Федеральное государственное образовательное бюджетное

учреждение высшего образования

**«Финансовый университет при Правительстве Российской Федерации»**

**(Финансовый университет)**

Колледж информатики и программирования

**ОТЧЁТ**

**По Учебной практике №6**

Студент: Рачков Дмитрий Сергеевич

Дисциплина/Профессиональный модуль: УЧ ПР ОС

Выполнил студент

Группы: 2ОИБАС-1222

Преподаватель

Сибирев И.В.

Оценка за работу :\_\_\_\_\_\_\_

**Москва – 2024г.**

# Оглавление

[**СЕТЕВЫЕ ТЕХНОЛОГИИ:**](#_bookmark0)

[теория и практика администрирования 1](#_bookmark0)

[Оглавление 4](#_bookmark1)

[Предисловие 6](#_bookmark2)

[Введение восновы администрирования 8](#_bookmark3)

[Безопасность в компьютерных сетях 8](#_bookmark4)

[Служба каталогов Active Directory 10](#_bookmark5)

[Мультисервисные сети 14](#_bookmark6)

[Модуль 1.](#_bookmark7)

[Проектирование и администрирование 23](#_bookmark7)

[Лабораторная работа 1.1.](#_bookmark8)

[Основы проектирования ЛВС 24](#_bookmark8)

[Лабораторная работа 1.2.](#_bookmark9)

[Установка серверной операционной системы 31](#_bookmark9)

[Лабораторная работа 1.3.](#_bookmark10)

[Установка и настройка сервера DNS 41](#_bookmark10)

[Лабораторная работа 1.4.](#_bookmark11)

[Работа с Active Directory 61](#_bookmark11)

[Примерные тестовые задания к модулю 1 71](#_bookmark12)

[Контрольные вопросы к модулю 1 71](#_bookmark13)

[Модуль 2.](#_bookmark14)

[Настройка домена и его безопасность 73](#_bookmark14)

[Лабораторная работа 2.1.](#_bookmark15)

[Настройка параметров безопасности домена 74](#_bookmark15)

[Лабораторная работа 2.2.](#_bookmark16)

[Работа с серверами HTTPи FTP 81](#_bookmark16)

[Примерные тестовые задания к модулю 2 88](#_bookmark17)

[Контрольные вопросы к модулю 2 89](#_bookmark18)

[Модуль 3.](#_bookmark19)

[Обеспечение информационной безопасности 90](#_bookmark19)

[Лабораторная работа 3.1.](#_bookmark20)

[Мониторинг состояния элементов сети 91](#_bookmark20)

[Лабораторная работа 3.2.](#_bookmark21)

[Исследование удаленной системы для выявления уязвимостей 100](#_bookmark21)

[Лабораторная работа 3.3.](#_bookmark22)

[Сетевая антивирусная защита 108](#_bookmark22)

[Примерные тестовые задания к модулю 3 114](#_bookmark23)

[Контрольные вопросы к модулю 3 115](#_bookmark24)

[Модуль 4.](#_bookmark25)

[Защита информации в компьютере 116](#_bookmark25)

[Лабораторная работа 4.1.](#_bookmark26)

[Настройка параметров безопасности Интернет браузера 117](#_bookmark26)

[Лабораторная работа 4.2](#_bookmark27)

[Технология защиты сетевых компьютеров. Брандмауэр. 122](#_bookmark27)

[Лабораторная работа 4.3](#_bookmark28)

[Создание резервных копий 130](#_bookmark28)

[Примерные тестовые задания к модулю 4 135](#_bookmark29)

[Контрольные вопросы к модулю 4 136](#_bookmark30)

[Модуль 5.](#_bookmark31)

[Возможности мультисервисных сетей 137](#_bookmark31)

[Лабораторная работа 5.1](#_bookmark32)

[Потоковое вещание 138](#_bookmark32)

[Лабораторная работа 5.2.](#_bookmark33)

[IP-телефония 145](#_bookmark33)

[Лабораторная работа 5.3.](#_bookmark34)

[Видеоконференция 151](#_bookmark34)

[Примерные тестовые задания к модулю 5 159](#_bookmark35)

[Контрольные вопросы к модулю 5 160](#_bookmark36)

[БАЗА ТЕСТОВЫХ ЗАДАНИЙ 160](#_bookmark37)

[Приложение 1 174](#_TOC_250001)

[Приложение 2 179](#_TOC_250000)

СЛОВАРЬ СПЕЦИАЛЬНЫХ ТЕРМИНОВ 180

[ОБЩИЙ СПИСОК ЛИТЕРАТУРЫ 205](#_bookmark39)

# Предисловие

Без компьютерных сетей сегодня не представляется ни одно образо- вательной учреждение. Компьютерные сети используют для совместного решения информационных, вычислительных, учебных и других задач. В учебных заведениях они представляют собой основу информационно-об- разовательных сред.

Для компьютерных сетей образовательных заведений, как и для других компьютерных сетей, необходимо профессиональное обслужива- ние, включающее администрирование, мониторинг, обеспечение информа- ционной безопасности. В современных образовательных заведениях, в силу ряда причин различного характера, такая работа возлагается на учите- ля информатики, который должен уметь эффективно решать возникающие в профессиональной деятельности задачи по обеспечению функционирова- ния учебной компьютерной сети, активно участвовать в поддержке и разви- тии информационно-образовательной среды учебного заведения.

Вторая часть учебно-методического пособия «Сетевые технологии: теория и практика администрирования» предназначена для обеспечения бу- дущих учителей информатики специальными компетентностями в области администрирования учебных компьютерных сетей, в частности, такими знаниями и умениями, как: проектирование и администрирование компью- терных сетей учебных заведений; настройка домена и его безопасности; обеспечение информационной безопасности сети; защита информации в компьютере; использование современных мультисервисных сетей.

В качестве средств освоения основ настройки и администрирования учебных компьютерных сетей предлагается использовать такие современ- ные технологии виртуализации, как виртуальные машины – специальное программное обеспечение, позволяющее на одном компьютере одновре- менно использовать не только различные операционные системы, но и со- здавать виртуальные компьютерные сети.

Пособие построено по модульному принципу, позволяющему сту- денту осваивать отдельные темы, независимо друг от друга. Каждый учеб- ный модуль содержит *цель* и *план* его освоения, *литературу* и *информаци- онные ресурсы*, *тестовые задания* и *контрольные вопросы* для защиты мо- дуля.

*План* изучения модуля содержит такие компоненты, как:

* изучение теоретических вопросов, необходимых для выполнения лабораторных работ и защиты модуля;
* выполнение лабораторных работ по предложенным разработкам;
* знакомство с примерными тестовыми заданиями к модулю, со- держащимися в контрольном тестировании по дисциплине;
* защита модуля на основе выполненных лабораторных работ и контрольных вопросов.

В каждом модуле присутствует несколько обязательных для выпол- нения лабораторных работ. Каждая лабораторная работа включает в себя такие компоненты, как: *цель*, *средства* для выполнения работ, *теоретиче- скиесведения*, *выполнениеработы*, *самостоятельныезадания*.

*Теоретическиесведения* помогут студенту сориентироваться в учеб- ном материале, подлежащем освоению в практической части модуля.

Компонент*Выполнениеработы* содержит не только задания, но и инструкции по их выполнению, а также *самостоятельныезадания*.

Представленные*базытестовыхматериалов* к модулям помогут сту- денту подготовиться к контрольному тестированию по дисциплине.

Представленный в пособии глоссарийпозволит обучаемым быстрее усвоить значение используемых в сетевых технологиях международных терминов и аббревиатур.

Обратим внимание на то, что перед выполнением лабораторных ра- бот надо ознакомиться с необходимыми для выполнения работы аппарат- ными, программными и информационными средствами и заблаговременно позаботиться об их наличии.

# Введение восновы администрирования

## Безопасность в компьютерных сетях

**Цели защиты** информации в сетях сводятся к обеспечению целостности (физической и логической) информации, а также предупреждение несанкционированной ее модификации, получения и размножения. Задачи защиты информации в компьютерных сетях определяются теми угрозами, которые потенциально возможны в процессе их функционирования, в частности:

* *прослушивание каналов*, т.е. запись и последующий анализ всего проходящего потока сообщений;
* *умышленное уничтожение или искажение* (фальсификация) информации;
* *присвоениезлоумышленником чужого идентификатора* своему узлу или ретранслятору;
* *преднамеренный разрыв линии связи*, что приводит к полному прекращению доставки сообщений;
* *внедрение сетевых вирусов*.

Таким образом,специфические задачи защиты информации в компьютерной сети состоят в следующем:

* *конфиденциальность (маскировка данных)*– предотвращение пассивных атак для передаваемых или хранимых данных;
* *арбитражное обеспечение,* т.е. защита от возможных отказов от фактов отправки, приема или содержания отправленных или принятых данных.
* *аутентификация объектов,* заключающая в подтверждении подлинности взаимодействующих объектов;
* *контроль доступа,* т.е. защита от несанкционированного использования ресурсов сети;
* *контроль и восстановление целостности* находящихся в сети данных;
* *доступность*– защита от потери или снижения доступности того или иного сервиса.

Для решения этих задач создаются специальные механизмы защиты

–т.н.сервисы безопасности, которые в общем случае могут быть представлены следующим образом: *идентификация/аутентификация; разграничение доступа; протоколирование/аудит; экранирование;*

*тунелирование; шифрование; контроль целостности; контроль защищенности; обнаружение отказов и оперативное восстановление и управление.*

Применительно к различным уровням семиуровнего протокола передачи данных задачи конкретизируются следующим образом:

* на *физическом уровне*– контроль электромагнитных излучений линий связи и устройств, поддержка коммутационного оборудования в рабочем состоянии (экранирующие устройства, генераторы помех, средства физической защиты передающей среды);
* на *канальном уровне*– это шифрование данных;
* *сетевой уровень*– наиболее уязвимый, поскольку сетевые нарушения (чтение, модификация, уничтожение, дублирование, переориентация, маскировка под другой узел) осуществляются и использованием его же протоколов. Здесь основой защиты выступают средства криптографии;
* на *транспортном уровне* все активные угрозы становятся видимыми, но не все угрозы можно предотвратить криптографическими методами, анализом регулярности трафика и посылкой параллельных дубликатов сообщений по другим путям, используемыми на данном уровне;
* протоколы *сеансового* и *представительного* уровня функций защиты практически не выполняют;
* в функции защиты протокола *прикладного уровня* входит управление доступом к определенным наборам данных, идентификация и аутентификация определенных пользователей и другие функции, определенные конкретным протоколом. Более сложными эти функции являются при реализации полномочной политики безопасности в сети.

Практически все механизмы сетевой безопасности могут быть реализованы на третьем уровне эталонной модели ***ISO/OSI***. Более того, ***IP***- уровень считается самым оптимальным для размещения защитных средств, поскольку при этом достигается компромисс между защищенностью, эффективностью функционирования и прозрачностью для приложений.

Наиболее проработанными являются вопросы защиты на ***IP***-уровне. Спецификации (протоколы) семейства ***IPsec*** (рабочая группа ***IP Security***)

обеспечивают: *управление доступом; контроль целостности на уровне пакетов (вне соединения); аутентификацию источника данных; защиту от воспроизведения; конфиденциальность (включая частичную защиту от анализа трафика); администрирование (управление криптографическими ключами).*

К основным механизмам безопасности относят:

* *Алгоритмы симметричного шифрования,* в которых для шифрования и дешифрования используется один и тот же ключ или ключ дешифрования может быть получен из ключа шифрования.
* *Алгоритмы ассиметричного шифрования,* в которых для шифрования и дешифрования используются два разных ключа, называемые открытым и закрытым ключами, причем, зная один, другой вычислить невозможно.
* *Хэш-функции* – функции, входным значением для которой является сообщение произвольной длины, а выходным значением

– сообщение фиксированной длины, которое может быть использовано для аутентификации исходных данных.

**Служба каталогов *Active Directory***

***A****ctive* ***D****irectory****(AD)***является службой каталогов, совместимой соблегчённым протоколом доступа к каталогам ***LDAP***(***L****ightweight* ***D****irectory* ***A****ccess* ***P****rotocol*). Она представляет собой средство иерархического представления ресурсов, принадлежащих некоторой отдельно взятой организации, и информации об этих ресурсах корпорации Майкрософт для операционных систем семейства ***Windows NT****.*

***Active Directory*** позволяет администраторам использовать глобальные политики, развёртывать программы на множестве компьютеров (через глобальные политики или посредством ***MicrosoftSystems Management Server 2003***) и устанавливать важные обновления на всех компьютерах в сети (с использованием ***WSUS****(****W****indows* ***S****erver* ***U****pdate* ***S****ervices)*,ранее***SUS*** *(****S****oftware* ***U****pdate* ***S****ervices)*. ***Active Directory*** хранит данные и настройки среды в централизованной базе данных. Сети ***Active Directory*** могут быть различного размера: от нескольких сотен до нескольких миллионов объектов.

***Active Directory*** имеет иерархическую структуру, состоящую из объектов,подразделяемых на три основные категории: ресурсы (например,

принтеры), службы (например, электронная почта) и люди (учётные записи пользователей и групп пользователей). ***Active Directory*** предоставляет информацию об объектах, позволяет организовывать объекты, управлять доступом к ним, а также устанавливает правила безопасности.

Каждый объект представляет отдельную *сущность*(пользователь, компьютер, принтер, приложение или общая сетевая папка) и его *атрибуты*. Объекты могут также быть *контейнерами* для других объектов. Объект уникально идентифицируется своим именем и имеет набор атрибутов – характеристик и данных, которые объект может содержать, – которые зависят от типа объекта. Атрибуты являются составляющей базовой структуры объекта и определяются в схеме. Схема определяет, какие типы объектов могут существовать в ***AD.***

Сама схема состоит из двух типов объектов: *объекты классов схемы* и *объекты атрибутов схемы*. Один объект класса схемы определяет один тип объекта ***Active Directory*** (например, объект «Пользователь»), а один объект атрибута схемы определяет атрибут, который объект может иметь.

Каждый объект атрибута может быть использован в нескольких разных объектах классов схемы. Эти объекты называются объектами схемы (или метаданными) и позволяют изменять и дополнять схему, когда это необходимо. Однако каждый объект схемы является частью определений объектов ***Active Directory***, поэтому деактивация или изменение этих объектов может иметь серьёзные последствия, так как в результате этих действий будет изменена структура ***AD***. Изменение объекта схемы автоматически распространяется в ***Active Directory***. Будучи однажды созданным объект схемы не может быть удалён, он может быть только деактивирован. Обычно все изменения схемы тщательно планируются.

#### Леса, деревья и домены

Верхним уровнем структуры является *лес*– совокупность всех объектов, атрибутов объектов и правил (синтаксиса атрибутов) в ***Active Directory***. Лес содержит одно или несколько деревьев, связанных транзитивными отношениями доверия. Дерево содержит один или несколько доменов, также связанных в иерархию транзитивными отношениями доверия. Домены идентифицируются своими структурами имён ***DNS***– пространствами имён.

Объекты в домене могут быть сгруппированы в контейнеры – подразделения. Подразделения позволяют создавать иерархию внутри домена, упрощают его администрирование и позволяют моделировать

организационную и/или географическую структуры компании в ***Active Directory***. Подразделения могут содержать другие подразделения. Корпорация Майкрософт рекомендует использовать как можно меньше доменов в ***Active Directory***, а для структурирования ***AD*** и политик использовать подразделения. Часто групповые политики применяются именно к подразделениям. Групповые политики сами являются объектами. Подразделение является самым низким уровнем, на котором могут делегироваться административные полномочия.

Другим способом деления ***AD*** являются «сайты», которые являются способом физической (но не логической) группировки на основе подсетей ***IP***. Сайты подразделяются на имеющие подключения по низкоскоростным каналам (например, по каналам глобальных сетей, с помощью виртуальных частных сетей) и по высокоскоростным каналам (например, через локальную сеть). Сайт может содержать один или несколько доменов, а домен может содержать один или несколько сайтов. При проектировании ***Active Directory*** важно учитывать сетевой трафик, создающийся при синхронизации данных ***AD*** между сайтами.

Ключевым решением при проектировании ***AD*** является решение о разделении информационной инфраструктуры на иерархические домены и подразделения верхнего уровня. Типичными моделями, используемыми для такого разделения, являются модели разделения по функциональным подразделениям компании, по географическому положению и по ролям в информационной инфраструктуре компании. Часто используются комбинации этих моделей.

#### Физическая структура и репликация

Физически информация ***AD*** хранится на одном или нескольких равнозначных контроллерах доменов, заменивших использовавшиеся в ***Windows NT*** основной и резервные контроллеры домена (хотя для выполнения некоторых операций сохраняется и так называемый сервер

«операций с одним главным сервером», который может эмулировать главный контроллер домена). Каждый контроллер домена хранит копию данных ***AD***, предназначенную для чтения и записи. Изменения, сделанные на одном контроллере, синхронизируются на все контроллеры домена при репликации. Серверы, на которых сама служба ***Active Directory*** не установлена, но которые при этом входят в домен ***AD***, называются рядовыми серверами.

*Репликация* ***AD*** выполняется по запросу. ***AD*** создаёт топологию

репликации, которая использует сайты, определённые в системе, для управления трафиком. Внутрисайтовая репликация выполняется часто и автоматически с помощью средства проверки согласованности.

Репликация между сайтами может быть настроена для каждого канала сайта (в зависимости от качества канала) – различная «оценка» может быть назначена каждому каналу (например,***DS3, T1, ISDN*** и т. д.), и трафик репликации будет ограничен, передаваться по расписанию и маршрутизироваться в соответствии с назначенной оценкой канала. Данные репликации могут транзитивно передаваться через несколько сайтов через мосты связи сайтов, если «оценка» низка, хотя ***AD*** автоматически назначает более низкую оценку для связей «сайт-сайт», чем для транзитивных соединений. Репликация «сайт-сайт» выполняется серверами-плацдармами в каждом сайте, которые затем реплицируют изменения на каждый контроллер домена своего сайта.

Если в ***Active Directory*** несколько доменов, репликация во всём лесу не выполняется, а создаётся глобальный каталог, содержащий все объекты леса, но с ограниченным набором атрибутов (*неполная реплика*). Каталог хранится на указанных серверах глобального каталога и обслуживает междоменные запросы. Внутридоменная синхронизация выполняется по протоколу ***RPC*** по ***IP***, синхронизация в лесу – по протоколу ***SMTP***.

Возможность операций с одним главным компьютером позволяет обрабатывать запросы, когда репликация с несколькими главными компьютерами недопустима. Есть пять типов таких операций: эмуляция главного контроллера домена; главный компьютер относительного идентификатора; главный компьютер инфраструктуры; главный компьютер схемы; главный компьютер именования домена. Первые три роли относятся к домену, последние две – ко всему лесу. В каждом домене может быть только один сервер, обслуживающий любую из таких задач.

***AD*** можно разделить на три логические хранилища или разделы. Схема является шаблоном для ***AD*** и определяет все типы объектов, их классы и атрибуты, синтаксис атрибутов (все деревья находятся в одном лесу, потому что у них одна схема). Конфигурация является структурой леса и деревьев ***AD***. Домен хранит всю информацию об объектах, созданных в этом домене. Первые два хранилища реплицируются на все контроллеры доменов, но только часть каждого хранилища домена может быть использована контроллерами других доменов путём глобального каталога, так как границы домена ограничивают репликацию всей

информации домена.

База данных ***AD*** (хранилище каталогов) в ***Windows 2000*** использует расширяемую подсистему хранения ***Microsoft Jet Blue***, которая позволяет для каждого контроллера домена иметь базу размером до 16 терабайт и 1 миллиард объектов (теоретически, практические тесты выполнялись только с приблизительно 100 миллионами объектов). Файл базы называется ***ntds.dit***и имеет две основные таблицы: таблицу данных и таблицу связей. В ***Windows Server 2003***добавлена ещё одна таблица для обеспечения уникальности экземпляров дескрипторов безопасности.

#### Именование

***AD*** поддерживает следующие форматы именования объектов: универсальные имена типа ***UNC***, ***URL*** и ***LDAP URL***. Версия ***LDAP*** формата именования *X.500* используется внутри ***Active Directory***.

Каждый объект имеет *различающееся имя****DN***(***D****istinguished* ***N****ame*). Например, объект принтера с именем ***HPLaser3*** в подразделении

«Маркетинг» и в домене ***foo.org*** будет иметь следующее различающееся имя: ***CN=HPLaser3,OU=Маркетинг,DC=foo,DC=org***, где ***CN***– это общее имя, ***DC***– класс объекта домена. Различающиеся имена могут иметь намного больше частей, чем четыре части в этом примере.

У объектов также есть канонические имена. Это различающиеся имена, записанные в обратном порядке, без идентификаторов и с использованием косых черт в качестве разделителей: ***foo.org/Маркетинг/HPLaser3***.

Чтобы определить объект внутри его контейнера, используется *относительное различающееся имя:* ***CN=HPLaser3***. У каждого объекта также есть *глобально уникальный идентификатор* (***GUID***)–уникальная и неизменная 128-битная строка, которая используется в ***AD*** для поиска и репликации. Определённые объекты также имеют *имя участника- пользователя* (***UPN***, в соответствии с ***RFC 822***) в формате ***объект@домен***.

## Мультисервисные сети

Стремительный прогресс в области телекоммуникационных и информационных технологий привел к появлению новых терминов: мультимедиа-телекоммуникации, услуги широкополосного доступа, услуги с гарантией времени доставки трафика и др. Постепенно в западной литературе сформировался термин ***Time Warner F****ull* ***S****ervice* ***N****etwork* ***(FSN)***, означающий *полносервисные сети, предупреждающие потерю*

*качества из-за несвоевременной (с запаздыванием) доставки трафика*.

В российской литературе этот термин аналогичен понятию *мультисервисные сети*,которые готовы к предоставлению любых телекоммуникационных и информационных услуг – передачу голоса, мультимедийные услуги, передачу данных и многое другое. Мультисервисные сети могут быть созданы на основе как существующих цифровых, так и виртуальных сетей.

В общем случае*мультисервисная сеть (МСС)* представляет собой универсальную многоцелевую среду, предназначенную для передачи речи, изображения и данных с использованием технологии коммутации пакетов (***IP***). Она отличается степенью надежности, характерной для телефонных сетей (в противоположность негарантированному качеству связи через Интернет) и обеспечивает низкую стоимость передачи в расчете на единицу объема информации (приближенную к стоимости передачи данных по Интернету).

Основная задача мультисервисных сетей заключается в обеспечении работы разнородных информационных и телекоммуникационных систем и приложений в единой транспортной среде, когда для передачи обычного трафика (данных) и трафика другой информации (речи, видео и др.) используется единая инфраструктура.МСС использует единый канал для передачи данных разных типов, позволяет уменьшить разнообразие типов оборудования, применять единые стандарты, технологии и централизованно управлять коммуникационной средой.

Интерактивные ММС предоставляют абонентам широкий спектр услуг: пакеты аналогового и цифрового телевидения; потоковое вещание; Интернет, телефонию, видеоконференции; голосование и опрос населения; видеотелефонию; видео по требованию; дистанционное обучение; медицинские консультации; оплату коммунальных услуг с автоматическим съемом показаний со счетчиков воды, тепла и электроэнергии; охранную сигнализацию; видеонаблюдение и др.

Основными составляющими мультисервисной сети являются: *телепорт*, *транспортная сеть* и *кластеры*. Топология сети определяется спецификой местности, на которой она развертывается.

Под *телепортом* понимается единый центр управления, получения, обработки, создания и передачи информации. Он строится по модульной технологии (с возможностью поэтапного наращивания предоставляемых услуг) и формируется из оборудования и программного обеспечения для

организации приема эфирных и спутниковых ТВ- и радиопрограмм; формирования студийных программ; подключения к телефонной сети; подключения к сети Интернет; сбора и обработки данных телеметрии(показания датчиков воды, электричества и т.п.); сбора и обработки данных видеонаблюдения и датчиков пожарно-охранной сигнализации; мониторинга, контроля и управления состоянием сети и доступом к информационным потокам; и других видов услуг.

*Транспортная сеть*– двунаправленная широкополосная магистральная кабельная сеть, построенная по волоконно-оптической технологии со структурой *кольцо* или *звезда*. На транспортной сети располагаются узлы ввода-вывода и обработки информации, к которым осуществляется подключение телепорта и кластеров.

*Кластеры* представляют собой группы от 500 до 2 тыс. абонентов, территориально расположенных в непосредственной близости друг от друга, и охватываются интерактивной распределительной сетью.

Для создания мультисервисной сети необходимо сделать следующее:

* принять решение местными органами власти о необходимости создания сети;
* получить информацию о состоянии существующих телекоммуникационных сетей, услугах и тарифах;
* провести маркетинговые исследования;
* формировать концепцию создания сети;
* выпустить постановление об организации предприятия с определением учредителей;
* создать технико-экономическое обоснование создания сети;
* определить источники финансирования;
* организовать предприятие;
* провести изыскательские работы;
* составить пилотный проект; бизнес-план; проектно-сметную документацию;
* приобрести материалы и оборудование;
* выполнить строительно-монтажные работы;
* определить оператора сети;
* определить порядок осуществления технического обслуживания сети.

Классификации основных услуг ММС:

*Классификация услуг по типу передаваемой информации (контенту):* услуги телефонии (и видео-телефонии); услуги передачи данных; широковещательные услуги; услуги выделенных каналов (услуги, безразличные к типу передаваемой информации); инфраструктурные услуги (не связаны с передачей клиентом информации – сдача в аренду инфраструктуры, консультационные услуги).

*Классификация услуг по типу клиента:* услуги, оказываемые другим операторам связи (провайдерам); услуги, оказываемые корпоративным клиентам; услуги, оказываемые индивидуальным пользователям.

*Классификация услуг по способу доступа клиента:*коммутируемые телефонные каналы или ***ISDN***; каналы ***SDH*** различной пропускной способности; каналы ***Ethernet*** с различной скоростью передачи; технологии ***ADSL***; гибридные сети на основе коаксиального кабеля и оптического волокна; сети беспроводного доступа и др.

*Классификация услуг по типу обмена информацией:*предоставление доступа к ресурсам своей сети (и, возможно, через ресурсы своей сети к ресурсам других сетей); двусторонний обмен; транзит; центр обмена информацией (с центром взаиморасчетов или без него).

*Услуги, входящие в группу услуг телефонии****:*** предоставление услуг телефонной связи; оказание дополнительных услуг добавленной ценности; организация шлюзов международного доступа для российских операторов телефонии и ***IP***-телефонии и др.

*Услуги передачи данных:* услуги передачи информации по протоколу ***ATM***; услуги передачи информации по протоколу ***FR***; услуги передачи информации по протоколу ***IP*** и др.

#### Потоковое вещание

*Потоковое вещание* позволяет передавать мультимедийную информацию и одновременно обеспечивает её прием группой абонентов, территориально удалённых друг от друга. Оно применяется для передачи данных большого объема, для рассылки идентичной информации большому количеству адресатов (трансляция заседаний и конференций, консультирование групп пользователей, дистанционное обучение).

Суть потоковой передачи данных заключается в следующем. Передаваемые медиа-файлы сжимаются и разделяются на части (пакеты), а затем последовательно передаются пользователю. Размер пакетов определяется пропускной способностью участка сети или канала связи

между клиентом и сервером, передающим видеосигнал. Накопив достаточное количество пакетов в буфер, программа-клиент приступает к воспроизведению одного из них и одновременно получает и выполняет декомпрессию следующих. Основной задачей, стоящей перед буфером, является обеспечение плавного и непрерывного воспроизведения видеосигнала. На практике результаты работы таких приложений по- прежнему очень сильно зависят от быстродействия компьютера и от скорости сетевого соединения, поэтому качество звука/видео – это всегда компромисс. Размер потока (*битрейт*) напрямую влияет на качество воспроизведения, от него также во многом зависит и то, можно ли будет смотреть видео по сети. Размер потока можно узнать в свойствах файла, однако многие кодеки используют динамически меняющийся битрейт, поэтому даже указанному значению иногда не следует верить.

**Службы *Windows Media***

***Windows Media***– набор служб, работающих под управлением ***Microsoft Windows 2000 Server.*** Эти службы предназначены для передачи звуковой и видеоинформации при помощи одноадресного и группового вещания клиентам. Поставляемое содержимое может быть создано, приобретено у поставщика или передаваться с телевизионных камер и микрофонов, его называют *живым потоком* ***(live stream)***.

Ключевым решением при проектировании ***AD*** является решение о разделении информационной инфраструктуры на иерархические домены и подразделения верхнего уровня. Типичными моделями, используемыми для такого разделения, являются модели разделения по функциональным подразделениям компании, по географическому положению и по ролям в информационной инфраструктуре компании. Часто используются комбинации этих моделей.

Службы ***Windows Media*** соcтоят из *служб-компонентов* и *административной утилиты –Администратор* ***Windows Media (Windows Media Administrator)***. *Администратор* ***Windows Media***– набор веб-страниц, который функционирует в окне браузера ***Microsoft Internet Explorer*** версии

5.0 и управляет *службами-компонентами* ***Windows Media***. При помощи администратора ***Windows Media*** можно управлять локальным сервером или одним или несколькими удаленными серверами. Чтобы управлять несколькими серверами, нужно добавить серверы в список серверов, а затем соединиться с сервером, которым необходимо управлять.

Службы***Windows Media*** предоставляют возможность доставки

мультимедийной информации большому количеству клиентов, использующих форматы**.*ASF, .WMA и .WAV***. Клиенты могут проигрывать такие файлы, не загружая их целиком, поскольку они принимаются по сети в виде потоковых данных. Потоковая передача данных существенно уменьшает время загрузки и требования к памяти на клиентской стороне. Она также позволяет транслировать данные неограниченной длины, например, предоставляет возможность живых трансляций.

#### IP-телефония

*Интернет-телефония*– это технология передачи телефонных речевых сообщений по сети Интернет. Работа устройств в сети Интернет осуществляется с использованием специального Интернет-протокола ***IP*** *(****I****nternet* ***P****rotocol )*. В настоящее время протокол ***IP*** используется не только в сети Интернет, но и в других сетях передачи данных с пакетной коммутацией. И во всех этих сетях, в принципе, имеется возможность передавать речевые сообщения с использованием пакетов данных. Такой способ передачи речи и получил название ***IP****-телефония (*более узкий термин *Интернет-телефония)*. За рубежом обычно употребляется аббревиатура ***VoIP– V****oice* ***o****ver* ***IP***.

Процесс передачи голоса по ***IP***-сети состоит из нескольких этапов.

На *первом* осуществляется оцифровка голоса. Затем оцифрованные данные анализируются и обрабатываются для уменьшения физического объема данных, передаваемых получателю. На этом этапе происходит подавление ненужных пауз, фонового шума, компрессирование.

На *втором* этапе полученная последовательность данных разбивается на пакеты и к ней добавляется протокольная информация – адрес получателя, порядковый номер пакета на случай, если они будут доставлены не последовательно, и дополнительные данные для коррекции ошибок. При этом происходит временное накопление необходимого количества данных для образования пакета до его непосредственной отправки в сеть.

Извлечение переданной голосовой информации из полученных пакетов также происходит в несколько этапов. Когда голосовые пакеты приходят на терминал получателя, то сначала проверяется их порядковая последовательность. Поскольку ***IP***-сети *не гарантируют* время доставки, то пакеты со старшими порядковыми номерами могут прийти раньше, более того, интервал времени получения также может колебаться. Для восстановления исходной последовательности и синхронизации

происходит временное накопление пакетов. Однако некоторые пакеты могут быть вообще потеряны при доставке, либо задержка их доставки превышает допустимый разброс.

В обычных условиях приемный терминал запрашивает повторную передачу потерянных данных. Но передача голоса слишком критична ко времени доставки, поэтому в этом случае либо включается алгоритм аппроксимации, позволяющий на основе полученных пакетов приблизительно восстановить потерянные, либо эти потери просто игнорируются, а пропуски заполняются данными случайным образом.Полученная таким образом (не восстановленная!) последовательность данных декомпрессируется и преобразуется непосредственно в аудио-сигнал, несущий голосовую информацию получателю.

Таким образом, с большой степенью вероятности, полученная информация не соответствует исходной (искажена) и задержана (обработка на передающей и приемной сторонах требует промежуточного накопления). Однако в некоторых пределах избыточность голосовой информации позволяет мириться с такими потерями.

В настоящее время в ***IP***-телефонии существует два основных способа передачи голосовых пакетов по ***IP****-*сетям:

* *через глобальную сеть Интернет (Интернет-телефония)*, в которой полоса пропускания напрямую зависит от загруженности сети Интернет пакетами, содержащими данные, голос, графику и т.п.;
* *сети передачи данных на базе выделенных каналов(IP-телефония)*, которые гарантируют фиксированную (или почти) скорость передачи. Для того чтобы осуществить междугородную (международную)

связь с помощью телефонных серверов, организация или оператор услуги должны иметь по серверу в тех местах, куда и откуда планируются звонки. Стоимость такой связи на порядок меньше стоимости телефонного звонка по обычным телефонным линиям. Особенно велика эта разница для международных переговоров.

При предоставлении услуг в рамках сети ***IP***-телефонии участвует большое количество субъектов, выполняющих различные организационно- технические функции. В рекомендациях ***TIPHON***, разработанных ***ETSI*** *(The* ***E****uropean* ***T****elecommunications* ***S****tandards* ***I****nstitute****–***Европейский институт стандартизации по телекоммуникациям), определена следующая классификация для субъектов ***IP-***телефонии:

* + *конечный пользователь****IP (IPEU)*** – пользователь, соединенный с

***IP***-сетью;

* + *провайдердоступа****IP (IPАР)***– компания или организация, предоставляющая доступ к ***IP***-услугам, который может быть или доступом к частой ***IP***-сети, или к сети Интернет;
  + *провайдер****IP***-*сети* (***IPNP***) – компания или организация, который принадлежит ***IP***-сеть;
  + *провайдеруслугИнтернет*-*телефонии* (***ITSP***) – компания или организация, которая предлагает услуги телефонии через сеть Интернет;
  + *провайдервзаимодействия* (***IСP***) – компания или организация, которая предлагает услуги по взаимодействию между IP-сетями и сетями с коммутацией каналов для телефонного соединения;
  + *провайдеруслугсети с коммутацией каналов* (***SCNP***) – компания или организация, которой принадлежит сеть с коммутацией каналов;
  + *провайдер доступа к сети с коммутацией каналов* (***SCАP***) – компания или организация, которая предоставляет доступ к сети с коммутацией каналов;
  + *конечныйпользователь сети с коммутацией каналов* (***SCЕU***) – пользователь, соединенный с сетью коммутации каналов;
  + *провайдеринформационныхуслуг* (***DSP***–***D****irectory* ***S****ervice* ***P****rovider*)

– провайдер справочной информации;

* + *провайдердополнительныхуслуг* (***VASP***) – провайдер, который предоставляет дополнительные услуги помимо телефонии;
  + *брокер*– провайдер делового обслуживания, обеспечивающий возможность обмена между провайдерами ***IP*** услуг и операторами сетей с коммутацией каналов, включая урегулирование расчетов.

#### Видеоконференция

*Видеоконференция*–вид телекоммуникаций между двумя и более абонентами, который позволяет им видеть и слышать друг друга независимо от расстояния. Для организации видеоконференций используется технология –*видеоконференцсвязь*. Общение в режиме видеоконференций также называют сеансом видеоконференцсвязи.

*Видеоконференцсвязь (ВКС)*– телекоммуникационная технология,

обеспечивающая организацию видеоконференций между двумя и более абонентами по сети передачи данных. Во время Сеанса ВКС обеспечивается интерактивный обмен звуком и изображением. Также абоненты могут транслировать телеметрические данные, компьютерные данные, демонстрировать документы и объекты с использованием дополнительных видеокамер. Передача потока звука и видео по сети передачи данных обеспечивается путем кодирования/декодирования данных с использованием стандартизованных аудио- и видео-кодеков.

Основные области применения систем видеоконференцсвязи, это, как правило:

* + поддержка принятия оперативных решений;
  + сопровождение проектов на удаленных объектах;
  + пресс-конференции;
  + повышение квалификации специалистов;
  + дистанционное обучение.

Наибольший интерес в области образования представляет дистанционное обучение. Сочетание web-технологий и систем видеоконференций позволяет проводить лекции и семинары из одной аудитории для нескольких вузов одновременно. Тем самым значительно экономится время преподавателей, которым больше нет необходимости совершать утомительные перелеты; достигается синхронизация образовательного процесса в региональных отделениях центральных вузов, экономятся средства частных учебных учреждений на оплату приглашенных преподавателей и др.

При использовании дистанционных технологий для проведения семинаров и практических занятий, с одной стороны, слушатели получают наглядную информацию к материалам, сопровождающим занятие, а с другой – преподаватель имеет возможность удаленнооценить эффективность занятия, ответить на вопрос конкретного слушателя.

# Модуль 1.

# Проектирование и администрирование

**Цель:**познакомиться с основными принципами администрирования компьютерных сетей.

**Результат:** уметь: проектировать локальную вычислительную сеть организации(строить информационную модель и архитектурную схему сети организации); устанавливать серверную ОС; создавать домен (устанавливать компоненту ***Active Directory***; организовывать домен и просматривать его структуру (***Active Directory Manager***); присоединять созданный сервер и компьютеры к домену; настраивать сервер ***DNS****)*.

#### План освоения модуля:

1. Изучите следующие темы в указанных источниках:
   * *Основные этапы проектирования компьютерных сетей: определение исходных данных, выбор размера и структуры сети, оборудования, сетевых программных средств, расчет примерной стоимости оборудования.*
   * *Функции, процедуры и службы администрирования. Задачи администратора учебной компьютерной сети. Требования, предъявляемые к компьютерным сетям.*
   * *Службакаталогов Active Directory (AD).*
   * *Система доменных имен (Domain Name System, DNS).*
2. Выполните и представьте преподавателю лабораторные работы:
   * ЛР 1.1. *Основы проектирования ЛВС.*
   * ЛР 1.2. *Установка серверной операционной системы.*
   * ЛР 1.3. *Установка и настройка сервера DNS.*
   * ЛР1.4. *Работас Active Directory.* **III.**Выполните самостоятельные задания к модулю. **IV.**Выполните тестовые задания к модулю. **V.**Защитите модуль по контрольным вопросам. **Литература:**
3. Новиков Ю.В. Основы локальных сетей: курс лекций: учеб. пособие : для студентов вузов, обучающихся по специальностям в обл. информ. Технологий / Ю.В.Новиков [и др.]– М.: Интернет – Ун-т Информ. Технологий, 2005. – 360 с. – (Серия «Основы информационных технологий» / Интернет Ун-т информ. технологий). (Гл. 11).
4. Таненбаум Э. Компьютерные сети. 4-е изд. / Э.Таненбаум – Спб.: Питер, 2003. – 992 с.: ил. – (Серия «Классика computer science»). (Гл.1)
5. Холме Дэн. Управление и поддержка Microsoft Windows Server 2003. MCSA/MCSE / Пер. с англ. – М.: Издательско-торговый дом "Русская редакция", 2004. – 448 стр.: ил. (Гл. 1–3).
6. Ханикат Дж. Знакомство с Microsoft Windows Server 2003 / Пер. с англ. / Дж Ханикат– М.: ИЗдательско-торговый дом "Русская редакция", 2003. – 464 с.: ил. (Гл. 3–4).
7. АндреевА.Г.Microsoft Windows XP. Руководство администратора / А.Г.Андреев [и др.] под ред. А.Н.Чекмарева. – СПб.: БХВ–Петербург, 2006. – 848 с.: ил. (Гл. 1).

## Лабораторная работа 1.1.

## Основы проектирования ЛВС

**Цель:** научиться проектировать компьютерную сеть.

#### Средства для выполнения работы:

* + **аппаратные:** компьютер с установленной ОС ***Windows XP***;
  + **программные:*OpenOffice.org***;
  + **информационные:** доступ к сети Интернет.

***Теоретические сведения***

Процесс построения (проектирования) сети представляет собой упрощенное моделирование не наступившей действительности и включает в себя следующие основные этапы:

 *Анализ задач*, для решения которых создается сеть, а также определение объема финансирования проекта.

 *Проектирование физической структуры*– этап, на котором *анализируются* начальные условия (планировка здания, имеющиеся технические средства и т.п.) и создается детальный проект физической организации сети.

 *Проектирование инфраструктуры*– этап, на котором определяются *протоколы* взаимодействия, используемые службы, политика безопасности и т.п. – т.е. логическая организация сети.

 *Развертывание*– этап, связанный с прокладкой линий связи, *установкой*

и настройкой оборудования.

*Этап анализа* является одним из важнейших, поскольку определяет все остальные решаемые задачи: как физическую структуру сети

(например, места расположения компьютеров), так и логическую (используемые протоколы, службы и т.п.). Именно на данном этапе выступает основное различие компьютерных сетей. Основной целью использования учебных компьютерных сетей в образовательных заведениях выступает организационно-методическая поддержка учебно- воспитательного процесса средствами современных сетевых технологий.

На *этапе проектирования* решаются следующие задачи:

1. На основе определенных целевых требований к сети определяется необходимый состав оборудования и, прежде всего, компьютеров: количество, характеристики и т.д.
2. Определяется физическое расположение рабочих мест, и определяются этажи и аудитории, которые будут охватываться сетью. При решении этой задачи должна учитываться принципиальная возможность прокладки линий связи к рабочим местам/помещениям.
3. Исходя из решаемых задач, стоимости и расположения, определяется тип физических линий связи, соединяющих рабочие места, состав и расположение коммуникационного оборудования (концентраторов).
4. Определяется способ подключения к Интернету: выбирается провайдер – организация, обеспечивающая подключение организации к сети Интернет. При выборе провайдера учитываются факторы: характеристики возможных физических соединений с провайдером, требования к оборудованию и необходимое дополнительное оборудование, начальная стоимость подключения, стоимость эксплуатации подключения, технологические ограничения подключения (невозможность использования некоторых служб).
5. Исходя из технических требований, определяется узел проектируемой сети, который будет являться шлюзом для подключения к Интернету и определяется место его расположения. При этом учитывается удобство физического соединения шлюза с проектируемой сетью и удобство подведения физических линий для подключения к Интернету.

Приведем *общий алгоритм, описывающий процесс построения сети:*

1. *Определение исходных данных:*
   * цели использования сети;
   * требования к сети;
   * характеристики используемого оборудования (компьютеры, сетевое оборудование, принтеры, модемы и др.);
   * характеристика сетевого ПО (серверное, ОС, антивирусное);
   * примерная схема здания, в котором планируется строить сеть.
2. *Проектирование сети:*
   * способ сегментирования и объединения сегментов (определение необходимых сегментов оборудования для их формирования);
   * тип кабеля (обычно выбирается неэкранированная витая пара);
   * активные устройства (модемы, маршрутизаторы и т.п.);
   * программное обеспечение (серверные и клиентские ОС, серверное ПО и т.п.);
   * разработка схемы сети (указываются узлы сети и длины соединительных кабелей);
3. *Определение стоимости:*
   * анализ основных направлений затрат;
   * составление примерной сметы затрат.
4. *Примерный план проведения работ.*
5. *Развертывание сети.*

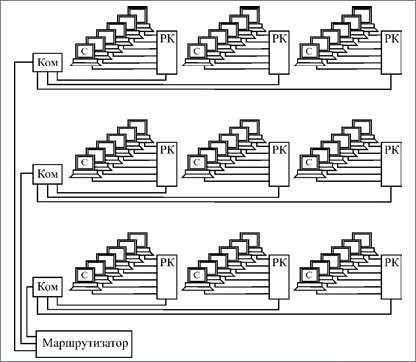
*При создании новой сети* желательно учитывать следующие факторы:

* + требуемый размер сети (в настоящее время, в ближайшем будущем и по прогнозу на перспективу);
  + структура, иерархия и основные части сети (по подразделениям предприятия, а также по комнатам, этажам и зданиям предприятия); основные направления и интенсивность информационных потоков в сети (в настоящее время, в ближайшейи дальней перспективах); характер передаваемой по сети информации;
  + технические характеристики оборудования (компьютеров, адаптеров, кабелей, репитеров, концентраторов, коммутаторов);
  + возможности прокладки кабельной системы в помещениях и между ними, а также меры обеспечения целостности кабеля;
  + обслуживание сети и контроль ее безотказности и безопасности;
  + требования к программным средствам по допустимому размеру сети, скорости, гибкости, разграничению прав доступа,

стоимости, по возможностям контроля обмена информацией и т.д. (например, если предполагается использование одного ресурса многими пользователями, то следует использовать серверную ОС);

* + необходимость подключения к другим сетям (например, глобальным);
  + имеющиеся компьютеры и их программное обеспечение, а также периферийные устройства (принтеры, сканеры и т.д.).
  + При выборе размера (под размером сети в данном случае понимается как количество объединяемых в сеть компьютеров, так и расстояния между ними) и структуры сети необходимо учитывать:
  + количество компьютеров (следует оставлять возможность для дальнейшего роста количества компьютеров в сети);
  + требуемую длину линий связи сети (например, если расстояния очень большие, может понадобиться использование дорогого оборудования);
  + способы объединения частей сети (для объединения частей сети могут использоваться репитеры, репитерные концентраторы, коммутаторы, мосты и маршрутизаторы, причем в ряде случаев стоимость этого объединительного оборудования может даже превысить стоимость компьютеров, сетевых адаптеров и кабеля;
  + возможность масштабирования (например, лучше приобретать коммутаторы или маршрутизаторы с количеством портов, несколько большим, чем требуется в настоящий момент).

**Пример.** Пусть небольшое предприятие занимает три этажа, на каждом по пять комнат, и включает в себя три подразделения, по три группы. В этом случае можно построить сеть таким образом (*рис. 1*):



**Рисунок 1. Структура сети предприятия (С - серверы рабочих групп, РК - репитерные концентраторы, Ком - коммутаторы)**

* + рабочие группы занимают по 1–3 комнаты, их компьютеры объединены между собой репитерными концентраторами. Концентратор может использоваться один на комнату, один на группу или один на весь этаж. Концентратор целесообразно расположить в помещении, в которое имеет доступ минимальное количество сотрудников;
  + подразделения занимают отдельный этаж. Все три сети рабочих групп каждого подразделения объединяются коммутатором, а для связи с сетями других подразделений используется маршрутизатор. Коммутатор вместе с одним из концентраторов лучше поместить в отдельной комнате;
  + общая сеть предприятия включает три сегмента сетей подразделений, объединенных маршрутизатором. Этот же маршрутизатор может использоваться для подключения к глобальной сети;
  + серверы рабочих групп располагаются в комнатах рабочих групп, серверы подразделений – на этажах подразделений.

