ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

**БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ**

**ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ**

(НИУ «БелГУ»)

ИНСТИТУТ ИНЖЕНЕРНЫХ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

КАФЕДРА МАТЕМАТИЧЕСКОГО

И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

**Отчет по лабораторной работе 3**

**по дисциплине: «Компьютерные сети»**

студента очного отделения

4 курса 12001801 группы

Капустина Виктора Сергеевича

Проверил(а):

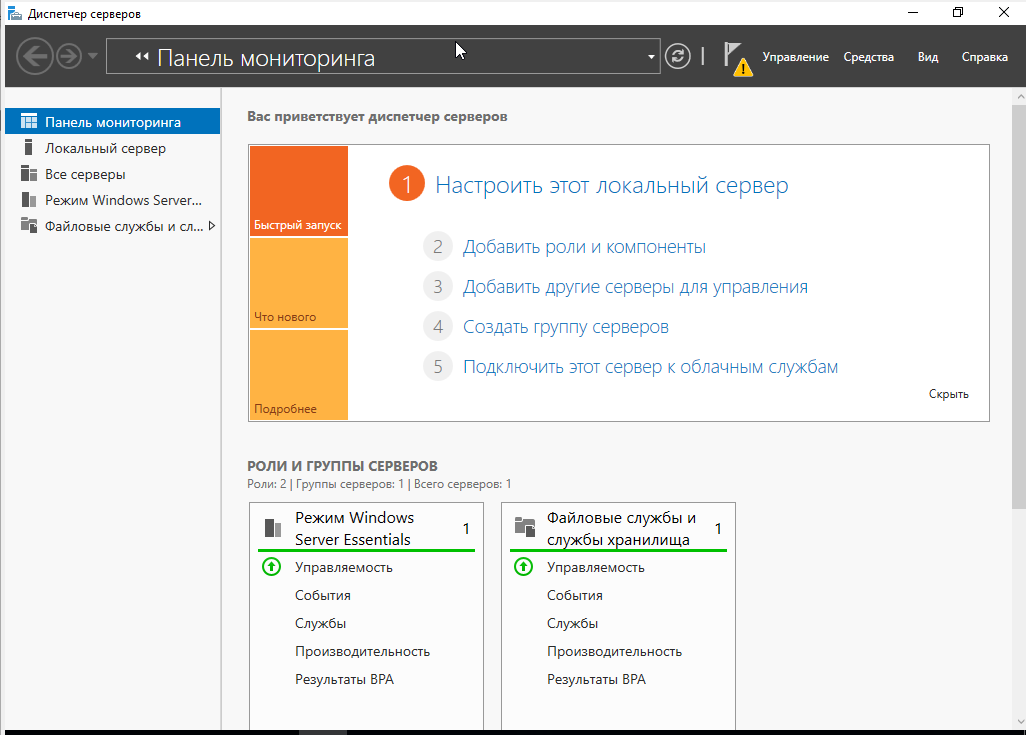
Маматов Евгений Михайлович

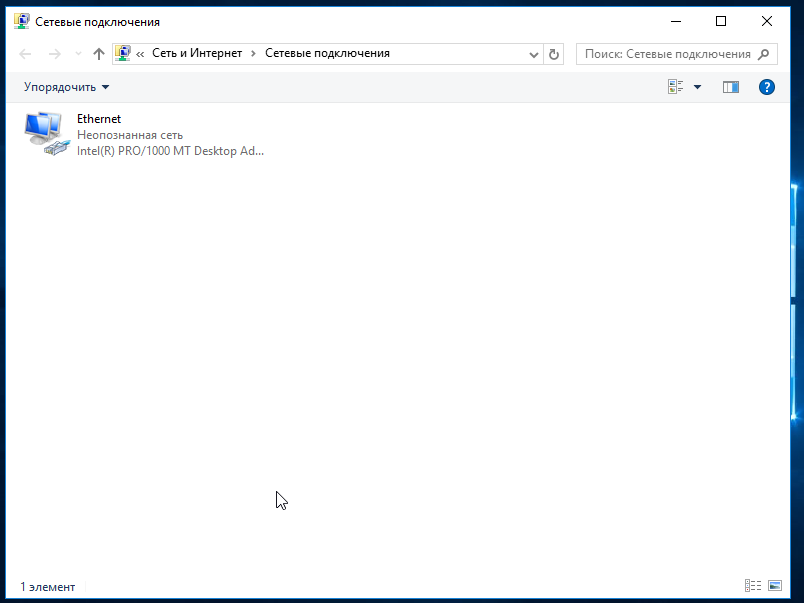
Белгород 2022

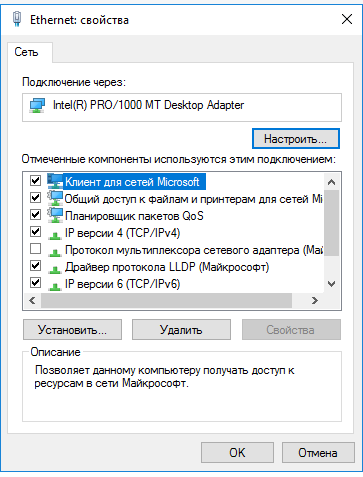
**Лабораторная работа 3**

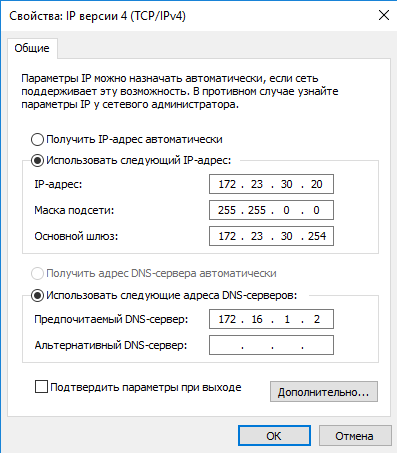
**Цель работы:** установка службы каталогов Active Directory в Windows 2016 Server.

