МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УДМУРТСКОЙ РЕСПУБЛИКИ

Автономное профессиональное образовательное учреждение
Удмуртской Республики
«Техникум радиоэлектроники и информационных технологий
имени Александра Васильевича Воскресенского»

Практические работы

по МДК 01.02 «Технология монтажа и обслуживания компьютерных сетей**»**

Разработали преподаватели: Е.В. Нагорнова, А.Д. Насретдинов

Практическая работа № 1

«Монтаж кабельных сред технологий Ethernet»

Цель: Изучение назначения и способов монтажа разъемов для витой пары.

Время выполнения: 2 часа.

Оборудование: ПК; образец «витой пары»; обжимные клещи; коннектор RJ-45 (2 шт.); мультиметр.

Ход работы:

Теоретические сведения:

Назначение и структура витой пары. Самая простая витая пара – это два перевитых изолированных медных провода. Согласно стандарту, различают два вида витых пар:

– UTP - кабель на основе неэкранированной медной пары;

– STP - кабель на основе экранированной медной пары.

Неэкранированная витая пара (UTP, unshielded twisted pair) - это кабель, в котором изолированная пара проводников скручена с небольшим числом витков на единицу длины. Скручивание проводников уменьшает электрические помехи извне при распространении сигналов по кабелю.

Кабель на основе неэкранированной медной пары различают по его пропускной способности, выделяя тем самым несколько категорий:

Категория 3: Кабель этой категории имеет частоту передачи сигналов до 16 МГц и предназначен для использования в сетях скоростью до 10 Мбит/с.

Категория 4: Кабель 4-й категории передает данные с частотой до 20 МГц, используется в сетях Token Ring (скорость передачи до 16 Мбит/с)

Категория 5: Кабель этой категории предназначен для передачи сигнала с частотой 100 МГц при на скорости 100М\бит 4 витые пары.

Категория 5е: Кабель этой категории предназначен для передачи сигнала с частотой 100 МГц при на скорости 1000М\бит для сетей 1000BaseT, Gigabit Ethernet.

Категория 6: Кабель этой категории является одной из наиболее совершенных сред передачи данных среди вышеперечисленных категорий. Его частота передачи сигнала доходит до 250 МГц, что почти в два раза больше пропускной способности категории 5е. Улучшена помехозащищенность.

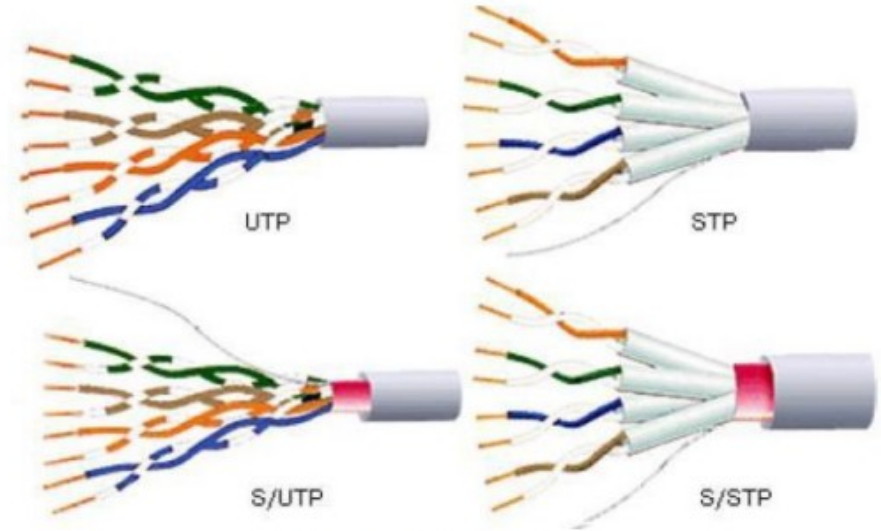


Рисунок 1 – Витая пара

Монтаж кабельной системы на основе витой пары.

Прямая разводка – применяется, когда кабель соединяет ПК с концентратором или концентратор с концентратором

Кросс-разводка – применяется для соединения ПК друг с другом.

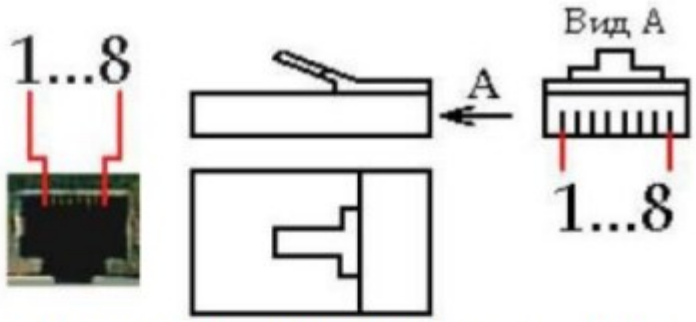


Рисунок 2 – Порт MDI/MDI-X и разъем RJ-45

Таблица 1 – Прямая разводка кабеля

№ контакта коннектора	Цвет проводника
1.	Бело-зеленый
2.	Зеленый
3.	Бело-оранжевый
4.	Синий
5.	Бело-синий
6.	Оранжевый
7.	Бело-коричневый
8.	Коричневый

Таблица 2 – Кросс-разводка кабеля

Контакта коннектора	Первый конец	Второй конец
1.	Бело-зеленый	Бело-оранжевый
2.	Бело-синий	Оранжевый
3.	Бело-оранжевый	Бело-зеленый
4.	Синий	Синий
5.	Бело-синий	Бело-синий
6.	Оранжевый	Бело-синий
7.	Бело-коричневый	Бело-коричневый
8.	Коричневый	Коричневый

После подключения коннекторов кабель следует проверить с помощью специального тестера, который определит, правильно ли проводники витых пар подсоединены к контактам коннекторов, а также целостность самого кабеля.

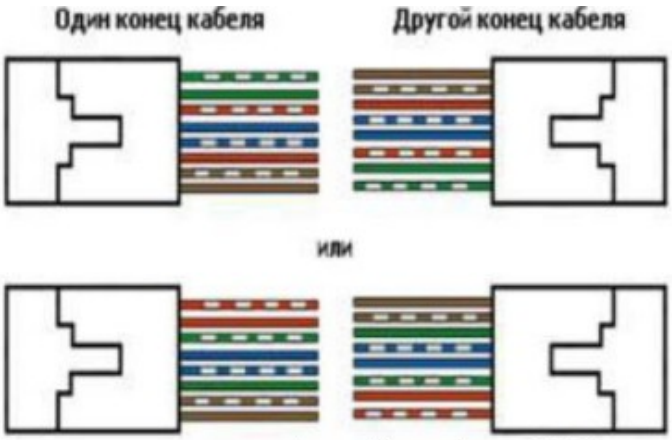


Рисунок 3а – Соединение компьютера/устройства (порта MDI) с концентратором (портом MDI-X)

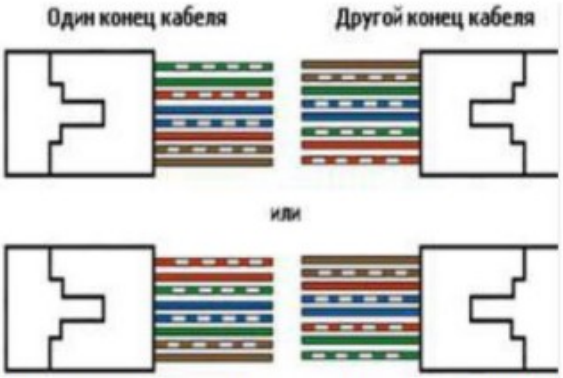
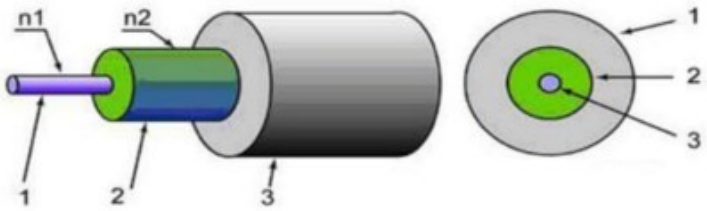


Рисунок 3б – Соединение компьютера/устройства (порта MDI) с компьютером (портом MDI)

Назначение и функции оптоволокна. В оптоволоконном кабеле цифровые данные распространяются по оптическим волокнам в виде модулированных световых импульсов. Это относительно защищенный способ передачи, поскольку при нем не используются электрические сигналы. Следовательно, к оптоволоконному кабелю невозможно подключиться, не разрушая его, и перехватывать данные, от чего не застрахован любой кабель, проводящий электрические сигналы.