При выборе сетевого оборудования надо учитывать множество факторов, в частности:

* + уровень стандартизации оборудования и его совместимость с наиболее распространенными программными средствами;
  + скорость передачи информации и возможность ее дальнейшего увеличения;
  + возможные топологии сети и их комбинации (шина, пассивная

звезда, пассивное дерево);

* + метод управления обменом в сети (***CSMA/CD***, полный дуплекс или маркерный метод);
  + разрешенные типы кабеля сети, максимальную его длину, защищенность от помех;
  + стоимость и технические характеристики конкретных аппаратных средств (сетевых адаптеров, трансиверов, репитеров, концентраторов, коммутаторов).

В настоящее время для организации локальных сетей в подавляющем большинстве случаев используется неэкранированная витая пара ***UTP***. Более дорогие варианты на основе экранированной витой пары, оптоволоконного кабеля или беспроводных соединений применяются на предприятиях, где в этом существует действительно острая необходимость. Например, оптоволокно может использоваться для связи между удаленными сегментами сети без потери скорости.

*При выборе сетевого программного обеспечения* надо, в первую очередь, учитывать следующие факторы:

* + какую сеть поддерживает сетевое ПО: одноранговую, сеть на основе сервера или оба этих типа;
  + максимальное количество пользователей (с запасом 20%);
  + количество серверов и возможные их типы;
  + совместимость с разными операционными системами и компьютерами, а также с другими сетевыми средствами;
  + уровень производительности программных средств в различных режимах работы;
  + степень надежности работы, разрешенные режимы доступа и степень защиты данных;
  + какие сетевые службы поддерживаются;
  + стоимость программного обеспечения, его эксплуатации и модернизации.

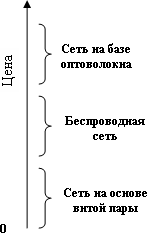
Еще до установки сети необходимо решить вопрос об управлении сетью. Даже в случае одноранговой сети лучше выделить для этого отдельного специалиста (*администратора*), который будет иметь всю информацию о конфигурации сети и распределении ресурсов, и следить за корректным использованием сети всеми пользователями. Если сеть большая, то одним сетевым администратором уже не обойтись, нужна группа, возглавляемая *системным администратором.*После установки и

запуска сети решать эти вопросы, как правило, слишком поздно.

При проектировании следует определить возможные направления финансовых затрат (к данному этапу проектирования необходимые предпосылки для решения этой задачи уже, как правило,выявляются):

* + дополнительные компьютеры и апгрейд существующих компьютеров. Необязательное направление затрат: при достаточном количестве и качестве существующих компьютеров их апгрейд не требуется (или требуется в минимальном объеме – например, для установки более современных сетевых карт); в одноранговой сети не нужен (хотя и желателен) также специальный файл-сервер;
  + сетевые аппаратные средства (кабели и все, необходимое для организации кабельной системы, сетевые принтеры, активные сетевые устройства – повторители, маршрутизаторы и т.п.);
  + сетевые программные средства, прежде всего, сетевая ОС на необходимое число рабочих станций (с запасом);
  + оплата работы приглашенных специалистов при организации кабельной системы, установке и настройке сетевой ОС, при проведении периодической профилактики и срочного ремонта. Необязательное направление затрат: для небольших сетей со многими из этих работ может и должен справляться штатный сетевой администратор (возможно, с помощью других сотрудников данного предприятия).

Примерное распределение стоимости установки сети с использованием различных сред передачи данных приведено на *рисунке 2.*



**Рисунок 2. Примерное распределение стоимости сети на базе различных сред**

**передачи данных**

### Выполнение работы

**Задание 1. Учитывая исходную информацию** (примерный план здания образовательного заведения, количество и специфику устанавливаемых ПК и где) **спроектировать учебную компьютерную сеть** (собрать исходные данные; выбрать: размер и структуру сети, оборудование, сетевые программные средства; спроектировать кабельную систему; рассчитать примерную стоимость оборудования):

* 1. Ознакомьтесь с решением поставленной задачи (*Приложение 1*).
  2. Выполните расчеты стоимости программного обеспечения в таблице

«Составление сметы примерных затрат».

* 1. Модифицируйте план проектирования сети, увеличив количество компьютеров до 36 (например, добавьте еще 1 кабинет информатики на 1-м этаже).
  2. Сохраните результат работы в личной папке.

#### Задание 2. Самостоятельно сформируйте план-проект модернизации кабинета, в котором проходят занятия, увеличив в нем количество компьютеров на 5 и добавив выделенный сервер и выход в Интернет по технологии *ADSL*.

**Задание 3. Самостоятельно спроектируйте компьютерную сеть для подъезда, в котором Вы проживаете.**

## Лабораторная работа 1.2.

## Установка серверной операционной системы

**Цель:** научиться устанавливать и выполнять первоначальную настройку серверной ОС семейства ***Windows***.

#### Средства для выполнения работы:

* **аппаратные:** компьютер с установленной ОС ***Windows XP;***
* **программные:** приложение ВМ: ***VirtualBox***; виртуальная машина:

***VM-2***; образ диска: ***win2003-1.iso, win2003-2.iso***;

* **информационные:** лицензионный ключ для ***Windows Server 2003***.

***Теоретические сведения***

*Операционная система* (ОС)–совокупность программных средств, осуществляющая управление ресурсами компьютера, запуск прикладных программ и их взаимодействие с внешними устройствами и другими программами, а также обеспечивающая диалог пользователя с ЭВМ.

*Назначение серверной операционной системы*–управление приложениями, обслуживающими всех пользователей корпоративной сети, а нередко и внешних пользователей. К таким приложениям относятся современные системы управления базами данных, средства управления сетями и анализа событий в сети, службы каталогов, средства обмена сообщениями и групповой работы, Web-серверы, почтовые серверы, корпоративные брандмауэры, серверы приложений самого разнообразного назначения, серверные части бизнес-приложений.

Требования к производительности и надежности указанных операционных систем очень высоки; нередко сюда входят и поддержка кластеров (набора ряда однотипных компьютеров, выполняющих одну и ту же задачу и делящих между собой нагрузку), и возможности дублирования и резервирования, и переконфигурации программного и аппаратного обеспечения без перезагрузки операционной системы.

Выбор серверной операционной системы и аппаратной платформы для нее в первую очередь определяется тем, какие приложения под ее управлением должны выполняться (как минимум, выбранные приложения должны существовать в версии для данной платформы) и какие требования предъявляются к ее производительности, надежности и доступности.

**Семейство*Windows***

Серверные версии ОС***Windows*(*Windows NT,Windows 2000, Windows Server 2003*)** сегодня применяются широко благодаря удобству администрирования и невысокой совокупной стоимости владения.

##### Windows NT

Самой популярной стала версия ОС***Windows NT Server 4.0***, существовавшая в варианте не только для *Intel-совместимых компьютеров*, но и для ***RISC****-систем*. Данная операционная система обладала привычным пользовательским интерфейсом ***Windows 95***, удобными средствами администрирования, встроенным Web-сервером, средствами диагностики сети, управления процессами и задачами, интеграции с другими операционными системами (например, с ***Novell NetWare***), а также утилитами и службами управления рабочими станциями.

Позже для этой операционной системы появились такие сервисы, как: монитор транзакций и сервер приложений ***Microsoft Transaction Server***; сервер управления очередями сообщений ***Microsoft Message Queue Server***; ряд коммерческих продуктов, в том числе серверные СУБД, средства групповой работы и обмена сообщениями, серверы приложений как от компании ***Microsoft***, так и от других производителей.

##### Windows 2000

На данный момент является самой популярной операционной системой ***Microsoft*** в корпоративном секторе. К серверным ОС этого семейства относятся:

* + ***Windows 2000 Server***– универсальная сетевая операционная система для серверов рабочих групп и отделов;
  + ***Windows 2000 Advanced Server***– операционная система для эксплуатации бизнес-приложений и приложений для электронной коммерции;
  + ***Windows2000 Datacenter Server***– ОС для наиболее ответственных приложений, осуществляющих обработку данных.

В состав ***Windows 2000 Server***, по сравнению с ***Windows NT 4.0***, включены и дополнительные службы, облегчающие управление серверами, сетями и рабочими станциями, например службы каталогов ***Active Directory***, позволяющие создать единое хранилище учетных записей пользователей, клиентов, серверов и приложений ***Windows***, дополнительные средства конфигурирования сетей и подключения удаленных пользователей, терминальные службы для удаленного управления компьютерами. Кроме того, в данную операционную систему были добавлены службы компонентов, являющиеся дальнейшим развитием ***Microsoft Transaction Server***, что позволило создавать для этой ОС корпоративные приложения, обладающие масштабируемостью и надежностью.

**Семейство*Windows Server 2003***

Создание семейства ***Windows Server 2003*** стало следующим шагом в развитии операционных систем ***Windows 2000***. Основными особенностями данного семейства операционных систем являются наличие в их составе платформы ***Microsoft .NET Framework*** и поддержка ***Web-сервисов XML****.*

***Windows Server 2003*** существует в четырех редакциях:

* + ***Windows Server 2003 Web Edition***– операционная система для

развертывания и обслуживания *Web-приложений* и *Web- сервисов*, включая приложения ***.ASP .NET***;

* + ***Windows Server 2003 Standard Edition***– сетевая ОС для выполнения серверной части бизнес-решений и рассчитанная на применение в небольших компаниях и подразделениях. Здесь имеются средства совместного использования ресурсов и централизованного развертывания приложений для настольных компьютеров, а также реализована поддержка до 4 Гбайт оперативной памяти и симметричной многопроцессорной обработки с использованием двух процессоров;
  + ***Windows Server 2003 Enterprise Edition***– ОС, которая, прежде всего, предназначена для средних и крупных компаний. Она поддерживает серверы на базе 64-разрядных процессоров (до восьми штук) и объем оперативной памяти до 64 Гбайт и выпускается в версиях для 32- и 64-разрядных платформ;
  + ***Windows Server 2003 Datacenter Edition***–ОС, которая служит для создания критически важных технических решений с высокими требованиями к масштабируемости и доступности. К таким решениям относятся приложения для обработки транзакций в режиме реального времени, а также решения, основанные на интеграции нескольких серверных продуктов. Здесь реализована поддержка симметричной многопроцессорной обработки с использованием до 32 процессоров, имеются службы балансировки нагрузки и создания кластеров, состоящих из восьми узлов. Она доступна для 32- и 64-разрядных платформ. Процесс установки серверной ОС семейства ***Windows*** практически ничем не отличается от установки других ОС этого семейства, кроме необходимости указания в процессе установки количества одновременных подключений.

**Семейство*UNIX***

Операционная система ***UNIX*** относится к «долгожителям» рынка серверных операционных систем – она была создана в конце 60-х годов в ***Bell Laboratories*** фирмы ***AT&T***. Отличительной особенностью этой ОС, обусловившей ее «живучесть» и популярность, было то, что ядро операционной системы, написанное на ассемблере, было невелико, тогда как вся оставшаяся часть операционной системы реализована на языке С.

Такой подход делаллегко переносимым на самые разнообразные аппаратные платформы и самуОС, и созданные для нее приложения. Важным ее достоинством стала ее открытость, позволившая одновременно существовать как коммерческим, так и некоммерческим версиям ***UNIX***.

Общими для всех версий ***UNIX*** особенностями являются: многопользовательский режим со средствами защиты данных от несанкционированного доступа; реализация мультипрограммной обработки в режиме разделения времени; использование механизмов виртуальной памяти и свопинга; унификация операций ввода-вывода; иерархическая файловая система; разнообразные средства взаимодействия процессов, в том числе межсетевого.

##### Solaris (Sun Microsystems)

|  |  |  |  |
| --- | --- | --- | --- |
| ОС***Sun*** | ***Solaris*** | сегодня | входит в число самых известных |
| коммерческих | версий | ***UNIX***. | Она обладает развитыми средствами |

поддержки сетевого взаимодействия и представляет собой одну из самых популярных платформ для разработки корпоративных решений – для нее существует около 12 тыс. различных приложений, в том числе серверов приложений и СУБД почти от всех ведущих производителей. ***Solaris*** соответствует многим промышленным стандартам и характеризуется

|  |  |  |
| --- | --- | --- |
| высокой масштабируемостью. | Для подавляющего | большинства |
| приложений эта операционная | система обеспечивает | практически |

линейный рост производительности при увеличении числа процессоров за счет симметричных многопроцессорных вычислений. В настоящее время ***Solaris*** поддерживает процессоры ***SPARC*** и ***Intel x86***. Из особенностей***Solaris 9*** следует отметить следующие: поддержка до 1 млн. одновременно работающих процессов, до 128 процессоров в одной системе и до 848 процессоров в кластере, до 576 Гбайт физической оперативной памяти; поддержку файловых систем размером до 252 Тбайт; наличие средств управления конфигурациями и изменениями; встроенную совместимость с ***Linux***. Операционная система ***Solaris 9*** представляет собой основу открытой сетевой среды ***Sun Open Net Environment (Sun ONE)***.

Вкомплектпоставки***Solaris 9***входяттакиеключевыеприложения***Sun ONE:Application Server, Directory Server, Integration Server, Message Queue, Portal Server, Web Server*.**

**Операционная система *HP-UX (Hewlett-Packard)***

Операционнаясистема***HP-UX***, разработаннаявкомпании***Hewlett- Packard***, являетсяпотомком***AT&TSystemV***. Еепоследняяверсия, ***HP-UX 11i***, доступнадлядвухаппаратныхплатформ–***PA\_RISC***и***Itanium***– иориентированаглавнымобразомнасерверыпроизводства***Hewlett-Packard***.

Из особенностей***HP-UX 11i*** нужно назвать следующие: средства интеграции с ***Windows*** и ***Linux***, в том числе средства переноса ***Java****-* приложений, разработанных для этих платформ; средства повышения производительности ***Java****-*приложений. Кроме того, ***HP-UX 11i*** поддерживает ***Linux API***, что гарантирует перенос приложений между ***HP- UX*** и ***Linux*** (без изменений и перекомпиляции).

Говоря о производительности и масштабируемости ***HP-UX 11i***, следует отметить, что одна копия ОС поддерживает до 256 процессоров; кластеры размером до 128 узлов; подключение и отключение дополнительных процессоров; замену аппаратного обеспечения; динамическую настройку и обновление операционной системы без необходимости перезагрузки; резервное копирование в режиме ***on-line***; дефрагментацию дисков без выключения системы.

Выбор программного обеспечения для данной ОС широк – это и серверы приложений ведущих производителей, и ***Web***- и ***WAP***-серверы, и поисковые серверы, и средства кэширования, и службы каталогов.

**ОС *Linux и FreeBSD***

Операционная система ***Linux***–некоммерческий продукт категории ***Open Source*** для платформы ***Intel***, который в течение десяти лет создавали тысячи энтузиастов. Список серверных продуктов для ***Linux***, пожалуй, не менее внушителен, чем для ***Solaris, HP-UX и AIX***, и включает такие популярные продукты, как ***Web-сервер Apache***, серверные СУБД и серверы приложений практически от всех производителей.

Одним из серьезных преимуществ ***Linux*** является низкая стоимость ее приобретения (хотя сама операционная система является некоммерческим продуктом, сертифицированные дистрибутивы ***Linux***– обычно продукты коммерческие). Кроме того, ряд компаний, в частности ***IBM***, вкладывают значительные средства в развитие ***Linux*** как серверной платформы, одновременно стремясь реализовать совместимость с ***Linux*** в своих коммерческих версиях ***UNIX*** в расчете на возможный переход с ***Linux*** на указанные операционные системы.

**Сетевая ОС*NetWare (Novell)***

В начале и середине 90-х годов ***Novell NetWare*** была доминирующей сетевой операционной системой. Хотя в настоящее время снизилась доля серверов, управляемых ***NetWare***, как и количество создаваемых для нее приложений и инфраструктурного программного обеспечения, эта ОС популярна благодаря надежности, масштабируемости, способности управлять большим количеством рабочих станций.

Основными особенностями последней версии данной операционной системы, ***Novell NetWare 6.5***, являются возможность создания географически распределенных кластеров, наличие средств поддержки мобильных и удаленных пользователей, инструментов управления удаленными сетевыми ресурсами, а также средств синхронизации информации о пользователях и приведения в соответствие между собой каталогов в смешанных средах. Защита данных в ***Novell NetWare 6.5*** осуществляется с помощью служб каталогов ***NDS eDirectory****.*

В состав ***Novell NetWare 6.5*** входят известные ***OpenSource****-*продукты, в частности: ***Web-сервер Apache, СУБД MySQL, сервер приложений Apache Tomcat***. Кроме того, в ***NetWare 6.5*** включены сертифицированный на соответствие спецификации ***J2EE 1.3*** сервер приложений, среда разработки ***Novell exteNd*** и виртуальный офис, позволяющий через Web- интерфейс обращаться к бизнес-ресурсам пользователя, включая файлы, электронную почту, средства календарного планирования.

**Операционная система *Mac OS X (Apple)***

Операционная система ***Mac OS X***, созданная компанией ***Apple*** совместно основана на ***BSD UNIX***. В 1999 году версия ***Mac OS X Server*** была выпущена в виде продукта ***Open Source****,* что позволило разработчикам адаптировать еедля конкретных заказчиков, а также привлечь их к дальнейшему развитию этой ОС.

***Mac OS X*** характеризуется наличием менеджера виртуальной памяти, возможностью полной изоляции приложений друг от друга, поддержкой многозадачности, сравнимой с аналогичной поддержкой в **Windows**. В ***Mac OS X*** имеются такие компоненты, как: эмулятор предыдущих версий ***Mac OS***; средства редактирования графических изображений; встроенная поддержка **OpenGL**; почтовый клиент; средства

управления паролями для доступа к Web-ресурсам.

В целом ***Mac OS X*** представляется многообещающей серверной операционной системой, и для нее уже начали выпускаться серверные СУБД и иное инфраструктурное программное обеспечение, хотя корпоративные пользователи пока относятся к ней достаточно осторожно.

### Выполнение работы

**Задание 1. Установите *Windows 2003 Server:***

* 1. Запустите приложение ВМ ***VirtualBox*** и подключите к созданной ранее виртуальной машине ***VM-2*** образ установочного диска ***Windows 2003 Server***.
  2. Запустите ВМ и начните установку ОС.
  3. Ознакомьтесь с информацией программы установки и нажмите

##### Enter.

* 1. Ознакомьтесь с лицензионным соглашением и согласитесь с ним (клавишa ***F8***).
  2. Создайте раздел для ОС на всем жестком диске клавишей ***Enter***.
  3. Выполните форматирование созданного раздела в файловой системе

***NTFS***– нажмите ***Enter***.

*Дождитесь окончания форматирования раздела, и копирования файлов установки на него. В процессе копирования компьютер перезагрузится и продолжит установку автоматически.*

* 1. Самостоятельно укажите параметры языка и раскладки клавиатуры и перейдите к следующему шагу кнопкой ***Далее***.
  2. Укажите регистрационные данные:
     + ведите в поле ***Имя***–*USER*
     + ведите в поле ***Организация***–*MSPU*
     + завершите ввод кнопкой ***Далее***.
  3. Введите в поле ***Ключ продукта*** лицензионный ключ и щелкните

##### Далее.

* 1. Укажите вариант лицензирования, при котором для каждого подключения требуется отдельная лицензия:
     + установите радиокнопку *На сервере*;
     + введите в текстовое поле количество одновременных подключений, например *10*;
     + подтвердите параметры кнопкой ***Далее***.
  2. Укажите имя компьютера и пароль администратора:
     + введите в поле ***Имя компьютера***–*WIN2003*;
     + введите в поле ***Пароль администратора***–*123456*;
     + введите в поле ***Подтверждение***–*123456*;
     + подтвердите сделанные изменения кнопкой ***Далее***. *Появится диалоговое окно сообщающее о том что пароль слишком простой.*
     + ознакомьтесь с информацией о том что вы указали простой пароль и продолжите установку кнопкой ***Да***.
  3. Укажите *дату и время* и щелкните ***Далее***.
  4. Установите сетевые параметры для использования статического IP- адреса:
     + выберите радиокнопку *Обычные параметры* и щелкните ***Далее***;
  5. Укажите сетевую группу, например *Workgroup* и щелкните ***Далее***.
  6. Дождитесь окончания выполнения установки ОС. *По окончании установки компьютер перезагрузится. После этого загрузится операционная система* ***Windows 2003 Server****.*

**Задание 2. Выполните первоначальную настройку ОС:**

* 1. Выполните вход в систему на сервере:
     + вызовите в ВМ событие *нажатие комбинации клавиш* ***CTRL+ALT***

***+DEL***, для этого нажмите ***RCTRL+DEL***;

* + - введите ***пароль администратора***–*123456*;
    - подтвердите введенные данные кнопкой ***ОК***.
  1. Установите дополнительные компоненты со 2-го диска:
     + откройте менеджер виртуальных дисков (***команда меню ВМ Устройства/Подключить CD/DVD-ROM/Образ CD/DVD-ROM***);
     + добавьте образ:
       - откройте окно добавления кнопкой ***Добавить***;
       - перейдите в каталог с образами ОС и выберите файл

##### win2003-2.iso;

* + - подтвердите выбор образа ***Выбрать***;
    - ознакомьтесь с информацией мастера установки и щелкните ***Далее***;
    - ознакомьтесь с лицензионным соглашением и примите его (***Далее***).
    - активизируйте копирование файлов кнопкой ***Далее***;
    - завершите работу мастера установки кнопкой ***Готово***.
  1. Ознакомьтесь с информацией диалогового окна ***Послеустановочные обновления безопасности Windows Server*** (***Готово***). *После нажатия кнопки* ***Готово*** *появится окно, предупреждающее о*

*том, что после этого будет разрешено подключение по сети к вашему серверу.*

* 1. Подтвердите закрытие диалогового окна кнопкой ***Да***.
  2. Ознакомьтесь с информацией в окне ***Управление данным сервером*** и закройте его.
  3. Выполните настройку сетевого интерфейса:

##### откройте диалоговое окно Состояние подключения по локальной сети (Пуск/Панель управления/Сетевые подключения/Подключение по локальной сети);

* + - откройте диалоговое окно свойств подключения по локальной сети кнопкой ***Свойства***;
    - откройте диалоговое окно ***Параметры протокола Интернет TCP/IP*** двойным щелчком;
    - включите использования статического адреса соответствующей радиокнопкой и укажите следующие данные:

 ***IP-адрес***–*192.168.1.2*;

 ***Маска подсети***–*255.255.0.0*;

 ***Основной шлюз***–*192.168.1.1*;

* + - * завершите ввод параметров кнопкой ***ОК***;
    - закройте диалоговое окно свойств подключения по локальной сети кнопкой ***ОК***;
    - закройте диалоговое окно **Состояние подключения по локальной сети** кнопкой ***Закрыть***.
  1. Установите дополнения гостевой ОС:
     + запустите ***Мастер дополнений гостевой ОС***

##### (Устройства/Установить дополнение гостевой ОС);

* + - ознакомьтесь с информацией мастера и щелкните ***Next***;
    - ознакомьтесь с лицензионным соглашением и согласитесь с ним (***I accept the terms in License Agreement/Next***)
    - подтвердите путь установки дополнений по умолчанию кнопкой

##### Install;

* + - подтвердите установку графического адаптера ***VirtualBox Graphic Adapter*** кнопкой ***Продолжить***;
    - разрешите ОС доверять устанавливаемому драйверу графического адаптера кнопкой ***ДА***;
    - завершите установку дополнений кнопкой ***Finish***.

*После этого компьютер перезагрузится.*

* 1. Установите самостоятельно в ВМ более высокое разрешение экрана, например ***1024х768***.
  2. Остановите виртуальную машину.

## Лабораторная работа 1.3.

## Установка и настройка сервера *DNS*

**Цель:** научиться устанавливать сервер имён, добавлять зоны расширения имён, включать автоматическое обновление зон.

#### Средства для выполнения работы:

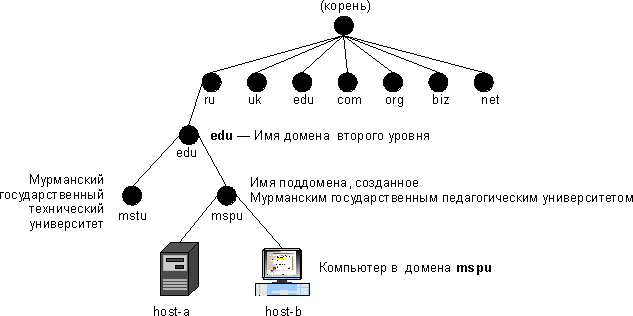
* **аппаратные**: компьютер с установленной ОС ***Windows XP***;
* **программные**: приложение ВМ: ***VirtualBox***; виртуальные машины:

***VM-1, VM-2***; установочные образы ОС: ***win98.iso.***

***Теоретические сведения***

*Система доменных имен (****DNS****)* была исходно определена в документах ***RFC* (*R****equest****F****or* ***C****omments***) *1034 и 1035***. Эти документы определяют следующие элементы, общие для всех реализаций программного обеспечения ***DNS***:

* + пространство доменных имен ***DNS***, которое задает структурированную иерархию доменов, используемую для организации имен;
  + записи ресурсов, сопоставляющие доменные имена ***DNS*** определенным типам информации о ресурсах, которые используются при регистрации и разрешении имен в пространстве имен;
  + ***DNS***-серверы, которые сохраняют записи ресурсов и отвечают на запросы клиентов;
  + ***DNS***-клиенты, которые также называют системами разрешения имен, запрашивающие серверы для поиска и разрешения имен по типам записей ресурсов, указанным в запросе.



**Рисунок 3. Пространство доменных имен**

Пространство доменных имен ***DNS***, как показано на *рисунке 3*, базируется на концепции дерева именованных доменов. Каждый уровень дерева может представлять ветвь или лист дерева. Ветвь представляет уровень, на котором используется несколько имен, определяющих семейство именованных ресурсов. Лист представляет единственное имя, которое используется на этом уровне для указания конкретного ресурса.

В процессе разрешения имен существенно, что ***DNS***-серверы часто действуют как ***DNS***-клиенты, запрашивая другие серверы с целью полного разрешения имени в запросе. Любое доменное имя ***DNS*** в дереве технически представляет домен. Однако принято считать, что имена идентифицируются одним из пяти способов на основании уровня и способа использования имени (*Табл.1*).

**Таблица 1. Способы идентификации имен доменов**

|  |  |  |
| --- | --- | --- |
| **Тип**  **имени** | **Описание** | **Пример** |
| Корень доменов | Вершина дерева, представляющая неименованный уровень, иногда обозначается парой прямых кавычек (""), указывающих пустое значение. При использовании в доменном имени ***DNS***  для этого применяется завершающая | Единственная точка (.) или точка, использованная в конце имени, например, ***example.microsoft.com*** |

|  |  |  |
| --- | --- | --- |
|  | точка (.), свидетельствующая, что имя расположено в корне или на самом верхнем уровне иерархии доменов. В данном случае доменное имя ***DNS*** рассматривается как полное и указывает на точное расположение в дереве имен. Имена, установленные таким способом, называют полными доменными именами  (***Fully Qualified Domain Name, FQDN***). |  |
| Домен верхнего уровня | Имя из двух или трех букв, которое используется, чтобы указать страну/регион или тип организации. | **.*ru*** указывает имя, зарегистрированное для коммерческого  использования в Интернете. |
| Домен второго уровня | Имена переменной длины, зарегистрированные для индивидуальных пользователей или организаций для использования в Интернете. Эти имена всегда базируются на соответствующем домене верхнего уровня в зависимости от типа организации или географического расположения, в котором используется  имя. | ***edu.ru*** является именем домена второго уровня, зарегистрированным для образовательных учреждений регистратором доменных имен ***DNS*** Интернета. |
| Поддомен | Дополнительные имена, которые организация может создавать как производные от зарегистрированного имени домена второго уровня. Такие имена обеспечивают рост дерева имен ***DNS*** в организации и его распределение по отделам или по географическому  расположению. | ***mspu.edu.ru*** представляет имя поддомена Мурманского государственного педагогического университета. |
| Имя узла или ресурса | Имя, представляющее лист в дереве имен ***DNS***, которое определяет конкретный ресурс. Обычно крайняя левая метка в доменном имени ***DNS*** определяет конкретный компьютер в сети. Например, имя этого уровня, используемое в записи ресурса узла (A), используется для поиска ***IP-***адреса  компьютера по его имени узла. | ***host-a.mspu.edu.ru***- первая метка (***host-a***) представляет имя узла ***DNS*** для конкретного компьютера в сети. |

Например, доменное имя ***DNS***, зарегистрированное для образовательных учреждений (***edu.ru***), представляет домен второго уровня. Это имя состоит из двух частей (называемых метками), показывающих, что

оно находится на втором уровне сверху от корня или вершины дерева. Большинство доменных имен ***DNS*** содержат две или большее число меток, каждая из которых задает новый уровень в дереве. Точки используются в именах для разделения меток.

***DNS*** представляет способ интерпретации полного пути к доменному имени ***DNS*** аналогично интерпретации полного пути к файлу или каталогу в окне командной строки. Например, путь в дереве каталогов помогает указать на точное расположение файла, сохраненного на компьютере. Для компьютеров с операционной системой ***Windows*** обратная косая черта (**\**) указывает каждый новый каталог, ведущий к точному расположению файла. Эквивалентным символом в ***DNS*** является точка (**.**), указывающая каждый новый уровень домена в имени.

Для ***DNS*** примером имени с несколькими уровнями может служить следующее полное доменное имя узла: ***host-a.mspu.edu.ru***

В отличие от имен файлов, при чтении полного доменного имени узла ***DNS*** слева направо осуществляется переход от наиболее конкретной информации (имя ***DNS*** компьютера ***host-a***) к наиболее общей (завершающая точка (**.**), которая указывает корень в дереве имен ***DNS***). Этот пример демонстрирует четыре уровня доменов ***DNS***, которые ведут от конкретного расположения ***host-a***:

* + домен ***mspu***, в котором зарегистрировано для использования имя компьютера ***host-a***;
  + домен ***edu***, который соответствует родительскому домену, являющемуся корнем поддомена ***mspu***;
  + домен ***ru***, который соответствует домену верхнего уровня, предназначенному для использования организациями из России, который является корнем для домена ***edu***;
  + завершающая точка (**.**), представляющая стандартный символ разделителя, которая используется, чтобы сделать полным доменное имя ***DNS*** в дереве пространства имен ***DNS***.

#### Работа запросов *DNS*

Когда ***DNS***-клиенту требуется найти имя, используемое в программе, он запрашивает ***DNS***-серверы для сопоставления имени. Каждое сообщение с запросом, отправляемое клиентом, содержит информацию трех типов, определяющую вопрос, на который отвечает сервер:

* + указанное доменное имя ***DNS*** в виде полного доменного имени узла (***FQDN***);
  + указанный тип запроса, в котором задается либо тип записей ресурсов, либо тип операции запроса;
  + указанный класс доменного имени ***DNS***.

Для ***DNS***-серверов ***Windows*** этот класс всегда должен быть указан как класс Интернета (***IN***).Например, указанное имя может представлять полное доменное имя узла для компьютера, такое как ***host-a.mspu.edu.ru*** и тип запроса на поиск записей ресурсов адреса (A) для этого имени. Запрос ***DNS*** можно представить как вопрос клиента, состоящий из двух частей, например:*«Имеются ли записи ресурсов A для компьютера с именем hostname.mspu.edu.ru?»*Когда клиент получает ответ от сервера, он читает и интерпретирует содержащуюся в ответе запись ресурса A, узнавая ***IP***-адрес компьютера, запрошенного по имени.

Запросы ***DNS*** используют несколько способов сопоставления имен. Клиент может иногда ответить на запрос с помощью локальной кэшированной информации, полученной в предыдущем запросе. ***DNS***- сервер может использовать собственный кэш информации о записях ресурсов для ответа на запрос. ***DNS*-**сервер может также запросить или обратиться к другим ***DNS***-серверам в интересах запрашивающего клиента для полного сопоставления имени, а затем отправить ответ клиенту. Этот процесс называют *рекурсией*.

В дополнение к этому, клиент может самостоятельно пытаться установить контакт с дополнительными ***DNS***-серверами для сопоставления имени. При этом клиент использует отдельные дополнительные запросы, базирующиеся на ссылочных ответах от серверов. Этот процесс называют *итерацией*. Процесс запроса ***DNS*** выполняется в две стадии:

1. Запрос к имени начинается на клиентском компьютере и передается в систему сопоставления имен службы ***DNS***-клиент;
2. Когда не удается ответить на запрос на локальном уровне, можно для сопоставления имени запрашивать ***DNS***-серверы по мере необходимости.

Обе стадии процесса подробнее рассматриваются далее.

#### Локальная система разрешения имен

На начальных этапах процесса в программе на локальном компьютере используется доменное имя ***DNS***. Затем запрос передается в

службу ***DNS***-клиент для сопоставления с помощью локальной кэшированной информации. Если удается разрешить запрошенное имя, поступает ответ на запрос и процесс завершается. Кэш локального сопоставления имен может включать информацию об именах из двух возможных источников:

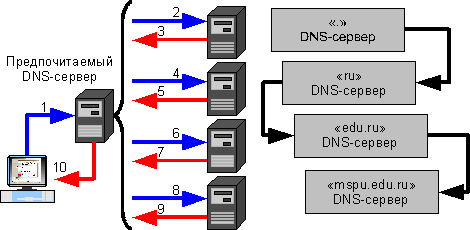
* + если имеется локальный файл ***Hosts***, все сопоставления имен и адресов из этого файла предварительно загружаются в кэш при запуске службы ***DNS***-клиент;
  + записи ресурсов, полученные в ответах на запросы из предыдущих запросов ***DNS***, добавляются в кэш и сохраняются в нем в течение определенного периода времени.

Если клиент не находит сопоставления в кэше, процесс продолжается с помощью запроса на разрешение имени от клиента к ***DNS***- серверу.

#### Запрос к *DNS*-серверу

Клиент запрашивает основной ***DNS***-сервер. Из глобального списка выбирается сервер, используемый на начальной стадии запроса от клиента к серверу. Когда ***DNS***-сервер принимает запрос, он сначала проверяет, можно ли дать удостоверяющий ответ на базе записей ресурсов, содержащихся в локальной зоне в конфигурации сервера. Если запрошенное имя соответствует информации в записи ресурса в локальной зоне, сервер дает удостоверяющий ответ, используя эту информацию для разрешения имени. Если в зоне нет информации для запрошенного имени, сервер проверяет, можно ли разрешить имя, используя информацию предыдущих запросов в локальном кэше. Если здесь обнаруживается совпадение, сервер отвечает с использованием этой информации. И в этом случае, если основной сервер может дать запрашивающему клиенту утвердительный ответ на сопоставление из собственного кэша, запрос завершается. Если на основном сервере не удается найти запрошенное имя

– ни в кэше, ни в зонах – процесс выполнения запроса может продолжаться с использованием рекурсии для полного разрешения имени. При этом другие ***DNS***-серверы помогают разрешить имя. Служба ***DNS***-клиент по умолчанию указывает серверу использовать процесс рекурсии для полного разрешения имен в интересах клиентов перед возвращением ответа. В большинстве случаев ***DNS***-серверы по умолчанию настраиваются на поддержку процесса рекурсии, как показано на *рисунке 4*.



**Рисунок 4. Процесс рекурсии при разрешении имени**

Для правильного выполнения рекурсии ***DNS***-сервером ему необходимы сведения о контактах с другими ***DNS***-серверами в пространстве доменных имен ***DNS***. Такая информация обеспечивается в виде корневых ссылок, списка предварительных записей ресурсов, которые могут использоваться службой ***DNS*** для обнаружения других ***DNS***- серверов, которые являются удостоверяющими для корня дерева пространства доменных имен ***DNS***. Корневые серверы являются удостоверяющими для корня доменов и доменов верхнего уровня в дереве пространства доменных имен ***DNS***.

Процесс заканчивается возвращением клиенту утвердительного ответа. Однако запросы могут возвращать и другие ответы, в частности: удостоверяющий, ссылочный и отрицательный.

*Утвердительный ответ* может содержать запрошенную запись ресурса или список записей ресурсов (который также называют набором записей), соответствующих запрошенному доменному имени ***DNS*** и типу записи, указанному в сообщении запроса.

*Удостоверяющий ответ* представляет утвердительный ответ, возвращенный клиенту и доставленный с установленным битом полномочий в сообщении ***DNS***, указывающим, что ответ получен от сервера, имеющего прямые полномочия для запрашиваемого имени.

*Ссылочный ответ* содержит дополнительные записи ресурсов, не указанные по имени или типу в запросе. Ответ этого типа возвращается клиенту, если процесс рекурсии не поддерживается. Эти записи должны рассматриваться как справочные, которые могут использоваться клиентом

для продолжения запроса с помощью итераций. Если клиент способен использовать итерации, он может выполнить дополнительные запросы в попытке полностью разрешить имя самостоятельно.

*Отрицательный ответ* от сервера может указывать на один из двух возможных результатов попытки сервера обработать и рекурсивно полностью и удостоверяющим образом сопоставить имя в запросе:

* удостоверяющий сервер ответил, что запрошенное имя не существует в пространстве имен ***DNS***;
* удостоверяющий сервер ответил, что запрошенное имя существует, но для этого имени отсутствуют записи указанного типа.

Система сопоставления имен передает результаты запроса в виде утвердительного или отрицательного ответа в запрашивающую программу и кэширует ответ. Итерации представляют тип сопоставления имен, используемый ***DNS***-клиентами и серверами при выполнении следующих условий:

* клиент запрашивает использование рекурсии, но рекурсия отключена на ***DNS***-сервере.
* клиент не запрашивает использование рекурсии при запросе к

***DNS***-серверу.

Итерационный запрос от клиента сообщает ***DNS***-серверу, что клиент ожидает от ***DNS***-сервера наиболее точный ответ немедленно без обращения к другим ***DNS***-серверам. Когда используются итерации, ***DNS***- сервер отвечает клиенту о запрошенных именах на основании собственной информации о пространстве имен. Например, если ***DNS***-сервер в интрасети получает запрос от локального клиента для имени [***www.edu.ru***,](http://www.edu.ru/) он может возвратить ответ из кэша имен. Если в данный момент запрошенное имя не сохраняется в кэше сервера, то сервер может ответить предоставлением ссылки – т.е. списка записей ресурсов других ***DNS***- серверов, которые ближе к имени, запрошенному клиентом. Когда предоставляется ссылка, ***DNS***-клиент принимает на себя ответственность за продолжение итерационных запросов на сопоставление имени к другим указанным в конфигурации ***DNS***-серверам.

Например, в наиболее общем случае ***DNS***-клиент может расширить область поиска до серверов корневого домена в Интернете в попытках обнаружить удостоверяющие ***DNS***-серверы для домена ***ru***. После установления контакта с корневыми серверами Интернета клиент может

получить от них дальнейшие итерационные ответы, указывающие на фактические ***DNS***-серверы Интернета для домена ***edu.ru***. Когда клиенту предоставляются записи для этих ***DNS***-серверов, он может отправить дальнейший итерационный запрос внешним ***DNS***-серверам ***edu*** в Интернете, которые могут дать определенный и удостоверяющий ответ. При использовании итераций ***DNS***-сервер может также содействовать в запросе на сопоставление имени, предоставив клиенту собственный наиболее точный ответ. Для большинства итерационных запросов клиент использует локальный список ***DNS***-серверов для обращения к другим серверам имен в пространстве имен ***DNS***, если его собственный основной ***DNS***-сервер не может сопоставить имя в запросе.

По мере того как ***DNS***-серверы обрабатывают запросы клиентов с помощью рекурсии или итераций, они находят и накапливают значительный объем информации о пространстве имен ***DNS***. Эта информация *кэшируется* сервером. Кэширование дает возможность ускорить сопоставление часто используемых имен ***DNS*** в последующих запросах и существенно снижает трафик запросов ***DNS*** в сети.

При выполнении рекурсивных запросов ***DNS***-серверами для клиентов они временно кэшируют записи ресурсов. Кэшированные записи ресурсов содержат информацию, полученную от ***DNS***-серверов, которые являются удостоверяющими для доменных имен ***DNS***. Эта информация накапливается при выполнении итерационных запросов в процессе поиска и полного ответа на рекурсивный запрос, выполняемый в интересах клиента. Когда затем другие клиенты размещают новые запросы на информацию, отвечающую кэшированным записям ресурсов, ***DNS***-сервер может использовать данные из кэшированных записей ресурсов для ответа.

При кэшировании информации значение срока жизни применяется ко всем кэшированным записям ресурсов. Пока не истек срок жизни кэшированной записи ресурса, ***DNS***-сервер может продолжать кэшировать и снова использовать запись ресурса при ответах на соответствующие запросы клиентов. Значения срока жизни кэширования, используемые записями ресурсов в большинстве конфигураций зон, назначаются в параметре ***Мин. срок жизни TTL (по умолчанию)***, который задается в начальной записи зоны. По умолчанию задается значение минимального срока жизни 3600 секунд (1 час), но это значение может быть изменено, но могут также задаваться и отдельные значения срока жизни для каждой записи ресурса.

#### Обратный просмотр

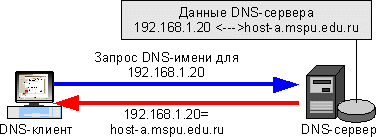
В большинстве операций просмотра ***DNS***-клиенты обычно выполняют *прямой просмотр*, т. е. поиск, основанный на имени ***DNS*** другого компьютера, сохраненного в записи ресурса адреса (A). В этом типе запроса в качестве данных для ответа на запрос ожидается ***IP***-адрес. ***DNS*** также обеспечивает возможность *обратного просмотра*, в котором клиенты используют известный ***IP***-адрес для поиска имени компьютера по этому адресу. Обратный просмотр фактически является формой вопроса типа:*«Можете ли вы сказать мне имя* ***DNS*** *компьютера, который использует IP-адрес 192.168.1.20?».*

Система ***DNS*** не разрабатывалась изначально для поддержки запросов этого типа. Одной из проблем при поддержке запросов обратного просмотра является различие в способах организации и индексации пространства имен ***DNS*** и способов назначения ***IP***-адресов. Если бы единственным таким способом был бы поиск во всех доменах пространства имен ***DNS***, то для обработки обратного запроса потребовалось бы много времени, такой запрос оказался бы бесполезным.

Чтобы разрешить эту проблему, в стандартах ***DNS*** был определен и зарезервирован специальный домен в пространстве имен ***DNS*** Интернета, ***in-addr.arpa***, обеспечивающий практичный и надежный способ выполнения обратных запросов. Чтобы создать обратное пространство имен, поддомены в домене ***in-addr.arpa*** формируются с помощью обратного упорядочения чисел в точечно-десятичной нотации ***IP***-адресов. Такое обратное упорядочение доменов для каждого октета необходимо, поскольку в отличие от имен ***DNS***, для которых ***IP***-адреса читаются слева направо, здесь интерпретация выполняется в обратном порядке. Когда ***IP***- адрес читается слева направо, информация анализируется от наиболее общей (***IP***-адрес сети в левой части адреса) до наиболее конкретной (***IP***- адрес узла в последнем октете). По этой причине порядок октетов ***IP***- адреса должен быть обращен при построении дерева домена ***in-addr.arpa***. ***IP***-адреса дерева ***DNSin-addr.arpa*** могут делегироваться организациям, которым назначается ограниченный набор ***IP***-адресов в границах определенных для Интернета классов адресов. И, наконец, для дерева домена ***in-addr.arpa***, встроенного в ***DNS***, требуется определение дополнительного типа записей ресурсов – запись ресурса указателя (***PTR***). Такая запись ресурса используется для сопоставления в зоне обратного просмотра, обычно соответствующего записи ресурса именованного узла

1. для имени ***DNS*** компьютера в зоне прямого просмотра.

*Рисунок5* иллюстрирует обратный запрос, инициируемый ***DNS***- клиентом (***host-b***), которому требуется узнать имя другого узла (***host-a***) по его ***IP***-адресу 192.168.1.20.



**Рисунок 5. Обратный запрос**

Обратный запрос включает следующие этапы:

* 1. Клиент ***host-b*** запрашивает ***DNS***-сервер о записи ресурса указателя (***PTR***), сопоставляющей IP-адрес 192.168.1.20 для имени ***host-a***.

*Поскольку запрос относится к записям* ***PTR****, система сопоставления имен обращает адрес и добавляет имя домена* ***in- addr.arpa*** *в конец обращенного адреса. В результате образуется полное доменное имя узла (****20.1.168.192.in-addr.arpa.****), для которого будет проводиться поиск в зоне обратного просмотра;*

* 1. После обнаружения имени удостоверяющий ***DNS***-сервер для имени ***20.1.168.192.in-addr.arpa*** может возвратить ответ с информацией записи ***PTR***. В этой информации содержится доменное имя ***DNS*** узла ***host-a***, что приводит к завершению процесса обратного просмотра. *Необходимо помнить, что если запрошенное обратное имя не может быть возвращено* ***DNS****- сервером, можно использовать сопоставление имен* ***DNS*** *(либо рекурсию, либо итерации) для обнаружения* ***DNS****-сервера, который является удостоверяющим для зоны обратного просмотра и содержит запрашиваемое имя. В этом смысле процесс сопоставления имен при обратном просмотре аналогичен процессу прямого просмотра.*

#### Инвертированные запросы

*Инвертированные запросы* являются устаревшим средством, которое ранее было предложено как часть стандарта ***DNS*** для поиска имени узла по его IP-адресу. В них используются нестандартные операции запросов ***DNS***, а их применение ограничено ранними версиями программы ***Nslookup***, которая является утилитой командной строки для устранения неполадок и тестирования службы ***DNS***.

Служба ***DNS*** распознает и принимает сообщения инвертированных запросов и отвечает на них с имитацией ответа на запрос.

#### Динамическое обновление

*Динамическое обновление* позволяет компьютерам ***DNS***-клиентов регистрировать и динамически обновлять собственные записи ресурсов с помощью ***DNS***-сервера при каждом возникновении изменений. Это снижает необходимость администрирования записей зон вручную, в особенности для клиентов, которые путешествуют или часто меняют расположение и получают IP-адреса через ***DHCP***.