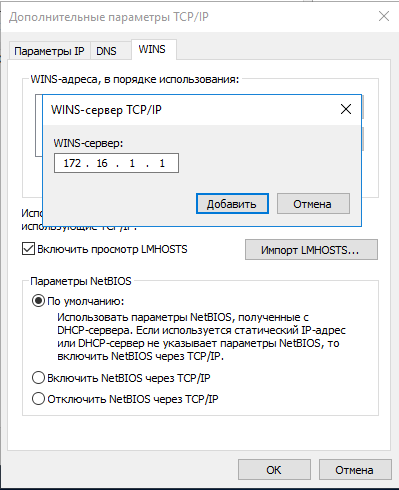
**Ход работы**

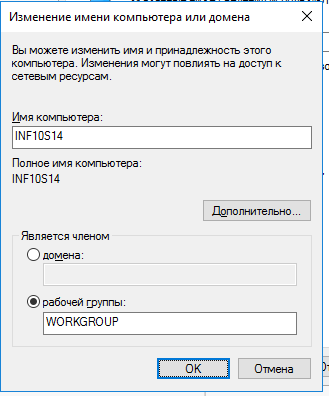
  
Рис. 1 Диспетчер серверов

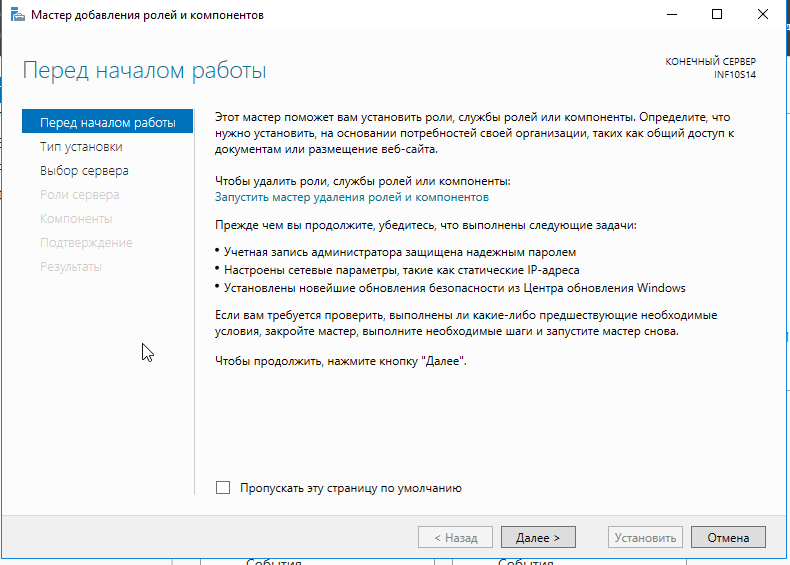
  
Рис. 2 Список адапетров

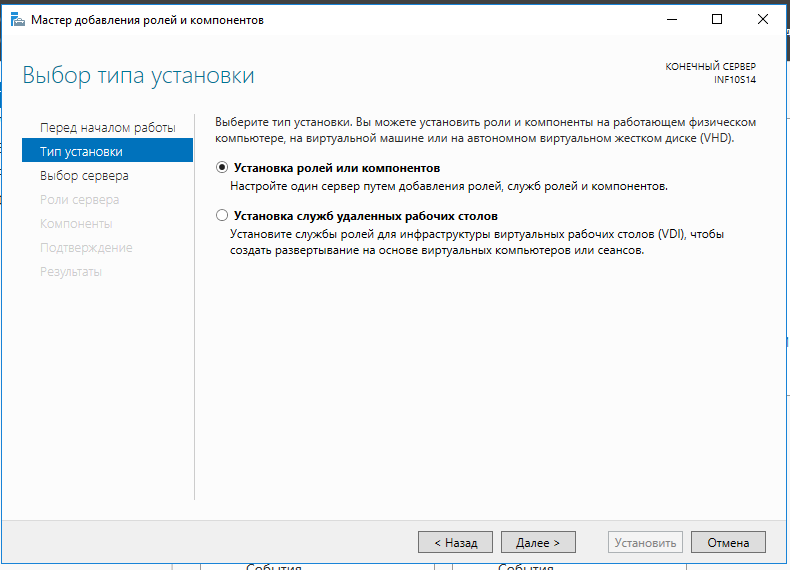
  
Рис. 3 Свойства адаптера

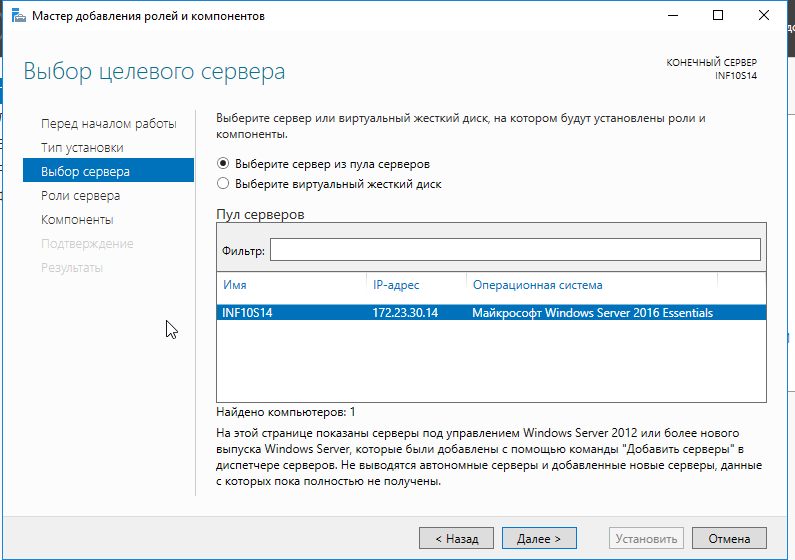
  
Рис. 4 Настройка IPv4