1) сердцевина с показателем преломления n1; 2) отражающая оболочка с показателем преломления n2, n1>n2; 3) защитное покрытие

Рисунок 4 – Структура оптоволоконного кабеля:

Кабель содержит несколько световодов, хорошо защищенных пластиковой изоляцией. Он обладает сверхвысокой скоростью передачи данных (до 2 Гбит), и абсолютно не подвержен помехам. Расстояние между системами, соединенными оптиковолокном, может достигать 100 километров. Казалось бы, идеальный проводник для сети найден, но стоит оптический кабель чрезвычайно дорого, и для работы с ним требуется специальные сетевые карты, коммутаторы и т.д. Без специального оборудования оптоволокно практически не подлежит ремонту. Данное соединение применяется для объединения крупных сетей, высокосортного доступа в Интернет (для провайдеров и крупных компаний), а также для передачи данных на большие расстояния. В домашних сетях, если требуется высокая скорость соединения, гораздо дешевле и удобнее воспользоваться гигабитной сетью на витой паре.

Лучи, входящие под разными углами в оптоволокно, называются модами, а волокно, поддерживающее несколько мод - многомодовым. По одномодовому волокну распространяется только один луч.

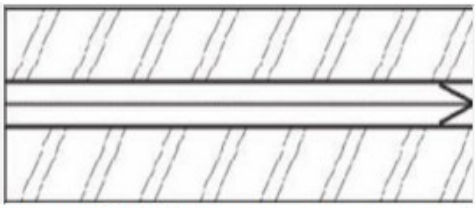


Рисунок 5а – Одномодовое оптоволокно

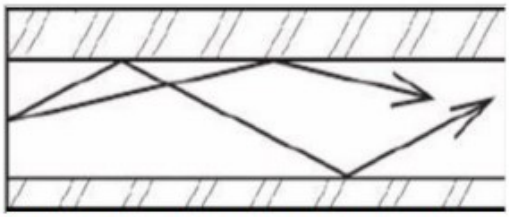


Рисунок 5б – Многомодовое оптоволокно

III. Правила выполнения заданий:

При монтаже кабеля витой пары должен выдерживаться минимально допустимый радиус изгиба — сильный изгиб может привести к увеличению внешних наводок на сигнал или привести к разрушению оболочки кабеля.

При монтаже экранированной витой пары необходимо следить за целостностью экрана по всей длине кабеля. Растяжение или изгиб приводит к разрушению экрана, что влечёт уменьшение сопротивляемости наводкам. Дренажный провод должен быть соединен с экраном разъема.

Задание 1.

1. Отрезать кусок витой пары нужной длины от бухты, при этом можно воспользоваться резаком, встроенным в обжимной инструмент.
2. Аккуратно снять изоляцию с кабеля. Для этого лучше использовать специальный инструмент для зачистки изоляции витой пары, его лезвие выступает ровно на толщину изоляции, чтобы не повредить проводники.
3. Расплести и развести проводники, выровнять их в один ряд, при этом соблюдая схему обжима витой пары.
4. Обкусить проводники таким образом, чтобы их длина от изоляции была чуть больше сантиметра. Для этого можно воспользоваться инструментом для обрезки витой пары, или ножами, встроенными в обжимной инструмент.
5. Аккуратно вставить проводники в коннектор RJ-45. Обратить внимание, чтобы расположение проводов относительно коннектора при обжиме второго конца провода полностью совпадало с первым.

6. Проверить, не перепутались ли проводники и правильно ли они вошли в коннектор, при этом все провода должны упереться в переднюю стенку коннектора.
7. Поместить коннектор с расположенными в нем проводниками в клещи, затем плавно, но сильно произвести обжим витой пары. Обязательно следует проверить правильность обжима витой пары на предмет отсутствия контакта в отдельных проводниках. Это можно сделать при помощи мультиметра.

Задание 2.

Осуществите обжим витой пары по типу прямой разводки и кросс-разводки. Сделать сравнительную характеристику полученных образцов с рисунком 5а и 5б.

Задание 3.

Проверьте правильность изготовления патч-кордов RJ-45 кабельным тестером. С помощью простейшего кабельного тестера необходимо обязательно проверить правильность монтажа и целостность линий. Кабельный тестер состоит из двух частей – основной и удаленной, обозначенных соответственно Master и Remote. Соединить получившимся патчкордом обе части прибора и включить главную. При этом на главной части должны поочередно загораться по одному из 9 светодиодов, каждый из которых соответствует отдельной жиле (последний соответствует экрану). При правильном соединении, светодиоды удаленной части должны гореть синхронно с главной. При этом загорание вразброс, пропуск одного из диодов или их совместное загорание соответствуют дефектам линии: перепутанные жилы, обрыв или короткое замыкание.

Задание 4.

Ответить на контрольные вопросы:

1. Какие существуют типы кабелей? В чем их достоинства и недостатки? Раскрыть суть. Обоснуйте ответ.
2. Какие существуют разновидности витой пары? Дать определение понятию витая пара.
3. Коаксиальный кабель: назначение и структура.
4. Неэкранированная витая пара: назначение и структура.
5. Экранированная витая пара: назначение и структура.
6. Оптоволоконный кабель: назначение и структура.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 2

«Прямое соединение компьютеров и через внешний сетевой концентратор»

Цель: Изучить и освоить методы прямого соединения двух компьютеров с использованием сетевого кабеля, а также подключение через внешний сетевой концентратор. Ознакомиться с настройкой сетевых параметров, проверкой соединения и анализом работы локальной сети.

Время выполнения: 4 часа.

Оборудование:

- Два компьютера с сетевыми картами.
- Ethernet-кабели (прямые или кроссоверные).
- Сетевой концентратор (Hub) или коммутатор (Switch) — для второго способа.
- Операционная система (Windows/Linux).

Ход работы:

Теоретические сведения:

1. Прямое соединение компьютеров (Компьютер-компьютер, Direct Connection)

Прямое соединение двух компьютеров может осуществляться с помощью сетевого кабеля (обычно витая пара) без использования промежуточного сетевого оборудования.

Варианты подключения:

С помощью Ethernet-кабеля (витая пара, кроссоверный кабель)

Ранее использовался кроссоверный (перекрестный) кабель для соединения двух ПК напрямую, но современные сетевые адаптеры поддерживают автоопределение (Auto-MDIX), что позволяет использовать обычный прямой кабель.

Через USB-кабель для передачи данных

Специальные USB-кабели позволяют соединять компьютеры напрямую.

С помощью беспроводной сети (Wi-Fi Direct, Ad-Hoc)

Позволяет организовать беспроводное соединение между двумя устройствами.

Настройки соединения по Ethernet:

Оба компьютера должны находиться в одной подсети.

IP-адреса задаются вручную (например, 192.168.1.1 и 192.168.1.2).

Проверка соединения с помощью команды ping.

2. Соединение через сетевой концентратор (Hub) или коммутатор (Switch)

Если компьютеры соединены через сетевое оборудование (концентратор или коммутатор), они могут взаимодействовать в одной локальной сети (LAN).

Разница между Hub и Switch:

Hub (концентратор) — передает данные всем устройствам в сети, снижая общую скорость передачи.

Switch (коммутатор) — направляет данные только конкретному получателю, что делает его более эффективным.

Настройка соединения через Hub/Switch:

Обычные прямые Ethernet-кабели.

Автоматическое получение IP-адресов при наличии DHCP-сервера или ручная настройка.

Проверка соединения через ping.