Клиентские и серверные службы ***DNS*** поддерживают использование динамических обновлений, как описано в документе ***RFC 2136(Dynamic Updates in the Domain Name System)***. Служба ***DNS***-сервер поддерживает включение и отключение динамических обновлений отдельно для каждой зоны на каждом сервере, настроенном для загрузки либо стандартной основной зоны, либо зоны, интегрированной в каталоги. Служба ***DNS***- клиент будет по умолчанию динамически обновлять свои записи ресурсов узла (A) в ***DNS***, когда была выполнена настройка для ***TCP/IP***.

Динамические обновления обычно запрашиваются, когда изменяется имя ***DNS*** или ***IP***-адрес компьютера. Например, для клиента с именем ***oldhost*** в окне ***Свойства системы*** заданы следующие имена:

**Имя компьютера *oldhost***

**Доменное DNS-имя компьютера *mspu.edu.ru***

**Полное имя компьютера *oldhost. mspu.edu.ru***

В этом примере в конфигурации компьютера нет доменных имен ***DNS***, специфических для подключения. В дальнейшем компьютер переименовывается из ***oldhost*** в ***newhost***, в результате имена изменяются следующим образом:

**Имя компьютера *newhost***

**Доменное DNS-имя компьютера *mspu.edu.ru***

**Полное имя компьютера *newhost.mspu.edu.ru***

После изменения имени в окне ***Свойства системы*** отображается

приглашение перезагрузить компьютер. Когда при перезагрузке компьютер запускает ОС, служба ***DHCP***-клиент выполняет следующие действия для обновления ***DNS***:

1. Служба ***DHCP***-клиент отправляет запрос для типа начальной записи зоны (**SOA**) с использованием доменного имени ***DNS*** компьютера. Клиентский компьютер использует текущее полное доменное имя узла компьютера (в данном случае ***newhost.mspu.edu.ru***) как имя, указанное в этом запросе;
2. Удостоверяющий ***DNS***-сервер зоны, содержащей полное доменное имя узла клиента, отвечает на запрос типа ***SOA***;
3. После этого служба ***DHCP***-клиент пытается установить контакт с основным ***DNS***-сервером:

*Клиент обрабатывает ответ на запрос* ***SOA*** *для его имени, чтобы определить* ***IP****-адрес* ***DNS****-сервера, удостоверенного как основной сервер, для принятия его имени. Далее он выполняет такую последовательность шагов, необходимых, чтобы установить контакт и динамически обновить его основной сервер.*

* клиент отправляет запрос на динамическое обновление основному серверу, определенному в ответе на запрос **SOA**. *Если обновление выполняется успешно, другие действия не предпринимаются;*
* при отказе на обновление клиент отправляет запрос типа **NS** (о серверах имен) для зоны, имя которой указано в записи **SOA**;
* когда клиент получает ответ на этот запрос, он отправляет запрос

**SOA** на первый ***DNS***-сервер, перечисленный в ответе;

* после разрешения имен в запросе ***SOA*** клиент отправляет динамическое обновление серверу, указанному в возвращенной записи ***SOA***. *Если обновление выполняется успешно, другие действия не предпринимаются;*
* при отказе на обновление клиент повторяет запрос ***SOA***, отправляя его к следующему ***DNS***-серверу, перечисленному в ответе;

1. Как только находится основной сервер, который может выполнить обновление, клиент отправляет запрос на обновление, который обрабатывается сервером.

Содержимое запроса на обновление включает инструкции добавить

записи ресурсов A (и возможно ***PTR***) для имени ***newhost.mspu.edu.ru*** и записи этих типов для ранее зарегистрированного имени ***oldhost.mspu.edu.ru***.

Сервер также выполняет проверку, разрешены ли обновления для запроса клиента. Для стандартных основных зон динамические обновления не являются безопасными, поэтому для клиентов должны выполняться любые попытки обновления. Для зон, интегрированных в службу каталогов ***Active Directory***, обновления являются безопасными и выполняются с помощью параметров безопасности, устанавливаемых на основе каталогов.

Динамические обновления отправляются или выполняются периодически. По умолчанию компьютер отправляет обновления каждые 7 дней. Если в результате обновления данные в зоне не изменяются, зона остается в текущей версии и никакие изменения не записываются. Обновления выполняются только при фактических изменениях имен и адресов в зоне или в результате добавочной зонной передачи.

#### Безопасное динамическое обновление

Безопасные обновления ***DNS*** доступны только для зон, интегрированных в службу каталогов ***Active Directory***. После преобразования зоны в интегрированную становится возможным использование с консоли ***DNS*** списков управления доступом. Можно добавлять пользователей и группы в списки или удалять их для указанной зоны или записи ресурса. Параметры безопасного динамического обновления для ***DNS***-серверов и клиентов по умолчанию обрабатываются следующим образом:

* ***DNS***-клиенты сначала предпринимают попытки выполнить небезопасные динамические обновления. При отказе на небезопасные обновления клиенты пытаются выполнить безопасные обновления;

*Кроме того, клиенты используют политику обновления по умолчанию, которая позволяет им пытаться переписывать ранее зарегистрированную запись ресурса, если она специально не заблокирована условиями безопасности обновления.*

* после интегрирования зоны в службу каталогов ***Active Directory DNS***-серверам ***Windows Server 2003*** по умолчанию разрешаются только безопасные динамические обновления.

*При использовании стандартного сохранения зон настройки по умолчанию службы* ***DNS****-сервер не разрешают динамические обновления зон. И для зон, интегрированных в каталоги, и для использующих стандартное сохранение в файлах можно изменить параметры зоны и разрешить динамические обновления. Это позволяет принимать любые обновления.*

При развертывании ***DNS***-серверов совместно с ***Active Directory*** необходимо иметь в виду следующее:

* служба ***DNS*** требуется для обнаружения контроллеров доменов ***Windows Server 2003***. Служба сетевого входа в систему использует новые средства поддержки ***DNS***-серверов для обеспечения регистрации контроллеров доменов в пространстве доменных имен ***DNS***;
* ***DNS***-серверы ***Windows Server 2003*** могут использовать службу каталогов ***Active Directory*** для сохранения и репликации зон. *При интегрировании зон в службу каталогов пользователи получают возможность использовать дополнительные средства* ***DNS****, такие как безопасные динамические обновления и средства устаревания и очистки записей.*

Способы интеграции ***DNS*** со службой каталогов ***Active Directory***:

* при установке ***Active Directory*** на сервер выполняется повышение сервера до роли контроллера указанного домена. Когда данный процесс завершается, пользователю выводится приглашение указать доменное имя ***DNS*** для домена ***Active Directory***, для которого выполняется присоединение и повышение сервера;
* если в этом процессе удостоверяющий ***DNS***-сервер для указанного домена либо не обнаруживается в сети, либо не поддерживает протокол динамического обновления ***DNS***, выводится приглашение установить ***DNS***-сервер. Такая возможность предоставляется, поскольку ***DNS***-серверу необходимо отыскать этот сервер или другие контроллеры домена для рядовых серверов домена ***Active Directory***.

После установки ***Active Directory*** имеются две возможности сохранения и репликации зон при работе с ***DNS***-сервером на новом контроллере домена:

* стандартное сохранение зоны с помощью файла в текстовом

формате. *Зоны, сохраняемые этим способом, размещаются в файлах с расширением* ***DNS****, которые сохраняются в папке* ***systemroot\System32\Dns*** *на каждом компьютере, на котором выполняется* ***DNS****-сервер. Имя файла зоны соответствует имени, которое пользователь выбрал для зоны при ее создании, например,* ***mspu.edu.ru.dns****, если именем зоны является* ***mspu.edu.ru.dns****;*

* сохранение зон, интегрированных в службу каталогов, с помощью базы данных ***Active Directory***. *Зоны, сохраняемые таким образом, размещаются в дереве* ***Active Directory*** *под разделом каталога домена или приложения. Каждая зона, интегрированная в службу каталогов, сохраняется в контейнере* ***dnsZone****, который идентифицируется по имени, выбранному пользователем при ее создании.*

**Преимущества интеграции с *Active Directory***

В сетях с развертыванием ***DNS*** для поддержки службы каталогов ***Active Directory*** настоятельно рекомендуется использовать основные зоны, интегрированные в службу каталогов, которые предоставляют следующие преимущества:

* обновление с несколькими главными серверами и расширенные средства безопасности, базирующиеся на возможностях ***Active Directory***. В модели стандартного сохранения зон обновления ***DNS*** выполняются на основе модели с единственным главным сервером. В такой модели единственный удостоверяющий ***DNS***- сервер зоны обозначается как основной источник для зоны. Это сервер содержит главную копию зоны в файле на локальном диске. В этой модели основной сервер зоны представляет единственную фиксированную точку отказа. Если этот сервер недоступен, запросы на обновление зоны от ***DNS***-клиентов не обрабатываются. При сохранении зон, интегрированных в службу каталогов, динамические обновления ***DNS*** выполняются с использованием модели с несколькими главными серверами. В этой модели любой удостоверяющий ***DNS***-сервер, например, контроллер домена, выполняющий службу ***DNS***-сервер, обозначается как основной источник для зоны. Поскольку главная копия зоны поддерживается в базе данных ***Active***

***Directory***, которая полностью реплицируется на все контроллеры домена, зона может обновляться любыми ***DNS***-серверами, выполняющимися на любом контроллере домена.При использовании модели ***Active Directory*** с несколькими главными серверами любой из основных серверов для зоны, интегрированной в каталоги, может обрабатывать запросы от ***DNS***-клиентов на обновление зоны, пока контроллер домена является доступным по сети. Кроме того, при использовании зон, интегрированных в службу каталогов, можно с помощью списков управления доступом защитить объект-контейнер ***dnsZone*** в дереве каталогов. Это средство обеспечивает дифференцированный доступ к зоне или к конкретной записи ресурса в зоне. Например, список управления доступом для записи ресурса в зоне можно ограничить так, чтобы разрешить динамические обновления только указанному компьютеру клиента или группе безопасности, например, группе администраторов домена. Это средство безопасности недоступно для стандартных основных зон. Необходимо отметить, что при преобразовании зоны к типу интегрированной в службу каталогов настройка по умолчанию для обновлений зоны изменяется, и разрешаются только безопасные обновления. Кроме того, при использовании списков управления доступом на объектах ***Active Directory***, относящихся к ***DNS*** , списки управления доступом могут применяться только к службе ***DNS***- клиент;

* репликация и синхронизация зон с новыми контроллерами домена выполняется автоматически при каждом добавлении нового контроллера в домен ***Active Directory***. Хотя службу ***DNS*** можно выборочно удалять с контроллеров домена, зоны, интегрированные в службу каталогов, всегда сохраняются на каждом контроллере домена. В результате сохранение и управление зонами не является дополнительным ресурсом. Кроме того, способы синхронизации информации, сохраняемой в службе каталогов, обеспечивают повышение быстродействия по сравнению со стандартными способами сохранения обновлений зон, которые могут потенциально потребовать передачи зоны целиком;
* за счет сохранения баз данных зон ***DNS*** в ***Active Directory*** имеется возможность рационализировать репликацию баз данных в сети. Когда пространство имен ***DNS*** и домены ***Active Directory*** сохраняются и реплицируются независимо, необходимо обеспечить планирование и администрирование каждого из них в отдельности. Например, при одновременном использовании стандартного сохранения зон ***DNS*** и службы каталогов ***Active Directory*** необходимо обеспечить структуру, реализацию, тестирование и управление для двух различных топологий репликации баз данных. Одна топология требуется для репликации данных из каталогов между контроллерами домена, а другая топология может потребоваться для репликации баз данных зон между ***DNS***-серверами.Это приведет к дополнительным трудностям при планировании и разработке структуры сети с учетом ее естественного роста. За счет интеграции сохранения информации ***DNS*** появляется возможность унифицировать вопросы управления и репликации для ***DNS*** и ***Active Directory***, объединяя их в единое административное целое;
* репликация каталогов выполняется быстрее и эффективнее, чем стандартная репликация ***DNS***. Поскольку репликация ***Active Directory*** выполняется на уровне отдельных свойств, распространяются только необходимые изменения. При этом для зон, интегрированных в службу каталогов, используется и отправляется меньший объем данных.

### Выполнение работы

#### Задание 1. Установите сервер*DNS*:

* 1. Запустите виртуальную машину ВМ ***VM-2***.
  2. Подключите к виртуальной машине образ установочного диска

##### win2003.iso.

* 1. Откройте диалоговое окно ***Управление данным сервером***

##### (Пуск/Администрирование/Управление Данным Сервером).

* 1. Активизируйте установку сервера имен:
     + запустите мастер добавления ролей сервера, кнопкой ***Добавить или удалить роль***;
     + ознакомьтесь с информацией мастера и продолжите установку кнопкой ***Далее***;
     + укажите тип установки Особая конфигурация и продолжите установку кнопкой ***Далее***;
     + выберите в списке доступных ролей сервера пункт ***DNS***-сервер. Нажмите ***Далее***;
     + ознакомьтесь с сводкой выбранных параметров и продолжите установку кнопкой ***Далее***.

*После завершения установки сервера имен, автоматически запуститься* ***Мастер настройки DNS-сервера****.*

* 1. Выполните первоначальную настройку ***DNS***-сервера с помощью мастера:
     + ознакомьтесь с информацией мастера (***Далее***);
     + ознакомьтесь с предлагаемыми вариантами настройки сервера;
     + выберите создание зоны прямого просмотра для небольших сетей, соответствующей радиокнопкой (***Далее***);
     + укажите ваш ***DNS***-сервер в качестве ***DNS***-сервера, который будет обслуживать зону прямого просмотра, радиокнопкой *Управление зоной выполняется этим сервером*. Продолжите установку кнопкой ***Далее***;
     + задайте имя зоны, например ***example.edu.ru*** и продолжите установку кнопкой ***Далее***;
     + введите в поле ***Создать новый файл*** имя файла (например,*example.edu.ru.dns*)в котором будет храниться конфигурация зоны. Продолжите установку кнопкой ***Далее***;
     + запретите динамическое обновление соответствующей радиокнопкой и продолжите настройку кнопкой ***Далее***;
     + откажитесь от пересылки запросов на другие ***DNS***-сервера, выбрав радиокнопку *Нет, не пересылать запросы* (***Далее***);
     + ознакомьтесь с информацией о недоступности корневых сертификатов и щелкните ***ОК***;
     + завершите первоначальную настройку ***DNS***-сервера кнопкой

***Готово***.

#### Задание 2. Настройте сервер *DNS*:

* 1. Переключитесь в диалоговое окно ***Управления данным сервером***.
  2. Перейдите в управление ***DNS***-сервером, кнопкой ***Управление этим***

##### DNS-сервером.

*Появится окно консоли администрирования, с открытой оснасткой управления* ***DNS****-сервером*

* 1. Настройте зону прямого просмотра:
     + откройте диалоговое окно свойств созданной ранее зоны

##### example.edu.ru (контекстное меню/Свойства);

* + - настройте очистку и обновление содержимого ***DNS***-сервера:
      * откройте окно очистки, кнопкой ***Очистка***;
      * установите флажок ***Удалять устаревшие записи ресурсов***;
      * установите ***интервал блокирования***–*1 день*;
      * установите ***интервал обновления***–*7 дней*;
      * подтвердите изменения кнопкой ***ОК***;
    - установите ***срок жизни (TTL) записи***–*2 часа*:
      * перейдите на вкладку ***Начальная запись зоны (SOA)***;
      * введите в поле ***Срок жизни (TTL) записи***–*0: 2: 0: 0*;
      * установите ***желаемые интервалы для обновления и повтора***–*не менее 1 и не более 15 минут*;
    - завершите настройку кнопкой ***ОК***.
  1. Создайте запись в ***DNS***-сервере соответствующую физическому компьютеру:
     + откройте диалоговое окно **добавления новых узлов (*контекстное меню example.edu.ru/Создать узел (А)*)**;
     + введите в поле ***Имя***–<*имя\_физического\_компьютера*>
     + введите в поле ***IP-адрес***–*192.168.1.1*
     + завершите добавление кнопкой ***Добавить***.
  2. Создайте новую основную зону обратного просмотра:

##### откройте мастер создания новых зон (контекстное меню Зоны обратного просмотра/Создать новую зону);

* + - ознакомьтесь с информацией мастера и щелкните ***Далее***;
    - укажите ***тип создаваемой зоны***–*Основная зона* (***Далее***);
    - укажите ***код сети***–*192.168.1* (***Далее***); *Поскольку IP-адреса создаваемой сети к сети класса C, то в IP- адресах сети будет меняться только последний разряд адреса.*
    - укажите имя файла для зоны по умолчанию и продолжите установку кнопкой ***Далее***;
    - установите запрет динамических обновлений (***Далее***);
    - завершите создание зоны кнопкой ***Готово***.
  1. Протестируйте работу ***DNS***-сервера:
     + откройте диалоговое окно свойств ***DNS***-сервера (***контекстное меню Wind2003/Свойства***);
     + перейдите на вкладку ***Наблюдение***;
     + установите флажок *Простой запрос к этому DNS-серверу*;
     + активируйте тестирование кнопкой ***Тест***;

*Результат отобразиться в поле* ***Результаты теста****;*

* + - создайте и сохраните в своей папке снимок экрана с результатами теста;
    - закройте диалоговое окно свойств кнопкой ***ОК***.
  1. Выключите ВМ.

#### Задание 3. Самостоятельно добавьте в зону прямого и обратного просмотра несколько узлов (не менее 5).

**Задание 4. Самостоятельно проверьте работу *DNS*-сервера с помощью эхо-запросов на соответствующие узлы.**

**Лабораторная работа 1.4. Работа с *Active Directory***

**Цель:** научиться устанавливать и просматривать ***Active Directory***, научится подключать компьютеры к домену.

#### Средства для выполнения работы:

* **аппаратные:** компьютер с установленной ОС ***Windows XP;***
* **программные:** приложение ВМ ***VirtualBox***; виртуальные машины:

***VM-1, VM-2.***

### Теоретические сведения

***Active Directory*** является ***LDAP***(***L****ightweight* ***D****irectory* ***A****ccess* ***P****rotocol*, *облегчённый протокол доступа к каталогам*) – совместимой реализацией службы каталогов (это средство иерархического представления ресурсов, принадлежащих некоторой отдельно взятой организации, и информации об этих ресурсах) корпорации ***Мicrosoft*** для операционных систем семейства ***Windows NT***.

***Active Directory*** позволяет администраторам использовать

глобальные политики, развёртывать программы на множестве компьютеров (через глобальные политики или посредством ***Microsoft Systems Management Server 2003***) и устанавливать важные обновления на всех компьютерах в сети (с использованием ***Windows Server Update Services (WSUS); Software Update Services (SUS)*** ранее). ***Active Directory*** хранит данные и настройки среды в централизованной базе данных. Сети ***Active Directory*** могут быть различного размера: от нескольких сотен до нескольких миллионов объектов.

Помимо обычных для служб каталогов задач, ***Active Directory*** способна удовлетворить широкий спектр потребностей по обработке имен, обслуживанию запросов, регистрации, администрированию и устранению конфликтов. В ***Active Directory*** используется тесно увязанный набор ***API*** и протоколов, так что она может работать с несколькими пространствами имен, собирать и предоставлять информацию о каталогах и ресурсах, находящихся в удаленных филиалах и под управлением разных ОС. ***Active Directory*** имеет следующие возможности и характеристики:

* + поддержка открытых стандартов для облегчения межплатформных операций с каталогами, в т. ч. доменной системы имен ***DNS*** и стандартных протоколов, таких как ***LDAP***;
  + поддержка стандартных форматов имен для простоты миграции и эксплуатации;
  + богатый набор ***API***, которые могут использоваться как для командных сценариев, так и в программах на ***C/C+***;
  + простой и интуитивно понятный процесс администрирования благодаря несложной иерархической доменной структуре и использованию технологии «перетащить и оставить»;
  + возможность расширения набора объектов в каталогах, за счет гибкой логической схемы;
  + быстрый поиск по глобальному каталогу;
  + быстрое и удобное обновление информации посредством многоуровневой (*multimaster*) репликации данных;
  + совместимость с предыдущими версиями ОС ***Windows NT***;
  + взаимодействие с сетями ***NetWare***.

***Active Directory*** позволяет управлять с одного рабочего места всеми заявленными ресурсами (файлами, периферийными устройствами, базами данных, подключениями к серверам, доступом к Web, пользователями, другими объектами, сервисами и т. д.). В качестве идентификационной

службы в ней используется доменная система имен (***DNS***), применяемая в Интернете, объекты в доменах строятся в иерархию организационных единиц (***ОЕ***), а домены могут быть объединены в древовидную структуру. Администрирование становится еще проще, так как в ***Active Directory*** отсутствует понятие главного контроллера доменов (***ГКД***) и резервного контроллера доменов (***РКД***). В ***Active Directory*** существуют только контроллеры домена (***КД***), и все они равны между собой. Администратор может сделать изменения на любом ***КД***, и эти изменения будут скопированы на всех остальных ***КД***.

***Active Directory*** отделяет логическую структуру иерархии доменов ***Windows 2003*** от физической структуры сети.Ресурсы хранятся в виде объектов. Схема ***Active Directory***:

* + *домены*: базовая организационная структура;
  + *деревья*: несколько доменов объединяются в иерархическую структуру;
  + *леса*: группа из нескольких деревьев домена.

Организационные единицы позволяют делить домен на зоны и делегировать на них права.Логическая структура ***Active Directory*** не базируется на физическом местонахождении серверов или сетевых соединениях в пределах домена. Это позволяет структурировать домены, отталкиваясь не от требований физической сети, а от административных и организационных требований.

Объекты хранятся в ***Active Directory*** в виде иерархической структуры контейнеров и подконтейнеров, упрощающей поиск, доступ и управление, она похожа на файловую систему ***Windows*** с файлами и папками.

Классы объектов. Объект представляет собой просто набор атрибутов. Например, объект пользователя (*user object*) состоит из таких атрибутов, как имя, пароль, телефонный номер, сведения о членстве в группах и т. п. Атрибуты, образующие объект, определяются классом объекта.Классы и атрибуты, определяемые ими, собирательно называются ***Active Directory Schema***– в терминологии баз данных схема (***schema***) – это структура таблиц и полей и их взаимосвязи. Ее можно считать набором данных (классов объектов), определяющим то, как организована и хранится реальная информация (атрибуты объекта) в каталоге.

***Active Directory*** не единственная служба каталогов. В современных сетях используется несколько служб каталогов и стандартов,в частности:

* ***Х.500****и****D****irectory****A****ccess****P****rotocol* ***(DAP).X.500***– спецификация ***I****nternet* ***S****tandards* ***O****rganization* ***(ISO)***, определяющая, как должны быть структурированы глобальные каталоги. Онатакже описывает применение ***DAP*** для обеспечения взаимодействия между клиентами и серверами каталогов;
  + ***LightweightDirectoryAccessProtocol (LDAP)*** была разработана в ответ на критические замечания по ***DAP***, которая оказалась слишком сложной для применения в большинстве случаев. ***LDAP*** быстро стала стандартным протоколом каталогов в Интернете.
  + ***Novell Directory Services (NDS)***. Служба каталогов для сетей

***Novell NetWare***, совместимая со стандартом ***Х.500***.

* + ***Active Directory*** – составная часть сетей под управлением ***Windows Server 2000*** или ***Windows Server 2003***. Соответствует стандарту ***LDAP***.

### Выполнение работы

**Задание 1. Установите *Active Directory:***

* 1. Подготовьте виртуальную машину ***VM-2*** к установке службы каталогов:
     + подключите к ВМ образ установочного диска ***win2003-1.iso***.
  2. Откройте диалоговое окно ***Управление данным сервером***

##### (Пуск/Администрирование/Управление Данным Сервером).

* 1. Проверьте наличие установленного сервера доменных имен (***DNS***).

*Установка службы каталогов невозможна без* ***DNS****.*

* 1. Активизируйте добавление новых ролей для сервера (***Добавить или удалить роль***).
  2. Выберите пункт ***Контроллер домена (Active Directory)*** . Перейдите к следующему шагу кнопкой ***Далее***.
  3. Ознакомьтесь с информацией об устанавливаемых компонентах и щелкните ***Далее***.
  4. Ознакомьтесь с информацией ***Mастера установки Active Directory*** и щелкните ***Далее***.
  5. Ознакомьтесь с информаций о совместимости с операционной системой и щелкните ***Далее***.
  6. Укажите ***вариант созданий контроллера домена***–*Контроллер домена в новом домене* и щелкните ***Далее***.
  7. Укажите ***тип создаваемого домена***–*Новый домен в новом лесу* и щелкните ***Далее***.
  8. Введите ***полное DNS-имя создаваемого домена***–*example.edu.ru* и щелкните ***Далее***.
  9. Введите ***NetBIOS-имя домена***–*EXAMPLE* и щелкните ***Далее***. *Обычно оно уже указанно по умолчанию, исходя из того, какое* ***DNS****- имя было дано создаваемому домену. Например, при создании домена с именем* ***example.edu.ru****, по умолчанию* ***NETBIOS-имя*** *будет* ***EXAMPLE****.*
  10. Укажите место хранения баз данных и журналов ***Active Directory:***
      + введите в поле ***Папка расположения Баз* –**

*C:\WINDOWS\NTDS\BASE*;

* + - введите в поле ***Папка расположения журнала*–**

*C:\WINDOWS\JOURNAL*;

* + - подтвердите изменения кнопкой ***Далее***.
  1. Ознакомьтесь с информацией об общей папке и щелкните ***Далее***. *Если ваш* ***DNS****-сервер настроен неправильно, вы получите сообщение об ошибке и возможных путях её устранения (выберите* ***Проблема будет решена позже****).*
  2. Установите разрешения для объектов службы каталогов – *Разрешения, совместимые только с* ***Windows 2000*** *или* ***Windows Server 2003*** и щелкните ***Далее***.
  3. Укажите пароль, для учётной записи администратора режима восстановления:
     + введите в поле ***Пароль режима восстановления***–*123456*;
     + введите в поле ***Подтверждение***–*123456*;
     + подтвердите изменения кнопкой ***Далее***.
  4. Ознакомьтесь с сводной информацией об установке службы каталогов и запустите ее установку кнопкой ***Далее***.
  5. Завершите работу мастера кнопкой ***Готово***.
  6. Перезагрузите виртуальную машину кнопкой ***Перезагрузить сейчас***.
  7. Войдите в систему после перезагрузки и завершите установку службы каталогов кнопкой ***Готово***.

**Задание 2. Выполните следующие операции с*ActiveDirectoryManage****r****:***

* 1. Откройте диалоговое окно ***Пользователи и компьютеры* (*Пуск/Администрирование/Active Directory – пользователи и компьютеры*)**.
  2. Ознакомьтесь с структурой созданного ранее домена:
     + разверните узел ***example.edu.ru***;
     + просмотрите стандартных пользователей домена (***Builtin***);
     + просмотрите контроллеры домена (***Domain Controllers***).
  3. Создайте новый каталог (подразделение/контейнер) в корне сервера:
     + активизируйте узел ***example.edu.ru***;
     + щелкните по кнопке ***Создание нового подразделения в текущем контейнере*** на панели инструментов;
     + в появившемся диалоговом окне введите **имя создаваемого подразделения**–*Students* (***OK***);

*Будет создан новый контейнер для подразделения и выделение автоматически переместиться на него.*

* 1. Создайте новую учетную запись пользователя в контейнере ***Students***:
     + откройте диалоговое окно ***Новый объект – Пользователь***, кнопкой

##### Создание нового пользователя в текущем контейнере;

* + - введите данные о пользователе:
      * ***Полное имя пользователя***–*Просто Пользователь*;
      * ***Имя входа пользователя (логин)***–*JustUser*;
      * подтвердите введенные данные кнопкой ***Далее***.
    - установите пароль для пользователя:
      * введите в поле ***Пароль***–*User1234*;
      * введите в поле ***Подтверждение***–*User1234*;
      * установите флажок *Срок действия пароля не ограничен*;
      * завершите ввод пароля кнопкой ***Далее***.

*В правой области отобразится запись, соответствующая созданному пользователю.*

* 1. Введите более полную информацию о пользователе:
     + откройте диалоговое окно***свойств пользователя*** (двойной щелчок по надписи ***Просто пользователь*)**;
     + введите в поле ***Описание***–*это тестовый пользователь*;
     + введите в поле ***Комната***–*316* (номер кабинета, в котором проходит занятие);
     + введите в поле ***Телефон***–<*номер\_телефона*>;
     + укажите *адресные данные* на вкладке ***Адрес***;
     + укажите несколько дополнительных телефонов пользователя на вкладке ***Телефоны***;
     + завершите изменение данных пользователя кнопкой ***ОК***.
  2. Создайте группу ***group1*** в контейнере ***Students***:
     + откройте диалоговое окно ***создания групп* (*контекстное меню/Создать/Группа*)**;
     + введите ***имя группы***–*group1*;
     + завершите создание группы кнопкой ***ОК***.
  3. Задайте дополнительную информацию для группы ***group1***:
     + откройте диалоговое окно ***свойств группы*** (двойной щелчок по надписи ***group1***);
     + введите в поле ***Описание***–*Это тестовая группа*;
     + завершите изменение данных группы кнопкой ***ОК***.
  4. Включите созданного ранее пользователя ***Просто пользователь (JustUser)*** в группу ***group1***:
     + откройте диалоговое окно ***свойств пользователя*** (двойной щелчок по записи пользователя);
     + перейдите на вкладку ***Член групп***;
     + откройте диалоговое окно выбора группы кнопкой ***Добавить***;
     + введите ***название группы***–*group1*;
     + завершите добавления пользователя в группу кнопкой ***ОК***;
     + закройте диалоговое окно свойств пользователя кнопкой ***ОК***.
  5. Выполните редактирование политики безопасности домена, созданной автоматически:
     + откройте диалоговое окно свойств домена ***example.edu.ru***

##### (контекстное меню/Свойства);

* + - перейдите на вкладку ***Групповая политика***; *В списке будет расположена политика домена по умолчанию* ***Default Domain Policy***;
    - откройте диалоговое окно (***Редактор объектов групповой политики***) изменения политики ***Default Domain Policy*** (двойной щелчок по политике);
    - внесите в изменения в политику паролей:
      * перейдите в раздел ***Политика паролей* (*Конфигурация компьютера/Конфигурация Windows/Параметры***

##### безопасности/Политики учётных записей/ Политики паролей);

* + - * установите минимальную длину пароля:
        + откройте окно ***изменения параметров пароля*** (двойной щелчок по надписи ***Мин. длинна пароля***);
        + введите в поле ***Длина пароля не менее***–*5*;
        + подтвердите изменения кнопкой ***ОК***;
      * отключите соответствие пароля требованиям сложности:
        + откройте диалоговое окно ***свойств требования сложности***(двойной щелок по надписи ***Пароль должен отвечать требованиям сложности***);
        + установите радиокнопку *Отключить*;
        + подтвердите изменения кнопкой ***ОК***;
    - закройте ***Редактор объектов групповой политики***

##### (Консоль/Выход);

* + - закройте диалоговое окно свойств домена кнопкой ***ОК***.
  1. Выполните выход из системы с повторным входом для активации изменений в политике безопасности. *Изменения в политике паролей вступят в силу только после выхода из системы и повторного входа в неё.*
  2. Измените пароль созданного ранее пользователя:
     + активизируйте раздел ***Students***;
     + задайте новый, более простой пароль пользователю ***Просто пользователь***:
       - откройте диалоговое окно ***задания пароль* (*контекстное меню/Смена пароля*)**;
     + введите в поле ***Пароль***–*123*;
     + введите в пол ***Подтверждение пароля***–*123*;

*Обратите внимание на то,что сообщений о слишком простом пароле не было.*

* 1. Исключите созданного ранее пользователя из группы ***group1****:*
     + откройте диалоговое окно ***свойств группы***;
     + перейдите на вкладку ***Члены группы***;
     + выделите в списке удаляемого пользователя и щелкните по кнопке

##### Удалить;

* + - подтвердите удаление кнопкой ***Да***;
    - закройте диалоговое окно свойств группы кнопкой ***ОК***.
  1. Включите созданного ранее пользователя в администраторы домена:
     + откройте диалоговое окно ***свойств пользователя Просто пользователь***;
     + перейдите на вкладку ***Член групп*** и щелкните ***Добавить***;
     + введите в поле Администраторы домена;
     + завершите добавление в группу кнопкой ***ОК***;
     + закройте окно свойств пользователя кнопкой ***ОК***.

**Задание 3. Присоедините компьютеры под управлением *Windows XP* к домен**у.

* 1. Запустите виртуальную машину ***VM-3*** и загрузите в ней ОС ***Windows XP***.
  2. Откройте диалоговое окно ***Свойства системы* (*Пуск/Панель управления/Система*)** и перейдите на вкладку ***Имя компьютера***(***Далее***).
  3. Откройте диалоговое окно ***Изменение имени*** кнопкой ***Изменить***.
  4. Укажите в разделе ***Является членом***–*домена*.
  5. Введите в поле левую часть имени созданного ранее домена, например ***example***.
  6. Подтвердите изменения кнопкой ***ОК***. *Через некоторое время домен, к которому подключается компьютер, запросит имя и пароль администратора домена.*
  7. Введите ***имя/пароль*** администратора в созданном ранее домене (*JustUser/123*).
  8. Ознакомьтесь с сообщением от домена *«Добро пожаловать в домен»*

и щелкните ***ОК***.

* 1. Ознакомьтесь с информацией о необходимости перезагрузки компьютера и закройте окно кнопкой ***ОК***.
  2. Закройте диалоговое окно ***Свойства системы*** кнопкой ***ОК***.
  3. В появившемся диалоговом окне согласитесь с перезагрузкой кнопкой ***Да***. *После этого компьютер начнет перезагружаться.*
  4. Войдите в систему с использованием любой из созданных вами учетных записей.
  5. Проверьте действие сделанных вами ограничений в домене.
  6. Выключите ВМ ***VM-1***.

#### Задание 4. Присоедините компьютеры под управлением *OpenSUSE*

***Linux* к домену.**

* 1. Запустите виртуальную машину ***VM-1*** и загрузите в ней ОС

##### OpenSUSE.

* 1. Откройте диалоговое окно ***Hастройки системы* (*Главное Меню/Компьютер/YaST Администратор*)**.
  2. В появившемся диалоговом окне введите ***пароль администратора системы***–*1233456* (задавался при установке системы).
  3. Перейдите в раздел ***Сетевые службы***.
  4. Запустите ***Mастер присоединения к домену***.В появившемся диалоговом окне подтвердите установку дополнительного пакета ***samba-client*** кнопкой ***Продолжить***.
  5. Введите в поле ***Домен или группа*** имя созданного ранее домена (левую часть полного имени домена) –*example*.
  6. Включите разрешение создания общих ресурсов пользователями.
  7. Щелкните по кнопке ***Завершить***. Появится сообщение с предложение присоединить компьютер к домену, щелкните по кнопке ***Да***.
  8. Укажите данные администратора домена:
     + введите в поле ***Имя пользователя***–*JustUser*;
     + введите в поле ***Пароль***–*123*;
     + подтвердите вод данный кнопкой ***Да***.
  9. Проверьте правильность подключения к домену:
     + выйдите из системы;
     + войдите в систему под одной из учетных записей пользователей домена.
  10. Завершите работу ВМ.

#### Задание 5. Самостоятельно создайте учтенную запись администратора домена.

**Задание 6. Самостоятельно создайте в домене контейнер для вашей группы и внесите в него всех студентов из вашей группы.**

**Задание 7. Самостоятельно измените политику безопасности домена (запретите изменение рабочего стола, установите длину пароля не менее 8 символов).**

## Примерные тестовые задания к модулю 1

1. Виртуализация – это
   * *общий термин, охватывающий абстракцию всех ресурсов;*
   * *общий термин, охватывающий абстракцию аппаратных ресурсов;*
   * *общий термин, охватывающий абстракцию программных ресурсов.*
2. Вершина дерева, представляющая не именованный уровень, это
   * *корень доменов;*
   * *домен верхнего уровня;*
   * *домен второго уровня;*
   * *поддомен.*
3. Обратное пространство имен формируется в домене, именуемом
   * *in-addr.arpa;*
   * *addr-in.arpa;*
   * *arpa-in.addr;*
   * *in-arpa.addr.*
4. Установите соответствие элементов адреса ***host- b.mspu.edu.ru***их обозначению в терминологии DNS:

***host-b*** *Поддомен*

***mspu*** *Домен второго уровня*

***edu*** *Домен верхнего уровня*

***ru*** *Имя узла*

## Контрольные вопросы к модулю 1

1.Этапы проектирования сети. 2.Сетевые операционные системы. 3.Алгоритм установки сетевой ОС. 4.Служба доменных имен DNS.

5.Пространство доменных имен. 6.Работа запросов DNS.

7.Процесс рекурсии при разрешении имени. 8.Локальная система разрешения имени.

9.Типы ответов DNS-сервера. 10.Обратный просмотр.

11.Динамическое обновление. 12.Службы каталогов.

13.Active Directory. 14.Объекты службы каталогов.

15.Алгоритм добавления объекта в службу каталогов.

# Модуль 2.

# Настройка домена и его безопасность

**Цель:** научиться выполнять основную настройку файлового сервера, Web- сервера (***HTTP***) и ***FTP***-сервера; настраивать параметры безопасности домена.

**Результат:** уметь настраивать основные сервера: файловый сервер, Web- сервер (***HTTP***), ***FTP***-сервер; уметь настраивать параметры безопасности домена.

#### План освоения модуля:

1. Изучите следующие темы в указанных источниках:
   * *Планирование безопасности домена;*
   * *Создание учетных записей пользователей;*
   * *Реализация запланированной политики безопасности домена;*
   * *Подготовка файлового сервера;*
   * *Алгоритм технологии установки и настройки FTP-сервера и Web- сервера.*
2. Выполните и представьте преподавателю лабораторные работы:
   * ЛР 2.1. *Настройка параметров безопасности домена.*
   * ЛР 2.2. *Работа с серверами HTTP и FTP.* **III.**Выполните самостоятельные задания к модулю. **IV.**Выполните тестовые задания к модулю. **V.**Защитите модуль по контрольным вопросам. **Литература:**
3. Немеет Э. Т. UNIX: руководство системного администратора. Для профессионалов. 3-е изд./ Э.Немет [и др.]; под ред. Э.Немет– СПб.: Питер; К.: Издательская группа BHV, 2006. – 925 с.: ил. (Гл. 27).
4. Холме Дэн. Управление и поддержка Microsoft Windows Server 2003. Учебный курс MCSA/MCSE / Пер. с англ. – М.: Издательско-торговый доме «Русская Редакция» / Холме Дэн [и др.], 2004. – 448 стр.: ил. (Гл. 1– 3).
5. Ханникат Дж. Знакомство с Microsoft Windows Server 2003 / Пер. с англ. / Дж Ханникат – М.: Издательско-торговый дом «Русская Редакция», 2003.

– 464 с.: ил. (Гл. 3–5).

1. УильямР. Станек. Microsoft Windows Server 2003. Справочник администратора / Пер. с англ. / УильямР. Станек– М.: Издательско- торговый доме «Русская Редакция», 2003. – 640 с.: ил. (Гл.1–3).

#### Лабораторная работа 2.1.

**Настройка параметров безопасности домена**

**Цель:** научиться устанавливать и просматривать ***Active Directory,*** научится подключать компьютеры к домену.

#### Средства для выполнения работы:

* + **аппаратные:** компьютер;
  + **программные:** ОС ***Windows 2003 server.***

***Теоретические сведения***

Словосочетание *"информационная безопасность"* в разных контекстах может иметь различный смысл. В **Доктрине информационной безопасности Российской Федерации** термин "информационная безопасность" (ИБ) используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В **Законе РФ "Об участии в международном информационном обмене"** информационная безопасность определяется аналогичным образом – как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Под *информационной безопасностью* будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

*Защита информации*– это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Комплекс работ по внедрению политики информационной безопасности можно разделить *на 3 этапа*.

*На первом этапе* определяются общие подходы к политике ИБ, определяются группы ИБ и общее описание разрешений.

*На втором этапе* осуществляется документирование политики ИБ: составление правил и инструкций для работников организации.

*На третьем этапе*производитсявнедрение политики ИБ как

программными, так и аппаратными средствами.

Следует разработать ряд правил, которые помогут регламентировать работу всех пользователей в сети (как привилегированных так и не привилегированных). В частности следует разработать:

* + - правила административного обслуживания;
    - перечень прав и обязанностей пользователей;
    - правила для администраторов;
    - правила создания «гостевых» учетных записей.

Разработка таких правил позволит получить ряд преимуществ, в частности: рутинные задачи,как правило, выполняются одинаково; уменьшение вероятности появления ошибок; работа по инструкциям выполняется гораздо быстрее и др.

Помимо разработки ряда правил для пользователей следует предусмотреть (разработать) стандартные методики подключения и конфигурирования и модернизации компьютеров; инсталляции и деинсталляции программного обеспечения; резервного копирования данных; назначения адресов и т.д. Например, считается, что управление адресами и именами компьютеров, идентификаторами пользователей и групп должно осуществляться единообразно.

#### Правила для пользователей

Во многих организациях существуют специально разработанные правила пользователей, только после подписания, которых пользователь получает доступ к сети организации.

В правилах для пользователя необходимо регламентировать такие вопросы, как:

* + - использование учетных записей совместно с друзьями и родственниками;
    - использование программ дешифровки паролей;
    - нарушение нормального процесса обслуживания;
    - использование чужих учетных записей;
    - использование файлов, чужих учетных записей;
    - использование системных ресурсов;
    - копирование защищенных авторскими правами материалов;
    - возможная незаконная деятельность (мошенничество, клевета и др.).
    - вовлечение в деятельность, которая является незаконной.

Пример соглашения, которое могут подписывать студенты факультета,можно посмотреть в приложении(*Приложение 2*).

#### Правила для администраторов

В правилах для администраторов должны быть сформулированы руководящие принципы использования предоставленных привилегий и соблюдения секретности пользовательских данных. Следует особо отметить использование учетных записей строго индивидуально.

#### Правила и методики для экстренных случаев

Следует заблаговременно предусмотреть действия при различных нештатных ситуациях. Например, для аварийных ситуаций следует указать лиц с их телефонами, которых надо предупредить в первую очередь. При выходе из строя программного обеспечения можно указать серийные номера для их самостоятельной переустановки или контактную информацию поставщика программного обеспечения.

#### Безопасность в домене под управлением *Windows*

Преимущества использования групповой политики:

* + - при интеграции со службой ***Active Directory*** позволяет как централизованно, так и децентрализовано управлять параметрами безопасности и настройками пользователей;
    - обладает гибкостью и масштабируемостью, поскольку онаможет быть применена в широком наборе конфигураций системы;
    - предоставляет администратору единый инструмент управления с простым и понятным интерфейсом –***Групповая политика***;
    - обладает высокой степенью надежности и безопасности.

Политика безопасности в сети на основе ***Windows*** хранится в двух типах объектов: *локальный объект групповой политики*; *объект групповой политики домена.*

Для работы с объектами групповой политики используется оснастка ***Групповая политика***, которая может запускаться как для локального компьютера, так и для удаленного.

В структуре объекта групповой политики выделяется 2 раздела

(узла):

* + - *Узел конфигурации компьютера.* Содержит параметры всех политик, определяющих работу компьютера. Они регулируют параметры функционирования операционной системы, определяют права пользователей в системе.
    - *Узел конфигурации пользователя.* Содержит параметры всех политик, определяющих работу пользователя на компьютере. Они регулируют вид рабочего стола и конфигурацию рабочей среды, управляют пользовательскими сценариями входа и выхода.

Каждый из перечисленных выше узлов содержит:

* + - *Административные шаблоны.* Здесь находится групповая политика, определяющая параметры реестра, задающие работу в и внешний вид рабочего стола, компоненты операционной системы и приложений.
    - *Параметры безопасности.* Служит для настройки параметров системы безопасности компьютеров: политик аудита и блокировки учетных записей, права пользователя и т.п.
    - *Установка программ.* Служит для централизованного управления программным обеспечением организации. С его помощью можно задать различные режимы установки новых программ на компьютеры пользователей.
    - *Сценарии.* Сценарии используются для автоматического выполнения набора команд при загрузке операционной системы и в процессе завершения ее работы.
    - *Перенаправление папок.* Позволяет перенаправлять обращение к специальным папкам в сеть.

### Выполнение работы

#### Задание 1. Создайте документы, описывающие политику ИБ для школы, и сохраните их в личной папке:

* 1. Правила административного обслуживания;
  2. Перечень прав и обязанностей пользователей;
  3. Правила для администраторов;
  4. Правила создания «гостевых» учетных записей.

#### Задание 2. Создайте и отредактируйте групповую политику:

* 1. Откройте диалоговое окно оснастки ***Пользователи и компьютеры***

##### (Пуск/Администрирование/Active Direcory – Пользователи и компьютеры).

* 1. Выполните редактирование политики безопасности домена, созданной автоматически:
     + откройте диалоговое окно свойств домена

##### example.edu.ru(контекстное меню/Свойства);

* + - перейдите на вкладку ***Групповая политика***;

*В списке будет расположена политика домена по умолчанию Default Domain Policy.*

* + - откройте диалоговое окно (***Редактор объектов групповой политики***) изменения политики ***Default Domain Policy*** (двойной щелчок по политике);
    - внесите в изменения в политику паролей:

##### перейдите в раздел Политика паролей (Конфигурация компьютера/Конфигурация Windows/Параметры безопасности/Политики учётных записей/Политики паролей);

* + - * установите ***минимальную длину пароля****:* откройте окно изменения параметров пароля (двойной щелчок по надписи ***Мин. длинна пароля***) и введите в поле ***Длина пароля не менее***–*5 (****ОК****)*;
      * отключите ***соответствие пароля требованиям сложности***:
        + откройте диалоговое окно свойств требования сложности (двойной щелок по надписи ***Пароль должен отвечать требованиям сложности***);
        + установите радиокнопку *Отключить*;
        + подтвердите изменения кнопкой ***ОК***;
      * отключите ***возможность использования экранных заставок***:
        + перейдите в раздел **Экран (*Конфигурация пользователя/Административные шаблоны/Экран*)**;
        + откройте диалоговое окно свойств ***Использовать экранные заставки*** и выберите *Отключен*;
        + подтвердите изменения кнопкой ***ОК***.

##### закройте Редактор объектов групповой политики

**(*Консоль/Выход*)**;

* + - закройте диалоговое окно свойств домена кнопкой ***ОК***.
  1. Создайте новую политику для учителей:
     + откройте диалоговое окно свойств домена ***example.edu.ru*(*контекстное меню/Свойства*)** и перейдите на *вкладку* ***Групповая политика***;
     + активизируйте создание новой политики кнопкой ***Создать***;
     + введите название политики –*Teachers*;
     + самостоятельно измените созданную политику, отключив пользователям возможность менять фон рабочего стола.
  2. Закройте редактор объектов групповой политики.