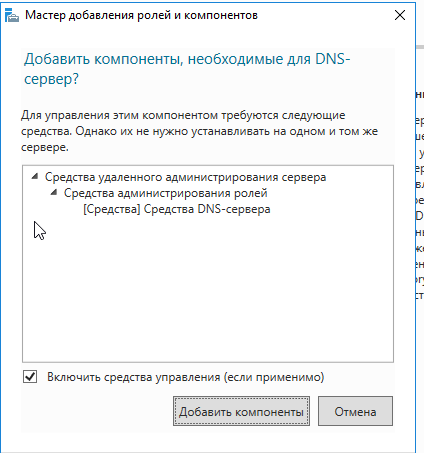
  
Рис. 5 Добавление WINS-адреса

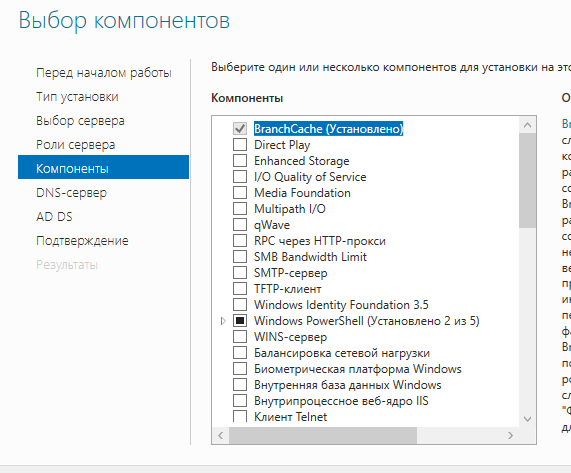
  
Рис. 6 Настройка имени домена

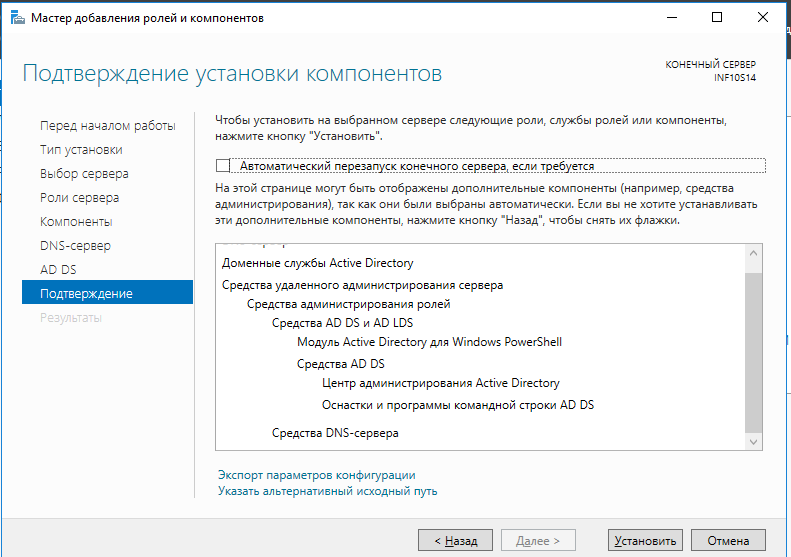
  
Рис. 7 Открытие Мастера добавления роли и компонентов

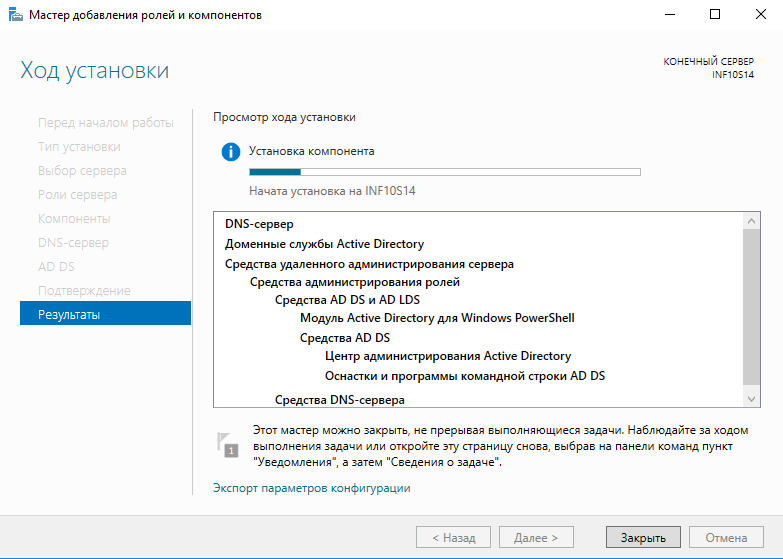
****Рис. 8 Выбор типа установки

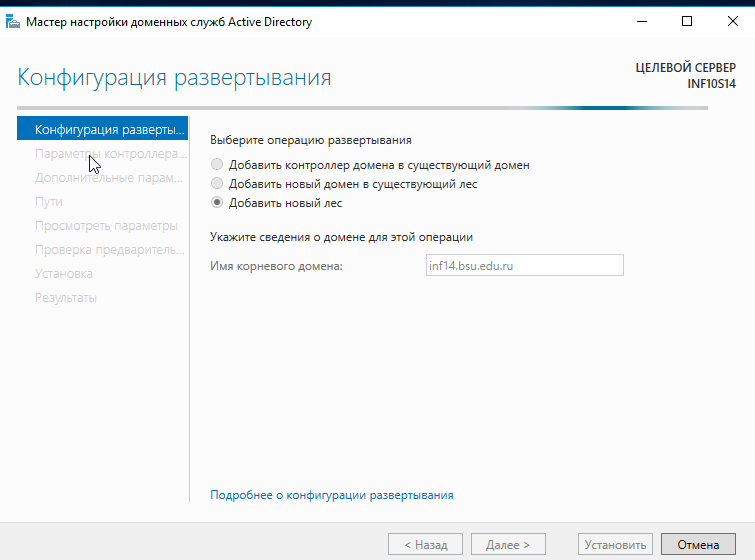
  
