

004.72(076)
Б 40



AUES

Since 1975

Некоммерческое
акционерное
общество

**АЛМАТИНСКИЙ
УНИВЕРСИТЕТ
ЭНЕРГЕТИКИ И
СВЯЗИ**

Кафедра систем
информационной
безопасности

БЕЗОПАСНОСТЬ И АДМИНИСТРИРОВАНИЕ WINDOWS SERVER

Методические указания по выполнению лабораторных работ для студентов
специальности 5В100200 – Системы информационной безопасности

Алматы 2019

СОСТАВИТЕЛЬ: Е.Г. Сатимова. Безопасность и администрирование Windows Server.. Методические указания к выполнению лабораторных работ для студентов специальности 5В100200 – Системы информационной безопасности. - Алматы: АУЭС, 2019. - 105 с.

Методические указания содержат указания по подготовке к проведению лабораторных работ, целью которых является изучение основ построения полноценной доменной структуры; приведены 6 лабораторных работ, дана методика проведения и ход выполнения, оговорен перечень рекомендуемой литературы и контрольные вопросы. Использована технология виртуальных машин, позволяющая при проведении лабораторных работ в компьютерном классе моделировать условия работы реальной компьютерной сети предприятия на основе домена.

Методические указания предназначены для студентов 3 курса всех форм обучения специальности 5В100200 – Системы информационной безопасности. Они могут быть использованы и для организации лабораторных занятий по идентичным темам аналогичных дисциплин, запланированных для других специальностей.

Ил. 71, табл. 1, библиогр. - 5 назв.

Рецензент: доцент Гармашова Ю.М.

Печатается по плану издания некоммерческого акционерного общества «Алматинский университет энергетики и связи» на 2018г.

Содержание

Введение.....	4
1 Лабораторная работа № 1. Установка Microsoft Windows Server 2012 R2	5
2 Лабораторная работа № 2. Установка DNS-сервера.....	25
3 Лабораторная работа №3. Установка и управление ролью DHCP-сервер.....	37
4 Лабораторная работа № 4. Управление учетными записями пользователей.....	49
5 Лабораторная работа № 5. Управление организационными единицами и группами в Active Directory.....	66
6 Лабораторная работа № 6. Управление профилями пользователей.....	81
Библиографический список.....	100

Введение

В настоящий сборник включены первые 6 лабораторных работ, целью которых является приобретение базовых навыков эффективного использования операционных систем в компьютерной сети предприятия; изучается студентами, обучающимися по направлению 5В100200 – Системы информационной безопасности в 6 семестре.

Основными задачами, которые решает выполнение лабораторного практикума, являются:

- формирование систематизированного представления о концепциях, принципах и моделях, положенных в основу построения клиент-серверной системы на базе MS Winsows® 2012 R2;

- получение практической подготовки в области выбора и применения базовых возможностей операционной системы Windows Server® для задач автоматизации обработки информации и управления;

- приобретение навыков и умений установки и настройки современной операционной системы Microsoft Windows и контроллера домена Active Directory.

Все лабораторные работы основаны на построении виртуальных сред, подключенных к серверу IBM. Для обеспечения возможности установки, настройки и исследования студенты разворачивают полигон, имитирующий корпоративную сеть, использующую технологии контроллера домена, создавая каждым обучающимся виртуальные машины индивидуально. При этом администрирование и настройка виртуальных объектов никак не влияет на реальную систему и не представляет для неё опасности. Виртуальная система легко переносится с компьютера на компьютер, очень просто восстанавливается в случае сбоев и неправильных настроек. Студент при минимуме затрат времени может создать точную копию системы, используемой в учебной лаборатории, на своем компьютере и заниматься самостоятельно и дополнительно совершенствовать свои навыки в условиях, моделирующих реальную систему предприятия. Это делает предлагаемый лабораторный комплекс уникальной средой для обучения работе с операционными системами, пригодной для всех форм обучения студентов.

При создании настоящего издания составитель использовал современную литературу и учебные пособия для профессионалов [1–5], свой опыт преподавания этой дисциплины как авторизованного преподавателя Microsoft, а также знания и навыки, полученные при обучении на сертификационных курсах компании Microsoft.

Ограниченный объем издания не позволил включить в методические указания все лабораторные работы, рассматриваемые в курсе «Безопасность и администрирование Windows Server».

1 Лабораторная работа № 1. Установка Microsoft Windows Server 2012 R2

Цель: освоить технологию установки операционной системы Windows Server R2 на виртуальной машине VMWare vSphere 5.5;

освоить технологию установки контроллера домена Active Directory Domain Services на Windows Server 2012 R2 различными способами.

План проведения занятия:

- 1) Ознакомиться с программным обеспечением VMWare vSphere 5.5.
- 2) Создать виртуальную машину, исходя из предоставленной информации о минимальных аппаратных требований, предлагаемой к установке и изучению операционной системы (ОС).
- 3) Установить Windows Server 2012 R2 на виртуальный компьютер. Разобрать процесс установки ОС на этапы.
- 4) Поднять контроллер домена Active Directory Domain Services .

Результат: виртуальная машина с установленным контроллером домена Windows 2012 Server R2 и Active Directory Domain Services.

Предварительные навыки: практические навыки работы в системе Windows.

1.1 Чистая установка Windows

1.1.1. Установка системы.

Рекомендуется всегда использовать англоязычные издания Windows Server. Как показывает практика, оригинальные (английские) версии Windows работают стабильнее. Под «чистой» понимается установка ОС на компьютере, на котором отсутствует текущая установленная копия или такая, которую требовалось бы сохранить. На нашем примере студенты имеют дело с компьютером (виртуальная машина), не имеющим предыдущей установленной копии, предполагаем, что ранее студенты сервер не разворачивали.

Так как используется виртуальная машина, можно перенаправить виртуальный CD/DVD на ISO-образ Windows Server DVD.

Запуск установки.

Запустите программу VMWare vSphere 5.5 (пароль у преподавателя).
Зайдите в консоль (Open Console).

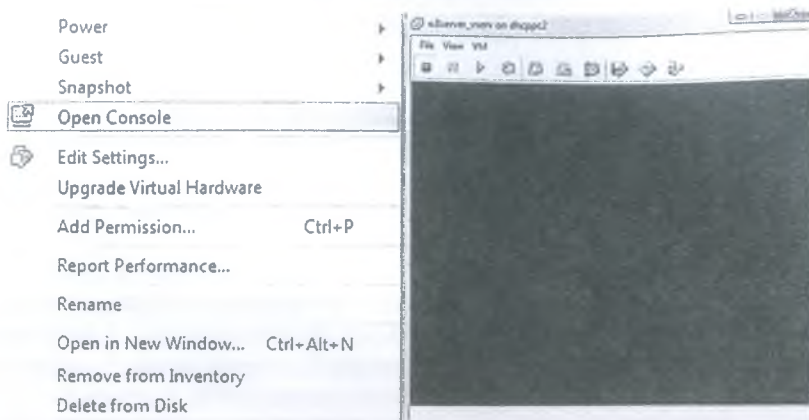


Рисунок 1.1 – Консоль VMWare vSphere 5.5

Подключение образа диска ОС.

Вариант 1.

1. Вставить в CD-дисковод установочный CD - Connect to host device (Подключить устройство хост машины, например, можно подключить CD ROM клиента).

2. Загрузить компьютер с компакт-диска .

3. Выбрать нужную редакцию системы.

Вариант 2.

1. Connect to ISO image on datastore (подключить образ ISO находящийся в хранилище гипервизора, предварительно надо его туда скопировать).

Системные требования:

1. Процессор - производительность процессора зависит не только от тактовой частоты процессора, но также от количества его ядер и от размера его кэша. Ниже перечислены требования к процессору для данного продукта.

2. Минимум: 64-разрядный процессор 1,4 GHz.

3. Минимум: 2 Gb ОЗУ.

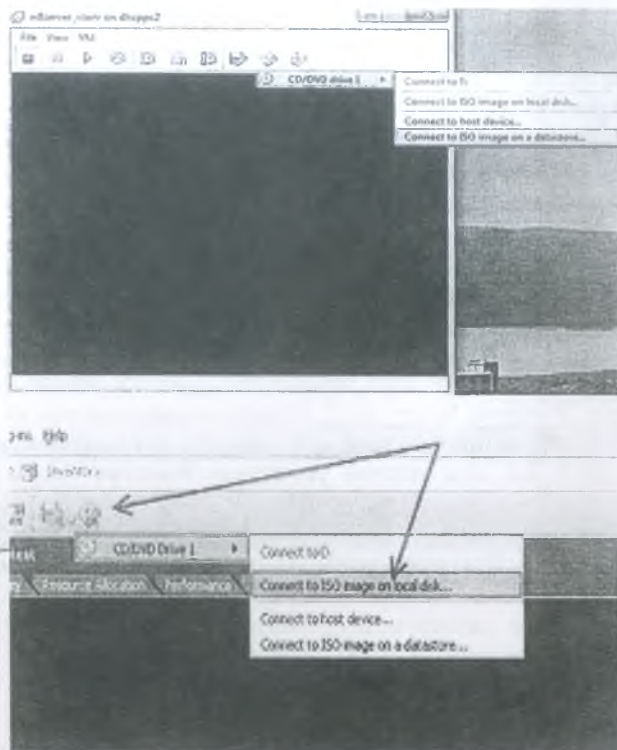
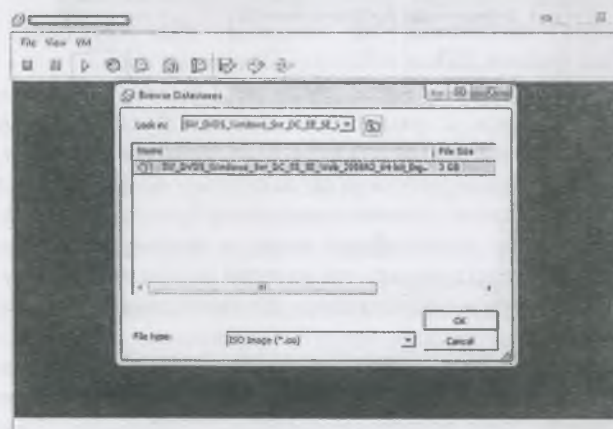


Рисунок 1.2 - Непосредственно подключение



1.1.2 Первоначальная настройка Microsoft Windows Server 2012.

Для успешной установки необходимо не менее 60 Gb свободного места на диске. Нажмите кнопку *Пуск*.

Файл .iso содержит все версии Windows Server 2012 R2, и здесь можно выбрать версию, которую нужно установить. Обратите внимание, что можно также установить версии Server Core. Установите версию. Windows Server 2012 R2 Enterprise (полная установка (Full Installation)) и нажмите *«Далее» (Next)*.

После чтения файлов установки с образа начнется установка.

1. Поставьте галочку напротив опции *«Я принимаю условия лицензионного соглашения»* на странице лицензионного соглашения и нажмите *«Далее» (Next)*.

2. На следующем шаге необходимо выбрать новую или специальную установку Windows Server 2012 R2 либо модернизацию на месте. Выбрать модернизацию можно только при наличии предыдущей версии Windows Server 2012 R2. Для чистой установки Windows Server 2012 выберите *«Выборочная: только установка Windows...» (Custom: Install Windows only)*.

3. Теперь разметьте жесткий диск для установки, если это не было сделано ранее. Для этого выберите незанятое пространство на каком-либо физическом жестком диске в списке и нажмите *«Создать» (New)*.

4. Введите размер создаваемого логического диска (по умолчанию полный объем) и нажмем *«Применить» (Apply)*.

5. В следующем окне, для первичной установки Windows Server нажмите *«Установить» (Install now)*.

Если необходимо разделить диск на несколько томов (может потребоваться создать том, чтобы отделить веб-содержимое от ОС в целях безопасности), следует щелкнуть на ссылке *Drive options (advanced) (параметры устройства (дополнительные))*.

Также согласимся на создание дополнительных разделов для системных файлов, нажав *«ОК»* в появившемся окне.

После вышеописанных действий, вместо неразмеченной области должны появиться 2 раздела: *Системный (System)* и *Основной (Primary)*. Выберите основной раздел для установки Windows и жмите *«Далее» (Next)*.

Дождитесь завершения установки компонент Windows Server 2012.

По завершении установки компьютер будет перезагружен.

Прежде чем можно будет войти в систему Windows Server 2012 R2 предлагается указать пароль для учетной записи локального администратора *«Администратор» (Administrator)*. По умолчанию пароль должен отвечать требованиям безопасности паролей, а именно:

- не содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков;
- иметь длину не менее 6 знаков;
- содержать знаки трех из четырех перечисленных ниже категорий:

1) Латинские заглавные буквы (от А до Z).

- 2) Латинские строчные буквы (от а до z).
- 3) Цифры (от 0 до 9).
- 4) Отличающиеся от букв и цифр знаки (например, !, \$, #, %).

Как изменить политику паролей рассмотрим в следующих лабораторных работах.

6. Выберите надежный пароль и запишите пароль в отведенное для хранения паролей место. Для этого удобно использовать различные менеджеры паролей, например бесплатную программу KeePass. Введите пароль администратора и нажмите «Готово» (*Finish*).

7. Далее вы попадете на стартовое окно Windows Server 2012. Нажмите одновременно CTRL, ALT и DEL и войдите в Windows под учетной записью Администратора, введя установленный на предыдущем шаге пароль. Первое, что вы увидите после входа в систему, - *диспетчер серверов* (*Server Manager*). Для настройки текущего локального сервера выберите вкладку «Локальный сервер» (*Local Server*) в панели вкладок слева.

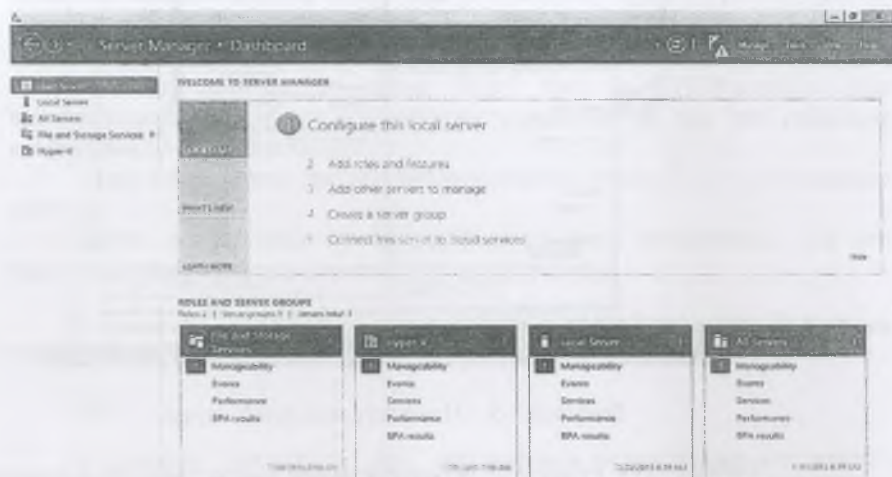


Рисунок 1.4 – Диспетчер серверов

Кнопка Start (Пуск) находится в нижнем левом углу.

При установке нового сервера необходимо пройти через ряд общих задач конфигурирования, чтобы подключить сервер к сети.

Каждый компьютер Windows должен иметь уникальное имя, чтобы уникальным образом идентифицироваться в рамках сети. Любая организация устанавливает свою политику именования компьютеров. В одних организациях применяют хорошо структурированные имена, которые описывают местоположение и функцию, в других используют не описательные имена с увеличивающимися числами и т.п. Процедура

установки не запрашивала имя компьютера - сервер автоматически получил случайно сгенерированное имя.

8. Измените имя компьютера (*Задать осмысленное имя компьютеру*). Для этого кликните по текущему имени компьютера в окне «Свойства» (*Properties*). Откроется окно «Свойства системы» (*System Properties*) на закладке «Имя компьютера» (*Computer Name*). Нажмите кнопку «Изменить...» (*Change...*) и введите новое имя сервера в появившемся окне. После чего закройте все окна, нажав последовательно «ОК» и «Применить» (*Apply*).

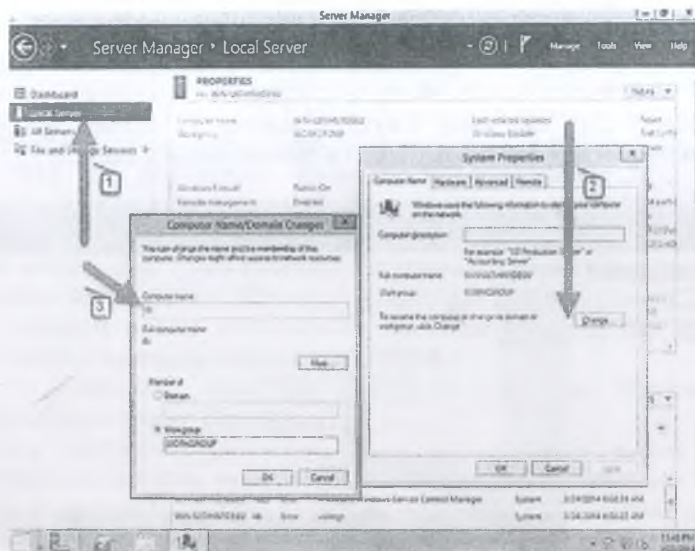


Рисунок 1.5 – Изменить имя компьютера

Аналогичную процедуру переименования можно провести в командной строке с помощью команды *netdom*:

```
C:\>netdom /renamecomputer WIN-DCL9MRNLVON /newname :  
BIGFIFMAPPSVR1
```

Эта операция переименует компьютер WIN-DCL9MRNLVON на BIGFIFMAPPSVR1.

9. Разрешите удаленный доступ к текущему серверу. Для этого кликните по ссылке напротив «Удаленный рабочий стол» (*Remote Desktop*) в окне свойств. Откроется окно «Свойства системы» (*System Properties*) на вкладке «Удаленный доступ» (*Remote*). Установите переключатель в «Разрешить удаленное подключение к этому компьютеру» (*Allow remote*

connections to this computer). По умолчанию только пользователи группы «Администраторы» (Administrators) имеют доступ к удаленному рабочему столу (для добавления пользователей необходимо нажать на «Выбрать пользователей...» (Select Users) и добавить пользователей системы из списка), после чего нажмите «Применить» (Apply). Подключение к серверу осуществляется с помощью встроенного в Windows RDP-клиента.

Для конфигурирования сетевой интерфейсной платы сервера щелкните правой кнопкой мыши на ее изображении и выберите в контекстном меню пункт Properties (Свойства). Задайте статический IP адрес и маску подсети сетевому адаптеру (конечно, если ваш сетевой адаптер не получает настройки по DHCP).

Откроются свойства сетевого соединения. Выберите в списке компонент «Протокол интернета версии 4 (TCP/IPv4)» (Internet Protocol Version 4 (TCP/IPv4)) (и снова нажмем «Свойства» (Properties)). В открывшемся окне можно задать нужные параметры IP. Это может быть динамический IP, если в сети есть DHCP-сервер, либо статический IP, который можно задать самостоятельно. По умолчанию новый сервер Windows Server 2012 R2 не имеет сконфигурированного IP-адреса. Он будет пытаться получить конфигурацию TCP/IPv4 от DHCP-сервера. Для производственного сервера это обычно нежелательно, так что *измените конфигурацию на статическую*.

То же самое можно проделать в командной строке с помощью команды *netsh*.

Позже понадобится проверить имя сетевого интерфейса; для его получения можно воспользоваться командой *ipconfig*.

```
C:\>netsh interface ip set address name="Local Area Connection" static 192.168.1.49 255.255.255.0 192.168.1.1
```

или

```
C:\>netsh interface ip set address name="Ethernet" static 192.168.1.49 255.255.255.0 192.168.1.1
```

Синтаксис команды *netsh* выглядит следующим образом:

```
C:\>netsh interface ip set address name="<Имя сетевого интерфейса>" static <Желаемый IP-адрес> <Желаемая маска подсети> <Желаемый стандартный шлюз>
```

При наличии вторичного DNS-сервера необходимо выполнить еще одну команду *netsh*, которая немного отличается:

```
C:\>netsh interface ip add dns "Local Area Connection" 192.168.1.22
C:\>
```

Чтобы проверить проделанную работу, следует запустить команду *ipconfig*:

```
C:\> ipconfig
```

В случае запуска команды *ipconfig /all* вы получите намного больше информации.

Следующее действие заключается в тестировании подключения. Это можно сделать с помощью команды *ping*, которая посылает тестовый пакет сетевому устройству или серверу:

```
C:\>ping 192.168.1.1
```

10. На следующем шаге выберите параметры обновления Windows Server 2012. Для этого пройдите по ссылке напротив пункта «Центр обновления Windows» (*Windows Update*), чтобы открыть соответствующую оснастку. Кликните на «Я хочу выбрать параметры» (*Let me choose my settings*).

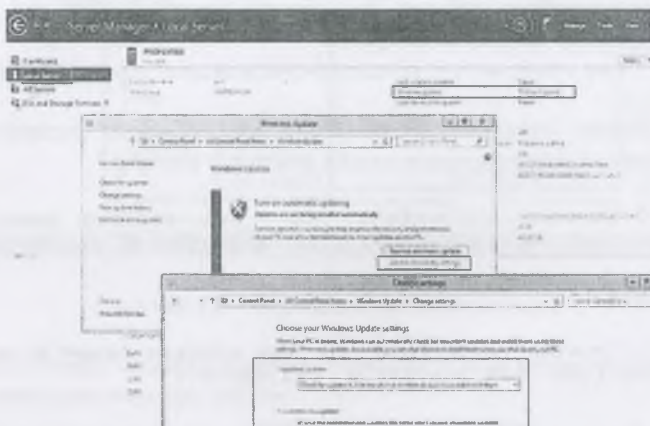


Рисунок 1.6 – Выбор способа обновления

В открывшемся окне выберите необходимые параметры центра обновлений Windows, например:

1) Важные обновления: «Загружать обновления, но решение об установке принимается мной» (*Check for updates but let me choose whether to download and install them*).

2) Рекомендованные обновления: *«Получать рекомендованные обновления таким же образом, как и важные обновления» (Give me recommended updates the same way I receive important updates)*.

После того, как параметры установлены, нажмите «ОК» для сохранения настроек.

11. После чего Windows выполнит поиск доступных обновлений. Отметьте все обновления в списке и нажмите «Установить» (*Install*) для запуска процесса установки.

12. Продолжите настройку сервера. Пройдите по ссылке напротив пункта «Дата и время» (*Time zone*) для установки этих параметров. Для изменения даты и времени нажмите «Изменить дату и время...» (*Change date and time...*) в открывшемся окне, и «Изменить часовой пояс...» (*Change time zone...*) для изменения часового пояса соответственно. Определившись с настройками, закрываем все окна кнопкой «ОК».

13. Активируйте Windows Server 2012. Для этого нажмите на ссылку в пункте «Код продукта» (*Product ID*). Откроется окно «Активация Windows» (*Windows Activation*) (в котором необходимо ввести текущий ключ продукта и нажать кнопку «Активировать» (*Activate*)).

Если код соответствует выбранной версии Windows Server 2012, через некоторое время появится сообщение об успешной активации Windows, а напротив пункта «Код продукта» (*Product ID*) вы должны увидеть текущий код и статус «(активировано)» (*activated*).

На этом установка и первоначальная настройка Microsoft Windows Server 2012 закончена. Осталось только дождаться установки текущих обновлений, перезагрузить сервер, затем повторить процедуру снова, до тех пор, пока все необходимые обновления не будут установлены.

1.2 Установка роли Active Directory на Windows Server 2012

Перед установкой доменных служб Active Directory убедитесь в том, что в сети функционирует DNS-сервер, иначе вам будет предложено установить его после установки AD.

После предварительной настройки сервера, переходим к установке роли службы каталогов. Применим установку на основе ролей для единственного сервера.

1. Войдите на сервер Windows Server 2012 с использованием учетной записи, имеющей полномочия администратора.

2. Откройте диспетчер серверов (*Server Manager*) и выберите в меню пункт *Manager -> Add Roles and Features* (*Управление -> Добавление роли и компоненты*).

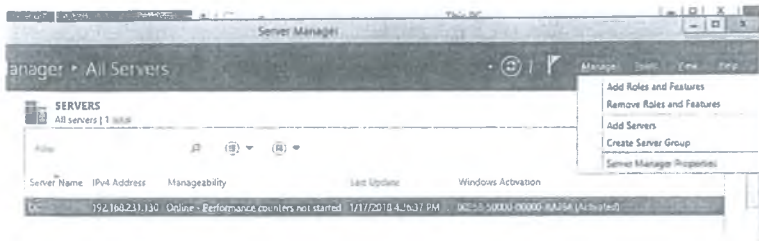


Рисунок 1.7 - Добавление роли

Запуск диспетчера серверов *Start -> Server Manager* (Пуск -> Диспетчер сервера).

3. Просмотрите сведения на экране *Before you begin* (Прежде чем начать) мастера *Add roles and features -> Next*.

4. Выберите переключатель *Role-based or Feature-based Installation* (Установка ролей и компонентов) -> *Next*

5. Появится экран *Select destination server* (Выбор сервера назначения). Выберите целевой сервер из пула серверов, на который устанавливается роль AD и нажать Далее. Выберите переключатель *Select a server from the server pool -> Next*

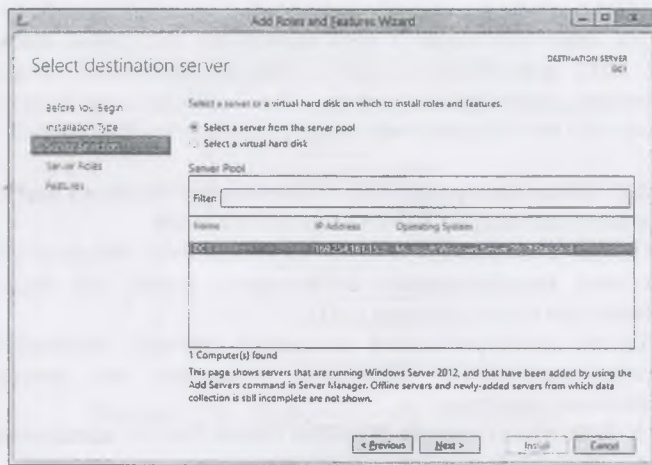


Рисунок 1.8 – Выбор сервера для установки

6. Вы увидите перечень всех доступных ролей, которые можно установить. При щелчке на каждой из них справа отображается краткое описание роли. Выберите роль *Active Directory Domain Services* (Служба домена *Active Directory*), после чего появляется окно с предложением

добавить роли и компоненты, необходимые для установки роли AD. Нажмите кнопку *Add Features*.

