлен вход под учетной записью Бато Бадмаева:



РАЗВЕРТЫВАНИЕ ФАЙЛОВОГО СЕРВЕРА

С чего начинается создание роли файлового сервера? Нет, не с создания общей папки, а, как и создание любой другой роли, с оснастки **Роли** в **Диспетчере сервера**. Выберем роль **Файловые службы** и посмотрим, что мы можем установить. Как видим выбор довольно богат, не будем пока трогать продвинутые службы, каждая из которых требует, минимум, отдельной статьи, а установим собственно службы **Файлового сервера** и **Диспетчера ресурсов**. Следующим шагом нам будет предложено настроить наблюдение над томами хранилища. Настраивать наблюдение за системным диском мы не видим смысла, поэтому выбираем только те тома, которые будут использоваться для хранения пользовательских данных.

Завершим установку роли и создадим необходимые общие ресурсы. Но не спешите открывать доступ пользователям, сначала посмотрим какие возможности по управлению хранилищем предоставляет нам система. Для этого запустим **Диспетчер ресурсов файлового сервера**.

Начнем по порядку, а именно с **Управления квотами**, оснастка позволяет устанавливать квоты как к тому хранилища в целом, так и отдельным ресурсам. Квоты могут быть мягкими, когда о превышении квоты уведомляется администратор, и жесткими, когда запись на том (общий ресурс) блокируется. По умолчанию для тома уже выставлена мягкая квота в 85%, это позволит избежать ситуации, когда место на дисках внезапно закончится, администратор будет своевременно предупрежден и будет иметь возможность расширить том или удалить ненужные данные.

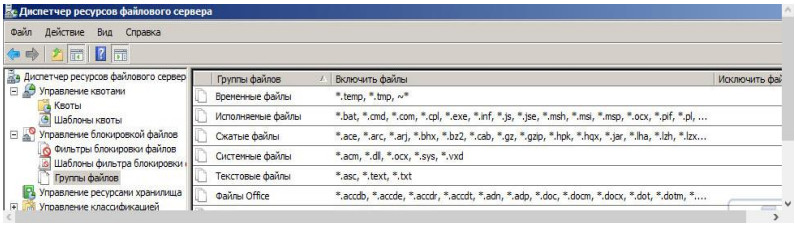
Для любого общего ресурса или папки на томе можно создать свою квоту, при создании квоты можно использовать один из шаблонов или установить все параметры вручную. В нашем случае мы создали для папки **Users** жесткую квоту 200+50 Мб, по превышению квоты администратор будет уведомлен, а пользователь сможет записать еще 50 Мб, после чего запись будет блокирована.

Следующим шагом перейдем к шаблонам, данный раздел уже содержит некоторое количество готовых настроек и мы можем создавать здесь новые. Мы рекомендуем задавать собственные

настройки квот именно через шаблоны, это позволит быстро применить однотипные настройки сразу к нескольким ресурсам и столь-же быстро изменить их в случае необходимости.

Разобравшись с квотами, перейдем к блокировке файлов. Не секрет, что пользователи хранят на общих ресурсах и то, что надо и то, что не надо, в частности очень любят размещать там коллекции фото, видео, музыки, причем часто не ограничиваясь одной папкой, а растаскивая одно и тоже содержимое по массе папок. В результате дисковое пространство стремительно сокращается, а у администратора появляется еще одна головная боль. Можно, конечно, бороться административными мерами, но как показывает практика - это малоэффективно.

Сразу перейдем к шаблонам. Там уже готовы настройки для блокирования основных типов "проблемных" файлов. Блокировка может быть активной, когда размещение данных типов файлов не допускается, или пассивной, когда об этом только уведомляется администратор. При необходимости можно создать свои шаблоны или отредактировать текущие. Определение того, что именно относится к тому или иному типу содержимого производится в разделе **Группы файлов**.



Как видим, файловые службы в Windows Server 2008 R2 это не только и не столько общие папки, за которыми в админской среде закрепилось меткое название "файлопомойка", а мощные средства контроля и управления, которые позволяют создать структурированное и управляемое файловое хранилище любых масштабов.

СОЗДАНИЕ И НАСТРОЙКА ГРУППОВЫХ ПОЛИТИК В ДОМЕНЕ

Групповые политики – это набор правил, обеспечивающих инфраструктуру, в которой администраторы локальных компьютеров и доменных служб Active Directory могут централизовано развертывать и управлять настройками пользователей и компьютеров в организации. Все настройки учетных записей, операционной системы, аудита, системного реестра, параметров безопасности, установки программного обеспечения и прочие параметры развертываются и обновляются в рамках домена при помощи параметров объектов групповой политики GPO (Group Policy Object).

I. Область действия групповых политик

Все групповые политики имеют свою область действия (scope), которая определяет границы влияния политики. Области действия групповых политик условно можно разделить на четыре типа:

Локальные групповые политики
Групповые политики, применяемые к локальному компьютеру, или локальные групповые политики. Эти политики настраиваются в оснастке «Редактор локальных групповых политик» и применяются только к тому компьютеру, на котором они были настроены. Они не имеют механизма централизованного развертывания и управления и, по сути, не являются групповыми политиками.

Групповые политики доменов
Объекты групповых политик, применяемые к домену Active Directory (AD) и оказывающие влияние на все объекты, имеющие отношение к данному домену. Поскольку в рамках домена работает механизм наследования, то все политики, назначенные на домен, последовательно применяются и ко всем нижестоящим контейнерам.

Групповые политики подразделения

Политики, применяемые к подразделению (Organizational Unit policy, сокр. OU) и оказывающие влияние на все содержимое данного OU и дочерних OU (при их наличии).