#### Задание 3. Создайте группу и учетные записи пользователей:

* 1. Откройте оснастку ***Пользователи и компьютеры***.
  2. Создайте новую учетную запись пользователя в контейнере ***Students***:
     + откройте диалоговое окно ***Новый объект – Пользователь***, кнопкой

##### Создание нового пользователя в текущем контейнере;

* + - введите данные о пользователе:
      * ***Полное имя пользователя***–*Просто Пользователь*;
      * ***Имя входа пользователя (логин)***–*JustUser*;
      * Подтвердите введенные данные кнопкой ***Далее***.
    - установите пароль для пользователя:
      * введите в поле ***Пароль***–*User1234*;
      * введите в поле ***Подтверждение***–*User1234*;
      * установите флажок *Срок действия пароля не ограничен*;
      * завершите ввод пароля кнопкой ***Далее***.

*В правой области отобразится запись, соответствующая созданному пользователю.*

* 1. Введите более полную информацию о пользователе:
     + откройте диалоговое окно свойств пользователя (двойной щелчок по надписи ***Просто пользователь***);
     + введите в поле ***Описание***–*это тестовый пользователь*;
     + введите в поле ***Комната***– номер кабинета, в котором проходит занятие –*316*;
     + введите в поле ***Телефон***–<номер своего мобильного телефона>;
     + укажите адресные данные на вкладке ***Адрес***;
     + укажите несколько дополнительных телефонов пользователя на вкладке ***Телефоны***;
     + завершите изменение данных пользователя кнопкой ***ОК***.
  2. Создайте группу ***group1*** в контейнере ***Students***:
     + откройте диалоговое окно создания групп (***контекстное меню/Создать/Группа***);
     + введите имя группы**–***group1*;
     + завершите создание группы кнопкой***ОК*.**
  3. Задайте дополнительную информацию для группы ***group1***:
     + откройте диалоговое окно ***свойств группы*** (*двойной щелчок по надписи group1*);
     + введите в поле ***Описание***–*Это тестовая группа*;
     + завершите изменение данных группы кнопкой ***ОК***.
  4. Включите созданного ранее пользователя ***Просто пользователь(JustUser)*** в группу ***group1***:
     + откройтедиалоговое окно свойств пользователя (*двойной щелчок по записи пользователя*);
     + перейдитена вкладку ***Член групп***;
     + откройтедиалоговое окно выбора группы кнопкой ***Добавить***;
     + введите название группы –*group1*;
     + завершитедобавления пользователя в группу кнопкой ***ОК***.
     + закройте диалоговое окно свойств пользователя кнопкой ***ОК***.
  5. Выполните выход из системы с повторным входом для активации изменений в политике безопасности. *Изменения в политике паролей вступят в силу только после выхода из системы и повторного входа в неё.*
  6. Измените пароль созданного ранее пользователя:
     + активизируйте раздел ***Students***;
     + задайте новый, более простой пароль пользователю *Просто пользователь*:
       - откройте диалоговое окно задания пароль (***контекстное меню/Смена пароля***);
       - введите в поле ***Пароль***–*123*;
       - введите в пол ***Подтверждение пароля***–*123*;

*Обратите внимание, что сообщений о слишком простом пароле не было.*

* 1. Исключите созданного ранее пользователя из группы ***group1:***
     + откройте диалоговое окно ***свойств группы***;
     + перейдите на вкладку ***Члены группы***;
     + выделите в списке удаляемого пользователя и щелкните по кнопке

##### Удалить;

* + - подтвердите удаление кнопкой ***Да***;
    - закройте диалоговое окно свойств группы кнопкой ***ОК***.
  1. Включите созданного ранее пользователя в администраторы домена:
     + откройтедиалоговое окно свойств пользователя ***Просто пользователь***;
     + перейдите на вкладку ***Член групп*** и щелкните ***Добавить***;
     + введите в поле ***Администраторы домена***;
     + завершите добавление в группу кнопкой ***ОК***;
     + закройте окно свойств пользователя кнопкой ***ОК***.
  2. Закройте оснастку ***Пользователи и компьютеры.***

#### Задание 4. Самостоятельно создайте учетную запись администратора домена.

**Задание 5. Самостоятельно создайте в домене контейнер для вашей группы и внесите в него всех студентов из вашей группы.**

#### Задание 6. Самостоятельно измените политику безопасности домена:

* 1. Запретите изменение рабочего стола.
  2. Установите длину пароля не менее 8 символов.

**Задание 7. Самостоятельно создайте политику информационной безопасности для учеников школы.**

## Лабораторная работа 2.2.

**Работа с серверами *HTTP*и *FTP***

**Цель:** научиться устанавливать и просматривать ***Active Directory***, научится подключать компьютеры к домену.

#### Средства для выполнения работы:

* + - **аппаратные:** компьютер;
    - **программные:** Виртуальная машина: ***VM-2***; Сервер ***FTP: Filezilla***; Образ установочного диска: ***win2003-1.iso, win2003-2.iso.***

***Теоретические сведения***

*Сервер*(в информационных технологиях)– программный компонент вычислительной системы, выполняющий сервисные функции по запросу

клиента, предоставляя ему доступ к определённым ресурсам.

*Сервер* (в локальных вычислительных сетях) – специализированная ЭВМ, управляющая использованием разделяемых между терминалами сети дорогостоящих ресурсов системы.

*Сервер*сети (*Server*) – это компьютер, подключенный к сети и предоставляющий пользователям сети определенные услуги, например, хранение данных общего пользования, печать заданий, обработка запроса к СУБД, удаленная обработка заданий и т.д. Сервер работает по заданиям клиентов. После выполнения задания сервер посылает полученные результаты клиенту, инициировавшему это задание.

Обычно связь между клиентом и сервером поддерживается посредством передачи сообщений, и при этом используется определенный протокол для кодирования запросов клиента и ответов сервера.

В сетевых технологиях используются различные виды серверов, в частности, такие как:***FTP****; Файловый;* ***Web****; Телефонный; Терминальный; Факс; Суперсервер* и т.п.

*Файл-серверы*представляют собой серверы для обеспечения доступа к файлам на диске сервера. Прежде всего, это серверы передачи файлов по заказу, по протоколам ***FTP*** и ***HTTP***. Протокол ***HTTP*** ориентирован на передачу текстовых файлов, но серверы могут отдавать в качестве запрошенных файлов и произвольные данные, например, динамически созданные веб-страницы, картинки, музыку и т. п. Другие серверы позволяют монтировать дисковые разделы сервера в дисковое пространство клиента и полноценно работать с файлами на них. Это позволяют серверы протоколов ***NFS*** и ***SMB***. Серверы ***NFS*** и ***SMB*** работают через интерфейс ***RPC***.

Недостатки файл-серверной системы:

* + - * очень большая нагрузка на сеть, повышенные требования к пропускной способности. На практике это делает практически невозможной одновременную работу большого числа пользователей с большими объемами данных;
      * обработка данных осуществляется на компьютере пользователей. Это влечет повышенные требования к аппаратному обеспечению каждого пользователя. Чем больше пользователей, тем больше денег придется потратить на оснащение их компьютеров;
      * блокировка данных при редактировании одним пользователем

делает невозможной работу с этими данными других пользователей;

* + - * безопасность. Для обеспечения возможности работы с такой системой Вам будет необходимо дать каждому пользователю полный доступ к целому файлу, в котором его может интересовать только одно поле

Файловый сервер выполняет следующие функции: хранение данных и их архивирование; согласование изменений данных, выполняемых разными пользователями; передача данных.

***FTP****-сервер*– это понятие, за которым скрывается обычный компьютер. Но так как он содержит общедоступные файлы и настроен на поддержку протокола ***FTP***, то его называют сервером – поставщиком информации. ***FTP****-клиент*– это сервисная программа, с помощью которой можно произвести соединение с ***FTP*** сервером. Обычно эта программа имеет командную строку, но некоторые имеют оконный интерфейс и не требуют запоминания команд.

***WEB****-сервер* необходим для обслуживания ***WEB***-страниц вашего сайта. Доступ к ***WEB***-серверу имеет пять уровней:

1. *Общедоступный* с возможностью только чтения всех ***URL*** за исключением тех, что помещены в каталогах ***/private***;
2. *Доступ сотрудников организации*, которой принадлежит сервер. Здесь также допустимо только чтение, но доступны и секции каталога ***/private***;
3. *Разработчики****WEB***-*сервера*. Имеют возможность модифицировать содержимое сервера, инсталлировать ***CGI***- скрипты, прерывать работу сервера.
4. *Администраторыузла* (*сервера*). Имеют те же привилегии, что и разработчики, но могут также реконфигурировать сервер и определять категорию доступа.
5. *Системныеадминистраторы*. Имеют идентичные привилегии с администраторами сервера.

***Оснастка I****nternet* ***I****nformation* ***S****ervice* ***(IIS)*** обеспечивает средства управления сервером для контроля над доступом и содержимым веб-узлов и узлов ***FTP***. Например, разработчикам это средство позволит выполнить доскональную проверку работы узла перед окончательной загрузкой на сервер интрасети организации или Интернета. Оснастка ***IIS*** имеет следующие особенности:

* + дополнительные параметры настройки сервера, в частности, для управления узлом ***FTP***, независимого выполнения приложений, настройки типов ***MIME*** и назначения дополнительных средств обработки сценариев;
  + мастер создания виртуальных каталогов;
  + возможность управления установками

##### InternetInformationServices в сети.

На сегодняшний день существует огромное множество программного обеспечения для работы с протоколом ***FTP*** под все операционные системы.

Все это множество программного обеспечения можно разделить на две части: *серверное ПО* и *клиентское ПО*.

*Серверное ПО* служит для создания и управления ***FTP***-сервером. *Клиентское ПО* используется для просмотра ресурсов на ***FTP***-сервере. Этот класс программ призван обеспечить комфортную работу с удаленными ресурсами. Сюда относятся такие программы как:

* + ***ftp.exe***– стандартное приложение ***Windows***;
  + ***FileZilla***– мощный ***FTP***-клиент с открытым исходным кодом (т.е. вы можете добавить что-нибудь новое в эту программу самостоятельно);
  + ***RigthFTP, CuteFTP***– графические ***FTP***-клиенты;
  + ***Total commander*** (или любой другой с интерфейсом

***NortonCommander***)– имеет встроенный ***FTP***клиент;

* + ***Explorer.exe***– стандартное приложение ***Windows***;
  + Любой браузер.

### Выполнение работы

#### Задание 1. Подготовьте файловый сервер:

* 1. Подключите к виртуальной машине ***VM-2*** образ установочного диска

##### win2003-2.iso.

* 1. Запустите виртуальную машину ***VM-2***.
  2. Добавьте новую **роль** серверу –*Файл-сервер*:
     + откройте диалоговое окно ***Управление данным сервером***

##### (Пуск/администрирование/Управление Данным Сервером);

* + - активизируйте добавление ролей кнопкой ***Добавить или удалить роль***;
    - выберите ***Файловый сервер*** и щелкните ***Далее***;
    - установите параметры файлового сервера:
      * Предоставить доступ ***UNIX***-системам к файлам;
      * Предоставить доступ ***Apple***–системам к файлам;
      * подтвердите введенные параметры кнопкой ***Далее***;
    - запустите установку роли сервера кнопкой ***Далее***.
  1. Перезагрузите виртуальный компьютер кнопкой ***Перезегрузить***.
  2. Откройте диалоговое окно ***Настройки файловогосервера* (*Пуск/ администрирование/Управление Данным Сервером/Управление этим файловым сервером*)**.
  3. Установите стандартные квоты использования места на диске:
     + установите флажок *Установить дисковые квоты по умолчанию для новых пользователей данного сервера*;
     + укажите ***размер квот***–*50Мб*;
     + установите ***предупреждение о квоте***–*40Мб*;
     + установите флажок *Не выделять место на диске при превышении дискового пространства*;
     + завершите ввод стандартных квот кнопкой ***Далее***.
  4. Откажитесь от включения службы индексирования.
  5. Укажите папку на сервере, для хранения файлов, например

##### C:\Documents and settings\Администратор\Рабочий стол\PUB.

* 1. Далее мастер установки завершит свою работу. Попробуйте теперь зайти на созданную вами сетевую папку с другого компьютера сети. Обратите внимание на способ подключения. Попробуйте заполнить папку для превышения квоты.

#### Задание 2. Настройте *Web*-сервер:

##### Установите Internet Information Service(IIS) (Пуск/администрирование/Управление Данным Сервером/Сервер приложений IIS):

* 1. Подготовьте тестовую страницу:создайте временную страницу, вызываемую по умолчанию: наберите в **Блокноте** и сохраните в файле с именем ***Default.html*** в каталоге ***\Inetpub\wwwroot***.

<HTML>

<HEAD>

<TITLE></TITLE>

</HEAD>

<BODY>

<H1 align=center>Тестовая страница</H1>

<P align=center>

<FONT color=green>

На этом месте будет размещена страница организации.<BR> В настоящий момент сайт находится в разработке.

</FONT>

</P>

</BODY>

</HTML>

* 1. Настройте ***Web***-сервер:
     + откройте консоль управления сервером ***IIS* (*Пуск/ Администрирование/Управление Данным Сервером/Управление этим сервером приложений*)**;
     + перейдите к ***web***-узлу, заданному по умолчанию (***Диспетчер служб IIS/Веб-узлы/Веб-узел по умолчанию***);
     + откройте диалоговое окно ***Cвойствaузла по умолчанию***

##### (контекстное меню/Свойства);

* + - добавьте страницу по умолчанию:
      * перейдите на вкладку ***Документы***;
      * установите флажок *Задать страницу содержания по умолчанию*;
      * откройте окно добавления кнопкой ***Добавить***;
      * введите в поле ***Default.html***;
      * подтвердите добавление кнопкой ***ОК***.
    - закройте окно свойств кнопкой ***ОК***.
  1. Проверьте настройку ***Web****-*сервера:
     + на вашем компьютере откройте ***Internet Explorer***

##### (Пуск/Программы/Internet Explorer);

* + - наберите в адресной строке [*http://127.0.01/*;](http://127.0.01/%3B)
    - сделайте скриншот экрана и сохраните его в своей папке.

#### Задание 3. Установите и настройте сервер *FTP*:

* 1. Установите ***FTP* -**сервер***FileZilla***.
  2. Запустите ***FileZilla Server Interface***.
  3. Ограничьте количество одновременных подключений к серверу:
     + откройте окно настройки сервера (***Edit/Settings***);
     + перейдите в раздел ***General Settings*** (Общие настройки);
     + введитевполе***Max.number of users***–*2*;
  4. Установите текст приветствия:
     + перейдите в раздел ***Welcome message***;
     + введите в поле ***Custom welcome message***–*Добро пожаловать на мой сервер*;
     + установите ограничения по скорости:
       - перейдите в раздел ***Speed Limits*** (Ограничения скорости);
       - включите использование правил ограничения скорости радиокнопкой *Use Speed Limit rules*;
       - добавьте ограничение по скорости *не более 3 Кб/с в понедельник:*
         * откройте окно задания параметров ограничений кнопкой ***Add***

(*Добавить*);

* + - * + сбросьте все флажки кроме *Monday* (*Понедельник*);
        + введите в поле ***Speed***–*3*;
        + подтвердите ввод данных кнопкой ***ОК***;
      * примените параметры кнопкой ***ОК***.
    - создайте группы пользователей ***FTP***-сервера:
      * откройте диалоговое окно ***добавления групп*** кнопкой на панели инструментов;
      * активируйте добавление групп кнопкой ***Add*** (*Добавить*);
      * введите ***имя группы***, например *Students* (***ОК***);
      * задайте общую папку для созданной группы:
        + перейдите в раздел ***Shared Folders*** (*Общиепапки*);
        + активируйте добавление папок кнопкой ***Add*** (*Добавить*);
        + укажите общую папку, например ***C:\Documents and settings\Администратор\Рабочий стол*** и подтвердите выбор кнопкой ***ОК***;
        + разрешите чтение и удаление содержимого общей папки – установите флажок ***Write*** и***Delete***;
      * завершите добавление групп пользователей кнопкой ***ОК***.
    - добавьте нового пользователя:
      * откройте диалоговое окно добавления пользователей кнопкой на панели инструментов;
      * активируйте добавление пользователей кнопкой ***Add*** (Добавить);
      * введите ***имя группы***, например *justuser*;
      * выберите в списке ***User should be member of the following group***

созданную ранее группу и подтвердите создание пользователя

кнопкой ***ОК***;

* + - * установите пароль для созданного пользователя:
        + перейдите на вкладку ***General*** (Общие);
        + введите в поле ***Password*** новый пароль, например *123*;
      * завершите добавление групп пользователей кнопкой ***ОК***.
    - проверьте работу сервер:
      * запустите командную строку (***Пуск/Программы/Стандартные/Командная строка***);
      * введите команду для подключения к ***FTP***-серверу на текущем компьютере: *FTP 127.0.0.1*
      * введите имя пользователя –*justuser* (***Enter***);
      * введите пароль –*123* (***Enter***);
      * просмотрите содержимое домашней папки: ***DIR***
      * отключитесь от сервера: ***QUIT***
      * закройте командную строку.
    - закройте интерфейс управления ***FTP****-сервером*.

#### Задание 4. Самостоятельно создайте небольшой *web*-сайт школы с помощью любых инструментов и разместите на ранее запущенном *web*-сервере.

**Задание 5. Создайте несколько группу и пользователей с разными домашними папками на *FTP*-сервере.**

## Примерные тестовые задания к модулю 2

1. Комплекс мероприятий, направленных на обеспечение информационной безопасности:
   * *защита информации;*
   * *информационная защита;*
   * *безопасность информации;*
   * *информационная безопасность.*
2. Преимущество использования стандартных правил, регламентирующих работу пользователей:
   * *рутинные задачи всегда выполняются одинаково;*
   * *уменьшение вероятности появления ошибок;*
   * *работа по инструкциям выполняется гораздо быстрее;*
   * *все выше перечисленное.*
3. Политика безопасности сети на основе ОС***Windows*** хранится в следующих типах объектов:

*локальный объект групповой политики; глобальный объект групповой политики;*

*объект групповой политики домена.*

1. Параметры узла ***Конфигурация компьютера*** в редакторе объектов групповой политики определяют работу:
   * *пользователя;*
   * *компьютера;*
   * *операционной системы;*
   * *все выше перечисленное.*

## Контрольные вопросы к модулю 2

1.Информационная безопасность. 2.Защита информации

3.Рекомендации по реализации информационной безопасности. 4.Безопасность в домене под управлением ОС ***Windows***.

1. Объекты групповой политики.
2. ***Web***-сервер: назначение, установка, настройка. 7.***FTP***-сервер:назначение, установка, настройка.

# Модуль 3.

# Обеспечение информационной безопасности

**Цель:** Познакомиться с основными принципами защиты информации в компьютерных сетях.

**Результат:**уметь осуществлять мониторинг состояния элементов сети: общих ресурсов, производительности системы;уметь исследовать удаленную систему: просматривать сетевые ресурсы локальной сети, анализировать удаленный компьютер на наличие открытых портов, блокировать открытые порты с помощью брандмауэра; уметь устанавливать сетевую антивирусную защиту: серверную и клиентскую части.

#### План освоения модуля:

1. Изучите следующие темы в указанных источниках:
   * *Цели, функции и задачи защиты информации в сетях: возможные угрозы, виды информационных атак;*
   * *Информационная безопасность в компьютерных сетях: уровни защиты; сервисы безопасности; проблемы защиты в беспроводных сетях;*
   * *Мониторинг сети: просмотр системных событий; работа с журналами (просмотр, настройка параметров); мониторинг производительности компьютера;*
   * *Работа с портами: категории портов; присвоение имени порту; SSL*

*– протокол защиты сокетов; сканирование портов;*

* + *Антивирусная защита: установка серверной и клиентской частей антивирусного пакета; конфигурирование сервера; планирование антивирусной проверки; настройка клиентов.*

1. Выполните и представьте преподавателю лабораторные работы:
   * ЛР 3.1. *Мониторинг состояния элементов сети.*
   * ЛР. 3.2. *Исследование удаленной системы для выявления уязвимостей.*
   * ЛР.3.3. *Сетевая антивирусная защита.* **III.**Выполните самостоятельные задания к модулю. **IV.**Выполните тестовые задания к модулю. **V.**Защитите модуль по контрольным вопросам. **Литература:**
2. Холме Дэн. Управление и поддержка Microsoft Windows Server 2003. Учебный курс MCSA/MCSE / Пер. с англ. / Холме Дэн [и др.]; под ред

Холме Дэн – М.: Издательско-торговый доме «Русская Редакция», 2004.

– 448 стр.: ил. (Гл. 12).

1. Ханникат Дж. Знакомство с Microsoft Windows Server 2003 / Пер. с англ. / Дж Ханникат– М.: Издательско-торговый дом «Русская Редакция», 2003.

– 464 с.: ил. (Гл. 4).

1. УильямР. Станек. Microsoft Windows Server 2003. Справочник администратора / Пер. с англ./ УильямР. Станек– М.: Издательско- торговый доме «Русская Редакция», 2003. – 640 с.: ил. (Гл.3).

# Лабораторная работа 3.1.

**Мониторинг состояния элементов сети**

**Цель:**научится использовать операционную систему ***Windows***с целью мониторинга состояния компонентов компьютерной сети.

#### Средства для выполнения работы:

* + **аппаратные:** компьютер с установленной ОС ***Windows XP.***
  + **программные:** приложения ВМ: ***VirtualBox***; виртуальные машины:

***VM-1, VM-2.***

***Теоретические сведения***

Системная служба***Журнал событий*** запускается по умолчанию при загрузке операционной системы и регистрирует события в трех журналах (в зависимости от роли сервера журналов может быть больше):

* + - ***Приложение*** (содержит информацию об изменении конфигурации в системе);
    - ***Система*** (содержит данные о системных событиях);
    - ***Безопасность*** (содержит записи о событиях входа в систему и о доступе к ресурсам).

Для мониторинга и оптимизации работы компьютера в системах ***Windows Server 2003*** имеется несколько инструментов, позволяющих администратору следить за работой любых компонентов системы и конфигурировать ее оптимальным образом:

* + - ***Task Manager*** *(****Диспетчерзадач****)* служит для просмотра текущих данных о производительности системы. В этой утилите основными являются три индикатора: использование процессора, использование виртуальной памяти и запущенные

процессы и программы;

* + - ***Оснастка Event Viewer*** *(****Просмотрсобытий****)*позволяет просматривать журналы событий, генерируемых приложениями, службой безопасности и системой;
    - ***Performance*** *(****Производительность)***– обновленная оснастка систем ***Windows XP*** и ***Windows Server 2003,*** аналог утилиты ***Performance Monitor*** в ***Windows NT 4.0.*** Оснастка ***Performance*** включает в себя два компонента: ***ActiveX-элемент System Monitor*** и оснастку ***Performance Logs and Alerts****(Оповещения и журналы безопасности).* Графические средства ***System Monitor*** позволяют визуально отслеживать изменение производительности системы. С помощью ***System Monitor*** можно одновременно просматривать данные с нескольких компьютеров в виде динамических диаграмм, на которых отображается текущее состояние системы и показания счетчиков. Оснастка ***PerformanceLogsandAlerts*** позволяет создавать отчеты на основе текущих данных производительности или информации из журналов. При превышении счетчиками заданного значения или уменьшения нижеуказанного уровня данная оснастка посредством службы сообщений (***Messenger***) посылает оповещения пользователю.

***Диспетчер задач*** можно использовать для отслеживания ключевых индикаторов производительности компьютера, он позволяет определять статус запущенных программ и завершать приложения, которые перестали отвечать на запросы системы. С помощью диспетчера задач можно отслеживать активность запущенных процессов по 25 параметрам и просматривать графики использования процессора и памяти.В ***Windows Server 2003*** диспетчер задач содержит пять вкладок/индикаторов. Ниже перечислены эти вкладки и указано их назначение.

* + - ***Applications*** *(****Приложения****)*– показывает статус приложений, запущенных на компьютере.
    - ***Processes*** *(****Процессы****)*– содержит информацию о процессах, запущенных на компьютере.
    - ***Performance*** *(****Быстродействие****)*– отображает динамическое состояние производительности компьютера, включая степень использования памяти и процессора.
    - ***Networking*** *(****Сеть****)*– показывает степень загрузки сети.

Индикатор отображается только при наличии на компьютере сетевой карты.

* + - ***Users*** *(****Пользователи****)*– содержит список зарегистрированных пользователей. Эти пользователи могут регистрироваться локально (с консоли) или являться клиентами служб ***TerminalServices***, подключенных с использованием технологий ***Terminal Server, RemoteAccess*** или ***Remote Assistant.***

В операционных системах ***Windows*** событием называется любое значительное "происшествие" в работе системы или приложения, о котором следует уведомить пользователей. В случае возникновения критических событий, таких как переполнение диска сервера или неполадки с электропитанием, на экран монитора будет выведено соответствующее сообщение. Остальные события, которые не требуют немедленных действий от пользователя, регистрируются в системных журналах. Служба регистрации событий в системных журналах активизируется автоматически при каждом запуске системы W***i***ndows ***Server2003***.

**Оснастка *Event Viewer***

В системе ***Windows Server 2003*** для просмотра системных журналов можно использовать оснастку ***Event Viewer*** *(****Просмотрсобытий****)*(группа ***Administr-tive Tools*** *(****Администрирование****)*на панели управления). Эту оснастку можно также запустить из окна оснастки ***Computer Management*** *(****Управлениекомпьютером****)*.

Оснастку ***Event Viewer*** можно также открыть с помощью команды ***Пуск/Программы/Администрирование/Просмотр событий***. С помощью оснастки ***Event Viewer*** можно просматривать три типа стандартных (основных) журналов:

* + - ***Журналприложений*** *(****Application log****)*– фиксирует события, зарегистрированные приложениями. Например, текстовый редактор может зарегистрировать в данном журнале ошибку при открытии файла;
    - ***Журналсистемы*** *(****System*** *l****o****g)*– записывает события, которые регистрируются системными компонентами ***Windows Server 2003.*** Например, в системный журнал записываются такие события, как сбой в процессе загрузки драйвера или другого системного компонента при запуске системы;
    - ***Журналбезопасности*** *(****Securitylog****)*– содержит записи, связанные с системой безопасности. С помощью этого журнала можно отслеживать изменения в системе безопасности и идентифицировать бреши в защите. В данном журнале можно регистрировать попытки входа в систему. Для просмотра журнала необходимо иметь права администратора. По умолчанию регистрация событий в журнале безопасности отключена.

Помимо стандартных журналов, на контроллере домена – могут быть и другие, создаваемые различными службами (например, ***Active Directory, DNS, File Replication Service*** и т. д.). Работа с такими журналами ничем не отличается от процедур просмотра стандартных журналов.

Журнал системы безопасности может просматривать только пользователь с правами системного администратора. По умолчанию регистрация событий в данном журнале отключена. Для запуска регистрации необходимо установить политику аудита.

Типы событий, регистрирующихся в журналах:

* + - ***Error*** *(****Ошибка****)*– событие регистрируется в случае возникновения серьезного события (такого как потеря данных или функциональных возможностей). Событие данного типа будет зарегистрировано, если невозможно загрузить какой-либо из сервисов в ходе запуска системы.
    - ***Warning*** *(****Предупреждение****)*– событие не является серьезным, но может привести к возникновению проблем в будущем. Например, если недостаточно дискового пространства, то будет зарегистрировано предупреждение.
    - ***Information*** *(****Уведомление****)*– значимое событие, которое свидетельствует об успешном завершении операции приложением, драйвером или сервисом. Такое событие может, например, зарегистрировать успешно загрузившийся сетевой драйвер.
    - ***SuccessAudit*** *(****Аудитуспехов****)*– событие, связанное с безопасностью системы. Примером такого события является успешная попытка регистрации пользователя в системе.
    - ***FailureAudit*** *(****Аудитотказов****)*– событие связано с безопасностью системы. Например, такое событие будет зарегистрировано, если попытка доступа пользователя к

сетевому диску закончилась неудачей.

Информация о событиях содержит следующие параметры:

* + - ***Параметр***–описание;
    - ***Туре*** *(****Тип****)*– тип события;
    - ***Date*** *(****Дата****)*–дата генерации события;
    - ***Time*** *(****Время****)*–время регистрации события;
    - ***Source*** *(****Источник****)*–источник (имя программы, системного компонента или компонента приложения), который привел к регистрации события;
    - ***Category*** *(****Категория****)*–классификация события по источнику, вызвавшему его появление;
    - ***Event ID*** *(****Событие****)*–идентификатор события;
    - ***User*** *(****Пользователь****)*–учетная запись пользователя, от имени которой производились действия, вызвавшие генерацию события;
    - ***Computer*** *(****Компьютер****)*–компьютер, на котором зарегистрировано событие.

Для просмотра дополнительной информации о событии нужно выбрать в меню ***Action*** *(****Действие****)* пункт ***Properties*** *(****Свойства****)*(либо щелкнуть дважды кнопкой мыши на строке в списке событий). На панели ***Description*** *(****Описание****)* приводится общая информация о событии. На панели ***Data****(****Данные****)* отображаются двоичные данные, которые могут быть представлены как ***Bytes*** *(****Байты****)* или как ***Words*** *(****Слова****)*. Эти данные могут быть интерпретированы опытным программистом или техническим специалистом службы поддержки, знакомым с исходным кодом приложения.

### Выполнение работы

#### Задание 1. Просмотрите сетевые подключения к компьютеру:

 Подготовьтесь к выполнению задания:

* запустите виртуальную машину ***VM-2***;
* создайте на рабочем столе общую папку ***MyFolder*** и разместите в ней документ с именем ***CompName.doc***, содержащий сведения об ***IP***-адресе и символьном имени компьютера;
* переключитесь в обычный компьютер и откройте документ

***CompName.doc***. Для этого воспользуйтесь ***Сетевым окружением***.

*Все остальные операции следует выполнять на виртуальном компьютере, где был создан файл* ***CompName.doc****.*

 Переключитесь в виртуальную машину ***VM-2***.

 Откройте оснастку ***Управление компьютером* (*контекстное меню значка Мой компьютер/Управление*)**.

 Разверните раздел ***Общие ресурсы***. *Здесь перечислены все опубликованные (общие) ресурсы вашего компьютера.*

 Отключите общий доступ к созданному ранее ресурсу ***MyFolder***. Для этого в контекстном меню ресурса выберите *Прекратить общий доступ*.

 Откройте раздел ***Сеансы***. *Здесь перечислены все открытые сеансы, т.е. какие пользователи и на каких компьютерах сейчас подключены к вашему компьютеру. Если вызвать контекстное меню раздела, то можно сразу отключить все сеансы.*

 Закройте открытый файл. Для этого перейдите в раздел ***Открытые файлы*** и в контекстном меню файла выберите *Закрыть открытый файл*.

#### Задание 2. Отключите пользователя с отправкой ему уведомления:

* 1. Подготовьтесь к выполнению задания. Для этого откройте на обычном компьютере файл ***CompName.doc***, расположенный в виртуальной машине ***VM-2***.
  2. Переключитесь в виртуальную машину;
  3. Откройте оснастку ***Управление компьютером***.
  4. Выполните для элемента ***Общие ресурсы*** команду ***контекстного меню/ Все задачи/Отправка сообщения консоли***.
  5. Введите в поле ***Сообщение*** текст выводимого сообщения: *Вы сейчас будете отключены от общего ресурса* и щелкните по кнопке ***Отправить***.
  6. Закройте окно ***Отправка сообщений консоли***.
  7. Для раздела ***Открытые файлы*** выполните команду контекстного меню ***Отключить все открытые файлы***.
  8. Просмотрите пришедшее сообщение.

#### Задание 3. Просмотрите сведения о процессах системы и ее состоянии:

* 1. Просмотрите информацию о производительности системы:
     + откройте окно диспетчера задач (***CTRL+SHIFT+ESC***);
     + перейдите на вкладку ***Процессы***;
     + просмотрите список и найдите процесс, использующий наибольшее количество памяти;
     + перейдите на вкладку ***Быстродействие*** и посмотрите количество выделенной памяти в соответствующем поле;
     + перейдите на вкладку ***Сеть*** и ознакомьтесь с информацией о производительности сети;
     + перейдите на вкладку ***Пользователи*** просмотрите информацию о пользователях, зарегистрированных в системе.
  2. Соберите с помощью ***Диспетчера задач*** информацию, указанную ниже:

Количество запущенных приложений. Имя процесса, занимающего больше всех оперативной памяти. Количество выделенной памяти. Имя пользователя зарегистрированного в системе.

* 1. Сохраните полученную информацию в личном каталоге в файле

формата ***ODT***.

#### Задание 4. Выполните мониторинг сетевых подключений:

* 1. Запустите оснастку ***Производительность***

##### (Пуск/Администрирование/Производительность).

* 1. Удалите все счетчики из системного монитора:
     + активируйте ***Системный монитор*** в левой части окна

##### Производительность;

* + - откройте диалоговое окно свойств ***Системного монитора*** кнопкой

##### Свойства ;

* + - перейдите на вкладку ***Данные***;
    - выделите один из счетчиков и удалите его кнопкой ***Удалить***;
    - аналогично удалите все остальные счетчики.
  1. Добавьте счетчик активных подключений ***TCP***:
     + активируйте добавление счетчика кнопкой ***Добавить***;
     + выберите в раскрывающемся списке ***Объект***–*TCPv4*;
     + выберите в списке ***Выбрать счетчик из списка***–*Активных подключений*;
     + просмотрите информацию о добавляемом счетчике, щелкнув по кнопке ***Объяснение***;
     + добавьте счетчик кнопкой ***Добавить***.
     + самостоятельно добавьте счетчик ***Всего байт/сек*** для объекта

##### Сервер;

* + - закройте окно добавления счетчиков кнопкой ***Закрыть***.
  1. Закройте диалоговое окно свойств ***Системного монитора*** кнопкой

***ОК***.

*В правой области начнет отображаться информация добавленных счетчиков в графическом виде.*

* 1. Переключите вид отображения информации счетчиков в текстовый вид кнопкой ***Просмотр отчета*** на панели инструментов.
  2. Настройте автоматический сбор информации о загруженности сервера в период **с** 8.00 **до** 17.00:
     + активируйте раздел ***Журналы счетчиков***в левой части окна

##### Производительность;

* + - активируйте создание новых параметров журнала (***Действие/Новые параметры журнала***);
    - введите название журнала в поле ***Имя***–*Дневная нагрузка* и подтвердите кнопкой ***ОК***;
    - добавьте объект ***Сервер***:
      * откройте окно добавления объектов кнопкой ***Добавить объект***;
      * выделите в списке ***Объект***–*Сервер*;
      * добавьте объект кнопкой ***Добавить***;
      * закройте окно добавления объектов кнопкой ***Закрыть***;
    - аналогично добавьте объект ***Сетевой интерфейс***;
    - установите время сбора данных:
      * перейдите на вкладку ***Расписание***;
      * установите в поле ***Время***–*8.00*;
      * установите время остановки –*17.00*;
    - закройте диалоговое окно параметров нового журнала кнопкой ***ОК***. *В правой части окна* ***Производительность*** *появится новый журнал. Просмотреть результат работы журнала можно в папке* ***C:\perflogs****.*
  1. Настройте оповещение, если количество доступной памяти станет менее ***100 Мб***.
     + активируйте раздел ***Оповещения*** в левой части оснастки

##### Производительность;

* + - откройте диалоговое окно ***Новые параметры оповещения***

##### (Действия/Новые параметры оповещения);

* + - введите ***имя новых параметров***–*Мало памяти* и подтвердите ввод кнопкой ***ОК***;
    - введите в поле ***Комментарий***–*Оповещение о малом количестве оперативной памяти*;
    - добавьте счетчик ***Доступно МБ*** для объекта ***Память***;
    - введите в поле ***Порог*** значение, при котором должно срабатывать оповещение –*100*;
    - задайте действие, которое должно срабатывать при установленном условии:
      * перейдите на вкладку ***Действие***;
      * установите флажок *Послать сетевоe сообщение* и введите в поле текст сообщения –*Слишком мало памяти*;
    - завершите настройку оповещения кнопкой ***ОК***.

#### Задание 5. Выполните просмотр событий:

* 1. Откройте оснастку ***Управление компьютером***

##### (Пуск/Администрирование/Управление компьютером).

* 1. Разверните узел ***Просмотр событий***.
  2. Просмотрите события ***Службы безопасности***:
     + перейдите в раздел ***Безопасность*** в левой части оснастки

##### Управление компьютером;

*Справа отобразятся все события данной службы.*

* + - выполните фильтрацию событий только для пользователя ***JustUser***:
      * откройте диалоговое окно свойств раздела ***Безопасность***

##### (Действия/Свойства);

* + - * перейдите на вкладку ***Фильтр***;
      * введите в поле ***Пользователь*** имя пользователя, для которого необходимо отобразить события, например *JustUser*;
      * самостоятельно установите в полях ***С*** и ***ДО*** сегодняшний день;
      * подтвердите применение фильтра кнопкой ***ОК***.
    - просмотрите событие ***Доступ к службе каталогов***:
      * найдите указанное событие в правой части окна оснастки

##### Управление компьютером;

* + - * откройте диалоговое ***окно свойств*** выбранного события (***Действия/Свойства***);
      * ознакомьтесь с информацией события, найдите имя компьютера, к которому осуществлялся доступ;
      * закройте диалоговое окно свойств события кнопкой ***ОК***.
    - снимите установленный ранее фильтр:
      * откройте диалоговое ***окно свойств*** раздела ***Безопасность***;
      * прейдите на вкладку ***Фильтр***;
      * восстановите стандартные значения кнопкой ***Восстановить умолчания***;
      * закройте диалоговое окно свойств раздела ***Безопасность*** кнопкой

***ОК***.

* 1. Экспортируйте список событий для раздела ***DNS-сервер*** в текстовый файл:
     + активизируйте раздел ***DNS-сервер***;

##### откройте диалоговое окно экспорта (Действие/Экспортировать список);

* + - введите *имя файла* в поле ***Имя***;
    - сохраните файл кнопкой ***Сохранить***;
    - просмотрите сохраненный файл стандартной программой ***Блокнот***.

**Задание 6. Самостоятельно экспортируйте в текстовый файл данные о пользователе *Администратор* из раздела *Безопасность*.**

## Лабораторная работа 3.2.

## Исследование удаленной системы для выявления уязвимостей

**Цель:** научиться анализировать сетевые компьютеры и выявлять потенциальные опасности в их настройках.

#### Средства для выполнения работы:

* **аппаратные:** компьютер с установленной ОС ***Windows XP***;
* **программные:** сканер локальной сети ***NetView***; сканер портов ***nmap***; монитор портов ***tcpview***; комплекс утилит ***IP-Tools*** для работы со стеком ***TCP/IP***;
* **информационные** (у преподавателя): ***IP***-адрес контроллера домена;

***IP***-адрес компьютера для сканирования.

***Теоретические сведения***

В сети Интернет применяют два основных протокола транспортного уровня: ***TCP***, ориентированный на создание соединений, и ***UDP*** (***U****ser* ***D****atagram* ***P****rotocol, пользовательский дейтаграммный протокол*) – без установления соединения.

*Протокол* ***UDP*** позволяет приложениям отправлять инкапсулированные ***IP***-дейтаграммы без установления соединений. Он практически представляет собой протокол ***IP*** с добавлением небольшого заголовка. Его отличие от использования IP заключается в указании портов источника и приемника.

*Протокол* ***TCP*** взаимодействует через межуровневые интерфейсы с ниже лежащим протоколом IP и выше лежащими протоколами прикладного уровня или приложениями. Его задача заключается в передаче данных между любыми прикладными процессами, выполняющимися на любых узлах сети. Т.е. доставленный в компьютер-получатель средствами ***IP***- протокола пакет должен быть направлен конкретному процессу- получателю.

Пакеты, поступающие на транспортный уровень, организуются операционной системой в виде множества очередей к точкам входа различных прикладных процессов. В терминологии ***TCP/IP*** такие системные очереди называют *портами*. Т.о. адресом назначения, который используется протоколом ***TCP***, является *идентификатор (номер) порта* прикладной службы. Номер порта в совокупности с номером сети и номером конечного узла однозначно определяют прикладной процесс в сети, который имеет название *сокет (****socket****)*.

В 1995 году корпорация ***Netscape Communications*** представила систему безопасности под названием ***SSL*** (***S****ecure* ***S****ockets* ***L****ayer, протокол защищенных сокетов*). Протокол ***SSL*** используется очень широко (в том числе ***InternetExplorer***), он создает защищенное соединение между двумя сокетами, позволяющее:

* + клиенту и серверу договориться об используемых параметрах;
  + клиенту и серверу произвести взаимную аутентификацию;
  + организовать тайное общение;
  + обеспечить защиту целостности данных.

По сути дела, между прикладным и транспортным уровнями появляется новый уровень, принимающий запросы от браузера и отсылающий их по ***TCP*** для передачи серверу. После установки защищенного соединения основная задача ***SSL*** заключается в поддержке

сжатия и шифрования. Если поверх ***SSL*** используется ***HTTP***, этот вариант называется ***HTTPS*** (***SecureHTTP****– защищенный* ***HTTP***) несмотря на то, что это обычный протокол ***HTTP***.

Область применения S***S***L не ограничивается исключительно веб- браузерами, но это наиболее распространенное применение. Существует несколько версий протокола ***SSL***. Третья версия протокола ***SSL*** поддерживает множество разных алгоритмов и может обладать разными функциями, среди которых сжатие, тот или иной алгоритм шифрования, а также некоторые компоненты, связанные с ограничениями экспорта в криптографии. ***SSL*** состоит из двух субпротоколов, *один* из которых предназначен для установления защищенного соединения, а *второй*– для использования этого соединения. ***SSL*** поддерживает разнообразные *криптографические алгоритмы*. Наиболее сильный из них использует для шифрации тройной стандарт шифрования ***DES*** (***D****ata* ***E****ncryption* ***S****tandard, стандарт шифрования данных*) с тремя отдельными ключами и функция вычисления профиля сообщения ***SHA-1*** (***S****ecure* ***H****ash* ***A****lgorithm, надежный алгоритм хэширования*) для обеспечения целостности данных. Такое сочетание алгоритмов работает медленно, поэтому применяется в основном в приложениях, в которых требуется высокий уровень защиты. В обычных приложениях для шифрации применяется 128-разрядный ключ, а для аутентификации – алгоритм ***MD5*** (***M****essage* ***D****igest 5 – профиль сообщения 5*). В качестве исходных данных алгоритму ***RC4***передается 128- разрядный ключ, который разрастается во много раз при работе алгоритма. Это внутреннее число используется для создания ключевого потока. Последний суммируется по модулю 2 с открытым текстом, в результате чего получается обычный потоковый шифр.

Для реальной передачи данных используется второй субпротокол. Сообщения, поступающие от браузера, разбиваются на единицы данных размером до 16 Кбайт. Если сжатие включено, каждая из этих единиц независимо сжимается. Затем по двум нонсам вычисляется закрытый ключ, подготовительный ключ объединяется со сжатым текстом и результат хэшируется по согласованному алгоритму (чаще всего ***MD5***). Хэш добавляется к каждому фрагменту в виде ***MAC*** (***M****essage* ***A****uthetication* ***C****ode, код аутентификации сообщения*). Этот сжатый фрагмент вместе с ***MAC*** кодируется согласованным алгоритмом с симметричным ключом (обычно это суммирование по модулю 2 с ключевым потоком ***RC4***). Наконец, присоединяется заголовок фрагмента, и фрагмент передается по

***ТСР***-соединению.

*Назначение номеров портов* прикладным процессам осуществляется либо *централизованно*, если эти процессы представляют собой популярные общедоступные службы (21 – служба удаленного доступа к файлам ***FTP***, 23 – служба удаленного управления ***Telnet***), либо *локально* для тех служб, которые еще не стали распространенными, чтобы закрепить за ними зарезервированные номера. Локальное присвоение номера порта заключается в том, что разработчик некоторого приложения просто связывает с ним любой произвольно выбранный числовой идентификатор, обращая внимание на то, чтобы он не входил в число зарезервированных. В дальнейшем все удаленные запросы к этому приложению от других приложений должны адресоваться с указаниемназначенного ему номера порта.

Номера портов делят на три категории:

1. Номера**от 0 до 1023** зарезервированы для хорошо известных портов, которые ассоциированы со службами на постоянной основе (например, HTTP-серверы всегда принимают запросы к порту 80).
2. Порты с номерами **от1024 до 49151** являются регистрируемыми и используются для различных целей.
3. Порты с номерами**от 49 151 до 65 535** представляют собой динамические и частные порты, с которыми не должна ассоциироваться ни одна служба.

Некоторые соответствия портов и служб/протоколов:

* + ***TCP 22***–наиболее активно работающий сетевой порт. Используется программой ***Secure Shell*** (***SSH***), которая применяется для подключения компьютера с ОС ***Linux*** с утилитой ***IPTraf***.
  + ***UDP 138***–задействованслужбой***NetBIOS Datagram Service***. Данныйпортиспользуетсянесколькимислужбами***Windows***, втомчисле***ComputerBrowser****,* ***DFS****,* ***License****,* ***Messenger****,* ***NetLogon***и***Server***.
  + В группу портов ***TCP*** и ***UDP135–139*** входит несколько специфических портов, используемых многими приложениями ***Windows***. Некоторые из этих портов придется держать открытыми, что, к сожалению, открывает доступ к другим приложениям ***Windows***.
  + ***TCP 80***–используется для незашифрованного трафика ***HTTP (Web)***.
  + ***UDP 137***и***UDP 53***–эти порты используются службами преобразования имен ***Windows***– в данном случае, ***NetBIOS***и***DNS***.
  + ***UDP 67***и***UDP 68***–используются ***DHCP-сервером*** для назначения динамических ***IP***-адресов.
  + ***UDP 123***–зарезервирован для протокола ***Network Time Protocol (NTP)*** или, в случае ***Windows***, ***S****imple* ***N****etwork* ***T****ime* ***P****rotocol****(SNTP)****.* Этот протокол синхронизирует время между компьютером и ***NTP*-*сервером***, например контроллером домена (***DC***).