7. На экране *Features* (Компоненты) ничего выбирать не придется.

8. Просмотрите сведения на экране *Active Directory Domain Services*.

9. Если вы хотите перезапустить сервер автоматически, отметьте флажок *Restart the destination server automatically if required* (При необходимости автоматически перезапускать целевой сервер). После установки двоичных файлов в диспетчере серверов появляется значок с восклицательным знаком желтого цвета.

10. Щелкните на этом значке с восклицательным знаком и затем щелкните на ссылке *Promote this server to a domain controller* (Повысить этот сервер до контроллера домена).

Это приведет к запуску мастера *Active Directory Domain Services Configuration*. Можно также выбрать роль *DNS Server*. Если вы забудете установить галочку для добавления роли *DNS Server*, можно особо не переживать, т.к. её можно будет добавить позже на стадии настройки роли AD. После этого нажимайте каждый раз кнопку *Next* и установите роль.

1.2.1 Настройка доменных служб Active Directory.

После установки роли, закройте окно — *Close*. Теперь необходимо перейти к настройке роли AD.

11. В окне *Server Manager* нажмите пиктограмму флага с уведомлением и нажать *Promote this server to a domain controller* (Повысить роль этого сервера до уровня контроллера домена) на плашке *Post-deployment Configuration*.

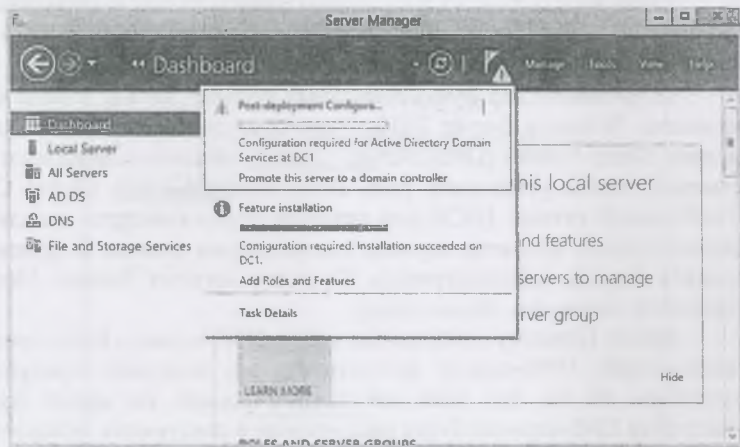


Рисунок 1.9 – Повысить роль сервера до уровня контроллера домена

12. На экране *Deployment Configuration* (Конфигурация развертывания) мастера выберите переключатель *Add a new forest* (Добавить новый лес), введите имя корневого домена, состоящее из 2-х частей и нажмите Далее. (корневое доменное имя в виде, например, <имя_домена>.com или <имя_домена>.net или любой домен верхнего уровня (top-level domain, TLD), назначенный вашей организации, например, aipet.kz (выбрать имя).

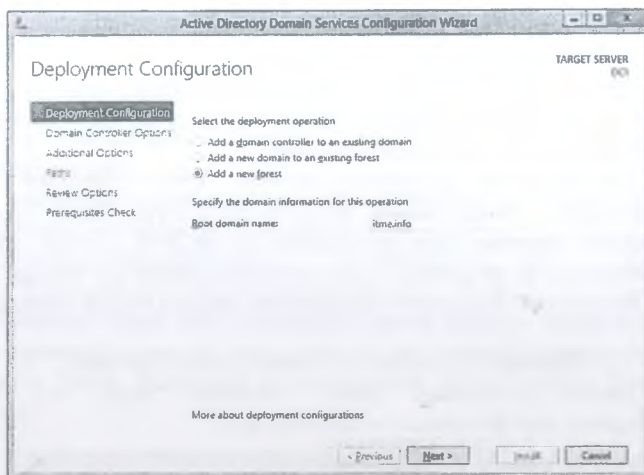


Рисунок 1.10 – Добавление нового леса

Далее необходимо указать режим работы леса и домена. Режим работы, который вы выберете, зависит от того, имеется ли у вас другой контроллер домена или лес, и от того, какие серверы вы используете.

13. Оставьте для функциональных уровней леса и домена стандартные варианты Windows Server 2012. Удостоверьтесь в том, что флажок возле Domain Name System (DNS) Server (Сервер системы доменных и мен (DNS)) отмечен, чтобы установить роль DNS. Флажок возле Global Catalog (GC) (Глобальный каталог (GC)) уже отмечен, и это изменить нельзя, поскольку данный сервер является первым контроллером домена в домене. Два раза введите пароль администратора Directory Services Restore Mode (DSRM). Щелкните на кнопке Далее (Next).

Active Directory попытается найти DNS-сервер. Если предварительно настроенный DNS-сервер отсутствует, вы получите предупреждение с указанием на то, что зона для вашего домена не может быть создана. Настройка DNS-сервера будет рассмотрена в следующих лабораторных.

14. Далее введите пароль для DSRM (Directory Service Restore Mode — режим восстановления службы каталога) и нажмите Далее (Next).



Рисунок 1.11 – Выбрать совместимость режима работы леса и корневого домена

На следующем шаге мастер предупреждает о том, что делегирование для этого DNS-сервера создано не было (*A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain «itme.info». Otherwise, no action is required.*).

Нажмите Далее (Next).

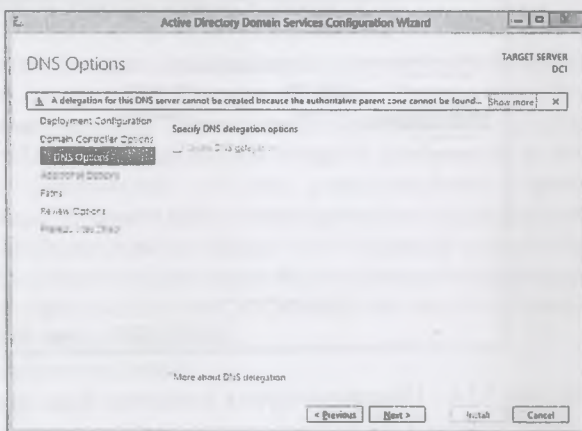


Рисунок 1.12 – Предупреждение о делегировании DNS сервера

Нет никаких причин изменять имя NetBIOS для домена. Оставьте имя, предложенное по умолчанию, и щелкните на кнопке Next (Далее).

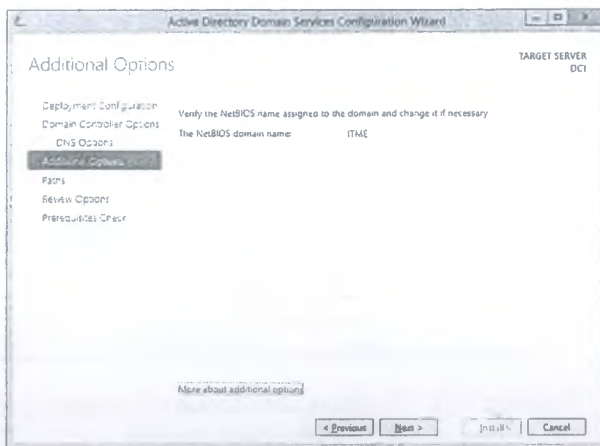


Рисунок 1.13 – Изменение имени NetBIOS

15. На следующем шаге отобразятся пути к файлу базы данных, файлу журнала и папке SYSVOL. Можно изменить пути к каталогам базы данных AD DS (Active Directory Domain Services – доменная служба Active Directory), файлам журнала, а также папке SYSVOL. Ничего менять не будем. Нажмите кнопку *Далее (Next)*.



Рисунок 1.14 – Изменение пути к каталогам базы данных AD DS

16. На следующем шаге отображается сводная информация по настройке. Обратите внимание на кнопку *View script (Просмотреть)*

сценарий) справа внизу. В результате щелчка на этой кнопке откроется окно редактора Notepad с подготовленными командами PowerShell для настройки леса, согласно выбранным ранее опциям, который произведет настройку доменных служб Active Directory.

```
# Windows PowerShell script for AD DS Deployment
Import-Module ADDSDeployment
Install-ADDSForest
-CreateDnsDelegation:$false
-DatabasePath "C:\Windows\NTDS"
-DomainMode "Win2012"
-DomainName "itme.info"
-DomainNetbiosName "ITME"
-ForestMode "Win2012"
-InstallDns:$true
-LogPath "C:\Windows\NTDS"
-NoRebootOnCompletion:$false
-SysvolPath "C:\Windows\SYSVOL"
-Force:$true
```

Командное окно PowerShell можно открыть на любом сервере Windows Server 2012, где установлена роль Active Directory Domain Services, и скопировать в него эти команды. В окне командной строки PowerShell будет запрошен пароль DSRM. По причинам безопасности мастер скрывает пароль, поэтому он не виден в сценарии PowerShell.

Для того, чтобы пароль не запрашивался каждый раз при запуске сценария, воспользуйтесь строкой, которая поместит пароль в сценарий:

```
-SafeModeAdministrator Password (ConvertTo-SecureString
"P@ssw0r " -AsPlainText - Force ) '
```

Убедившись, что все указано верно, нажмите на кнопку *Next*.

17. По завершении мастера на этапе *Prerequisite Check* (Проверка предварительных условий) производится проверка, все ли предварительные требования соблюдены, результаты которой отобразятся в отчёте. Одно из обязательных требований — это установленный пароль локального администратора. В самом низу можно прочитать предупреждение о том, что после того, как будет нажата кнопка *Install* уровень сервера будет повышен до контроллера домена и будет произведена автоматическая перезагрузка.

Должна появиться надпись *All prerequisite checks are passed successfully. Click «install» to begin installation.*

Нажмите кнопку *Install*.

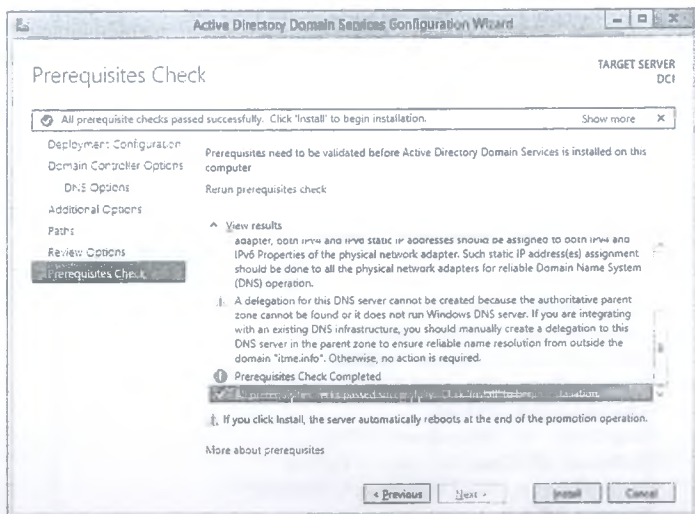


Рисунок 1.15 - Проверка предварительных требований

После завершения всех настроек, сервер перезагрузится, и вы совершите первый ввод компьютера в ваш домен.

18. Нажмите комбинацию клавиш <Ctrl+Alt+Del>, чтобы войти в систему. Пароль для учетной записи администратора домена - это тот же самый пароль, который был указан для учетной записи локального администратора до запуска мастера Active Directory Domain Services Configuration Wizard.

Вы создали лес с единственным доменом.

1.2.2 Добавление нового пользователя.

Создайте новое подразделение и добавьте в него пользователя, после чего присоедините компьютер к домену и войдите в домен под новым пользователем.

1. Для начала работы запустите оснастку "Пользователи и компьютеры Active Directory" (Пуск -> Панель управления -> Администрирование -> Пользователи и компьютеры Active Directory)

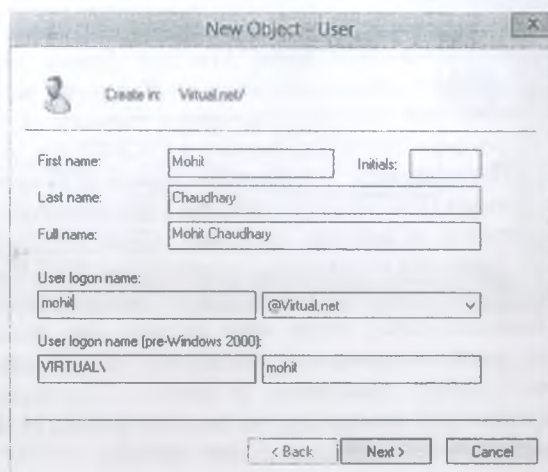
2. Выделите название домена и вызовите контекстное меню, в котором выбираете (Создать -> Подразделение). После чего введите имя для подразделения, а также можно снять защиту контейнера от случайного удаления, эту опцию оставьте включённой. Нажмите "ОК".

Подразделения служат для того, чтобы удобно управлять группами компьютеров пользователей и т.д. Например, можно разбить пользователей по группам с именами подразделений соответствующих

именам отделов компании, в которой они работают (Бухгалтерия, отдел кадров, менеджеры и т.д.)

3. Создайте нового пользователя в контейнере. Выделите контейнер «Пользователи», вызовите контекстное меню и выберите в нём (*Создать -> Пользователь*). Заполните поля «имя» и «фамилия», в полях «имя входа пользователя» укажите логин пользователя, под которым он будет заходить в домен.

Логин может содержать точки, например: «Ivan.Ivanov».



The screenshot shows a 'New Object - User' dialog box. At the top, it says 'Create in: Virtual.net/'. Below this, there are several input fields: 'First name' with 'Mohit', 'Initials' (empty), 'Last name' with 'Chaudhary', 'Full name' with 'Mohit Chaudhary', 'User login name' with 'mohit' and a dropdown menu showing '@Virtual.net', and 'User login name (pre-Windows 2000)' with 'VIRTUAL\' and 'mohit'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Рисунок 1.16 - Добавить нового пользователя

Нажмите кнопку *Next*, задайте пароль для пользователя (пароль должен соответствовать политике безопасности Windows), так же доступны четыре опции для изменения:

- требовать смены пароля пользователя при следующем входе в систему - при входе пользователя в ваш домен ему будет предложено сменить пароль;
- запретить смену пароля пользователем – отключает возможность смены пароля пользователем;
- срок действия пароля не ограничен – пароль можно не менять сколько угодно долго;
- отключить учётную запись – делает учётную запись пользователя не активной;
- нажмите *Next* затем нажмите «OK».

4. Выделите созданного пользователя и в контекстном меню выберите «Свойства». Перейдите на вкладку «Учётная запись» и поставьте галочку

напротив «Разблокировать учётную запись», после чего нажмите «Применить», затем нажмите «ОК».

1.2.3 Ввод компьютера в домен.

В результате проделанных манипуляций вы создали новое подразделение «Пользователи» и добавили в него нового пользователя «Иван Иванов» с логином «Ivan.Ivanov». Далее введите компьютер в ваш домен и попробуйте залогиниться под новым пользователем. Для этого на компьютере пользователя сделайте следующие:

1. Укажите на клиентском компьютере DNS-адрес. Для этого откройте «Свойства сетевого подключения» (Пуск -> Панель управления -> Центр управления сетями и общим доступом -> Изменить параметры адаптера), вызовите контекстное меню подключения и нажмите «Свойства». После чего выделите «Протокол Интернета версии 4 (TCP/IPv4)», нажмите «Свойства», выберите «Использовать следующие адреса DNS-серверов» и в поле «Предпочитаемый DNS –сервер» укажите адрес вашего DNS-сервера.

2. Откройте «Свойства системы» (Пуск -> Панель управления -> Система -> Изменить параметры), нажмите кнопку «Изменить».

3. Выберите «Компьютер является членом домена» и введите имя домена. Нажмите «ОК», после чего введите имя пользователя и пароль созданного вами пользователя; нажмите «ОК», после чего появится приветствие «Добро пожаловать в домен». Подтвердите «ОК», выйдет предупреждение, что компьютер необходимо перезагрузить, нажмите «ОК», потом «Закрывать», затем «Перезагрузить сейчас».

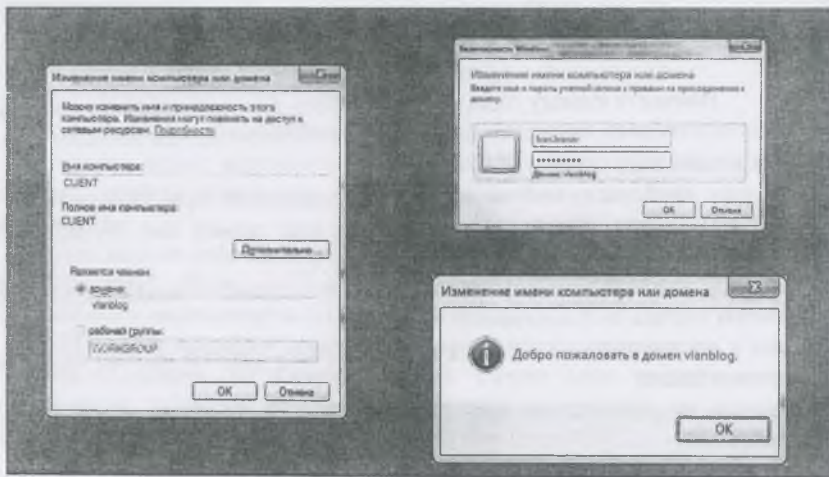


Рисунок 1.17 – Вход в домен

4. После того как клиентская машина будет перезагружена, введите в поле «Пользователь» имя домена/Ivan.Ivanov в поле пароль укажите пароль от учётной записи пользователя. Нажмите «Войти».

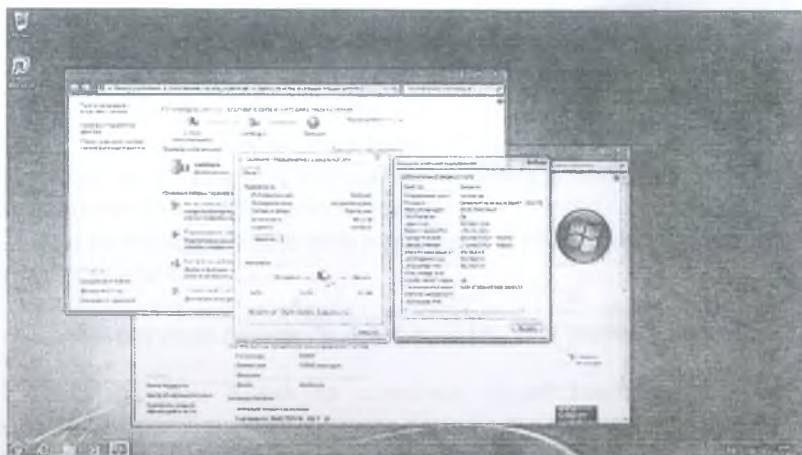


Рисунок 1.18 - Вход в систему под доменом нового пользователя

1.2.4 Вход в Windows 8.

1. Для начала добавьте новую группу в *Active Directory Administrative Center* – *HR Department*



Рисунок 1.19 – Добавление новой группы

9. Если на компьютере установлены протоколы TCP/IP, какую максимальную длину имени компьютера можно задать во время установки?

10. Можно ли изменить имя компьютера после установки ОС на клиентской машине и на контроллере домена?

11. Какое из следующих утверждений верно:

– вы можете подключить компьютер к рабочей группе или домену только во время установки;

– если вы подключите компьютер к рабочей группе во время установки, то к домену можно подключиться позже;

– если вы подключите компьютер во время установки к домену, то к рабочей группе можно подключиться позже;

– вы не можете подключить компьютер к рабочей группе или домену во время установки?

2 Лабораторная работа № 2. Установка DNS-сервера

Цель: изучение одной из основных служб контроллера домена – службы DNS (Domain Name Service). Приобретение навыков по установке службы DNS-сервера, настройке ее компонентов на Windows Server 2012 R2.

План проведения занятия:

- 1) Ознакомиться с системой доменных имён DNS.
- 2) Установить настройка службы DNS.
- 3) Установить прямую и обратную зоны DNS.
- 4) Создание записей.
- 5) Изучение утилит для работы с DNS

2.1 Установка DNS сервера на Windows Server 2012 R2

2.1.1 Установка и настройка службы DNS на компьютере с Windows Server 2012.

Active Directory использует систему доменных имен (Domain Name System, DNS). Домены DNS организованы в иерархическую структуру.

Процесс установки DNS на сервере Windows Server 2012 довольно прост и не требует перезагрузки системы. После указания статического IP-адреса и DNS-суффикса на сервере, не присоединенном к домену, выполните перечисленные ниже шаги для установки роли DNS.

1. Запустите диспетчер сервера (*Server Manager*) на сервере Windows Server 2012 с полным графическим интерфейсом.

2. Перейдите в раздел *Dashboard (Инструменты)* и щелкните на ссылке *Add Roles and Features (Добавить роли и компоненты)*.

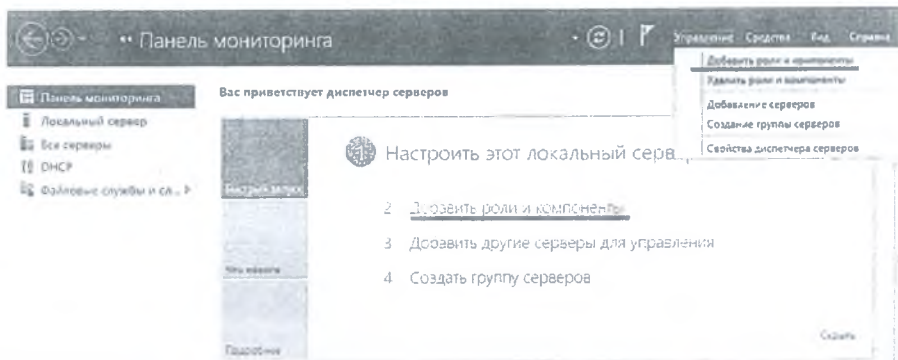


Рисунок 2.1 - Добавление ролей и компонентов

3. На странице *Before You Begin (Прежде чем приступить к работе)* щелкните на кнопке *Next (Далее)*.

4. Оставьте выбранным вариант *Role-Based or Feature-Based Installation (Установка на основе роли или компонента)* и щелкните на кнопке *Next*.

5. Выберите в серверном пуле сервер, на который нужно добавить роль DNS, и щелкните на кнопке *Next*.

6. Отметьте флажок *DNS Server Role (Роль сервера DNS)* и щелкните на кнопке *Next*.

Примечание - при отметке флажка *DNS Server Role* мастер выполнит проверку, что целевой сервер готов для выполнения роли DNS. Например, если для сервера не выделен статический IP-адрес, появится предупреждающее сообщение.

7. На странице *Features (Компоненты)* щелкните на кнопке *Next*.

8. На странице *Introduction to DNS Server (Вводные сведения о DNS-сервере)* щелкните на кнопке *Next*.

9. На странице *Confirmation (Подтверждение)* щелкните на кнопке *Install (Установить)*, чтобы запустить установку роли DNS.

10. Щелкните на кнопке *Close (Закрыть)*, чтобы завершить работу мастера.

Роль DNS можно установить локально на сервере, работающем в режиме *Server Core*, с помощью команды PowerShell.

```
Install-WindowsFeature -Name DNS-Server-Full-Role
```

2.2 Настройка роли DNS на компьютере с Windows Server 2012

1. Запустите диспетчер сервера (*Server Manager*) на сервере Windows Server 2012 с полным графическим интерфейсом, закладка *Tools*. Или через меню *Start (Пуск)*.

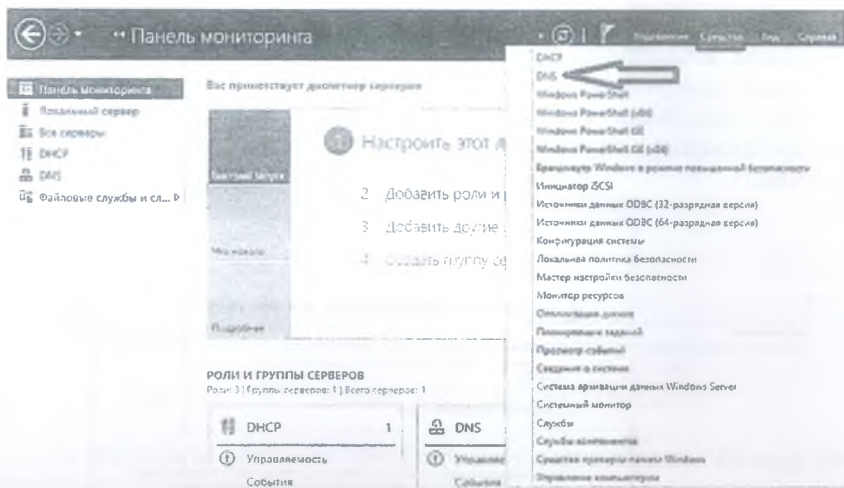


Рисунок 2.2 – Запуск роли DNS

2. Перейдите в раздел DNS. Появится список серверов в серверном пуле, на которых установлена роль DNS.

3. Щелкните правой кнопкой мыши на нужном сервере DNS и выберите в контекстном меню пункт DNS Manager (Диспетчер DNS).

4. Выберите имя сервера DNS, на котором нужно выполнить настройку.

5. В меню *Action (Действие)* выберите пункт *Configure a DNS Server (Настройка DNS сервера)*.

6. На странице приветствия мастера настройки сервера DNS (Configure DNS Server Wizard) щелкните на кнопке *Next*.

7. Выберите вариант *Create Forward and Reverse Lookup Zones (Recommended for Large Networks) (Создать зоны прямого и обратного просмотра (рекомендуется для больших сетей))* и щелкните на кнопке *Next*.

8. Выберите вариант *Yes, Create a Forward Lookup Zone Now (Recommended) (Да, создать зону прямого просмотра сейчас (рекомендуется))* и щелкните на кнопке *Next*.

9. Укажите тип создаваемой зоны - в данном случае выберите вариант *Primary Zone (Первичная зона)* - и щелкните на кнопке *Next*. Если сервер является контроллером домена с возможностью записи, будет также доступен флажок *Store Zone in Active Directory (Сохранить зону в Active Directory)*.

10. В случае сохранения зоны в Active Directory выберите область репликации и щелкните на кнопке *Next*.