Групповые политики сайтов

Сайты в AD используются для представления физической структуры организации. Границы сайта определяются одной или несколькими IP-подсетями, которые объединены высокоскоростными каналами связи. В один сайт может входить несколько доменов и наоборот, один домен может содержать несколько сайтов. Объекты групповой политики, примененные к сайту AD, оказывают влияние на все содержимое этого сайта. Следовательно, групповая политика, связанная с сайтом, применяется ко всем пользователям и компьютерам сайта независимо от того, к какому домену они принадлежат.

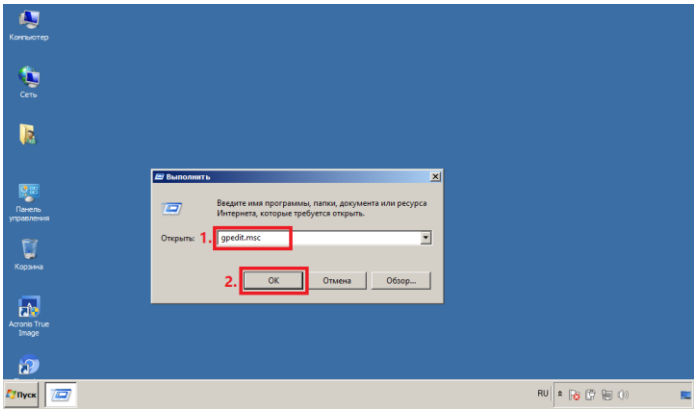
II. Порядок применения и приоритет групповых политик

Порядок применения групповых политик напрямую зависит от их области действия. Первыми применяются *Локальные политики*, затем *Групповые политики сайтов*, затем отрабатывают *Доменные политики* и затем *OU политики*. Если на одну OU назначено несколько GPO, то они обрабатываются в том порядке, в котором были назначены (Link Order).

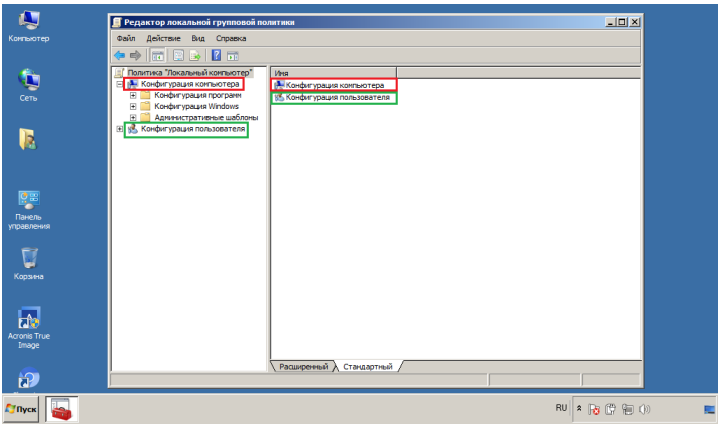
Приоритет GPO напрямую зависит от порядка их применения — ***чем позднее применяется политика, тем выше ее приоритет***. При этом нижестоящие политики могут переопределять вышестоящие — например *Локальная политика* будет переопределена *Доменной политикой сайта*, *Доменная политика — политикой OU*, а политика вышестоящего OU — *нижестоящими политиками OU*.

III. Создание локальной групповой политики

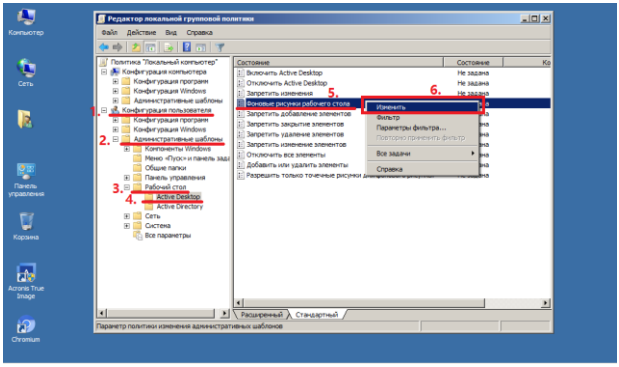
1. Для создания локальной групповой политики зайдите на рабочую станцию, нажмите **Пуск**, в поле поиска введите **Выполнить**, затем, в поисковой выдаче, выберите **Выполнить**. В открывшемся окне введите в поле **gpedit.msc**, затем нажмите **OK**



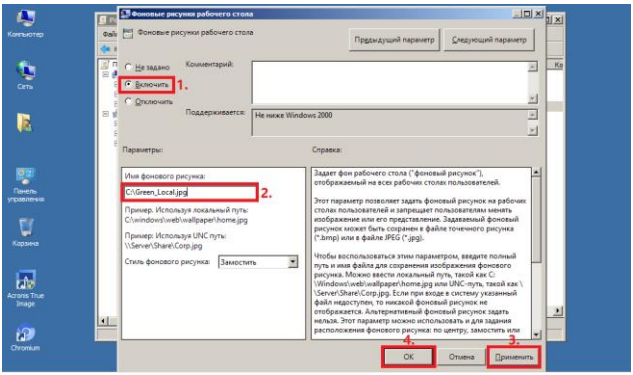
2. В открывшемся окне Вы увидите две основные категории параметров групповой политики — **параметры конфигурации компьютера** и **параметры конфигурации пользователя**. *Параметры конфигурации компьютера* применяются к компьютеру в целом, то есть действуют в отношении всех пользователей, входящих в систему на данном компьютере, без различия, гости они, пользователи или администраторы. *Параметры конфигурации пользователя* действуют только в отношении конкретно заданных пользователей



