# Практическое занятие №2. Защита информации в сети с контроллером домена.

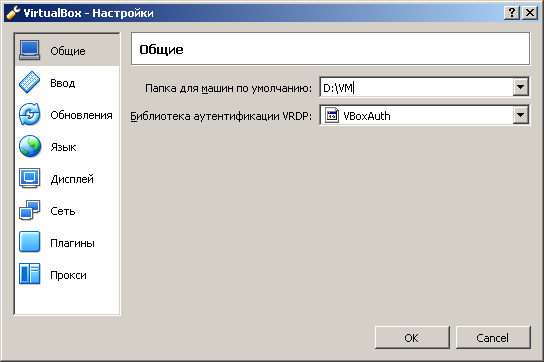
Задание №1. Установка Windows Server.

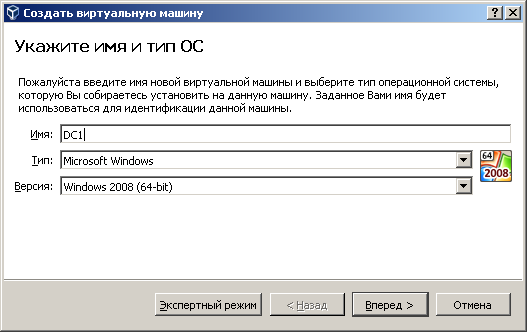
Сценарий.

Вам поручена начальная инсталляция (установка) и настройка нового сервера. Инсталляцию необходимо выполнить с DVD-диска. Когда установка будет завершена, выполните настройки, которые нужно выполнить после установки, в соответствии с прилагаемой документацией. Кроме того, требуется настроить параметры запуска для некоторых служб и тестировать новый драйвер устройства на предмет надлежащей функциональности.

Для установки нового сервера используйте следующие параметры установки:

* Язык: Русский
* Формат времени и денежных единиц: Русский (Россия)
* Раскладка клавиатуры или метод ввода: США
* Продукт: Windows Server 2008 R2 Standard (полная установка)
* Пароль администратора: P@ssw0rd
* Параметры настройки после установки: Часовой пояс: (UTC+03:00)
* IP-адрес: 192.168.100.10
* Маска подсети: 255.255.255.0
* Шлюз: 192.168.100.1
* DNS-серверы: 192.168.100.10 и 127.0.0.1
* Имя сервера: DC19521 или DC195212

*Запустите Oracle VM VirtualBox. Для этого выполните команды Пуск 🡺 Все программы 🡺 папка Oracle VM VirtualBox 🡺 Oracle VM VirtualBox. Установите расположение размещение папки для виртуальных машин D:\VMномер группы без знака «-«. Например: D:\VM9521 или D:\VM9522. Во время самоподготовки можно будет проработать задания практического занятия. Для этого выполните Файл 🡺 Настройки 🡺 D:\VM9521 или D:\VM9522.*

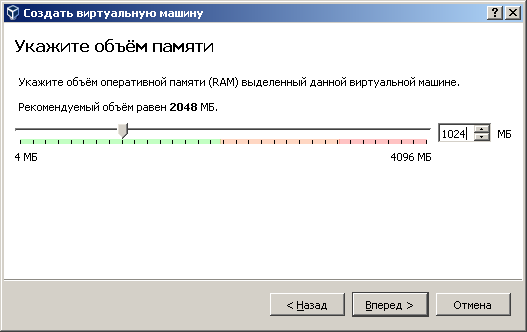
**

*Создать виртуальную машину 🡺 Имя DC19521 (DC19522) , Тип: Microsoft Windows 🡺 Версия : Windows 2008 (64-bit) 🡺Вперед.*

**Прочтите внимательно:**

Для работы с Windows Server 2008 R2 компьютер должен удовлетворять следующим требованиям.

|  |  |
| --- | --- |
| **Компонент** | **Требование** |
| Процессор | 1,4 ГГц (процессор с архитектурой x64).  *Примечание. Для работы с Windows Server 2008 R2 for Itanium-Based Systems необходим процессор Intel Itanium 2.* |
| Память | Минимальный объем: 512 МБ.  Максимальный объем: Foundation — 8 ГБ, Standard — 32 ГБ, Enterprise, Datacenter и Itanium-Based Systems — 2 ТБ. |
| Требования к свободному пространству на диске | Минимальный объем: 32 ГБ.  Windows Server 2008 R2 Foundation — 10 ГБ или более.  Windows Server 2008 R2 Foundation предназначена для небольших организаций, где рассматривается приобретение первого сервера или уже используется клиентская операционная система (например, Windows 7/XP) для обеспечения базовой инфраструктуры. Это недорогая, удобная в развертывании и надежная платформа, на которой можно запускать распространенные бизнес-приложения и обеспечивать общий доступ к информации и ресурсам. Windows Server 2008 R2 Foundation основан на Windows Server 2008 R2 и сможет обеспечить все ключевые элементы ИТ в Вашем бизнесе: совместная работа с файлами и принтерами, удаленный доступ, безопасность ИТ среды.  Однако Windows Server 2008 R2 Foundation имеет ограничения по количеству клиентских подключений и не поддерживает функции виртуализации.  *Примечание. На компьютерах, оснащенных более чем 16 ГБ ОЗУ, потребуется больше места на диске для файлов подкачки, спящего режима и дампа памяти.* |
| Монитор | Монитор с разрешением Super VGA (800x600) или более высоким. |
| Прочее | Дисковод для DVD-дисков, клавиатура и мышь (Microsoft) или совместимое указывающее устройство, доступ в Интернет (может предоставляться за дополнительную плату). |

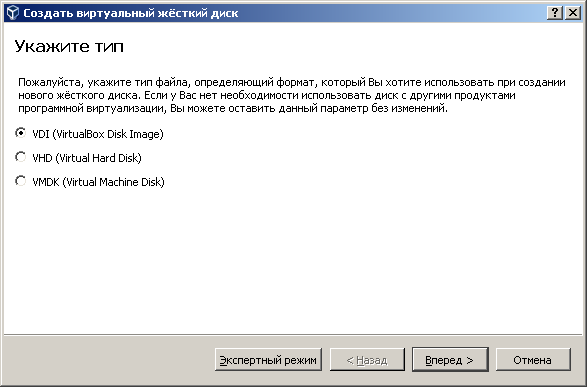
Фактические требования к системе зависят от конфигурации системы и от выбранных для установки приложений и компонентов. Производительность процессора зависит не только от его тактовой частоты, но и от числа ядер и объема кэша процессора. Необходимый объем свободного дискового пространства в системном разделе указан приблизительно. При установке по сети может потребоваться дополнительное место на диске.

*Задать объем оперативной памяти 1024 Мб 🡺 Вперед 🡺Создать новый диск 🡺 Создать.*

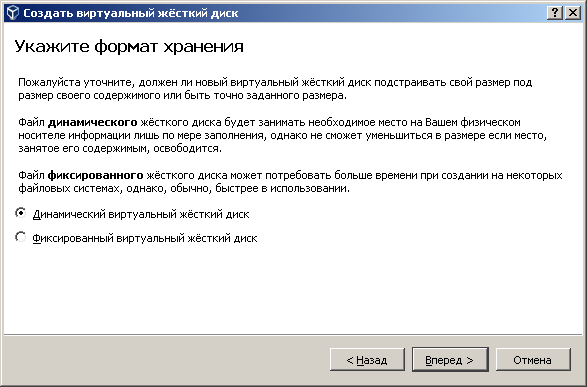
Запустить виртуальную машину DC19521 (DC19522).

*Далее в описании используется DC1. При выполнении DC1 = DC1*

*Оставить тип диска VDI.*

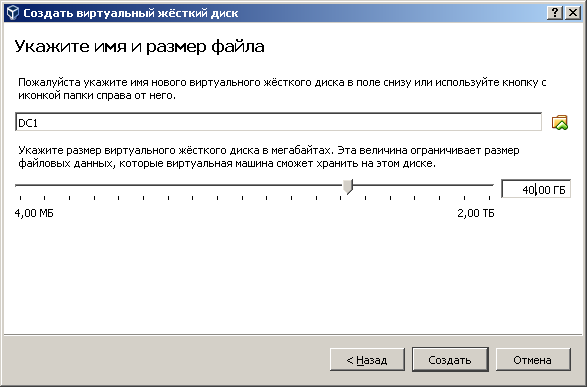


*Выбираем динамический виртуальный диск.*

Виртуальные диски могут быть, как фиксированного размера, так и динамически выделяемого, причем VirtualBox позволяет увеличить размер дискового пространства, независимо от объёма и формата диска и даже в том случае, если диск содержит данные. При выборе динамически выделяемого образа, файл контейнера будет «разрастаться» постепенно, по мере заполнения секторов данными, до тех пор, пока размер контейнера не достигнет указанного при создании виртуальной машины лимита.