Более полный список можно посмотреть на страницах электронной энциклопедии***Wikipedia****.*

Сетевые порты могут дать важнейшую информацию о приложениях, которые обращаются к компьютерам по сети. Зная приложения, которые используют сеть, и соответствующие сетевые порты, можно составить точные правила для брандмауэра и настроить хост- компьютеры таким образом, чтобы они пропускали только полезный трафик.

Задача администратора состоит в том, чтобы выявить недостатки в функционировании сети и устранить их. Самый распространенный способ

–*сканирование портов*– процесс обнаружения прослушивающих приложений путем активного опроса сетевых портов компьютера или другого сетевого устройства. Результаты сканирования и сравнения сетевых отчетов с результатами хост-опроса портов позволяет составить ясную картину трафика, проходящего через сеть.

Например, сканируя диапазон внешних ***IP***-адресов, можно собрать ценные данные о взломщике, проникшем из Интернет. Поэтому следует чаще сканировать сеть и закрыть все необязательные сетевые порты. Построив профиль сети, и разместив инструменты для распознавания сетевого трафика, можно более эффективно обнаруживать взломщиков, анализируя генерируемый ими сетевой трафик. Можно значительно уменьшить вероятность проникновения в систему, если отключить сетевую активность приложений (служб) или заблокировать неиспользуемые порты компьютера.

Каждый открытый порт – потенциальная лазейка для взломщиков,

которые используют пробелы в хост-приложении или тайком обращаются к приложению с именем и паролем другого пользователя (либо применяют другой законный метод аутентификации).

Можно обнаружить открытые порты с помощью стандартных приложений ОС. Например, в ОС ***Windows*** можно воспользоваться утилитой ***Netstat***. Она служит для отображения активных подключений ***TCP***, портов, прослушиваемых компьютером, статистики ***Ethernet***, таблицы маршрутизации ***IP***, статистики ***IPv4*** (для протоколов ***IP***, ***ICMP***, ***TCP*** и ***UDP***) и ***IPv6*** (для протоколов ***IPv6***, ***ICMPv6***, ***TCP*** через ***IPv6*** и ***UDP*** через ***IPv6***).

Запущенная без параметров, команда ***netstat*** отображает подключения ***TCP***. Результатом сканирования c параметром ***-an*** является список с открытыми портами компьютера и название служб/протоколов, работающих на этом порту.

***Windows XP*** содержит ряд утилит для диагностики, отслеживания производительности и восстановления сетевых подключений. Большая часть из них включена в ее состав, некоторые хранятся в наборе ***Windows Support Tools****,* который можно установить из папки ***\Support\ Tools на диске Windows XP***.

Сканировать можно с помощью специальных программ, называемых *сетевыми сканерами*.

*Сканерлокальной сети* ***NetView***– программа-заменитель ***Сетевого Окружения Windows***– ведет лог со списком машин, адресами и описаниями и регулярно проверяет его на наличие выключенных машин, ведет лог активных сетевых соединений (имеет функцию черного и белого списков). Имеет быстрый поисковик файлов в расшаренных (распределенных) ресурсах, сканер портов и диапазона ***IP***-адресов, встроенный ***PortListener***– монитор, отслеживающий соединения на заданные порты (полезен для обнаружения ***IP***-адресов, с которых проводятся попытки установить соединения на троянские порты или сканирования портов), а также возможность посылать сообщения по сети. Может составлять посегментную карту сети (через ***traceroute***), а также визуализировать сеть (картинки, линии, фоновая текстура). Позволяет открывать компьютеры, как по имени, так и по ***IP***-адресам.

*Сканер портов* ***Nmap***– утилита для обследования сетей и аудита защиты. В ней поддерживается сканирование на основе запроса отклика (определение жизнеспособности узлов), много методов сканирования портов (определение сервисов, доступных на узлах), определение версий

(какие приложения/службы работают на порте) и анализ трафика ***TCP***/***IP*** (***fingerprinting***, идентификация типа устройства или ОС узла). Имеются гибкие возможности спецификации целевых устройств и портов, сканирование на предмет ловушек и замаскированных угроз, сканирование SunRPC и многое другое. Для большинства платформ ***Unix*** и ***Windows*** поддерживаются режимы командной строки и графического интерфейса.

*Монитор портов* ***TCPView***– показывает все процессы, использующие интернет-соединения. Запустив ***TCPView***, можно узнать, какой порт открыт и какое приложение его использует, а при необходимости и немедленно разорвать соединение.

*Комплекс утилит* ***IP-Tools*** представляет собой набор программ (19 утилит) для сетевого мониторинга: сканеры, мониторы, трассировщик и другие программы. Допустимо использовать сразу несколько утилит, причем сканеры могут работать как с отдельным хостом, так и по диапазону ***IP***-адресов или по списку адресов. Всю информацию, выдаваемую программой, можно записывать в текстовые файлы (а некоторую – и в ***HTML***-файлы).

### Выполнение работы

#### Задание 1. Исследуйте локальную сеть:

* 1. Запустите сканер локальной сети –***NetView***.
  2. Разместите все найденные узлы в одном хост-листе (***Setting/Autosplit/Send all to Default***).
  3. Просмотрите свойства узла в списке (***контекстное меню узла/Properties***).
  4. Просмотрите активные подключения к компьютеру (***Tools/Net Watcher***).
  5. Просканируйте открытые ***TCP****-*порты контролера домена:
     + активизируйте инструмент ***Сканер сети* (*Tools/Network Scanner*)**;
     + введите в поле***IP diapasone***–<*IP-адрес котроллера домена*>;
     + установите ***диапазон сканирования TCP-портов(TCP Range)*** с *1* по

*65536* и запустите сканирование кнопкой ***Start***.

* 1. Аналогично просканируйте открытые ***UDP-порты контролера домена***.
  2. Просмотрите статистику работы протокола ***IP*** (***IP logger***).
  3. Найдите общедоступные ресурсы сети (***Tools/Resources scanner***).

#### Задание 2. Исследуйте удаленную систему и сохраните результаты

**исследования (*IP*-адрес компьютера, открытые порты с указанием сервисов, работающих на этих компьютерах) в файл с именем *scan.txt:***

* 1. Получите информацию об использовании сканера ***Nmap***:
     + откройте консоль (***Пуск/Выполнить/cmd***);
     + перейдите в каталог со сканером;
     + введите команду ***nmap.exe***.

*Если сканеру не передаются параметры, то он просто выдает справку об использовании. В общем случае синтаксис использования этого сканера следующий:*

*Nmap [-тип сканирования][-параметры] объект\_сканирования;*

* 1. Найдите открытые порты вторичного контролера домена ***Main***. Для этого введите команду ***nmap*** с параметром *Main*. На экран через некоторое время будет выдана информация об открытых портах из диапазона *1…1657*.
  2. Просканируйте все порты (с 1 по 65536) любого компьютера в кабинете. Для этого введите команду ***nmap*** с параметром *–p1-65535 nmap –p1-65535 IP-адрес\_компьютера*
  3. Просканируйте другой компьютер кабинета с попыткой определения

версии сервисов, работающих на тех или иных портах:

*nmap –sV IP-адрес\_компьютера*

* 1. Определите операционную систему первичного контроллера домена:

*nmap –O IP-адрес\_контроллера\_домена*

*Результат детектирования можно найти в строке OS Details.*

* 1. Просканируйте вторичный контроллер домена с обходом брандмауэра:

*nmap –f адрес\_контролера\_домена*

* 1. Просканируйте любой компьютер в кабинете с выводом отправленных и полученных пакетов:

*nmap –packet\_trace IP-адрес\_компьютера.*

* 1. Представьте отчет о проделанной работе преподавателю.

#### Задание 3. Самостоятельно, используя сканер портов *nmap*:

* 1. Определите открытые порты компьютера.
  2. Закройте доступ к этим портам с помощью брандмауэра;
  3. Повторно просканируйте компьютер.

#### Задание 4. Исследуйте локальную сеть с помощью комплекса утилит

***IP-Tools.***

**Задание 5. Просмотрите активные сетевые подключения локального ПК с помощью утилиты *netstat* и монитора портов *tpiview*.**

## Лабораторная работа 3.3.

## Сетевая антивирусная защита

**Цель:** научится обеспечивать антивирусную защиту сети.

#### Средства для выполнения работы:

* **аппаратные:** компьютер с установленной ОС ***Windows XP.***
* **программные:** приложения ВМ: ***VirtualBox;*** виртуальные машины: ***VM-1, VM-2;*** образы диска с программным обеспечением: ***CD-For- LAB.iso.***

***Теоретические сведения***

*Антивирусное ПО*– это компьютерные программы, которыемогут определить, нейтрализовать или уничтожить вредоносные программы. Большинство современных антивирусных программ создаются для борьбы с широким спектром угроз, включая вирусы-черви, фишинг-атаки, руткиты, троянские программы и другие вредоносные программы. Выделяют следующие виды антивирусов в зависимости от их принципа действия (определяющего функциональность):

* + ***Сканеры*** (*полифаги*) определяют наличие вируса по БД, хранящей сигнатуры (или их контрольные суммы) вирусов. Их эффективность определяется актуальностью вирусной базы и наличием эвристического анализатора (см. Эвристическое сканирование).
  + ***Ревизоры***запоминают состояние файловой системы, что делает в дальнейшем возможным анализ изменений. (Класс близкий к ***IDS***).
  + ***Мониторы***(*сторожа*) отслеживают потенциально опасные операции, выдавая пользователю соответствующий запрос на разрешение/запрещение операции.
  + ***Вакцины***изменяют прививаемый файл таким образом, чтобы вирус, против которого делается прививка, уже считал файл заражённым. В современных условиях (с 2007 г.), когда количество возможных вирусов измеряется десятками тысяч, этот подход уже неприменим.

Антивирусное программное обеспечение обычно использует два отличных друг от друга метода для выполнения своих задач:

* + *сканирование файлов* для поиска известных вирусов, соответствующих определению в антивирусных базах.
  + *обнаружение подозрительного поведениялюбой* из программ, похожего на поведение заражённой программы.

#### Метод соответствия определения вирусов в словаре.

Когда антивирусная программа, просматривая файл, обращается к антивирусным базам, которые составлены производителем программы- антивируса. В случае соответствия какого-либо участка кода просматриваемой программы известному коду (*сигнатуре*) вируса в базах, программа антивирус может по запросу выполнить одно из следующих действий:

* удалить инфицированный файл;
* заблокировать доступ к инфицированному файлу;
* отправить файл в карантин (т.е. сделать его недоступным для выполнения, с целью недопущения распространения вируса).
* попытаться восстановить файл, удалив сам вирус из тела файла;
* в случае невозможности лечения/удаления, выполнить эту процедуру при перезагрузке.

Хотя антивирусные программы, созданные на основе поиска соответствия определения вируса в словаре, при обычных обстоятельствах, могут достаточно эффективно препятствовать вспышкам заражения компьютеров, авторы вирусов стараются держаться впереди таких программ-антивирусов, создавая вирусы «олигоморфические»,

«полиморфические» и, самые новые, «метаморфические», в которых некоторые части шифруются или искажаются так, чтобы невозможно было обнаружить совпадение с определением в словаре вирусов.

#### Метод обнаружения странного поведения программ

Антивирусы, использующие метод обнаружения подозрительного

поведения программ не пытаются идентифицировать известные вирусы, вместо этого они прослеживают поведение всех программ. Если программа пытается записать какие-то данные в исполняемый файл (***exe***-файл), программа-антивирус может пометить этот файл, предупредить пользователя и спросить что следует сделать. В настоящее время, подобные превентивные методы обнаружения вредоносного кода, в том или ином виде, широко применяются в качестве модуля антивирусной программы, а не отдельного продукта.

Другими названиями этого метода выступают такие названия, как: ***Проактивная защита, Поведенческий блокиратор, H****ost* ***I****ntrusion* ***P****revention* ***S****ystem* ***(HIPS)***. В отличие от метода поиска соответствия определению вируса в антивирусных базах, метод обнаружения подозрительного поведения даёт защиту от новых вирусов, которых ещё нет в антивирусных базах. Однако следует учитывать, что программы или модули, построенные на этом методе, выдают также большое количество предупреждений (в некоторых режимах работы), что делает пользователя мало восприимчивым ко всем предупреждениям.

В последнее время эта проблема ещё более ухудшилась, так как стало появляться всё больше не вредоносных программ, модифицирующих другие ***exe***-файлы, несмотря на существующую проблему ошибочных предупреждений. Несмотря на наличие большого количества предупреждающих диалогов, в современном антивирусном программном обеспечении этот метод используется всё больше и больше. Так, в 2006 году вышло несколько продуктов, впервые реализовавших этот метод: ***Kaspersky Internet Security, Kaspersky Antivirus, Safe'n'Sec, F-Secure Internet Security, Outpost Firewall Pro, DefenceWall***. Многие программы класса «файрволл» издавна имели в своем составе модуль обнаружения странного поведения программ.

#### Метод обнаружения при помощи эмуляции

Некоторые программы-антивирусы пытаются имитировать начало выполнения кода каждой новой вызываемой на исполнение программы, перед тем как передать ей управление. Если программа использует самоизменяющийся код или проявляет себя как вирус (то есть немедленно начинает искать другие ***exe***-файлы), такая программа будет считаться вредоносной, способной заразить другие файлы. Однако этот метод тоже изобилует большим количеством ошибочных предупреждений.

#### Другие методы обнаружения вирусов

Ряд других методов предлагается в исследованиях и используется в антивирусных программах (см. Эвристическое сканирование).

В лабораторной работе используется программное обеспечение ***Symantec AntiVirus Corporate Edition***. Оно обеспечивает автоматическую защиту от вредоносного ПО рабочих станций и сетевых серверов, увеличивая время бесперебойной работы всей корпоративной системы. Централизованные средства конфигурирования, установки, сигнализации и регистрации определяют, какие узлы уязвимы для атак. Встроенные средства реагирования от лидера в области информационной безопасности помогают предприятиям максимизировать время бесперебойной работы, уменьшить стоимость владения и гарантировать целостность данных.

Основные характеристики:

* + обеспечивает улучшенную защиту от вирусов для всего предприятия и мониторинг с единой консоли управления;
  + имеющиеся средства постоянного осмотра автоматически выявляют и удаляют программы-шпионы, блокируя их запуск или установку на компьютере;
  + включает встроенные средства создания графических отчетов с веб-интерфейсом и централизованное управление с одной консоли.

В данном ПО предусмотрена эффективная защита от программ- шпионов и программ показа рекламы, в том числе:

* + усовершенствованная функция удаления программ-шпионов, которая автоматически предотвращает установку программ- шпионов;
  + обнаружение и удаление скрытых программ-шпионов;
  + изучение влияния программ-шпионов на основании таблицы влияния угроз, созданной компанией ***Symantec***.

### Выполнение работы

#### Задание 1. Установите серверную часть антивируса.

* 1. Подключите к виртуальной машине **VM-2** образ диска с программным обеспечением ***CD-For-LAB.iso***.
  2. Запустите виртуальную машину и перейдите в каталог с установочными файлами антивируса (***Symantec1***).
  3. Запустите установку (двойной щелчок по файлу ***Setup.exe***).
  4. Ознакомьтесь с информацией мастера и щелкните ***Далее***.
  5. Ознакомьтесь с лицензионным соглашением:
     + выберите *Я согласен с условиями лицензионного соглашения*;
     + подтвердите выбор кнопкой ***Далее***.
  6. Выберите установку **сервера** радиокнопкой *Установка сервера* и щелкните ***Далее***.
  7. Укажите ***тип установки****Полная* и щелкните ***Далее***.
  8. Укажите данные группы серверов:
     + введите в поле ***Группа серверов***, название группы серверов –

*Example Avir*;

* + - введите в поле ***Пароль***– пароль для создаваемой группы серверов –

*123456*;

* + - подтвердите изменения кнопкой ***Далее***.
    - подтвердите создание группы серверов, повторно введите пароль и щелкните ***ОК***.
  1. Ознакомьтесь с информацией о параметрах ***Автозащиты*** и щелкните ***Далее***.
  2. Ознакомьтесь с итоговой информацией мастера установки и запустите установку кнопкой ***Установить***.
  3. Завершите установку кнопкой ***Готово***.

*Автоматически откроется окно обновления антивируса.*

* 1. Обновите установленный антивирус кнопкой ***Обновить***.

#### Задание 2. Установите центр управления антивирусом.

* 1. Перейдите в каталог с установочными файлами (***Symantec2***).
  2. Запустите установку двойным щелчком по файлу ***Setup.exe***.
  3. Ознакомьтесь с информацией мастера и щелкните ***Далее***.
  4. Ознакомьтесь с лицензионным соглашением:
     + выберите *Я согласен с условиями лицензионного соглашения*;
     + подтвердите выбор кнопкой ***Далее***.
  5. Ознакомьтесь с информацией об устанавливаемых компонентах и щелкните ***Далее***.
  6. Укажите каталог установки *По умолчанию* и щелкните ***Далее***.
  7. Активируйте установку кнопкой Установить.
  8. Завершите установку кнопкой ***Готово***.

*Появится сообщение о необходимости перезагрузки компьютера.*

* 1. Перезагрузите виртуальный компьютер кнопкой ***Да***.

#### Задание 3. Выполните первоначальную настройку серверной части антивируса.

* 1. Запустите оснастку управления антивирусом (***Пуск/Symantec System Center Console/ Symantec System Center Console***).
  2. Укажите первичный (основной) антивирусный сервер:
     + активируйте группу, созданную при установке антивирусного сервера, например ***Example Avir***;
     + разблокируйте группу:
       - выполните команду контекстного меню ***Разблокировать группу серверов***;
       - введите ***пароль***, указанный при установке антивирусного сервера

–*123456*;

* + - * установите флажок *Запомнить пароль*;
      * подтвердите разблокирование группы кнопкой ***ОК***;
    - активируйте ваш сервер, например ***win2003*** и выполните команду контекстного меню ***Сделать сервер первичным***;
    - ознакомьтесь с информацией о назначении первичного сервера и щелкните ***Да***;
  1. Выполните настройку планового сканирования для клиентов:
     + активируйте в левой части оснастки управления антивирусом сервер ***win2003***;
     + откройте диалоговое окно ***Плановые осмотры* (*Действия/Все задачи/Плановые осмотры…*)** и перейдите на вкладку ***Осмотры клиентов***;
     + создайте регулярный осмотр каждую неделю в 20.00:
       - откройте диалоговое окно ***Новый осмотр*** кнопкой ***Создать***;
       - введите в поле ***Имя***–*Еженедельный осмотр*;
       - выберите в разделе ***Осматривать в***–<*Месяц*>;
       - введите в разделе ***Время***–*20.00*;
       - завершите ввод параметров кнопкой ***ОК***.
     + закройте диалоговое окно ***Плановые осмотры*** кнопкой ***ОК***.
  2. Закройте оснастку управления антивирусом.
  3. Переключитесь в физический компьютер.

#### Задание 4. Установите клиентскую часть антивируса.

* 1. Скопируйте в виртуальную машину ***VM-2*** каталог (***Symantec1***) с установочными файлами антивируса.
  2. Переключитесь в виртуальную машину.
  3. Запустите установку (двойной щелчок по файлу ***Setup.exe***).
  4. Ознакомьтесь с информацией мастера и щелкните ***Далее***.
  5. Ознакомьтесь с лицензионным соглашением:
     + выберите *Я согласен с условиями лицензионного соглашения*;
     + подтвердите выбор кнопкой ***Далее***.
  6. Выберите установку клиента радиокнопкой *Установка клиента* и щелкните ***Далее***.
  7. Укажите ***тип установки***–*Полная* и щелкните ***Далее***.
  8. Укажите ***тип сетевой установки***–*Управляемый* и щелкните ***Далее***.
  9. Введите ***имя компьютера*** с установленным серверным антивирусом

–*win2003*.

* 1. Активируйте установку кнопкой ***Установить***.
  2. Завершите установку кнопкой ***Готово***.

#### Задание 5. Самостоятельно скопируйте в виртуальную машину *VM-1* файлы, зараженные вирусами, с диска к лабораторным работам и выполните антивирусную проверку.

**Задание 6. Измените параметры сканирования клиентских компьютеров.**

**Задание 7. Выполните принудительное антивирусное сканирование клиента.**

# Примерные тестовые задания к модулю 3

1. … каналов – это запись и последующий анализ всего проходящего потока сообщений.
2. К сервисам безопасности относят:
   * *идентификация/аутентификация;*
   * *протоколирование/аудит;*
   * *шифрование;*
   * *аудит.*
3. … – подтверждение подлинности взаимодействующих

объектов.

1. Соответствие между понятиями и их определениями:

*Конфиденциальность предотвращение пассивных атак*

*для передаваемых или хранимых данных*

*Аутентификация защита от несанкционированного использования ресурсов*

*Контроль доступа подтверждение подлинности взаимодействующих объектов*

# Контрольные вопросы к модулю 3

1. Стандартные средства мониторинга ОС.
2. События системы. Параметры событий. Просмотр событий. 3.Межсетевой экран и его функции.
3. SSL-протокол защиты сокетов.
4. Категории портов. Присвоение имени порту. 6.Сканирование портов.

7.Сетевая антивирусная защита. 8.Алгоритм работы с сетевым антивирусом.

# Модуль 4.

# Защита информации в компьютере

**Цель:**познакомиться с основными принципами защиты информации на персональном компьютере.

**Результат:**уметь устанавливать защиту на локальном компьютере: настраивать параметры безопасности браузера ***Internet***, создавать политику ***IP***-безопасности на локальном компьютере, контролировать ***IP***–трафик, настраивать брандмауэр ***Windows***; уметь работать с резервными копиями файлов ОС: осуществлять резервное копирование и восстановление системных конфигурационных файлов;

#### План освоения модуля:

1. Изучите следующие темы в указанных источниках:
   * *Виды информационных атак. Переносимые программы: Java- апплеты, управляющие элементы ActiveX, скрипты;*
   * *Цифровая подпись. Сертификаты;*
   * *Параметры конфиденциальности браузера;*
   * *Межсетевой экран и его функции. Основные компоненты брандмауэра;*
   * *Резервное копирование системных конфигурационных файлов. Восстановление системных конфигурационных файлов.*
2. Выполните и представьте преподавателю лабораторные работы:
   * ЛР 4.1. *Настройка параметров безопасности Интернет браузера.*
   * ЛР 4.2. *Технология защиты сетевых компьютеров. Брандмауэр.*
   * ЛР 4.3. *Создание резервных копий.* **III.**Выполните самостоятельные задания к модулю. **IV.**Выполните тестовые задания к модулю. **V.**Защитите модуль по контрольным вопросам. **Литература:**
3. Компьютерные сети. 4-е изд. / Э. Таненбаум. – СПб.: Питер, 2003. – 992 с.: ил. – (Серия «Классика Computer Science»), (Гл. 8).
4. Анин Б. Ю.Защита компьютерной информации /Б.Ю.Анин– СПб.: БХВ- Петербург, 2000. – 384 с.: ил. (Гл. 1, 4, 5).
5. Партыка Т.Л. Информационная безопасность. Учебное пособие для студентов учреждений среднего профессионального образования /

Т.Л.Партыка [и др.]; под ред. И.И.Попов – М.: ФОРУМ: ИНФРА-М, 2005. – 368 с.: ил. – (Профессиональное образование), (Гл.4, 6).

1. Матвеев М.Д. Самоучитель Microsoft Windows XP. Все об использовании и настройках. Изд. 2-е, перераб. и доп. / М. Д. Матвеев[и др.]; под ред. М. В. Финкова.– СПб.: Наука и Техника, 2006. – 624 с.: ил. (Гл. 26).
2. Ботт Э. Эффективная работа: Windows XP / Э.Ботт[и др.]; под ред. К.Зихерт. – СПб.: Питер. –2004. –1069 с.: ил. (Ч.VI)
3. Microsoft Windows XP Professional/ Учебный курс MCSA/MCSE/ Пер. с англ. – 2-е изд., испр. – М.: Издательско-торговый дом «Русская Редакция», 2003. – 1008 стр.: ил.
4. АндреевА.Г. Microsoft Windows XP. Руководство администратора / А.Г. Андреев и др. – СПб.: БХВ-Петербург, 2006.– 848 с.:ил. (Гл.11, 16).

## Лабораторная работа 4.1.

## Настройка параметров безопасности Интернет браузера

**Цель:** научиться настраивать параметры безопасности в современных Интернет браузерах.

#### Средства для выполнения работы:

* + **аппаратные:** компьютер;
  + **программные:**ОС***Windows XP***или***Windows2000***; браузеры:

***InternetExplorer***; ***Firefox***, ***Opera***.

***Теоретические сведения***

Компьютер, подсоединенный к сети Интернет, может подвергнуться реальным атакам. *Основные опасности при работе в сети Интернет* с помощью браузера следующие:

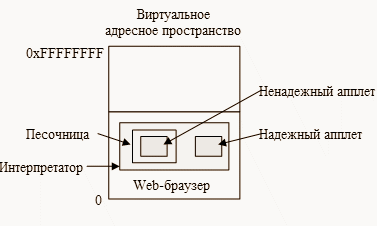
* + - переносимые программы (***ActiveX*** и ***Java-апплеты***) внедренные в web-страницу;
    - языки сценариев (***JavaScript*** и ***VBScript***), которые призваны превратить статичное содержимое HTML-страницы в динамическое;
    - ***cookie***, сохраняемые браузером могут позволить заинтересованным лицам следить за Вашими действиями в сети и знать о Ваших интересах.

Современные веб-страницы часто содержат небольшие программы:

***Java-апплеты***, управляющие элементы ***ActiveX***, скрипты ***JavaScript***.

Загрузка и выполнение таких переносимых программ, очевидно, связаны с большим риском возникновения массовых атак. Разработаны различные методы, направленные на минимизацию этого риска.

***Java-апплеты***– это программы на языке ***Java***, откомпилированные в машинный язык, которые размещаются на веб-странице и загружаются вместе с ней. Апплеты обрабатываются интерпретатором ***JVM* (*Java Virtual Machine***– виртуальная машина ***Java***) в браузере, как показано на рисунке 6.



**Рисунок 6. Обработка апплетов браузером**

Преимущество интерпретируемого кода перед компилируемым состоит в том, что перед его исполнением изучается каждая инструкция. Это дает интерпретатору возможность проверить состоятельность адреса инструкции. Кроме того, системные вызовы также перехватываются и интерпретируются. Как именно они обрабатываются, зависит от политики защиты информации:

* + - если апплет *надежный* (например, он был создан на локальном диске), его системные вызовы могут обрабатываться без дополнительных проверок;
    - если апплет *не может считаться надежным* (например, он был загружен из Интернета), его можно поместить в так называемую песочницу, регулирующую его поведение и пресекающую его попытки использовать системные ресурсы;
    - если апплет *пытается захватить системный ресурс*, вызов передается монитору безопасности, который может разрешить или запретить данное действие. Монитор исследует вызов с точки зрения локальной политики защиты информации и затем принимает решение.

Таким образом, можно предоставить апплетам доступ к некоторым (но не ко всем) ресурсам.

*Управляющие элементы* ***ActiveX***– двоичные программы, которые можно внедрять в веб-страницы. Когда на странице встречается такая программа, производится проверка необходимости ее выполнения, и в случае положительного ответа она запускается. Эти программы не интерпретируются и не помещаются в песочницы, поэтому они обладают такими же возможностями, как обычные пользовательские программы, и, в принципе, могут нанести большой вред. Таким образом, вся защита информации сводится к тому, стоит ли запускать управляющий элемент.

Для принятия таких решений корпорацией ***Microsoft*** был выбран метод, базирующийся на подписях кода (*система* ***Authenticode***). Суть в том, что каждый элемент ***ActiveX*** снабжается цифровой подписью, а именно *хэшем кода*, подписанным его создателем с использованием открытого ключа. Когда браузер встречает управляющий элемент, он проверяет правильность подписи, убеждаясь в том, что код не был заменен по дороге. Если подпись корректна, браузер проверяет по своим внутренним таблицам, можно ли доверять создателю программы. Если создатель надежный, программа выполняется, иначе игнорируется. Поскольку нет никакой возможности проследить за деятельностью всех компаний, пишущих переносимые программы, вскоре метод подписания кода может представлять собой довольно серьезную угрозу.

В ***JavaScript*** вообще отсутствует какая-либо официальная модель системы защиты информации. Каждый производитель пытается что-нибудь придумать. Например, в ***Netscape Navigator 2.0*** было реализовано нечто подобное ***Java***-модели, а в четвертой версии прослеживаются черты модели подписей кода.

В обозревателе ***Internet Explorer*** имеется несколько возможностей, позволяющих обеспечить защиту конфиденциальности, а также повысить безопасность личных данных пользователя.

Параметры конфиденциальности позволяют защитить личные данные пользователя – с помощью этих параметров можно понять, как просматриваемые web-узлы используют эти данные, а также задать значения параметров конфиденциальности, которые будут определять, разрешено ли web-узлам сохранять файлы ***cookie*** на компьютере.

К *параметрам конфиденциальности* ***Internet Explorer*** относят следующие:

* + - *параметры конфиденциальности*, определяющие обработку на компьютере файлов ***cookie***;
    - *оповещения безопасности*, выдаваемые пользователю при попытке получить доступ к web-узлу, не соответствующему заданным параметрам конфиденциальности;
    - *возможность просмотра политики конфиденциальности*

стандарта P3P (***Platform for Privacy Preferences***) для web-узла.

Средства безопасности позволяют предотвратить доступ других пользователей к таким сведениям, на доступ к которым у них нет разрешения. Это, например, сведения о кредитной карточке, вводимые при покупках в Интернете, от небезопасного программного обеспечения.

Когда производится загрузка или запуск программ, полученных из Интернета, необходимо убедиться, что программа получена из известного, надежного источника. В связи с этим, при выполнении загрузки на компьютер программы из Интернета, обозреватель ***Internet Explorer*** использует для проверки ее подлинности технологию ***Microsoft Authenticode***, проверяющую наличие у программы действующего сертификата. Следует отметить, что эта мера не препятствует загрузке и запуску на компьютере программ, разработанных с ошибками, но снижает риск использования фальсифицированной программы.

*Цифровая подпись*– это способ введения электронной метки для файла данных. В этом случае файл подписывается его создателем (издателем). Наличие цифровой подписи позволяет сделать следующие выводы: имеется имя издателя файла, и этот файл не был изменен с тех пор, как он был подписан. При любой попытке фальсификации подпись становится недействительной.Виды цифровых подписей:

* + - подписи с симметричным ключом;
    - подписи с открытым ключом.

В *первом случае* суть состоит в создании некоего центрального авторитетного органа, которому все доверяют. Затем каждый пользователь выбирает секретный ключ и лично относит его в офис этого авторитетного органа. Когда возникает необходимость послать открытым текстом подписанное сообщение, оно (сообщение) шифруется ключом. Затем сообщение посылается в авторитетный орган, который расшифровывает его и посылает получателю со своей собственной подписью. Этим авторитетный орган подтверждает, что сообщение подлинное.

Во *втором случае* ключ делится на две части: *закрытая* и

*открытая*. С помощью закрытой части можно подписать данные, причем это может сделать только владелец ключа, а с помощью открытой части можно проверить подпись.

*Сертификат*– цифровой документ, широко используемый для проверки подлинности и безопасного обмена данными в открытых сетях, таких как Интернет, экстрасети и интрасети. Сертификат связывает открытый ключ с объектом, хранящим соответствующий закрытый ключ. Сертификаты имеют цифровые подписи, поставленные выдавшими центрами сертификации, и могут предоставляться пользователю, компьютеру или службе. Наиболее широко применяемый формат для цифровых сертификатов определяется международным стандартом ***ITU-T***

***X.509*** версии 3.

### Выполнение работы

**Задание 1. Настройте параметры безопасности браузера *Internet Explorer:***

* 1. Откройте диалоговое окно ***Свойства: Интернет* (*Пуск/Панель управления/Свойства обозревателя*)**;
  2. Перейдите на вкладку ***Безопасность*** и откройте параметры зоны Интернет с помощью кнопки ***Другой…***;
  3. Установите ***Проверку имени пользователя*** в режим ***Запрос имени пользователя и пароля***;
  4. Разрешите в соответствующих полях указанные ниже действия:
     + *Блокировать всплывающие окна;*
     + *Доступ к источникам данных за пределами домена;*
     + *Переход между кадрами через разные домены.*
  5. Установите ***Разрешения канала программного обеспечения*** на

*Высокий уровень безопасности*;

* 1. Отключите *Использование элементов* ***ActiveX*** *не помеченных как безопасные*.
  2. Отключите загрузку *Неподписанных элементов* ***ActiveX***;
  3. Примените параметры кнопкой ***ОК***;
  4. Установите параметры конфиденциальности:
     + перейдите на вкладку ***Конфиденциальность***;
     + установите регулятор на уровень *Умеренно высокий*;
     + разрешите загружать файлы ***cookie*** с узла[***www.mail.ru***:](http://www.mail.ru/)
       - щелкните по кнопке ***Узлы***;
       - введите в поле [***www.mail.ru***](http://www.mail.ru/) и щелкните по кнопке ***Разрешить***;
     + аналогично разрешите загружать ***cookie*** со следующих узлов:

##### [www.yandex.ru,](http://www.yandex.ru/) www.pochta.ru;

* + - примените параметры кнопкой ***ОК***;
  1. Настройте ограничения на доступ к ресурсам по содержанию информации на них:
     + перейдите на вкладку ***Содержание*** и откройте окно ***Ограничение доступа*** кнопкой ***Включить*** в разделе ***Ограничения доступа***;
     + установите пароль:
       - перейдите на вкладку ***Общие***;
       - откройте окно создания пароля кнопкой ***Создать пароль***;
       - введите ***пароль***–*user* и ***подсказку*** к нему –*user*;
       - примените параметры кнопкой ***ОК***.
     + перейдите на вкладку ***Оценки*** и установите уровни ***Службыоценки Recreational Software Advisory Council*** по своему усмотрению;
     + примените параметры кнопкой ***OK***;
     + очистите пароли, которые браузер автоматически запоминает. Для этого на вкладке ***Содержание***, щелкните по кнопке ***Автозаполнение***, а затем по кнопке ***Очистить пароли***;
     + удалите временные фалы Интернет и ***cookies*** на вкладке ***Общие***.

**Задание 2. Самостоятельно очистите журнал в браузере Inter*n*et**

***Explorer*.**

#### Задание 3. Самостоятельно настройте параметры безопасности в браузере *Firefox*.

**Задание 4. Самостоятельно настройте параметры безопасности в браузере *Opera*.**

## Лабораторная работа 4.2

## Технология защиты сетевых компьютеров. Брандмауэр.

**Цель:** научиться защищать сетевой компьютер и настраивать брандмауэр.

#### Средства для выполнения работы:

* **аппаратные:** компьютер, подключенный к ЛВС;
* **программные:** ОС ***Windows XP***; приложение ВМ: ***VirtualBox***; виртуальная машина: ***VM-1***.

***Теоретические сведения***

Особенности защиты информации в компьютерных сетях обусловлены тем, что сети, обладая несомненными преимуществами обработки информации, по сравнению с локальными компьютерами, усложняют организацию защиты, образуя следующие основные проблемные направления:

* + разделение совместно используемых ресурсов;
  + расширение зоны контроля;
  + комбинация различных программно-аппаратных средств;
  + неизвестный периметр;
  + множество точек атаки;
  + сложность управления и контроля доступа к системе.

Сообществом Интернета под эгидой *Тематической группы по технологии Интернета* ***(I****nternet* ***E****ngineering* ***T****ask* ***F****orce****, IETF)*** разработано много рекомендаций по отдельным аспектам сетевой безопасности, тем не менее, целостной концепции или архитектуры безопасности пока не предложено. Основная идея состоит в том, чтобы средствами оконечных систем обеспечивать сквозную безопасность.

*Экранирование*– единственный сервис безопасности, для которого Гостехкомиссия России одной из первых в мире разработала и ввела в действие *Руководящий документ*, основные идеи которого получили международное признание и фигурируют в профилях защиты, имеющих официальный статус в таких странах, как США. Политика безопасности межсетевого экрана базируется на принципе *«все, что не разрешено, запрещено»*

*Межсетевой экран* или *Брандмауэр*– это *полупроницаемая мембрана,* которая располагается между защищаемым внутренним сегментом сети и внешней сетью или другими сегментами сети интранет и контролирует все информационные потоки во внутренний сегмент и из него. *Контроль трафика* состоит в его фильтрации, то есть выборочном пропускании через экран, а иногда и с выполнением специальных преобразований и формированием извещений для отправителя, если его данным в пропуске было отказано. Фильтрация осуществляется на основании набора условий, предварительно загруженных в брандмауэр и

отражающих концепцию информационной безопасности корпорации. Брандмауэры могут быть выполнены как в виде аппаратного, так и программного комплекса, записанного в коммутирующее устройство или сервер доступа (сервер-шлюз, прокси-сервер, хост-компьютер и т. д.). Работа брандмауэра заключается в анализе структуры и содержимого информационных пакетов, поступающих из внешней сети, и в зависимости от результатов анализа пропуска пакетов во внутреннюю сеть (сегмент сети) или полное их отфильтровывание. Эффективность работы межсетевого экрана обусловлена тем, что он полностью переписывает реализуемый стек протоколов ***TCP/IP***, и поэтому нарушить его работу с помощью искажения протоколов внешней сети (что часто делается хакерами) невозможно.

Межсетевые экраны обычно выполняют следующие функции:

* + физическое отделение рабочих станций и серверов внутреннего сегмента сети (внутренней подсети) от внешних каналов связи;
  + многоэтапная идентификация запросов, поступающих в сеть (идентификация серверов, узлов связи и прочих компонентов внешней сети);
  + проверка полномочий и прав доступа пользователей к внутренним ресурсам сети;
  + регистрация всех запросов к компонентам внутренней подсети извне;
  + контроль целостности программного обеспечения и данных;
  + экономия адресного пространства сети (во внутренней подсети может использоваться локальная система адресации серверов);
  + сокрытие ***IP***-адресов внутренних серверов с целью защиты от хакеров.

Брандмауэры могут работать на разных уровнях протоколов модели

***OSI***.

*На сетевом уровне* выполняется фильтрация поступающих пакетов,

основанная на ***IP***-адресах (например, не пропускать пакеты из Интернета, направленные на те серверы, доступ к которым извне не должен осуществляться; не пропускать пакеты с фальшивыми обратными адресами или с IP-адресами, занесенными в «черный список» и т. д.).

*На транспортном уровне* фильтрация возможна еще и по номерам портов ***TCP*** и флагов, содержащихся в пакетах (например, запросов на установление соединения).

*На прикладном уровне* может выполняться анализ прикладных протоколов (***FTP, HTTP, SMTP*** и т. д.) и контроль за содержанием потоков данных (запрет внутренним абонентам на получение каких-либо типов файлов: рекламной информации или исполняемых программных модулей, например).

В брандмауэре возможно наличие экспертной системы, которая, анализируя трафик, диагностирует события, потенциально представляющие угрозу безопасности внутренней сети, извещает об этом администратора сети, а в случае опасности она может автоматически ужесточать условия фильтрации и т. д.

К основным компонентам брандмауэра относят: политика сетевого доступа; механизмы усиленной аутентификации; фильтрация пакетов; прикладные шлюзы.

В качестве популярных эффективных брандмауэров называются: ***Netscreen 100, CyberGuard Firewall, Kerio Winroute Firewall, Zone Alarm, Agnitum Autpost Firewall, Jetico Personal Firewall, Internet Connection Firewall.***

Еще одним способом сетевой защиты может быть установленное на сервере специальное программное обеспечение, которое позволяет остальным компьютерам сети эмулировать выход в Интернет, оставаясь при этом «невидимым» со стороны глобальной сети. Такой компьютер называют *прокси-сервером (proxy – доверенный)*. Например, ***Microsoft Proxy Server 2.0.*** который, являясь кэширующим сервером (повышает эффективность работы сети – сокращает сетевой трафик), выполняет функции брандмауэра и обеспечивает безопасный доступ в Интернет и имеет два сетевых адаптера – один соединяет его с сетью, другой – с Интернет. Так как локальная сеть «не видна» из сети Интернет, то легальный ***IP***-адрес имеет только внешний сетевой интерфейс, а ***IP***-адреса внутри сети могут быть выданы из пула, зарезервированного для изолированных сетей.

В ОС ***Windows XP*** с установленным ***SP2*** (***S****ervice* ***P****ack 2*– пакет обновлений 2) входит брандмауэр. Основные возможности которого заключаются в следующих действиях: блокировка доступа компьютерным вирусам и червям; запрос пользователя о выборе действия; ведение журнала безопасности.

### Выполнение работы

#### Задание 1. Подготовьте компьютер для выполнения лабораторной работы:

* 1. Запустите виртуальную машину ***VM-1.***
  2. Перейдите в полноэкранный режим работы

***Выполняйте остальные задания лабораторной работы в виртуальной машине.***

#### Задание 2. Создайте новую политику *IP*-безопасности на локальном компьютере:

* 1. Откройте оснастку ***Управление политикой безопасности IP:***
     + откройте диалоговое окно ***Запуск программ* (*Пуск/Выполнить*)**;
     + введите команду ***mmc*** и нажмите клавишу ***Enter***;
     + выполните команду меню ***Консоль/Добавить или удалить***

оснастку;

* + - откройте окно с доступными оснастками с помощью кнопки

##### Добавить;

* + - выберите в списке элемент ***Управление политикой безопасности IP*** и добавьте его с помощью кнопки ***Добавить***;
    - завершите добавление оснастки кнопкой ***Готово***;
    - закройте диалоговое окно ***Добавить изолированнуюоснастку***;
    - закройте диалоговое окно ***Добавить/Удалить оснастку*** с помощью кнопки ***OK***.
  1. Активизируйте оснастку ***Политика безопасности IP на***

##### «Локальный компьютер».

*Справа отобразятся установленные по умолчанию политики.*

* 1. Запустите мастер создания политик безопасности:
     + вызовите контекстное меню оснастки ***Политика безопасности IP на «Локальный компьютер»***
     + выполните команду ***Создать политику безопасности IP…****.*
  2. Ознакомьтесь с информацией мастера и щелкните по кнопке ***Далее***.
  3. Установите Имя политики безопасности***IP***:
     + введите в поле ***Имя***–*My\_politic*.
     + введите в поле ***Описание***–*Это политика IP безопасности локального компьютера* и щелкните по кнопке ***Далее***.
  4. Настройте политику безопасного соединения. Для этого установите флажок *Использовать правило по умолчанию* и щелкните по кнопке

##### Далее.

* 1. Установите способ проверки подлинности правила отклика по умолчанию:
     + активизируйте ***Использовать данную строку для защиты обмена ключами***;
     + введите в нижнее поле *123456789*;
     + закройте окно кнопкой ***Далее***.
  2. Закройте мастера создания политики безопасности кнопкой ***Готово***.

*Откроется диалоговое окно* ***Свойства: My\_politic****.*

* 1. Запустите ***Мастер правил безопасности*** и настройте правила безопасности:
     + запустите мастер кнопкой ***Добавить***;
     + ознакомьтесь с описанием мастера и –***Далее***;
     + выберите *Это правило не определяет туннель* и щелкните ***Далее***;
     + выберите *Локальные сетевые подключения* и щелкните ***Далее***;
     + выберите *Использовать сертификат данного центра*

сертификации *(ЦС)*;

* + - щелкните ***Обзор*** и выберите ***любой сертификат***, кнопка ***Далее***;
    - в списке фильтров ***IP*** выберите *Полный IP трафик* и щелкните

##### Далее;

* + - добавьте *новое действие фильтра*:
      * щелкните по кнопке ***Добавить***;
      * ознакомьтесь с описанием запустившегося мастера и –***Далее***;
      * введите в поле ***Имя***–*My\_filter* и щелкните по кнопке ***Далее***;
      * выберите *Разрешить* и щелкните по кнопке ***Далее***;
    - завершите добавление нового действия кнопкой ***Готово***;
    - активизируйте созданное вами действие и измените его параметры:
      * щелкните по кнопке ***Изменить***;
      * выберите *Согласовать безопасность*;
      * щелкните по кнопке ***Добавить*** и выберите *Шифрование и обеспечение целостности*;
      * установите флажок *Принимать небезопасную связь, но отвечать с помощью IPSEC* и щелкните по кнопке ***Далее***;
      * завершите работу мастер кнопкой ***Готово***.
    - добавьте в политику фильтр для блокировки всех входящих подключений:
      * отключите использование мастера (флажок *Использовать мастер*);
      * откройте диалоговое окно ***Созданий новых правил*** кнопкой

##### Добавить;

* + - * откройте диалоговое окно ***Добавление фильтра*** кнопкой

***Добавить*** и добавьте новый фильтр:

* + - * + сбросьте флажок *Использовать мастер*;
        + откройте диалоговое окно ***Свойства: Фильтр*** кнопкой

##### Добавить;

* + - * + в поле ***Адрес источника пакетов*** выберите *Любой адрес IP*;
        + в поле ***Адрес назначения пакетов*** выберите *Мой IP адрес*;
        + установите флажок *Отраженный для блокировки приходящих пакетов*;
        + установите протокол ***TCP*** для фильтрации (***вкладка Протокол / раскрывающийся список Выберите протокол***);
        + завершите настройку нового фильтра кнопкой ***ОК***;
      * закройте диалоговое окно ***Список фильтров*** кнопкой ***ОК***.
      * завершите добавление нового правила кнопкой ***ОК***.
  1. Закройте диалоговое окно ***Свойства: My\_politic***.
  2. Активизируйте выбранную политику (***контекстное меню созданной политики/Назначить***).
  3. Проверьте работу политики, воспользовавшись утилитой ***ping*** на другом компьютере.

*Если политика настроена верно, то утилита* ***ping*** *выдаст сведения о том что данный компьютер недоступен.*

#### Задание 3.Настройте фильтрацию *IP*-трафика.

* 1. Откройте диалоговое окно свойств ***Подключения по локальной сети* (*Пуск/Панель управления/Сетевые подключения*)**.
  2. Откройте диалоговое окно ***Свойства: Протокол Интернета (TCP/IP)*** и щелкните по кнопке ***Дополнительно***.
  3. Перейдите на вкладку ***Параметры***.
  4. Откройте окно ***Фильтрация TCP/IP*** с помощью кнопки ***Свойства***.
  5. Установите ***TCP***-порты, которые можно использовать:
     + выберите в разделе ***TCP-порты*** переключатель *Только* и щелкните по кнопке ***Добавить***;
     + введите ***номер порта для протокола HTTPS***–*443*;
     + аналогично добавьте порты
       - для ***протокола отправки почты SMTP***–*25*;
       - для ***протокола получения почты POP3***–*110*;
       - для ***протокола FTP***–*21*;
       - для ***протокола Telnet***–*23*.
     + щелкните ***ОК*** для применения параметров.
  6. Запретите использование протокола ***Telnet***.
  7. Закройте окно ***Дополнительные параметры TCP/IP*** кнопкой ***ОК***.
  8. Закройте окно ***Свойства: Протокол Интернета (TCP/IP)*** кнопкой

***ОК***.

* 1. Проверьте настроенную фильтрацию. Для этого подключитесь по протоколу ***Telnet*** с другого компьютера (*программа* ***Telnet*** *входит в состав ОС* ***Windows*** *и используется для работы на удаленном компьютере в командной строке*).