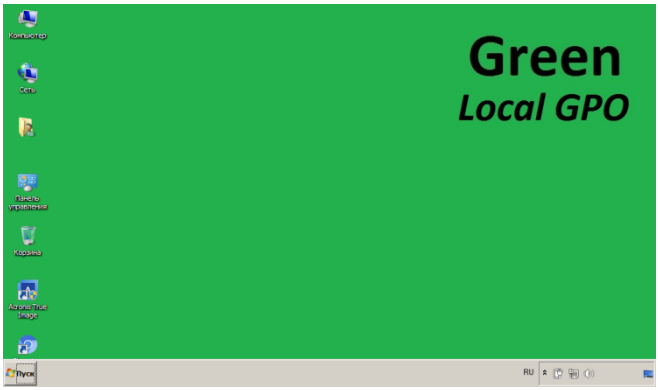
3. Выберите: **Конфигурация пользователя > Административные шаблоны > Рабочий стол > Active Desktop**. В правой колонке выберите **Фоновые рисунки рабочего стола** и нажмите **Изменить** (меню вызывается через правую кнопку мыши)



4. В появившемся окне выберите пункт **Включить**, затем в поле Имя фонового рисунка введите **путь к фоновому рисунку** (*прим. в данном примере это C:\Green_Local.jpg*), после чего нажмите **Применить** и **ОК**. Затем **перезагрузите компьютер**.

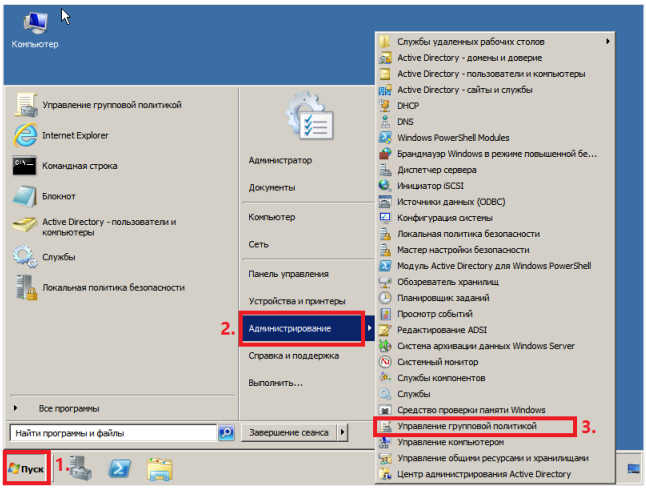


5. После перезагрузки компьютера Вы увидите, что политика отработала и фон рабочего изменился:

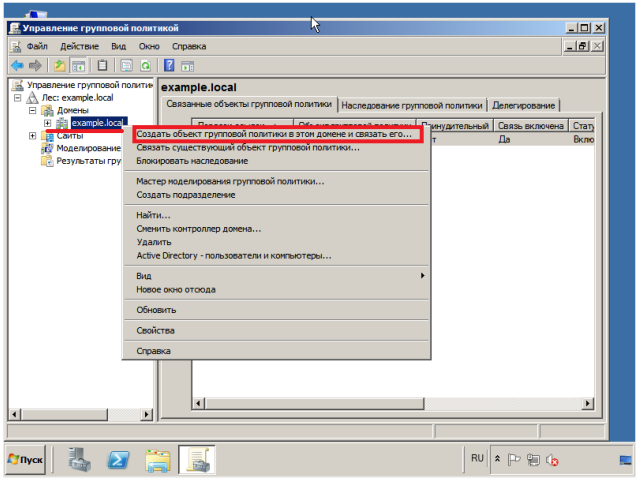


IV. Создание и настройка групповой политики на уровне домена

1. Для создания групповой политики на уровне домена зайдите на сервер, выберите **Пуск** > **Администрирование** > **Управление групповой политикой**:

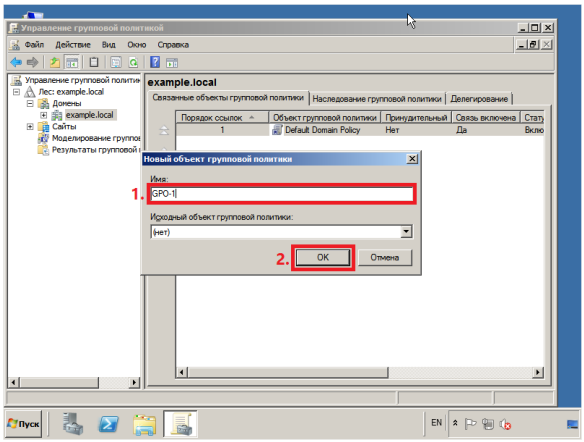


2. Выберите домен (*прим. в данном руководстве это example.local*), через правую кнопку мыши вызовите меню, в котором выберите **Создать объект групповой политики в этом домене и связать его…**

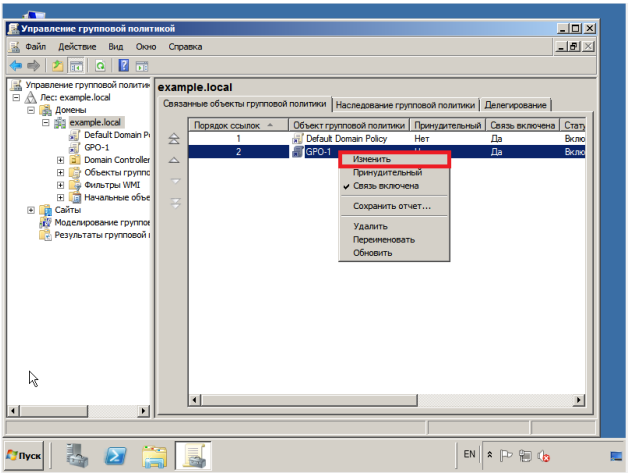


3. В появившемся окне выберите, в соответствующем поле, имя новой групповой политики (*прим. в данном руководстве это GPO-*