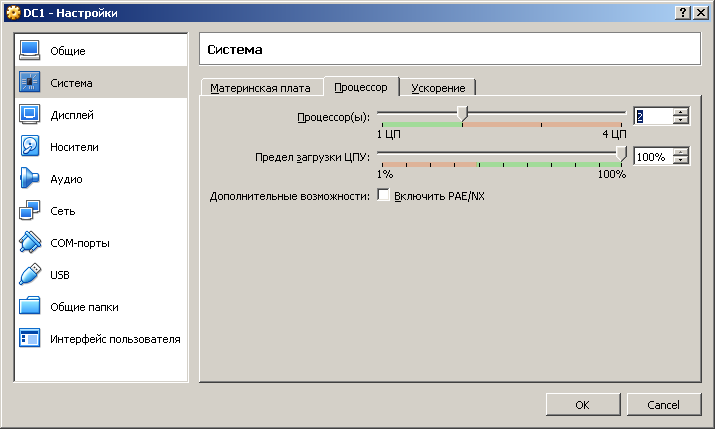
Учитывая то, что в процессе регулярного увеличения размера контейнера задействуются дополнительные вычислительные ресурсы, скорость записи при использовании опции с фиксированным размером, как правило выше, в с равнении с динамическим диском. Тем не менее, если размер динамического диска в долгосрочной перспективе значительно не увеличивается, то разница в скорости записи практически нивелируется.

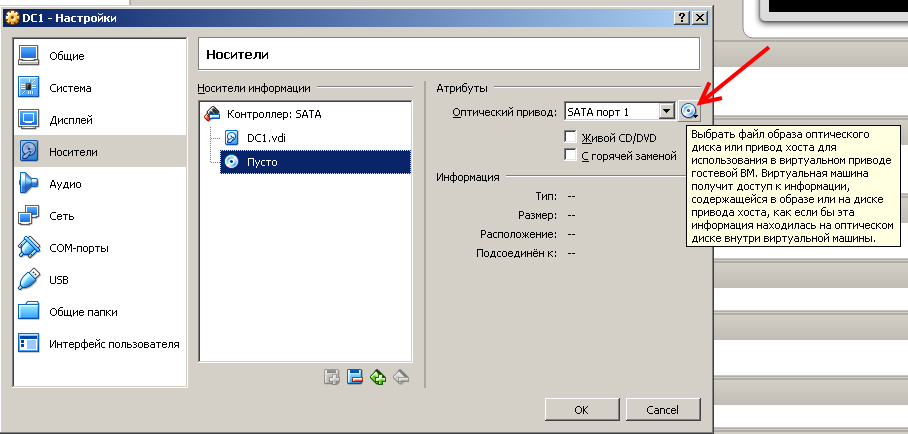
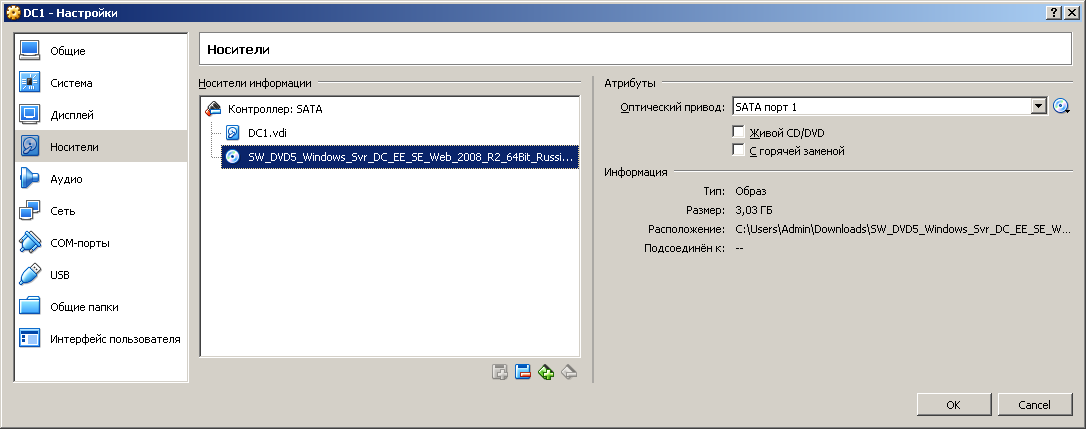
Установить размер жесткого диска (HDD) 40 Гб.



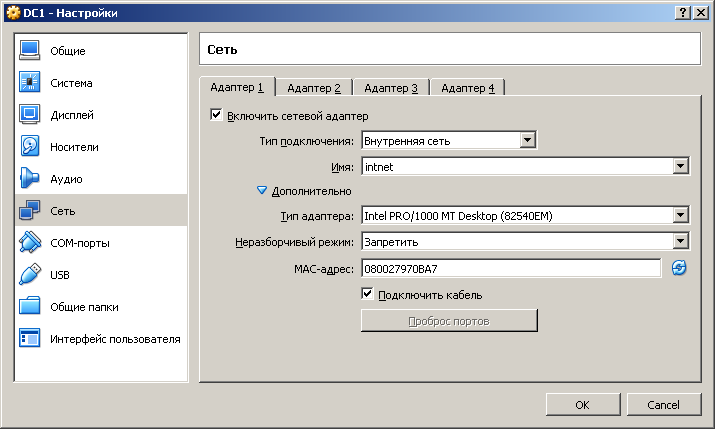
ПКМ (Клик Правой кнопки мыши) по виртуальной машине DC1 🡺 Настроить 🡺

Система 🡺 Процессоры 🡺Выбрать 2 процессора.



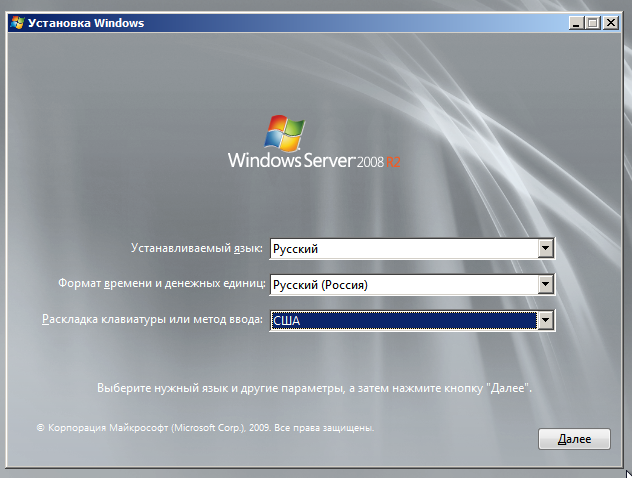
Носители 🡺 Выбрать образ дистрибутива Windows Server 2008 R2 SW\_DVD5\_Windows\_Svr\_DC\_EE\_SE\_Web\_2008\_R2\_64Bit\_Russian\_w\_SP1\_MLF\_X17-22616.iso из папки D:\ISO 🡺 ОК

*Выберите тип подключения «Внутренняя Сеть».*

Режим ***«Внутренняя сеть»*** похож на режим ***«Сетевой мост»*** в котором ВМ может связываться с внешним миром. Однако, "внешний мир" ограничен другими виртуальными машинами на том же хосте и которые подключены к той же внутренней сети.