Рис. 9 Выбор сервера

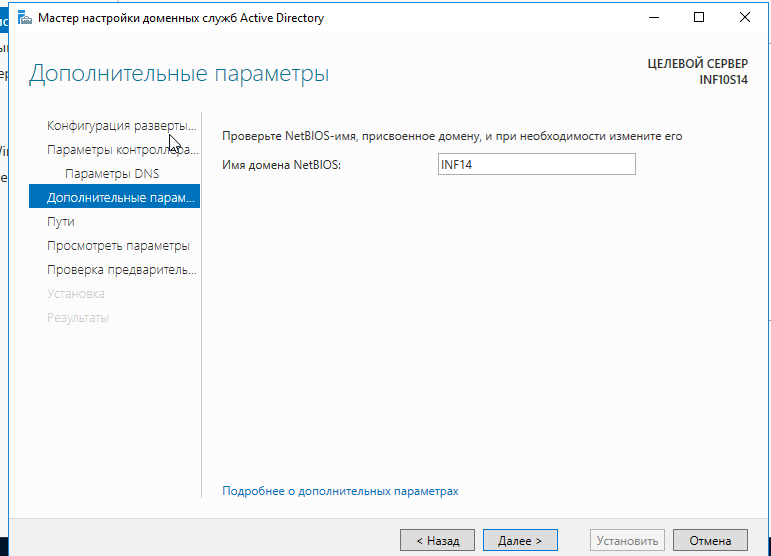
  
Рис. 10 Добавление компонента для DNS-сервера

  
Рис. 11 Компонент BranchCache уже установлен

  
Рис. 12 Установка компонентов

  
Рис. 13 Ход установки

  
Рис. 14 Конфигурация развертывания

  
Рис. 15 Имя домена NetBIOS

**Вывод:** на данной лабораторной установил службы каталогов Active Directory в Windows 2016 Server.

**Ответы на контрольные вопросы:**

**1.** **Понятие процесса**

**Процесс** — выполнение пассивных инструкций компьютерной программы на процессоре ЭВМ. Часто процессом называют выполняющуюся программу и все её элементы: адресное пространство, глобальные переменные, регистры, стек, открытые файлы и т. д.