1), затем нажмите **ОК**

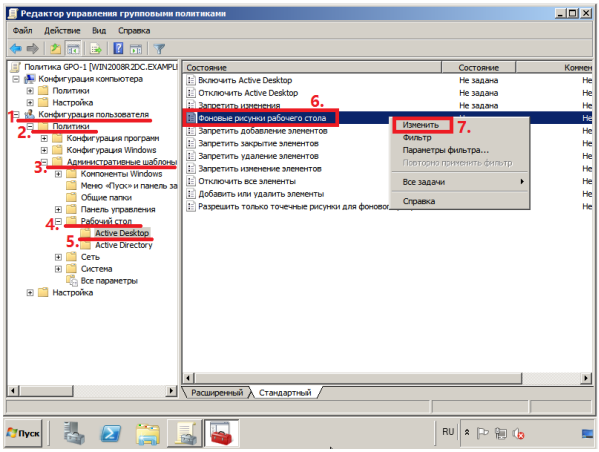


4. Выберите созданную групповую политику (*прим. GPO-1*), через правую кнопку мыши вызовите меню, в котором выберите **Изменить**

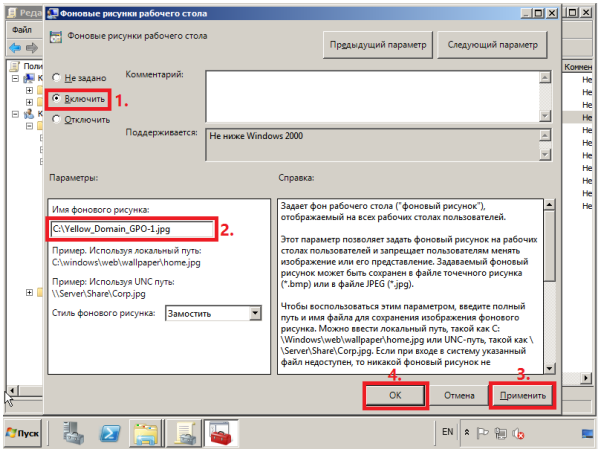


5. Выберите: **Конфигурация пользователя** > **Политики** > **Административные шаблоны** > **Рабочий стол** > **Active Desktop**. В правой колонке выберите **Фоновые рисунки рабочего стола** и

нажмите **Изменить** (меню вызывается через правую кнопку мыши)



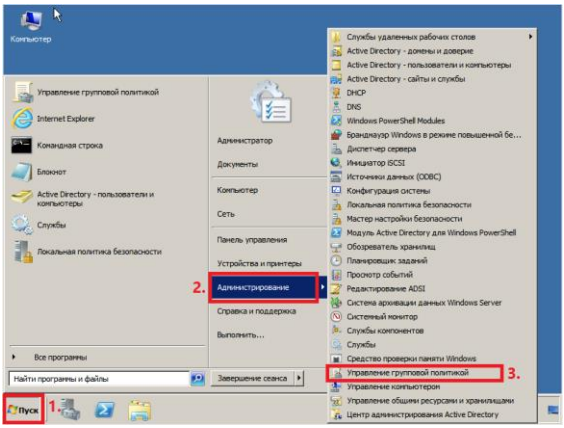
6. В появившемся окне выберите пункт **Включить**, затем в поле Имя фонового рисунка введите **путь к фоновому рисунку** (*прим. в данном примере это C:\Yellow_Domain_GPO-1.jpg*), после чего нажмите **Применить** и **ОК**. Затем **перезагрузите компьютер** на котором ранее устанавливали локальную групповую политику



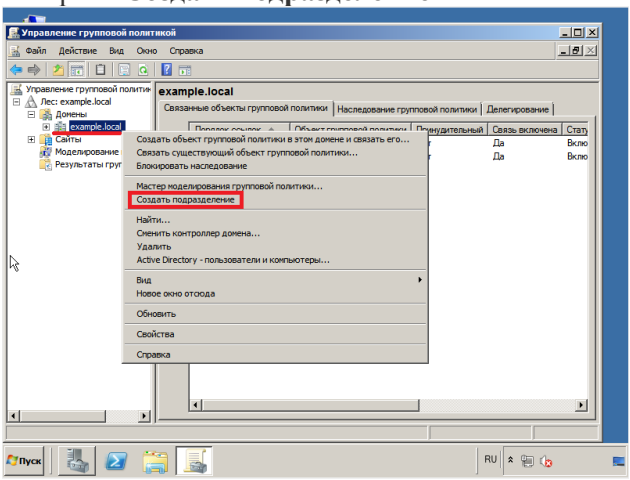
7. После перезагрузки компьютера Вы увидите, что групповая политика домена отработала и фон рабочего стола на компьютере изменился (*Т.о. установленный локальной политикой зеленый фон был переопределён и, в соответствии с доменной политикой, стал жёлтым*)

V. Создание и настройка групповой политики на уровне подразделения

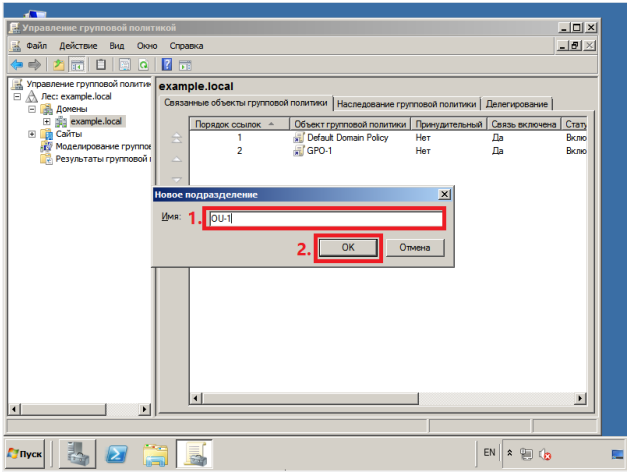
1. Для создания групповой политики на уровне подразделения (Organizational Unit policy, сокр. OU) зайдите на сервер, выберите **Пуск** > **Администрирование** > **Управление групповой политикой**



2. Выберите домен, через правую кнопку мыши вызовите меню, в котором выберите **Создать подразделение**.