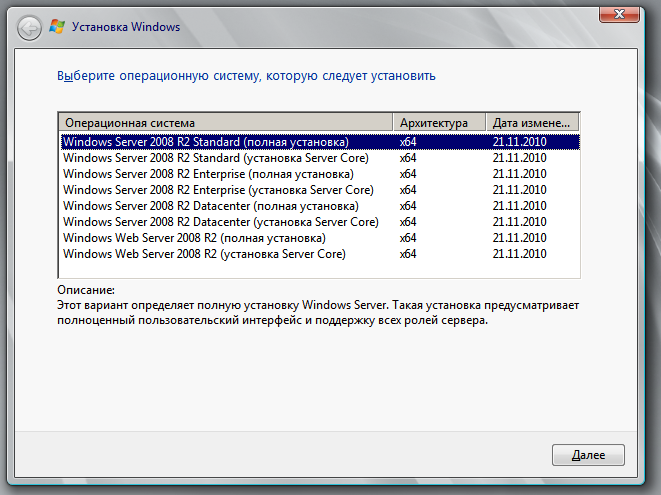
Хотя с технической стороны, все что можно сделать используя режим внутренняя сеть , можно также сделать в режиме сетевого моста, но в режиме внутренней сети есть преимущества в безопасности. В режиме моста, весь трафик проходит через физический интерфейс хоста. Поэтому возможно подключение анализаторов пакетов (например, Wireshark) к интерфейсу хоста и сбор всего трафика проходящего через него. Если по каким либо причинам Вам необходимо чтобы две и более виртуальные машины имели защищенное соединение, скрывая свои данные от хост системы и других пользователей, то режим сетевой мост не является лучшим выбором. В разделе «Дополнительно» автоматически назначается MAC-адрес сетевой карты.

**MAC-адрес (от англ. Media Access Control — управление доступом к среде, также Hardware Address) — уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet.**

При проектировании стандарта Ethernet было предусмотрено, что каждая сетевая карта (равно как и встроенный сетевой интерфейс) должна иметь уникальный шестибайтный номер (MAC-адрес), «прошитый» в ней при изготовлении. Этот номер используется для идентификации отправителя и получателя фрейма; и предполагается, что при появлении в сети нового компьютера (или другого устройства, способного работать в сети) сетевому администратору не придётся настраивать этому компьютеру MAC-адрес вручную.

*Запустить ВМ DC1 и начать установку Windows Server 2008 R2. В окне «Установка Windows» задать параметры, указанные выше.*

*В следующем окне выбрать Windows Server R2 Standart (полная установка) 🡺 Далее 🡺 Я принимаю условия лицензии 🡺 Далее*

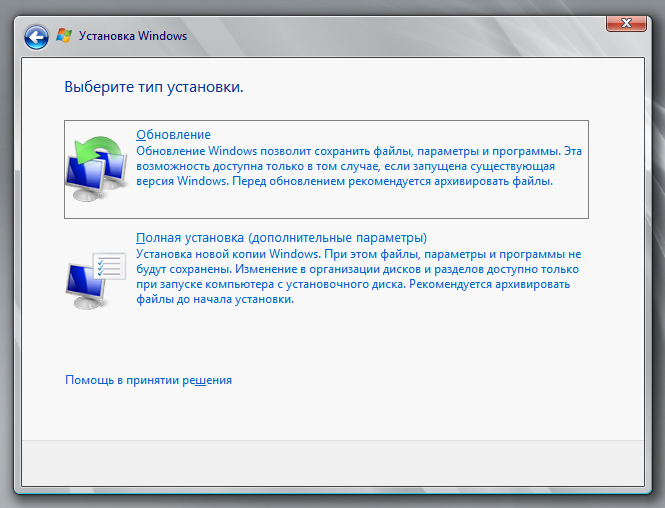
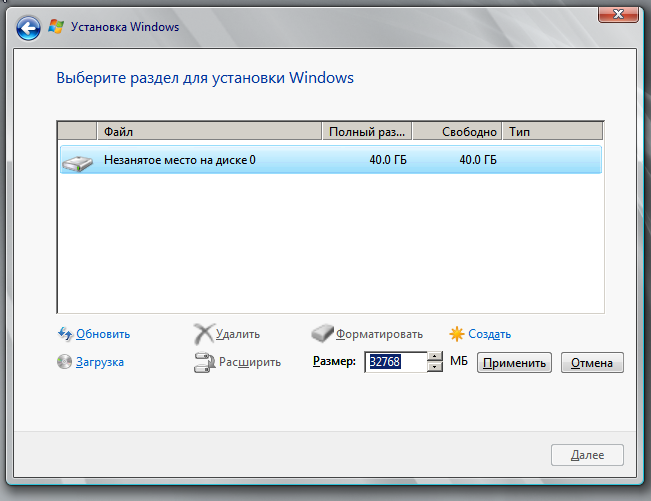
Windows MultiPoint Server — упрощенный терминальный сервер Windows, вариант реализации терминальной службы Remote Desktop Services, предназначенный для образовательных учреждений.

Windows MultiPoint Server был выпущен в 2010 г, версия Windows MultiPoint Server 2010 была основана на ОС Windows Server 2008 R2, однако, в отличие от Windows Server 2008, в качестве клиентских устройств используются не «классические» тонкие клиенты, подключаемые по Ethernet, а специализированные устройства, подключаемые по шине USB.

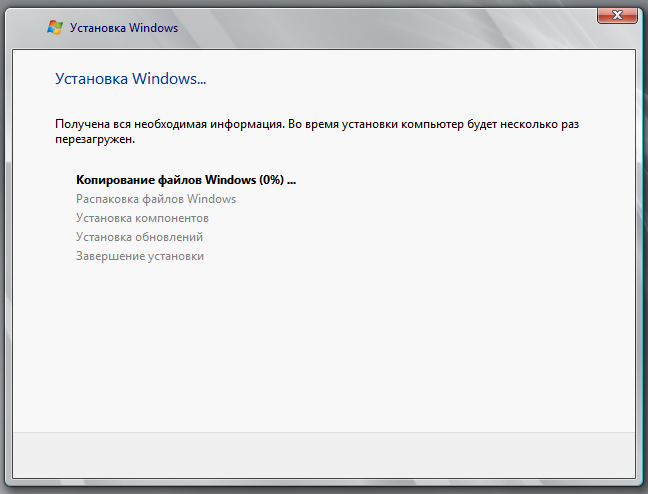
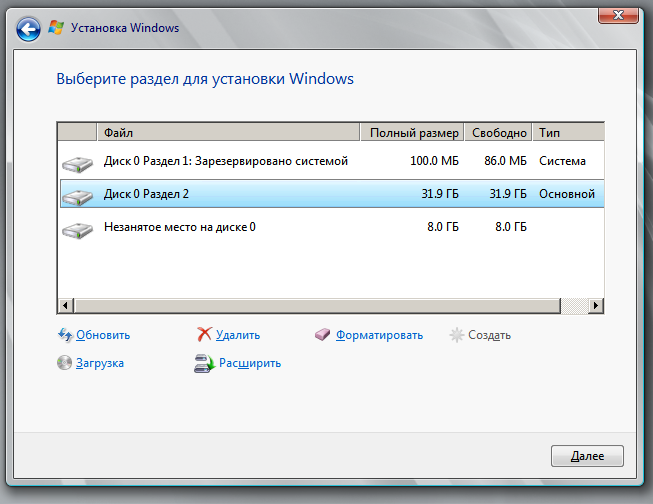
Другой особенностью MultiPoint Server является упрощенный, по сравнению с Windows Server, административный интерфейс.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Технические характеристики | MultiPoint Server (ОЕМ) | Windows Server 2008 R2 Foundation | Windows Server 2008 R2 Standard | Windows Server 2008 R2 Enterprise | Windows Server 2008 R2  Datacenter |
| Количество CPU | 1 | 1 | 4 | 8 | 64 |
| Объем ОЗУ | 8 Гб | 8 Гб | 32 Гб | 2 ТБ | 2 ТБ |
| Количество подключений для удаленного управления (Remote Desktop) | Нет | 2 | 2 | 2 | 2 |
| Кол-во CAL (Max)  (CAL - Client Access License, Клиентская лицензия) | 10 | Не требуются Ограничено подключением до 15 пользователей | Без ограничений | Без ограничений | Без ограничений |
| Кол-во терминальных лицензий (Max) | Нет | 15 | Без ограничений | Без ограничений | Без ограничений |
| Сетевые подключения (IAS) | Нет | 10 | 50 | Без ограничений | Без ограничений |
| Поддержка виртуализации | Нет | Нет | Лицензия на 1 физическую машину + лицензия на 1 виртуальную машину | Лицензия на 1 физическую машину + лицензия на 4 виртуальных машины. При использовании 4 виртуальных машин - на физической машине роль только Hyper-V. | Лицензия на 1 физическую машину + лицензия на неограниченное количество виртуальных машины. |

*Выберите тип установки «Полная установка». Настройка диска. Создать. Задать размер диска 32768 МБ 🡺 Применить 🡺 ОК.*