11. Введите в поле *Zone Name (Имя зоны)* полностью определенное доменное имя зоны (FQDN) и щелкните на кнопке *Next*.

12. На этом этапе в случае создания не интегрированной с AD зоны можно либо создать новый текстовый файл для зоны, либо импортировать уже существующий. В нашем случае выберите вариант *Create a New File with This File Name* (Создать новый файл с таким именем) и оставьте предложенные по умолчанию параметры, после чего щелкните на кнопке *Next*.

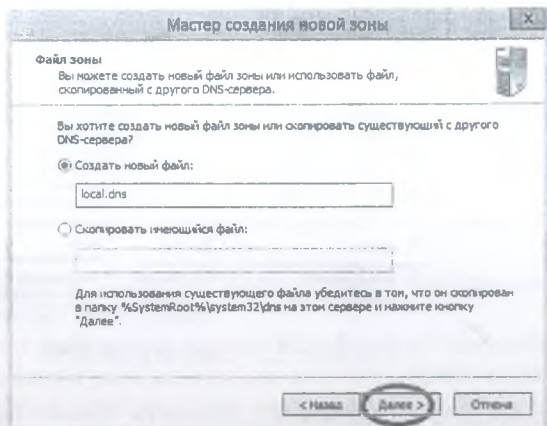


Рисунок 2.3 – Создание новой консоли

13. На следующей странице можно разрешить или запретить динамические обновления. В нашем примере оставьте динамические обновления отключенными, выбрав вариант *Do Not Allow Dynamic Updates* (Не разрешать динамические обновления), и щелкните на кнопке *Next*.

14. На следующей странице можно создать зону обратного просмотра. Выберите переключатель *Yes, Create a Reverse Lookup Zone Now* (Да, создать зону обратного просмотра сейчас) и щелкните на кнопке *Next*.

Обратная зона позволяет выполнить разрешение FQDN-имен хостов по их IP-адресам. В процессе добавления ролей AD и DNS по умолчанию не создаются, поскольку предполагается, что в сети может существовать другой DNS-сервер, контролирующий обратную зону. Поэтому создайте ее сами, для этого перейдите в диспетчер *DNS (DNS Manager)*, на вкладку *Reverse Lookup Zones*, кликните правой кнопкой и выберите *New Zone*.

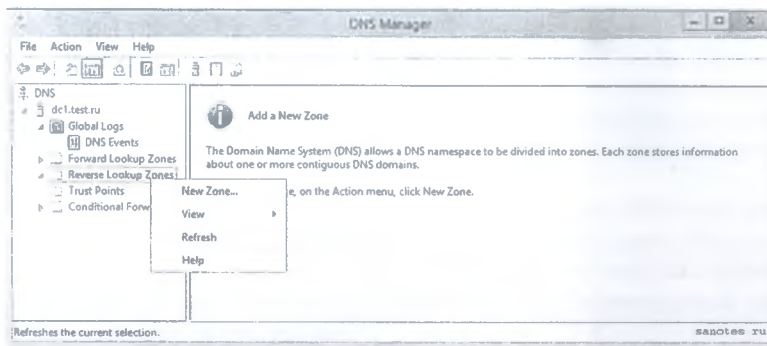


Рисунок 2.4 – Создание зоны обратного просмотра

15. Выберите для зоны обратного просмотра вариант *Primary Zone* (Первичная зона) и щелкните на кнопке *Next*.

16. Если надо хранить эту зону в Active Directory, выберите область репликации и щелкните на кнопке *Next*.

Здесь предлагается выбрать, как зона будет реплицироваться, обмениваться данными с другими зонами, расположенными на контроллерах и DNS-серверах. Возможны следующие варианты:

- для всех DNS-серверов, расположенных на контроллере домена в этом лесу (*To all DNS servers running on domain controllers in this forest*). Репликация во всем лесу Active Directory включая все деревья доменов;

- для всех DNS-серверов, расположенных на контроллере домена в этом домене (*To all DNS servers running on domain controllers in this domain*). Репликация внутри текущего домена и его дочерних доменов;

- для всех контроллеров домена в этом домене (*To all domain controllers in this domain*). Репликация на все контроллеры домена внутри текущего домена и его дочерних доменов;

- на все контроллеры домена в указанном разделе каталога приложений (*To all domain controllers specified in the scope of this directory partition*). Репликация на все контроллеры домена, но DNS-зона располагается в специальном каталоге приложений. Поле будет доступно для выбора, после создания каталога.

17. Оставьте предложенный по умолчанию вариант *IPv4 Reverse Lookup Zone* (Зона обратного просмотра IPv4) и щелкните на кнопке *Next*.

18. Введите сетевой идентификатор для зоны обратного просмотра и щелкните на кнопке *Next*. (Как правило, в качестве сетевого идентификатора вводятся первые октеты из IP адреса зоны. Например, если в сети используется диапазон IP-адресов класса C 198.168.0.0 с маской подсети 255.255.0.0, то нужно ввести значения 192.168.0, как показано на рисунке 2.5).

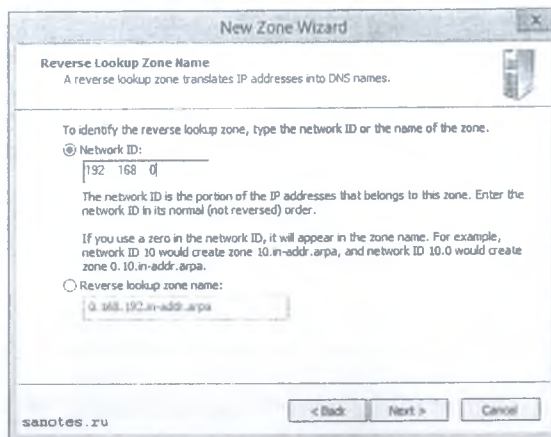


Рисунок 2.5 – Ввод сетевого идентификатора

19. В случае создания не интегрируемой с AD зоны будет снова предложено либо создать новый файл для зоны, либо импортировать уже существующий. В рассматриваемом примере выберите переключатель *Create a New File with This File Name (Создать новый файл с таким именем)* и щелкните на кнопке *Next*.

20. На экране *Dynamic Update* (динамические обновления), выберем один из трех возможных вариантов динамического обновления.

В данном примере выберите вариант *Do Not Allow Dynamic Updates (Не разрешать динамические обновления)* и щелкните на кнопке *Next*.

1. *Разрешить только безопасные динамические обновления (Allow Only Secure Dynamic Updates)*. Это опция доступна, только если зона интегрирована в Active Directory.

2. *Разрешить любые, безопасные и не безопасные динамические обновления (Allow Both Nonsecure And Secure Dynamic Updates)*. Данный переключатель позволяет любому клиенту обновлять его записи ресурса в DNS при наличии изменений.

3. *Запретить динамические обновления (Do Not Allow Dynamic Updates)*. Это опция отключает динамические обновления DNS. Ее следует использовать только при отсутствии интеграции зоны с Active Directory.

21. На следующей странице можно настроить параметры ретрансляторов. Выберите вариант *No, It Should Not Forward Queries (Нет, не следует переадресовывать запросы)* и щелкните на кнопке *Next*.

22. Последняя страница содержит все изменения и зоны, подготовленные для внесения и добавления в базу данных DNS. Щелкните на кнопке *Finish (Готово)*, чтобы внести все эти изменения и создать нужные зоны.

В зависимости от структуры сети, после щелчка на кнопке Finish может появиться еще одно диалоговое окно (со своей кнопкой Finish). Если сервер не подключен к локальной сети, появится диалоговое окно с сообщением об ошибке, связанной с поиском корневых ссылок. Но, несмотря на указанную ошибку, щелчок на кнопке ОК в этом окне приведет к успешной настройке DNS.

Конфигурация клиента DNS находится на вкладке DNS-окна свойств сети. Вполне очевидно, что обязательным является IP-адрес DNS-сервера. Подключение должно осуществляться к ближайшему серверу, как правило, на контроллере домена внутри локального сайта. Рекомендуется указать также дополнительный DNS-сервер.

2.3 Создание вторичной зоны и переносы зон (дополнительно)

1. Запустите диспетчер сервера (Server Manager) на сервере Windows Server 2012 с полным графическим интерфейсом.

2. Перейдите в раздел DNS. Появится список серверов в серверном пуле, на которых установлена роль DNS.

3. Щелкните правой кнопкой мыши на нужном сервере DNS и выберите в контекстном меню пункт DNS Manager (Диспетчер DNS).

4. Выберите имя сервера DNS, на котором нужно выполнить настройку.

5. Выделите узел Forward Lookup Zones (Зоны прямого просмотра).

6. В меню Action (Действие) выберите пункт New Zone (Создать зону).

7. На странице приветствия щелкните на кнопке Next (Далее).

8. В списке типов зон выберите вариант Secondary Zone (Вторичная зона). Вторичные зоны не могут интегрироваться в AD, поэтому все опции будут неактивны. Щелкните на кнопке Next.

9. Введите имя для создаваемой зоны (оно должно совпадать с именем первичной зоны) и щелкните на кнопке Next.

10. Введите IP-адрес или FQDN-имя сервера, с которого будут переноситься записи зоны.

Нажимайте клавишу <Enter> после ввода адреса каждого сервера для проверки его правильности. Затем щелкните на кнопке Next.

2.4 Создание записи A

Создайте запись типа A, например, для вашего же сервера. Для этого по зоне щелкните правой кнопкой мыши и нажмите «Создать узел A или AAAA».

Затем введите имя вашего узла, которое вы хотите, чтобы у него было и соответственно его IP адрес, это уже по факту. Нажмете «Добавить узел».

Появится сообщение о том, что узел создан и появится соответствующая запись.

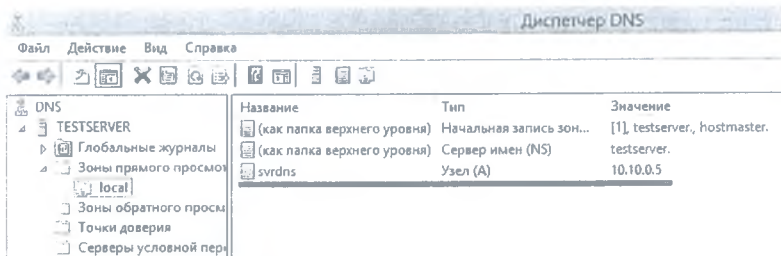


Рисунок 2.6 –Создание записей

Затем не забудьте проверить, какой DNS-сервер установлен у вас в настройках сетевого интерфейса (он должен быть соответственно наш, т.е. ip адрес этого сервера). Потом соответственно вы можем проверить работу только что установленного DNS-сервера, например, запустить командную строку и попробовать пропинговать узел который вы создали чуть ранее. Система распознала по доменному имени IP-адрес сервера.

2.5 Обратная сторона обратной зоны DNS

Зона обратного просмотра и ресурсные записи PTR, позволяющие выполнить разрешение FQDN-имен хостов по их IP-адресам, используются разными службами, особенно на платформе Unix/Linux. Обратное разрешение имен применяется во многих системах электронной почты в качестве первичного средства защиты от спама.

Обратная зона и записи PTR, по умолчанию, не создаются в процессе добавления ролей AD + DNS на домен-контроллерах, поскольку предполагается, что в сети может существовать другой DNS-сервер, контролирующий обратную зону. На самом деле, зона обратного просмотра DNS не требуется для работы AD, тем не менее, специалисты столкнулись как минимум уже с двумя ситуациями, когда возникающие ошибки связаны именно с отсутствием обратной зоны DNS.

2.6 Неизвестный DNS-сервер

На компьютере, включенном в домен при выполнении из командной строки *nslookup*, выводится ошибка (рисунок 2.7).



Рисунок 2.7 - Выполнение команды nslookup

На самом деле, проблема не влечет каких-либо последствий, и все остальные действия в консоли *nslookup* проходят без проблем. Кроме того, при явном подключении к другому DNS-серверу команда выполняется совершенно корректно.



Рисунок 2.8 – Команда nslookup при подключении к DNS-серверу

Ошибка при первоначальном запуске *nslookup* происходит потому, что в конфигурации сетевого подключения в настройках TCP/IP явно или по DHCP задается список IP-адресов серверов DNS для разрешения имен. При запуске *nslookup* подключение происходит к первому доступному DNS-серверу из списка. Именно этот DNS-сервер используется для выполнения запросов *nslookup*, пока явно не будет определен другой DNS-сервер. Вот только разрешить по IP-адресу собственное имя DNS-сервера не удастся ввиду отсутствия на нем самой обратной зоны. Разумеется, после настройки обратной зоны и добавления PTR-записи для этого сервера проблема исчезает.

Ошибка при вводе компьютера в домен. Данная проблема не столь очевидна, наблюдается не всегда и, вообще говоря, источником такого поведения могут быть несколько причин. В процессе ввода компьютера в домен на финальной стадии возникает ошибка «Не удалось изменить DNS-имя основного контроллера домена на «...» для этого компьютера»:

Самое интересное, что если компьютер перезагрузить, то он тем не менее оказывается в домене и далее работает без проблем. Ошибку можно игнорировать, и тем не менее, отсутствие зоны обратного просмотра и PTR-записей домен-контроллеров (и по совместительству DNS-серверов) тоже может быть причиной указанной ошибки.

2.7 Утилиты для работы с DNS

2.7.1 Применение утилиты командной строки *nslookup*.

Утилита командной строки *nslookup* является наиболее полезным инструментом для поиска и устранения проблем, связанных с клиентами DNS. Полученная с ее помощью информация оказывает неоценимую помощь в выявлении проблем, связанных с DNS. В простейшем случае утилита *nslookup* связывается со стандартным DNS-сервером клиента и пытается преобразовать введенное имя. Например, чтобы протестировать с ее помощью поиск имени *www.companyabc.com*, нужно ввести команду *nslookup www.companyabc.com*. В *nslookup* можно вводить и другие типы запросов. Например, она позволяет создавать запросы для просмотра записей MX или SOA, связанные с определенным доменом. Ниже перечислены необходимые шаги.

1. Откройте окно командной строки, выбрав в меню Start (Пуск) пункт All Programs=> Accessories=>Command Prompt (Все программы =>Стандартные =>Командная строка).

2. Введите *nslookup* и нажмите клавишу <Enter>.

3. Введите *set query=mx* и нажмите клавишу <Enter>.

4. Введите <имя домена> и нажмите клавишу <Enter>.

5. Введите *set query=soa* и нажмите клавишу <Enter>.

6. Введите <имя домена> и нажмите клавишу <Enter>.

Возможности утилиты *nslookup* не ограничиваются только такими простыми поисками. С помощью команды *nslookup /?* можно просмотреть полный перечень доступных функций. В общем, утилита *nslookup* является замечательным инструментом для решения многих задач и должна обязательно входить в арсенал любого, кто занимается выявлениями устранением неполадок.

2.7.2 Применение утилиты командной строки *ipconfig*.

Утилита *ipconfig* удобна и для решения вопросов с TCP/IP. В отношении DNS утилита *ipconfig* позволяет выполнять несколько важных операций. Эти операции запускаются из командной строки с помощью соответствующих параметров.

– *ipconfig /flushdns*. При возникновении проблем с кешем на стороне клиента содержимое кеша можно сбросить с помощью флага *flushdns*. Этот флаг позволяет удалить все помещенные ранее в кэш запросы, которые

может хранить клиент, и особенно полезен, если на сервере имен только что поменялись IP-адреса и у каких-то клиентов теперь не могут обратиться к нему.

– *ipconfig /registerdns*. Флаг *registerdns* заставляет клиента динамически перерегистрировать себя в DNS, если соответствующая зона поддерживает динамические обновления.

– *ipconfig /displaydns*. Этот интересный флаг позволяет просмотреть содержимое клиентского кэша и помогает в выявлении определенных проблем с отдельными записями.

2.7.3 Применение утилиты командной строки *tracert*.

Утилита *tracert* – ценный источник информации, позволяющий получить представление о пути, который проходит DNS-запрос при его пересылке по сети. Например, указав в качестве параметра *tracert* адрес *www.microsoft.com*, можно увидеть, через сколько маршрутизаторов и DNS-серверов приходится проходить пакету. Принцип, по которому работает *tracert*, прост, но довольно интересен. Сначала отправляется DNS-запрос с TTL-значением 1. Поскольку все маршрутизаторы должны уменьшать TTL-значение каждого обрабатываемого пакета на 1, это означает, что первый же маршрутизатор откажется переадресовывать данный пакет и вернет отправителю сообщение с отказом. После этого компьютер увеличивает TTL-значение на 1 и отправляет пакет снова. На этот раз пакет пройдет через первый маршрутизатор, но получит отказ от второго. Этот процесс продолжается до тех пор, пока пакет не достигнет места назначения. Понятно, что данная утилита предоставляет простой, но очень эффективный способ для просмотра пути, который DNS-запрос проходит при его передаче через Интернет.

2.8 Применение утилиты командной строки *DNSCmd*

Утилита *DNSCmd* представляет собой командную версию консоли диспетчера DNS. Она устанавливается в виде части роли DNS Server (DNS-сервер) Windows Server 2012 и позволяет администраторам создавать зоны, изменять записи и выполнять другие важные административные операции из командной строки. Полный список всех ее возможностей можно просмотреть, введя команду *dnscmd /?*.

Подобная проверка может быть осуществлена при помощи стандартной системной утилиты *DnsCmd.exe*. Утилиту можно запускать непосредственно на DNS-сервере. В этом случае в параметрах утилиты можно не указывать имя сервера. Для проверки зон можно использовать ключ */EnumZones*:

```
C:\dnscmd /EnumZones Enumerated zone list: Zone count = 3
Zone name Type Storage Properties Cache File _msdcs.khsu.ru
```

Primary AD-Forest Secure khsu.ru Primary AD-Domain Secure
Command completed successfully.

Следует заметить, что в приведенном примере зона "." представляет ссылки на корневые серверы пространства имен DNS, загружаемые при запуске DNS-сервера. Поле Type определяет тип зоны. Поле storage определяет способ хранения зоны и область распространения изменений. Поле Properties позволяет получить информацию о свойствах зоны.

Для получения более подробной информации о зоне необходимо использовать ключ /ZoneInfo.

```
c:\dnscmd /Zoneinfo khsu.ru Zone query result: Zone info:
ptr = 00083140 zone name = khsu. ru zone type = 1 update = 2
DS integrated = 1 data file = (null) using WINS = 0 using
Nbstat = 0 aging = 0 refresh interval =168 no refresh = 168
scavenge available = 3520930 Zone Masters NULL IP Array.Zone
Secondaries NULL IP Array, secure sees
rectory partition = AD-Domain flags 00000015 zone DN 4>=
DC=khsu.ru,cn=MicrosoftDNS,DC=DomainDnsZones, DC=khsu,DC=ru
Command completed successfully.
```

Для получения информации о ресурсных записях определенной зоны необходимо выполнить утилиту с ключом /EnumRecords. Ниже приводится пример работы утилиты:

```
c:\dnscmd /EnumRecords khsu.ru _tcp /Type SRV Returned
records: _gc [Aging:3520762] 600 SRV 0 100 3268 store.khsu.ru.
_kerberos [Aging:3520762] 600 SRV 0 100 88 store.khsu.ru.
_kpasswd [Aging:3520762] 600 SRV 0 100 464 store.khsu.ru.
_ldap [Aging:3520762] 600 SRV 0 100 389 store.khsu.ru. Command
completed successfully.
```

В приведенном примере отображаются все ресурсные записи типа SRV, содержащиеся в контейнере _tcp зоны khsu. ru.

В последующих версиях Windows разработчики Microsoft могут удалить команду *dnscmd.exe*. Если вы уже используете команду *dnscmd.exe* для настройки DNS-сервера и управления его работой, Microsoft рекомендует перейти на Windows PowerShell.

Для просмотра списка команд для управления DNS-сервером введите команду *Get -Command -Module DnsServer* в окне командной строки Windows PowerShell.

Контрольные вопросы.

1. Опишите назначение компонентов DNS: зона, сервер имен, доменное пространство имен.
2. Для чего предназначены прямые и обратные запросы поиска?
3. Назовите основные типы зон и их назначение.

4. Назовите основные правила именования доменов.
5. Какова максимально допустимая длина имени домена?
6. Какова максимально допустимая длина имени FQDN?
7. С какой целью используют несколько серверов имен?
8. Приведите примеры использования утилиты nslookup.
9. Можно ли одному IP-адресу присвоить несколько имен?

3 Лабораторная работа №3. Установка и управление ролью DHCP-сервер

Цель: освоить технологию установки серверных ролей и служб на Windows Server 2012 R2.

План проведения занятия:

- 1) Ознакомиться с DHCP.
- 2) Научиться устанавливать роль Active Directory – DHCP.
- 3) Научиться устанавливать службу Active Directory – Certificate Services.

3.1 Установка роли сервера DHCP в Windows Server 2012 R2

Сервер DHCP выдает клиенту IP-адрес с помощью трехшаговой процедуры.

1. Клиент DHCP загружается и рассылает DHCP-запрос на IP-адрес всем узлам в локальной сети.

2. DHCP-сервер в локальной сети получает запрос и готовится к отправке IP-адреса этому клиенту в виде DHCP-аренды IP-адреса.

3. После определения DHCP-сервером нужной информации из запроса клиента он выдает клиенту DHCP-аренду IP-адреса, в том числе и дополнительные параметры аренды - маску подсети, стандартный шлюз и (скорее всего) IP-адрес сервера.

Перед тем как устанавливать роль DHCP сервера, необходимо выполнить предварительную подготовку, например, составить план добавления областей (подсеть, диапазон), какие IP исключить из раздачи, какие параметры необходимо раздавать, это для ускорения процесса установки и настройки, также необходимо задать статический IP-адрес того сервера, на котором Вы собираетесь устанавливать роль сервера DHCP.

1. Откройте «Диспетчер серверов», но в случае, если он закрыт, нажмите Пуск->Диспетчер серверов

2. Нажимите «Add roles and services», можно непосредственно через быстрый запуск, а можно через меню «Manage», рисунок 3.1.

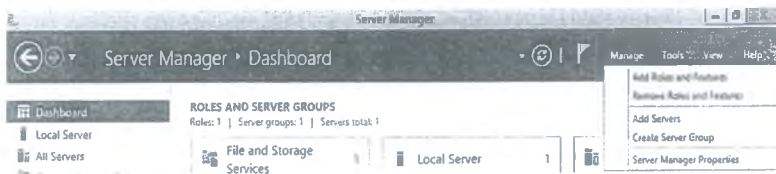


Рисунок 3.1 – Server Manager

3. Когда откроется консоль диспетчера серверов, на странице приветствия (Welcome to Server Manager) щелкните на ссылке **Add roles and features** (Добавление ролей и компонентов) в правой панели «Next», как показано на рисунке 2

4. Далее уже по умолчанию выбран необходимый пункт, т.е. «Установка ролей или компонентов», нажмите «Далее».

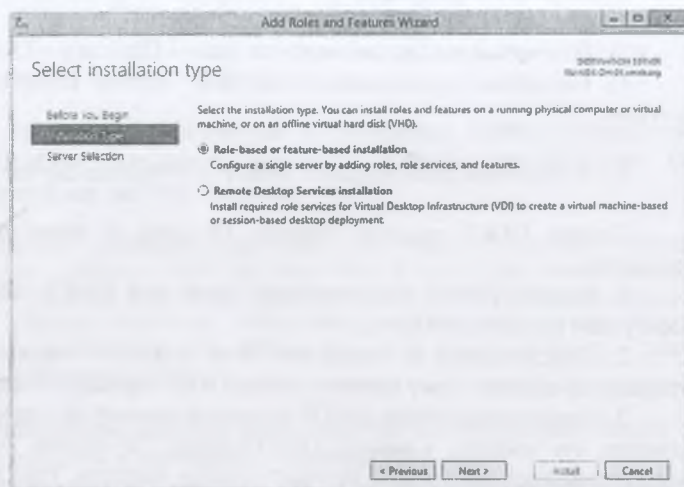


Рисунок 3.2 –Выбрать тип установки

5. Затем необходимо выбрать, на какой сервер или виртуальный жесткий диск будет устанавливаться DHCP сервер. На странице *Select Destination Server (Выбор целевого сервера)* выберите вариант *Select a Server from the Server Pool (Выбор сервера из серверного пула)* и выберите локальный сервер. Для продолжения щелкните на кнопке *Next*.

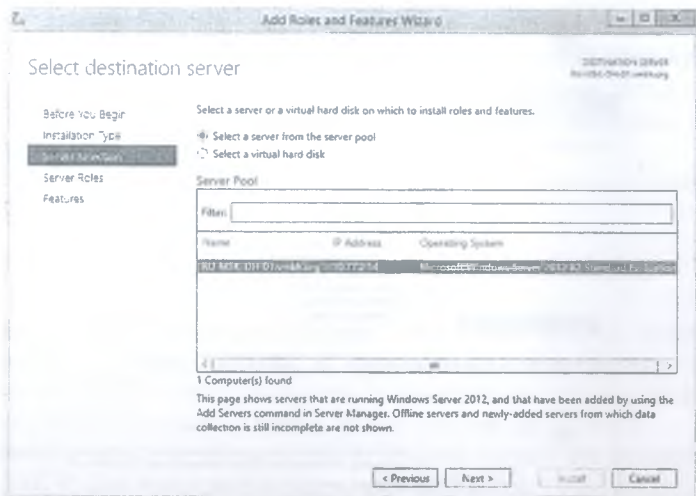


Рисунок 3.3 – Выбрать сервер назначения

6. На странице *Select Server Roles (Выбор серверной роли)* отметьте роль *DHCP Server (Сервер DHCP)*, а в раскрывающемся списке *Add Roles and Features Wizard (Мастер добавления ролей и компонентов)* выберите пункт *Add Features (Добавить компоненты)*, чтобы установить также серверные средства DHCP. Для продолжения щелкните на кнопке *Next*.

После нажатия откроется окно, в котором предложат выбрать для установки средства администрирования DHCP сервера, вы соглашаетесь, иначе далее вам все равно придется это выбирать, если вы хотите администрировать DHCP с этого компьютера.

На странице *Select Features (Выбор компонентов)* найдите группу *Remote Server Administration Tools Features (Средства администрирования удаленного сервера)*, разверните ее, затем разверните узел *Role Administration Tools (Средства администрирования ролей)* и проверьте, что отмечен компонент *DHCP Server Tools (Средства сервера DHCP)*. Нажмите *Next*.