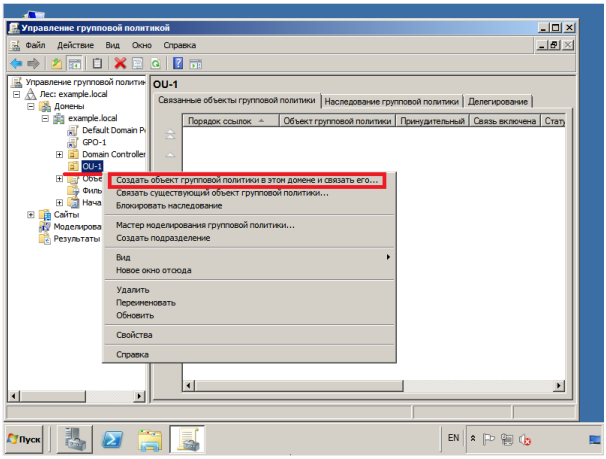


3. В появившемся окне выберите, в соответствующем поле, имя нового подразделения, затем нажмите **ОК**

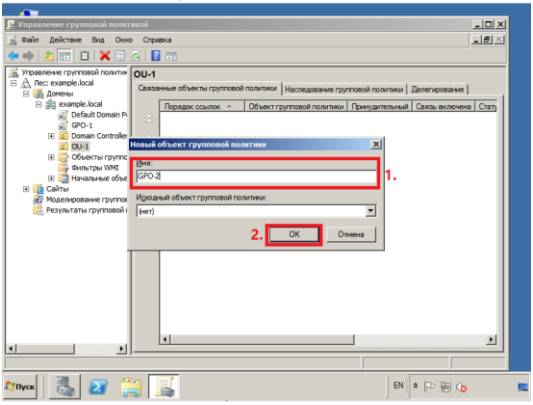


4. Выберите созданное подразделение (*прим. OU-1*), через правую кнопку мыши вызовите меню, в котором выберите **Создать объект**

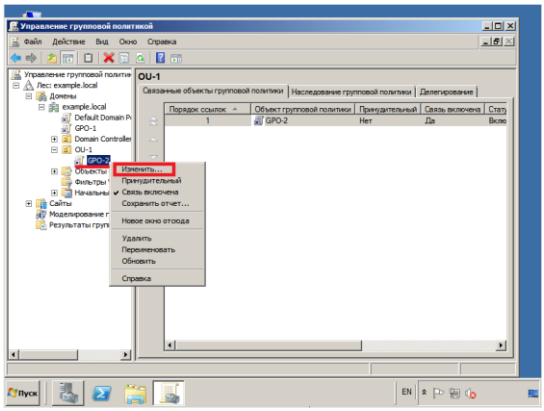
групповой политики в этом домене и связать его…



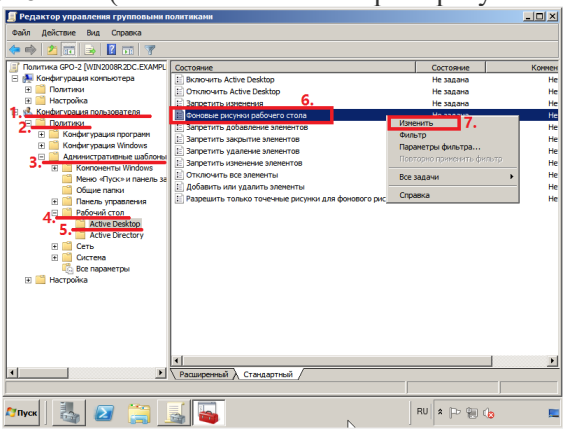
5. В появившемся окне выберите, в соответствующем поле, имя новой групповой политики, затем нажмите **ОК:**



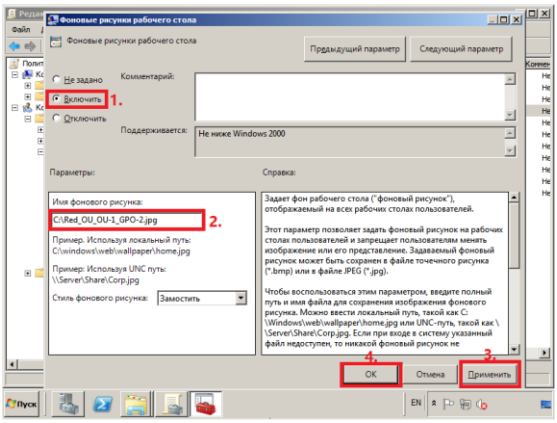
6. Выберите созданную групповую политику (*прим. GPO-2*), через правую кнопку мыши вызовите меню, в котором выберите **Изменить**



7. Выберите: **Конфигурация пользователя** > **Политики > Административные шаблоны > Рабочий стол > Active Desktop**. В правой колонке выберите **Фоновые рисунки рабочего стола** и нажмите **Изменить** (меню вызывается через правую кнопку мыши)