Задание:

1. Прямое соединение компьютеров через Ethernet

Шаги:

Подключите два ПК с помощью Ethernet-кабеля.

Откройте настройки сетевого адаптера:

Windows: Панель управления → Сеть и Интернет → Центр управления сетями и общим доступом → Изменение параметров адаптера.

Linux: ip a или ifconfig (в зависимости от системы).

Назначьте IP-адреса вручную:

Компьютер 1: 192.168.1.1, маска 255.255.255.0.

Компьютер 2: 192.168.1.2, маска 255.255.255.0.

Проверьте связь с помощью ping 192.168.1.2 (с первого ПК) и ping 192.168.1.1 (со второго).

2. Соединение через сетевой концентратор (Hub) или коммутатор (Switch)

Шаги:

Подключите оба компьютера к концентратору/коммутатору с помощью Ethernet-кабелей.

Если в сети нет DHCP-сервера, задайте IP-адреса вручную (аналогично первому варианту).

Проверьте соединение с помощью ping.

При необходимости настройте общий доступ к файлам и папкам.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания

Оценка «4» ставится, если выполнено не менее 80% заданий

Оценка «3» ставится, если выполнено не менее 60% заданий

Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 3

«Соединение компьютеров через концентратор»

Цель: Ознакомиться с принципами подключения компьютеров через сетевой концентратор, изучить его роль в организации локальной сети, научиться настраивать сетевые параметры и проверять работоспособность соединения.

Время выполнения: 2 часа.

Оборудование:

- Концентратор (Hub).
- Два или более компьютеров с сетевыми картами.
- Прямые Ethernet-кабели (витая пара).
- Операционная система Windows/Linux.

Ход работы:

Теоретические сведения:

1. Что такое концентратор (Hub)?

Сетевой концентратор (Hub) — это устройство, которое используется для объединения нескольких компьютеров в локальную сеть (LAN). Он передает входящие данные на все подключенные устройства без анализа их содержимого.

Особенности концентратора:

Работает на 1-м уровне модели OSI (физическом).
Не фильтрует и не направляет трафик, а просто транслирует его на все порты.
Может вызывать перегрузку сети при большом количестве устройств.
Используется в небольших локальных сетях или для тестирования.

2. Принцип работы соединения через Hub

Все компьютеры подключаются к концентратору с помощью Ethernet-кабелей.
При передаче данных концентратор дублирует их на все порты.
Получатель проверяет, предназначены ли данные для него, и, если да, принимает их.

3. Требования для работы сети через Hub

Все компьютеры должны быть в одной подсети (например, 192.168.1.x).
Должны использоваться прямые Ethernet-кабели.
Можно использовать статическую или динамическую (DHCP) настройку IP-адресов.

Задание:

1. Подключение компьютеров через концентратор

Шаги:

Подключите концентратор к электросети.
Соедините каждый компьютер с концентратором с помощью Ethernet-кабеля.
Убедитесь, что на каждом компьютере включен сетевой адаптер.

2. Настройка сети (Windows/Linux)

Автоматическая настройка (через DHCP)

Если в сети есть DHCP-сервер (например, маршрутизатор), компьютеры автоматически получат IP-адреса.

Ручная настройка IP-адресов (если DHCP нет)

Откройте настройки сетевого адаптера:

Windows: Панель управления → Сеть и Интернет → Центр управления сетями и общим доступом → Изменение параметров адаптера.

Linux: ip a или ifconfig.

Выберите "Протокол Интернета версии 4 (TCP/IPv4)" и задайте IP-адреса вручную:

Компьютер 1: IP 192.168.1.2, Маска 255.255.255.0, Шлюз 192.168.1.1 (если есть).

Компьютер 2: IP 192.168.1.3, Маска 255.255.255.0.

Сохраните настройки.

3. Проверка соединения

Откройте командную строку (cmd в Windows, Terminal в Linux).

Введите команду ping 192.168.1.3 (с первого ПК) и ping 192.168.1.2 (со второго).

Если пакеты успешно передаются, значит сеть работает.

4. Дополнительные тесты

Открытие общего доступа к файлам и папкам.

Использование ipconfig /all (Windows) или ifconfig (Linux) для проверки настроек.

Тестирование передачи файлов через общий доступ или FTP.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания

Оценка «4» ставится, если выполнено не менее 80% заданий

Оценка «3» ставится, если выполнено не менее 60% заданий

Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 4

«Настройка стека протоколов TCP/IP»

Цель: Изучить способы диагностики настроек стека протоколов TCP/ IP; получить сведения о настройке TCP/IP для работы с DHCP сервером.

Время выполнения: 2 часа.

Оборудование:

- аппаратные: компьютер с установленной ОС Windows XP.
- программные: виртуальные машины: VM-1.
- информационные: IP_адрес; маска подсети; основной шлюз; предпочитаемый DNS.

Ход работы:

Теоретические сведения:

На концептуальной модели взаимодействия открытых систем OSI основан стек протоколов ***TCP/IP*** *(Transmission Control Protocol - протокол управления передачей / Internet Protocol – Интернет-протокол)*, который предоставляет ряд стандартов для связи компьютеров и сетей.

Стек протоколов TCP/IP – промышленный стандарт, который позволяет организовать сеть масштаба предприятия и связывать компьютеры, работающие под управлением различных операционных систем.

Применение стека протоколов TCP/IP дает следующие преимущества:

1. поддерживается почти всеми операционными системами; почти все большие сети основаны на TCP/IP;
2. технология позволяет соединить разнородные системы;
3. надежная, расширяемая интегрированная среда на основе модели «клиент — сервер»;
4. получение доступа к ресурсам сети Интернет.

Каждый узел ***TCP/IP*** идентифицирован своим логическим IP-адресом, который идентифицирует положение компьютера в сети почти таким же способом, как номер дома идентифицирует дом на улице.

Реализация ***TCP/IP*** позволяет узлу ***TCP/IP*** использовать статический IP-адрес или получить IP-адрес автоматически с помощью ***DHCP-сервера*** *(Dynamic Host Configuration Protocol- протокол динамической конфигурации хоста).*

Для простых сетевых конфигураций, основанных на локальных сетях (*LAN, Local Area Network*), он поддерживает автоматическое назначение IP-адресов.

По умолчанию компьютеры клиентов, работающие под управлением ОС **Windows** или **Linux**, получают информацию о настройке протокола ***TCP/IP*** автоматически от службы ***DHCP***.

Однако даже в том случае, если в сети доступен ***DHCP-сервер***, необходимо назначить статический IP-адрес для отдельных компьютеров в сети. Например, компьютеры с запущенной службой ***DHCP*** не могут быть клиентами ***DHCP***, поэтому они должны иметь статический IP-адрес.

Если служба ***DHCP*** недоступна, можно настроить ***TCP/IP*** для использования статического IP-адреса.

Для каждой платы сетевого адаптера в компьютере, которая использует ***TCP/IP***, можно установить IP-адрес, маску подсети и шлюз по умолчанию.

Ниже описаны параметры, которые используются при настройке статического адреса ***TCP/IP***.

Параметр	Описание
IP-адрес	Логический 32-битный адрес, который идентифицирует TCP/IP узел. Каждой плате сетевого адаптера в компьютере с запущенным протоколом TCP/IP необходим уникальный IP-адрес, такой, как 192.168.0.108. Каждый адрес имеет две части: ID сети, который идентифицирует все узлы в одной физической сети и ID узла, который идентифицирует узел в сети. В этом примере ID сети — 192.168.0, и ID узла — 108.
Маска подсети	Подсети делят большую сеть на множество физических сетей, соединенных маршрутизаторами. Маска подсети закрывает часть IP-адреса так, чтобы TCP/IP мог отличать ID сети от ID узла. При соединении узлов TCP/IP, маска подсети определяет, где находится узел получателя: в локальной или удаленной сети. Для связи в локальной сети компьютеры должны иметь одинаковую маску подсети.
Шлюз по умолчанию	Промежуточное устройство в локальной сети, на котором хранятся сетевые идентификаторы других сетей предприятия или Интернета. TCP/IP посылает пакеты в удаленную сеть через шлюз по умолчанию (если никакой другой маршрут не настроен), который затем пересылает пакеты другим шлюзам, пока пакет не достигнет шлюза, связанного с указанным адресатом.