7. На следующем шаге вам предложат выбрать необходимые компоненты, если на прошлом шаге вы выбрали «Добавить компоненты», то необходимые компоненты уже будут выбраны, если поискать в этих компонентах, то вы это увидите, нажмите *Next*.

8. Далее вас предупреждают о том, что необходимо составить план настройки DHCP и задать хотя бы один статический адрес на данном компьютере, нажмите *Next*.

9. Затем вы должны будете подтвердить установку, и в случае необходимости поставить галочку «Автоматический перезапуск конечного сервера», но в данном случае это делать не обязательно, поэтому нажмите «Установить». На странице *Installation Progress (Процесс установки)* можно

наблюдать за выполнением установки. Не закрывайте это окно до завершения процесса.

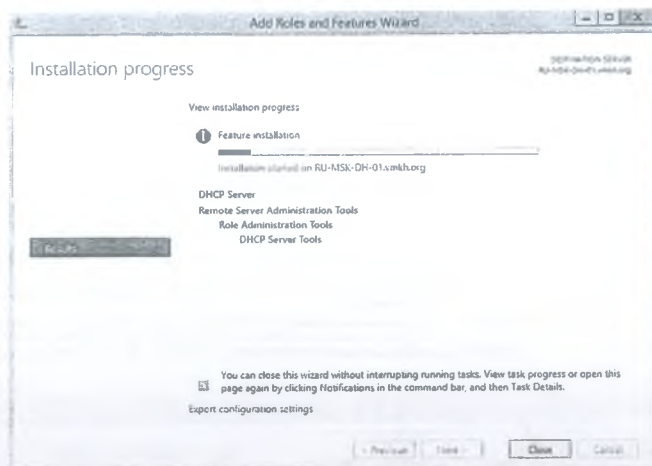


Рисунок 3.4 - Процесс установки

10. После завершения установки щелкните на ссылке *Complete DHCP Configuration (Завершить настройку DHCP)* на странице *Installation Progress*. В этом мастере можно создать соответствующие группы безопасности *DHCP Administrators (Администраторы DHCP)* и *DHCP Users (Пользователи DHCP)* на локальном компьютере и авторизовать сервер в Active Directory. Для делегирования полномочий управления DHCP сервером нажмите кнопку «*Завершение настройки DHCP*».

11. На странице *Description (Описание)* мастера настройки щелкните на кнопке *Next*.

12. Если учетная запись, от имени которой выполнен вход, имеет права на авторизацию данного сервера в Active Directory, щелкните на кнопке *Commit (Применить)*, чтобы выполнить эту задачу. Если нужна другая учетная запись, введите необходимые входные данные и щелкните на кнопке *Commit*.

13. На странице *Summary (Резюме)* проверьте правильность создания групп безопасности и завершения авторизации. Щелкните на кнопке *Close (Закрыть)*, чтобы закрыть окно мастера настройки, и еще раз на кнопке *Close*, чтобы закрыть окно мастера добавления ролей и компонентов.

После завершения установки вы вернетесь в окно диспетчера серверов. Мастер настройки после установки выполнил авторизацию *DHCP-сервера* и создал локальные группы *DHCP Administrators (Администраторы DHCP)* и *DHCP Users (Пользователи DHCP)* для делегирования сервера DHCP.

Авторизация DHCP сводится к регистрации нового сервера в Active Directory, чтобы он мог выполнять функции службы DHCP в сети. Этот мастер следует запустить после установки всех серверов DHCP. Но если авторизация сервера DHCP не требуется, пропустите этот шаг и просто позволяйте мастеру создать группы делегирования.

На этом установка сервера DHCP и его инструментальных средств завершена.

3.2 Настройка DHCP сервера на Windows Server 2012 R2

Прежде чем запустить сервер DHCP в работу, следует его авторизовать, а также создать и активировать область его действия. Авторизацию DHCP можно выполнить с помощью мастера настройки после установки DHCP, но можно и позже, из консоли серверов DHCP.

Создайте простую область DHCP IPv4 на только что авторизованном сервере DHCP. Для этого выполните следующие шаги.

1. На сервере, на котором установлены средства сервера DHCP (DHCP Server Tools), щелкните на элементе Server Manager (Диспетчер серверов) в панели задач.

2. В открывшейся консоли диспетчера серверов выберите пункт меню Tools->DHCP (Сервис->DHCP).

Также это можно сделать через «Диспетчер серверов», меню «Средства» или через Пуск-> администрирование.

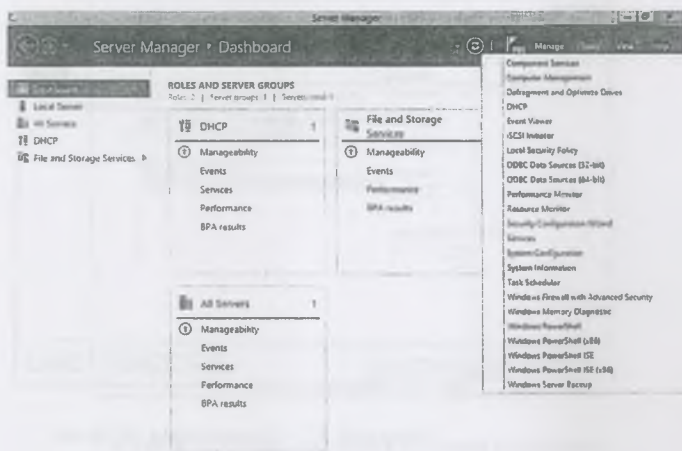


Рисунок 3.5 - Запуск средств администрирования DHCP

3. Откроется консоль DHCP. Если на ней нет списка серверов, щелкните правой кнопкой мыши на элементе DHCP в панели древовидного представления и выберите в контекстном меню пункт *Add Server (Добавить сервер)*.

4. Откроется окно Add Server. Если нужный сервер уже авторизован, выберите его в разделе *Authorized Server (Авторизованный сервер)* и щелкните на кнопке ОК. Если сервер еще не авторизован, введите имя сервера и щелкните на кнопке ОК.

5. После добавления сервера на консоль разверните узел сервера, чтобы были видны узлы 1 Pv4 и 1 Pv6. Проверьте, что около каждого из этих узлов установлен зеленый флажок - это означает успешную авторизацию в Active Directory.

6. Выберите IPv4 правой кнопкой «Создать область».

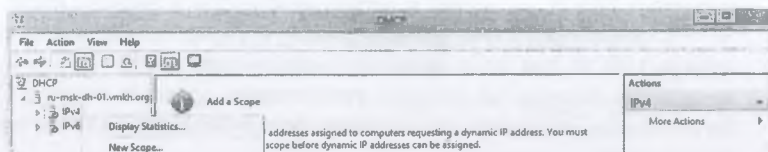


Рисунок 3.6 – Создание области

7. Далее откроется «Мастер создания области», нажмите *Next*.

8. Задайте имя нашей области и нажмите *Next*.

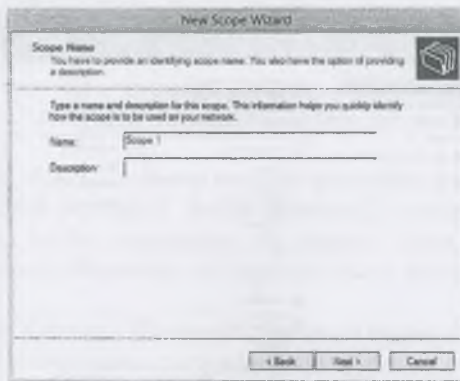


Рисунок 3.7 – Задать имя области

9. Затем необходимо сделать важный шаг - это настроить *диапазон адресов*, из которого DHCP сервер будет раздавать IP компьютерам в сети. Для примера введите диапазон с 10.77.2.1 до 10.10.2.254 с 24 маской. После настройки нажмите *Next*.

Рисунок 3.8 - Диапазон адресов

10. На странице *Add Exclusions and Delay* (Добавление исключений и задержки) введите диапазоны исключений IP-адресов или интервалы задержки для подсети DHCP, т.к. необходимо указать какие IP-адреса или диапазон адресов *исключить из раздачи*. Для того чтобы IP-адреса серверов или какой-то оргтехнике со статическими адресами, не раздавались, здесь можно указать шлюз, DNS сервера и другие. Щелкните на кнопке *Next*.

Рисунок 3.9 – Исключение адресов из раздачи

11. На странице *Lease Duration* (Длительность аренды) укажите нужную длительность аренды IP-адресов (по умолчанию 8 дней) и щелкните

на кнопке *Next*. В различных организациях часто применяются периоды 1 день, 8 часов и 30 дней.

12. На странице *Configure DHCP Options* (Настройка параметров DHCP) выберите вариант *Yes I Want to configure Options Now* (Да, я хочу настроить параметры сейчас) и щелкните на кнопке *Next*. После этого мастер проведет вас через шаги настройки наиболее употребительных параметров области DHCP, например, *Router (Default Gateway)* (Маршрутизатор (Стандартный шлюз)), *Domain Name Suffix & DNS Servers* (Суффикс доменных имен и серверы DNS) и *WINS Servers* (Серверы WINS).

Первое - укажите шлюз по умолчанию.

Второе - укажите DNS-сервера, для раздачи, здесь также можно указать название домена, но так как у вас его нет, просто введите IP адреса DNS-серверов. Сервер WINS в данном руководстве не используется. Нажмите на кнопку *Next*.

На странице *Activate Scope* (Активация области) выберите вариант *Yes, I Want to Activate This Scope Now* (Да, я хочу активировать эту область сейчас) и щелкните на кнопке *Next*.

Вы создали область и настроили основные параметры, далее произойдет завершение работы мастера создания области, нажмите «Готово».

3.3 Настройка клиентов на работу с DHCP сервером

На DHCP сервере появится запись о том, что он выдал IP-адрес такому-то компьютеру, это можно посмотреть в оснастке «DHCP», в меню «*Address Leases*» (Арендованные адреса).

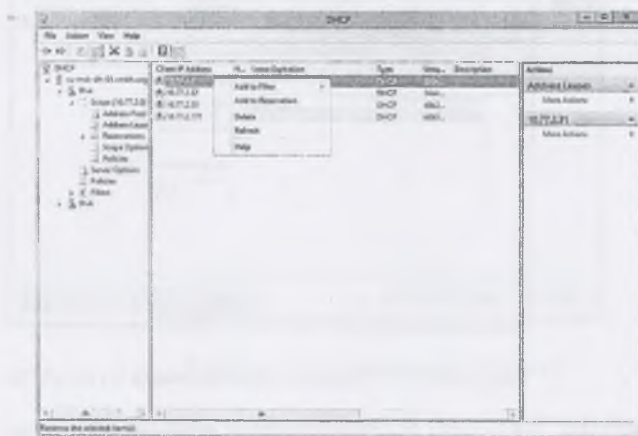


Рисунок 3.10 – Арендованные адреса DHCP

Для того чтобы зарезервировать под устройство полученный им IP-адрес, необходимо в разделе «*Address Leases*» нажать правой кнопкой мыши на одном из устройств, которое уже получило IP-адрес, и в открывшемся меню выбрать «*Add to Reservation*».

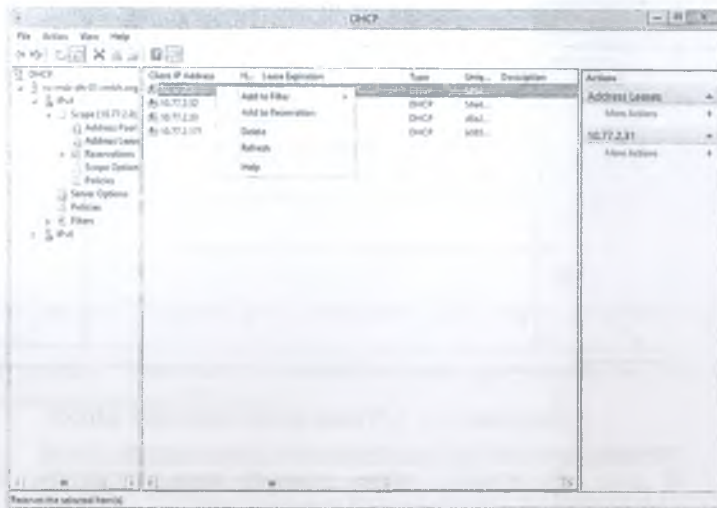


Рисунок 3.11 – Зарезервировать IP-адрес для устройства

Под указанное устройство успешно зарезервирован полученный им IP-адрес. Нажимите на кнопку «*OK*».

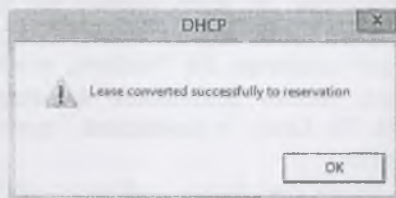


Рисунок 3.12 – Успешное резервирование

Резервацию можно добавить и вручную, указав нужный IP-адрес и MAC-адрес сетевой карты устройства.

Нажмите правой кнопкой мыши на разделе «*Reservations*» и выберите «*New Reservation*».

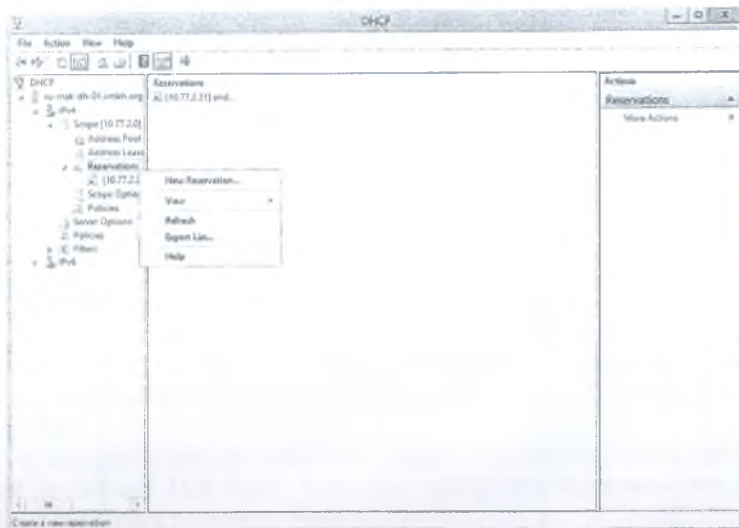


Рисунок 3.13 – Ручное резервирование адреса

В поле «Reservation name» укажите имя устройства, под которое необходимо сделать резервацию IP-адреса.

В поле «IP address» укажите IP-адрес, который необходимо зарезервировать под устройство.

В поле «MAC address» укажите MAC-адрес (Physical Address, Физический адрес) сетевой карты устройства, под которое необходимо сделать резервацию IP-адреса.

Обратите внимание: по факту именно под MAC-адрес сетевой карты резервируется IP-адрес. MAC-адрес на любом устройстве можно посмотреть в свойствах сетевого адаптера. На Windows, чтобы посмотреть MAC-адрес сетевого адаптера, можно выполнить команду «`ipconfig /all`» в командной строке. На Linux, в командной строке, необходимо выполнить команду «`ifconfig`».

В разделе «Supported types» выберите «Both». Нажмите на кнопку «Add».



Рисунок 3.14 – Резервация адреса

Резервация IP-адреса под указанный MAC-адрес устройства успешно добавлена.

В разделе “Reservations” можно увидеть все устройства, под которые были зарезервированы IP-адреса.

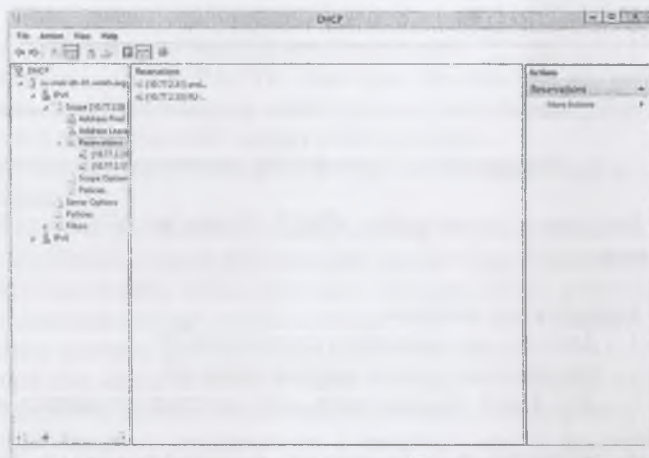


Рисунок 3.15– Зарезервированные адреса

База данных и логи сервера DHCP можно найти в каталоге “%systemroot%\system32\dhcp”. Рекомендуется выполнять резервную копию этого каталога.

dhcp.mdb – файл базы данных сервера DHCP.

j50.log – журнал всех транзакций базы данных. Этот файл используется базой данных DHCP для восстановления данных в случае необходимости.

j50.chk – файл контрольной точки.

tmp.edb – временный рабочий файл DHCP-сервера.

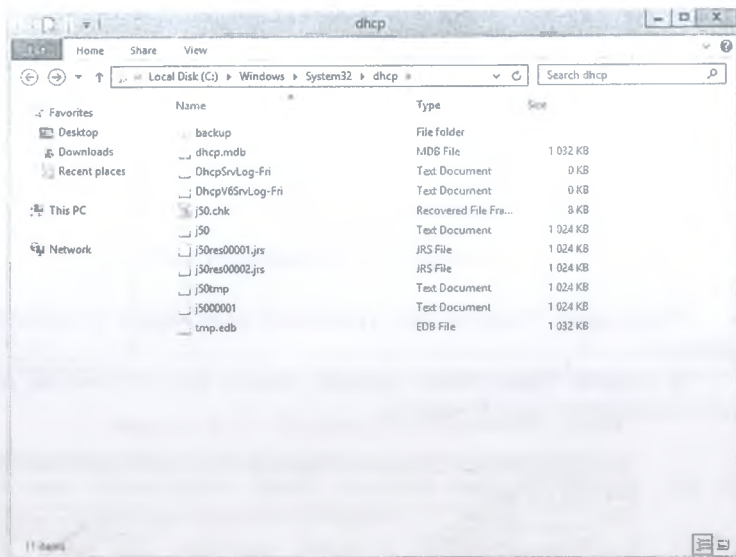


Рисунок 3.16 - Каталог базы данных и логов сервера

Установка и настройка DHCP Server на Windows Server 2012 R2 завершена.

Контрольные вопросы.

1. Для чего предназначена служба DHCP?
2. Что означает термин «аренда адреса»?
3. Для каких компьютеров сети следует применять резервирование адреса?
4. Какой IP-адрес шлюза по умолчанию определяют для подсети DHCP-сервера?
5. Какой IP-адрес вы дадите шлюзу по умолчанию для компьютера-арендатора адреса, находящегося в другой подсети (маска 255.255.240.0), если IP-адрес DHCP-сервера 201.212.96.1, а маска подсети 255.255.240.0? Как указать в настройках сетевой конфигурации узла host3 какой из интерфейсов использовать для передачи данных «по умолчанию»?
6. Что такое диапазон адресов (range)?
7. Как используется резервирование и зачем?

4 Лабораторная работа № 4. Управление учетными записями пользователей

Цель: изучение типов учетных записей пользователей, планирование учетных записей пользователей, создание и настройка учетных записей пользователей.

План проведения занятия.

1. Используя шаблон планирования учетных записей, создать девять пользователей с определенными правами.
2. Создать пользователей, используя командную строку (cmd) и средства Windows PowerShell.

4.1 Требования к результатам выполнения лабораторного практикума

Лабораторная работа направлена на ознакомление с основными понятиями учетных записей пользователей в Windows Server 2012, получения навыков при планировании, создании и настройке учетных записей.

4.1.1 Планирование новых учетных записей.

Компания «stdCOMPANY» ежегодно принимает на работу новых сотрудников (по контракту на один год и в постоянный штат). Каждому пользователю требуется собственная учетная запись.

Вам, как сетевому администратору, необходимо зарегистрировать 9 учетных записей.

Составьте свой «Шаблон планирования учетных записей» со своими именами, по образцу отдела бухгалтерии (Accounting). Помимо этого отдела, существуют еще отделы такие, как: отдел продаж (Sales), отдел кадров (HR), IT-отдел и администрация (Administration). Необходимо занести в «Шаблон планирования учетных записей» следующие сведения:

Полное имя каждого из пользователей (колонок «Полное имя»).

1) Разработать свое соглашение об именах. Затем по нему определить учетное имя каждого пользователя и записать его в колонку «Учетная запись».

2) Разработать требования к паролю каждого из пользователей и перечислить их в колонке «Требования к паролю».

3) В колонке «Местонахождение домашнего каталога» указать один из двух вариантов: локальный компьютер или сервер.

4) В колонке «Время работы» записать допустимые часы регистрации для каждого пользователя (например, 24/7, если пользователю разрешено регистрироваться круглые сутки 7 дней в неделю).

5) В колонке «Допустимые рабочие места» указать «Да», если работа пользователя с разных машин будет ограничена и «Нет» — в противном случае.

б) Заполняя шаблон, помните о некоторых тонкостях:

- постоянным сотрудникам нужно разрешить менять свои пароли;
- управление паролями временных сотрудников в целях безопасности возлагается на администратора;
- постоянные сотрудники, работающие в ночную смену, должны иметь доступ в сеть с 6 вечера до 6 утра;
- постоянные сотрудники, работающие в дневную смену, должны иметь доступ в сеть круглосуточно 7 дней в неделю;
- временные сотрудники должны иметь возможность регистрации только с назначенных им компьютеров с 8 утра до 5 вечера.

Рассмотрим в качестве примера отдел бухгалтерии (Accounting).

4.1.2 Шаблон планирования учетных записей.

Полное имя	Учетная запись	Описание	Местонахождение домашнего каталога	Время работы
Robert Palmer	robertpalmer@std5lab.net	Account-mgr		Всегда
Barbara Blade	barbarablade@std5lab.net	1 st accountant		Всегда
John West	johnwest@std5lab.net	2 nd accountant		18.00-6.00 24/7
Ann Spencer	annspencer@std5lab.net	3rd accountant		Всегда
Taylor Bass	taylorbass@std5lab.net	4rd accountant		18.00-6.00 24/7
Keira Hudson	keirahudson@std5lab.net	5 th accountant		8.00-17.00

Имя домена *std5lab.net* является примером в данном шаблоне. Вам следует указывать свое имя домена вместо него.

4.2 Теоретический материал

4.2.1 Основные понятия.

Учетная запись пользователя — основа защиты Windows Server 2012, это уникальный личный код, предоставляющий право на доступ к ресурсам.

Каждый пользователь, регулярно работающий в домене или на одном из его компьютеров, должен иметь учетную запись. Учетные записи позволяют администратору контролировать доступ пользователей к ресурсам домена и локальным ресурсам компьютера, например, ограничить часы, когда пользователь может зарегистрироваться в домене.

4.2.2 Стандартные учетные записи.

При установке Windows Server 2012 создаются стандартные учетные записи пользователей. Они предназначены для начальной настройки, необходимой для развития сети. Рассмотрим три типа стандартных учетных записей:

- *встроенные (built-in)* учетные записи пользователей устанавливаются вместе с ОС, приложениями и службами;
- *предопределенные (predefined)* учетные записи пользователей устанавливаются вместе с ОС;
- *неявные (implicit)* - специальные группы, создаваемые неявно при обращении к сетевым ресурсам; их также называют специальными объектами (special identities).

Примечание - удалить пользователей и группы, созданные ОС, нельзя.

4.2.3 Встроенные учетные записи.

Все системы Windows Server 2012 обладают тремя встроенными учетными записями:

- *локальная система (Local System)* — учетная псевдозапись для выполнения системных процессов и обработки задач системного уровня, доступная только на локальной системе.
- *Local Service* — учетная псевдозапись для запуска служб, которым необходимы дополнительные привилегии или права входа на локальной системе.
- *Network Service* — учетная псевдозапись для служб, которым требуются дополнительные привилегии или права входа на локальной системе и в сети.

4.2.4 Типы пользовательских учетных записей.

В Windows Server 2012 определены пользовательские учетные записи двух типов:

- *доменные учетные записи (domain user accounts)* определены в Active Directory. Посредством системы однократного ввода пароля такие учетные записи могут обращаться к ресурсам во всем домене. Они создаются в консоле (оснастке) *Active Directory — пользователи и компьютеры* (Active Directory Users and Computers);
- *локальные учетные записи (local user accounts)* определены на локальном компьютере, имеют доступ только к его ресурсам и должны аутентифицироваться, прежде чем получают доступ к сетевым ресурсам. Локальные учетные записи пользователей создают в консоле (оснастке) *«Локальные пользователи и группы» (Local Users and Groups)*.

Примечание: локальные учетные записи пользователей и групп хранятся только на рядовых серверах и рабочих станциях. На первом контроллере домена они перемещаются в Active Directory и преобразуются в доменные учетные записи.

4.2.5 Предопределенные учетные записи пользователей.

Вместе с Windows Server 2012 устанавливаются некоторые записи: Администратор (Administrator), Гость (Guest), ASPNET и Support. На рядовых серверах предопределенные учетные записи являются локальными для той системы, где они установлены.

У предопределенных учетных записей есть аналоги в Active Directory, которые имеют доступ по всему домену и совершенно независимы от локальных учетных записей на отдельных системах.

4.2.6 Учетная запись Администратор (Administrator).

Эта предопределенная учетная запись обладает полным доступом к файлам, папкам, службам и другим ресурсам; ее нельзя отключить или удалить. В Active Directory она обладает доступом и привилегиями во всем домене. В остальных случаях Администратор (Administrator) обычно имеет доступ только к локальной системе. Файлы и папки можно временно закрыть от администратора, но он имеет право в любой момент вернуть себе контроль над любыми ресурсами, сменив разрешения доступа.

4.2.7 Учетная запись Гость (Guest).

Эта учетная запись предназначена для пользователей, которым нужен разовый или редкий доступ к ресурсам компьютера или сети. Гостевая учетная запись обладает весьма ограниченными системными привилегиями, тем не менее применяйте ее с осторожностью, поскольку она потенциально снижает безопасность.

4.3 Создание учетных записей пользователей для компьютеров, состоящих в домене

В серверной операционной системе Windows Server 2012 или Windows Server 2012 R2 в домене Active Directory учетные записи пользователей можно создавать несколькими способами.

4.3.1 Создание пользователей при помощи оснастки «Active Directory – пользователи и компьютеры».