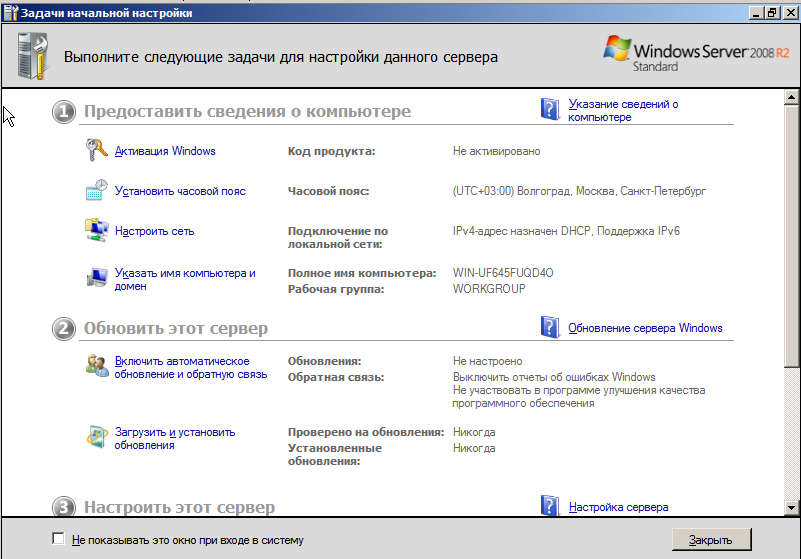
 

*Далее. Началась установка Windows.*



По окончанию установки смените пароль локальной учетной записи «Администратор» на P@ssw0rd 🡺 OK

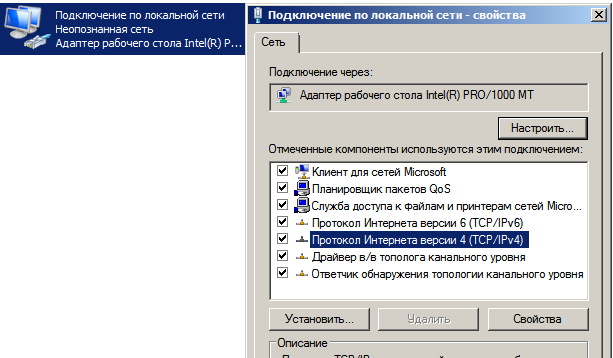
Задание №2. Настройка сетевого интерфейса. Изменение имени компьютера.

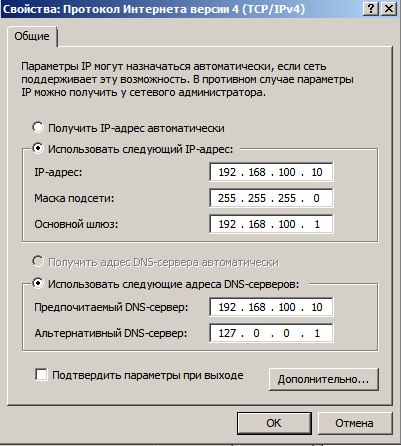
*В окне «Задачи начальной настройки» выберите задачу «Настроить сеть».*

Откроется окно «Сетевые подключения» (СП).

*Закройте окно СП.*

*Откройте окно СП через «Панель управления» 🡺 Сеть и Интернет\Центр управления сетями и общим доступом 🡺 Изменение параметров адаптера.*

*Щелкните ПКМ по «Подключение по локальной сети» и откройте свойства Протокола Интернета версии 4 (TCP/IPv4).*

**

*Настройте параметры IP согласно парметрам установки, указанным в Задании №1.*

*Проверьте настройки сетевой карты с помощью*

*команды msconfig/all. Задайте имя компьютера DC1 и рабочую группу WG. Перезагрузите ВМ DC1 для принятия настроек.*

## Задание 3. Создание и настройка рабочей станции WS71.

*Создайте ВМ WS9521 (WS9522) со следующими параметрами:*

* Формат времени и денежных единиц: Русский (Россия)
* Раскладка клавиатуры или метод ввода: США
* Продукт: Windows 7 Professional 64 bit
* Пароль учетной записи Администратор: P@ssw0rd
* Параметры настройки после установки: Часовой пояс: (UTC+03:00)
* IP-адрес: 192.168.100.100
* Маска подсети: 255.255.255.0
* Шлюз: 192.168.100.1
* DNS-серверы: 192.168.100.10
* Имя рабочей станции: WS9521 (WS9522). Далее WS=WS9521 или WS9522
* Рабочая группа: WG
* ОЗУ: 1 Gb
* HDD: 30 Gb
* Сеть 🡺 Тип Подключения 🡺 Внутренняя сеть

## Задание 4. Использование диагностических утилиты TCP/IP.

*После прочтения материала про диагностические утилиты TCP/IP, выполнить команды:*

*Ipconfig /all ; arp –a ; ping 192.168.100.10 ; ping –t 192.168.100.10 ; pathping DC1 ; netstat –a ; nbtstat –n.*

Любая операционная система имеет набор диагностических утилит для тестирования сетевых настроек и функционирования коммуникаций. Большой набор диагностических средств есть и в системах семейства Windows (как графических, так и режиме командной строки).

Перечислим утилиты командной строки, являющиеся инструментами первой необходимости для проверки настроек протокола TCP/IP и работы сетей и коммуникаций. Название TCP/IP происходит из двух наиважнейших протоколов семейства — Transmission Control Protocol (TCP) и Internet Protocol (IP). Подробное описание данных утилит содержится в системе интерактивной помощи Windows. В Таблице укажем основные и наиболее часто используемые параметры этих команд и дадим их краткое описание.

|  |  |  |
| --- | --- | --- |
| **Название утилиты** | **Параметры** | **Комментарии** |
| ipconfig | /? - Отобразить справку по команде  /all - Отобразить полную информацию о настройке параметров всех адаптеров  /release - Освободить динамическую IP-конфигурацию  /renew - Обновить динамическую IP-конфигурацию с DHCP-сервера  /flushdns - Очистить кэш разрешений DNS  /registerdns - Обновить регистрацию на DNS-сервере  /displaydns - Отобразить содержимое кэша разрешений DNS | Служит для отображения всех текущих параметров сети TCP/IP и обновления параметров DHCP и DNS. При вызове команды ipconfig без параметров выводятся IP-адрес, маска подсети и основной шлюз для каждого сетевого адаптера.  DHCP (англ. Dynamic Host Configuration Protocol — протокол динамической настройки узла) — сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве сетей TCP/IP.  DNS (англ. Domain Name System — система доменных имён) — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене (SRV-запись). |
| arp | -a - Отображает текущие ARP-записи | Отображение и изменение ARP-таблиц. |
| ping | Формат команды:  "ping <сетевой узел> параметры"  Параметры:  -t - Бесконечная (до нажатия клавиш <Ctrl>+<Break>) отправка пакетов на указанный узел  -a - Определение имени узла по IP-адресу  -n <число> - Число отправляемых запросов  -l <размер> - Размер буфера отправки  -w <таймаут> - Таймаут ожидания каждого ответа в миллисекундах | Мощный инструмент диагностики (с помощью протокола ICMP). ICMP = Internet Control Message Protocol — протокол межсетевых управляющих сообщений.  Команда ping позволяет проверить:   * работоспособность IP-соединения; * правильность настройки протокола TCP/IP на узле; * работоспособность маршрутизаторов; * работоспособность системы разрешения имен FQDN или NetBIOS; * доступность и работоспособность какого-либо сетевого ресурса. |
| tracert | -d - Без разрешения IP-адресов в имена узлов  -h <максЧисло> - Максимальное число прыжков при поиске узла  -w <таймаут> - Таймаут каждого ответа в миллисекундах | Служебная программа для трассировки маршрутов, используемая для определения пути, по которому IP-дейтаграмма доставляется по месту назначения. |
| pathping | -n - Без разрешения IP-адресов в имена узлов  -h максЧисло - Максимальное число прыжков при поиске узла  -q <число\_запросов> - Число запросов при каждом прыжке  -w <таймаут> - Таймаут каждого ответа в миллисекундах | Средство трассировки маршрута, сочетающее функции программ ping и tracert и обладающее дополнительными возможностями.  Эта команда показывает степень потери пакетов на любом маршрутизаторе или канале, с ее помощью легко определить, какие маршрутизаторы или каналы вызывают неполадки в работе сети. |
| netstat | -a - Отображение всех подключений и ожидающих (слушающих) портов  -n - Отображение адресов и номеров портов в числовом формате  -o - Отображение кода (ID) процесса каждого подключения  -r - Отображение содержимого локальной таблицы маршрутов | Используется для отображения статистики протокола и текущих TCP/IP-соединений. |
| nbtstat | –n - Выводит имена пространства имен NetBIOS, зарегистрированные локальными процессами  –c - Отображает кэш имен NetBIOS (разрешение NetBIOS-имен в IP-адреса)  –R - Очищает кэш имен и перезагружает его из файла Lmhosts  –RR - Освобождает имена NetBIOS, зарегистрированные на WINS-сервере, а затем обновляет их регистрацию | Средство диагностики разрешения имен NetBIOS. NetBIOS (Network Basic Input/Output System) — протокол для работы в локальных сетях на персональных ЭВМ типа IBM/PC, разработан в виде интерфейса, который не зависит от фирмы-производителя. Был разработан фирмой Sytek Corporation по заказу IBM в 1983 году. Он включает в себя интерфейс сеансового уровня (англ. NetBIOS interface), в качестве транспортных протоколов использует TCP и UDP.  Имя NetBIOS содержит до 16 символов, последний из которых регистрируется в Windows для идентификации конкретных функций определенных компьютеров, например, контроллеров домена или браузеров. Если включена служба NetBIOS, то каждому компьютеру операционной системой присваивается имя NetBIOS. Это имя может совпадать или не совпадать с именем входа пользователя или хост-именем компьютера. Вы используете имена NetBIOS, когда вводите UNC-имя пути, указывающее какой-либо узел сети Windows. |