*Таблица 1. Параметры, используемые при настройке статического адреса **TCP/IP***

Если сервер с запущенной службой ***DHCP*** доступен в сети, он автоматически предоставляет информацию о параметрах ***TCP/IP*** клиентам ***DHCP***.

Задание 1. Проверьте работоспособность стека протоколов TCP/IP.

1. Запустите виртуальную машину **VM-1** и загрузите ОС **Windows**.
2. Запустите консоль ***(Пуск/Программы/Стандартные/Командная строка)***.
3. В командной строке введите **ipconfig /all | more**.
4. Используя приведенную ниже информацию, создайте в своей папке текстовый документ со следующими данными:
    - Имя компьютера;
    - Основной DNS-суффикс;
    - Описание DNS-суффикса для подключения;
    - Физический адрес;
    - DHCP включен;
    - Автоконфигурация включена;
    - IP-адрес автоконфигурации;
    - Маска подсети;
    - Шлюз по умолчанию.
5. Убедитесь в работоспособности стека ***TCP/IP***, отправив эхо-запросы на IP-адреса. Для этого воспользуйтесь командой **ping**:

- отправьте эхо-запросы на локальный адрес компьютера (*loopback*) **ping 127.0.0.1** (на экране должны появиться сообщения о полученном ответе от узла 127.0.0.1);
- отправьте эхо-запрос по другому IP-адресу, например **172.21.5.1**.

Задание 2. Настройте стек протоколов *TCP/IP* для использования статического IP-адреса.

1. Откройте окно **Сетевые подключения *(Пуск/Панель управления/Сетевые подключения)***.
2. Вызовите **свойства подключения по локальной сети**. Для этого можно воспользоваться контекстным меню.
3. В появившемся диалоговом окне на вкладке **Общие** откройте свойства **Протокол Интернета TCP/IP**.
4. Щелкните переключатель *Использовать следующий IP-адрес* и введите в соответствующие поля данные: **IP_адрес; Маску подсети; Основной шлюз; Предпочитаемый DNS**.
5. Примените параметры кнопкой ***OK***.
6. Закройте окно свойств подключения кнопкой ***OK*** (если потребуется, то согласитесь на перезагрузку компьютера).
7. Проверьте работоспособность стека протоколов ***TCP/IP***.

Задание 3. Настройте TCP/IP для автоматического получения IP-адреса.

1. Откройте окно **Сетевые подключения**.
2. Вызовите свойства **Подключения по локальной сети**.
3. Откройте свойства **Протокол Интернета TCP/IP**.
4. Установите переключатель *Получить IP-адрес автоматически*.
5. Закройте диалоговое окно **Свойства: Протокол Интернета TCP/IP** кнопкой ***OK***.
6. Примените параметры кнопкой ***OK***.
7. Проверьте настройку стека протоколов ***TCP/IP***.
8. Получите другой адрес для своего компьютера. Для этого:
   - запустите консоль (командную строку);
   - введите команду для сброса назначенных адресов - **ipconfig /release**;
   - введите команду для получения нового адреса **ipconfig / renew**;
9. Проверьте работоспособность стека протоколов ***TCP/IP***.

Задание 4. Создайте IP-калькулятор в табличном процессоре для облегчения формирования маски подсети.

1. Откройте табличный процессор и сформируйте таблицу по следующему шаблону:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG
1		1-й октет								2-й октет								3-й октет								4-й октет							
2	биты	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
3		ID-сети																													ID-узла		
4	IP- адрес	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1
5	Десятичная запись	192								0								1								255							
6	Маска подсети	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0
7	Десятичная запись	255								255								255								248							

Рисунок 1. Образец оформления таблицы

*Далее необходимо ввести в ячейки **B5, J5, R5, Z5** формулы для перевода двоичного представления IP-адреса в точечную десятичную нотацию по октетам.*

2. Введите в ячейку **B5** формулу для преобразования 1-го октета IP-адреса в десятичную систему счисления:

=I4*2^I2+H4*2^H2+G4*2^G2+F4*2^F2+E4*2^E2+D4*2^D2+C4*2^C2+B4*2^B2

3. Скопируйте введенную формулу в остальные ячейки (**J5, R5, Z5**).
4. Самостоятельно введите в ячейки **B5, J5, R5, Z5** формулы для преобразования маски подсети из двоичного представления в точечную десятичную нотацию.
5. Сохраните файл в своей папке с именем ***IPCALC***.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 5

«Диагностические утилиты протокола TCP/IP»

Цель: Изучить и освоить работу диагностических утилит протокола TCP/IP, таких как ping, tracert, ipconfig, netstat и других. Научиться анализировать сетевые подключения, выявлять и устранять возможные проблемы в работе сети.

Время выполнения: 2 часа.

Оборудование:

- Компьютер с ОС Windows/Linux.
- Доступ в локальную сеть или Интернет.

Ход работы:

Теоретические сведения:

1. Что такое TCP/IP?

TCP/IP (Transmission Control Protocol / Internet Protocol) — это набор сетевых протоколов, используемых для связи устройств в компьютерных сетях, включая Интернет.

2. Назначение диагностических утилит

Диагностические утилиты TCP/IP позволяют:

- Проверять доступность узлов в сети.
- Определять маршруты передачи данных.
- Выявлять проблемы в работе сетевых соединений.

3. Основные утилиты диагностики TCP/IP

Утилита	Описание
`ping`	Проверяет доступность удаленного узла, отправляя пакеты ICMP.
`tracert` (Windows) / `traceroute` (Linux)	Показывает маршрут передачи данных до узла.
`ipconfig` (Windows) / `ifconfig` (Linux)	Отображает текущие сетевые настройки.
`nslookup`	Проверяет работу DNS и отображает IP-адрес домена.
`netstat`	Показывает активные сетевые соединения и статистику.
`arp`	Показывает таблицу ARP (сопоставление IP и MAC-адресов).
`route`	Отображает таблицу маршрутизации.
`telnet` / `nc` (netcat)	Проверяет доступность портов на удаленном хосте.

Задание:

1. Проверка связи с хостом (ping)

1. Открыть командную строку (cmd в Windows, Terminal в Linux).
2. Ввести команду:

```nginx
ping 8.8.8.8
```

Если получен ответ, значит хост доступен.
Если пакеты теряются, возможны проблемы с сетью.

2. Определение маршрута до узла (tracert/traceroute)

1. Ввести команду:
   - Windows:

```nginx
tracert ya.ru
```

   - Linux:

```nginx
traceroute ya.ru
```

2. В результате отобразятся все промежуточные узлы на пути к серверу.

3. Просмотр сетевых настроек (ipconfig / ifconfig)

1. Ввести команду:
   - Windows:

```bash
ipconfig /all
```

   - Linux:

```nginx
ifconfig
```

2. Можно узнать IP-адрес компьютера, шлюз и DNS-серверы.

4. Проверка работы DNS (nslookup)

1. Ввести команду:

```nginx
nslookup google.com
```

2. Отобразится IP-адрес сайта и DNS-сервер, который использовался для запроса.

Просмотр активных соединений (netstat)

1. Ввести команду:

```nginx
netstat -an
```

2. Будут показаны все активные сетевые соединения и порты.

6. Проверка таблицы ARP (arp -a)

1. Ввести команду:

```css
arp -a
```

2. Отобразится список MAC-адресов, связанных с IP-адресами.

7. Проверка доступности порта (telnet / netcat)

1. В Windows:

```nginx
telnet google.com 80
```

2. В Linux:

```nginx
nc -zv google.com 80
```

3. Если соединение установлено, порт доступен.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 6

«Поиск неисправностей в локальной сети»

Цель: Ознакомиться с методами диагностики и устранения неисправностей в локальной сети, изучить основные причины сбоев, освоить использование сетевых утилит и инструментов для выявления и устранения проблем в работе сети.