В подавляющем большинстве случаев системные администраторы для создания основных принципов безопасности предпочитают использовать оснастку «Active Directory – пользователи и компьютеры». Этот метод является наиболее удобным, так как для создания принципов 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 создания нового пользователя в домене при помощи оснастки «*Active Directory – пользователи и компьютеры*» нужно сделать следующее:

1) Открыть оснастку «*Active Directory – пользователи и компьютеры*».

2) В дереве консоли разверните узел, предоставляющий домен и найдите контейнер, в котором нужно создать учетную запись пользователя.

3) Нажмите на подразделение или контейнер правой кнопкой мыши, выберите опцию «Создать» и примените команду «Пользователь».

4) В появившемся диалоговом окне «Новый объект - Пользователь» введите следующую информацию:

- в поле «Имя» введите имя пользователя;
- в поле «Инициалы» введите его инициалы (чаще всего инициалы не используются);

- в поле «Фамилия» введите фамилию создаваемого пользователя;
- поле «Полное имя» используется для создания таких атрибутов создаваемого объекта, как основное имя CN (Common Name) и отображения свойств имени. Это поле должно быть уникальным во всем домене, и заполняется автоматически, а изменять его стоит лишь в случае необходимости;

- 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 @;

- 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.

5) 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 «Next». Эта страница мастера изображена на следующей иллюстрации:

6) В последнем диалоге можно просмотреть введенные параметры и нажать на кнопку «Готово» для создания нового пользователя.

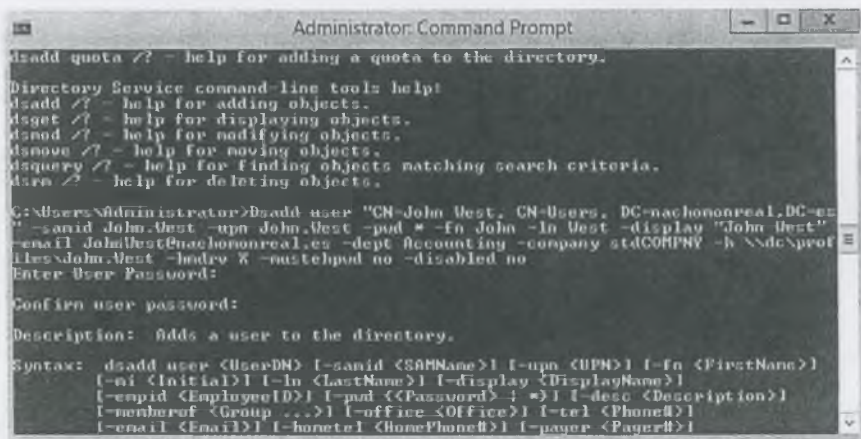
4.3.2 Создание пользователей с помощью командной строки.

Для автоматизации создания любых объектов в домене Active Directory можно использовать команду **DSADD USER UserDN**, при помощи которой можно создавать объекты пользователей и принимать параметры, указывающие его свойства. Нового пользователя при помощи командной строки можно создать следующим образом: 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. Рассмотрите и приведите пример в лабораторной работе самые распространенные из них.

Запускать командную строку следует от имени администратора.



```
Administrator: Command Prompt

Dsadd quota /? - help for adding a quota to the directory.

Directory Service command-line tools help!
dsadd /? - help for adding objects.
dsget /? - help for displaying objects.
dsmod /? - help for modifying objects.
dsmove /? - help for moving objects.
dsquery /? - help for finding objects matching search criteria.
dsrm /? - help for deleting objects.

C:\Users\Administrator>Dsadd user "CN=John West, CN=Users, DC=nachononreal,DC=ec"
-samid John.West -upn John.West -pwd * -fn John -ln West -display "John West"
-email JohnWest@nachononreal.es -dept Accounting -company stdCOMPNY -h %dc%\prof
iles\John.West -hmdir % -natchpod no -disabled no
Enter User Password:
Confirm user password:

Description: Adds a user to the directory.

Syntax: dsadd user <UserDN> [-samid <SAMName>] [-upn <UPN>] [-fn <FirstName>]
[-mi <Initial>] [-ln <LastName>] [-display <DisplayName>]
[-empid <EmployeeID>] [-pwd <Password>] [-*] [-desc <Description>]
[-memberof <Group ...>] [-office <Office>] [-tel <Phone#>]
[-email <Email>] [-hometel <HomePhone#>] [-pager <Pager#>]
```

Рисунок 4.1 - Создание пользовательской учетной записи средствами утилиты Dsadd

```

C:\Users\Administrator>Dsadd user "CN=Egor Zernov, OU=Users, OU=Administration,
OU=Chocolate Factory, DC=ipic1, DC=ru" -samid Egor.Zernov -upn Egor.Zernov -pwd
* -fn Egor -ln Zernov -display "Egor Zernov" -tel "+7707-195-32-17" -email egor.
zernov@ipic1.ru -dept Administration -company "Chocolate Factory Rakhat" -hndrv
* -disabled no
Enter User Password:
Confirm user password:
dsadd succeeded:CN=Egor Zernov,OU=Users,OU=Administration,OU=Chocolate Factory,D
C=ipic1,DC=ru

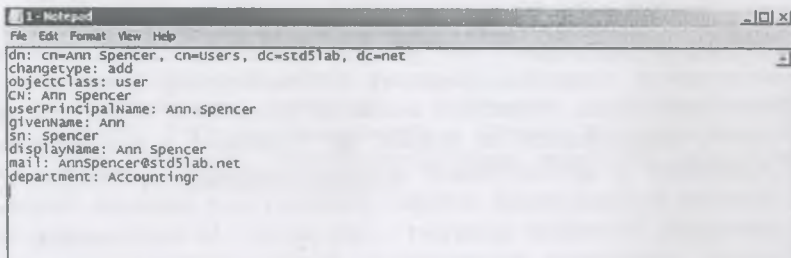
C:\Users\Administrator>Dsadd user "CN=Uladimir Zernov, OU=Users, OU=Administrati
on, OU=Chocolate Factory, DC=ipic1, DC=ru" -samid Uladimir.Zernov -upn Uladimir.
Zernov -pwd * -fn Uladimir -ln Zernov -display "Uladimir Zernov" -tel "+7707-195
-33-14" -email uladimir_zernov@ipic1.ru -dept Administration -company "Chocolate
Factory Rakhat" -title "Deputy Director" -hndrv * -disabled no
Enter User Password:
Confirm user password:
dsadd succeeded:CN=Uladimir Zernov,OU=Users,OU=Administration,OU=Chocolate Facto
ry,DC=ipic1,DC=ru
C:\Users\Administrator>

```

Рисунок 4.2 - Создание 2-х пользовательских учетных записей с другими свойствами

4.3.3 Импорт пользователей с помощью команды LDIFDE.

Утилита командной строки *Ldifde* позволяет также импортировать или экспортировать объекты Active Directory, используя файловый формат *LDIF* (*Lightweight Directory Access Protocol Data Interchange File*). Данный файловый формат состоит из блока строк, которые образуют конкретную операцию. В отличие от файлов CSV, в данном файловом формате каждая отдельная строка представляет собой набор атрибутов, после которого следует двоеточие и само значение текущего атрибута. Также как и в CSV файле, первой строкой обязан быть атрибут DN. За ним следует строка *changeType*, которая указывает тип операции (*add*, *change* или *delete*). Для того чтобы научиться разбираться в этом файловом формате, вам нужно выучить, по крайней мере, ключевые атрибуты принципов безопасности. Пример предоставлен ниже.



```

1 - Notepad
File Edit Format View Help
dn: cn=Ann Spencer, cn=users, dc=std5lab, dc=net
changetype: add
objectClass: user
CN: Ann Spencer
userPrincipalName: Ann.Spencer
givenName: Ann
sn: spencer
displayName: Ann Spencer
mail: AnnSpencer@std5lab.net
department: Accounting

```

Рисунок 4.3 - Пример LDF файла

Синтаксис команды следующий:

```
Ldifde -i -f filename.csv -k
```

где

- i. Параметр, который отвечает за режим импорта. Если вы не укажете данный параметр, то эта команда будет использовать по умолчанию режим экспорта;
- f. Параметр, идентифицирующий имя файла, которое предназначено для импорта или экспорта;
- k. Параметр, предназначенный для продолжения импорта пропуская все возможные ошибки;
- v. Параметр, используя который, вы можете вывести подробную информацию;
- j. Параметр, отвечающий за расположение файла журнала;
- d. Параметр, указывающий корень поиска LDAP;
- f. Параметр, предназначенный для фильтра поиска LDAP;
- p. Представляет собой область или глубину поиска;
- l. Предназначен для указания списка атрибутов с разделительными запятыми, который будет включен в экспорт результирующих объектов.

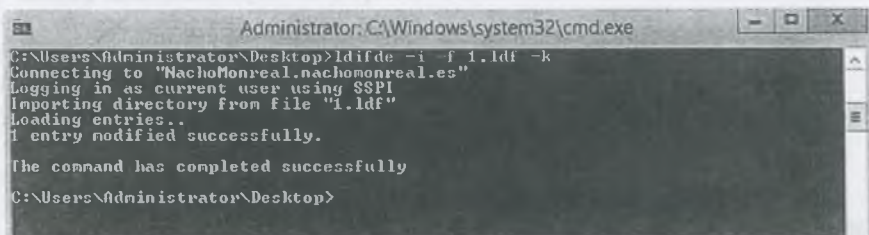


Рисунок 4.4 – Использование команды Ldifde

4.3.4 Создание пользователей с помощью Windows PowerShell.

В операционной системе Windows Server 2012 R2 появилась возможность управлять объектами Active Directory средствами Windows PowerShell. Среда PowerShell считается мощнейшей оболочкой командной строки, разработанной на основе *.Net Framework* и предназначенной для управления и автоматизации администрирования операционных систем Windows и приложений, которые работают под данными операционными системами. PowerShell включает в себя свыше 150 инструментов командной строки, называемых командлетами, которые предоставляют возможность управления компьютерами предприятия из командной строки. Данная оболочка является компонентом операционной системы.

Для создания нового пользователя в домене Active Directory используется командлет *New-ADUser*, большинство значений свойств которого можно добавлять при помощи параметров данного командлета. Для отображения имени LDAP используется параметр *-Path*. Данный параметр задает контейнер или подразделение (OU) для нового пользователя. Если параметр *Path* не задан, командлет создает объект пользователя в контейнере по умолчанию для объектов пользователя в данном домене, то есть в контейнере *Users*. Для того чтобы указать пароль, используется параметр *-AccountPassword* со значением *Read-Host -AsSecureString* (*Пароль для вашей учетной записи*). Также стоит обязательно обратить внимание на то, что значением параметра *-Country* выступает именно код страны или региона выбранного пользователем языка. Синтаксис командлета следующий:

```
New-ADUser [-Name] <string> [-AccountExpirationDate
<System.Nullable[System.DateTime]>] [-AccountNotDelegated
<System.Nullable[bool]>] [-AccountPassword <SecureString>]
[-AllowReversiblePasswordEncryption <System.Nullable[bool]>]
[-AuthType {Negotiate | Basic}] [-CannotChangePassword
<System.Nullable[bool]>] [-Certificates <X509Certificate[]>]
[-ChangePasswordAtLogon <System.Nullable[bool]>] [-City
<string>] [-Company <string>] [-Country <string>]
[-Credential <PSCredential>] [-Department <string>] [-
Description <string>] [-DisplayName <string>] [-Division
<string>] [-EmailAddress <string>] [-EmployeeID <string>] [-
EmployeeNumber <string>] [-Enabled <System.Nullable[bool]>]
[-Fax <string>] [-GivenName <string>] [-HomeDirectory
<string>] [-HomeDrive <string>] [-HomePage <string>] [-
HomePhone <string>] [-Initials <string>] [-Instance
<ADUser>] [-LogonWorkstations <string>] [-Manager <ADUser>]
[-MobilePhone <string>] [-Office <string>] [-OfficePhone
<string>] [-Organization <string>] [-OtherAttributes
<hashtable>] [-OtherName <string>] [-PassThru <switch>]
[-PasswordNeverExpires <System.Nullable[bool]>] [-
PasswordNotRequired <System.Nullable[bool]>] [-Path
<string>] [-POBox <string>] [-PostalCode <string>] [-
ProfilePath <string>] [-SamAccountName <string>] [-
ScriptPath <string>] [-Server <string>] [-
ServicePrincipalNames <string[]>] [-SmartcardLogonRequired
<System.Nullable[bool]>] [-State <string>]
[-StreetAddress <string>] [-Surname <string>] [-Title
<string>] [-TrustedForDelegation <System.Nullable[bool]>]
[-Type <string>] [-UserPrincipalName <string>] [-Confirm] [-
WhatIf] [<CommonParameters>]
```

Пример:

```
New-ADUser -SamAccountName 'Evgeniy.Romanov' -Name 'Evgeniy
Romanov' -GivenName 'Evgeniy' -Surname 'Romanov' -
DisplayName 'Evgeniy Romanov' -Path
```

```
'OU=dsdsfdfsdf,OU=ASD,DC=aipet,DC=kz' -CannotChangePassword
$false -ChangePasswordAtLogon $true -City 'Almaty' -State
'Almaty' -Country RK -Department 'dsdsfdfsdf' -Title 'Saler'
-UserPrincipalName 'Evgeniy.Romanov@aipet.kz' -EmailAddress
'evgeniy.romanov@aipet.kz' -Enabled $true -AccountPassword
(Read-Host -AsSecureString "AccountPassword")
```

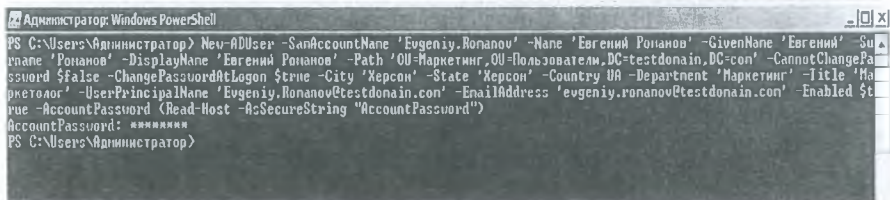


Рисунок 4.5 - Создание учетной записи пользователя средствами Windows PowerShell

4.4 Настройка атрибутов учетных записей пользователей

Любой системный администратор знает, что самыми распространенными задачами, выполняемыми в доменных службах Active Directory, являются задачи, связанные с управлением принципами безопасности такими, как учетные записи пользователей. Но создание учетной записи пользователя – это лишь первый шаг всего жизненного цикла пользователей в домене Active Directory. После создания учетной записи пользователя вам еще нужно отконфигурировать атрибуты объекта пользователя в зависимости от требований вашей организации, а также, возможно, настроить определенные свойства учетной записи. При создании пользовательской учетной записи средствами графического интерфейса, а именно: при помощи оснастки *«Active Directory – пользователи и компьютеры»* – вы заполняете такие атрибуты объекта пользователя, как имя пользователя, фамилию, имя входа, а также пароль. При создании объекта одни атрибуты являются обязательными, а другие – опциональными. Объект пользователя может содержать свыше 250 атрибутов, как созданных операционной системой, так и созданных системным администратором.

Из всех атрибутов объектов учетных записей пользователей, существуют всего *шесть обязательных атрибутов*:

- *sn*. Атрибут, который используется для отображения свойств имени. Это поле должно быть уникальным во всем домене, и заполняется автоматически;

- *instanceType*. Текущий атрибут указывает экземпляр объекта пользователя, который будет использоваться в качестве шаблона для нового объекта пользователя;

- *objectCategory*. Данный атрибут определяет категорию схемы Active Directory. Например,
CN=Person, CN=Schema, CN=Configuration, DC=BIOPHARMACEUTIQUE, DC=COM;
- *objectClass*. Этот атрибут определяет класс объекта;
- *objectSid*. Определяет идентификатор безопасности объекта, который назначается автоматически;
- *sAMAccountName*. Задаёт имя учётной записи SAM пользователя. Максимальная длина описания – 256 знаков. Конфигурируется данный атрибут непосредственно на основе данных, обеспечиваемых при создании учётной записи пользователя.

4.4.1 Изменение атрибутов на вкладках свойств учётной записи пользователя.

В большинстве случаев дополнительные свойства пользовательских учётных записей конфигурируются при помощи оснастки «*Active Directory – пользователи и компьютеры*». Для изменения объекта пользователя откройте диалоговое окно свойств учётной записи. В данном диалоговом окне, атрибуты объекта пользователя распределяются по нескольким обширным категориям на различных вкладках. Большинство атрибутов объекта пользователя вполне понятны.

Рассмотрим шесть основных вкладок, которые в первую очередь подлежат изменениям с соответствующими атрибутами:

- *вкладка «Общие»*. Данная вкладка содержит свойство имени, которое настраивается при создании объекта пользователя, а также его основное описание и контактные данные. На данной вкладке вы можете отконфигурировать девять атрибутов объекта пользователя, а именно: имя пользователя (атрибут *givenName*), фамилию (атрибут *sn*), инициалы (атрибут *initials*), выводимое имя (атрибут *displayName*), описание объекта (атрибут *description*), номер комнаты (атрибут *physicalDeliveryOfficeName*), контактный номер телефона (атрибут *telephoneNumber*), адрес электронной почты (атрибут *mail*), а также адрес веб-сайта пользователя (атрибут *wwwHomePage*). Кроме того, на данной вкладке вы можете указать дополнительный телефонный номер, который указывается атрибутом *otherTelephone*. Также вы можете указать дополнительный веб-сайт, определяемый атрибутом *url*. Если вы добавите более двух номеров телефона или веб-сайтов, они будут записываться в последние атрибуты через точку с запятой «;»;

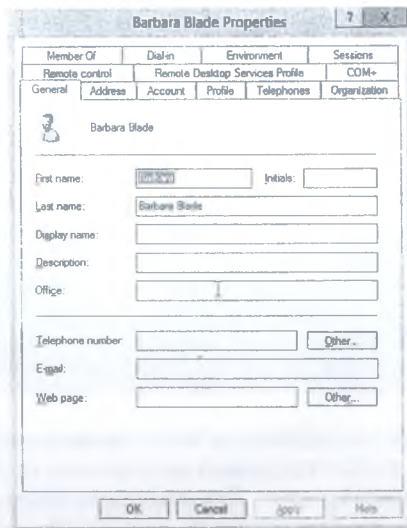


Рисунок 4.6 - Вкладка «Общие» диалогового окна свойств объекта пользователя

– вкладка «Адрес». На этой вкладке вы можете указать контактные сведения о месте проживания вашего сотрудника. Для редактирования доступны шесть тестовых полей и, соответственно, шесть атрибутов. Вы можете изменять следующие параметры: улицу, на которой живет ваш сотрудник (атрибут *streetAddress*), номер дома, который можно указать в текстовом поле «Почтовый ящик» (атрибут *postOfficeBox*), город, в котором живет ваш пользователь (атрибут *l*). Помимо этого, вы можете указать область или край (атрибут *st*), почтовый индекс (атрибут *postalCode*), страну (за этот параметр отвечают три атрибута, а именно: *c* – буквенное сокращение страны, *co* – название страны, *countryCode* – код страны);

– вкладка «Учетная запись». Для администрирования данная вкладка является самой важной, так как именно здесь вы можете настроить имена входа, пароль и параметры учетной записи. Здесь вы можете задать следующие атрибуты: имя входа пользователя (атрибут *userPrincipalName*), имя входа пользователя пред-Windows 2000 (атрибут *sAMAccountName*), время входа пользователя (определяется атрибутом *logonHours* в шестнадцатеричном формате). Также вы можете указать компьютеры, на которые пользователь может выполнять вход (атрибут *userWorkstations*). Если учетная запись пользователя заблокирована, то вы можете ее разблокировать, установив соответствующий флажок. Помимо этого, вы можете добавить следующие параметры учетной записи: требовать смены пароля при следующем входе в систему, запрещение смены пароля пользователем, установка неограниченного срока действия пароля и прочее.

Также вы можете указать срок действия учетной записи (атрибут *accountExpires*). Откройте окно *Active Directory Users and Computers* выберите вкладку *User* и выберите пользователя, которому хотите ограничить время работы. Далее нужно выбрать вкладку *Account* и нажать *Logon Hours*. Далее нужно указать, в какое время сотрудник имеет право работать;

- вкладка «Профиль». На этой вкладке вы можете настроить путь к профилю пользователя (атрибут *profilePath*), сценарий входа (атрибут *scripPath*), а также домашнюю папку, указав локальный путь (атрибут *homeDirectory*) или сетевой диск (атрибут *homeDrive*);

- вкладка «Телефоны». Текущая вкладка предназначена для заполнения таких контактных сведений о пользователе, как номера его телефонов. На этой вкладке доступно для редактирования шесть параметров, а именно: домашний, в котором вы можете указать домашний номер телефона пользователя (атрибут *homePhone*), номер пейджера (атрибут *pager*), номер мобильного телефона (атрибут *mobile*). Также вы можете указать номер факса (атрибут *facsimileTelephoneNumber*) или номер IP-телефона (атрибут *ipPhone*). Помимо этого, на данной вкладке размещено текстовое поле «Заметки», сопоставленное с атрибутом *info*, которое используется для занесения дополнительной информации. Также вы можете добавить дополнительные номера телефонов (например, за дополнительный номер мобильного телефона отвечает атрибут *otherMobile*, за дополнительный номер пейджера – *otherPager*, за дополнительные номера домашнего телефона, факса и IP-телефона, соответственно, *otherHomePhone*, *otherFacsimileTelephoneNumber* и *otherIpPhone*);

- вкладка «Организация». Эта вкладка содержит такую информацию, которая относится к должности, отделу пользователя и т.п. Для изменения на этой вкладке доступны пять следующих опций: должность данного сотрудника (атрибут *title*), название отдела (атрибут *department*), наименование организации (атрибут *company*). Помимо этого на данной вкладке вы можете указать непосредственного начальника для текущего пользователя (атрибут *manager*), а также просмотреть всех прямых подчиненных в поле «Прямые подчиненные».

4.4.2 Просмотр и изменение атрибутов, не отображаемых в свойствах объектов пользователей.

Для того чтобы просмотреть все атрибуты, которые принадлежат конкретному пользователю, вам нужно в диалоговом окне свойств текущего пользователя перейти на вкладку «Редактор атрибутов». По умолчанию данная вкладка не отображена, и для того, чтобы она отобразилась, вам нужно в меню «Вид» самой оснастки установить флажок на опции «Дополнительные компоненты» (*Advanced Features*). Редактор атрибутов отображает все системные атрибуты для текущего объекта. С помощью кнопки «Фильтр» вы можете отфильтровать вывод системных атрибутов в

таком виде, как вам будет удобнее с ними работать. Вы можете просмотреть обязательные атрибуты, установив соответствующий флажок, дополнительные атрибуты, только те атрибуты, в которых указаны значения, а также атрибуты, доступные для записи.

Обратными ссылками называются атрибуты, которые образуются в результате ссылок на объект из других объектов. Рассмотрим простой пример: при добавлении пользователя в группу изменяется многозначный атрибут группы *member*, в который добавляется отличительное имя пользователя, называемое прямой ссылкой. В свою очередь, в объекте пользователя, при ссылке на пользователя атрибутом *member* группы, атрибут *memberOf* обновляется автоматически.

4.5 Защита учетной записи Administrator

4.5.1 Создание новой учетной записи с правами администратора домена.

Если у Вас еще нет учетной записи (отличной от встроенной учетной записи Администратор), входящей в состав группы Администраторы домена, создайте ее и используйте для выполнения процедур, представленных в данном руководстве. Как администратор сети, Вы будете использовать эту учетную запись только для выполнения задач, требующих полномочий администратора домена. Завершайте сеанс работы под этой учетной записью после выполнения всех необходимых задач. Если на компьютер с запущенным сеансом работы администратора домена попадет вирус, то он будет выполняться в контексте администратора домена и сможет использовать все его привилегии, чтобы заразить остальные компьютеры в сети. Для повседневного управления данными такими, как работа с приложениями Microsoft Office или прием и отправка почтовых сообщений, создайте отдельную учетную запись пользователя, но не добавляйте ее в группу администраторов домена. Советы и рекомендации по использованию административных учетных записей будут представлены в следующих разделах данного руководства.

Для создания новой учетной записи с правами администратора домена выполните следующие действия:

- 1) Войдите в систему под учетной записью из группы *Администраторы домена* и откройте оснастку *Active Directory – пользователи и компьютеры*.

Примечание - снимки экранов, представленные в этом документе, сделаны в лабораторной среде и могут немного отличаться от того, что Вы видите на экране своего компьютера.

- 2) Правой кнопкой мыши щелкните на контейнере *Users* и в меню *Создать* выберите пункт *Пользователь*.

- 3) Заполните поля *Имя*, *Фамилия* и *Имя входа пользователя*, и нажмите кнопку *Далее*. При создании административных учетных записей Вы можете

использовать общепринятые соглашения о создании имен. В этом примере Вы можете использовать добавочный суффикс «-ALT», который будет содержаться в имени входа административной учетной записи пользователя.

4) Задайте и подтвердите пароль пользователя, снимите флажок *Требовать смену пароля при следующем входе в систему* и нажмите кнопку *Next*.

5) Просмотрите информацию о пользователе и нажмите кнопку *Готово*.

6) Выберите контейнер *Users* и в области сведений дважды щелкните на имени группы *Администраторы домена*.

7) Перейдите на вкладку *Члены группы*.

8) Нажмите кнопку *Добавить*, в диалоговом окне *Выбор: «Пользователи», «Контакты» или «Компьютеры»* введите имя входа административной учетной записи, которую Вы только что создали, и нажмите кнопку *ОК*.

9) Убедитесь, что новая учетная запись отображается в списке членов группы *Администраторы домена*.

Каждый установленный экземпляр службы каталогов Active Directory имеет в каждом домене учетную запись с именем *Администратор*, которая не может быть удалена или заблокирована. В Windows Server 2012 эта учетная запись может быть отключена, но она автоматически включается вновь, когда Вы запускаете компьютер в безопасном режиме.

Злоумышленники, намеревающиеся получить доступ к системе, в первую очередь пытаются заполучить пароль учетной записи *Администратор*, поскольку она обладает самыми широкими полномочиями. По этой причине следует переименовать эту учетную запись и изменить ее описание так, чтобы никаким образом нельзя было определить, что она является административной учетной записью. В дополнение к этому создайте ложную учетную запись с именем *Администратор*, не имеющую никаких специальных разрешений и полномочий.