#### Задание 4. Настройте брандмауэр *Windows*:

##### Откройте настройки брандмауэра (Пуск/Панель управления/Центр обеспечения безопасности/Брандмауэр Windows).

* 1. Разрешите доступ браузеру ***Internet Explorer*** к Интернету:
     + перейдите на вкладку ***Исключения*** и щелкните по кнопке

##### Добавить программу.

* + - выберите в списке ***Internet Explorer*** и щелкните по кнопке ***ОК***.
  1. Включите ведение журнала безопасности:
     + перейдите на вкладку ***Дополнительно***;
     + щелкните по кнопке ***Параметры*** в разделе ***Ведение журнала безопасности***;
     + включите запись пропущенных и успешных пакетов;
     + сохраните сделанные изменения кнопкой ***ОК***.
  2. Завершите конфигурирование брандмауэра кнопкой ***ОК***.
  3. Подключитесь к сети Интернет с помощью браузера ***Internet Explorer***.

*Если все настроено правильно, то вы сможете выйти в Интернет, в противном случае брандмауэр выдаст сообщение о том, что какая-то программа пытается получить доступ в Интернет.*

#### Задание 5. Самостоятельно откройте следующие порты на

**компьютере: *139, 444, 8080, 3128.***

#### Задание 6. Самостоятельно предоставьте доступ к Интернету браузерам *Opera* и *Firefox*.

**Задание 7. Самостоятельно запретите доступ к Интернету проигрывателю *WindowsMedia*.**

## Лабораторная работа 4.3 Создание резервных копий

**Цель:** научиться выполнять архивирование данных и пользоваться службой восстановления системы.

#### Средства для выполнения работы:

* **аппаратные:** компьютер с установленной ОС ***Windows XP.***
* **программные:** приложения ВМ: ***VirtualBox***; виртуальная машина***VM-1***.

***Теоретические сведения***

#### Архивация и восстановление

***Мастер архивации и восстановления* (*Backup or Restore Wizard*)** создает копию файлов и папок на указанном пользователем носителе информации. В случае потери или повреждения пользовательских данных их можно восстановить из файла резервной копии. Специалисты рекомендуют выполнять регулярное создание резервных копий важных файлов и папок. Частота архивации (*резервного копирования*) зависит от частоты изменений файлов, так как в случае потери данных придется повторно создать то, что было сделано после последней архивации. По этой причине многие компании создают резервные копии важных файлов ежедневно. Пользователь может выбирать различные типы архивации в зависимости от его требований:

* + для типа *Обычная (****Normal****)* происходит архивация всех выбранных файлов и системных настроек для определенной папки или диска, и каждый файл маркируется как прошедший архивацию (имеющий резервную копию);
  + для типа *Копирование (****Copy****)* происходит архивация всех выбранных файлов и системных настроек для определенной папки или диска, но файлы не маркируются как прошедшие архивацию;
  + для типа *Добавочная (****Incremental****)* происходит архивация только тех файлов, которые были созданы или изменены вслед за последней обычной или добавочной архивацией, и каждый файл маркируется как прошедший архивацию;
  + для типа *Разностная (****Differential****)* происходит архивация только тех файлов, которые были созданы или изменены вслед за последней обычной или добавочной архивацией, но файлы не маркируются;
  + для типа *Ежедневная (****Daily****)* происходит архивация только тех файлов, которые были созданы или изменены в данный день, но файлы не маркируются.

Тип архивации, который применяется, определяет, насколько сложным будет процесс восстановления. Для восстановления после нескольких добавочных или разностных архиваций необходимо выполнить восстановление из последней обычной резервной копии и из всех добавочных или разностных копий, полученных после обычной архивации и вплоть до настоящего момента.

Выполняя архивацию данных, пользователь указываете имя и место для файла резервной копии. По умолчанию файлы резервных копий сохраняются с расширением ***.bkf***. Файлы архивации можно сохранять на жестком диске, на гибком диске или на любом другом типе съемного носителя. При выборе места для резервной копии нужно учитывать размер файла архивации, типы имеющихся носителей, а также возможное требование того, что файлы резервных копий нужно хранить отдельно от компьютера на случай катастрофы.

#### Функция восстановления системы

Восстановление системы позволяет выполнить откат состояния операционной системы к одной из точек восстановления, фиксирующих состояние на момент, когда система стабильно работала. Преимуществом данной функции заключается в том, что она предоставляет возможность быстрого восстановления ("отката" состояния системы к состоянию, в котором она находилась в один из предыдущих моментов во времени) без

переустановки системы, а также не подвергает риску случайного перезаписывания рабочих файлов пользователей. Возможно выполнение отката к любому из следующих типов контрольных точек и точек восстановления:

* + *начальная контрольная точка (****initial system checkpoint****)* системы создается при первом запуске компьютера с вновь установленной ОС;
  + точки восстановления *для автоматических обновлений (****Automatic update restore points****)* создаются, когда инсталлируются обновления, которые загружаются с помощью ***Windows Update***;
  + точки восстановления *при восстановлении с резервной копии (****Backup recovery restore points****)* создаются, когда пользователь использует мастер архивации или восстановления (***Backup or Restore Wizard***);
  + пользователь может создавать свои *собственные точки восстановления вручную ("ручные" контрольные точки* ***– manual checkpoints****)* в любой момент с помощью мастера восстановления системы (***System Restore Wizard***);
  + точки восстановления *при инсталляции программ (****Program name installation restore points****)* создаются, при установке программного обеспечения;
  + точки восстановления *для операции восстановления (****Restore operation restore points****)* создаются каждый раз, когда пользователь осуществляете какое-либо восстановление;
  + *системные контрольные точки (****System checkpoints****)*– это запланированные точки восстановления, которые создаются компьютером регулярно, даже если пользователь не вносил никаких изменений в систему;
  + точки восстановления *для неопознанного устройства (****Unsigned device driver restore points****)* создаются, когда устанавливается драйвер устройства, который не был опознан или сертифицирован.

Средство ***Восстановление системы* (*System Restore*)** обычно сохраняет набор контрольных точек восстановления за период от одной до трех недель. Количество контрольных точек восстановления, доступных в любой заданный момент времени, ограничено объемом пространства,

которое выделено пользователем для работы системы восстановления. Максимальный размер пространства, которое можно выделить, составляет приблизительно 12 процентов.

В ходе процедуры восстановления происходит восстановление ОС и программ, инсталлированных на компьютере, к состоянию, в котором они находились на момент выбранной контрольной точки восстановления. Этот процесс не затрагивает личные файлы пользователя (включая сохраненные документы, сообщения электронной почты, адресную книгу, список ***Избранные* (*Favorites*)** и список ***Журнал* (*History*) *Интернет Explorer***).

Все изменения, внесенные утилитой ***Восстановление системы*(*System Restore*)**, полностью обратимы, и если пользователя не удовлетворяют результаты, то можно восстановить предыдущие настройки и выполнить все снова.

### Выполнение работы

#### Задание1. Выполните резервное копирование системных конфигурационных файлов.

* 1. Запустите виртуальную машину ***VM-1*** и загрузите ОС ***Windows***.
  2. Запустите ***Мастер Архивации***

##### (Пуск/Программы/Стандартные/Служебные/Архивация данных).

* 1. Ознакомьтесь с информацией мастера и щелкните ***Далее***.
  2. Выберите возможность мастера –*Архивация файлов и параметров*и щелкните ***Далее***.
  3. Укажите выбор элементов архивирования в самостоятельном режиме

–*Предоставить возможность выбора объектов для архивации* и щелкните ***Далее***.

* 1. Укажите элементы для архивации – папки ***Documents and Settings*** и

***Program Files*** и щелкните ***Далее***.

* 1. Укажите место хранения архива:
     + откройте диалоговое окно ***Сохранить*** как кнопкой ***Обзор***;
     + перейдите в корневой каталог диска **C:**
     + введите в поле ***Имя Файла***– имя сохраняемого файла –*Резервная Копия*;
     + сохраните файл кнопкой ***Сохранить***;
     + подтвердите введенные данные кнопкой ***Далее***.
  2. Настройте дополнительные параметры архивации:
     + откройте диалоговое окно дополнительных параметров кнопкой

##### Дополнительно;

* + - выберите в раскрывающемся списке ***тип архивации***–*Обычный* и щелкните ***Далее***;
    - установите флажок *Проверять данные после архивации* (***Далее***);
    - укажите ***способ добавления архива***–*Добавить этот архив к*

существующему (***Далее***);

* + - укажите ***время архивации***:
      * установите радиокнопку *Позднее*;
      * введите имя задания в соответствующее поле;
      * откройте диалоговое окно ***Запланированное задание*** кнопкой

##### Расписание;

* + - * введите в поле ***Время начала*** время на *2* минуты позже текущего (например, если сейчас 12.40, то вам необходимо ввести 12.42);
      * подтвердите введенные параметры кнопкой ***ОК***;
    - завершите ввод времени выполнения архивации кнопкой ***Далее***;
    - введите данные пользователя от имени которого будет выполняться архивирование:
      * введите в поле ***Пользователь*** имя пользователя на компьютере –

*USER*;

* + - * введите в поля ***Пароль*** *и* ***Подтверждение пароля*** для пользователя *USER*;
      * подтвердите ввод данных кнопкой ***ОК***;
  1. Завершите работу мастера кнопкой ***Готово***.

#### Задание 2. Выполните восстановление системных конфигурационных файлов.

* 1. Запустите ***Мастер Архивации***

##### (Пуск/Программы/СтандартныеСлужебные/Архивация данных).

* 1. Ознакомьтесь с информацией мастера и щелкните ***Далее***.
  2. Выберите возможность мастера – ***Восстановление файлов и параметров*** и щелкните ***Далее***.
  3. Выберите для восстановления в левом списке с содержимым архива, папку ***Мои рисунки*** (***Далее***).
  4. Ознакомьтесь с выбранными параметрами и активизируйте восстановление кнопкой ***Готово***.
  5. Откройте отчет кнопкой ***Отчет*** и просмотрите его.
  6. Закройте диалоговое окно ***Ход восстановления*** кнопкой ***Закрыть***.

#### Задание 3. Создайте точку восстановления.

* 1. Запустите мастер ***Восстановление системы***

##### (Пуск/Программы/Стандартные/Служебные).

* 1. Ознакомьтесь с информацией мастера.
  2. Создайте точку восстановления:
     + Установите радиокнопку *Создать точку восстановления* (***Далее***);
     + введите в текстовое поле ***Oписание контрольной точки***восстановления–*Тестовая точка восстановления*;
     + создайте точку восстановления кнопкой ***Создать***.
  3. Завершите работу мастера кнопкой ***Закрыть***.

**Задание 4. Самостоятельно выполните восстановление системы по созданной ранее контрольной точке.**

## Примерные тестовые задания к модулю 4

1. К сервисам безопасности относят:

*идентификация/аутентификация;*

*протоколирование/аудит;*

*шифрование;*

*аудит.*

1. Потенциальные угрозы, определяющие задачи защиты информации в

*прослушивание каналов;*

*уничтожение или искажение информации;*

*выход из строя операционной системы;*

*внедрение сетевых вирусов.*

1. Конфиденциальность – это:
   * *предотвращение пассивных атак для передаваемых или хранимых данных;*
   * *защита от возможных отказов от фактов отправки, приема или содержания отправленных или принятых данных;*
   * *подтверждении подлинности взаимодействующих объектов;*
   * *защита от несанкционированного использования ресурсов*

*сети.*

1. К механизмам безопасности относят:

*хэш-функции;*

*целостность сообщения;*

*алгоритмы симметричного шифрования;*

*невозможность отказа от полученного сообщения.*

## Контрольные вопросы к модулю 4

1.Потенциально возможные угрозы. 2.Основные механизмы безопасности.

3.Основные опасности при работе в Интернет с помощью браузера. 4.Java-апплеты.

5.Управляющие элементы ActiveX. 6.Параметры конфиденциальности браузера. 7.Цифровые подписи.

8.Сертификаты.

# Модуль 5.

# Возможности мультисервисных сетей

**Цель:**познакомиться с основными принципами построения и использования мультисервисных сетей.

**Результат:**уметь организовывать потоковое вещание(настраивать и запускать потоковый сервер, подключаться к потоковому серверу); использовать программы IP-телефонии (организовывать передачу голосовых данных по локальной сети, настраивать работу программного ***IP***-телефона); организовывать видеоконференции (подключать web-камеру, настраивать программное обеспечение web-камеры, проводить сеанс телеконференции).

#### План освоения модуля:

1. Изучите следующие темы в указанных источниках:
   * *Мультисервисная сеть (МСС):основная задача и возможности.*
   * *Архитектура МСС.*
   * *Основные услуги МСС.*
   * *Спутниковые технологии сети SPIN.*
2. Выполните и представьте преподавателю лабораторные работы:
   * ЛР 5.1. *Потоковое вещание.*
   * ЛР 5.2. *IP-телефония.*
   * ЛР 5.3. *Видеоконференция.*
3. Выполните самостоятельные задания к модулю.
4. Выполните тестовые задания к модулю. **V.**Защитите модуль по контрольным вопросам. **Литература:**
5. Звук в сети Интернет \\ Компьютер Пресс. – 2001 – № 6.
6. Ханикат Дж. Знакомство с Microsoft Windows Server 2003 / Пер. с англ. –/ Дж Ханикат, М.: Издательско-торговый дом «Русская Редакция», 2003. – 454 с. (Гл. 10).
7. Величко В.В. Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 3. – Мультисервисные сети. / В.В.Величко[и др.]; под ред. В.П.Шувалова. – М.: Горячая линия – Телеком, 2005. – 592 с. (Гл. 2)
8. Таненбаум Э. Компьютерные сети. 4-е изд. / Э.Таненбаум. – СПб.: Питер, 2003. – 992 с. (Гл. 5, с.458; Гл. 7, с. 167)
9. Галичский К.В. Компьютерные сети в телефонии / К.В. Галичский–

СПб.: БХВ-Петербург, 2002. – 400 с. (Гл. 1)

1. Росляков А.В. IP-телефония / А.В.Росляков [и др.]; под ред. М.Ю.Самсонов– М.: Эко-Трендз, 2003. – 252 с.
2. Экслер А.Б. Общение в Интернете / А.Б. Экслер. – М.: НТ Пресс, 2006. – 384 с. (Гл. 2)
3. Корнилов Д. Проектирование и построение сетей видеоконференцсвязи \\ Connect!Мир связи. / Д. Корнилов – 2004 – №3 (Электронная версия журнала: <http://www.connect.ru/article.asp?id=4514> )
4. Корнилов Д. Проектирование и построение сетей видеоконференцсвязи \\ Connect!Мир связи. / Д. Корнилов– 2004 – №4 (Электронная версия журнала: <http://www.connect.ru/article.asp?id=4545> )
5. Ершов В.А. Мультисервисные телекоммуникационные сети / В.А.Ершов

* М.: Изд-во МГТУ им. Н.Э.Баумана, 2003. – 432 с. (Гл. 1)

**Лабораторная работа 5.1 Потоковое вещание**

**Цель:** научиться организовывать потоковое вещание.

#### Средства для выполнения работы:

* + **аппаратные:** компьютер, подключенный к ЛВС;
  + **программные:** приложение ВМ ***VirtualBox***, виртуальная машина

***VM-2.***

***Теоретические сведения***

***Потоковая передача данных (streaming)***– способ передачи данных малыми *порциями (пакетами)*, причем каждая переданная порция может использоваться без того, чтобы ожидать окончания передачи всего файла.

Потоковая передача данных позволяет передавать мультимедийную информацию и одновременно обеспечивает её прием группой абонентов, территориально удалённых друг от друга.

*Суть потоковой передачи данных* заключается в следующем. Передаваемые медиа-файлы сжимаются и разделяются на части (пакеты), а затем последовательно передаются пользователю. Размер пакетов определяется пропускной способностью участка сети или канала связи между клиентом и сервером, передающим видеосигнал. Накопив достаточное количество пакетов в буфер, программа-клиент приступает к воспроизведению одного из них и одновременно получает и выполняет

декомпрессию следующих. Основной задачей, стоящей перед буфером, является обеспечение плавного и непрерывного воспроизведения видеосигнала. На практике результаты работы таких приложений по- прежнему очень сильно зависят от быстродействия компьютера и от скорости сетевого соединения, поэтому качество звука/видео – это всегда компромисс. Размер потока (*битрейт*) напрямую влияет на качество воспроизведения, от него также во многом зависит и то, можно ли будет смотреть видео по сети. Размер потока можно узнать в свойствах файла, однако многие кодеки используют динамически меняющийся битрейт, поэтому даже указанному значению иногда не следует верить.*Достоинство* такого метода передачи файлов состоит в возможности воспроизводить файл практически мгновенно, быстро прокручивать запись вперед, начинать проигрывание с любого места, приостанавливать и прекращать его, не тратя при этом время и ресурсы сети на полную загрузку файла. *Основной проблемой* потокового вещания является качество воспроизводимого продукта. Производители ищут алгоритмы, позволяющие делать интеллектуальный анализ для аппроксимации (замещения) потерянных данных, надеясь таким образом улучшить качество передаваемой информации. Этим и обусловлено отсутствие общего стандарта среди существующих программ приема потокового вещания.

Существует *два способа воспроизведения удалённых медиа-файлов:*

 использовать ПК или другое устройство, способное работать с локальными и сетевыми файлами. В этом случае достаточно найти в сети и запустить на воспроизведение нужный файл. Он будет воспроизводиться через ту сетевую файловую систему, которую использует ваша ОС. В большинстве случаев это будет ***SMB (Server Message Block)*** , работающая на верхних уровнях стека ***TCP/IP***;

 использовать для воспроизведения медиа-сервер и протокол потокового вещания, который будет доставлять медиа-поток от сервера к плееру. Для передачи потока используются такие *протоколы*, как ***RTP*** и ***RTCP***, работающие поверх ***UDP***.

Отличие между ними заключается в том, что ***TCP/IP*** обеспечивает надёжную доставку, а ***UDP***– нет, поскольку ***TCP*** имеет встроенные

механизмы контроля доставки и целостности данных. Однако ***TCP*** нельзя назвать лучшим решением для передачи мультимедиа, поскольку этот протокол добавляет в пакеты данных большое количество служебной информации. Для ***TCP*** главное – безошибочно передать данные, а время доставки вторично.

С другой стороны, ***UDP*** использует гораздо меньше служебных данных, чем ***TCP***, поэтому он лучше подходит для приложений, работающих с потоковыми данными, где на первый план выходит время доставки информации. Что касается пропусков и искажений пакетов, то решение этой проблемы возлагается на принимающую сторону.

Реализация второго способа воспроизведения удаленных медиа- файлов возлагается на серверную операционную систему. ***Службы Windows Media*** в составе ***Microsoft Windows Server 2003***– это группа служб, которые предназначены для передачи клиентам аудио- и видеоинформации при помощи одноадресного и группового вещания. ***Службы Windows Media*** используются также для передачи файлов клиентам. Поставляемое содержимое может быть создано, приобретено у поставщика или передаваться с телевизионных камер и микрофонов. В последнем случае его называют живым потоком (*live stream*). Они так же позволяют управлять распространением содержимого, используя серверные списки воспроизведения и механизмы демонстрации рекламных материалов. Это гарантирует своевременную доставку содержимого по назначению и позволяет объединять серверы при помощи новейших протоколов и механизмов кэширования/замещения. Пользователи могут обращаться к поставляемому содержимому через Интернет, через корпоративную или образовательную интрасеть или через специализированные группы, которые получают содержимое в выделенной сети или в интрасети.

### Выполнение работы

#### Задание 1. Установка и настройка потокового сервера

##### Установите Сервер потоков мультимедиа (Пуск / Администрирование / Управление данным сервером / Добавить или удалить роль):

* + - выберите из списка предлагаемых ролей сервера *Сервер потоков мультимедиа*;
    - перейдите к установке необходимых компонентов (***Далее***);
    - после появления сообщения *Этот сервер теперь является сервером потоков мультимедиа* закройте окно мастера (***Готово***).
  1. Ознакомьтесь с возможностями установленного сервера потоков мультимедиа – откройте диалоговое окно***Службы Windows Media*(*Пуск /Администрирование / Управление данным сервером / Сервер потоков мультимедиа / Управление этим сервером потоков мультимедиа*)**:
     + раскройте список с именем сервера в левой части панели (по умолчанию создается сервер с именем компьютера):
       - *Диагностика*– отображение диагностических сведений при работе с сервером;
       - *Управление прокси-сервером и кэшем*– управление подключаемого извне прокси-сервера и кэша (существующий или созданный модуль) – используется для сохранности полосы пропускания, снижения задержки по сети и снятия нагрузки с сервера источника;
       - *Пункты публикации*– управление существующими пунктами публикации на сервере, которые отображаются в списке и на вкладке ***Краткие сведения*** (правая часть окна). При выборе конкретного пункта публикации предоставляет следующие элементы управления: мониторинг вещания (*Монитор*), определение источника вещания (*Источник*), управление потоками рекламных объявлений (*Объявления*) и способами их подключения (*Объявить*), свойства пункта публикации(*Свойства*).

#### Задание 2. Организация вещания в сети.

* 1. Создайте новый пункт публикации:
     + откройте ***Мастер добавления публикаций***: выберите в списке левой части панели ***Пункты публикаций*** и нажмите кнопку ***Добавить пункт публикации*** на вкладке ***Краткие сведения*** и нажмите кнопку ***Далее***;
     + введите ***имя публикации***–*Media*и перейдите к следующему шагу (***Далее***);
     + укажите ***Тип содержимого для потоковой передачи***–*Файлы (мультимедиа или списки воспроизведения) в каталоге* и перейдите к следующему шагу (***Далее***);
     + укажите ***Тип пункта публикации***–*Широковещательный пункт публикации* и перейдите к следующему шагу (***Далее***);
     + укажите ***Способ передачи содержимого***–*Одноадресный* и перейдите к следующему шагу (***Далее***);
     + укажите ***Каталог содержимого***–*C:\WMPub\WMRoot* (по умолчанию) и перейдите к следующему шагу (***Далее***);
     + укажите ***режим Воспроизведения содержимого***–*Повтор* и перейдите к следующему шагу (***Далее***);
     + НЕ включая регистрацию данных о клиентах, перейдите к следующему шагу (***Далее***);
     + проверьте все указанные ***Параметры пункта публикации***, снимите флажок *Запустить пункт публикации при закрытии мастера* и перейдите к следующему шагу (***Далее***);
     + на завершающем этапе создания пункта публикации снимите флажок *После завершения работы мастера* и закончите работу ***Мастера добавления пункта публикации*** (***Готово***);
     + убедитесь в наличии добавленного пункта публикации ***Mediа*** в списке ***Пункты публикации*** (и на вкладке ***Краткие сведения****).*
  2. Настройте созданный пункт публикации:
     + создайте список воспроизведения, который будет транслироваться сервером потоков мультимедиа;
     + выделите в левой панели ***Службы Windows Media*** пункт публикации ***Media***и перейдите в правой панели на вкладку ***Объявления***;
     + создайте файл списка воспроизведения, включив в него 2 статических рекламных объявления и видеоролик:
       - запустите ***Мастер создания сопровождения*** кнопкой***Редактор сопровождений***, установите радиокнопку *Создать файл списка воспроизведения* и флажок *Использовать мастер создания сопровождения* (***ОК***);
       - начните работу мастера, нажав кнопку ***Далее***.

*Файл списка воспроизведения сопровождения по умолчанию содержит элемент* ***Содержимое, запрошенное клиентом (%requestedurl%)****, который представляет запрашиваемое пользователем содержимое с пункта публикации. В списке воспроизведения он может стоять либо первым, либо последним.*

* + - * в диалоговом окне ***Добавление объявления*** (кнопка ***Добавить объявление***) укажите каталог объявления (кнопка ***Обзор...***) – выберите файл ***proseware\_leadin.jpg*** и нажмите кнопку ***Выбрать файл*** (при необходимости можно выбрать другой файл из другой папки, имеющейся на компьютере). Убедитесь, что в поле окна Добавление объявления появилась строка ***C:\WMPub\WMRoot\proseware\_leadin.jpg*** (***ОК***);
      * самостоятельно добавьте этот же файл еще раз: рекламное объявление будет начинать и заканчивать показ.

*Обратите внимание на то, что добавленные файлы помечаются синим флажком.*

* + - * самостоятельно добавьте видеоролик ***industrial.wmv***, расположенный в той же папке (кнопка ***Добавить мультимедиа***);
      * расположите выбранные файлы в указанном порядке, выделяя соответствующие файлы и перемещая их по списку с помощью кнопок *Вверх* и *Вниз* в окне ***Мастера создания сопровождения***, и перейдите к следующему шагу (***Далее***);
      * сохраните файл списка воспроизведения (в предлагаемом месте и с предлагаемым именем –***Media\_wrapper.wsx***) и перейдите к следующему шагу (***Далее***);
      * на завершающем этапе работы ***Мастера создания сопровождения*** снимите флажок *Запустить пункт публикации при закрытии мастера* и оставьте флажок *Включить список воспроизведения сопровождения после закрытия мастера*. Нажмите кнопку Готово;
  1. Выполните редактирование источника содержимого потоковой передачи:
     + активизируйте вкладку ***Источник***;
     + укажите в качестве источника в группе ***Источник*** содержимого созданный файл списка воспроизведения сопровождения – кнопка ***Изменить...***– полный путь к файлу списка воспроизведения автоматически будет размещен в строке ***Папка***:

*При этом содержимое файла списка воспроизведения отобразится на вкладке ниже.*

* + - выполните пробное потоковое вещание:
      * убедитесь что кнопка ***Повторять список воспроизведения*** на

панели инструментов находится в состоянии *выключено*;

* + - * запустите пункт публикации соответствующей кнопкой на панели инструментов в нижней части окна. При этом значок подключения на левой панели окна ***Службы Windows Media*** сменится на активный, а на вкладке ***Источник*** начнется воспроизведение указанного файла;
      * подключите ***Проигрыватель Windows Media*** кнопкой ***Пробный поток*** в нижней части окна. В открывшемся окне ***Пробный поток – Media (широковещательный) на WIN2003*** просмотрите весь ролик и убедитесь, что созданный вами порядок воспроизведения мультимедийных файлов сохранен;
        + закройте пробное вещание кнопкой ***Выход***.
* НЕ останавливая пункт публикации, сверните окно ***Службы Windows Media*** на ***Панель задач***.

#### Задание 3. Организуйте прием потокового вещания в сети.

* 1. Настройте клиент в среде ВМ:

##### запустите приложение Проигрыватель Windows Media (Пуск / Все программы / Стандартные / Развлечения / Проигрыватель Windows Media);

* + - выполните настройку сетевых подключений:
      * откройте диалоговое окно ***Параметры* (*Контекстное меню зоны заголовка / Сервис / Параметры...*)**;
      * убедитесь, что на вкладке ***Сеть*** выбраны все протоколы потоковой передачи и установлен флажок ***Использовать порты 7000–7007*** для получения данных;
      * установите скорость подключения на вкладке ***Быстродействие***: выберите из открывающегося списка *ЛВС (10Мбит/с и более)*.
      * подтвердите установленные параметры (***ОК***).
  1. Подключите клиент к серверу (в среде ВМ):
     + откройте диалоговое окно ***Открытие адреса URL* (*Контекстное меню зоны заголовка / Файл / Открыть адрес URL...*)**;
     + в строке ***Открыть***: укажите адрес открываемого файла –

***mms: \\Win2003\Media\Media\_wrapper.wsx*** и нажмите ***ОК***;

* + - просмотрите транслируемый мультимедийный ролик;
    - сверните приложение ***Проигрыватель Windows Media*** на ***Панель задач***.

#### Задание 4. Самостоятельно выполните настройку клиента (на физическом компьютере) и его подключение к серверу потоков мультимедиа.

**Задание 5. Выполните одновременное подключение к серверу клиента на физическом компьютере и клиента в среде ВМ.**

**Задание 6. Создайте список воспроизведения, состоящий из стандартных звуковых файлов Windows (C:\Windows\Media) и настройте его потоковое вещание.**

## Лабораторная работа 5.2.

## IP-телефония

**Цель:** научиться организовывать передачу голосовых данных в ***IP***-сети.

#### Средства для выполнения работы:

* **аппаратные:** 2 компьютера с возможностью подключения к ***Internet***, гарнитура (наушники и микрофон);
* **программные:** ОС ***WindowsXP***; программный ***IP***-телефон (***SipPoint***,

***Skype***).

***Теоретические сведения***

*Телефония* основана на коммутации соединений, когда для создания соединения между абонентами на все время разговора выделяются каналы для передачи звука. Кроме этого, телефонные соединения можно организовывать и в цифровых сетях, где для передачи данных используется принцип коммутации пакетов. Именно эту задачу и решает Интернет- телефония (***IP****-телефония,* ***VoIP***). Главное преимущество ***IP****-телефонии*– себестоимость: минута разговора в случае междугородной, и тем более, международной связи оказывается во много раз дешевле, чем при использовании традиционной связи по сетям с коммутацией соединения. Это в значительной степени оправдывает даже сравнительно низкое качество звука, присущее современной *IP-телефонии*.

Сеть ***IP****-телефонии* представляет собой совокупность оконечного оборудования, каналов связи и узлов коммутации. Сети ***IP****-телефонии* строятся по тому же принципу, что и сети Интернет. Однако в отличие от сетей Интернет, к сетям ***IP****-*телефонии предъявляются особые требования

по обеспечению качества передачи речи. Одним из способов уменьшения времени задержки речевых пакетов в узлах коммутации является сокращение количества узлов коммутации, участвующих в соединении.

Существует несколько классификаций сетей ***IP***-телефонии:

* + *По способу связи оконечных устройств между собой:*

выделенные, интегрированные, смешанные.

* + - *В выделенных сетях* связь между оконечными устройствами осуществляется по выделенным каналам, и пропускная способность этих каналов используется только для передачи речевых пакетов. Чаще всего провайдеры ***IP****-телефонии* не строят собственную сетевую инфраструктуру, а арендуют каналы у провайдеров первичной сети. Главное преимущество выделенной сети – это высокое качество передачи речи. Кроме этого, для обеспечения гарантированного качества предоставляемых услуг в этих сетях, кроме протокола ***IP***, применяются и другие транспортные протоколы: ***АТМ*** и ***FrameRelay***.
    - *В интегрированных сетях* ***IP****-телефонии* для связи между устройствами используется глобальная сеть Интернет. Это может быть уже существующая собственная сеть или доступ к сети Интернет через провайдеров.
    - *В сетях смешанного типа* для объединения устройств используются выделенные каналы и сеть Интернет. Вопрос о том, какие каналы использовать *для* связи устройств между собой, решается оператором индивидуально в зависимости от возможностей.
  + *По масштабу:* международные, региональные, местные.
    - *Международная сеть IP-телефонии* имеет точки своего присутствия в нескольких странах и обеспечивает терминацию трафика практически в любую точку мира при минимальном использовании телефонной сети общего пользования. Эти сети строятся с использованием выделенных каналов и на базе уже существующих сетей Интернет.
    - *Национальная сеть* имеет точки своего присутствия в одной или, в *крайнем* случае, в нескольких близлежащих странах и обслуживает абонентов и местных операторов только этого региона. С помощью заключения договоренности с

международными сетями национальная сеть предоставляет своим абонентам и другим местным сетям возможность терминации вызовов в любую точку мира.

* + - *Местная сеть IP-телефонии* предоставляет возможность абонентам местной телефонной сети и частным компаниям воспользоваться *услугамиIP-телефонии*. В основном, операторы местных сетей являются провайдерами доступа к сети ***IP-***телефонии. Чаще всего, их сети имеют всего один *шлюз*, подключенный к более крупным сетям через сеть Интернет или по выделенным каналам. Для большинства операторов местная сеть является лишь промежуточным этапом развития, и они стремятся выйти на международный или национальный уровень.

Международный союз электросвязи (***IUT-T***) предложил стандарт ***Н.***

***323*** для построения сетей ***IP***-телефонии. Этот стандарт охватывает практически все аспекты создания таких сетей и в настоящее время является наиболее распространенным. Сети ***Н.323*** ориентированы на интеграцию с обычными телефонными сетями и рассматриваются как сети ***ISDN***, работающие поверх сетей передачи данных –***TCP/IP*** (Интернет), сетей ***IPX, Ethernet, Fast Ethernet, Token Ring*** и т.д. Стандарт ***Н.323*** содержит большое количество протоколов, связанных с регистрацией оборудования, различными сценариями установления соединений, передачи речи, видео и данных, аутентификацией пользователей, тарификацией и многими другими задачами.

При использовании ***IP***-телефонии необходимо учитывать, что адресация узлов в сети Интернет определяется не обычным числовым номером абонента, а ***IP***-адресом компьютера, с которого (и на который) устанавливается соединение. Во многих случаях ***IP***-адрес компьютера динамически меняется при очередном подключении, поэтому для соединения используют специальный узел сети –*сервер каталогов (****directory server****)*. Этот сервер хранит списки зарегистрированных на нем пользователей, причем каждый из них имеет уникальное имя в виде строки символов (обычно в формате адреса электронной почты) или традиционный номер, состоящий из цифр.

Существует такая разновидность узлов сети ***IP***-телефонии –*шлюз (****gateway****)*. Это посредник между традиционной телефонной сетью и сетью передачи данных, преобразующий звонки одного типа в другой и обратно.

Передача телефонных переговоров по сети Интернет может осуществляться по нескольким сценариям.

*Использование программы* ***IP****-телефонии*. В этом случае на двух компьютерах, подключенных к Интернету, необходимо запустить специальную программу, которая на одном конце преобразует звук от микрофона в пакеты данных, а на другом конце выполняет обратное преобразование и проигрывает звук в динамик. Далее работа осуществляется по следующему алгоритму:

1. Пользователь ***А*** запускает программу при установленном подключении к Интернет;
2. Программа ***IP***-телефонии автоматически сообщает серверу каталогов, что вызывающий пользователь (***А***) доступен для входящих звонков и имеет такой-то ***IP***-адрес;
3. Программа ***IP***-телефонии пользователя ***В*** запросит сервер каталогов по символьному имени пользователя ***А*** соответствующий ему ***IP***-адрес и начнет передачу пакетных данных.
4. Пользователь ***А*** получит уведомление о входящем Интернет- звонке от пользователя***В*** и, ответив на звонок, окончательно установит соединение.

*Использование* ***IP****-телефона*. Внешне это устройство выглядит как обычный телефон, но подключается непосредственно к сети передачи данных. В отличие от компьютера ***IP***-телефон, как и обычный телефон, всегда готов к работе. ***IP***-телефония помимо передачи звуковой информации между двумя собеседниками может быть использована в качестве организации конференцсвязи (большинство существующих программ ***IP***-телефонии поддерживает эту возможность), и как средство для организации видеотелефонии, если с обеих сторон имеется соответствующее программное и аппаратное обеспечение.

### Выполнение работы

#### Задание 1.Создайте учетную запись (на сайте поставщика услуг IP- телефонии).

* 1. Откройте в окне браузера сайт поставщика услуг ***IP***-телефонии: [***www.sipnet.ru***.](http://www.sipnet.ru/)
  2. В верхней части окна выберите ссылку ***Зарегистрироваться!***

(Регистрация новых пользователей).

* 1. Заполните ***Регистрационную форму данных***. Обратите внимание на *обязательно заполняемые поля* и *Примечания*, описывающие правила заполнения регистрационной формы. Для принятия введенных данных выберите ***Продолжить регистрацию***.
  2. В случае успешной регистрации будет выведено окно ***Клиент успешно зарегистрирован***. Вернитесь на главную страницу сайта (ссылка ***Перейти на сайт*** в правом верхнем углу).
  3. Зайдите в ***Личный кабинет***, используя только что созданную учетную запись (логин/пароль).
  4. Изучите ***Информацию об аккаунте*** (верхняя часть окна): ***SIP ID*** *(персональный идентификатор – аналог телефонного номера), Статус аккаунта, количество средств на счете* и др.
  5. Ознакомьтесь с информацией о возможностях присвоенного вам статуса аккаунта (ссылка ***Изменить статус аккаунта***).
  6. Сверните окно браузера на ***Панель задач***.

#### Задание 2.Установите и настройте работу программного IP-телефона.

* 1. Установите программу ***SipPoint*** (файл инсталляции

##### SippointSetup.exe):

* + - оставьте все предлагаемые по умолчанию параметры установки, приняв лицензионное соглашение;
    - на шаге ***Выберите дополнительные задачи*** снимите флажок

*Запускать программу при каждой загрузке Windows*.

* 1. Выполните настройку программы ***SipPoint***, оставляя настройки «по умолчанию», за исключением:
     + при выборе полосы пропускания вашего подключения к сети Интернет установите радиокнопку ***Dialupподключение 56 кбит/с*;**
     + введите *учетные данные*, полученные вами при регистрации на сайте;
     + при выборе способа подключения к службе мгновенных сообщений оставьте *Автоматическая настройка*.

*После закрытия* ***Мастера определения подключения к сети*** *программа* ***IP****-телефонии автоматически предлагает настройку звуковых и видеоустройств, подключенных к вашему ПК – окно* ***Audio and Video Tuning Wizard****.*

* 1. Настройка гарнитуры для общения в программе ***SipPoint***.
     + подключите гарнитуру к соответствующим разъемам звуковой

карты ПК и убедитесь, что закрыты любые другие программы воспроизведения медиа-файлов (***Далее***);

* + - установите гарнитуру в рабочее положение (***Далее***);
    - проверьте правильность выбранных устройств в раскрывающемся списке (***Далее***);
    - настройте оптимальную громкость звука в наушниках, нажав кнопку ***Click to Test*** и используя бегунок регулятора ***SpeakerVolume***(***Далее***);
    - настройте оптимальную чувствительность микрофона: проговаривая любую фразу и перемещая бегунок регулятора ***MicrophoneVolume***, добейтесь наилучшей слышимости собственного голоса в наушниках (***Далее***);
    - закончите настройку гарнитуры (***Готово***).
  1. Ознакомьтесь с интерфейсом программы ***SipPoint*** (подключение к сети происходит автоматически после запуска программы)
     + вкладка ***Телефоны*** содержит добавленные номера телефонов, на которые осуществляются звонки (является основной для осуществления звонка);
     + вкладка ***Контакты*** содержит доступные для работы группы;
     + вкладка ***Звонки*** показывает информацию о состоянии соединения (*Звонки отсутствуют, Звоним, Разговариваем, Конец разговора*), продолжительности разговора, используемом кодеке (в случае установленного соединения), уровень чувствительности микрофона и громкости наушников;
     + панель с кнопками ***Осуществить или принять звонок*** и ***Закончить или отклонить разговор*** (активны только для вкладок ***Телефоны*** и ***Звонки***);
     + ***статус-строка***, показывающая текущее значение счета и статус пользователя в сети.

#### Задание 3.Организуйте звонок с помощью программы SipPoint.

* 1. Организуйте звонок по номеру, не состоящему в списке контактов:
     + перейдите на вкладку ***Телефоны*** и введите в строку ***Здесь введите SIP ID или номер для быстрого звонка*** номер телефона (городской АТС) в формате:

*<код\_страны>–<код\_города>–<номер\_телефона>*;

* + - установите соединение, нажав на кнопку ***Осуществить или***

##### принять звонок;

* + - закончите разговор, нажав на кнопку ***Закончить или отклонить разговор***.
  1. Организуйте звонок абоненту из телефонной книги:
     + добавьте новый контакт на вкладке ***Телефоны*** в предложенном формате (***Контекстное меню/Добавить телефон***);

*В качестве нового телефона укажите, например, номер своего мобильного телефона или номер своего друга. Входящий звонок для него будет бесплатным.*

* + - выполните вызов двойным щелчком по названию контакта. *Обратите внимание, что автоматически произойдет переключение на вкладку* ***Звонки****, вверху которой отобразится номер, на который вы осуществляете вызов.*
    - закончите разговор, нажав на кнопку ***Закончить или отклонить разговор***.
  1. Проверьте текущее значение счета в статус-строке и закройте приложение (***Файл/Выход***).
  2. Создайте снимок экрана с обновленной информацией ***Личного кабинета*** в браузере и сохраните его в личной папке.
  3. Выполните деинсталляцию программы ***SipPoint* (*Пуск/Панель управления/Установка и удаление программ*)**.

#### Задание 4.Самостоятельно выполните установку и настройку программы *IP*-телефонии *Skype* (на два компьютера).

**Задание 5.Самостоятельно организуйте звонок с одного компьютера на другой.**

## Лабораторная работа 5.3.

## Видеоконференция

**Цель:** научиться организовывать видеоконференцию в локальной сети.

#### Средства для выполнения работы:

* **аппаратные:** 2 компьютера, подключенных к ЛВС; 2 Web-камеры; 2 гарнитуры;
* **программные:** ОС ***Windows XP***; программное обеспечение для Web- камеры; программа ***Windows Messenger,Mail.RuАгент***.

***Теоретические сведения***

*Видеоконференция*–вид телекоммуникаций между двумя и более абонентами, который позволяет им видеть и слышать друг друга независимо от разделяющего их расстояния. Для организации видеоконференций используется технология –*видеоконференцсвязь*. Общение в режиме видеоконференций также называют сеансом видеоконференцсвязи.

*Видеоконференцсвязь (ВКС)*– телекоммуникационная технология, обеспечивающая организацию видеоконференций между двумя и более абонентами по сети передачи данных. Во время cеанса ВКС обеспечивается интерактивный обмен звуком и изображением. Также абоненты могут транслировать телеметрические данные, компьютерные данные, демонстрировать документы и объекты с использованием дополнительных видеокамер. Передача потока звука и видео по сети передачи данных обеспечивается путем кодирования/декодирования данных (аудио и видео потока) с использованием стандартизованных аудио- и видео-кодеков.

По количеству участников выделяют: *настольные (индивидуальные), групповые и студийные*видеоконференции*.*

*Настольные видеоконференции (НВ)* характеризуются следующими параметрами:

* + доступная аудитория и вариант общения– обычно диалог двух лиц;
  + качественная характеристика связи– нет необходимости в большой производительности (*ширине полосы связи*);
  + стиль общения– неформальный, спонтанный;
  + необходимые затраты– только программное и аппаратное обеспечение, используемое на рабочем месте;
  + необходимое оборудование– компьютер с установленной поддержкой аудио и видео, микрофон, динамики или наушники, видеокамера, ***LAN***, ***ISDN*** соединение.

В настоящее время большинство наиболее популярных *НВ* систем использует ***whiteboard***, или доску объявлений. С ее помощью отдельная экранная область зарезервирована для просмотра и совместного использования документов в дополнение к окну конференцсвязи, на котором отображаются участники *НВ*. Обычно под доской объявлений

нужно понимать программное обеспечение, дающее возможность совместного создания и редактирования документа всеми участниками конференции. Причем сам документ может состоять не только из текстовой информации, но и включать и графику, и различные элементы оформления, такие, как,например, выделение участков текста маркером. Преимуществом доски объявлений над другими средствами групповой обработки информации, имеющимися в *НВ*, является относительно высокое быстродействие ее по сравнению с разделяемыми приложениями.

*Групповые видеоконференции (ГВ)* характеризуются следующими параметрами:

* + доступнаяаудитория и вариант общения– группа с группой;
  + качественная характеристика связи– необходима большая производительности (ширина полосы связи);
  + стиль общения– практически формальный, ориентирующийся на регламент;
  + необходимые затраты– программное и аппаратное обеспечение, а также затраты на специализированные средства и помещения;
  + необходимое оборудование– обязательны дисплей (29 или 37 дюймов) с возможностью масштабирования изображения, ***switched56, ISDN*** соединение, специализированное оборудование.

*ГВ* подходят для организации эффективного взаимодействия больших и средних групп пользователей. Причем благодаря значительно более высокому качеству видеоизображения сегодня возможны обмен и просмотр документов, демонстрация которых в *НВ* исключается. Кроме того, *ГВ* идеально подходят для проведения дискуссий и выступлений там, где личное присутствие невозможно.

*Студийные видеоконференции (СВ)* характеризуются следующими параметрами:

* + доступная аудитория и вариант общения– обычно один говорящий с аудиторией;
  + качественная характеристика связи– необходима максимальная производительность (ширина полосы связи);
  + стиль общения– формальный, жестко регламентированный, устанавливаемый ведущим;
  + необходимые затраты– на оборудование студии, на специализированное оборудование;
  + необходимое оборудование– студийная камера(ы),

соответствующее звуковое оборудование, контрольное оборудование и мониторы, доступ к спутниковой связи или оптоволоконной линии связи.

Реализовать видеоконференцию можно разными путями, из них два наиболее реальны:

1. Использование оборудования, каналов и программного обеспечения ***ISDN***. Полоса и качество здесь гарантируются, но стоимость весьма высока.
2. Применение каналов Интернет, соответствующего (обычно общедоступного) программного обеспечения и оборудования общего применения. Вариант относительно дешев, но качество здесь пока не гарантируется, ведь информационный поток при проведении сеанса конкурирует с потоками от других процессов в Интернет.

В основе любой современной системы проведения видеоконференций лежит устройство, называемое *кодер-декодером (кодеком)*. Кодек ответствен за кодирование, декодирование, сжатие и декомпрессию звуковых и видеосигналов. При всех прочих равных условиях (например, при одинаковом качестве камер) чем лучше реализован кодек, тем лучше звуковой и видеосигнал.

Базовым протоколом для работы в ЛВС, где не гарантируется нужный уровень качества обслуживания***QоS* (*Q****uality* ***o****f* ***S****ervice*) являетсястандарт ***H.323***. Он обеспечивает видеоконференции для соединений точка-точка и для многоточечных топологий в рамках стека протоколов ***TCP/IP*** и регламентирует и принципы сжатия видео и аудио информации.