**2.** **Проблема синхронизации процесса**

Процессам часто нужно взаимодействовать друг с другом, например, один процесс может передавать данные другому процессу, или несколько процессов могут обрабатывать данные из общего файла. Во всех этих случаях возникает проблема синхронизации процессов, которая может решаться приостановкой и активизацией процессов, организацией очередей, блокированием и освобождением ресурсов.

**3.** **Виды ресурсов ПК, распределяемых между процессами и задачами**

Ресурсом является любой компонент ЭВМ и предоставляемые им возможности: центральный процессор, оперативная или внешняя память, внешнее устройство, программа и т.д. Ресурсы подразделяются на четыре вида.

Виды ресурсов персонального компьютера:

1. Аппаратные ресурсы (Hardware)

2. Файловые ресурсы

3. Программные ресурсы (Software)

4. Сетевые ресурсы

*Аппаратные ресурсы* – это системный блок, периферийные устройства, любое оборудование, подключенное к компьютеру.

*Файловые ресурсы* – это файлы и папки, а также вся файловая система.

*Программные ресурсы* – это все программы установленные в компьютере (ПО).

Программное обеспечение подразделяется на два вида: системное и прикладное ПО:

· Системное программное обеспечение набор программ необходимой для функционирования компьютерной системы в целом.

· Прикладное программное обеспечение программы необходимые пользователю для решения тех или иных задач.

*Сетевые ресурсы* – это ресурсы других компьютеров доступные по локальной или глобальной сети. Могут быть: оборудование(т.е. аппаратные ресурсы другого ПК или сетевые устройства, например, сетевой принтер); информация(т.е. фалы и папки другого компьютера - информация в Интернете или на сервере); программное обеспечение(установленное на другом компьютере).

По характеру использования могут различаться следующие категории ресурсов:

- *выделяемые* (монопольно используемые, неперераспреде­ляемые) ресурсы характеризуются тем, что выделяются процессам в момент их возникновения и освобождаются только в момент завершения процессов; в качестве такого ресурса может рассматриваться, например, устройство чтения на магнитных лентах;

- *повторно распределяемые ресурсы* отличаются возможностью динамического запрашивания, выделения и освобождения в ходе выполнения процессов (таковым ресурсом является, например, оперативная память);

- *разделяемые* ресурсы, особенность которых состоит в том, что они постоянно остаются в общем использовании и выделяются процессам для использования в режиме разделения времени (как, например, процессор, разделяемые файлы и т.п.);

- *многократно используемые* (реентерабельные) ресурсы выделяются возможностью одновременного использования несколькими процессами (что может быть обеспечено, например, при неизменяемости ресурса при его использовании; в качестве примеров таких ресурсов могут рассматриваться реентерабельные программы, файлы, используемые только для чтения и т.д.).

**4.** **Понятие дедлоков, нитей**

**Deadlock или взаимная блокировка –** ситуация в многозадачной среде или СУБД, при которой несколько процессов находятся в состоянии ожидания ресурсов, занятых друг другом, и ни один из них не может продолжать своё выполнение.

**Thread или нить -** это виртуальный процессор, имеющий свой собственный набор регистров, аналогичных регистрам настоящего центрального процессора.

**5.** **Архитектура Active Directory**

Active Directory — это технология Microsoft, которая представляет собой распределенную базу данных, в которой хранятся объекты в иерархическом, структурированном и безопасном формате.