Время выполнения: 2 часа.

Оборудование:

- Компьютер с Windows/Linux.
- Доступ к локальной сети.
- Командная строка (cmd в Windows, Terminal в Linux).
- Диагностические утилиты (ping, tracert, ipconfig, netstat).

Ход работы:

Теоретические сведения:

1. Что такое локальная сеть (LAN)?

Локальная сеть (Local Area Network, LAN) — это группа соединенных между собой устройств (компьютеров, серверов, принтеров и др.), которые находятся в пределах одного здания или кампуса.

2. Основные причины неисправностей в локальной сети

Неисправности могут быть связаны с:

Проблемами с физическим подключением

Неисправные или плохо подсоединенные кабели.
Поврежденные разъемы или сетевые порты.
Отключенное или неработающее сетевое оборудование (маршрутизатор, коммутатор).
Неправильными сетевыми настройками

Неверные IP-адреса, маска подсети, шлюз.
Дублирование IP-адресов в сети.
Проблемы с DHCP-сервером.
Программными проблемами

Блокировка соединений брандмауэром или антивирусом.
Ошибки в драйверах сетевых адаптеров.
Перегрузкой сети или аппаратными сбоями

Высокая нагрузка на сетевой канал.
Выход из строя сетевого оборудования.

Задание:

1. Проверка физического соединения
Осмотр кабелей и разъемов

Убедитесь, что кабель надежно подключен.
Попробуйте заменить кабель, если есть подозрение на его неисправность.

Проверка сетевого оборудования

Убедитесь, что сетевой адаптер включен (ipconfig / ifconfig).
Перезагрузите маршрутизатор/коммутатор.
Проверьте индикаторы активности портов (обычно они мигают при передаче данных).

2. Проверка сетевых настроек

Ввести команду для просмотра текущих параметров сети:
Windows

```bash
ipconfig /all
```

Linux

```nginx
ifconfig
```

1. Убедиться, что:
   - IP-адрес находится в правильной подсети.
   - DHCP-сервер назначает корректные адреса.
   - Адрес шлюза (роутера) совпадает с ожидаемым.
2. Если DHCP не работает, задать IP-адрес вручную:
   - IP: 192.168.1.100
   - Маска: 255.255.255.0
   - Шлюз: 192.168.1.1

3. Проверка связи с другими устройствами

1. Проверить подключение к локальной сети с помощью ping:

```nginx
ping 192.168.1.1
```

- Если есть ответ, соединение с маршрутизатором работает.
- Если нет ответа, проблема может быть в кабеле, сетевом адаптере или настройках.

2. Проверить доступ к интернету:

```nginx
ping 8.8.8.8
```

Если работает, но сайты не открываются, возможны проблемы с DNS.

4. Проверка работы DNS

1. Ввести команду:

```nginx
nslookup ya.ru
```

Если IP-адрес возвращается корректно, значит, DNS работает.

5. Проверка маршрута передачи данных

1. Выполнить команду:

```nginx
tracert ya.ru
```

Или в Linux:

```
nginx

traceroute ya.ru
```

Если маршрут обрывается на первом узле, проблема в локальной сети.

6. Проверка занятых портов и соединений

1. Ввести команду

```
nginx

netstat -an
```

Если все порты заняты или есть подозрительная активность, возможно, система заражена или перегружена.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 7

«Адресация пакетов в IP сетях»

Цель: Приобретение навыков классификации и анализа IP-адресов.

Время выполнения: 2 часа.

Ход работы:

Теоретические сведения:

В IP-сетях все сетевые устройства (хосты, серверы, шлюзы, маршрутизаторы и т.д.) получают уникальные IP-адреса.

IP-адрес состоит из 4-х байтов (32 битов). Этот адрес используется на сетевом уровне эталонной модели OSI. В IP-адресе выделяются две части – **адрес сети** и **адрес узла**. Деление происходит с помощью маски – 4-х байтного числа, которое поставлено в соответствие IP-адресу. Маска содержит двоичные «единицы» в тех разрядах IP-адреса, которые определяют адрес сети и двоичные «нули» в тех разрядах IP адреса, которые определяют адрес узла.

Правила об особенностях IP-адресов:

- если IP-адрес состоит только из двоичных нулей, то он обозначает адрес того узла, который сгенерировал этот пакет;
- если в поле номера сети стоят «нули», то по умолчанию считается, что этот узел принадлежит той же самой сети, что и узел, который отправил пакет;
- если все двоичные разряды IP-адреса равны «единицы», то пакет с таким адресом назначения должен рассылаться **всем** узлам, находящимся в той же сети, что и источник этого пакета. Такая рассылка называется ограниченным широковещательным сообщением (limited broadcast);
- если в поле адреса назначения стоят сплошные «единицы», то пакет, имеющий такой адрес, рассылается всем узлам сети с заданным номером. Такая рассылка называется широковещательным сообщением (broadcast);
- адрес 127.0.0.1 зарезервирован для организации обратной связи при тестировании работы программного обеспечения узла без реальной отправки пакета по сети. Этот адрес имеет название loopback.

Адрес получателя должен содержать в себе:

- адрес (номер) подсети;
- адрес (номер) хоста (узла) внутри подсети.

Часто возникает необходимость разделить IP-адрес на эти две части: номер подсети и номер узла. Для разделения IP-адреса используют один из способов:

- использование фиксированной границы – (не нашел применения; весь адрес делится на две части фиксированной длины, в одной из них всегда размещается номер сети, в другой - номер узла);
- использование маски, которая позволяет максимально гибко установить границу между номером сети и номером узла;
- использование классов адресации (самый распространенный, компромисс между первым и вторым способом). Вводится 5 классов: A, B, C, D, E. Классы A, B и C - используют для адресации сетей; D, E - имеют специальное назначение. Для каждого класса определены границы между номером сети и номером узлов, таблица 1.

Таблица 1 – Диапазон адресов сетей и хостов классов A, B и C:

Класс	Диапазон номера сети	Диапазон номеров узлов	Изме

			няемые байты IP-адреса
A	1 – 126	0.0.1 – 255.255.254	N.*.*.*
B	128.0 – 191.255	0.1 – 255.254	N. N.*.*
C	192.0.0 – 223.255.255	1-254	N. N. N.*

Чтобы получить из IP-адреса номер сети и номер узла надо разбить адрес на две соответствующие части (см. таблицу 1) и дополнить каждую из них нулями до полных четырёх байт.

Пример: Дан IP-адрес класса **B**: 129.64.134.5.

Так как IP-адрес для класса **B** разбивается пополам, то номер сети равен **129.64**.0.0; номер узла равен 0.0.**134.5**.

Адресное пространство IP-протокола делится на три класса – **A**, **B**, **C**.

IP-адреса класса A

Сети класса A имеют 8-битный сетевой префикс «/8».

Структура адреса класса **A**:

0	1 2 3 … 7	8 … … 31
0		
Номер сети		Номер устройства

Максимальное число сетей класса **A** составляет $2^7 - 2 = 126$.

Каждая сеть класса **A** поддерживает до $2^{24} - 2 = 16\ 777\ 214$ сетевых устройств.

Адресное пространство, выделенное классу **A,** занимает 50 % общего адресного пространства сети Интернет. Диапазон сетевых адресов сетей класса **A** приведён ниже.

Класс адреса	Диапазон значений
A	**1.0.0.0—126.255.255.255**

IP-адреса класса B

Сети класса B имеют 16-битный сетевой префикс «/16».

Структура адреса класса **B**:

0 1	2 … …15	16… … 31
10		
Номер сети		Номер устройства

Максимальное число сетей класса **B** составляет $2^{14} = 16384$.

Каждая сеть класса **B** поддерживает до $2^{16} - 2 = 65\ 534$ сетевых устройств.

Адресное пространство, выделенное классу **B,** занимает 25 % общего адресного пространства сети Интернет. Диапазон сетевых адресов сетей класса **B** приведён ниже.

Класс адреса	Диапазон значений
B	**128.0.0.0 – 191.255.255.255**

IP-адреса класса C

Сети класса C имеют 24-битный сетевой префикс «/24».