Привлекательность стандарта заключается в том, что он применим к уже существующей инфраструктуре телекоммуникаций с широкими вариациями задержек отклика. Способствует этому возрастающая пропускная способность локальных **(*fast ethernet и gigabit ethernet***) и региональных сетей (***SDH, ATM, FDDI, Fibre Channel*** и т.д.), а также новейшие протоколы из семейства ***IP (RTP***и***RSVP)*** и поддержкастандарта

***H.323*** компаниями ***Intel, Microsoft*, *Cisco и IBM.*** Стандарт ***H.323*** не привязан ни к одной операционной системе и не предполагает использования какого-либо специализированного оборудования.

Персональные системы обычно выполняются как приложения для

***Windows***, с видеоизображением в маленьком окне на рабочем столе. Они

также используют одиночную ***ISDN*** линию (один или два 64-Kбит/с b- канала). Кроме традиционной двухсторонней звуковой и видеосвязи, эти системы, как правило, предоставляют возможности, которые облегчают совместное использование данных, разделяемых приложений, что позволяет обеим сторонам редактировать документ или электронную таблицу. Термин «говорящие головы» иногда характеризует звуковое и видеокачество этих систем. Быстрые движения приводят к значительному искажению изображений, именуемому обычно *эффектом тени*. Такое качество – результат ограничений ширины полосы частот, компромиссов в реализации кодека, дешевой камеры и звуковых компонентов. Поэтому в данных системах, хотя и декларируется совместимость со стандартами ***Н. 320***и ***G.261***, в большинстве случаев частота кадров не превышает 10, а разрешение ***CIF*** вообще недоступно.

Еще одна серьезная проблема – проведение конференций с числом участников более 20 и совместное использование не совсем совместимых систем. Для решения этих проблем используются технологии многоточечной ВКС, которая может быть реализована на видеосервере ***MCU***(***M****ultipoint* ***C****onference* ***U****nit*) или программно на некоторых терминалах ВКС. В число основных функций видеосервера **MCU** входит кодирование, декодирование, микширование аудио- и видеосигнала, а также управление, контроль за проведением видеоконференции.

Однако сейчас название ***MCU*** ошибочно дается тем бриджам, которые поддерживают многосторонние конференции с использованием только данных или данных и аудио и несовместимы со стандартом***Н.320****.* На самом деле эти устройства называются **MCS (*Multimedia Conferencing Server*)**.

Типичным источником видео реального времени являются небольшие камеры с зарядовой связью (***C****harged* ***C****oupled* ***D****evice***–*CCD***). В зависимости от мощности настольного ПК эти камеры (обычно размещаемые над монитором) осуществляют съемку с частотой от 5 до 30 кадров в секунду, причем последняя величина соответствует нормальному качеству вещания. Разрешение видео реального времени может меняться в значительных пределах от крупных изображений, требующих большей пропускной способности, но более подходящих для нормального общения, до небольших «почтовых марок», вмещающих только говорящую голову.

### Выполнение работы

#### Задание 1. Подключите оборудование, необходимое для организации настольной видеоконференции:

* 1. Подключите Web-камеру и выполните ее настройку:
     + вставьте установочный диск в ***CD-ROM*** и запустите программу установки (***setup.exe***);
     + выберите установку драйвера (кнопка ***Driver***) и следуйте указаниям мастера по установке;
     + завершите работу установочной программы (***Exit***).
     + подключите Web-камеру к соответствующему разъему ПК;
     + выполните диагностику работы устройства:

##### откройте окно Свойства (Контекстное меню значка Web- камеры/Свойства в окне Пуск/Панель управления/Сканеры и камеры);

* + - * на вкладке ***Общие*** щелкните кнопку ***Проверка камеры***, ознакомьтесь с результатами диагностики и закройте диалоговое окно;
    - получите при помощи Web-камеры пробные снимки:

##### запустите Мастер работы со сканером или цифровой камерой (Контекстное меню значка Web-камеры /Получить снимки в окне Пуск/Панель управления/Сканеры и камеры); Далее

* + - * сделайте изображение максимально статичным (по возможности) и зафиксируйте его, нажав на кнопку ***Снять***;

*Полученное изображение автоматически размещается в правой панели.*

* + - * сделайте еще несколько снимков;
      * оставьте выделенными только те, которые Вы считаете самыми удачными, и перейдите к следующему шагу (***Далее***);
      * введите шаблон для наименований созданных изображений и укажите папку, где они будут сохранены (***Далее***);
      * при выборе дальнейших действий установите радиокнопку

***Ничего***. Работа с этими изображениями закончена (***Далее***);

* + - * закончите работу ***Мастера* (*Готово*)**.
  1. Подключите гарнитуру и выполните ее настройку:

##### откройте окно Свойства: Звуки и аудиоустройства (двойной щелчок по значку Звуки и аудиоустройства в папке Пуск/Панель управления);

* + - выполните настройку динамиков и микрофона на вкладке **Аудио**:
      * откройте окно ***Дополнительные свойства звука*** *(*кнопка ***Настройка…*** в группе ***Воспроизведение звука***) и в списке ***Расположение динамиков*** выберите *Стереонаушники* (***ОК***);
      * откройте окно ***Record Control*** (кнопка ***Громкость…*** в группе ***Запись звука***) и установите необходимый *уровень громкости* на линейке ***Microphone***;
      * убедитесь, что установлен флажок ***Выбрать***, и закройте все окна (кнопка ***Закрыть*** или ***ОК***).
  1. Выполните аналогичную настройку на втором компьютере.

#### Задание 2. Настройте программное обеспечение, необходимое для организации настольной видеоконференции:

* 1. Запустите программу ***Windows Messenger* (*Пуск/Все программы/Сеть*)**.
  2. Создайте новую учетную запись для работы в этой программе:
     + щелкните ссылку ***Щелкните здесь***в Главном окне программы, чтобы выполнить вход;
     + в открывшемся окне выберите ссылку ***Получение .NET-паспорта***;
     + ознакомьтесь с предлагаемой информацией и перейдите к следующему шагу (***Далее***);
     + выберите вариант ***Да, использовать существующий адрес электронной почты*** (***Далее***);
     + подтвердите свое желание зарегистрироваться радиокнопкой ***Нет, зарегистрироваться*** (***Далее***);
     + запустите браузер для заполнения регистрационной формы, нажав кнопку ***Далее***;
     + заполните поля регистрационной формы и нажмите кнопку

##### Продолжить;

* + - ознакомьтесь с предлагаемыми соглашениями, введите в поле адрес вашей электронной почты и нажмите кнопку ***Я принимаю***;
    - перейдите в указанный почтовый ящик, чтобы подтвердить создание учетной записи;
    - закройте окно браузера;
    - продолжите работу Мастера, вернувшись на предыдущий шаг (***Назад***), и выберите радиокнопку ***Да, войти при помощи идентификатораWindows Live ID*** (***Далее***);
    - введите адрес электронной почты и пароль, снимите флажок об идентификации (***Далее***);
    - закончите работу Мастера (***Готово***).
  1. Выполните пункты 1 и 2 на втором компьютере, создав другую учетную запись.
  2. Добавьте в список контактов (на первом ПК) учетную запись, созданную в пункте 3:
     + выберите ***Добавить контакт*** в нижней панели действий;
     + укажите вариант ***с использованием адреса электронной почты***(***Далее***);
     + введите в поле электронный адрес пользователя, который необходимо добавить (***Далее***);
     + закончите добавление контакта (***Готово***).
  3. Аналогично добавьте в список контактов (на втором ПК) учетную запись, созданную в пункте 2.

#### Задание 3. Организуйте настольную видеоконференцию:

* 1. На первом ПК откройте окно ***Начать видеобеседу*** (кнопка ***Начать видеобеседу***на нижней панели действий).
  2. На вкладке ***Контакты*** выделите приглашаемого участника и нажмите (***ОК***).
  3. На втором ПК примите приглашение начать видеоконференцию: в пришедшем сообщение выберите ссылку ***Принять (ALT+T)***.
  4. В правой панели окна сообщений (на обоих компьютерах) отобразится картинка, передаваемая с Web-камеры, в режиме

«картинка в картинке».

* 1. Используя подключенную гарнитуру, кроме видео, выполните передачу голосового сообщения с одного компьютера на другой.
  2. Создайте снимок экрана с работающим окном сообщений, в котором отображается передаваемая видеоинформация с Web-камеры, и сохраните его в личной папке.
  3. Выйдите из приложения ***Windows Messenger***: в контекстном меню значка программы на панели индикации выберите пункт ***Выход***.

#### Задание 4. Самостоятельно создайте видеозвонок с одного компьютера на другой при помощи программы *Mail.Ru Агент,* создав при необходимости учетную запись и добавив нужный контакт.

**Задание 5. Самостоятельно удалите установленные на компьютеры Web-камеры, предварительно отключив их (Пуск/Панель управления/Установка и удаление программ)**

## Примерные тестовые задания к модулю 5

* + 1. Мультисервисные сети (ММС) – это…
       - *множество сетей, объединенных по выбранному признаку;*
       - *универсальная многоцелевая среда, предназначенная для передачи речи, изображения и данных с использованием технологии коммутации пакетов;*
       - *несколько сетей, каждая из которых направлена на реализацию определенного сервиса – передача голосовых данных, видео-изображения и т.д.*
    2. Основными элементами мультисервисной сети являются:
       - *кластеры, транспортная сеть, телепорт;*
       - *передачи информации, магистраль, сервера данных;*
       - *цифровая АТС, передающая и принимающие спутниковые антенны, устройства для видеонаблюдения.*
    3. Выберите услуги МСС, выделяемые в группу по типу передаваемой информации:

*услуга предоставления сети беспроводного доступа;*

*услуга предоставления доступа к ресурсам своей сети;*

*широковещательные услуги;*

*услуги, оказываемые корпоративным клиентам;*

*технологии ADSL;*

*услуги телефонии.*

* + 1. Способ передачи данных малыми порциями (пакетами) называется…
       - *пакетным*
       - *импортируемым*
       - *потоковым*

## Контрольные вопросы к модулю 5

1.Мультисервисная сеть (МСС):основная задача и возможности. 2.Архитектура МСС.

3.Элементы сети: телепорт, транспортная сеть, кластеры. 4.Основные услуги МСС.

1. Спутниковые технологии сети SPIN.
2. Потоковая передача данных: достоинства и недостатки. 7.Способы воспроизведения удаленных медиа-файлов.

8.IP-телефония: преимущества и недостатки. 9.Классификация сетей IP-телефонии.

1. Способы организации (сценарии) передачи телефонных переговоров по сети Интернет.
2. Видеоконференция, видеоконференцсвязь. 12.Виды видеоконференций.

# БАЗА ТЕСТОВЫХ ЗАДАНИЙ

## Модуль 1.

**Проектирование и администрирование компьютерных сетей**

1. Расположите сети в порядке увеличения стоимости: *сеть на основе оптоволокна; беспроводная сеть;*

|  |
| --- |
|  |
|  |
|  |

*сеть на основе витой пары.*

1. Вершина дерева, представляющая не именованный уровень:
   * *корень доменов;* *домен второго уровня;*
   * *домен верхнего уровня;* *поддомен.*
2. В записи ***host-a.mspu.edu.ru***узлом в поддомена ***mspu*** является …
3. Обратное пространство имен формируется в домене
   * *in-addr.arpa;* *addr-in.arpa;*
   * *arpa-in.addr;*  *in-arpa.addr.*
4. Установите соответствие элементов DNS-адреса ***host-b.mspu.edu.ru*** их обозначению в терминологии DNS:

*host-b Поддомен*

*mspu Домен второго уровня*

*edu Домен верхнего уровня*

*ru Имя узла*

1. Один из этапов проектирования сети, связанный с прокладкой линий связи, установкой и настройкой оборудования, это…
   * *развертывание;* *внедрение.*
   * *анализ;* *проектирование;*
2. Действия, выполняемые на этапе непосредственного проектирования сети:

*определение целей использования сети;*

*выбор способа сегментирования;*

*разработка схемы сети;*

*выбор программного обеспечения.*

1. Назначение серверной операционной системы:
   * *управление приложениями;*
   * *обслуживание всех пользователей сети;*
   * *все выше перечисленное.*
2. При выборе варианта лицензирования сервера «На сервер» указывается:
   * *количество одновременных подключений;*
   * *количество пользователей;*
   * *количество компьютеров в домене.*
3. Аббревиатура облегченного протокола доступа к каталогам …**.**
4. Этап проектирования, на котором создается детальный проект физической организации сети, это
   * *анализ;* *проектирование физической структуры;*
   * *развертывание;* *проектирование инфраструктуры.*
5. Установите порядок этапов проектирования сети:

|  |
| --- |
|  |
|  |
|  |
|  |

*анализ;*

*проектирование инфраструктуры; проектирование физической структуры; развертывание.*

1. Этап проектирования сети, на котором определяется логическая организация сети:
   * *анализ;* *проектирование физической структуры;*
   * *развертывание;* *проектирование инфраструктуры;*
2. Этап проектирования сети, на котором определяется логическая организация сети – проектирование ….
3. Этап проектирования, связанный с прокладкой линий связи, установкой и настройкой оборудования:
   * *анализ;* *проектирование физической структуры;*
   * *развертывание;* *проектирование инфраструктуры;*
4. Этап проектирования, связанный с прокладкой линий связи, установкой и настройкой оборудования –….
5. Установите порядок подключения компьютера под управлением Windows XP к домену:

|  |
| --- |
|  |
|  |
|  |
|  |

*открыть диалоговое окно Изменение имени компьютера; ввести имя домена;*

*выбрать принадлежность к домену;*

*ввести имя и пароль администратора домена.*

1. Ответ, полученный от сервера, имеющего прямые полномочия для запрашиваемого имени с установленным битом полномочий в сообщении DNS – … ответ.
2. Объект пользователя (*user object*) состоит из атрибутов:

*имя;*

*пароль;*

*сведения о членстве в группах.*

1. Структура, определяющая то, как организована и хранится реальная информация (атрибуты объекта) в каталоге Active Directory:
   * *схема (schema);*
   * *объект пользователя (user object);*
   * *объект домена (domain object).*

#### Модуль2.

**Настройка домена и его безопасность**

1. Комплекс мероприятий, направленных на обеспечение информационной безопасности:
   * *защита информации;* *информационная защита;*
   * *безопасность информации;* *информационная безопасность.*
2. Преимущества использования стандартных правил, регламентирующих работу пользователей, это

*рутинные задачи всегда выполняются одинаково;*

*уменьшение вероятности появления ошибок;*

*работа по инструкциям выполняется гораздо быстрее;*

*все выше перечисленное.*

1. Совокупность всех объектов, атрибутов объектов и правил (синтаксиса атрибутов) в Active Directory –….
2. Политика безопасности сети на основе Windows храниться в следующих типах объектов:

*локальный объект групповой политики;*

*глобальный объект групповой политики;*

*объект групповой политики домена.*

1. Параметры узла Конфигурация компьютера в редакторе объектов групповой политики определяют работу:
   * *пользователя;* *компьютера;*
   * *операционной системы;* *все выше перечисленное.*
2. Компонент групповой политики, определяющий параметры реестра, задающий внешний вид рабочего стола и компоненты операционной системы:
   * *административные шаблоны;* *сценарии.*
   * *параметры безопасности;* *установка программ;*
3. Программный компонент вычислительной системы, выполняющий сервисные функции по запросу клиента:
   * *сервер;* *клиент;*
   * *компьютер;* *пользователь.*
4. Сервер, в основную задачу которого входит предоставление доступа к файлам на диске:
   * *файл-сервер;**контроллер домена;* *терминальный сервер.*
5. Операции, выполняемые посредством оснастки Пользователи и компьютеры:
   * *создание пользователей;* *создание групп;*
   * *создание контейнеров;**все выше перечисленное.*
6. Основной компонент IIS:
   * *веб-сервер;* *ftp-сервер;* *почтовый сервер.*
7. Разделы в структуре объекта групповой политики:

*узел конфигурации компьютера;* *узел конфигурации системы;*

*узел конфигурации пользователя;* *все выше перечисленное.*

1. Порядок применения групповых политик в сети на базе ОС Windows:

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

*групповые политики ОП; локальные групповые политики; групповые политики сайта; групповые политики домена;*

*политики Windows NT 4.0 (NTConfig.pol);*

*групповые политики дочернего ОП.*

1. Порядок наследования политик:

|  |
| --- |
|  |
|  |
|  |

*сайт; домен;*

*подразделение.*

1. Домен напрямую наследует политику ….
2. База данных Active Directory:
   * *место, где хранится вся информация, относящаяся к Каталогу (включая объекты и атрибуты домена), схема, конфигурация и информация Глобального Каталога;*
   * *инструмент, который используется для установки (или удаления) Active Directory на сервер;*
   * *логическая группа пользователей и компьютеров (объектов), которые связаны как единица для администрирования и репликации;*
   * *контейнеры внутри AD, которые создаются для объединения объектов в целях делегирования административных прав и применения групповых политик в домене.*
3. Пользователь, имеющий права запуска процесса установки Active Directory:
   * *обычный пользователь с минимальными правами;*
   * *пользователь, входящий в группу "Опытные пользователи";*
   * *пользователь, входящий в группу "Администраторы".*
4. Цель создания организационных единиц (OU) внутри Active Directory:

*для объединения объектов в целях делегирования административных прав;*

*для применения групповых политик в домене;*

*для объединения объектов в целях осуществления репликации между поддоменами одного дерева.*

1. Доменв Active Directory, это…
   * *логическая группа пользователей и компьютеров (объектов), которые связаны как единица для администрирования и репликации;*
   * *контейнеры внутри AD, которые создаются для объединения объектов в целях делегирования административных прав и применения групповых политик в домене;*
   * *термин, применяемый для описания совокупности AD деревьев.*
2. Код ошибки «Файл не найден», возвращаемый web-сервером:
   * *401;*
   * *402;*
   * *403;*
   * *404.*
3. Код ошибки «Файл не найден», возвращаемый web-сервером ….

#### Модуль3.

**Обеспечение информационной безопасности в компьютерных сетях**

1. Потенциальные угрозы, определяющие задачи защиты информации в компьютерных сетях:

*прослушивание каналов;*

*умышленное уничтожение или искажение информации;*

*выход из строя операционной системы;*

*внедрение сетевых вирусов.*

1. … каналов – это запись и последующий анализ всего проходящего потока сообщений.
2. К сервисам безопасности относят:
   * *идентификация/аутентификация;* *аудит;*
   * *протоколирование/аудит;* *шифрование.*
3. …– это предотвращение пассивных атак для передаваемых или хранимых данных.
4. …– подтверждение подлинности взаимодействующих объектов.
5. Контроль …–это защита от несанкционированного использования ресурсов.
6. Соответствие между понятиями и их определениями:

*Конфиденциальность предотвращение пассивных атак для*

*передаваемых или хранимых данных Аутентификация защита от несанкционированного использования*

*ресурсов*

*Контроль доступа подтверждение подлинности*

*взаимодействующих объектов*

1. Конфиденциальность – это
   * *предотвращение пассивных атак для передаваемых или хранимых данных;*
   * *защита от возможных отказов от фактов отправки, приема или содержания; отправленных или принятых данных;*
   * *подтверждении подлинности взаимодействующих объектов;*
   * *защита от несанкционированного использования ресурсов сети.*
2. К механизмам безопасности относят:
   * *хэш-функции;* *целостность сообщения;*
   * *алгоритмы симметричного шифрования;*
   * *невозможность отказа от полученного сообщения.*
3. Активные угрозы становятся видимыми на уровне (модели OSI):
   * *физическом;* *канальном;*
   * *сетевом;* *транспортном.*
4. Алгоритм, использующий для шифровки два разных ключа (открытый и закрытый), это
   * *алгоритм симметричного шифрования;*
   * *алгоритм асимметричного шифрования;*
   * *алгоритм использования контрольных сумм;*
   * *алгоритм проверки подлинности.*
5. Алгоритм … шифрования – алгоритм шифрования, в котором для шифрования и дешифрования используется один и тот же ключ.
6. Алгоритм … шифрования – алгоритм шифрования, в котором используются два различных ключа, называемые открытым и закрытым ключами.
7. …–функция – это функция, входным значением для которой является сообщение произвольной длины, а выходным значением – сообщение фиксированной длины, которое может быть использовано для аутентификации исходных данных.
8. Двоичные программы, внедряемые в web-страницу:

*JavaScript;* *Java-апплеты;*

*аctiveX;* *VBScript.*

1. Цифровая подпись – это:
   * *способ введения электронной метки для файла данных;*
   * *файл, подтверждающий ваши права;*
   * *сведения о пользователе помещаемые в файл;*
   * *идентификатор документа.*
2. …– цифровой документ, используемый для проверки подлинности и безопасности обмена данными в открытых сетях.
3. Обозначение, семейства протоколов охватывающих проблемы безопасности на IP-уровне:
   * *FTP;* *UDP;* *TCP/IP;* *Ipsec.*
4. …– это средство, располагаемое между защищаемым внутренним сегментом сети и внешней сетью и контролирующее все информационные потоки во внутренний сегмент.
5. Средство, располагающееся между внутренним сегментом сети и внешней сетью и контролирующее все информационные потоки во внутренний сегмент и из него, называется:
   * *брандмауэр;*
   * *концентратор;*
   * *коммутатор;*
   * *шлюз.*

#### Модуль4.

**Защита информации в компьютере**

1. К сервисам безопасности относят:

*идентификация/аутентификация;* *аудит;*

*протоколирование/аудит;* *шифрование.*

1. Потенциальные угрозы, определяющие задачи защиты информации в компьютерных сетях:

*прослушивание каналов;*

*уничтожение или искажение информации;*

*выход из строя операционной системы;*

*внедрение сетевых вирусов.*

1. Конфиденциальность – это:
   * *предотвращение пассивных атак для передаваемых или хранимых данных;*
   * *защита от возможных отказов от фактов отправки, приема или содержания отправленных или принятых данных;*
   * *подтверждение подлинности взаимодействующих объектов;*
   * *защита от несанкционированного использования ресурсов сети.*
2. К механизмам безопасности относят:

*хэш-функции;* *целостность сообщения;*

*алгоритмы симметричного шифрования;*

*невозможность отказа от полученного сообщения.*

1. Активные угрозы становятся видимыми на уровне (модели OSI):
   * *физическом;* *канальном;* *сетевом;* *транспортном.*
2. Алгоритм, использующий для шифровки два разных ключа (открытый и закрытый):
   * *алгоритм симметричного шифрования;*
   * *алгоритм асимметричного шифрования;*
   * *алгоритм использования контрольных сумм;*
   * *алгоритм проверки подлинности.*
3. Двоичные программы, внедряемые в web-страницу:

*JavaScript;* *Java-апплеты;*

*аctiveX;* *VBScript.*

1. Цифровая подпись – это
   * *способ введения электронной метки для файла данных;*
   * *файл, подтверждающий ваши права;*
   * *сведения о пользователе помещаемые в файл;*
   * *идентификатор документа.*
2. Обозначение, семейства протоколов охватывающих проблемы безопасности на IP-уровне:
   * *FTP;**UDP;* *TCP/IP;* *Ipsec.*
3. Основные протоколы транспортного уровня, применяемые в Интернете:

*FTP;* *STP;* *TCP;* *UDP.*

#### Модуль5.

**Возможности мультисервисных сетей**

1. Мультисервисные сети (ММС) – это…
   * *множество сетей, объединенных по выбранному признаку;*
   * *универсальная многоцелевая среда, предназначенная для передачи речи, изображения и данных с использованием технологии коммутации пакетов;*
   * *несколько сетей, каждая из которых направлена на реализацию определенного сервиса – передача голосовых данных, видео- изображения и т.д.*
2. Основными элементами мультисервисной сети являются:
   * *кластеры, транспортная сеть, телепорт;*
   * *устройства передачи информации, магистраль, сервера данных;*
   * *цифровая АТС, передающая и принимающие спутниковые антенны, устройства для видеонаблюдения.*
3. Выберите услуги МСС, выделяемые в группу по типу передаваемой информации:

*услуга предоставления сети беспроводного доступа;*

*услуга предоставления доступа к ресурсам своей сети;*

*широковещательные услуги;*

*услуги, оказываемые корпоративным клиентам;*

*технологии ADSL;*

*услуги телефонии.*

1. Выберите услуги МСС, выделяемые в группу услуг по способу доступа к клиенту:

*услуга предоставления сети беспроводного доступа;*

*услуга предоставления доступа к ресурсам своей сети;*

*широковещательные услуги;*

*услуги, оказываемые корпоративным клиентам;*

*технологии ADSL;*

*услуги телефонии.*

1. Способ передачи данных малыми порциями (пакетами) называется
   * *пакетным;* *импортируемым;* *потоковым.*
2. Способ передачи данных малыми порциями (пакетами) –…
3. По способу связи устройств между собой сети IP-телефонии бывают:

*выделенные;* с*мешанные;* *национальные;*

*международные;* *интегрированные;* *местные.*

1. По масштабу охватываемой территории сети IP-телефонии бывают:

*выделенные;* с*мешанные;* *национальные;*

*международные;* *интегрированные;* *местные.*

1. Программное и аппаратное обеспечение, используемое на рабочем месте, характеризует видеоконференцию
   * *групповую;* *настольную;* *студийную.*
2. Максимальная производительность связи необходима при проведении
   * *настольной видеоконференции;*
   * *групповой видеоконференции;*
   * *студийной видеоконференции.*
3. Базовый протокол для работы в локальной сети, где не гарантируется нужный уровень качества обслуживания

 *TCP/IP;* *Н.320;* *H.323;* *G.261.*

1. Базовый протокол для работы в локальной сети, где не гарантируется нужный уровень качества обслуживания, называют …
2. … представляют собой группы от 500 до 2 тыс. абонентов, территориально расположенных в непосредственной близости друг от друга, и охватываются интерактивной распределительной сетью.
3. Установите соответствие понятий используемых в ММС их значениям:

*Телепорт двунаправленная широкополосная магистральная кабельная сеть, построенная по волоконно-оптической технологии со структурой «кольцо» или «звезда»;*

*Транспортная сеть*

*единый центр управления, получения, обработки, создания и передачи информации;*

*Кластеры группы от 500 до 2 тыс. абонентов, территориально расположенных в непосредственной близости друг от друга, и охватывающиеся интерактивной распределительной сетью.*

1. Группы от 500 до 2 тыс. абонентов, территориально расположенных в

непосредственной близости друг от друга, и охватывающиеся интерактивной распределительной сетью, это

* + *телепорт;* *транспортная сеть;* *кластер.*

1. Технология позволяющая передавать мультимедийную информацию и одновременно обеспечивает её прием группой абонентов, территориально удалённых друг от друга, называют … вещанием.
2. … Windows Media – набор веб-страниц, который функционирует в окне браузера Microsoft Internet Explorer версии 5.0 и управляет службами- компонентами Windows Media.
3. Этап процесса передачи голоса по IP-сети, на котором осуществляется оцифровка голоса, называют….
4. Этап процесса передачи голоса по IP-сети, на котором полученная последовательность данных разбивается на пакеты и к ней добавляется протокольная информация, называют….
5. Основные области применения систем видеоконференцсвязи это:

*поддержка принятия оперативных решений;*

*сопровождение проектов на удаленных объектах;*

*пресс-конференции;*

*повышение квалификации специалистов;*

*дистанционное обучение.*

**ПРИЛОЖЕНИЕ 1**

## План-проект учебной компьютерной сети школы

#### Описание задания

Необходимо спроектировать сегмент учебной компьютерной сети для школы. В школе уже существует две сети:

* административная сеть, объединяющая компьютеры директора, секретаря и бухгалтерии;
* компьютеры кабинетов информатики, имеющих выделенный сервер (обычный компьютер под управлением Windows XP).

Кроме этого еще в 3-ти кабинетах имеются демонстрационные компьютеры с проекторами и 1 компьютер в учительской.

Планируется одновременная трансляция видео и передача голосовых данных

#### Исходные данные

##### Цели использования сети:

* Обучение школьников различным дисциплинам с использованием сетевых технологий.
* Доступ к информационным ресурсам (библиотека, Интернет).
* Демонстрация видео уроков.
* Голосовое общение по сети.

##### Требуемые характеристики сети:

* скорость передачи достаточная для поддержания видеовещания и голосового общения;
* выход в интернет.
* отделение учебной сети от имеющейся административной сети;
* ограничение доступа пользователей к ресурсам сети.
* масштабируемость.

##### Характеристики существующих компьютеров и других устройств:

В организации имеется уже существующая сеть с выделенным сервером, объединяющая компьютеры в кабинетах информатики. количество компьютеров – 26:

* кабинет информатики 1 (10 ученических ПК + 1 учительский ПК);
* кабинет информатики 2 (10 ученических ПК + 1 учительский ПК + 1 сервер);
* по одному компьютеру в трех кабинетах (история, география, биология);
* один компьютер в учительской.

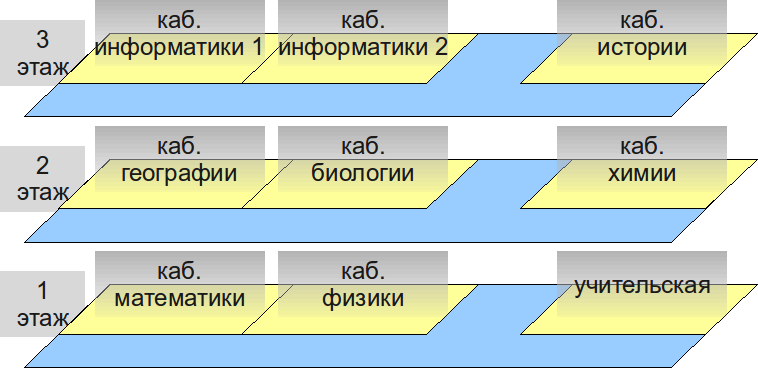
Все компьютеры типовые и имеют следующие характеристики:

* + Процессор – Athlon XP 1600+;
  + Оперативная память – 256 Мб;
  + Жесткий диск – 40 Гб;
  + Сетевой адаптер – встроенный (100 Мб, Ethernet).
  + количество принтеров – 2 (Samsung ML-1015).
  + модемы – аналоговый модем HSP56 MicroModem.

##### Характеристики используемого программного обеспечения:

1. Операционные системы: WindowsXP professional.

##### Примерная схема здания:



**Рисунок 7.Схема расположения кабинетов**

#### Проектирование сети

##### Способ сегментирования и объединения сегментов:

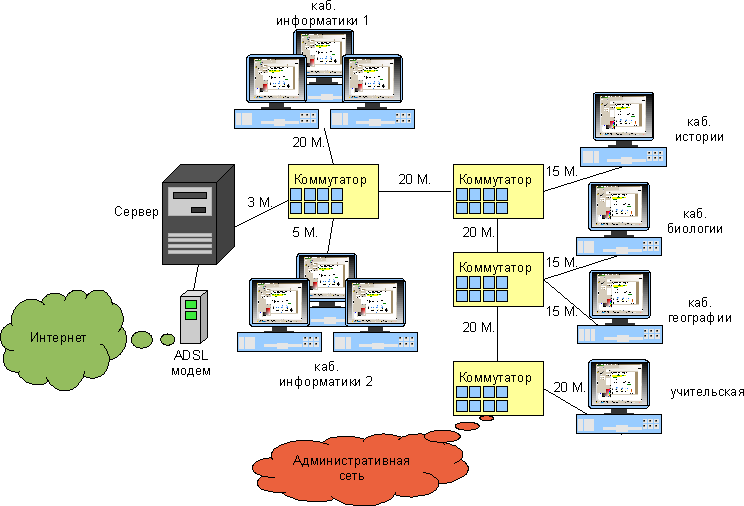
* целесообразно использовать концентраторы, т.к. планируется объединять в сеть не большое количество компьютеров (менее 30).
* целесообразно расположить на каждом этаже по концентратору, т.к. в будущем планируется покупка компьютеров для других кабинетов и подключение их к учебной компьютерной сети.

***Тип кабеля***– не экранированная витая пара 5-й категории. ***Активные устройства***– ADSL модем с встроенным брандмауэром. ***Программное обеспечение:***

* ОС для рабочих станций – Windows XP (уже имеется на ПК);
* ОС для сервера – Windows 2003 server (необходимо купить для установки на 1 компьютер);
* прокси-сервер – TrafficInspector (необходимо купить для установки на 1 компьютер);
* антивирусное программное обеспечение – Dr.Web (необходимо купить на каждый компьютер, используемый в сети)

#### Разработка схемы сети Определение стоимости

##### Анализ основных направлений затрат:



**Рисунок 8: Схема проектируемой сети**

* сетевое оборудование (концентраторы, не экранированная витая пара 5-й категории, ADSL модем, подключение по технологии ADSL, и т.д.);
* модернизация сервера (оперативная память, жесткий диск);
* монтажное оборудование и инструменты (клещи, короба и т.д.);
* программноеобеспечение (Windows 2003 server, TrafficInspector, Dr.Web).

##### Составление сметы примерных затрат

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование** | **Цена руб.** | **Кол-во** | **Всего** |
| Оперативная память 512 Мб | 777,00руб. | 1 шт. | 777,00руб. |
| Жесткий диск 160 Gb | 1 606,00руб. | 1 шт. | 1 606,00руб. |
| Витая пара | 8,00руб. | 200 М | 1 600,00руб. |
| Концентраторы | 440,00руб. | 3 шт. | 1 320,00руб. |
| ADSL модем | 932,00руб. | 1 шт. | 932,00руб. |
| Клещи | 1 530,00руб. | 1 шт. | 1 530,00руб. |
| Разъемы RJ-45 | 10,00руб. | 10 шт. | 100,00руб. |
| Короб | 33,00руб. | 7 шт. | 231,00руб. |
| Windows 2003  server | 82 706,00руб. | 1 шт. | 82 706,00руб. |
| TrafficInspector | 4 500,00руб. | 1 шт. | 4 500,00руб. |
| Dr.Web | 700,00руб. | 27 шт. | 18 900,00руб. |
| ADSL интернет | 1 500,00руб. | 1 шт. | 1 500,00руб. |
|  |  | **ИТОГО** | **115 702,00руб.** |

***Примерный план проведения работ***

|  |  |  |
| --- | --- | --- |
| **Наименование работ** | **Кол-во дней** | **Примечание** |
| Уточнение необходимой длины кабелей | 1 |  |
| Покупка материалов | 2 |  |
| Монтаж локальной сети | 5 |  |
| Установка программного обеспечения | 3 |  |
| **Всего** | **11** |  |

**ПРИЛОЖЕНИЕ 2**

## Пример соглашения для доступа к компьютерам факультета.

Я, нижеподписавшийся, настоящим объявляю, что буду придерживаться приведенных ниже правил:

Я буду использовать возможности компьютеров и сети факультета исключительно для учебных целей, относящихся к моему обучению.

Я знаю, что факультет предоставляет регистрационное имя исключительно для применения его получателем. Поэтому я не будут способствовать использованию моей учетной записи и файлов другими лицами и сообщать свой пароль другим лицам.

Я не буду осуществлять доступ или попытку доступа ни к одному компьютеру, регистрационной записи, сети или файлу без соответствующего и явного разрешения. Такой доступ является незаконным и противоречит университетским правилам. Если мне станет известно, что такой доступ имел место, я немедленно проинформирую об этом руководство факультета.

Я знаю, что некоторые программы и файлы, находящееся в файловой системе, могут быть защищены законом об авторских правах и другими законами или лицензионными либо другими соглашениями. Я не буду нарушать накладываемые ими ограничения.

Я не буду использовать университетские ресурсы для получения, разработки, запуска и распространения нелицензионного программного обеспечения.

Я обязуюсь сохранять конфиденциальность любых полученных мною от университета сведений о программном обеспечении (включая методы и принципы его использования), лицензированном для применения не компьютерах университета, и тем самым обезопасить университет от претензий любого рода, связанных с разглашением этой информации.

Я обязуюсь проявлять предельную честность и порядочность во всех вопросах, связанных с использованием компьютерных и сетевых возможностей факультета. Гарантирую что буду избегать любых действий, связанных с использованием компьютерных и сетевых возможностей университета, которые могут повредить репутации факультета или университета.

Я понимаю, что должен придерживаться Правил Университета, которые также определяют и регулируют порядок использования вычислительных средств университета.

Я понимаю, что действия, противоречащие изложенным выше принципам, повлекут за собой взыскания, включая отказ в изучении тему или предмета, временный запрет или лишение доступа к университетским вычислительным средствам, временное или полное исключение из университета.

« » г.

(ФИО) (подпись)

#### СЛОВАРЬ СПЕЦИАЛЬНЫХ ТЕРМИНОВ[1](#_bookmark38)

**Автоконтроль целостности** – использование в программе специальных алгоритмов, позволяющих после запуска программы определить, были ли внесены изменения в файл, из которого загружена программа или нет.

**Автоматический запрос на повторение** *(AutomaticRepetitionQuery, ARQ)*– способность автоматически запрашивать повторную передачу в случае обнаружения ошибки при передаче.

**Авторизация** *(authorization)* – полномочия, устанавливаемые администратором системы для конкретных лиц, позволяющие последним использовать транзакции, процедуры или всю систему в целом.

**Адрес** (*Address)*– закодированное обозначение пункта отправления либо назначения данных; идентификация объекта (например, объекта сети). Определяется числом, кодом или фразой.

**Алгоритм RSA**– алгоритм асимметричного шифрования, основанный на неразрешимости задачи факторизации. Может использоваться как для создания подписи, так и для шифрования.

**Анализ риска** *(riskanalysis)*– процесс изучения характеристик и слабых сторон системы, проводимый с использованием вероятностных расчетов, с целью определения ожидаемого ущерба в случае возникновения неблагоприятных событий. Задача анализа риска состоит в определении степени приемлемости того или иного риска в работе системы.

**Архитектура** (*architecture)*– концепция, определяющая модель, структуру, выполняемые функции и взаимосвязь компонентов сложного объекта. Архитектура сети определяет ее основные элементы, характер и топологию взаимодействия этих элементов. Архитектура информационной системы характеризует ее общую логическую организацию, программно-

1 Составлен на основе глоссариев из источников:

* Нехаев, С.А., Андреев И.Л., Кривошеин Н.В., Яскевич Я.С. Словарь прикладной ин- тернетики [Электронный ресурс] / С. А. Нехаев, И. Л. Андреев, Н. В Кривошеин, Я. С. Яскевич. Режим доступа:[http://www.webplan.ru/hold/r15-4.shtml,](http://www.webplan.ru/hold/r15-4.shtml) свободный.
* Партыка, Т.Л. Информационная безопасность :учебное пособие для студ сред .проф. образования [Текст] / Т. Л. Партыка, И. И. Попов– М.: ФОРУМ: ИНФРА-М, 2005. – 368 с.
* Столлингс, В. Современные компьютерные сети. / В. Столлингс; 2-е изд. – СПб.: Питер, 2003. – 783 с.
* AmericanNationalStandardDictionary of Information Technology, стандарт ANSI X3.172. – 1995(помеченызвездочкой).

аппаратное обеспечение, описывает методы кодирования и определяет интерфейс пользователя с системой.

**Архитектура информационного комплекса** *(architecture informationcomplexes)*–условно структурированная модель, определяющая выполняемые функции и взаимосвязь виртуальной (портал) и реальной (социально-экономическая система) частей комплекса. Имеет следующие блоки: сервер – портал (вкл. сервисы) – отрасль (вкл. производство, инфраструктуру, потребителей) – экономика и социум в целом.

**Архитектура протокола** *(protocolarchitecture)* – аппаратная и программная структура, реализующая функции обмена данными.

**Асинхронный режим передачи** *(AsynchronousTransferMode, ATM)*– стандартизованная союзом ITU технология коммутации пакетов фиксированной длины; является асинхронной в том смысле, что пакеты от отдельных пользователей передаются апериодически. ATM представляет собой интерфейс для широкополосной сети ISDN. В отличие от стандарта Х. 25, технология ATM не предоставляет механизмов контроля ошибок и управления потоком.

**Атака** *(attack)*– нарушение безопасности информационной системы, позволяющее захватчику управлять операционной средой; действие некоторого субъекта компьютерной системы (пользователя программы, процесса и т.п.) использующего уязвимость системы для достижения целей, выходящих за пределы авторизации данного субъекта в данной компьютерной системе.

**Аутентификация** (*authentication*) – процедура идентификации или проверки полномочности узлов, инициаторов или лиц для доступа к определенной категории информации.

**База данных** (*database)* – совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования, независимая от прикладных программ. Является информационной моделью предметной области. Обращение к базам данных осуществляется с помощью системы управления базами данных (СУБД).

**Базазнаний** (*knowledge base) –*семантическая модель, предназначенная для представления в компьютере знаний, накопленных человеком в определенной предметной области. Является основной составной частью интеллектуальных и экспертных систем.

**Байт** (*byte,octet)*– основная единица количества информации в

компьютерной технике, равная набору 8-ми разрядов двоичного кода (бита); группа из 8 бит, как правило, обрабатываемая как единое целое.

**Баннер**(*banner)*– изображение или текстовый блок рекламного характера, являющийся гиперссылкой на страницы с расширенным описанием продукта или услуги. Баннеры размещают на различных Интернет-ресурсах для привлечения посетителей, формирования имиджа или продвижения этого ресурса.

**Безопасность** *(security)*– состояние, в котором файлы данных и программы не могут быть использованы, просмотрены или модифицированы неавторизованными лицами, включая персонал системы, компьютерами или программами.

**Бит** (*bit)*– наименьшая единица представления информации в информационных системах. Термин является аббревиатурой выражения *"binary digit*" (двоичный разряд). Представляется сочетанием чисел – 0 и 1.

**Бит в секунду** (*bits per second, bps)*– единица измерения скорости передачи (компьютерной обработки) информации с учетом всех передаваемых битов данных, как полезной, так и служебной информации. Для измерения скорости передачи только полезной информации используется показатель “символы в секунду” *(characters per second, cps).*

**Бит четности** *(paritybit)\** –контрольный бит, добавляемый к массиву двоичных цифр таким образом, чтобы сумма всех разрядов массива, включая бит четности, была всегда четной (или нечетной).

**Брандмауэр**– программа, контролирующая и фильтрующая данные, передаваемые из одной сети в другую. Устанавливается с целью заблокировать несанкционированный доступ к компьютеру из Интернета.

**Браузер** (*browser)*– программа навигации и просмотра вэб-ресурсов. Обычно в комплекте с браузерами поставляются почтовые программы, средства работы с серверами новостей и средства общения в реальном времени.

**Брешь, дыра***(loophole, Fault, Flaw)*– программное или аппаратное упущение или недоработка, позволяющая обойти процессы управления доступа.

**Бутменеджер**– менеджер загрузки, позволяющий выбрать вариант загружаемой на компьютере операционной системы.

**Верификация** (*verification)* – использование теста или имитированной среды для выявления идентичности двух уровней спецификаций системы, например, политики безопасности в спецификации высшего уровня (исходном

коде) и объектном коде.

**Взаимодействие открытых систем** *(OpenSystemInterconnection, OSI)*– модель обмена данными между устройствами. Ей определяется семиуровневая архитектура функций обмена данными.

**Видеоконференция** (*video conferencing)*– методология проведения совещаний и дискуссий между группами удаленных пользователей с исполнением трансляции изображения в среде Интернет.

**Виртуальный канал** *(virtualcircuit)* –служба сети с коммутацией пакетов, в которой соединение (виртуальный канал) устанавливается между двумя станциями в начале передачи. Все пакеты следуют по одному и тому же маршруту, поэтому они не должны содержать полный адрес получателя. Кроме того, все пакеты, следующие по виртуальному каналу, прибывают к получателю в том же порядке, в котором они были отправлены.

**Виртуальная реальность** (*virtual reality)*– новая технология бесконтактного информационного взаимодействия, реализующая с помощью комплексных мультимедиа-операционных сред иллюзию непосредственного вхождения и присутствия в реальном времени в стереоскопически представленном “экранном мире”. Более абстрактно–это мнимый мир, создаваемый в воображении пользователя.

**Всемирная паутина** *(WorldWideWeb, WWW)* –сетевая ориентированная на использование графики гипермедийная система. Хранящаяся на серверах информация по сети передается клиентам, на которых отображается специальными прикладными программами, называемыми браузерами, в виде страниц, содержащих текст и изображения. Ведущее и наиболее популярное приложение в Интернете, позволяющее получать доступ к информации и найти сведения по заданной тематике независимо от места их расположения в сети. Удобство пользования Webобеспечивает гиперсреда, наглядность – интерактивные мультимедийные средства.

**Высокоуровневый протокол управления каналом** *(High- levelDataLinkControl, HDLC).* Распространенный бит-ориентированный протокол передачи данных (уровень 2 модели *OSI*), выпущенный Международной организацией по стандартизации (*ISO*);схож с протоколами *LAPB, LAPD* и *LLC*.

**Гиперсреда** (*hypermedia)*– технология представления любых видов информации в виде относительно небольших блоков, ассоциативно связанных друг с другом.

**Гиперссылка** (*hyperlink)***–**выделенный объект (текст или

изображение) вэб-страницы, устанавливающий связь с другим объектом**.** Позволяет переходить к другому объекту в среде [*WWW*.](http://WWW/)

**Гипертекст** (*hypertext)*– документ, содержащий ссылки на блоки текста внутри самого документа или на другие документы.

**Глобальная информационная инфраструктура –**качественно новое информационное образование, начатое формироваться в 1995 году группой развитых стран мирового сообщества. По замыслу создателей она должна представлять собой интегрированную общемировую информационную сеть массового обслуживания населения планеты на основе интеграции глобальных и региональных информационно- телекоммуникационных систем, а также систем цифрового телевидения и радиовещания, спутниковых систем и подвижной связи.

**Глобальные сети** (*wide area Network)****–***телекоммуникационные структуры, объединяющие локальные информационные сети, имеющие общий протокол связи, методы подключения и протоколы обмена данными. Каждая из глобальных сетей организовывалась для определенных целей, а в дальнейшем расширялась за счет подключения локальных сетей, использующих ее услуги и ресурсы.

**Групповой адрес** *(multicastaddress*) – адрес, идентифицирующий не одну, а группу сущностей в пределах домена (например, локальной или объединенной сети).

**Данные** (*Data)*– информация, представленная в формализованном виде, пригодном для автоматизированной обработки.

**Дейтаграмма** (*datagram*)\* – в сети с коммутацией пакетов пакет, независимый от других пакетов, в котором содержится информация, достаточная для выбора маршрута от терминального оборудования, генерирующего данные, до получающего терминального оборудования без необходимости установки соединения между DTE-устройствами и сетью.