Ping — утилита командной строки для проверки соединений в сетях TCP/IP. Она является одним из основных средств диагностики сети и входит в состав всех современных сетевых операционных систем. Принцип ее работы заключается в том, что она отправляет запросы (ICMP Echo-Request) протокола ICMP указаному узлу и фиксирует поступающие ответы (ICMP Echo-Reply).

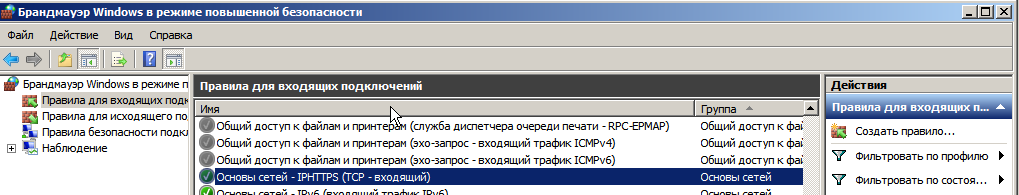
Время между отправкой запроса и получением ответа позволяет определить задержки при передаче и частоту потери пакетов, а также оценить загруженность канала передачи данных. Полное отсутствие ICMP-ответов может означать, что удалённый узел неисправен.

В серверных ОС начиная с Windows Server 2008 входящие эхо-запросы по умолчанию запрещены и блокируются брандмауэром Windows. Сделано это скорее всего с целью предотвратить сетевые атаки типа ICMP Flooding (затопление атакуемого узла пакетами ICMP), которые могут вызвать отказ в обслуживании (Denial of Service, DoS). Безопасность конечно важна, однако в результате при попытке проверить доступность сервера мы получаем ошибку.

Для разрешения входящих эхо-запросов необходимо активировать соответствующее правило брандмауэра Windows. Вот несколько вариантов того, как это сделать.

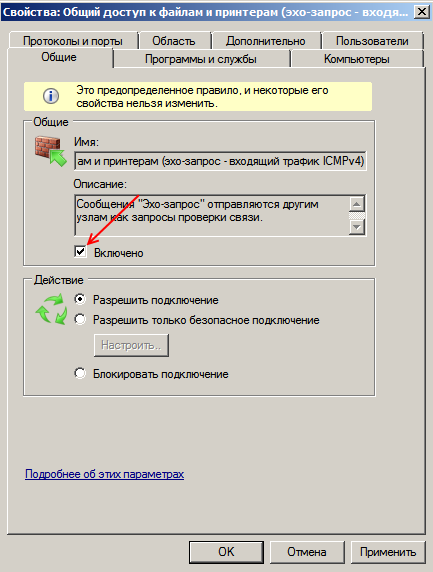
Самый простой способ разрешить ping — воспользоваться оснасткой «Брандмауэр Windows в режиме повышенной безопасности».

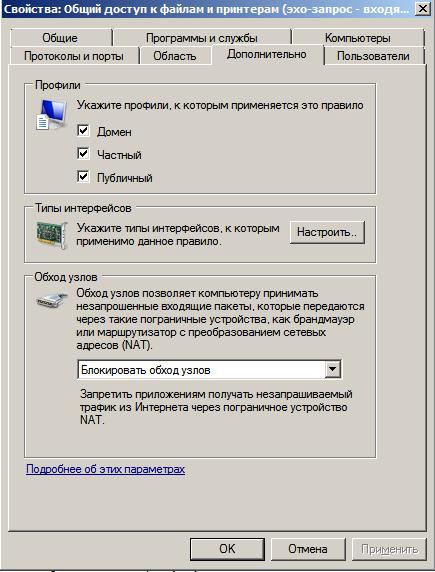
*Для ее запуска нажимите клавиши Win+R и вводим команду wf.msc.*



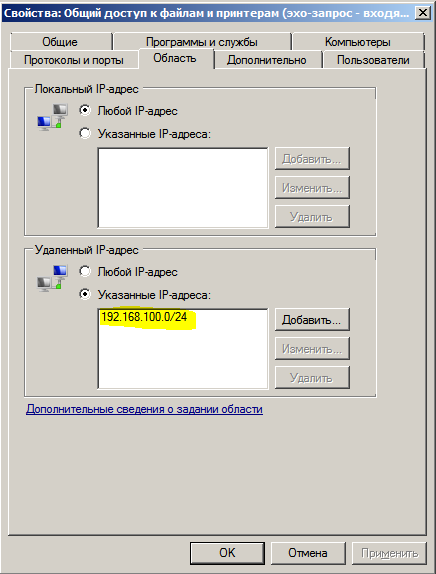
*Зайдите в раздел входящих правил (Inbound Rules). Здесь нас интересует предопределенное правило для IPV4 — ″Общий доступ к файлам и принтерам (эхо-запрос – входящий трафик ICMPv4)″.*

*Активируем это правило, отметив галочкой чекбокс Включено и проверяем, чтобы в поле Действие был выбран пункт ″Разрешить подключение″. Нажать «Применить».* Переходим на вкладку Дополнительно и выбираем профили, для которых это правило будет действовать. *Нажать «Применить» 🡺*  OK. Теперь сервер можно пинговать.

**



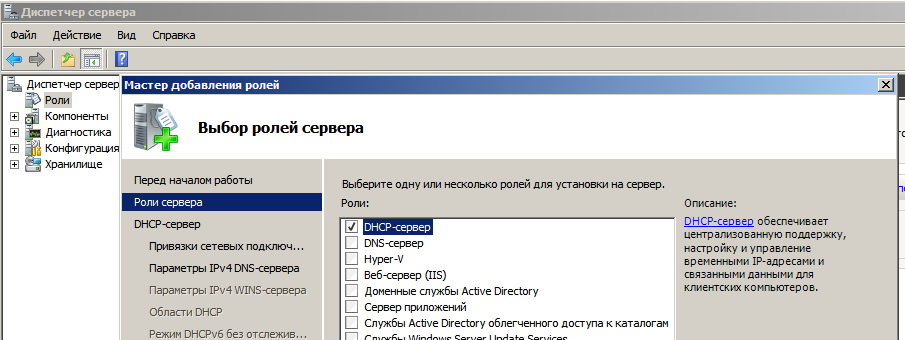
*Защитите сервер от атак. Для этого. Перейдите на вкладку Scope и в поле Remote IP address указываем, с каких адресов разрешено принимать входящие запросы. Здесь можно указать один адрес, диапазон адресов либо целиком подсеть.*