Структура адреса класса **C**:

0 1 2	3 4 5 … 23	24… … 30 31

110		
Номер сети		Номер устройства

Максимальное число сетей класса **C** составляет 2^{21} = 2 097 152.

Каждая сеть класса **C** поддерживает до 2^8 - 2 = 254 сетевых устройств.

Адресное пространство, выделенное классу **C,** занимает 12,5 % общего адресного пространства сети Интернет. Диапазон сетевых адресов сетей класса **C** приведён ниже.

Класс адреса	Диапазон значений
C	**192.0.0.0—223.255.255.255**

Остальные IP-адреса

Оставшийся резерв IP-адресов отводится следующим классам сетей:

Класс адреса	Диапазон значений
D	**224.0.0.0—239.255.255.255**
E	**240.0.0.0—247.255.255.255**
Резерв	**248.0.0.0—254.255.255.255**

В сетях класса **D** первые (0..3) биты адреса имеют значение **1110**. Адреса этого класса используются для поддержки групповой передачи данных.

В сетях класса **E** первые (0..4) биты адреса имеют значение **11110**. Адреса этого класса зарезервированы для экспериментального использования.

Запись IP-адресов возможна в 2-ой, 16-ой, точечно-десятичной нотациях.

Примеры записи IP-адресов:

0111 1001	**1100 0100**	**1111 0100**	**1100 0110**
79	**C4**	**F4**	**C6**
121.196.244.198			
1001 1001	**1110 0110**	**1101 1010**	**1011 0111**
99	**E6**	**DA**	**B7**
153.230.218.183			
1101 1110	**0110 0101**	**0111 0101**	**1100 0110**
DE	**65**	**75**	**78**
222.101.117.120			

Задание

По заданному IP-адресу определить класс сети, номер сети и номер узла. Выполнить запись IP-адреса в 2-ой, 16-ой нотациях.

Вариант 1	Вариант 2	Вариант 3
1.100.120.148	164.180.220.250	121.196.244.198
192.90.120.148	212.200.220.250	190.196.244.198
128.100.120.148	98.180.220.250	223.194.244.198

Результаты оформить в отчете в виде таблицы:

Заданный IP-адрес	Класс сети	№ сети	№ узла	Нотация	
				2-ая	16-ричная

Контрольные вопросы:

1. Какова разрядность IP-адреса?

2. Какова структура IP-адреса?
3. На каком уровне эталонной модели OSI используется IP-адрес?
4. Что означает IP-адрес, состоящий из одних нулей?
5. В сети какого класса самое большое количество хостов?
6. IP-адрес является программным или аппаратным?
7. Как назначается IP-адрес?
8. В каких нотациях может быть представлен IP-адрес?

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 8

«Построение подсетей в локальной сети»

Цель: Ознакомиться с принципами разбиения локальной сети на подсети, изучить основы адресации в IPv4, маски подсетей и методы их расчета. Научиться правильно настраивать подсети для оптимизации работы сети и эффективного распределения IP-адресов.

Время выполнения: 4 часа.

Оборудование:

- Компьютер с ОС Windows/Linux.
- Сетевой коммутатор или маршрутизатор.
- Командная строка (cmd в Windows, Terminal в Linux).

Ход работы:

Теоретические сведения:

1. Что такое подсеть?

Подсеть — это часть IP-сети, разделенная с помощью маски подсети для оптимизации работы сети и управления трафиком.

2. Зачем нужны подсети?

Разграничение трафика и уменьшение нагрузки на сеть.
Повышение безопасности за счет разделения сетей.
Оптимизация использования IP-адресов.

3. IP-адресация и маска подсети

IP-адрес состоит из двух частей:

Сетевой идентификатор (определяет сеть).
Хостовый идентификатор (определяет устройство внутри сети).
Пример IP-адреса:

```
192.168.1.10 / 255.255.255.0
```

192.168.1 — это сеть.
.10 — это конкретный хост в сети.

4. Классы IP-адресов

Класс	Диапазон IP	Маска по умолчанию	Кол-во хостов
A	1.0.0.0 - 126.255.255.255	255.0.0.0	16 млн
B	128.0.0.0 - 191.255.255.255	255.255.0.0	65 тыс.
C	192.0.0.0 - 223.255.255.255	255.255.255.0	254

5. Разделение сети на подсети (субсетьинг)

При разделении сети изменяется маска подсети, что позволяет создать несколько логических сетей внутри одной физической.

Пример:

- Исходная сеть: 192.168.1.0/24 (маска 255.255.255.0)
- Разделение на 2 подсети:
  - 192.168.1.0/25 (маска 255.255.255.128)

- 192.168.1.128/25 (маска 255.255.255.128)

Задание:

1. Определение сетевой архитектуры

1. Выяснить, сколько устройств в сети.
2. Рассчитать, сколько подсетей требуется.

2. Разбиение сети на подсети

Допустим, у нас есть сеть 192.168.1.0/24, и нам нужно 4 подсети.

1. Используем формулу:

```mathematica
2^N ≥ количество подсетей
```

Для 4 подсетей: 2^2 = 4, значит, берем 2 бита из хостовой части.

2. Новая маска:

```scss
255.255.255.192 (/26)
```

Подсеть 1: 192.168.1.0/26 (диапазон: 192.168.1.1 - 192.168.1.62)
Подсеть 2: 192.168.1.64/26 (диапазон: 192.168.1.65 - 192.168.1.126)
Подсеть 3: 192.168.1.128/26 (диапазон: 192.168.1.129 - 192.168.1.190)
Подсеть 4: 192.168.1.192/26 (диапазон: 192.168.1.193 - 192.168.1.254)
3. Настройка IP-адресов на компьютерах
Открыть настройки сети:

Windows: Панель управления → Сеть и Интернет → Центр управления сетями и общим доступом → Изменение параметров адаптера.
Linux: nano /etc/network/interfaces или ip addr add.
Назначить IP-адреса вручную:
Компьютер 1 (подсеть 1):

```makefile
IP: 192.168.1.10
Маска: 255.255.255.192
Шлюз: 192.168.1.1
```

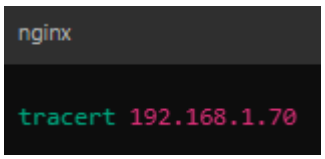
Компьютер 2 (подсеть 2):

```makefile
IP: 192.168.1.70
Маска: 255.255.255.192
Шлюз: 192.168.1.65
```

4. Проверка работоспособности сети
Проверить доступность узлов с помощью ping

```nginx
ping 192.168.1.70
```

Проверить маршруты с tracert (Windows) или traceroute (Linux)



Критерии оценивания
Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 9

«Настройка клиента службы DNS»

Цель: Получить сведения о настройке клиента службы DNS; научиться настраивать компьютер для разрешения имен при отсутствии DNS

Время выполнения: 2 часа.

- Оборудование: аппаратные: компьютер с установленной ОС Windows XP;
- программные: приложения ВМ: VirtualBox; виртуальные машины: VM-1;
- информационные: IP-адрес_1; IP-адрес_2; IP-адрес_3.

Ход работы:

Теоретические сведения:

*Система доменных имен (**Domain Name System, DNS**)* строится на основе распределенной базы данных, используемой в сетях **TCP/IP** для преобразования имен компьютеров в IP-адреса. ***Служба DNS*** облегчает идентификацию компьютеров и других ресурсов в сетях. Она обычно ассоциируется с Интернетом. Однако частные сети активно используют ее для определения имен компьютеров и идентификации компьютеров в локальной сети и Интернете.

*Пространство имен домена (**domain namespace**)* – система имен, которая обеспечивает иерархическую структуру для базы данных ***DNS***. Каждый узел называется *доменом (domain)* и представляет раздел базы данных ***DNS***.

База данных ***DNS*** индексирована по имени, поэтому каждый домен должен иметь имя. Имя домена идентифицирует его положение в иерархии. Поскольку домены добавляются в иерархию, имя родительского домена добавляется к дочернему домену, называемому *субдоменом (subdomain)*.