Всегда задавайте для учетной записи *Администратор* длинный, сложный пароль. Используйте различные пароли для учетной записи *Администратор* и для учетной записи администратора восстановления служб каталогов.

4.5.2 Переименование встроенной учетной записи «Администратор».

Следующая процедура удаляет из учетной записи всю явную информацию, которая может сообщить злоумышленнику о том, что данная учетная запись имеет права администратора. Хотя злоумышленнику, обнаружившему встроенную учетную запись *Администратор*, будет необходимо узнать ее пароль, переименование этой учетной записи обеспечивает дополнительный уровень защиты от атак. В целях такой защиты используйте вымышленные имя и фамилию, задавая их в том же формате, что и для остальных учетных записей пользователей. Не используйте имя и фамилию из следующего примера.

Для переименования встроенной учетной записи «Администратор» выполните следующие действия:

1) Войдите в систему под учетной записью из группы *Администраторы домена* и откройте оснастку *Active Directory – пользователи и компьютеры*.

2) В дереве консоли выберите контейнер *Users*.

3) В области сведений щелкните правой кнопкой мыши на имени учетной записи *Администратор* и в контекстном меню выберите команду *Переименовать (Rename)*.

4) Введите вымышленные имя и фамилию пользователя и нажмите клавишу *Enter*.

4.5.3 Создание ложной учетной записи «Администратор».

После того как Вы спрятали встроенную учетную запись администратора, следующая процедура добавляет дополнительный уровень защиты. Злоумышленника, пытающегося получить пароль учетной записи *Администратор*, можно обмануть, и его усилия будут направлены на взлом учетной записи, которая на самом деле не обладает никакими специальными привилегиями.

Для создания ложной учетной записи «Администратор» выполните следующие действия:

1) Войдите в систему под учетной записью из группы *Администраторы домена* и откройте оснастку *Active Directory – пользователи и компьютеры*.

2) Правой кнопкой мыши щелкните на контейнере *Users* и в меню *Создать* выберите пункт *Пользователь*.

3) В поля *Имя* и *Имя входа пользователя* введите имя *Администратор* и нажмите кнопку *Далее*.

4) Задайте и подтвердите пароль.

5) Снимите флажок *Требовать смену пароля при следующем входе в систему*.

6) Просмотрите информацию о пользователе и нажмите кнопку *Готово*.

7) В области сведений щелкните правой кнопкой мыши на имени учетной записи *Администратор* и в контекстном меню выберите пункт *Свойства*.

8) Перейдите на вкладку *Общие*, введите текст «Встроенная учетная запись администратора компьютера/домена» в поле *Описание* и нажмите кнопку *ОК*.

4.6 Защита гостевой учетной записи

Учетная запись *Гость (Guest)* позволяет пользователям, не имеющим доменной учетной записи, подключаться к домену в качестве гостя. По

умолчанию эта учетная запись отключена и должна оставаться в этом состоянии. Тем не менее, переименование этой учетной записи обеспечит дополнительный уровень защиты от неавторизованного доступа. Для такой защиты используйте вымышленные имя и фамилию, задавая их в том же формате, что и для остальных учетных записей пользователей.

Для переименования встроенной учетной записи *Гость (Guest)* выполните следующие действия:

1) Войдите в систему под учетной записью из группы *Администраторы домена* и откройте оснастку *Active Directory – пользователи и компьютеры*.

2) В дереве консоли выберите контейнер *Users*.

3) В области сведений щелкните правой кнопкой мыши на имени учетной записи *Гость (Guest)* и в контекстном меню выберите команду *Переименовать (Rename)*.

4) Введите вымышленные имя и фамилию пользователя и нажмите клавишу *Enter*.

5) В области сведений щелкните правой кнопкой мыши на новом имени учетной записи и в контекстном меню выберите пункт *Свойства (Properties)*.

6) Перейдите на вкладку *Общие (General)*, удалите текст *«Встроенная учетная запись для доступа гостей к компьютеру или домену» (Built-in account for guest access to the computer/domain)* из поля *Описание (Description)* и введите новое описание, такое же, как и у остальных учетных записей пользователей (во многих организациях это поле оставляют пустым).

7) Измените значения полей *Имя (Name)* и *Фамилия (Last name)* в соответствии с введенным именем учетной записи.

8) Перейдите на вкладку *Учетная запись (Account)* и в поле *Имя входа пользователя (User logon name)* введите новое имя в том же формате, что и для остальных учетных записей, например, первую букву имени и фамилию.

Удостоверьтесь, что учетная запись отключена (напротив имени должен отображаться красный значок с крестиком). Если учетная запись не отключена, щелкните правой кнопкой мыши на ее имени и в контекстном меню выберите команду *Отключить учетную запись (Disable account)*.

Контрольные вопросы.

1. Как создается учетная запись компьютера в домене?
2. Как создается учетная запись пользователя домена?
3. Какими учетными записями должен обладать пользователь для того, чтобы он мог выполнить первоначальное присоединение компьютера к домену?
4. Какая команда служит для управления группами и пользователями домена?

5 Лабораторная работа № 5. Управление организационными единицами и группами в Active Directory

Цель работы: изучение ОС Windows Server 2012. Получение навыков работы с учетными записями, организационными единицами, локальными и глобальными группами.

План проведения занятия:

- 1) Создать организационными единицами согласно заданию.
- 2) Создать учетные записи локальных и глобальных групп, согласно заданию.
- 3) Включить в состав групп учетные записи пользователей.

5.1 Задание к выполнению лабораторного практикума

Планирование групп.

При внедрении службы каталогов *Active Directory* на предприятии, необходимо тщательно обдумать структуру подразделений (*Organization Unit*). Хорошо продуманная структура подразделений упрощает администрирование служб *Active Directory*. Подразделения могут включать — компьютеры, пользователи, группы и другие ресурсы. В зависимости от масштабов предприятия модель структуры подразделений может структурироваться по *географическому местонахождению филиалов или по организационной структуре предприятия*. У каждого подразделения должен быть владелец, который управляет поддеревом объектов в *Active Directory*. Сильно сложная структура подразделений может затруднить администрирование.

Предположим, пользователям доменов компании «stdCompany» необходим доступ к ресурсам. Вам — администратору сети компании — придется принять решение по следующим вопросам:

- глобальные группы и членство в них для каждого из доменов;
- локальные группы для каждого ресурса, включая местонахождение каждой группы;
- включение глобальных групп в состав локальных для предоставления пользователям доступа к ресурсам.

Запишите свои соображения в шаблон планирования групп.

Название группы	Локальная или глобальная	Члены	Местонахождение
-----------------	--------------------------	-------	-----------------

Занесите в шаблон планирования групп приведенные ниже сведения:

- 1) Имя группы — в графу «Название группы».
- 2) Тип группы — локальная или глобальная — в графу «Локальная или глобальная».

3) Учетные записи пользователей для каждой глобальной группы — в графу «Члены» (учетные записи пользователей доменов перечислены в приведенной ниже таблице; состав доменов одинаков).

4) Названия всех глобальных групп, которые будут включены в состав локальных групп, — в графу «Члены».

5) Местонахождение сервера: главный контроллер домена, резервный контроллер или сервер — в графу «Местонахождение».

Заполняя шаблон, руководствуйтесь следующим списком пользователей, как примером.

Полное имя	Учетная запись	Описание
Robert Palmer	robertpalmer@std5lab.net	Account-mgr
Barbara Blade	barbarablade@std5lab.net	1st accountant
John West	johnwest@std5lab.net	2nd accountant
Ann Spencer	annspencer@std5lab.net	3rd accountant
Taylor Bass	taylorbass@std5lab.net	4rd accountant
Keira Hudson	keirahudson@std5lab.net	5th accountant

Причем, бухгалтеры относятся к двум отделам Salary (зарплата), Material Liability (материальная ответственность)

Barbara Blade	}	Salary
John West		
Ann Spencer		
Taylor Bass	}	Material Liability
Keira Hudson		

5.2 Теоретический материал

Контейнер - это объект Active Directory, который создается внутри Active Directory, когда вы повышаете сервер до контроллера домена. Такой объект содержит стандартные пользователи и группы для Active Directory и также имеет полностью отличающиеся от организационной единицы атрибуты. Другое крупное отличие заключается в том, что к этому контейнеру не могут применяться групповые политики.

Организационные подразделения, или организационные единицы, являются подгруппами в доменах, которые часто зеркально отражают функциональную или деловую структуру организации. Также можно представлять организационные подразделения как логические контейнеры, в которые помещаются учетные записи, общие ресурсы и другие организационные подразделения. Например, можно создать организационные подразделения HumanResources, IT, Engineering и Marketing для домена microsoft.com.

Организационные единицы имеют тип объекта *OU*, а контейнеры *Users* и *Computers* идентифицируются посредством *CN* (*common name* - *общее имя*).

5.2.1 Подразделения (*Organization Unit*) - организационные единицы.

Дерево организационных подразделений (OU) – это, прежде всего, рабочий инструмент администратора сети, поэтому структура должна быть понятной и удобной именно администратору для выполнения ежедневных операций. Организационное подразделение в Active Directory, как и обычная папка-контейнер, может содержать различные объекты: пользователей, группы, компьютеры, другие папки и организационные подразделения.

Это единственный контейнерный объект, который вы можете создавать в домене.

OU - это минимальная единица, которую вы можете использовать для применения групповых политик и делегирования ответственности.

Этот подход интересен и логичен - переместить объекты в OU и использовать тот факт, что Windows позволяет вам создавать иерархии организационных единиц. Родительские элементы, несколько дочерних элементов и несколько «внуков» - это простой способ использования «нисходящего» принципа администрирования.

Возможность назначать групповые политики на организационные подразделения (OU) - основное отличие от обычного контейнера AD. Для OU, как и для обычного контейнера, можно гибко задавать права доступа и делегировать управление.

Таким образом, задачи OU, помимо хранения объектов в Active Directory, это:

- делегирование управления другим администраторам компании;
- назначение групповых политик.

Групповые политики имеют дополнительные методы контроля назначения – фильтрация по группам безопасности (как пользователей, так и компьютеров) и WMI фильтрация. Таким образом, делегирование прав и удобство ежедневного администрирования – это входные данные для оптимизации вашего дерева организационных подразделений.

По умолчанию AD содержит *OU Domain Controllers*, куда включаются все контроллеры данного домена. Каждый раз, как вы запускаете DCPROMO на рядовом сервере домена, компьютерная учетная запись этого компьютера перемещается в *OU Domain Controllers*.

Создать простую структуру подразделений для примера (можно варьировать по желанию). Откройте оснастку «Active Directory – пользователи и компьютеры». Открыть ее можно одним из способов, например, в окне выполнить (Win+R) набрать *dsa.msc*. Также оснастка доступна в Диспетчере сервера (*Server Manager*).

Для создания OU выполните следующие шаги.

1. Щелкните правой кнопкой на узле, для которого хотите создать OU (например, на узле домена) и выберите *New/Organizational Unit* (*Создать/Организационная единица*).

2. В диалоговом окне *New Object - Organizational Unit* введите имя вашей OU. В данном примере используется *OU stdCompany*.

3. Щелкните на кнопке *OK*.

4. Диалоговое окно закроется, и вы увидите новую созданную OU под узлом домена.

Вы можете создавать вложенные OU, помещая их внутри этой OU, но обычно при создании структуры OU не рекомендуется создавать более 5 уровней вложенности.

Откроется окно, в котором задайте требуемое имя подразделения, например, «*stdCOMPANY*». Далее щелкните ПКМ (правой кнопкой мышки) на новом подразделении и создайте подразделения нижнего уровня. В качестве примера создается отдел бухгалтерии (*Accounting*), в который добавляются подразделения Компьютеры, Пользователи, Серверы и т.д. Должна получиться следующая структура подразделений:

Структура подразделений у Вас может быть совсем иная (самое главное в ней не запутаться). Данная структура приведена для примера, Вы можете создать более сложную структуру, можете создать еще под-под-подразделения, все зависит от Вашего задания. Не забывайте только о том, что структура должна быть понятной и легкой в управлении. Подразделения можно создать и через командную строку или с помощью PowerShell.

5.2.2 Свойства OU.

Чтобы просмотреть и изменить свойства OU, в дереве консоли управления *Active Directory - пользователи и компьютеры* - щелкните нужный объект подразделения правой кнопкой мыши и в контекстном меню выберите *Свойства*.

На вкладке *Общие* измените ряд атрибутов OU.

В поле *Описание* введите произвольное описание, характеризующее деятельность подразделения, в поле *Улица* - полный адрес офиса (улица, дом, корпус, строение и т. п.), где располагается подразделение. В поля *Город*, *Область*, *Почтовый индекс* и *Страна* вводятся соответствующие части адреса подразделения. Заполнение этих полей имеет смысл только в том случае, если подразделения организации размещены в нескольких офисах и/или на большой территории - эта информация должна помочь пользователям локальной сети найти сотрудников подразделения.

На вкладке *Управляется* указывается пользователь, управляющий ОП.

На вкладке *Групповая политика (Group Policy)* вы можете управлять групповыми политиками уровня подразделения. Работа с ними будет рассмотрена позднее.

5.2.3 Размещение объектов в OU.

Вы можете включать в OU пользователей, компьютеры или другие OU. Однако добротное планирование требует продуманного подхода, и вы можете использовать как «кальку» организацию своей компании. Например,

если ваша компания организована в виде отделов (департаментов), то, видимо, вы захотите использовать главный объект, связанный с отделами. Обычно, если отдел соответствует физическому подразделению (этаж или здание) и каждый отдел работает в одной локальной сети или подсети, то, видимо, включение компьютеров отдела в OU будет наиболее подходящим решением.

С другой стороны, если вы хотите управлять групповыми политиками для руководителей не так, как для обычных сотрудников, то, видимо, нужно включить в OU группы или пользователей. В этом случае будет наиболее эффективным создание новой группы в этой OU для пользователей, которыми вы хотите управлять. Это позволит вам совместно управлять полномочиями доступа к ресурсам и групповыми политиками, а также делегировать администрирование этой OU.

Чтобы переместить в OU существующий объект такой, как компьютер, щелкните правой кнопкой на этом объекте (или на нескольких объектах, выделенных при нажатой клавише CTRL) и выберите в контекстном меню пункт Move (Переместить). В диалоговом окне Move выберите нужную OU.

5.2.4 Делегирование администрирования OU.

Лишь немногие администраторы создают организационные единицы исключительно в целях делегирования работы по администрированию предприятия. Они организуют свои OU в соответствии с организацией их компании и делегируют административные задачи членам отдела ИТ. Например, если компания организована по этажам здания, то делегированный администратор занимает свое место на соответствующем этаже.

Чтобы делегировать управление организационной единицей, щелкните правой кнопкой на объекте-OU в дереве консоли и выберите в контекстном меню пункт *Delegate Control* (Делегировать управление). В результате будет запущен мастер *Delegation of Control Wizard*. В появившемся окне щелкните на кнопке *Next*.

В следующем окне щелкните на кнопке Add, чтобы открыть диалоговое окно Select Users, Computers, or Groups. Используйте опции выбора в этом диалоговом окне, чтобы выбрать тип объекта (обычно это пользователь, но если вы создали группу пользователей с административными правами, то можете выбрать группу). Кроме того, выберите местоположение (обычно домен), в котором нужно выбрать делегата. Чтобы выполнить поиск нужного имени с помощью фильтров, щелкните на кнопке *Advanced*, затем б. выберите пользователя. Если вы знаете имя пользователя или группы для этой OU, то можете ввести имя без его поиска. Заполнив список делегатов, щелкните на кнопке *Next*.

В следующем окне выберите задачи, которые хотите назначить этому делегату. Чем больше задач вы назначаете, тем более эффективной будет ваша схема делегирования, если ваш делегат имеет достаточные знания и

опыт для правильного выполнения этих задач. По окончании щелкните на кнопке *Next*.

В следующем окне мастер выводит сводку вашего выбора. Щелкните на кнопке *Back* (Назад), если вы хотите что-то изменить, иначе щелкните на кнопке *Finish*.

5.2.5 Управление делегированием.

Вы можете следить за делегированными функциями или управлять ими. В Windows Server 2012 нет встроенного средства, которое бы показывало, что определенная OU передана делегированному администратору. Поэтому вы должны следить за своими делегированными задачами извне Active Directory. Создайте электронную таблицу, базу данных или просто используйте блокнот для пояснительных записей. Неприятности на этом не кончаются - у вас нет также средства, чтобы модифицировать делегированные задачи (если вы изменили свое решение относительно области действия этих задач).

Управление делегированием - это один из существенных недостающих компонентов в Active Directory.

5.2.6 Удаление OU.

В административных средствах Windows Server 2012 появилась новая опция — *Защитить контейнер от случайного удаления (Protect Container From Accidental Deletion)*. Она предусматривает для подразделения (OU) возможность использовать переключатель безопасности, позволяющий избежать случайного удаления OU. В подразделение добавляются два разрешения: *Everyone::Deny::Delete* и *Everyone::Deny::Delete Subtree*. Поэтому пользователи и даже администраторы не могут случайно удалить подразделение и его содержимое.

Настоятельно рекомендуется включать эту защиту для всех новых подразделений.

Для того чтобы все же удалить подразделение, вначале следует отключить переключатель безопасности. Чтобы удалить защищенное подразделение, выполните следующие действия:

- 1) В оснастке *Active Directory — пользователи и компьютеры (Active Directory Users and Computers)* щелкните меню *Вид (View)* и выберите команду *Дополнительные компоненты (Advanced Features)*.

- 2) Щелкните подразделение правой кнопкой мыши и примените команду *Свойства (Properties)*.

- 3) Перейдите на вкладку *Объект (Object)*. Если вкладка *Объект* не отображается, значит, вы не включили дополнительные компоненты в шаге 1.

- 4) Сбросьте флажок *Защитить контейнер от случайного удаления (Protect Container From Accidental Deletion)*.

- 5) Щелкните *OK*.

6) Щелкните подразделение правой кнопкой мыши и примените команду *Удалить (Delete)*.

7) Вам будет предложено подтвердить удаление OU. Щелкните кнопку *Да (Yes)*.

8) Если подразделение содержит другие объекты, в диалоговом окне *Подтвердить удаление поддерева (Confirm Subtree Deletion)*, вам будет предложено подтвердить удаление подразделения и всех содержащихся в нем объектов. Щелкните кнопку *Да (Yes)*.

5.3 Группы Windows Server 2012

Группа — это набор учетных записей пользователей с похожими служебными обязанностями или потребностями в ресурсах. Организация учетных записей в группы значительно упрощает решение каждодневных административных задач.

Операционная система Windows Server 2012 предоставляет учетные записи пользователя и группы (членом которых являются пользователи).

Учетные записи пользователя предназначены для отдельных пользователей.

Учетные записи групп разработаны для упрощения администрирования множества пользователей. Хотя можно войти в систему, используя учетную запись пользователя, нельзя использовать для входа учетную запись группы. Учетные записи группы часто называют просто группами.

Принадлежность к конкретной группе определяет значительную часть возможностей пользователя сети и конкретного компьютера, так как при этом он получает все привилегии и права группы. Группы — очень удобный метод присвоения прав и привилегий сразу нескольким сотрудникам. Например, если нескольким пользователям необходим доступ к какому-то файлу, можно добавить их учетные записи в группу и присвоить право доступа к этому файлу группе, а не каждому пользователю в отдельности.

5.3.1 Типы групп.

ОС Windows Server поддерживает группы трех типов.

1. *Локальные группы (Local groups)* — группы, определенные на локальном компьютере. Они используются только на локальном компьютере и создаются с помощью утилиты *Локальные пользователи и группы (Local Users And Groups)*.

2. *Группы безопасности (Security groups)* — группы, которые имеют связанные с ними дескрипторы безопасности. Группы безопасности в доменах создаются с помощью оснастки *Active Directory — пользователи и компьютеры*.

3. *Группы рассылки (Distribution group)* — группы, которые используются в списках рассылки электронной почты. Они не имеют дескрипторов безопасности, связанных с ними. Создаются оснасткой *Active*

Directory — пользователи и компьютеры. В большинстве случаев речь идет либо о локальных группах, либо о группах безопасности, но не о группах рассылки. Группы рассылки используются только для рассылки e-mail, а не для назначения или управления доступом.

5.3.2 Область действия группы.

В Active Directory есть несколько областей (диапазонов) групп — локальный домен, встроенный локальный, глобальный и универсальный, то есть группы можно создавать и использовать в разных областях.

1. *Локальные группы домена* — группы в основном используются для назначения разрешений доступа к ресурсам в пределах одного домена. Локальные группы домена могут включать членов из любого домена в лесу и из доверяемых доменов в других лесах. Обычно глобальные и универсальные группы являются членами локальных групп домена.

2. *Встроенные локальные группы* — группы со специальной областью группы, имеют разрешения локального домена и часто, для простоты, относятся к локальным группам домена. Разница между локальными встроенными группами и другими группами в том, что нельзя создавать или удалять встроенные локальные группы. Можно только модифицировать встроенные локальные группы. Упоминание локальных групп домена относится и к встроенным локальным группам, если явно не указано иное.

3. *Глобальные группы* — группы, которые используются преимущественно для определения прав пользователей и компьютеров в одном и том же домене, разделяющих подобную роль, функцию или работу. Члены глобальных групп — только учетные записи и группы из домена, где они были определены.

4. *Универсальные группы* — группы, используемые преимущественно для определения наборов пользователей или компьютеров, которые должны иметь широкие разрешения по всему домену или лесу. Членами универсальных групп могут быть учетные записи пользователей, глобальные группы и другие универсальные группы из любого домена в дереве доменов или лесу.

5.3.3 Идентификаторы безопасности и учетные записи групп.

Как и с учетными записями пользователей, ОС Windows Server отслеживает учетные записи группы с помощью уникальных SID. Это означает, что невозможно удалить учетную запись группы, воссоздать ее снова и затем ожидать, что все полномочия останутся теми же. У новой группы будет новый SID, и все полномочия старой группы будут потеряны.

ОС Windows Server создает маркеры безопасности для каждого входа пользователя. Маркеры безопасности определяют ID учетной записи и SID всех групп безопасности, к которым принадлежит пользователь. Размер маркера увеличивается по мере добавления пользователя в дополнительные группы безопасности, и у этого есть последствия:

– маркер безопасности должен быть передан процессу входа пользователя перед завершением входа. Когда число групп безопасности высокое, процесс входа занимает больше времени;

– чтобы определить права доступа, маркер безопасности отправляется на каждый компьютер, к которому пользователь хочет получить доступ. Поэтому у размера маркера безопасности есть прямое влияние на загрузку сети.

5.3.4 Изменение областей действия.

Если вы создаете группу, то это по умолчанию глобальная группа. Если ваше предприятие работает не в смешанном режиме, то вы можете изменить область действия создаваемой группы следующим образом:

1) *Глобальная в универсальную.* Глобальную группу нельзя вложить в другую глобальную группу; она должна существовать как группа верхнего уровня.

2) *Локальная в домене в универсальную.* Локальная в домене группа может иметь в качестве своих членов только пользователей, но не другие локальные в домене группы.

3) *Универсальные в глобальные.* Универсальная группа не может иметь в качестве своего члена другую универсальную группу.

4) *Универсальные в локальные в домене.* Для этого изменения нет никаких ограничений.

5.3.5 Обозначения.

Для единообразия будем следовать обозначениям объектов, принятым в англоязычной литературе:

A - учётные записи пользователей (User Accounts).

G - глобальные группы (Global groups).

DL - локальные доменные группы (Domain Local groups).

U - универсальные группы (Universal groups).

P - право доступа (Permission).

5.3.6 Стратегии использования групп.

1. *Локальные Группы хоста* – находятся в SAM (Security Account Manager), могут включать Глобальные Группы, Локальные Группы своего Домена, Универсальные Группы.

2. *Локальные Группы Домена* – создаются только на DC. Являются подмножеством возможностей Глобальных Групп. Они могут содержать Глобальные Группы из любого другого домена, но их можно включать только в Локальные Группы своего Домена. Они могут также содержать другие Локальные Группы своего Домена.

3. *Глобальные Группы Домена* – могут помещаться в другие Глобальные Группы своего Домена. Они выходят за пределы своего домена в поисках ресурсов. Их направление – вовне. Глобальные Группы включают в

себя пользователей и Глобальные Группы своего домена и предназначены для включения в локальные ресурсные группы как своего, так и других доменов.

4. *Универсальные Группы* – сочетают достоинства как локальных групп (могут содержать другие группы), так и глобальных групп (могут помещаться в другие группы). Они, как ферзь, сочетают достоинства ладьи и туры. Универсальные Группы сильно влияют на размер и скорость GC – и в этом их недостаток. GC знает не только названия Универсальных Групп, но и всех их членов.

5.3.7 Самая распространенная стратегия (стратегия A G DL P).

Эту стратегию можно обозначить, как A G DL P. Это означает, что учётные записи пользователей являются членами глобальной группы, а для локальной доменной группы настроены права доступа к ресурсу (например, к папке с файлами). Чтобы пользователи получили доступ к этому ресурсу, остаётся сделать только одно — включить глобальную группу в локальную доменную группу.

Весь этот процесс можно проще изобразить следующим образом:

A -> G -> DL <- P

Для примера используем эту стратегию в нашем домене *study.local*. Пусть пользователям из торгового отдела требуется доступ к папке «Договоры».

Если мы будем придерживаться правила, что разрешение на доступ даётся не отдельными пользователями, а только группам, то порядок наших действий будет таким:

- 1) Создание глобальной группы безопасности.
- 2) Включение учётных записей продавцов в эту группу.
- 3) Создание локальной доменной группы безопасности.
- 4) Настройка разрешений на доступ к папке «Договоры» для этой локальной группы.
- 5) Включение глобальной группы в локальную доменную группу.

5.4 Создание учетной записи группы

5.4.1 Создание учетной записи группы с помощью интерфейса Windows.

Откройте оснастку «Active Directory - пользователи и компьютеры», нажмите кнопку *Пуск*, щелкните *Панель управления*, дважды щелкните *Администрирование*, а затем дважды щелкните *Active Directory - пользователи и компьютеры*.

В строке «Выполнить» наберите *dsa.msc*.