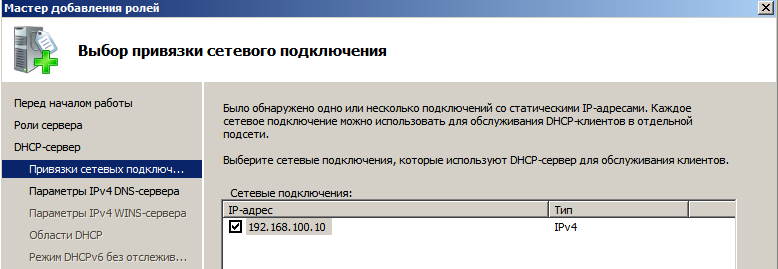
*Перейдите на вкладку Область и в поле Указанные IP-адреса укажите, с каких адресов разрешено принимать входящие запросы. Здесь можно указать один адрес, диапазон адресов либо целиком подсеть. Например, добавьте 192.168.100.0/24. Проверьте пингуется ли сервер DC1. Измените 192.168.100.0/24 на 192.168.1.0/24. Проверьте пингуется ли сервер DC1. Какой результат? Почему он получен?*

*Верните значение 192.168.100.0/24. Проверьте пингуется ли сервер DC1. Пингуется! Ура!*

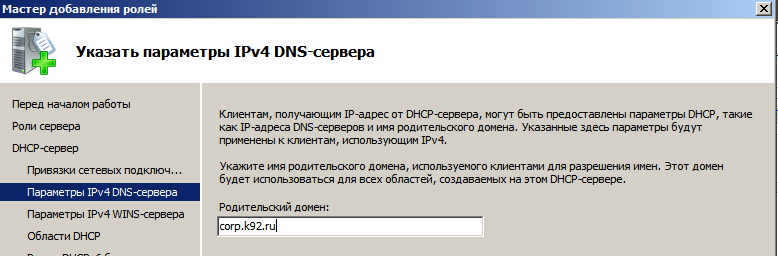
## Задание 5. Настройка DHCP –сервера.

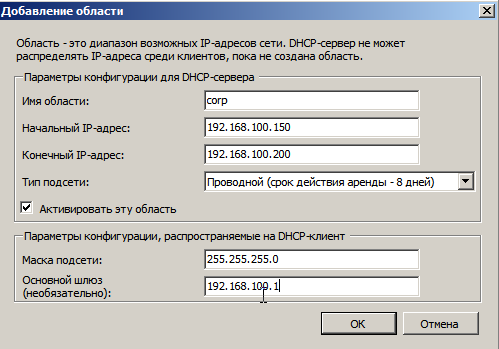
1. *Добавьте роль DHCP – сервера.*



*Вы* *берите роль DHCP-сервер 🡺 Далее*

*Далее. Введите: Родительский домен: corp.k92.ru. Далее.*



*Укажите в качестве Wins-сервера 192.168.100.10.*

*Добавьте область corp. DHCP-сервер будет выдавать адреса из диапазона 192.168.100.150 – 192.168.100.200. Маска подсети 255.255.255.0. Основной шлюз 192.168.100.1.*

*Далее🡺 Далее 🡺 Далее🡺Установить*

### Задание 6. Настройте клиентский компьютер на динамическое получение IP-адреса .

*1. Переключитесь на компьютер WS.*

*2. Откройте Панель управления.*

*3. Выберите Сеть и Интернет, а затем Центр управления сетями и общим доступом.*

*4. В левой области щелкните Изменение параметров адаптера.*

*5. Щелкните правой кнопкой мыши Подключение по локальной сети*

*и выберите пункт Свойства.*

*6. Измените свойства элемента Протокол Интернета версии 4 (TCP/IPv4), указав следующие параметры.*

*7. Получить IP-адрес автоматически.*

*8. Получить адрес DNS-сервера автоматически.*

*9. Дважды нажмите кнопку ОК.*

### Задание 7. Проверьте, что клиентский компьютер получил адрес

*Откройте командную строку на WS.*

*В командной строке введите следующую команду* **ipconfig /all** *и нажмите клавишу ВВОД.*

*Вопрос. Каков текущий IPv4-адрес?*

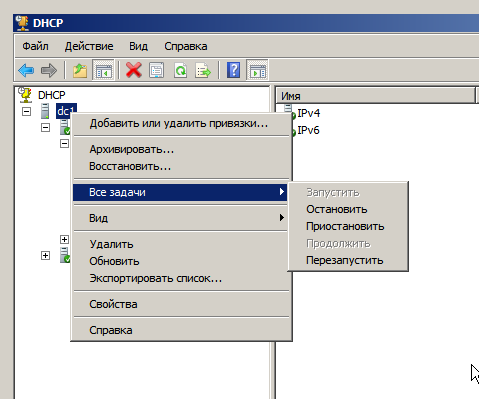
*Вопрос. В поле «DHCP включен» указано значение «Да»?*

*Вопрос. Какой IP-адрес у DHCP-сервера?*

*Вопрос. Когда истекает аренда DHCP?*

### Задание 8. Ipconfig /release и Ipconfig /renew

*Остановите работу DHCP-сервера. Для этого переключитесь на сервер DC1 🡺 В оснастке DHCP щелкните ПКМ по dc1, выберите «Все задачи» 🡺Остановить.*



*Переключитесь на компьютер WS. В настройках TCP/IP отключите протокол IPv6.*

*Освободите IPv4-адрес. Запустите командную строку. В командной строке введите следующую команду* **ipconfig /release** *и нажмите клавишу Enter.*

*Попытайтес получить новый IP-адрес от DHCP-сервера. В командной строке введите команду* **ipconfig /renew** *и нажмите клавишу Enter.*

*Примечание. Это может занять несколько минут, поскольку клиентский компьютер пытается подключиться к исходному DHCP¬серверу, а затем к любому другому DHCP-серверу.* Получить новый IP-адрес от DHCP-сервера не удалось и сетевому интерфейсу системой был назначен Link-Local Address IP адрес. Link-Local Address — адреса сети, которые предназначены только для коммуникаций в пределах одного сегмента местной сети или магистральной линии. Они позволяют обращаться к хостам, не используя общий префикс адреса.

Подсети link-local не маршрутизируются: маршрутизаторы не должны отправлять пакеты с адресами link-local в другие сети.

Адреса link-local часто используются для автоматического конфигурирования сетевого адреса, в случаях, когда внешние источники информации об адресах сети недоступны.

Типичное использование link-local адресов — автоматическое конфигурирование IP-адресов в локальных сетях Ethernet. Адрес из диапазона link-local назначается ОС хоста автоматически в случае недоступности других источников информации, например сервера DHCP.

*Запустите DHCP-сервер на DC1. Переключитесь на рабочую станцию WS и в командной строке введите следующую команду Ipconfig /renew, после чего нажмите клавишу Enter.*

*Вопрос. Какой IPv4-адрес отобразился? Вопрос. На что это указывает?*

*Удалите роль DHCP-сервер и перезагрузите DC1.*

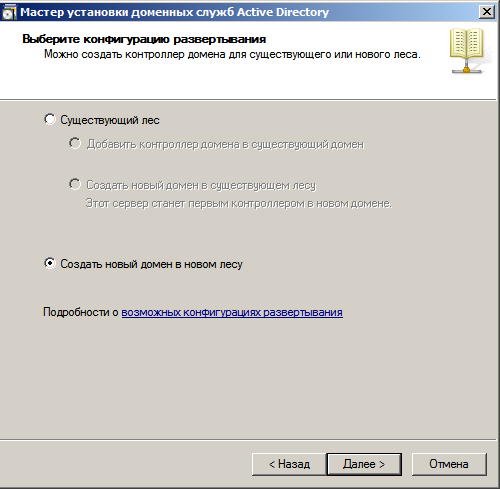
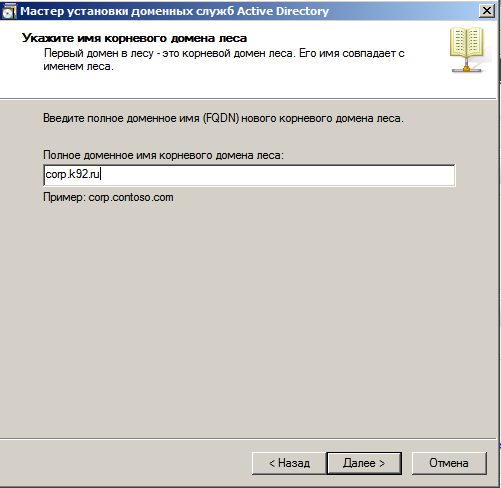
## Задание №9. Установка контроллера домена.