Active Directory составляют несколько основных архитектурных компонентов: схема, мо­дели данных, безопасности и администрирования.

**Модель данных**

Каталог содержит объекты, представляющие раз­личные компоненты сети. Каждый объект представлен атрибутами. Совокупность объек­тов, допустимых для хранения в каталоге, определяется схемой.

**Схема**

Реализована как набор экземпляров классов объектов, хранимых в каталоге. Схема обновляется путем создания или из­менения хранимых в каталоге объектов схемы. Как и все объекты хранилища Active Directory, объекты схемы защищены *списками управления доступом* (access control list, ACL), поэтому изменять схему разрешено только правомочным пользователям.

**Модель безопасности**

Каталог — полноценная составляющая инфраструктуры безопасности Windows 2003. ACL защищает все объекты в хранилище Active Directory. Средства авторизации доступа Windows 2003 применяют ACL для разрешения доступа к объектам или атрибутам в хра­нилище Active Directory.

**Модель администрирования**

Active Directory администрируют только авторизованные пользователи. Администратор праве предоставить пользователю некий стандартный набор разрешений для выполнения только определенных действий над указанной совокупностью экземпляров или классов объектов в конкретном поддереве каталога.

**6.** **Планирование пространства имён**

Важно сразу решить, будут ли одинаковы внутреннее (защищенное брандмауэром) и внеш­нее (за его пределами) пространство имен. Иначе говоря, будет ли пространство имен Active Directory соответствовать пространству имен DNS (как правило, имени домена в Интернете), которое, возможно, уже определено для Вашей организации?

Допустим, внешнее пространство имен DNS организации — microsoft.com. Мы можем использовать пространство имен Active Directory, соответствующее microsoft.com, или вы­брать другое внутреннее пространство имен.

Существует два варианта разработки пространства имен Active Directory.

Первый вариант подразумевает, что внутреннее и внешнее пространства имен одинаковы, т. е. названия доменов высшего уровня идентичны по обе стороны брандмауэра. Во втором случае внутреннее и внешнее пространства имен различны, т. е. имя домена высшего уровня в пределах брандмауэра отличается от высшего зарегистрированного имени домена DNS, видимого из Интернета. Внутреннее пространство имен будет expedia.com, а внешнее – microsoft.com.

**Вариант 1. Внутреннее и внешнее пространства имен идентичны**

По этому сценарию организация использует одно и то же имя для внешнего и внутренне­го пространств имен. Например, имя microsoft.com будет применяться для доступа к ре­сурсам как изнутри организации, так и из Интернета. Для реализации этого сценария надо соблюсти следующие условия:

• клиенты внутренней сети должны иметь доступ к внутреннему и внешнему серверам (по обе стороны брандмауэра);

• клиенты, обращающиеся к ресурсам извне, не должны иметь доступ к внутренним ре­сурсам организации или разрешению имен.

Для реализации этого сценария необходимы две раздельные зоны DNS. Одна – за пределами брандмауэра — будет обеспечивать разрешение имен только для общедоступ­ных ресурсов.

*Преимущества*

*•* Имя дерева, microsoft.com, согласовано в частной сети и Интернете.

• Появляется возможность унифицировать вход в систему — для этого пользователи ло­кальной сети и Интернета смогут применять одно и то же имя, например, username@microsoft.com будет служить как регистрационное имя и как идентификатор элек­тронной почты.

*Недостатки*

*•* Усложняется конфигурация — при настройке прокси-клиентов надо учесть, что внут­ренние и внешние ресурсы отличаются.

• Придется следить, чтобы внутренние ресурсы случайно не стали общедоступными.

• Вдвое усложняется управление ресурсами — например, придется дублировать записи зоны для внутреннего и внешнего разрешения имен.

• Даже если пространство имен одно и то же, внутренние и внешние ресурсы будут пред­ставляться пользователям по-разному.