**Дифференцированные службы** *(DifferentiatedServices, DS)* – архитектура, в которой трафик разбивается на несколько групп. Каждая группа помечается соответствующим образом и каждой группе сетевыми элементами предоставляется обслуживание, зависящее от членства в группе, так что пакеты, принадлежащие к разным группам, обрабатываются по- разному. Архитектура дифференцированных служб не пытается рассматривать весь совокупный трафик в каком-либо едином смысле, а также не пытается заранее резервировать сетевые ресурсы.

**Домен** (*domain)*– организационная единица в Интернете, служащая

для идентификации узла или группы родственных узлов. Крупные домены могут подразделяться на поддомены, отражающие различные области интересов или ответственности. Пример доменного имени***:*** [***www.internevod.com.***](http://www.internevod.com/)

**Доступ** *(access)* – 1) в обработке данных: взаимодействие между субъектом и объектом, обеспечивающее передачу информации между ними; 2) в физической безопасности: возможность входа на защищенную территорию.

**Заголовок** (*header*). Определяемая системой управляющая информация, предшествующая данным пользователя.

**Задержка распространения** *(propagationdelay)* – интервал времени между моментом поступления сигнала в канал и моментом его получения.

**Закрытый ключ**–один из ключей асимметричного шифрования, известный только владельцу. С помощью данного ключа осуществляется подписывание сообщения, если алгоритм асимметричного шифрования используется для создания подписи, либо осуществляется дешифрование, если алгоритм асимметричного шифрования используется для шифрования.

**Захватчики паролей**–программы, ворующие пароли путем обманных воздействий на операционную систему.

**Защита информации**– комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности (целостности, доступности, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных).

**Звезда** (*star*) – топология, в которой все станции соединены с центральным коммутатором. Обмен данными между двумя станциями осуществляется путем коммутации каналов.

**Идентификация** *(identification)*– процесс анализа персональных, технических или организационных характеристик или кодов для получения (предоставления) доступа к компьютерным ресурсам.

**Инкапсуляция** (*encapsulation*) –добавление к данным, получаемым от пользователя, протокола управляющей информации, выполняемое протокольной сущностью.

**Интегрированные службы** *(IntegratedServices, IS)* – архитектура интегрированных служб предоставляет интегрированные, или коллективные, услуги для удовлетворения набора требований трафика в данном домене (например, части Интернета, в которой реализован определенный элемент архитектуры интегрированных служб). Поставщик

интегрированных услуг рассматривает суммарные требования трафика и, во- первых, ограничивает удовлетворяемый трафик объемами, соответствующими текущим возможностям сети, во-вторых, резервирует ресурсы домена для предоставления обслуживания определенного уровня.

**Идентификация пользователя** (*user identification)–*опознавание пользователей (по фамилии и паролю) для определения его полномочий – права на доступ к данным и выбора режима их использования.

**Индексирование** (*indexing)* –процесс описания содержания документов и запросов в терминах информационно-поискового языка; назначение документу набора ключевых слов, отражающих его смысловое содержание.

**Интернет** (*Internet) –*открытая мировая коммуникационная инфраструктура, состоящая из взаимосвязанных компьютерных сетей, обеспечивающая доступ к удаленной информации и обмен информацией между компьютерами. Более формально это зафиксировано в определении Federal Networking Council USA от 24. 10. 1995: “Интернет*–* глобальная информационная система, части которой логически взаимосвязаны друг с другом посредством уникального адресного пространства, основанного на протоколе IP или его последующих расширениях, способная поддерживать связь с использованием комплекса протоколов TCP/IP, их последующих расширений или других IP-совместимых протоколов, и которая обеспечивает, использует или делает доступным, публично или частным образом, коммуникационный сервис высокого уровня”. При написании со строчной буквы (*internet*) означает объединенную сеть (см. *объединенная сеть).*

**Интернет-2***(Internet-2 ("Abilene"))*– проект создания инфраструктуры нового Интернета. Основан на новом протоколе IPv6 и объединяет уже свыше 150 университетов. Обладает повышенной производительностью, надежностью, скоростью передачи данных (2,4 Гигабит в сек.). Гарантирует передачу изображений и звука без задержки, устойчивую ширину каналов передачи. С его помощью решается проблема сетевой перегрузки, появляется возможность ранжирования трафика и его практически мгновенная передача. В перспективе открывается путь к созданию сетевого телевидения, передачи голографического и осязаемого изображения.

**Интернет-провайдер** (*Internet service provider, ISP)* **–**компания, предоставляющая пользователям доступ к Интернет.

**Интернет-протокол** *(InternetProtocol, IP).* Межсетевой протокол, поддерживающий не требующую соединений службу между несколькими соединенными сетями с коммутацией пакетов.

**Интранет** (*intranet*) – корпоративная объединенная сеть, обеспечивающая работу ключевых Интернет-приложений, в частности Всемирной паутины. Интранет функционирует в пределах организации для внутренних целей и может существовать как изолированная самостоятельная объединенная сеть или соединяться с Интернетом.

**Интерфейс** (*interface)*– определенная стандартами граница между взаимодействующими в информационном пространстве объектами.

**Интерфейспользователя** (*user interface)*– интерфейс, определяющий процессы взаимодействия пользователя с информационным ресурсом в Интернет.

**Информатизация** (*informatization) –* организационный социально- экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов.

**Информатика** (*informatics)*– комплексное научное междисциплинарное направление, изучающее модели, методы и средства сбора, хранения, обработки и передачи информации. Теоретической информатикой называют науку о структурах, основывающихся на математике и логике. Практическая информатика является инженерной дисциплиной, опирающейся на сети и системы. В круг ее вопросов входят базы данных и знаний, информационно-поисковые системы, гиперсреда, вопросы языков, компьютерного перевода. Она опирается на теорию информации, искусственный интеллект, электронику, семиотику и др.

**Информационная инфраструктура** (*information Infrastructure)*– совокупность организационных структур, которые обеспечивают функционирование и развитие информационного пространства страны, а также средств информационного взаимодействия, обеспечивающих доступ граждан и организаций к информационным ресурсам.

**Информационная культура** (*nformation culture)*– способность общества эффективно использовать информационные ресурсы и средства информационных коммуникаций, а также применять для этих целей передовые достижения в области развития средств информатизации и

информационных технологий.

**Информационная преступность –**противоправные действия в информационной сфере общества, нарушающие установленные законом права личности, организации или государства и наносящие им моральный вред или материальный ущерб.

**Информационная сеть** (*information Network)* – совокупность информационных систем, использующих средства вычислительной техники и взаимодействующих друг с другом посредством коммуникационных каналов.

**Информационная система** (*information system) –* совокупность элементов (материальных или идеальных), определенным образом связанных между собой и образующих некоторую целостность. В качестве системы можно рассматривать любой объект действительности. Любая система уже по своей сути является информационным образованием, т.к. взаимосвязи ее элементов осуществляются посредством перетоков информации. Понятие системы в интернетике используется очень широко, имеет множество смысловых значений и чаще всего относится к взаимосвязанному набору средств технического и программного обеспечения, а также организационно упорядоченной совокупности документов.

**Информационная среда** (*information environment)*– совокупность окружающих информационную систему элементов (объектов), которые оказывают на нее влияние или, наоборот, на которые она воздействует. Внешняя среда любой системы рассматривается как подсистема информационной структуры более высокого уровня и, поэтому, является информационным образованием уже по своей сущности. Интернет, например, представляет среду для своих объектов и одновременно сам функционирует в информационном пространстве ноосферы.

**Информационное взаимодействие** (*information interaction)* – процесс обмена сведениями (информацией), приводящий к изменению знания хотя бы одного из получателей этих сведений. В живых и технических системах существует сложная иерархия уровней информационных взаимодействий, которые основываются на двух схемах:

* 1. Передатчик – кодирующее устройство – канал связи – декодирую- щее устройство – приемник (классическая схема К.Шеннона);
  2. Схема управления Н.Винера, в которой наряду с прямым потоком информации, присутствует обратный, передающий информацию о состоянии управляемого объекта (системы).

Организация оптимальных условий для информационных взаимодействий между пользователями при решении прикладных задач, по сути, является основным предназначением Интернета.

**Информационное пространство** (*information space)*–форма существования информационных систем, характеризующаяся структурностью, протяженностью и дифференцированностью.

**Информационно-поисковая система** (*information retrieval system)*– система, предназначенная для поиска информации в базе данных и всей совокупности информационных ресурсов.

**Информационные процессы** (*information processes)* –процессы создания, сбора, обработки, поиска, распространения и хранения информации.

**Информационные технологии** (*information technology)*– совокупность методов, производственных и программно-технологических средств, объединенных в технологическую цепочку, обеспечивающую сбор, хранение, обработку, вывод и распространение информации для снижения трудоемкости процессов использования информационных ресурсов, повышения надежности и оперативности.

**Информационный ресурс** (*information resources)* –отдельные документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других видах информационных систем).

**Информация** (*information)*– одно из наиболее актуальных, фундаментальных и дискуссионных понятий в современной науке и практике. В связи с отсутствием общего определения, в различных предметных областях имеет различные интерпретации. Философия рассматривает две противостоящие друг другу концепции: первая квалифицирует информацию как свойство всех материальных объектов, т.е. как атрибут материи (атрибутивный подход), а вторая связывает ее лишь с функционированием самоорганизующихся систем (функциональный подход). В информатике – это совокупность фактов, явлений, событий, представляющих интерес, подлежащих регистрации и обработке (по Э.А.Якубайтису). Наиболее прагматичным определением оперирует вычислительная техника, в которой информация есть содержание,

присваиваемое данным (по В.И.Першикову и В.М.Савинкову).

**Искусственный интеллект** (*artificial intelligence*) – способность прикладного процесса обнаруживать свойства, ассоциируемые с разумным поведением человека.

**Кадр** (*frame*) – группа битов, включающих данные, а также один или несколько адресов и прочую управляющую информацию протокола. Как правило, обозначает протокольный модуль данных (единицу передачи данных) уровня передачи данных (уровень 2 модели OSI).

**Канал** (*channel)*– средство или путь, по которому передаются сигналы или данные.

**Качество обслуживания***(QualityofService, QoS)* –означает свойства сети, соответствующие степени удовлетворения требований пользователя относительно производительности сети. Как правило, при оценке качества обслуживания учитываются четыре параметра: пропускная способность, или скорость передачи данных; задержка, или время ожидания; флуктуация (неравномерность) задержки и доля потерянных данных.

**Коллизия** (*collision*) – событие, возникающее при одновременной передаче двух пакетов по общему каналу связи. В результате оба пакета становятся непригодными.

**Кольцо** (*ring*) – топология локальной сети, в которой станции соединены с повторителями, образуя замкнутое кольцо. Данные передаются по кольцу в одном направлении и могут читаться всеми присоединенными станциями.

**Коммутация пакетов** *(packetswitching)* – метод передачи сообщений по сети, при котором длинные сообщения разбиваются на короткие пакеты. Затем пакеты передаются так же, как в сети с коммутацией сообщений.

**Коммутируемая сеть** *(switchedcommunicationnetwork)* – компьютерная сеть, состоящая из сети узлов, соединенных двухточечными линиями. Данные от отправителя к получателю передаются через промежуточные узлы.

**Компьютерная безопасность** *(computersecurity)*– комплекс технических и административных мер, применяемых в отношении аппаратных средств, программ, данных и служб с целью обеспечения доступности, целостности и конфиденциальности связанных с компьютерами ресурсов; сюда же относятся и процедуры проверки

выполнения системой определенных функций в строгом соответствии с их запланированным порядком работы.

**Компьютерный вирус** (*computer virus)*– программа, имеющая возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие объекты с целью искажения и уничтожения данных и программ. При этом дубликаты сохраняют способность к дальнейшему распространению. Такие программы, как правило, составляются на языке ассемблера, никаких сообщений на экран дисплея не выдают. Переносятся при копировании с диска на диск либо по сети Интернет.

**Конкуренция** (*contention*) – ситуация, возникающая, когда две или более станций пытаются одновременно использовать один и тот же канал.

**Контент**(*content)*– любое информационно значимое наполнение сервера, информационного комплекса – тексты, графика, мультимедиа. Организуется в виде страниц средствами гипертекстовой разметки. Существенными параметрами контента является его объем, актуальность и релевантность.

**Контроль с помощью циклического избыточного кода** *(CyclicRedundancyCheck, CRC*–код обнаружения ошибок; разновидность группового кода, все строки образующей матрицы которого могут быть получены при помощи циклического сдвига одной и той же комбинации.

**Контрольная последовательность кадра** (*FrameCheckSequence, FCS)* – помехоустойчивый код, вставляемый в виде поля в блок передаваемых данных. Этот код служит для обнаружения ошибок при приеме кадра.

**Контрольная сумма** *(checksum)*–код, используемый для обнаружения ошибок, основанный на суммировании разрядов контролируемых данных.

**Конфиденциальность**– сервис безопасности, предназначенный для предотвращения пассивных атак для передаваемых или хранимых данных; обеспечивает недоступность информации неавторизованным способом.

**Криптография** – область криптологии, в которой рассматриваются принципы, способы и методы преобразования данных для того, чтобы скрыть информационное содержание.

**Криптология**– наука о передаче/хранении информации.

**Логическое соединение** *(logicalconnection)\**– связь, устанавливаемая между функциональными модулями для передачи данных.

**Локальная сеть** *(LocalAreaNetwork, LAN) –* сеть, обеспечивающая соединение обменивающихся данными устройств, расположенных на небольшой территории.

**Маркерное кольцо** *(tokenring)* – метод управления доступом к несущей для локальной сети с кольцевой топологией. По кольцу циркулирует маркер (токен). Получившая маркер станция может передать пакет, после чего должна отдать маркер другой станции.

**Маршрутизатор** (*router*) – устройство объединенной сети, соединяющее две компьютерных сети. Оно использует межсетевой протокол и предполагает, что все соединенные устройства сети имеют одну и ту же архитектуру обмена данными и протоколы. Маршрутизатор функционирует на уровне 3 модели OSI.

**Маршрутизация** (*routing*)–определение пути для модуля данных (кадра, пакета, сообщения) от отправителя к получателю.

**Межсетевой экран** *(FireWall)*– устройство, программа, которые осуществляют фильтрацию данных на основе заранее заданной базы правил, что позволяет, по сравнению с традиционными операционными системами, реализовывать более гибкую политику безопасности. При комплексной фильтрации, охватывающей сетевой, транспортный и прикладной уровни, в правилах могут фигурировать сетевые адреса, количество переданных данных, операции прикладного уровня, параметры окружения (например, время) и т.п.

**Механизм безопасности**– программное или аппаратное средство, которое определяет и/или предотвращает определенную атаку.

**Модем** (*Modem)*– внешнее или внутреннее устройство, подключаемое к компьютеру для передачи и приема сигналов по разным линиям связи. Сокращение от "модулятор – демодулятор", что указывает на принцип работы этого устройства: преобразование цифрового сигнала, полученного от компьютера, в аналоговую форму для передачи и обратное преобразование принятого сигнала из аналоговой формы в цифровую.

**Множественный доступ с контролем несущей** *(CarrierSenseMultipleAccess, CSMA)*– метод управления доступом к несущей коллективного доступа. Станция, желающая передавать данные, сначала

опрашивает несущую и начинает передачу, только если несущая свободна.

**Множественный доступ с контролем несущей и обнаружением коллизий** *(CarrierSenseMultipleAccesswithCollisionDetection, CSMA/CD)*– усовершенствованный метод CSMA, при котором станции прекращают передачу в случае коллизий.

**Мост** (*bridge*)\* – функциональный модуль, соединяющий две локальные сети, в которых используется одинаковый протокол управления логической связью, но могут использоваться разные протоколы управления доступом к передающей среде.

**Мультимедиа** (*multimedia)*– взаимодействие визуальных и аудио эффектов под управлением интерактивного программного обеспечения. Обычно означает сочетание текста, звука и графики, а в последнее время все чаще – анимации и видео. Характерная, если не определяющая, особенность мультимедийных вэб-узлов и компакт-дисков – гиперссылки.

**Мультиплексирование** (*multiplexing*) – в системе передачи данных функция, позволяющая двум или более источникам данных совместно использовать общийноситель данных таким образом, что каждый источник данных получает собственный канал.

**Мультиплексирование с временным разделением** *(TimeDivisionMultiplexing, TDM)*– одновременная передача по двум или более информационным каналам в рамках одного физического канала.

**Немодулированная передача** (*baseband*) – передача сигналов без модуляции. В сети с передачей немодулированных сигналов цифровые сигналы (1 и 0) передаются напрямую по кабелю в виде импульсов напряжения. Сигнал использует весь спектр кабеля. Эта схема не допускает частотного мультиплексирования.

**Нонс** (*nonce*– данный случай, данное время) – уникальный порядковый номер, приписываемый к сообщению для предотвращения атак с повторным воспроизведением.

**Объединенная сеть** (*internet*) – группа сетей с коммутацией пакетов и широковещательных сетей, соединенных друг с другом маршрутизаторами. При написании с прописной буквы (Internet) означает всемирную сеть Интернет (см. *Интернет).*

**Оконечная система** *(EndSystem, ES)* – устройство, соединенное с одной из подсетей объединенной сети и используемое для обслуживания приложений или служб конечных пользователей.

**Оконечное оборудование линии передачи данных** *(DataCircuit-*

*terminatingEquipment, DCE*) –оборудование, осуществляющее преобразование сигнала и кодирование, обеспечивая сопряжение терминального оборудования с линией. Оконечное оборудование линии передачи данных может быть самостоятельным либо являться частью терминального или промежуточного оборудования. Оконечное оборудование линии передачи данных может также выполнять дополнительные функции, обычно выполняемые на сетевом конце линии.

**Онлайновые технологии** (*on line)*–средства коммуникации сообщений в сетевом информационном пространстве, обеспечивающие синхронный обмен информацией в реальном времени: "разговорные каналы" (чаты), аудио- и видеоконференции и др.

**Операционная система Linux** *(operating system Linux)* – сетевая операционная система, ядро которой разработано на базе операционной системы *Unix*. Одна из важнейших особенностей – она распространяется бесплатно по открытой лицензии *GNU* в рамках Фонда бесплатного программного обеспечения. Применяется в основном для создания серверов в Интернете и интрасетях.

**Остановка с ожиданием** *(stopandwait)* –протокол управления потоком, в котором отправитель передает блок данных, а затем, прежде чем отправить следующий блок, ждет подтверждения.

**Открытый ключ** – один из ключей алгоритма асимметричного шифрования, который делается доступным всем. С помощью данного ключа осуществляется проверка подписи, если алгоритм асимметричного шифрования используется для подписывания, либо осуществляется зашифрование, если алгоритм асимметричного шифрования используется для шифрования.

**Оффлайновые технологии***(off line)* –средства коммуникации сообщений в сетевом информационном пространстве, допускающие существенную асинхронность в обмене данными и сообщениями: списки рассылки, группы новостей, вэб-форумы и т. д.

**Пакет***(packet)*– производственная единица информации, передаваемая по сети или по каналу связи. Группа битов, включающая данные и управляющую информацию. Как правило, обозначает протокольный модуль данных (единицу передачи данных) сетевого уровня (уровня 3 модели OSI). Размер пакета определяется используемым протоколом, но в принципе пакет – это набор байтов, содержащий собственно передаваемые данные и информацию об отправителе и

адресате.

**Пароль** *(Password)*– секретное слово, предъявленное пользователем системе для получения доступа к данным и программам. Является средством их защиты от несанкционированного доступа.

**Передача данных, не требующая соединения** *(connectionlessdatatransfer)* –протокол «стихийного» (без предварительного согласования) обмена данными(например, дейтаграммами).

**Передача данных с установлением соединения** *(connection- orienteddatatransfer)* –протокол обмена данными, при котором между оконечными точками устанавливается логическое соединение (например, виртуальный канал).

**Персональный идентификационный номер** *(PersonalIdentificationNumber, PIN)* – персональный код некоторого лица, обеспечивающий ему возможность входа в систему с управляемым доступом.

**Подсеть** (*subnetwork*)–одна из сетей, составляющих объединенную сеть. Употребление этого термина позволяет избежать двусмысленности, так как с точки зрения пользователя объединенная сеть представляет собой единую сеть.

**Политика безопасности** – правила, директивы и практические навыки, которые определяют то, как информационные ценности обрабатываются, защищаются и распространяются в организации и между ИТ-системами; набор критериев для предоставления сервисов безопасности.

**Полнодуплексная передача** *(full-duplextransmission)–*

одновременная передача данных в обоих направлениях.

**Полудуплексная передача** *(half-duplextransmission)* - поочередная передача данных в каждом из направлений.

**Помехоустойчивый код** *(errordetectingcode)\**–код, строящийся по определенным правилам и содержащий определенное количество избыточной информации, что позволяет обнаруживать или исправлять ошибки.

**Порт** (*port*)–точка доступа к устройству либо программе. Средство идентификации пользователя протокольной службы. Протокольная сущность предоставляет один или несколько номеров портов для использования сущностями более высокого уровня. Эквивалентным

термином в эталонной модели OSI является *точка доступа к службе*

(ServiceAccessPoint, SAP).

**Портал** (*portal) –*сайт, организованный как системное многоуровневое объединение разных ресурсов и сервисов. Дает пользователю четкую информацию, осуществляет доступ к таким сервисам, как поисковые системы, электронный шоппинг, бесплатная электронная почта, торговая реклама, мгновенная рассылка сообщений, вэб-аукционы, чаты.

**Порядковый номер** *(sequencenumber)*–число, содержащееся в заголовке протокольного модуля данных (единицы передачи данных), служащее (отдельно или вместе с другими полями заголовка) для однозначной идентификации этого модуля данных в последовательности протокольных модулей данных.

**Прикладной уровень** *(applicationlayer)*–уровень 7 в модели OSI. Этот уровень определяет интерфейс системы с пользователем.

**Приложение** (*application)*–совокупность программ, реализующих обработку данных в определенной области применения.

**Протокол** (*Protocol)*–набор правил, управляющий работой функциональных модулей и обеспечивающий обмен данными, т.е. набор правил, которым следуют компьютеры и программы при обмене информацией. Существует масса различных протоколов, которые управляют всеми аспектами связи и передачи данных – от аппаратного до прикладного уровня, но все они сходны в том, что задают правила, делающие связь возможной.

**Протокол передачи гипертекстовой информации***(hyper* t*ext transfer protocol, HTTP)*– транспортный протокол, обеспечивающий доступ к документам на вэб-узлах. В этом качестве он фактически выполняет все запросы к вэб-узлам.

**Протокол управления передачей/межсетевой протокол** (*transmission control protocol / Internet protocol, TCP/IP)*– набор протоколов, разработанный для Интернета и ставший его основой. TCP гарантирует, что каждый посланный байт дойдет до получателя без потерь. IP присваивает локальные IP-адреса физическим сетевым адресам, обеспечивая тем самым адресное пространство, с которым работают маршрутизаторы. В семейство TCP/IP входят и протокол Telnet, который позволяет удаленным терминалам подключаться к удаленным узлам (компьютерам), система доменной адресации DNS, дающая возможность

пользователям адресоваться к узлам сети по символьному доменному имени вместо цифрового IP-адреса, протокол передачи файлов FTP, который определяет механизм хранения и передачи файлов, а также протокол передачи гипертекста HTTP.

**Протокольный модуль данных** *(ProtocolDataUnit, PDU)\**– единица передачи данных, состоящая из управляющей информации протокола этого уровня, а также, возможно, данных пользователя этого уровня.

**Региональная сеть** (*wide area network, WAN)*– крупная, нередко географически рассредоточенная сеть, коммуникационными средствами объединяющая в единое целое компьютеры в разных пунктах. Может охватывать и множество зданий в одном районе, и выходить за пределы государственных границ. Несколько распределенных сетей, связанных между собой, чаще называют не региональными сетями, а интерсетями или сетевыми комплексами.

**Релевантность** (*relevance)*– мера соответствия получаемого результата желаемому. В терминах поиска – это мера соответствия результатов поиска задаче поставленной в запросе

**Ретрансляция кадров** *(framerelay)*– форма коммутации пакетов, связанная с использованием кадров переменного размера на уровне передачи данных. В сети ретрансляции кадров нет сетевого уровня, кроме того, для повышения производительности упрощены или исключены многие базовые функции.

**Ретрансляция ячеек** *(cellrelay)*–механизм коммутации пакетов фиксированного размера, называемых ячейками. Эта технология применяется в ATM.

**Рунет** (*Runet) –* российская часть Интернета.

**Сеансовый уровень** *(sessionlayer)*–уровень 5 модели OSI. Управляет логическим соединением (сеансом) между двумя процессами или приложениями, обменивающимися данными.

**Секретный ключ** – ключ алгоритма симметричного шифрования, который используется как для зашифрования, так и для дешифрования.

**Семантика** (*semantics)* – раздел языкознания, исследующий с семиотических (семиотика – наука о знаках и знаковых системах) позиций смыслы и значения единиц языка (слов, предложений и др.), его выражений и логических форм, участвующих в его порождении, построении и изменении. В компьютерном программировании –

определяет сущность кодов, команд, сообщений и охватывает совокупность операций, служащих для определения либо кодирования смысла данных.

**Сервер** (*server)*– объект, предоставляющий сервис другим объектам по их запросам. В Интернете это, обычно, компьютер, подключенный к сети, и/или выполняющаяся на нем программа, предоставляющие клиентам доступ к общим ресурсам и управляющая этими ресурсами. Наиболее важными типами серверов являются:серверы WWW, предназначенные для представления взаимосвязанной мультимедийной информации и содержимого баз данных; серверы электронной почты; серверы FTP, предназначенные для обмена файлами; серверы общения в реальном времени (чаты); серверы, обеспечивающие работу Интернет- телефонии; системы трансляции радио и видео через Интернет.

**Сервис** (s*ervice) –*совокупность средств для обслуживания пользователей; набор функций одного из уровней программной структуры сети, обеспечивающих доступ к объектам вышележащего уровня через интерфейс между этими уровнями.

**Сервис безопасности** – сервис, который обеспечивает безопасность систем или передаваемых данных в соответствии с конкретной политикой безопасности. Сервис использует один или более механизмов безопасности и может также определять осуществление атаки.

**Сервисы Интернет** (*Internet servise)–*процессы обслуживания объектов Интернет. Сервисы предоставляются пользователям, программам, системам, уровням, функциональным блокам. Наиболее распространенными видами являются: хранение данных, передача сообщений и блоков данных, электронная и речевая почта, организация и управление диалогом партнеров, предоставление соединений, проведение сеансов, видео-сервис. Сервис осуществляют сетевые службы.

**Сертификат –**открытые ключи пользователя вместе с некоторой другой информацией, обработанные некоторым не подделываемым способом с использованием асимметричного шифрования Уполномоченным органом сертификации.

**Сертификационный центр***(Certificationauthority, CA)* – уполномоченный орган, который создает и подписывает сертификаты открытого ключа. Дополнительно может создавать пары закрытый/открытый ключ конечного участника. Отвечает за сертификаты открытого в течение всего времени их жизни, а не только в момент выпуска.

**Сетевая операционная система** *(network operating system) –* комплекс программ, обеспечивающих в сети обработку, хранение и передачу данных. Определяет взаимосвязанную группу протоколов верхних уровней, обеспечивающих основные функции сети. К ним в первую очередь относятся: адресация объектов, функционирование служб, обеспечение безопасности данных, управление сетью.

**Сетевой уровень** *(networklayer)*–уровень 3 моделиOSI. Отвечает за маршрутизацию данных в сети.

**Сеть связи** *(communicationnetwork)*–множество соединенных друг с другом функциональных модулей, предоставляющих услуги по обмену данными между станциями, присоединенными к сети.

**Симметричное шифрование** – криптосистема, в которой шифрование и дешифрование выполняется с использованием одного и того же ключа.

**Синхронное мультиплексирование с временным разделением** *(synchronoustimedivisionmultiplexing)*–разновидность мультиплексирования с временным разделением, при которой интервалы времени для доступа к общему носителю данных предоставляются каналам ввода-вы вода на заранее определенной основе.

**Скользящее окно** *(slidingwindow)*–метод управления потоком, при котором передающая станция может посылать нумерованные пакеты в пределах определенного диапазона номеров. Окно динамически изменяется для передачи дополнительных пакетов.

**Согласование битов** *(bitstuffing)*–включение в поток данных дополнительных битов, чтобы не допустить появления в потоке управляющих последовательностей.

**Спам** (*spam)* –рассылка какого-либо сообщения (чаще всего – рекламного или коммерческого содержания) множеству адресатов, для которых данное сообщение нежелательно, или во множество списков и групп новостей, тематика которых не соответствует содержанию сообщения. Справедливо считается тяжелым нарушением этикета и правил применения компьютерных сетей.

**Спецификация**– формализованное описание аппаратных или программных компонентов, способов их функционирования, взаимодействия с другими компонентами, условий эксплуатации, ограничений и особых характеристик. *Открытые спецификации*– опубликованные, общедоступные, соответствующие стандартам и

принятые в результате всестороннего обсуждения и согласования всеми заинтересованными сторонами.

**Списки рассылки** (*maillists)*–простой сервис Интернет, не имеющий собственного протокола и работающий исключительно через электронную

|  |  |  |
| --- | --- | --- |
| почту. Осуществляет коммуникацию сообщений | всем | подписчикам с |
| одного специального адреса. |  |  |
| **Статистическое мультиплексирование** | **с** | **временным** |
| **разделением** *(statisticaltimedivisionmultiplexing)* | – | разновидность |

мультиплексирования с временным разделением, при котором интервалы времени для доступа к общему носителю данных предоставляются каналам ввода-вывода по требованию.

**Страница** (*page)*– документ, снабженный уникальным адресом, который можно открыть и посмотреть с помощью программы просмотра. Страницы составляют [WWW.](http://WWW/) Как правило, это мультимедийные документы, включающие текст, графику, звук, видео или анимацию, гиперссылки на другие документы.

**Телеконференция** (*telecoferencing)*– метод проведения дискуссий между удаленными группами пользователей. Она осуществляется в режиме реального времени или просмотра документов.

**Терминальное оборудование** *(DataTerminalEquipment, DTE)\** – оборудование, состоящее из оконечных цифровых инструментов, преобразующее информацию пользователя в передаваемые сигналы, а получаемые сигналы в данные пользователя.

**Топология** (*topology*) – применительно к компьютерным сетям, геометрическая конфигурация (форма) сети, рассматриваемой в виде графа, состоящего из линий связи и узлов.

**Точка доступа к службе** *(ServiceAccess Point, SAP).* См. *порт.*

**Точка-точка** *(point-to-point)*–конфигурация, в которой две станции напрямую соединяются линиями связи.

**Транспортный уровень** *(transportlayer)*– уровень 4 эталонной модели OSI. Предоставляет надежную и прозрачную передачу данных между оконечными точками.

**Трафик** (*traffic)*– совокупный объем передаваемой информации за единицу времени, выраженный в единицах измерения компьютерной памяти (бит/с).

**Угроза** *(threat)*– характеристики, свойства системы и окружающей ее среды, которые в соответствующих условиях могут вызвать появление

опасного события. Атаки – частный вид угроз.

**Удаленный доступ** (*remote Access)*– технология взаимодействия абонентских систем с локальными сетями через территориальные коммуникационные сети.

**Узел** (*node)*– компьютер, терминал или любое другое устройство, подключенное к сети. Каждому узлу сети присвоен уникальный адрес, позволяющий другим компьютерам сети связываться с ним.

**Универсальный локатор ресурсов** (*uniform resourse locator, URL) –* стандартный способ представления местонахождения определённого ресурса в Интернете. В него входит, кроме названия файла и каталога, сетевой адрес машины и метод доступа к файлу. По сути, является протоколом работы с программами-серверами, функционирующими на удаленных компьютерах.

**Управление доступом к носителю** *(MediumAccessControl, MAC)* – применяемый в широковещательных сетях метод определения устройства, которое может получить доступ к передающей среде.

**Управление потоком** *(flowcontrol)*– выполняемая получающей сущностью функция, ограничивающая объем или скорость передачи данных от передающей сущности.

**Управляющая информация протокола** *(protocolcontrolinformation)\**–информация, позволяющая координировать совместную работу. Этой информацией обмениваются сущности данного уровня при помощи службы, предоставляемой ближайшим более низким уровнем.

**Уровень адаптации ATM***(ATMAdaptationLevel, AAL)*– уровень, обеспечивающий сопряжение между протоколами передачи информации и уровнем ATM.

**Уровень передачи данных** *(datalinklayer)\**–в архитектуре OSI уровень, предоставляющий услуги по передаче данных между двумя сущностями сетевого уровня, как правило, соседними узлами сети. Уровень передачи данных обнаруживает и по возможности исправляет ошибки, которые возникают на физическом уровне.

**Уровень представления** *(presentationlayer)\** – уровень 6 модели OSI. Обеспечивает выбор общей синтаксической формы представления данных и преобразования прикладных данных в эту форму и обратно.

**Уровень** (layer)\* – обладающая концептуальной полнотой группа служб, функций и протоколов из набора иерархически организованных групп сетевой

архитектуры.

**Уязвимость***(vulnerability)*– любая ошибка или слабая проработка, существующая в системе. Уязвимость создает предпосылки для нарушения безопасности системы и существует независимо от того, известны или нет какие-либо угрозы.

**Физический уровень***(physicallayer)*–уровень 1 моделиOSI. К этому уровня относятся электрические, механические и временные аспекты передачи сигнала по носителю.

**Формат***(format)* –структура информационного объекта. Определяет способ расположения и представления данных в разнообразных объектах: таблицах, базах данных, принтерах, блоках данных.

**Хакер** (*hacker)*– (букв. "взломщик") пользователь, путем обхода средств контроля доступа в сети вторгающийся в программное обеспечение в целях кражи (искажения, порчи) данных. Действия хакера преследуются по закону.

**Хост** (*host*) –установленный в узлах сети компьютер (сервер), решающий вопросы коммуникации и доступа к сетевым ресурсам: модемам, факс-модемам, большим компьютерам и др.; главный, ведущий, центральный компьютер.

**Хэш-функция** – функция, отображающая данные произвольной длины в строку битов фиксированной длины, которая может использоваться для аутентификации исходных данных.

**Целостность системы** *(systemintegrity)*– состояние системы, в котором существует полная гарантия того, что при любых условиях компьютерная система базируется на логически завершенных аппаратных и программных средствах, обеспечивающих работу защитных механизмов, логическую корректность и достоверность операционной системы и целостность данных. **Цифровая подпись** – блок данных, являющийся результатом функции подписывания, на вход которой подаются закрытый ключ подписывающей стороны (ключ подписывания), сообщение (или хэш-функция от сообщения) и параметры домена. Данный блок данных позволяет получателю проверить

целостность данных и источник данных.

**Частота ошибок** *(errorrate)\**– отношение числа модулей данных с ошибками к общему числу модулей данных.

**Чат** (*chat)*– канал обмена текстовыми сообщениями в режиме реального времени.

**Шина** *(bus)\** – один или несколько проводников, служащих для

соединения группы устройств.

**Широковещание** *(broadcast)* – одновременная передача данных нескольким станциям.

**Широковещательная сеть связи** *(broadcastcommunicationnetwork)* – сеть связи, в которой передача данных осуществляется путем широковещательной рассылки и принимается всеми остальными станциями.

**Широковещательный адрес** *(broadcastaddress)*– адрес, идентифицирующий сразу все станции домена (например, сети или объединенной сети).

**Экранирование** – как сервис безопасности выполняет разграничение межсетевого доступа путем фильтрации передаваемых данных, а также преобразование передаваемых данных.

**Электронная доска объявлений** (*bulletin board system)*– частный случай телеконференции, специальная база данных, на которой "вывешиваются" различные объявления и сообщения с целью их обмена.

**Электронная почта** (*electronic mail)*– один из сервисов Интернет для передачи сообщений или документов между пользователями без применения бумажного носителя.

**Язык гипертекстовой разметки HTML –***hypertext markup language***–** язык, используемый для создания документов, содержащих специальные команды форматирования и гипертекстовые ссылки и предназначенных для размещения в WWW и других службах и сетях.

**Язык гипертекстовой разметки WML** (*wireless markup language) –* язык, специально созданный для отображения информации на маленьком экране мобильного телефона в соответствии с протоколом WAP. Разработчикам публичных WAP-ресурсов приходится ориентироваться на то, что каждая WML-страница – это короткая текстовая информация с возможностью использования очень простых черно-белых изображений. Эквивалент HTML на базе XML.

**Язык гипертекстовой разметки XML** (*eXtensible markup language)*– расширяемый языкгипертекстовой разметки, используемой для создания и размещения документов в среде [WWW.](http://WWW/) В отличие от языка HTML, его можно использовать не только для передачи инструкций по представлению данных, но и для описания содержимого файлов практически любых типов. Позволяет автоматизировать обмен данными, не прибегая для этого к существенному объему программирования.

**Язык Java** (*language Java)*–интерпретируемый язык с синтаксисом С

++, специально рассчитанный на работу в открытой сетевой среде. Разработан компанией Sun Microsistems (США). Появление Jаva произвело переворот в области создания, применения и распространения программ и мультимедийной информации. Программы, написанные на этом языке, можно переносить на разные платформы (типы компьютеров), выполнять в мультипроцессорных системах, загружать по сети и выполнять программы в машине пользователя, а также одновременно по сети всем пользователям. Чтобы пользоваться возможностями языка Java, операционная система должна быть обеспечена интерпретатором, который помимо навигации обеспечиваетсвободную миграцию программ.

**Cookie**– это созданные веб-узлом объекты (файлы), которые сохраняют на жестком диске компьютера определенные сведения (о предпочтениях пользователя, личные данные пользователя, имя и адрес электронной почты) при посещении данного узла и считываются при последующих обращениях к узлу.

# ОБЩИЙ СПИСОК ЛИТЕРАТУРЫ

1. ***Айвенс, К.*** Компьютерные сети. Хитрости. / Айвенс К. – СПб.: Питер, 2006. – 298 с.
2. ***Анин, Б. Ю.*** Защита компьютерной информации. / Анин Б. Ю.–СПб.: БХВ–Петербург, 2000. – 384 с.
3. ***Барановская Т.П., Лойко В.И.*** Архитектура компьютерных систем и се- тей: учеб. пособие / Т. П. Барановская, В.И. Лойко [и др.]; под ред. В.И. Лойко. – М.: Финансы и статистика, 2003. – 256 с.: ил.
4. ***Баричев, С. Г.***Основы современной криптографии. / Баричев С. Г., Се- ров Р.Е.–СПб. Издательство «Наука и Техника», 2004. – 152 с.
5. ***Блэк, У.***Интернет: протоколы безопасности :учебный курс. / Блэк У. – СПб.: Питер, 2001. – 288 с.
6. ***Бормотов, С.В.*** Системное администрирование на 100% (+CD). / Бор- мотов С.В. – СПб.: Питер, 2006. – 256 с.
7. ***Ботт,Э.*** Эффективная работа: Windows XP/ Э. Ботт, К. Зихерт – СПб.: Питер.– 2004. – 1069 с.
8. ***Бройдо, В. Л.*** Вычислительные системы, сети и телекоммуникации / В. Л. Бройдо.– СПб.: Питер, 2003. – 688 с.
9. ***Галатенко, В.А.***Основы информационной безопасности : курс лекций / Галатенко В.А.;под ред. В.Б. Бетелина;изд.третье. –М.:ИНТУИТ.РУ «Ин- тернет-университет ИТ», 2006.–208 с.
10. ***Галатенко, В.А.*** Стандарты информационной безопасности: курс лек- ций / Галатенко В.А.;под ред. В. Б. Бетелина; изд второе издание– М.:ИНТУИТ.РУ «Интернет-университет ИТ», 2006.–264 с.
11. ***Гук,М.*** Аппаратные средства локальных сетей. Энциклопедия / М. Гук. – СПб.: Питер, 2004. – 573 с.
12. ***Гультяев, А.К.*** Виртуальные машины: несколько компьютеров в одном (+CD). / А.К. Гультяев.–СПб.: Питер. 2006. – 224 с.
13. ***Завгородний, В. И.*** Комплексная защита информации в компьютерных системах: учебное пособие. / Завгородний В. И. – М.: Логос; ПБОЮЛ Н.

А. Егоров, 2001. – 264 с.

1. ***Иванов, В.*** Компьютерные коммуникации :учебный курс. / Иванов В. – СПб.: Питер 2002. – 224 с.
2. ***Кингсли-Хью, Э.*** JavaScript 1.5: учебный курс. / Кингсли-Хью Э., Кинг- сли-Хью К. – СПб.: Питер, 2002 – 272 с.
3. ***Костромин, В.А.*** Самоучитель Linux для пользователя. / В.А. Костро- мин. –СПб.: БХВ–Петербург, 2003.–672 с.
4. ***Кульгин, М. В.***Компьютерные сети. Практика построения. Для профес- сионалов. / М. В. Кульгин; 2-е изд.–СПб.: Питер, 2003. 462 с.
5. ***Лапонина, О.Р.*** Основы сетевой безопасности: криптографические алго- ритмы и протоколы взаимодействия: учебное пособие. / О.Р. Лапонина; под ред. В.А. Сухомлина; изд. третье. –М.:ИНТУИТ.РУ «Интернет-уни- верситет ИТ», 2005. – 608 с.
6. ***Матвеев, М. Д.*** Самоучитель Microsoft Windows XP. Все об использова- нии и настройках. / М. Д. Матвеев[и др.];под ред. М. В. Финкова; изд. 2- е, пер. и доп.– СПб.: Наука и Техника, 2006. – 624 с.
7. ***Могилев, А.В.*** Информатика: учеб. пособие для студ. пед. вузов / А.В. Могилев[и др.]; под ред. Е.К. Хеннера; 3-е изд., перераб. и доп.–М.: Из- дательский центр«Академия», 2004.–848 с.
8. ***Назаров, С. В.*** Администрирование локальных сетей Windows NT/2000/.NET : учебное пособие / Назаров С. В. ; 2-е изд., перераб. и доп. – М.: Финансы и статистика, 2003. – 480 с.
9. ***Нанс, Б.*** Компьютерные сети. / Бэрри Нанс;пер. с англ.–М.: Восточная Книжная Компания, 1996.–400 с.
10. ***Немеет,Э.*** UNIX: руководство системного администратора. Для профес- сионалов. / Э.Немеет, Г. Снайдер, С.Сибасс, Т.Хейн; 3-е изд. – СПб.: Пи- тер: издательская группа BHV, 2006. – 925 с.
11. ***Новиков, Ю.В.*** Основы локальных сетей: учеб. пособие. / Ю.В.Новиков, С.В.Кондратенко. – М.: Интернет–Университет ИТ, 2005. – 360 с.
12. ***Олифер В.Г.*** Основы сетей передачи данных : учебное пособие / В.Г. Олифер, Н.А. Олифер; изд. второе. –М.:ИНТУИТ.РУ «Интернет-универ-

ситет Информационных Технологий», 2005. –76 с.

1. ***Олифер, В. Г.*** Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер; 3-е изд. – СПб.: Питер, 2006. – 958 с.
2. ***Олифер, В. Г.*** Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – СПб.: Питер, 2001. – 672 с.
3. ***Пасько, В.П.*** Энциклопедия ПК. Аппаратура. Программы. Интернет. / Пасько В.П. – Киев: Издательская группа BHV, 2004. – 800с.
4. ***Поляк-Брагинский, А. В.*** Администрирование сети на примерах. – СПб.: БХВ-Петербург, 2005. – 320 с.
5. ***Пятибратов, А. П.***Вычислительные системы, сети и телекоммуника- ции: учебник. / А. П. Пятибратов[и др.]; под ред. А. П. Пятибратова; 2-е изд., перераб. и доп.– М.: Финансы и статистика, 2004. – 512с.
6. ***Ратбон, Э.***Windows 2000 Professional для “чайников”. / Э. Ратбон, Ш. Крауфорд;пер. с англ. –Издательский дом “Вильямс”, 2003. – 352 с.
7. ***Симонович, С.В.*** Информатика: Базовый курс./ С.В. Симонович[и др.]– СПб.: Питер, 2003. – 640 с.
8. ***Станек, УильямР.*** Microsoft Windows XP Professional. Справочник адми- нистратора. / Уильям Р. Станек;пер. с англ.; 2-е изд. – М.: Издательско- торговый дом «Русская редакция», 2003. – 448 с.
9. ***Столлингс, В.*** Современные компьютерные сети. / В. Столлингс; 2-е изд. – СПб.: Питер, 2003. – 783 с.
10. ***Таненбаум, Э.*** Современные операционные системы. /Э. Таненбаум; 2-е изд. – СПб.: Питер, 2004 – 1040 с.
11. ***Таненбаум, Э.*** Компьютерные сети. / Э. Таненбаум; 4-е изд.. – СПб.: Пи- тер, 2003. – 992 с.
12. ***Управление*** сетевой средой Microsoft Windows 2000/ Учебный курс MCSA/MCSE/;пер. с англ. – М.: Издательско-торговый дом «Русская Ре- дакция», 2003. – 896 с.
13. ***Ханикат, Дж.*** Знакомство с MicrosoftWindowsServer 2003 / Дж. Хани- кат;пер. с англ.–М.: Издательско-торговый дом "Русская редакция",

2003.–464 с.

1. ***Хефлин, Д.*** Разработка Web-скриптов. Библиотека программиста. / Хе- флин Д., Ней Т. – СПб.: Питер, 2001. – 496 с.
2. ***Холме, Д.*** Управление и поддержка Microsoft Windows Server 2003. MCSA/MCSE / Д. Холме, О. Томас;пер. с англ.–М.: Издательско-торго- вый дом "Русская редакция", 2004.–448 с.
3. ***Холмогоров, В.*** Тонкая настройка Windows XP. / В. Холмогоров– СПб.: Питер , 2006. – 288 с.
4. ***Шнаер, Б.***Секреты и ложь. Безопасность данных в цифровом мире / Б. Шнаер. – СПб.: Питер, 2003. – 368 с.
5. ***Щеглов, А. Ю.*** Защита компьютерной информации от несанкциониро- ванного доступа. / А. Ю. Щеглов. – СПб.: Издательство «Наука и Техни- ка», 2004. – 384 с.
6. ***Mandriva*** Linux. Полное руководство пользователя.–СПб.:БХВ–Петер- бург, 2006.–544 с.
7. ***Microsoft*** Windows XP Professional/ Учебный курс MCSA/MCSE/ пер. с англ.; 2-е изд., испр. – М.: Издательско-торговый дом «Русская Редакция», 2003. – 1008 с.
8. ***Microsoft*** Windows XP. Руководство администратора / под общ. ред.

А.Н.Чекмарева. – СПб.: БХВ-Петербург, 2006. – 848 с.