*В меню Пуск выберите пункт Выполнить, введите dcpromo и нажмите кнопку ОК.*

*На странице "Службы установки доменных служб Active Directory" нажмите кнопку Далее.*

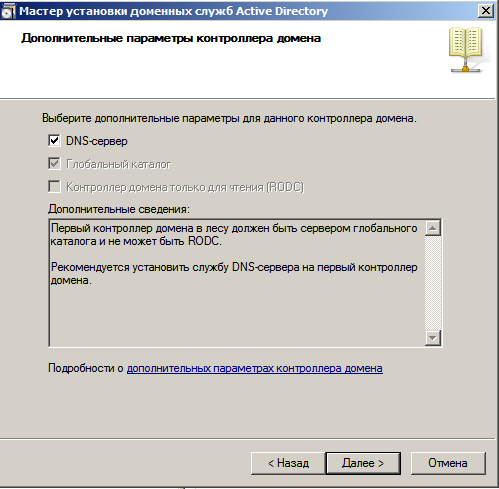
*На странице "Совместимость операционной системы" нажмите кнопку Далее.*

*На странице "Выберите конфигурацию развертывания" выберите параметр Создать новый домен в новом лесу, а затем нажмите кнопку Далее.*

*На странице "Укажите имя корневого домена леса" введите* **corp.k92.ru** *в поле Полное доменное имя корневого домена леса, а затем нажмите кнопку Далее.*

*На странице "Задание режима работы леса" выберите Windows Server 2008 R2 в раскрывающемся списке и нажмите кнопку Далее.*

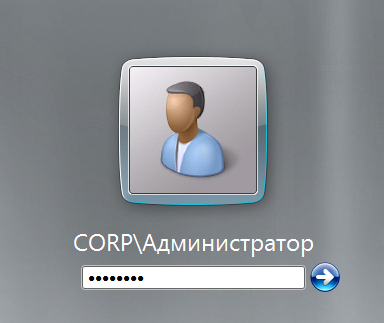
 *На странице "Дополнительные параметры контроллера домена" убедитесь, что установлен флажок DNS-сервер, а затем нажмите кнопку Далее.*

*В диалоговом окне с предупреждением нажмите кнопку Да.*

*На странице "Расположение для базы данных, файлов журнала и папки SYSVOL" примите значения по умолчанию и нажмите кнопку Далее.*

*На странице "Пароль администратора для режима восстановления служб каталогов" введите и подтвердите пароль P@ssw0rd, а затем нажмите кнопку Далее.*

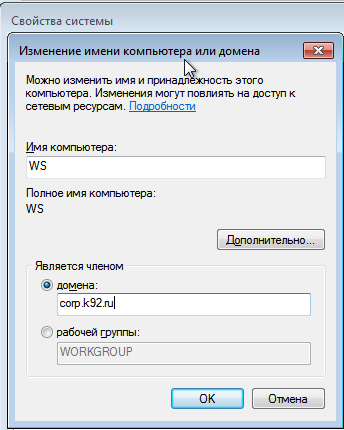
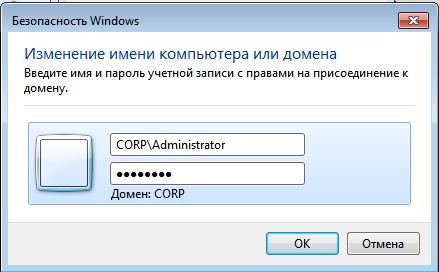
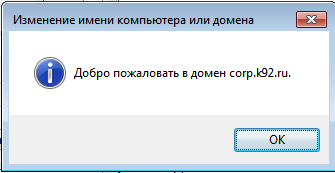
*На странице сводных данных нажмите кнопку Далее.*

*После завершения работы мастера нажмите кнопку Готово.*

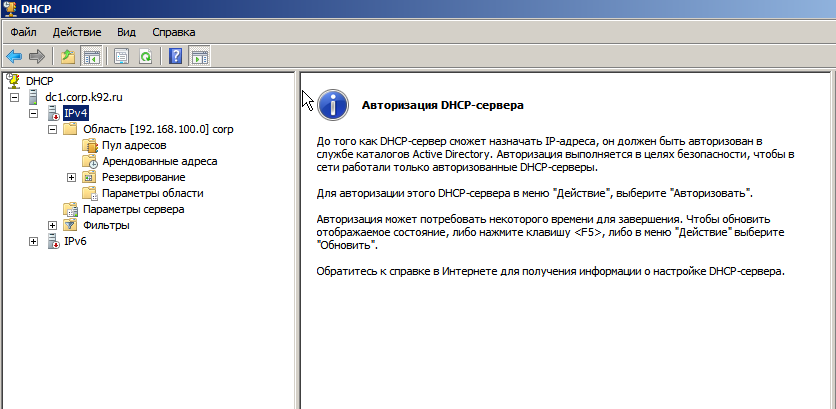
*Перезапустите виртуальную машину. Зайдите на контроллер домена DC1 с учетной запиью Администратор.*

### Задание №9. Ввод рабоей станции WS в домен.

*Пуск 🡺 ПКМ на Компьютер 🡺 Свойства 🡺 Дополнительные параметры системы 🡺 Имя Компьютера 🡺 Изменить 🡺 Является членом домена corp.k92.ru 🡺 ОК.*



*Перезагрузить WS. Зайти в WS под доменной учетной записью CORP\Администратор.*

*Вопрос: Удалось ли зайти? В чем проблема? Ответ: WS не получила IP адрес от DHCP сервера, так как он не авторизован.*

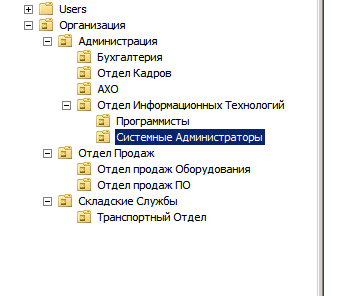
*Авторизуйте сервер DHCP. Действие 🡺 Авторизовать 🡺 Обновить*

*Войдите как WS\Admin и проверьте, что WS получила IP-адрес от DHCP-сервера.*

*Завершение работы 🡺 Выйти из системы 🡺 Зайти в WS как CORP\Администратор.*

### Задание №10. Создание контейнеров, пользователей и групп.

Создайте следующую структуру подразделений в Active Directory



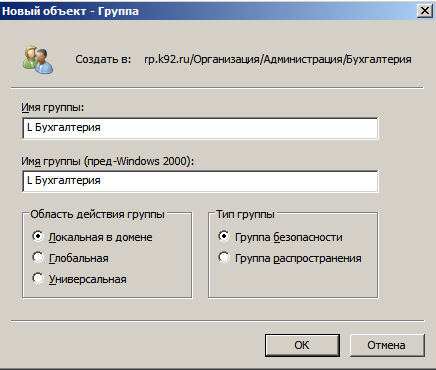
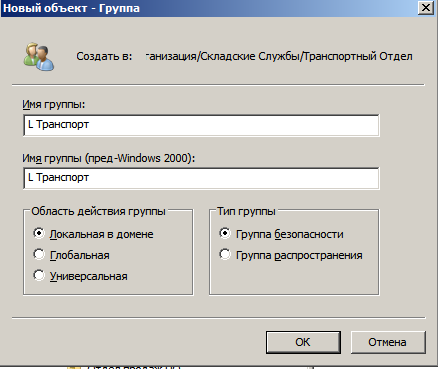
Создайте пользователя Мария Ивановна Кузнецова (Главный Бухгалтер) в контейнере Бухгалтерия.

Создайте пользователя Ксения Федоровна Иванова (Бухгалтер) в контейнере Бухгалтерия.

Создайте пользователей Иван Павлович Дорожный (Начальник Транспортного отдела) и Федор Семенович Каталкин (Логист) в контейнере Транспортный Отдел.

Создайте группу безопасности «L Бухгалтерия» и добавьте в нее Кузнецову М.И. и Иванову К.Ф.

Создайте группу безопасности «L Транспорт» и добавьте в нее Дорожного и Каталкина.

### Задание №12. Создание сетевой папки.

На DC1 создайте сетевую папку «Buh» и предоставьте полный доступ к ней бухгалтерам. Остальные сотрудники не должны иметь доступ к папке «Buh». Протестируйте доступ с WS к [\\DC1\Buh](file:///\\DC1\Buh) под разными учетными записями.