1. В дереве консоли щелкните правой кнопкой мыши папку, в которой требуется создать группу. Расположение - *Active Directory - пользователи и компьютеры\узел домена\папка*.

2. Щелкните *Создать*, а затем щелкните *Группа*.

3. Введите имя группы. По умолчанию вводимое имя также служит именем новой группы для операционных систем, предшествующих Windows 2000.

4. Щелкните один из параметров в разделе *Область группы*.

5. Щелкните один из параметров в разделе *Тип группы*.

Чтобы создать группу необходимо: в диалоговом окне New Object - Group введите имя вашей группы

5.4.2 Создание учетной записи группы с помощью командной строки.

1. Чтобы открыть командную строку, нажмите кнопку *Пуск*, щелкните *Выполнить*, введите *cmd*, а затем нажмите кнопку *OK*.

2. Введите следующую команду и нажмите клавишу *Enter*:

```
dsadd group <GroupDN> -samid<SAMName> -secgrp {yes|no} -  
scope {l|g|u}
```

3. Для просмотра полного синтаксиса данной команды, а также сведений о вводе в командную строку информации учетной записи пользователя введите следующую команду, а затем нажмите клавишу *Enter*:

```
dsadd group /?
```

5.5 Добавление члена в группу

Вы можете добавлять объекты в любую группу. Этими объектами могут быть локальные пользователи, доменные пользователи или даже другие локальные или доменные группы. Для добавления членов в группу выполните следующие шаги.

Членство в группах Операторы учета, Администраторы домена, Администраторы предприятия или в эквивалентной является минимальным необходимым требованием для выполнения этой процедуры.

5.5.1 Добавление члена в группу с помощью интерфейса Windows.

1. Чтобы открыть оснастку *Active Directory - пользователи и компьютеры* можно выполнить любое из следующих действий:

– нажмите кнопку *Пуск*, щелкните *Панель управления*, дважды щелкните *Администрирование*, а затем дважды щелкните *Active Directory - пользователи и компьютеры*;

– нажмите кнопку *Пуск*, щелкните *Выполнить*, введите команду *dsa.msc*.

2. В дереве консоли щелкните папку, содержащую группу, в которую требуется добавить члена.

3. В области сведений щелкните правой кнопкой мыши группу, а затем щелкните *Свойства*.

4. На вкладке *Члены* нажмите кнопку *Добавить*.

5. В поле *Введите имена выбираемых объектов* введите имя пользователя, группы или компьютера, которые нужно добавить в группу, а затем нажмите кнопку *ОК*.

5.5.2 Добавление члена в группу с помощью командной строки.

1. Чтобы открыть командную строку можно выполнить любое из следующих действий:

– нажмите кнопку *Пуск*, щелкните *Выполнить*, введите *cmd*, а затем нажмите кнопку *ОК*;

– нажмите кнопку *Пуск* щелкните *Выполнить*, введите *cmd*, а затем нажмите кнопку *ОК*.

2. Введите следующую команду и нажмите клавишу *Enter*:

```
dsmod group <GroupDN> -addmbr <MemberDN>
```

Для просмотра полного синтаксиса данной команды, а также сведений о вводе в командную строку информации учетной записи пользователя введите следующую команду, а затем нажмите клавишу *Enter*.

```
dsmod group /?
```

5.6 Преобразование группы в группу другого типа

Членство в группах *Операторы учета*, *Администраторы домена*, *Администраторы предприятия* или в эквивалентной является минимальным необходимым требованием для выполнения этой процедуры.

5.6.1 Преобразование группы в группу другого типа с помощью интерфейса Windows.

Откройте оснастку *«Active Directory - пользователи и компьютеры»*, нажмите кнопку *Пуск*, щелкните *Панель управления*, дважды щелкните *Администрирование*, а затем дважды щелкните *Active Directory - пользователи и компьютеры*.

1. В дереве консоли щелкните папку, содержащую группу, которую требуется преобразовать в группу другого типа.

2. В области сведений щелкните правой кнопкой мыши группу, а затем щелкните *Свойства*.

3. На вкладке *Общие* в разделе *Тип группы* щелкните тип группы.

5.6.2 *Преобразование группы в группу другого типа с помощью командной строки.*

1. Чтобы открыть командную строку, нажмите кнопку *Пуск*, щелкните *Выполнить*, введите *cmd*, а затем нажмите кнопку *ОК*.

2. Введите следующую команду и нажмите клавишу *Enter*:

```
dsmod group <GroupDN> -secgrp {yes|no}
```

Для просмотра полного синтаксиса данной команды, а также сведений о вводе в командную строку информации учетной записи пользователя введите следующую команду, а затем нажмите клавишу *Enter*.

```
dsmod group /?
```

5.7 Изменение области действия группы

Членство в группах *Операторы учета*, *Администраторы домена*, *Администраторы предприятия* или в эквивалентной является минимальным необходимым требованием для выполнения этой процедуры.

5.7.1 *Изменение области действия группы с помощью интерфейса Windows.*

1. Откройте оснастку *Active Directory - пользователи и компьютеры*.
2. В дереве консоли щелкните папку, содержащую группу, область действия которой требуется изменить.
3. В области сведений щелкните правой кнопкой мыши группу, а затем щелкните *Свойства*.
4. На вкладке *Общие* в разделе *Область группы* выберите область действия группы.

5.7.2 *Изменение области действия группы с командной строки.*

1. Откройте командную строку.
2. Введите следующую команду и нажмите клавишу *Enter*.

```
dsmod group <GroupDN> -scope {L|G|U}
```

Для просмотра полного синтаксиса данной команды, а также сведений о вводе в командную строку информации учетной записи пользователя введите следующую команду, а затем нажмите клавишу *Enter*:

```
dsmod group /?
```

5.8 Удаление группы

Членство в группах *Операторы учета*, *Администраторы домена*, *Администраторы предприятия* или в эквивалентной является минимальным необходимым требованием для выполнения этой процедуры.

5.8.1 Удаление учетной записи группы с помощью интерфейса Windows.

1. Откройте оснастку *Active Directory - пользователи и компьютеры*.
2. В дереве консоли щелкните папку, содержащую группу, которую требуется удалить.
3. В области сведений щелкните правой кнопкой мыши группу, а затем щелкните *Удалить*.

5.8.2 Удаление учетной записи группы с помощью командной строки.

1. Откройте командную строку.
2. Введите следующую команду и нажмите клавишу *Enter*:

```
dsrm <GroupDN>
```

Для просмотра полного синтаксиса данной команды, а также сведений о вводе в командную строку информации учетной записи пользователя введите следующую команду, а затем нажмите клавишу *Enter*:

```
dsrm /?
```

5.9 Поиск групп, членом которых является пользователь

Для выполнения этой процедуры отсутствуют минимальные требования к членству в группах.

5.9.1 Поиск групп, членом которых является пользователь, с помощью интерфейса Windows.

1. Откройте оснастку *Active Directory - пользователи и компьютеры*.
2. В дереве консоли щелкните элемент *Пользователи*. Или щелкните папку, которая содержит учетную запись пользователя, членство в группах которого требуется просмотреть.
3. В области сведений щелкните правой кнопкой мыши учетную запись пользователя, а затем щелкните *Свойства*.

4. Щелкните вкладку *Входит в группы*.

Чтобы открыть Модуль *Active Directory* откройте *Диспетчер серверов*, щелкните *Сервис*, а затем щелкните *Модуль Active Directory для Windows PowerShell*.

5.9.2 Поиск групп, членом которых является пользователь, с помощью командной строки.

1. Чтобы открыть командную строку, нажмите кнопку *Пуск*, щелкните *Выполнить*, введите *cmd*, а затем нажмите кнопку *ОК*.

2. Введите следующую команду и нажмите клавишу *Enter*:

```
dsget user <UserDN> -memberof
```

Для просмотра полного синтаксиса данной команды, а также сведений о вводе в командную строку информации учетной записи пользователя введите следующую команду, а затем нажмите клавишу *Enter*:

```
dsget user /?
```

Новая учётная запись компьютера автоматически помещается в группу *Domain Computers*.

Чтобы передать полномочия по управлению членством в группе одному из состоящих в ней пользователей, выполните следующие действия:

1) Зарегистрируйтесь на SRVR001 как администратор и запустите консоль *Active Directory — пользователи и компьютеры*. Вызовите окно свойств любой доменной группы и перейдите на вкладку *Управляется*.

2) Нажав на кнопку *Изменить*, вы можете ввести или выбрать имя пользователя (но не группы), который будет отвечать за эту группу. После этого в свойствах группы появится указание на того, кто является ее администратором, но у этого пользователя всё ещё нет необходимых полномочий.

3) Для того чтобы дать пользователю эти полномочия, установите флажок *Менеджер может изменять членство в группе*.

4) Нажав на кнопку *ОК*, закройте окно свойств группы.

Пользователи и группы с полномочиями по данной папке являются локальными для этого компьютера. В большинстве случаев системные серверы такие, как компьютер Windows Server 2012, не используются интерактивным пользователем, за исключением задач обслуживания серверов. Серверы на предприятии обычно используются для обслуживания сетевых пользователей, которые выполняют доступ со своих собственных рабочих станций.

Но если пользователи работают с какой-либо программой непосредственно на данном компьютере, то вполне достаточно существующих полномочий. По умолчанию для локальной группы *Users* заданы полномочия *Read & Execute (Чтение и выполнение)*, *List Folder Contents (Вывод списка содержимого папок)* и *Read*. Для типичных приложений таких, как текстовые процессоры и электронные таблицы, где пользователи записывают документы в свои собственные папки документов

(в папку *Note* на сервере или локально), достаточно использовать эти полномочия. Если это приложение, работающее с базой данных, и файлы находятся в той же папке, что и ПО, то вам следует внести изменения в полномочия группы *Users*, разрешив использовать права *Write (Запись)* и *Modify (Изменение)*.

Контрольные вопросы.

1. Какие типы групп могут быть созданы в домене?
2. Чем отличаются группы безопасности от групп распространения?
3. Назовите порядок размещения пользователей и групп в группах домена большого предприятия с несколькими доменами.
4. В чем главное отличие групп локального компьютера от групп домена?
5. Почему уровень безопасности сети на основе домена выше, чем в одноранговой сети?
6. В чем отличие глобальных и локальных доменных групп?
7. Какие группы могут быть отнесены к универсальным группам домена?

6 Лабораторная работа № 6 – Управление профилями пользователей

Цель: научиться работать с профилями пользователей

План проведения занятия:

- 1) Создать локальные профили пользователей.
- 2) Конфигурирование профилей пользователей по умолчанию.
- 3) Создание, проверка и применение перемещаемых профилей.
- 4) Настройки безопасности перемещаемых пользователей.
- 5) Создание, проверка функциональности шаблонов для профилей.
- 6) Преобразование профиля пользователя по умолчанию в сетевой профиль по умолчанию в Windows 8/10 и Windows Server 2012 R2.
- 7) Преобразование профиля пользователя по умолчанию в обязательный профиль пользователя в Windows 8 и Windows Server 2012 R2.

6.1 Управление рабочей средой пользователя

Профиль пользователя - это группа настроек, которые определяют рабочее окружение пользователя. Windows Server 2012 использует профиль для создания рабочего окружения пользователя при входе. Типичные настройки профиля пользователя включают конфигурацию рабочего стола, содержимое меню, настройки панели управления (*Control Panel*), соединения с сетевым принтером и т.д.

Рабочая среда пользователя состоит из настроек рабочего стола, например, цвета экрана, настроек мыши, размера и расположения окон, из настроек процесса обмена информацией по сети и с устройством печати, переменных среды, параметров реестра и набора доступных приложений. Для управления средой пользователя предназначены следующие средства систем Windows Server 2003/2012:

1) Профили пользователей. В профиле пользователя хранятся все настройки рабочей среды системы, определенные самим пользователем. Это могут быть, например, настройки экрана и соединения с сетью. Все настройки, выполняемые самим пользователем, автоматически сохраняются в папке, имя которой для вновь установленной системы выглядит следующим образом: `%SystemDrive%\Users\<имя_пользователя>`.

2) Сценарий входа в систему (сценарий регистрации) представляет собой командный файл, имеющий расширение `.bat` или `.cmd`, исполняемый файл с расширением `.exe` или сценарий *VBScript*, который запускается при каждой регистрации пользователя в системе или выходе из нее. Сценарий может содержать команды операционной системы, предназначенные, например, для создания соединения с сетью или для запуска приложения. Кроме того, с помощью сценария можно устанавливать значения переменных сред, указывающих пути поиска, каталоги для временных файлов и другую подобную информацию.

3) Сервер сценариев Windows (Windows Scripting Host, WSH). Сервер сценариев независим от языка и предназначен для работы на 32-разрядных платформах Windows. Он включает в себя как ядро сценариев Visual Basic Scripting Edition (VBScript), так и JScript. Сервер сценариев Windows предназначен для выполнения сценариев прямо на рабочем столе Windows или в окне консоли команд. При этом сценарии не нужно встраивать в документ HTML.

6.2 Профили пользователей

6.2.1 Описание профилей пользователей.

В операционных системах Windows существуют четыре типа профилей, изменяя параметры которых могут как системные администраторы, так и конечные пользователи:

1) *Временный профиль пользователя*. Временный профиль используется в тех случаях, когда из-за ошибки не удается загрузить профиль пользователя. По завершении сеанса временный профиль удаляется, и изменения, внесенные в настройки пользователя, не сохраняются.

2) *Локальный профиль пользователя (Local)*. Создается при первом входе пользователя в систему и хранится на локальном жестком диске. Любые изменения, сделанные в локальном пользовательском профиле, относятся только к компьютеру, на котором они были произведены.

3) *Перемещаемый* или «блуждающий» профиль пользователя (*Roaming*). Копия локального профиля хранится на общем ресурсе сервера. Профиль загружается при каждом входе пользователя на компьютер локальной сети. Все изменения в перемещаемом профиле синхронизируются с копией на сервере по завершении пользовательского сеанса. Данный профиль удобен тем, что пользователь имеет доступ к своей рабочей среде, выполняя вход на любом компьютере в организации;

4) *Обязательный профиль пользователя (Mandatory)*. ИТ специалисты могут использовать этот тип профиля, чтобы задать определенные пользовательские настройки. Изменения в обязательный профиль пользователя могут вносить лишь системные администраторы. Пользовательские изменения сохраняются только до окончания текущего сеанса.

Вы можете использовать любое сочетание профилей на всем предприятии, отвечающее потребностям ваших пользователей.

Примечание - если организации требуется управление конфигурациями различных групп пользователей и компьютеров, можно воспользоваться групповыми политиками вместо обязательных профилей.

6.2.2 Преимущества профилей.

Основное назначение профиля пользователя — разграничение настроек и данных для разных пользователей одного и того же компьютера. Если дисковый раздел, на котором хранятся профили, отформатирован в файловой системе NTFS, то можно настроить разрешения NTFS так, чтобы разные пользователи не имели доступа к данным друг друга. Менять эти разрешения может только локальный администратор.

Профиль пользователя обладает следующими преимуществами:

- при регистрации пользователя в системе «Рабочий стол» получает те же настройки, какие существовали в момент предыдущего выхода пользователя из системы;
- несколько пользователей могут работать на одном и том же компьютере в индивидуальных средах (нельзя только иметь собственные параметры разрешения экрана и частоты развертки; здесь нужно применять профили оборудования);
- при работе компьютера в домене профили пользователей могут быть сохранены на сервере. В этом случае пользователь получает возможность работать со своим профилем при регистрации на любом компьютере сети. Такие профили называются *перемещаемыми (roaming profile)*. Разновидностью перемещаемых профилей являются *обязательные профили (mandatory profiles)*. Такой профиль пользователь не может изменять, и все изменения, сделанные в настройках системы, теряются при выходе из нее. В Windows XP/8 и Windows Server 2012 обязательные профили поддерживаются только для совместимости, вместо них рекомендуется применять групповые политики

- данные пользователя и настройки его рабочей среды можно сохранять и вне компьютера, на котором работает пользователь. Тогда в случае аварии (например, жесткого диска) пользователь не лишается своих данных и после переустановки операционной системы может продолжать работу в привычной рабочей среде.

- профиль можно настроить так, чтобы он перемещался вместе с пользователем. Тогда пользователь сможет работать в одной и той же рабочей среде независимо от того, на какой из рабочих станций он зарегистрировался, что значительно повышает продуктивность его работы.

Не все настройки локального профиля входят в его перемещаемый профиль!

Пользовательские профили можно применять различным образом:

- создать несколько типов профилей и назначить их определенным группам пользователей. Это позволит получить несколько типов рабочих сред, соответствующих различным задачам, решаемым пользователями;
- назначать общие групповые настройки всем пользователям;
- назначать обязательные профили, какие-либо настройки которых пользователи изменять не могут.

6.2.3 Структура профиля .

Пользовательский профиль содержит в себе огромное количество установок и данных пользователей. Знание о расположении его отдельных составляющих необходимо для любых манипуляций с профилем, устранения неполадок или настройки резервного копирования.

Установки содержатся в двух местах: в системном реестре и в специальных папках файловой системы. Данные реестра в ОС Windows, начиная с версии NT, тоже можно экспортировать как обычный файл и импортировать обратно в реестр. Реестровая часть пользовательского профиля содержится в файле NTUSER.DAT, который при активации профиля (при регистрации пользователя) читается в реестр, точнее в его ветвь `HKEY_CURRENT_USER`.

Файл NTUSER.DAT содержит следующие настройки:

1) Настройки Проводника Windows, все пользовательские настройки Проводника и сетевых подключений (например, сокрытие расширений зарегистрированных типов файлов или подключенные сетевые диски).

2) Параметры Панели задач (например, присутствие панели быстрого запуска).

3) Установленные принтеры (различные локальные и сетевые принтеры).

4) Настройки Панели управления.

5) Рабочие панели (их наличие и вид).

6) Стандартные программы. Все пользовательские настройки приложений Windows, многие из которых доступны из меню *Пуск* –

Программы – Стандартные (Калькулятор, Блокнот, Paint, HyperTerminal и другие)

7) Настройки приложений (некоторые приложения сохраняют свои настройки в ветви *HKEY_CURRENT_USER* — примером может служить главная панель приложений Microsoft Word).

В системах семейства Windows 8/10 и Windows Server 2012 профиль пользователя по умолчанию располагается в папке *%SYSTEMDRIVE%\Documents and Settings \%username%*. В этой папке находятся файл *NTUSER.DAT* и иерархия папок, представленная на рисунке 6.1.

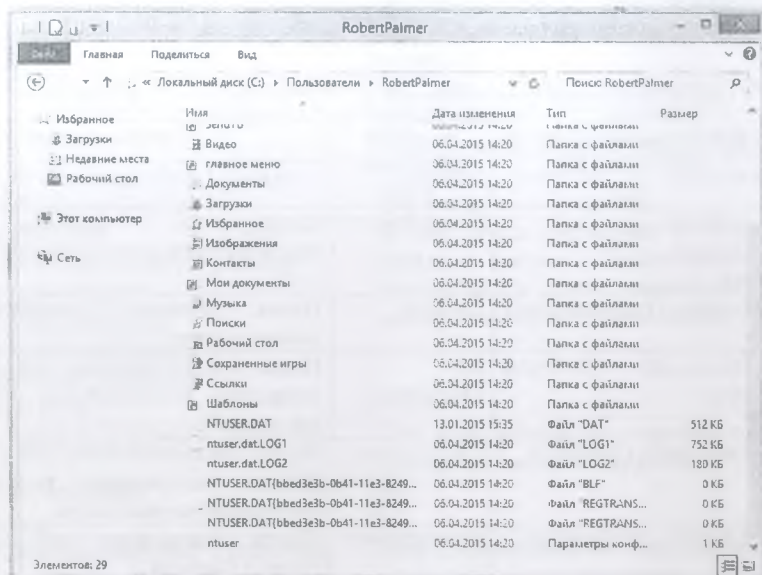


Рисунок 6.1 - Папка профиля пользователя

В операционных системах, начиная с Windows Vista и Windows Server 2012, все пользовательские профили расположены в папке *Users*. Администратор может удалить из списка любой профиль, кроме своего собственного. Если вы не являетесь администратором, то в списке будет присутствовать только ваш профиль, который также нельзя удалить.

6.3 Локальные профили

Windows 7, Windows Vista, Windows Server 2012 и Windows Server 2012 R2 создает локальный профиль при первом входе каждого пользователя на компьютер. Каждый пользовательский профиль хранится в папке *\Users\User*, где *User* - это имя входа этого пользователя. Часть файла реестра

в пользовательском профиле - это кэшированная копия части реестра HKEY CURRENT USER, хранящаяся под именем Ntuser.dat. Остальную часть профиля образует структура папок конкретного пользователя. Ntuser.dat определяет оборудование данного компьютера, установленное ПО и настройки рабочей среды. Структура папок и находящиеся в них значки (ссылки) определяют рабочий стол пользователя и окружения для приложений. В таблице 1 описывается конкретное содержимое структуры папок, включаемой в профиль пользователя.

Таблица 6.1 - Описание содержимого структуры папок профиля пользователей

Стандартные папки пользователей		
Windows Vista/7/Server 2012/2012 R2	Windows XP/Server 2003	Краткое описание
Contacts (Контакты)	Отсутствует	Папка для хранения контактов пользователей по умолчанию
Desktop (Рабочий стол)	Desktop	Папка, которая содержит элементы рабочего стола
Documents (Рабочий стол)	My Documents	Папка, предназначенная для хранения всех созданных пользователем документов по умолчанию
Downloads (Загрузки)	Отсутствует	Папка, предназначенная для хранения всех файлов, загруженных пользователем из Интернета по умолчанию
Favorites (Избранное)	Отсутствует	Папка, содержащая избранное браузера Internet Explorer
Links (Ссылки)	Отсутствует	Папка, в которой хранятся избранные ссылки браузера Internet Explorer
Music (Моя музыка)	My Music	Папка, предназначенная для хранения музыкальных файлов пользователя по умолчанию
Pictures (Изображения)	My Pictures	Папка, предназначенная для хранения файлов изображений пользователя по умолчанию
Saved Games (Сохраненные игры)	Отсутствует	Папка, в которой расположены сохранения для игр пользователя по умолчанию
Searches (Поиски)	Отсутствует	Папка, предназначенная для хранения поисковых запросов пользователя
Videos (Мои видеозаписи)	My Videos	Папка, предназначенная для хранения файлов видео пользователя по умолчанию
Virtual Machines (Виртуальные)	Отсутствует	Папка, предназначенная для хранения виртуальных машин пользователя по умолчанию

машины)*		умолчанию (данная папка отсутствует в операционной системе Windows Vista)
Точки соединения		
AppData	Отсутствует	Данная папка является скрытой, и в ней по умолчанию содержатся данные приложений пользователей. Эта папка содержит вложенные папки Local и Roaming, содержимое которых описано ниже, а также папка LocalLow, которая хранит параметры приложений для защищенных процессов и не перемещаются при разворачивании перемещаемых профилей
AppData\Roaming	Application Data	В этой точке соединения хранятся программные данные, которые определяются разработчиками приложений
AppData\Roaming\Microsoft\Windows\Cookies	Cookies	Содержит сведения о пользователе и параметры его настройки
AppData\Local	Local Settings	В этих точках соединения вы можете найти файлы данных приложений, файлы журналов, а также временные файлы, которые входят в перемещаемый профиль
AppData\Local\Microsoft\Windows\History		
AppData\Local\Temp		
AppData\Local\Microsoft\Windows\Temporary Internet Files		
AppData\Roaming\Microsoft\Windows\Network Shortcuts	NetHood	Эта точка соединения содержит ярлыки для элементов сетевого окружения
AppData\Roaming\Microsoft\Windows\Printer Shortcuts	PrintHood	Эта точка соединения содержит ярлыки для элементов папки принтеров
AppData\Roaming\Microsoft\Windows\Recent	Recent	Эта точка соединения содержит ярлыки для последних используемых документов и папок
AppData\Roaming\Microsoft\Windows\Send To	SendTo	Эта точка соединения содержит ярлыки служебных программ по работе с документами
AppData\Roaming\Microsoft\Windows\Start Menu	Start Menu	Эта точка соединения содержит ярлыки для программ из меню «Пуск»
AppData\Roaming\Microsoft\Windows\Templates	Templates	Данная точка соединения включает шаблоны пользователя
\Documents	My Documents	Содержит документы и подпапки пользователя

В первый раз, когда пользователь выполняет вход на компьютер Windows 7, Windows Vista, Windows Server 2012 и Windows Server 2012 R2, система создает иерархию папок для этого пользователя. Чтобы заполнить эти папки и создать профиль, Windows копирует содержимое папки Default User (Пользователь по умолчанию) в папки профиля пользователя, где происходит административное управление начальным профилем пользователя.

6.4 Перемещаемые профили

6.4.1 Описание перемещаемых профилей.

Профили пользователя позволяют настраивать цветовую гамму и обои рабочего стола, создавать ярлыки для быстрого доступа, выбирать комбинацию клавиш для переключения раскладки клавиатуры, вносить изменения в Панель задач и Главное меню и делать многое другое по своему усмотрению. Все настройки, сделанные на компьютере, сохраняются и восстанавливаются при следующем входе в систему. С другой стороны, созданные настройки не влияют на других пользователей, регистрирующихся на этом же компьютере, и наоборот. Иными словами, операционная система Windows сохраняет индивидуальные настройки для каждого пользователя. Структура данных, предназначенная для хранения пользовательской информации, называется *профилем пользователя*.

Нередки ситуации, когда специфика работы или обучения пользователей заставляет их регистрироваться в разное время на разных компьютерах. В этом случае важно предоставлять пользователю одно и то же рабочее окружение, независимо от компьютера, на котором он входит в систему. Наиболее простым решением является применение перемещаемого профиля.

Перемещаемым называется такой профиль, который «странствует» по узлам сети вместе с пользователем и вступает в силу на любом компьютере, на котором пользователь регистрируется. Перемещаемость профиля нужно указывать в свойствах доменной учетной записи. Для того чтобы пользователь смог оценить преимущества перемещаемого профиля, должны быть выполнены следующие условия:

- 1) Перемещаемые профили должны храниться на компьютере, который постоянно доступен по сети (то есть включён и работает).

- 2) Этот компьютер с перемещаемыми профилями ни в коем случае не должен отвергать попытку подключения, то есть на нем должна быть установлена серверная операционная система с достаточным количеством лицензий на клиентский доступ.