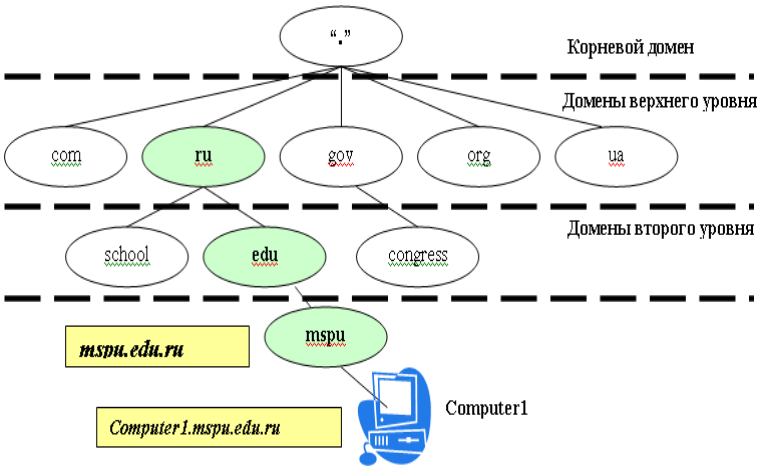


Рисунок 1. Пример образования иерархии пространства имен домена

Например, на рисунке 1 имя домена **mspu.edu.ru** идентифицирует этот домен **mspu** как субдомен домена **edu.ru**, а **edu** – как субдомен домена **ru**.

Иерархическая структура пространства имен домена состоит из *корневого домена, доменов верхнего уровня, доменов второго уровня и имен узлов*. *Корневой домен* располагается на самом верху иерархии и обозначается точкой. Корневой домен

Интернета управляется несколькими организациями, включая **Network Solutions, Inc**. *Домены верхнего уровня* – коды имени длиной два или три символа. Домены верхнего уровня сгруппированы по типу организации или географическому положению. Например:

Домен верхнего уровня	***Описание принадлежности***
gov	Правительственные организации
com	Коммерческие организации
edu	Образовательные учреждения
org	Некоммерческие организации
ru	Код России

Таблица 1. Назначение доментов верхнего уровня

Домены верхнего уровня содержат *домены второго уровня* и *имена узлов (компьютеров)*. Организации типа **Network Solutions, Inc.** назначают и регистрируют домены Интернета второго уровня для частных лиц и организаций. *Имя второго уровня* имеет две части: имя верхнего уровня и уникальное имя второго уровня. *Имена узлов* относятся к определенным компьютерам в Интернете или частной сети.

На рисунке 1 ***Computer1*** – это имя узла - левая часть полного доменного имени, которое определяет точное местонахождение узла в иерархии домена. Тогда полное доменное имя (включая последнюю точку) запишется как ***Computer1.mspu.edu.ru***.

Чтобы преобразовать имя узла в IP-адрес, служба ***DNS*** использует полное доменное имя узла. *Разрешение имен* – процесс преобразования имен узлов в IP-адреса. Он напоминает поиск имени в телефонном справочнике, где каждому имени соответствует номер телефона. Например, имя ***www.mspu.edu.ru*** используется при соединении с Web-узлом Мурманского государственного педагогического университета. ***DNS*** находит соответствующий этому (**www.mspu.edu.ru**) имени IP-адрес. Проекции имен на адреса IP хранятся в распределенной базе данных службы ***DNS***.

Серверы ***DNS*** осуществляют поиск соответствия в обе стороны. Прямой запрос преобразовывает имя в IP-адрес, а обратный запрос находит имя для IP-адреса. Сервер ***DNS*** имеет право делать запрос только для зоны, для которой он имеет полномочия. Если сервер ***DNS*** не может сделать запрос, он передает запрос на другие серверы имен, имеющие соответствующие полномочия.

Для разрешения имен служба ***DNS*** использует *модель «клиент-сервер»*. Чтобы осуществить прямой запрос соответствия, клиент передает запрос на локальный сервер имен. Локальный сервер ***DNS*** или обрабатывает и находит IP-адрес или делает запрос на разрешение имени на другой сервер имен.

На рисунке 2 показан клиент, запрашивающий IP-адрес для символьного адреса **www.mspu.edu.ru** с сервера имен.

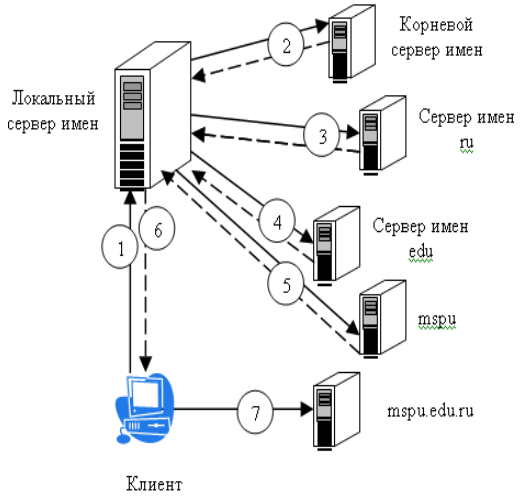


Рисунок 2. Процесс разрешения адреса

Процесс строится следующим образом:

- клиент передает прямой запрос для **www.mspu.edu.ru** на свой локальный сервер имен;
- локальный сервер имен проверяет свои файлы данных зоны, чтобы определить, содержит ли тот проекцию имени на IP-адрес для запроса клиента и т.к. локальный сервер доменных имен не имеет полномочий для домена **mspu.edu.ru**, поэтому передает запрос на один из корневых серверов ***DNS***, требуя разрешения имени узла, а корневой сервер доменных имен отправляет назад ссылку на серверы имен **ru**;
- локальный сервер имен посылает запрос на сервер имен **ru**, который отвечает ссылкой на серверы имен **edu**;
- локальный сервер имен посылает запрос на сервер имен **edu**, который отсылает клиенту ссылку на сервер имен **mspu**;
- локальный сервер имен посылает запрос на сервер имен **mspu** и, поскольку сервер имен **mspu** имеет полномочия для той части пространства имен домена, то при получении запроса отсылает адрес для **www.mspu.edu.ru** на локальный сервер имен;
- сервер имен отправляет IP-адрес для символьного адреса **www.mspu.edu.ru** клиенту и поскольку разрешение имени выполнено, то клиент может обратиться к адресу **www.mspu.edu.ru**;
- клиент обращается к символьному адресу **www.mspu.edu.ru**.

Задание 1. Настройте клиентскую часть DNS.

1. Запустите виртуальную машину **VM-1** и загрузите ОС **Windows**.
2. Откройте окно **Сетевые подключения**.
3. Вызовите свойства **Подключения по локальной сети (*контекстное меню/Свойства*)**.
4. Вызовите свойства **Протокол Интернета TCP/IP**.
5. Установите адреса ***DNS*** серверов:
   - установите переключатель *Использовать следующие адреса DNS-серверов*;
   - в поле **Предпочитаемый DNS-сервер** введите *<IP-адрес_1>*;
   - в поле **Альтернативный DNS-сервер** ведите *<IP-адрес_2>*.
6. Добавьте 3-й DNS сервер. Для этого:

- щелкните ***Дополнительно***;
- перейдите на вкладку ***DNS***;
- щелкните ***Добавить*** в разделе **Адреса DNS-серверов**;
- введите *<IP-адрес_3>* сервера имен и закройте окно кнопкой ***OK***.

7. Закройте диалоговое окно **Свойства: Протокол Интернета TCP/IP** кнопкой ***OK***.
8. Закройте окно свойств локального подключения.
9. Закройте окно **Сетевые подключения**.
10. Проверьте настройки. Для этого с помощью команды **ping** отправьте эхо-запросы не на IP адрес другого компьютера, а на его символьный адрес, например **edc**.

Задание 2. Настройте компьютер для разрешения имен при отсутствии DNS-сервера.