**Вариант 2. Внутреннее и внешнее пространства имен различаются**

По разные стороны брандмауэра — внутри и вне корпоративной сети — применяются разные имена. Например, пользователи Интернета будут видеть имя microsoft.com, а интрасети — expedia.com. Оба этих пространства имен должны быть зарегистрированы в DNS Интернета во избежание дублирования внутреннего имени в другой общей сети. Если внутреннее имя не зарезервировано и используется другой организацией, внутренние кли­енты не отличат внутреннее имя от чужого публично зарегистрированного пространства имен DNS.

Будут установлены две зоны: одна будет отвечать за разрешение имен в пространстве microsoft.com, а другая — в пространстве expedia.com. В результате клиенты смогут четко различать внутренние и внешние ресурсы.

*Преимущества*

1 Четкая разница между внутренними и внешними ресурсами за счет применения различных доменных имен.

2 Упрощается настройка прокси-клиентов, поскольку списки исключения при опозна­вании внешних ресурсов должны будут содержать только expedia.com.

*Недостатки*

1 Регистрационные имена отличаются от имен электронной почты. Например, если кто-нибудь входит под именем usemame@microsoft.com, то адрес его электронной почты будет username@expedia.com, что неудобно.

2 В DNS Интернета придется зарегистрировать больше имен.

**7.** **Выбор архитектуры пространства имён**

Архитектура пространства имен должна отражать структуру предприятия и одновре­менно обеспечивать степень административной детализации, необходимую для эффектив­ного управления корпоративной и глобальной сетью посредством Active Directory.

Соблюсти эти условия позволяет наличие трех уровней доменов:

1 корневой домен;

2 домен первого уровня;

3 доменвторого уровня.

**Корневой домен**

*Корневой домен* (root domain) Active Directory определяет пространство имен компании. Все внутренние домены являются частью этого домена, создавая непрерывное связное пространство имен в виде дерева доменов. Кроме того, серверы, содержащие корень пространства, скрыты за брандмауэром и, следовательно, не будут видимы из Интернета.

**Домены первого уровня**

Этот уровень модели отвечает за создание доменных имен, которые не изменяются даже при внутренней реорганизации предприятия. Простейший вариант – давать названия таким доменам, исходя из географических или политических границ.

Доверительные отношения между корневым доменом и всеми доменами первого уровня делают ресурсы доступными для всех ветвей дерева доменов.

**Домены второго уровня**

В идеале должны содержать только коды стран и ответвления от доменов первого уровня. Преимущество этого подхода: ниже доменов второго уровня можно создавать дочерние домены.

Используйте те же правила именования при создании ОП в доменах — это позволит при необходимости повысить ОП до уровня домена с минимальными издержками.

**8.** **Планирование организационных подразделений.**

ОП должны отражать подробности структуры организации. Создание ОП позволяет делегировать полномочия по администрированию небольших групп пользователей, групп и ресурсов. Вы вправе предоставить полный административный контроль или ограниченный.

ОП устраняют необходимость предоставлять пользователям административный дос­туп на уровне домена для выполнения таких задач как, например, создание учетных запи­сей и установка паролей. Теперь можно предоставить пользователям административные полномочия на уровне ОП и тем самым освободить от этих администраторов доменов. ОП добавляет новый уровень защиты путем ограничения видимости общедоступных ре­сурсов — пользователь видит лишь объекты, к которым имеет доступ. ОП наследует политику безопасности от родительского домена и ОП.

**Создание структуры ОП**

Целесообразно начинать с разработки структуры ОП для первого домена в пространстве имен. Используйте этот домен и структуру ОП как модель для добавляемых в будущем доменов.

При создании ОП важно определить, кто сможет просматривать определенные объек­ты и управлять ими и какими полномочиями в отношении данного объекта будет обла­дать каждый администратор. Надо также выбрать администраторов, которым будет пре­доставлен глобальный доступ к некоторым ОП и объектам, и корректно ограничить пол­номочия остальных администраторов.