8. В появившемся окне выберите пункт **Включить**, затем в поле Имя фонового рисунка введите **путь к фоновому рисунку** (*прим. в данном примере это Red_OU_OU-1_GPO-2.jpg*), после чего нажмите **Применить** и **ОК**. Затем **перезагрузите компьютер** на котором ранее устанавливали локальную групповую политику (*прим. на этом же компьютере она была переопределена доменной групповой политикой*)

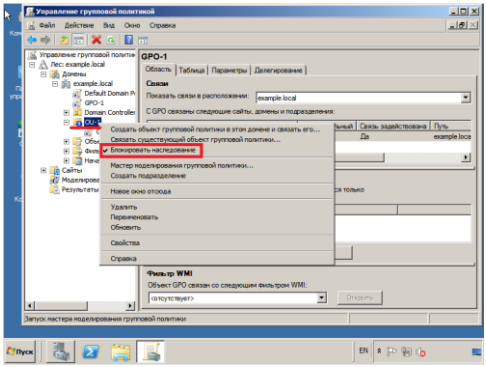


9. После перезагрузки компьютера Вы увидите, что доменная политика (GPO-1) переопределена политикой (GPO-2), назначенной на OU.

VI. Наследование в групповых политиках

1. На все политики в домене распространяется наследование, т.е. политики, назначенные на родительский контейнер (домен или OU), последовательно применяются ко всем дочерним контейнерам. При необходимости это можно изменить, отключив наследование для отдельно взятого OU. Для этого необходимо перейти в управление групповой, выбрать нужное OU, кликнуть на нем правой клавишей мыши и в контекстном меню отметить пункт **Блокировать наследование**.

После этого для данного OU и его дочерних OU (при их наличии) отменяется воздействие всех вышестоящих политик:



VII. Форсирование применения групповых политик

1. Форсирование применения групповых политик применяется тогда, когда данная политика должна отработать независимо от остальных политик.

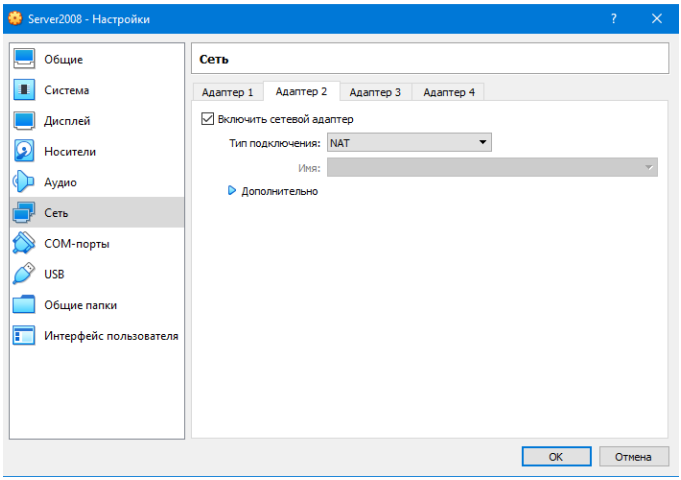
Если политика форсирована, то, вне зависимости от своей области действия она получает наивысший приоритет. Это значит, что ее настройки не могут быть переопределены нижестоящими политиками, а также на нее не действует отмена наследования.

Чтобы форсировать политику, необходимо перейти в управление групповой политикой (*прим. Пуск > Администрирование > Управление групповой политикой*), выбрать нужную политику (*прим. в данном руководстве это GPO-1*), кликнуть на ней правой клавишей мыши и в контекстном меню отметить пункт **Принудительный**.

ОРГАНИЗАЦИЯ ОБЩЕГО ДОСТУПА В ИНТЕРНЕТ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОГО ПРОКСИ-СЕРВЕРА

Администрирование доступа в интернет является одной из важных задач для больших организаций. Необходимость этого вызвана задачами обеспечения безопасности вашей сети, блокировки каких либо сайтов (социальные сети, сайты азартных игр и т.п.) для всех, либо для конкретной группы пользователей. Фильтрация контента является одной из самых распространенных функций прокси-серверов.

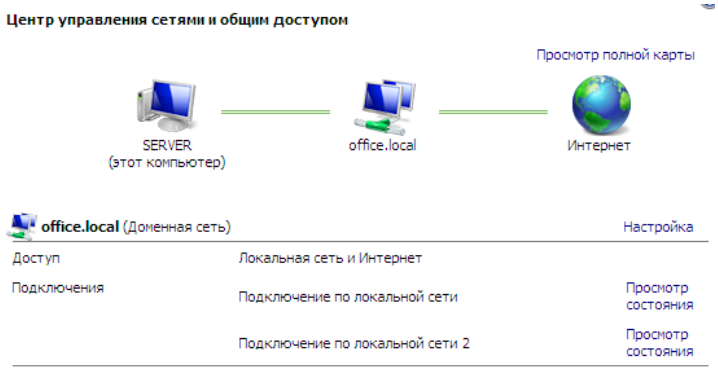
Для работы нам понадобится канал интернета, подключенный к нашей виртуальной машине. Для этого при выключенной виртуальной машине зайдем в сетевые настройки:



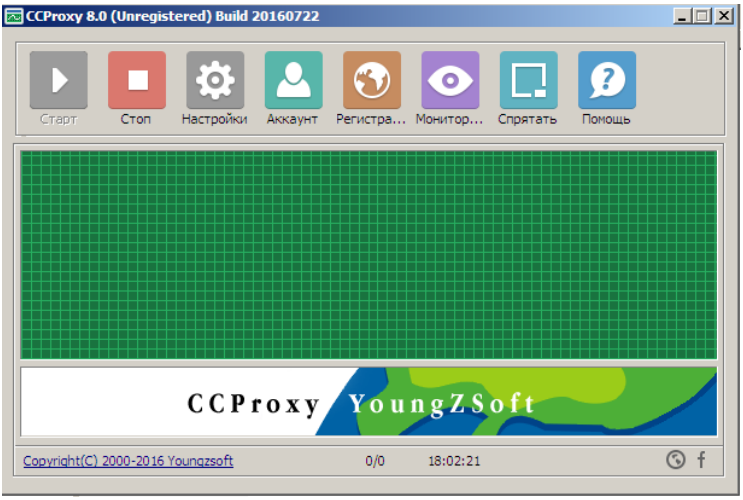
Здесь необходимо включить Адаптер 2 и выбрать тип подключения NAT. После этой операции в виртуальной машине появляется возможность выхода в сеть интернет.