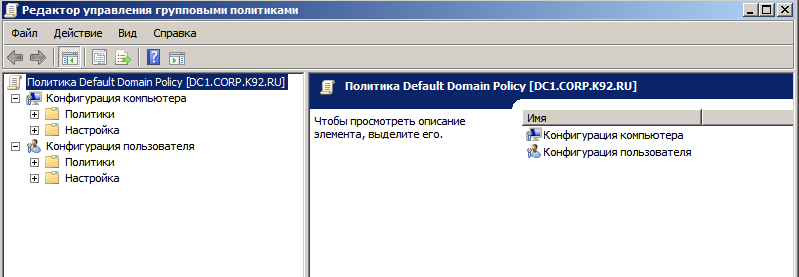
На DC1 создайте сетевую папку «Transport» и предоставьте полный доступ к ней сотрудникам Транспортного Отдела. Остальные сотрудники не должны иметь доступ к папке «Transport». Протестируйте доступ с WS к [\\DC1\](file:///\\DC1\)Transport под разными учетными записями.

### Задание №11. Редактирование Default Domen Policy.

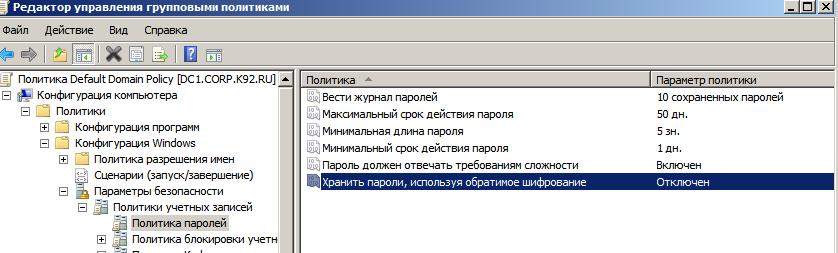
Групповая политика представляет собой самый простой способ настройки компьютера и параметров пользователей в сетях на основе доменных служб Active Directory. Если ваша компания не использует групповую политику, вы упускаете отличную возможность для снижения расходов, управления конфигурациями, поддержания производительности и удобства для пользователей, а также повышения уровня безопасности. Групповая политика дает возможность настроить многочисленные параметры одновременно.

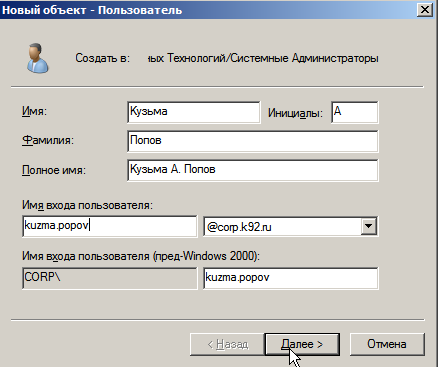
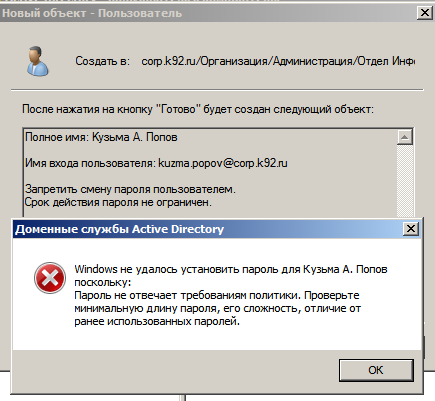
Консоль управления групповыми политиками запускается из меню «Пуск». Щелкните Пуск, Все программы, Администрирование, Управление групповыми политиками.

Откройте для изменения Политику Default Domain Policy



Отредактируйте Политику паролей. Вести журнал паролей: 10. Максимальный срок действия паролей 50 дн. Минимальная длина пароля 5 зн.



Создайте учетную запись Попов Кузьма Анатольевич (Системный Администратор) и попробуйте создать для него пароль «777».

Не получилось!

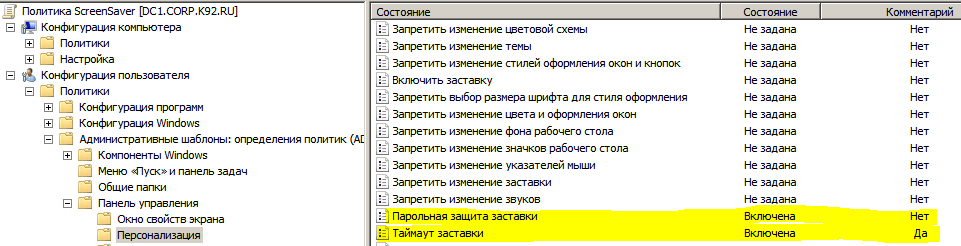
Поменяйте «Политику паролей», чтобы сделать для Попова К.А. пароль 777.

Создайте учетную запись для Попова К.А. с паролем 777.

### Задание №11. Настраиваем блокировку компьютера при простое через screen saver с помощью Group Policy.

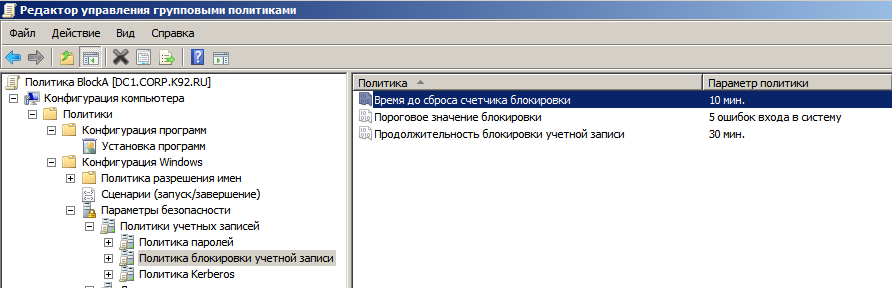
В большинстве организаций, применяющих в своей ИТ инфраструктуре локальные стандарты и регламенты информационной безопасности, уделяется отдельное внимание вопросу блокировки консолей рабочих станций пользователей при наступлении некоторого периода бездействия. Например, в качестве обязательного требования для большинства категорий пользователей может выставляться блокировка рабочего стола компьютера при отсутствии пользовательской активности более 15 минут. В управляемой среде Active Directory в доменных групповых политиках администраторам предоставляется ряд параметров, позволяющих централизованно настроить пользовательскую среду для форсированного применения механизма блокировки рабочего стола посредствам срабатывания программы - хранителя экрана (screen saver), или как её ещё называют, экранной заставки.

Создайте групповую политику ScreenSaver для контейнера Организация, которая будет блокировать экран через 600 секунд простоя с парольной защитой заставки.



## Задание №11. Создать политику блокировки учетной записи BlockA для контейнера Организация.

*Даже после создания сложного пароля и правильной настройки политик безопасности, учетные записи ваших пользователей все еще могут быть подвергнуты атакам недоброжелателей. Например, если вы установили минимальный срок действия пароля в 20 дней, у хакера достаточно времени для подбора пароля к учетной записи. Узнать имя учетной записи не является проблемой для хакеров, так как, зачастую имена учетных записей пользователей совпадает с именем адреса почтового ящика. А если будет известно имя, то для подбора пароля понадобится какие-то две-три недели.*

*Групповые политики безопасности Windows могут противостоять таким действиям, используя набор политик узла «Политика блокировки учетной записи». При помощи данного набора политик, у вас есть возможность ограничения количества некорректных попыток входа пользователя в систему. Разумеется, для ваших пользователей это может быть проблемой, так как не у всех получится ввести пароль за указанное количество попыток, но зато безопасность учетных записей перейдет на «новый уровень». Для этого узла доступны только три политики, которые рассматриваются ниже.*

*Время до сброса счетчиков блокировки. Active Directory и групповые политики позволяют автоматически разблокировать учетную запись, количество попыток входа в которую превышает установленное вами пороговое значение. При помощи этой политики устанавливается количество минут, которые должны пройти после неудачной попытки для автоматической разблокировки. Вы можете установить значение от одной минуты до 99999. Это значение должно быть меньше значения политики «Продолжительность блокировки учетной записи».*

*Пороговое значение блокировки. Используя эту политику, вы можете указать количество некорректных попыток входа, после чего учетная запись будет заблокирована. Окончание периода блокировки учетной записи задается политикой «Продолжительность блокировки учетной записи» или администратор может разблокировать учетную запись вручную. Количество неудачных попыток входа может варьироваться от 0 до 999. Я рекомендую устанавливать допустимое количество от трех до семи попыток.*

*Продолжительность блокировки учетной записи. При помощи этого параметра вы можете указать время, в течение которого учетная запись будет заблокирована до ее автоматической разблокировки. Вы можете установить значение от 0 до 99999 минут. В том случае, если значение этой политики будет равно 0, учетная запись будет заблокирована до тех пор, пока администратор не разблокирует ее вручную.*