Перемещаемый профиль располагается в сетевой папке на файловом сервере. В процессе регистрации пользователя Windows копирует профиль из сетевой папки в кэшированную копию на локальном компьютере. При

наличии предыдущей кэшированной копии копируются только изменения, а не весь профиль. Когда пользователь выходит из системы, операционная система копирует измененные данные профиля в сетевую папку. Это гарантирует, что пользовательские данные и рабочее окружение следуют за пользователем, даже если он входит в систему на разных компьютерах.

Инструмент управления профилями пользователей в предыдущих операционных системах, и его функциональность существенно ограничена в Windows 7 и Windows Server 2012 R2. Отсутствует возможность копирования локальных профилей между пользователями, а также в профиль по умолчанию.

6.4.2 Создание перемещаемых профилей.

Способ создания профиля перемещающегося пользователя на сервере зависит от обстоятельств, при которых этот пользователь выполняет вход в домен. Когда этот пользователь выполняет вход, Windows проверяет учетную запись пользователя, чтобы прочитать путь к профилям пользователей.

Если этот путь существует (поскольку вы ввели его во вкладке *Profile*, как это описано в предыдущем разделе), то система ищет подпапку с профилем этого пользователя в указанной папке профилей.

Если эта подпапка не существует и компьютер, с которого пользователь выполняет вход, содержит его локальный профиль, то подпапка профиля создается на сервере и локальный профиль становится профилем, записанным на сервере.

Если эта подпапка не существует и компьютер, с которого пользователь выполняет вход, не содержит его локального профиля, то подпапка профиля создается на сервере и пользовательский профиль по умолчанию на локальном компьютере становится профилем, записанным на сервере.

Если эта подпапка существует, то возможен один из двух сценариев: это уже не первый вход после того, как вы активизировали перемещаемые профили для этого пользователя, или вы уже предварительно заполнили подпапку профиля этого пользователя (см. следующий раздел).

Вы можете копировать какой-либо локальный профиль в используемый по умолчанию локальный профиль пользователя, чтобы профиль пользователя по умолчанию соответствовал нужным вам опциям конфигурирования. Вы можете также скопировать локальный профиль в папку *Profiles* на сервере, которая содержит профили пользователей.

Если перемещающийся пользователь имеет локальный профиль на какой-либо рабочей станции, скопируйте этот профиль на сервер. Затем, когда вы активизируете перемещаемые профили для этого пользователя и он выполняет вход с любого другого компьютера, его профиль становится перемещаемым профилем. (Вам не обязательно выполнять эту задачу, если вы знаете, что после того, как вы активизируете перемещаемые профили для

этого пользователя, он выполнит вход с того компьютера, где содержится его локальный профиль; в этом случае профиль копируется автоматически).

Если перемещающийся пользователь не имеет локального профиля на рабочей станции, скопируйте на сервер другой профиль, подходящий для этого перемещающегося пользователя.

Внимание. «Подходящий» профиль означает, что ПО и утилиты, представленные в различных меню, имеются на всех компьютерах, с которых перемещающийся пользователь может выполнять вход в домен.

6.4.3 Безопасность перемещаемых профилей.

При первой регистрации пользователя в сети на сервере создаётся пустая папка профиля «Robert Palmer». Она наполняется данными только по завершении сеанса работы пользователя. Разрешения NTFS для этой папки по умолчанию настроены так, чтобы доступ к ней имел только соответствующий пользователь. Даже членам группы администраторов доступ запрещен.

В такой конфигурации администратор, желающий получить доступ к файлам профиля, должен стать владельцем этого профиля — папки и всей иерархии ее подпапок. Смена владельца может отрицательно повлиять на функционирование перемещаемых профилей. Это нежелательно, но в то же время доступ к профилям администратору нужен. Эта проблема решается при помощи групповой политики.

6.4.4 Правила использования перемещаемых профилей.

Запрет на регистрацию на рабочих станциях до запуска сетевых служб. Возможность регистрации в домене без сети впервые появилась в системе Windows XP Professional. По умолчанию эта возможность разрешена. В таком случае пользователь с перемещаемым профилем при регистрации загружает копию профиля из локального кэша. Это значит, что при переходе на перемещаемые профили с локальных изменения вступают в силу только со второго сеанса работы.

Если вы заранее не отключили эту возможность, то найти ее можно в объекте групповой политики Default Domain Policy, в ветви *Конфигурация компьютера\Административные шаблоны\Система \Регистрация*. Это настройка *При включении компьютера и входе пользователя всегда дожидаться ответа сети (Always wait for the network at computer startup and logon)*.

Избегайте использования перемещаемых профилей в неоднородной сети.

Обеспечьте доступ администраторов к профилям пользователей. Доступ к профилям пользователей необходим с точки зрения управления сетью. Если это возможно, обеспечьте его ещё до начала работы пользователей.

Исключите папку «Мои документы» из перемещаемого профиля. Переадресацией папки «Мои документы» и исключением ее из профиля вы добьетесь того, что при первой регистрации пользователя на конкретной рабочей станции все содержимое этой папки не будет копироваться по сети на эту рабочую станцию. Таким образом, регистрация пройдет быстрее и без лишней нагрузки на сеть.

Не шифруйте файлы в перемещаемых профилях. Применение шифрующей файловой системы (EFS) несовместимо с перемещаемыми профилями. Если вы зашифруете файлы или папки, профиль потеряет способность к перемещению.

6.5 Профиль по умолчанию

Когда пользователь впервые приступает к работе, профиль для него создается операционной системой из некоторого шаблона. Этот шаблон может не соответствовать требованиям предприятия, а просить пользователей настроить свой профиль самостоятельно не всегда позволяет их квалификация. Решением будет предварительная настройка шаблона силами администратора. Возможность последующих изменений профиля самим пользователем можно отрегулировать с помощью групповой политики. При первой регистрации пользователя на компьютере, где у него еще нет профиля, операционная система начинает поиск шаблона профиля с папки *NETLOGON\Default User* на контроллере домена. Это относится как к перемещаемым профилям, так и к локальным.

6.6 Обязательный профиль

Обязательный профиль - это перемещаемый профиль, который нельзя изменять. В отличие от перемещаемого профиля, обязательный профиль загружается, но не сохраняет изменения в папке перемещаемых профилей; иными словами, все изменения, сделанные пользователем, сбрасываются после его выхода из системы, не сохраняются в профиле на сервере и недоступны при следующем входе этого пользователя в сеть. Такая возможность оказывается востребованной в ряде случаев, например, в компьютерных классах и для компьютеров, устанавливаемых в общедоступных местах. Однако администраторы могут вносить изменения в обязательные профили пользователей. Поскольку обязательные профили нельзя изменять в соответствии с личными настройками пользователя, их можно применять к группам пользователей.

Обязательные профили очень похожи на перемещаемые профили; фактически это перемещаемые профили, однако, этот профиль должен существовать в подпапке профилей пользователя на сервере, прежде чем этот пользователь выполнит вход, поскольку обязательный профиль не может быть записан на сервер клиентской рабочей станцией.

Создавая подпапку профилей для пользователя, вы должны реально создать эту подпапку на сервере, поскольку рабочая станция не может этого делать автоматически, как в случае перемещаемых профилей. Задайте полномочия *Read and Execute (Чтение и выполнение)*.

Кроме того, нужно добавить расширение .map к последнему компоненту UNC-пути. Например, если бы вы создавали обычный перемещаемый профиль, то задали бы UNC-путь в диалоговом окне *Properties* для пользователя как *\\Server\ProfileFolder\Имя_пользователя*. Для обязательного профиля UNC-путь задается как *\\Server\ProfileFolder\Имя_пользователя.map*.

После копирования какого-либо профиля в подпапку этого пользователя переименуйте файл NTUSER.DAT в NTUSER.MAN, что делает его доступным только по чтению. Расширение .map в имени подпапки предупреждает Windows Server 2012, что профиль является обязательным, и это, в свою очередь, вынуждает Windows Server 2012 запрещать пользователю вход в домен, если сервер, содержащий этот профиль, недоступен.

Упражнение №1. Локальные профили.

Локальный администратор имеет возможность проверить все существующие локальные профили:

- 1) Зарегистрируйтесь на Windows 8 как локальный администратор.
- 2) В главном меню щелкните правой кнопкой мыши по пункту *Компьютер* и из контекстного меню выберите команду *Свойства*.
- 3) Перейдите на вкладку *Дополнительно* и в части *Профили* пользователей нажмите кнопку *Параметры*. Откроется окно с профилями всех пользователей, которые зарегистрированы на этом компьютере.

Упражнение №2. Конфигурирование профиля пользователя по умолчанию.

Создайте пользователя Robert Palmer, который впервые регистрируется на рабочей станции (WIN 8). В этот момент компьютер выполняет следующие действия:

- 1) В ветви реестра *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList* он попытается найти информацию о профиле пользователя Robert Palmer. Поскольку пользователь Robert Palmer на этом компьютере до сих пор не регистрировался, ссылки на профиль в реестре не существует, и компьютер продолжает поиск.
- 2) Если компьютер является членом домена, он проверит, существует ли «доменный» профиль в папке *NETLOGON\Default User* на контроллере домена.
- 3) Если такой профиль найден, он копируется во вновь созданную папку *%SYSTEMDRIVE%\Users\Robert Palmer*. Если же «доменного» профиля не существует, то в эту папку будет скопирован локальный профиль

по умолчанию из папки %SYSTEMDRIVE%\Documents and Settings\Default User.

4) Реестровая часть пользовательского профиля (файл NTUSER.DAT) считывается в ветвь реестра HKEY_CURRENT_USER.

Теперь пользователь Robert Palmer может настроить свою рабочую среду в соответствии со своими вкусами и служебными задачами. Поскольку никаких ограничений пока введено не было, пользователь может изменить практически все настройки. Например:

- отобразить расширения известных типов файлов;
- создать файл на рабочем столе;
- переключить главное меню на классический вид;
- показать панель быстрого запуска на панели задач;
- сменить тему рабочего стола.

После того, как пользователь Robert Palmer завершит сеанс работы, эти настройки будут сохранены в его локальном профиле на жестком диске данного компьютера. При следующей регистрации этого пользователя на этом компьютере локальный профиль будет прочитан и настройки применены к новому сеансу, то есть пользователь сможет работать в той же самой рабочей среде.

Упражнение №3. Конфигурирование профиля пользователя по умолчанию.

Вы можете вносить изменения в профиль пользователя по умолчанию, чтобы создать профиль, предоставляемый каждому пользователю, выполняющему вход на данный компьютер.

1. Выполните вход как *Administrator*.

2. Щелкните правой кнопкой на *My Computer* и выберите в контекстном меню пункт *Properties*, чтобы открыть диалоговое окно *System Properties (Свойства системы)*.

3. Перейдите во вкладку *Advanced System settings (Дополнительные параметры системы)*.

4. В секции *User Profiles (Профили пользователей)* этого диалогового окна щелкните на кнопке *Settings (Параметры)*.

5. Выберите пользователя, который установил ПО и выполнил другие описанные здесь задачи.

6. Щелкните на кнопке *Copy to (Копировать)* и введите *\Users\Default User* как целевую папку (или щелкните на кнопке *Browse* и выберите эту папку).

7. В секции *Permitted to use (Разрешено использовать)* щелкните на кнопке *Change*.

8. Введите *Everyone* в поле *Enter the object name*.

9. Щелкните на кнопке *OK*, чтобы увидеть сводку вашего выбора.

10. Щелкните на кнопке *OK* и подтвердите процедуру копирования.

Примечание - кнопка Copy to недоступна для профиля текущего выполнившего вход пользователя, и поэтому вам приходится создавать профиль под учетной записью одного пользователя и копировать его как другой пользователь.

Упражнение №4. Перемещаемые профили.

1. Зарегистрируйтесь на сервере как администратор.

2. Создайте на диске C:\ папку «TravProfiles», в которой будут храниться перемещаемые профили. Откройте сетевой доступ (*Sharing*) к этой папке и нажмите *Share*. В появившемся окне нажмите на стрелочку вниз и нажмите на *Everyone* (*Все*).

3. Запустите консоль Active Directory — Пользователи и компьютеры и отобразите свойства учетной записи Robert Palmer. Перейдите на закладку *Profile* (*Профиль*) и в поле *Profile Path* (*Путь к профилю*) введите сетевой путь к подпапке пользователя, которая будет создана в папке, хранящей перемещаемые профили. Путь должен быть в формате UNC, т.е. содержать имя сервера и имя разделяемой папки и начинаться с двух символов обратной черты (backslash). Указанная подпапка будет создана автоматически.

Если в свойствах учетной записи назначен путь к профилю, то при следующей регистрации пользователя в системе в папке сетевых профилей будет создана папка с именем пользователя и расширением V2, например, Пользователь1.V2.

Выполните эти задачи до активизации перемещаемых профилей для пользователя. Иначе, если этот пользователь выполнит вход в домен раньше, чем вы разместите профиль на сервере, локальный компьютер автоматически создаст профиль на сервере.

Упражнение №5. Проверка созданного перемещаемого профиля.

Проверка созданного нами перемещаемого профиля состоит из следующих этапов:

1) Зарегистрируйтесь на рабочей станции (Win 8) как пользователь «Robert Palmer». Откройте окно свойств «Мой компьютер» и перейдите на вкладку Дополнительно. Нажмите кнопку *Параметры* в части *Профили пользователей* и убедитесь, что ваш профиль имеет тип «Перемещаемый». Если Ваш пользователь не является администратором, для изменения параметров Вы должны вводить пароль администратора.

2) Создайте на рабочем столе новый текстовый документ, а в папке «Мои документы» (меню Пуск —> Мои документы) — новый файл типа «Звук Wav».

3) Завершите сеанс работы на компьютере. В ходе завершения сеанса изменения в настройках профиля будут не только сохранены в локальном профиле пользователя Robert Palmer на компьютере, но и скопированы на сервер, в папку «TravProfiles».

4) Зарегистрируйтесь на сервере как администратор. Откройте папку «*TravProfiles\Robert Palmer*». Проверьте наличие текстового документа в подпапке «Рабочий стол» и звукового файла в подпапке «Документы».

Упражнение №6. Применение перемещаемого профиля.

Для того чтобы внутри профиля пользователя, размещенного на сервере, сохранялся в папке «Рабочий стол» какой-нибудь новый документ, и пользователь увидел бы его сразу после начала работы, нужно сделать следующие шаги:

1) Убедиться, что пользователь Robert Palmer не зарегистрирован ни на одном из компьютеров сети.

2) Как администратор, создать в папке «*TravProfiles\Robert Palmer\Рабочий стол*» на сервере новый документ MS Word.

3) Зарегистрироваться под именем Robert Palmer на той рабочей станции, где в последний раз был завершен сеанс как пользователь Robert Palmer. Проверьте наличие созданного документа на рабочем столе профиля.

Упражнение №7. Создание шаблона (профиля по умолчанию).

Для создания шаблона сделайте следующее:

1) Выберите пользователя, для которого еще не существует никакого профиля (иначе содержимое, например, его папки «Мои документы» станет частью шаблона). Зарегистрируйтесь на рабочей станции (Win 8/10) под именем, например, Barbara Blade.

2) Настройте этот профиль. Для наглядности внесите следующие изменения:

– Смените фоновый рисунок рабочего стола (щелкните правой кнопкой мыши на рабочем столе, выберите команду *Свойства*, перейдите на вкладку Рабочий стол, выберите рисунок из списка и нажмите *OK*).

– Создайте на рабочем столе документ под названием «Срочно прочитайте» и разместите его значок примерно посередине рабочего стола.

– В папке «*Мои документы*» создайте подпапку «*Правила для новых сотрудников*». На реальном предприятии именно так быстрее всего провести инструктаж нового работника. Закончите сеанс работы.

Упражнение №8. Копирование шаблона на сервер.

Копирование шаблона на сервер осуществляется следующим образом:

1) Зарегистрируйтесь на Вашем сервере как администратор.

2) Создайте в папке *WINDOWS\SYSTEM32\sysvol\study.local\scripts* подпапку «Default User».

3) Выполните команду *Пуск -> Выполнить* и в поле *Открыть* введите путь *\\<Имя рабочей станции>\C\$*. Отобразится содержимое диска C: рабочей станции (Win 8). Перейдите в папку «*Users*».

4) В окне Проводника включите режим отображения скрытых файлов, чтобы увидеть профиль полностью.

5) Скопируйте содержимое папки пользователя в подпапку «Default User» на сервере. Процесс копирования должен занять не больше нескольких секунд.

Перемещаемые профили можно хранить на рядовом сервере, но шаблон профиля (папка «Default User») обязательно должен располагаться на контроллере домена. Если в вашей сети несколько контроллеров домена, то следует подождать, пока завершится репликация базы данных, потому что папка «Default User» должна присутствовать на любом контроллере, через который регистрируется пользователь, а определить заранее, какой это будет, невозможно.

Упражнение № 9. Проверка функциональности шаблона.

Для проверки функциональности шаблона выполните следующие действия:

1) Выберите пользователя, для которого вы определили в свойствах учетной записи, но еще не создали перемещаемого профиля (например, Ann Spencer). Если профили уже существуют, можно удалить соответствующую папку профиля из папки C:\TravProfiles на сервере, а затем уничтожить ее локальную копию на той рабочей станции, за которой собираетесь проверять шаблон. Зарегистрируйтесь на этой рабочей станции под именем Ann Spencer.

2) Убедитесь, что настройки, выполненные вами от имени пользователя Barbara Blade и затем скопированные на контроллер домена в качестве шаблона, действительны для пользователя Ann Spencer.

3) Откройте окно свойств системы, перейдите на вкладку Дополнительно и, нажав на кнопку Параметры в части Профили пользователей, убедитесь, что ваш профиль действительно перемещаемый.

4) Теперь выберите пользователя, для которого определен, но еще не создан, локальный профиль (например, Lee Priest). Зарегистрируйтесь под его именем и убедитесь, что его локальный профиль тоже создан на основе шаблона Barbara Blade.

Таким образом, настройка шаблона на контроллере домена является универсальным системным решением, с помощью которого легко раз и навсегда определить, как будет выглядеть рабочая среда нового пользователя независимо от того, перемещаемый ли у него профиль или локальный.

Гораздо худшим решением было бы создавать шаблон на каждой рабочей станции в папке %SYSTEMDRIVE%\Docuents and Settings\Default User (здесь операционная система ищет шаблон на следующем шаге). Это ненамного уменьшит нагрузку на сеть, но намного прибавит работы администраторам, особенно, если количество пользователей сети исчисляется сотнями.

Упражнение №10. Преобразование профиля пользователя по умолчанию в сетевой профиль по умолчанию в Windows 7 и Windows Server 2012 R2.

1. Войдите в систему на компьютере, на котором используется настроенный профиль пользователя по умолчанию, с учетной записью, обладающей правами администратора.

2. Подключитесь к общей папке NETLOGON на контроллере домена с помощью команды *Выполнить* и введите путь, который имеет следующий вид:

\\ <имя_сервера>\NETLOGON

3. Создайте в общей папке NETLOGON новую папку и присвойте ей имя *Default User.v2*.

4. Нажмите кнопку *Пуск*, щелкните правой кнопкой мыши пункт *Компьютер*, выберите пункт *Свойства*, затем - *Дополнительные параметры системы*.

5. В группе *Профили пользователей* нажмите кнопку *Параметры*. Откроется диалоговое окно *Профили пользователей* со списком хранящихся на компьютере профилей.

6. Выберите пункт *Профиль по умолчанию* и нажмите кнопку *Скопировать*.

7. В поле *Копировать профиль на* введите сетевой путь к папке профиля пользователя по умолчанию на Вашей рабочей станции, то есть, введите следующий путь:

\\<имя_сервера>\NETLOGON\Default User.v2

8. В разделе *Разрешить использование* нажмите кнопку *Изменить*, введите имя группы *Все* и нажмите кнопку *ОК*.

9. Нажмите кнопку *ОК*, чтобы начать копирование профиля.

10. Выйдите из системы после завершения копирования.

Рассмотрим инструмент управления профилями пользователей. В *Панели управления – Система* щелкните пункт *Дополнительные параметры*. Откроется окно *Профили пользователей*, в котором отображается список профилей, когда-либо созданных на локальном компьютере.

Для каждого профиля отображается его тип (локальный или перемещаемый), размер и дата последнего изменения. Администратор может удалить выбранный профиль, если, например, текущий профиль поврежден и приводит к каким-либо ошибкам при входе пользователя в систему. Для перемещаемого профиля возможно изменение типа.

Активизируя перемещаемые профили для этого пользователя на контроллере домена, обязательно используйте тот же путь, чтобы подпапка с именем пользователя соответствовала целевой подпапке вашего копирования.

Упражнение 11. Преобразование профиля пользователя по умолчанию в обязательный профиль пользователя в Windows 7 и Windows Server 2012 R2.

Локальный профиль пользователя по умолчанию можно сделать обязательным профилем. В результате для всех пользователей будет использоваться один центральный профиль. Для этого необходимо подготовить расположение обязательного профиля, скопировать в это расположение локальный профиль пользователя по умолчанию и настроить расположение профиля пользователя таким образом, чтобы оно указывало на обязательный профиль.

1. Подготовка расположения обязательного профиля. На сервере в созданной папке *TravProfiles* создайте папку в папке. Если обязательный профиль предназначен для конкретного пользователя, имя этой папки должно начинаться с имени входа для учетной записи этого пользователя. Если обязательный профиль предназначен для нескольких пользователей, присвойте ему соответствующее имя, например, *mandatory*.

2. Копирование профиля пользователя по умолчанию в расположение обязательного профиля:

а) войдите в систему на компьютере, на котором используется настроенный локальный профиль пользователя по умолчанию, с учетной записью, обладающей правами администратора;

б) нажмите кнопку *Пуск*, щелкните правой кнопкой мыши пункт *Компьютер*, выберите пункт *Свойства*, а затем - *Дополнительные параметры системы*;

в) в группе *Профили пользователей* нажмите кнопку *Параметры*. Откроется диалоговое окно *Профили пользователей* со списком хранящихся на компьютере профилей;

г) выберите пункт *Профиль по умолчанию* и нажмите кнопку *Скопировать*;

д) в поле *Копировать профиль на* введите сетевой путь к папке пользователя по умолчанию на рабочей станции (Win 8/10), созданной при выполнении пункта 1;

\\<имя_сервера>\Travprofiles\lee.V4

е) в разделе *Разрешить использование* нажмите кнопку *Изменить*, введите имя группы *Все* и нажмите кнопку *ОК*;

ж) нажмите кнопку *ОК*, чтобы начать копирование профиля;

з) выйдите из системы после завершения копирования;

и) если у Вас не отображаются скрытые файлы и папки, зайдите в *Панели управления (Control Panel)* в *Folder Options*. Затем во вкладке *View (Вид)* установите флажок *Show hidden folders and files* и уберите флажок с *Hide protected operating system files*;

к) найдите файл *NTUSER.DAT*, щелкните его правой кнопкой мыши, выберите команду *Переименовать*, измените имя файла на *NTUSER.MAN* и нажмите клавишу *Enter*.

3. Подготовка учетной записи пользователя:

а) используя учетную запись администратора домена, откройте на компьютере с системой Windows Server 2012 R2 или Windows Server 2012 консоль управления «*Пользователи и компьютеры Active Directory*»;

б) щелкните правой кнопкой мыши учетную запись пользователя, к которой необходимо применить обязательный профиль пользователя (например, пользователь Lee Priest), и выберите пункт *Свойства*;

в) откройте вкладку *Профиль* и введите в текстовое поле пути к профилю сетевой путь, созданный при выполнении пункта 1. В данном примере путь будет выглядеть следующим образом:

\\<имя_сервера>\Profiles\Users\lee

г) нажмите кнопку *OK* и закройте консоль управления «Пользователи и компьютеры Active Directory».

Теперь к пользователю будет применяться настроенный обязательный профиль.

Контрольные вопросы.

1. Что понимается под профилем пользователя?
2. Что хранится в профиле пользователя?
3. Что называется локальным профилем?
4. Что называется перемещаемым профилем?
5. Что называется обязательным профилем? Когда он создается?
6. Когда создается временный профиль?
7. Как изменить тип профиля для пользователя?
8. Как изменить домашнюю папку для пользователя?
9. Как настроить права доступа на папку для пользователей?
10. Для каких целей используются квоты? Как настроить квоты?
11. В чём отличие мягкой квоты и от жёсткой?
12. Как узнать, какой тип профиля у пользователя?
13. Зачем создавать домашнюю папку для пользователя?

Список литературы

1 Станек У. Р. Microsoft Windows Server® 2012. Справочник администратора: Пер. с англ. — М.: Издательство «Русская редакция»; СПб.: «БХВ-Петербург», 2014. — 688 с.

2 Минаси М., Грин К., Бус К. и др. Windows Server 2012 R2. Полное руководство. Том 1. Пер. с англ.— М.: ООО «И.Д.Вильямс». 2015. -960 с.

3 Моримото Р., Нозл М., Ярдени Г. и др. Microsoft Windows Server 2012. Полное руководство. Пер. с англ. — М.: ООО «И.Д.Вильямс». 2013. - 1456 с.

4 Дерек М. Групповая политика Windows. Ресурсы Windows Server 2008, Windows Vista, Windows XP, Windows Server 2003: —Москва, Русская Редакция, БХВ-Петербург, 2009г.- 544 с.

5 Холл Майк Д. Официальный учебный курс Microsoft : Внедрение, управление и поддержка сетевой инфраструктуры Microsoft Windows Server 2003. Учебный курс Microsoft / Пер. с англ. — М. : Издательство «Русская редакция», 2011. — 960 стр.

Сатимова Елена Григорьевна

БЕЗОПАСНОСТЬ И АДМИНИСТРИРОВАНИЕ WINDOWS SERVER

Методические указания по выполнению лабораторных работ
для студентов специальности
5В100200 – «Системы информационной безопасности»

Редактор Л.Т. Сластихина
Специалист по стандартизации Г.И. Мухаметсариева

Подписано в печать 28.01. 2019г.
Тираж 40 экз.
Объем 6,5 уч.-изд.л.

Формат 60x84 1/16.
Бумага типографская №1
Заказ № 73 Цена 3250 тенге

Копировально-множительное бюро
некоммерческого акционерного общества
«Алматинский университет энергетики и связи»
050013, Алматы, ул. Байтурсынова, 126