В качестве примера установим прокси-сервер CCProxy на нашу серверную машину. Данное программное обеспечение бесплатно (ограничивается в бесплатной версии только число пользо-

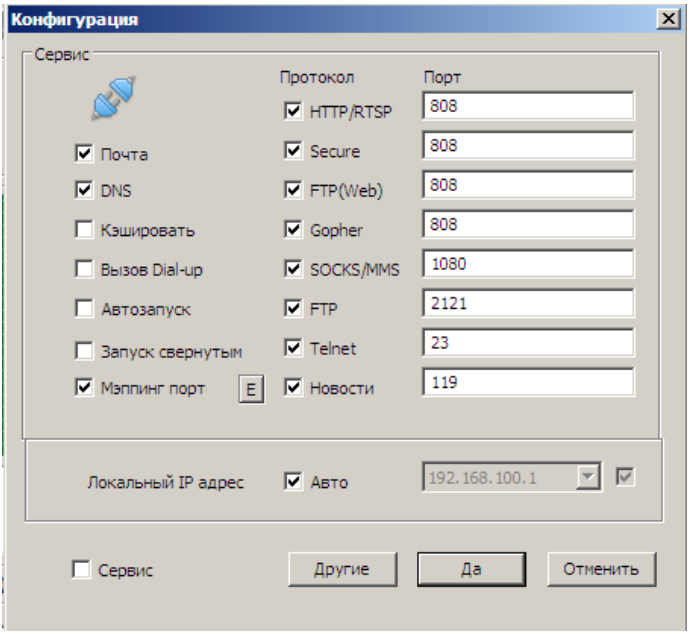
вателей) и вы можете его скачать прямо с сайта производителя: https://www.youngzsoft.net/ccproxy/
Убеждаемся, что наш сервер теперь имеет выход в интернет:



Процесс установки CCProxy не вызывает сложности: запускаем установочный пакет и кликаем несколько раз на клавишу **Next.** Основное окно программы после установки выглядит таким образом:

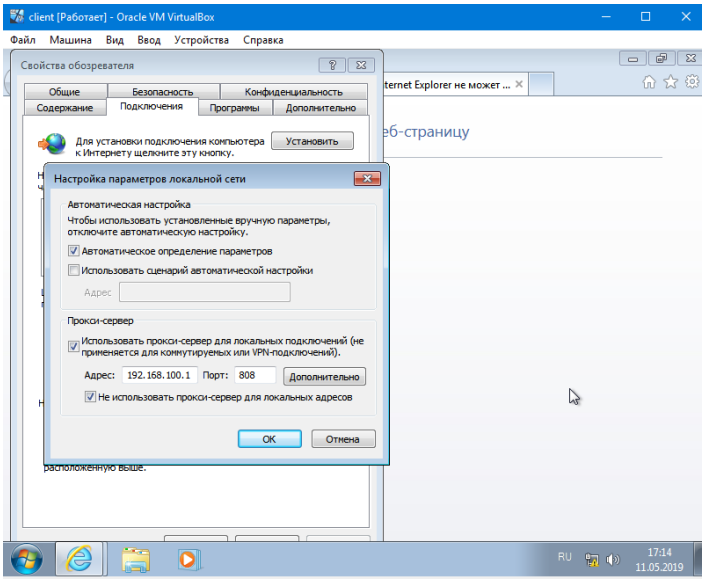


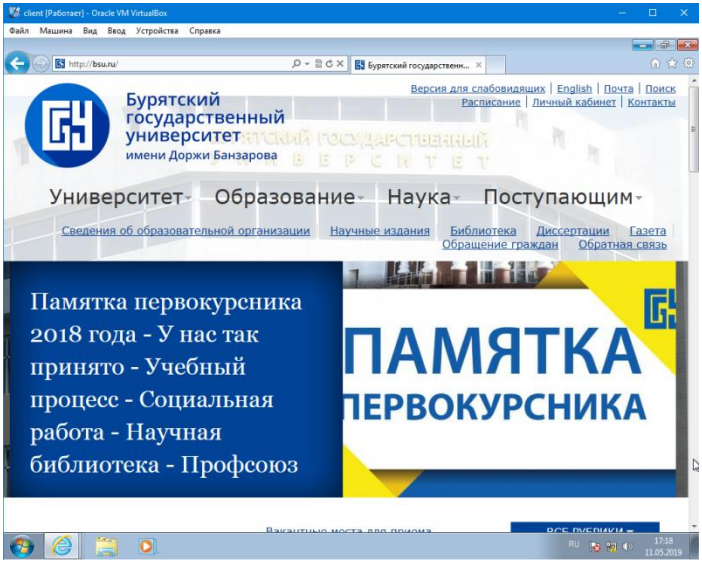
Нажимаем на кнопку **Настройки:**



При необходимости вы можете изменить порты, используемые программой, либо отключить ненужные протоколы (снять галочки).

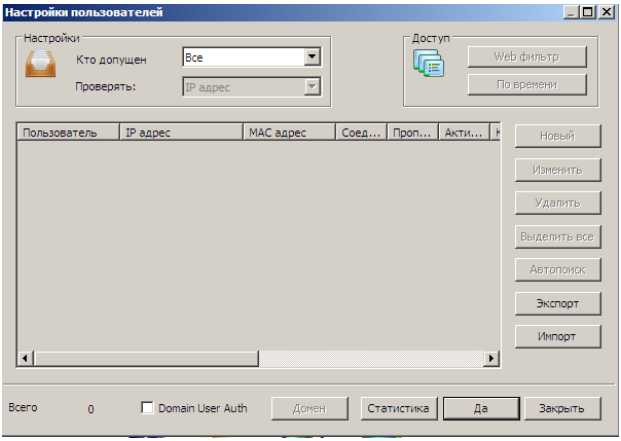
По умолчанию прокси-сервер уже работает. Пользователи локально-вычислительной сети, у которых в настройках браузера указан IP адрес сервера и порт, используемый CCProxy, уже могут пользоваться интернетом. Для того, чтобы на клиентской машине прописать верные настройки необходимо сделать следующие операции: Запустить браузер, зайти в его настройки, найти настройки прокси-сервера и прописать туда IP **192.168.100.1** и порт **808** (в нашем случае).





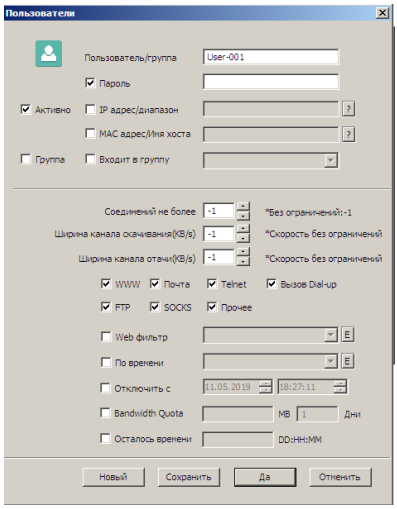
Поздравляем, интернет на клиентской машине работает!

Если мы хотим, чтобы доступ в интернет был не у всех, а у избранных пользователей, то нужно внести дополнительные настройки. Для этого нужно нажать на кнопку **«Аккаунт»:**



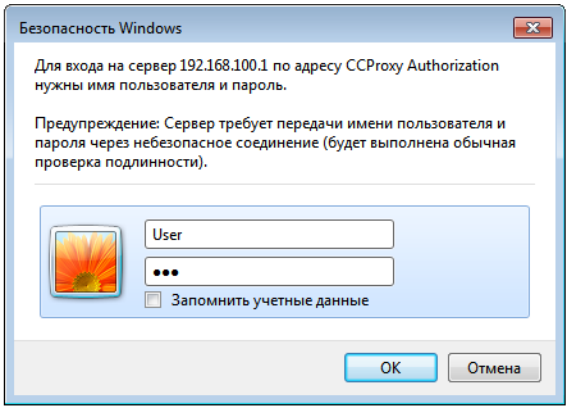
Напротив строчки **Кто допущен** выберем **Указанные**, а в **Проверять – Логин/Пароль.**

Станет доступной кнопка **Новый**. При нажатии на нее появится следующее окно:



В этом окне нужно указать имя пользователя, его пароль. При необходимости можно установить ограничения для этого пользователя – ограничить скорость соединения, включить web-фильтр (список хостов, которые можно или нельзя посещать данному пользователю), временной график, ограничить объем используемого трафика.

В итоге на клиентской машине при попытке выйти в интернет будет выскакивать диалоговое окно:



Пользователь в этом окне вводит свой логин и пароль и получает доступ в интернет согласно тем правилам, которые установил администратор для этого аккаунта.

ПРИМЕР ИТОГОВОГО КОНТРОЛЬНОГО ЗАДАНИЯ ПО ТЕМЕ

1. В организацию, в которой вы работаете системным администратором, устроился новый сотрудник в отдел маркетинга. Необходимо создать пользовательскую среду для нового сотрудника:

- Учетную запись пользователя в домене. Добавить в группу пользователей "Маркетинг".

- Доступ на файловый сервер (в папку "Для всех" с правом на чтение и "Маркетологи" с полным доступом).

- Предоставить доступ в сеть интернет с ежемесячным лимитом в 500 Мб трафика. Ограничить доступ в социальные сети "Вконтакте" и "Одноклассники".

2. Средствами управления групповой политикой запретить на компьютерах, объединенных в группу "Маркетинг", запуск браузеров Opera и Google Chrome.

Библиографический список

1. Администрирование структурированных кабельных систем/Семенов А.Б.. —Москва: ДМК Пресс, 2009
Режим доступа:
http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1145 2.

2. Администрирование VMware vSphere/М. О. Михеев. — Москва: ДМК Пресс, 2012. —504 с. Режим доступа:
http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=9124

3. Интеллектуальные информационные системы и технологии: учебно-методическое пособие для студентов направления подготовки 09.03.02 Информационные системы и технологии/М-во образования и науки Рос. Федерации, Бурят. гос. ун-т; сост. Т. С. Цыбикова ; рец. Н. С. Хитерхеева. —Улан-Удэ: Изд-во Бурятского 3 госуниверситета, 2015. —94, [1] с.

4. Хагеман С. SAP R/3 : системное администрирование /С. Хагеман, Л. Вилл. —М.: Лори, 2010. —460 с. 3. О'Брайен Д. Администрирование Microsoft IIS 5/Д. О'Брайен. —М.: Вильямс, 2001. — 462 с.

5. Назаров С. В. Администрирование локальных сетей Windows NT: Учеб.пособие для вузов по спец."Прикл.информатика"/С. В. Назаров. —М.: Финансы и статистика, 2001. —329 с.

Оглавление