1. Соберите информацию об адресах компьютеров в кабинете (символьные адреса и IP-адреса). Для этого воспользуйтесь командой **ping**.
2. Откройте файл ***hosts (c:\WINDOWS\system32\drivers\etc\hosts)***.
3. Внесите в этот файл собранную информацию о первом компьютере в кабинете, например: **Computer_1 - 172.21.5.32**
4. Аналогично внесите информацию об остальных компьютерах.
5. Проверьте внесенные изменения:
   - удалите в настройках **Подключения по локальной сети** все записи ***DNS*** серверов;
   - отправьте эхо-запрос на какой-нибудь компьютер по его символьному адресу (если будет получен ответ, то настройки верны).

Критерии оценивания
Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 10

«Настройка параметров безопасности»

Цель: Научиться настраивать параметры безопасности в современных Интернет браузерах.

Время выполнения: 4 часа.

- Оборудование: аппаратные: компьютер
- программные: ОС Windows XP или Windows 2000; браузеры: Internet Explorer; Firefox, Opera.

Ход работы:

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 1.

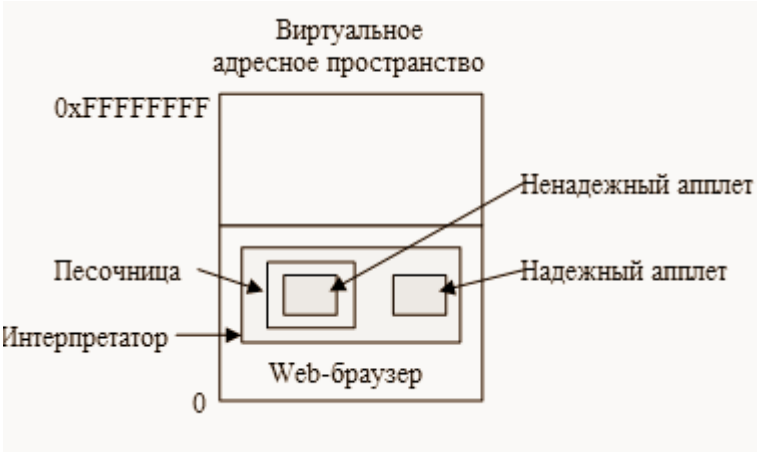


Рисунок 1. Обработка апплетов браузером

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 в данном случае сводится к вопросу о том, 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 сначала 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, в противном случае 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 метода 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 части. 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.

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*;
6. Отключите *Использование элементов ActiveX не помеченных как безопасные*;
7. Отключите загрузку *Неподписанных элементов ActiveX*;
8. Примените параметры кнопкой ***OK***;
9. Установите параметры конфиденциальности:
    - перейдите на вкладку **Конфиденциальность**;
    - установите регулятор на уровень *Умеренно высокий*;
    - разрешите загружать файлы ***cookie*** с узла **www.mail.ru**:
        - щелкните по кнопке ***Узлы***;
        - введите в поле *www.mail.ru* и щелкните по кнопке ***Разрешить***;
    - аналогично разрешите загружать cookie со следующих узлов: **www.yandex.ru, www.pochta.ru**;
    - примените параметры кнопкой ***OK***;
10. 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 ***OK***.
    - перейдите на вкладку **Оценки** и установите уровни **Службы оценки 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**.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 11

«Маршрутизация пакетов в IP сетях»

Цель: Получить представление о работе IP маршрутизатора, попрактиковаться в составлении таблиц маршрутизации и работе протоколов внутренней маршуртизации. Дополнительной целью работы является приобретение опыта работы в средах виртуализации.

Время выполнения: 4 часа.

Оборудование: Семь компьютеров, объединенных локальной сетью. Установление на них программа VMWare Workstation и сташе. Виртуальные машины Windows 2003 Server и Windows XP.

Ход работы:

Теоретические сведения:

1. Маршрутизаторы (аппаратные или программные) выполняют задачу выбора оптимального маршрута следования IP пакета и его отправки по этому маршруту. Для принятия решения анализируется адрес получателя и устанавливается маршрут следования на основе неких формализованных записей о структуре составной сети. Эти записи называются таблицами маршрутизации.
2. В таблице маршутизации присутствуют как минимум следующие поля: адрес назначения (адрес IP-сети или IP адрес хоста), идентификатор порта, через который пакет идет до сети назначения (порт обозначается IP-адресом или внутренним номером), шлюз (IP адрес на который необходимо пойти после того как пакет покинет порт), метрика (показатель качества маршрута).
3. На каждом маршрутизаторе сети присутствует таблица полностью описывающая структуру всей сети и, иногда, содержащая записи о маршрутах по умолчанию.
4. Таблицы маршрутизации составляются вручную или с помощью протоколов маршрутизации, автоматизирующих этот процесс. Одним из таких протоколов является протокол RIP2.
5. В работе используется пакет виртуализации VMWare. Принцип его работы заключается в программной эмуляции в рамках основной операционной системы аппаратной среды выполнения для гостевой операционной системы. Такой подход позволяет запускать операционные системы в выделенной виртуальной машине, программные интерфейсы которой перехватывают обращение гостевой ОС к аппаратуре и передающей их реальным устройствам от имени основной ОС. В работе такой подход позволяет безболезненно развернуть серверную ОС на компьютере без угрозы штатной операционной системе.

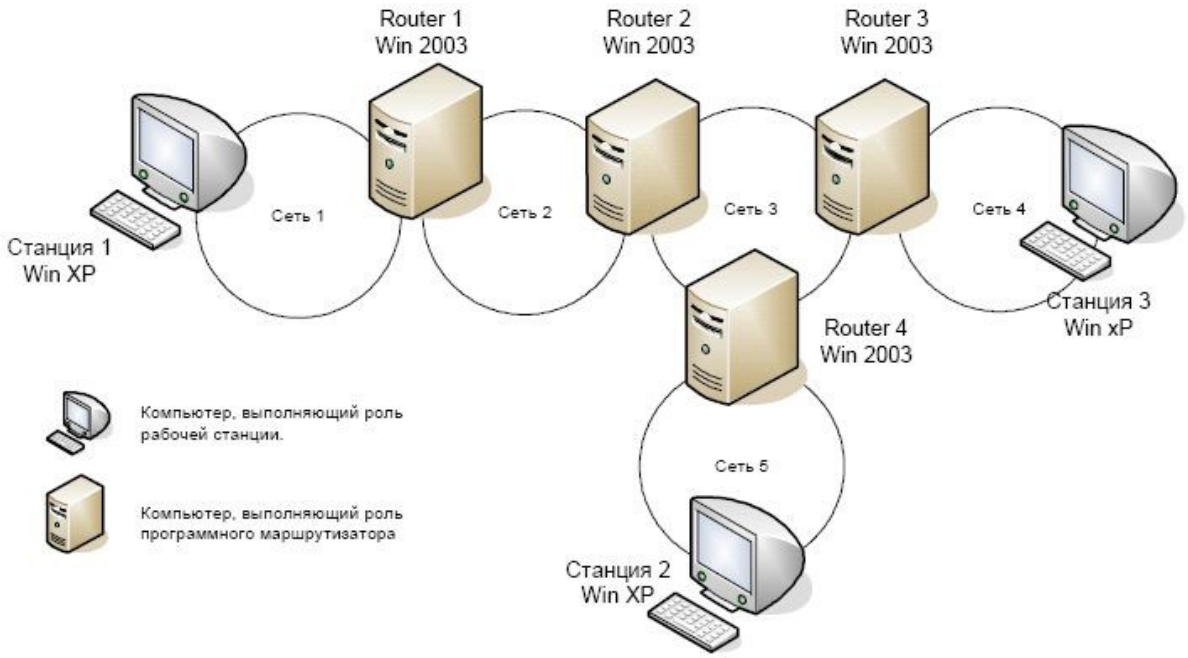


Рис 1.

Задание:

В нашей сети 7 компьютеров. Три рабочих станции и четыре маршуртизатора. В качестве этих компьютеров будут выступать гостевые операционные системы. Рабочие станции будут работать под windows XP, а программные маршрутизаторы под управлением Windows 2003 (XP не поддерживает программную маршрутизацию). Как было сказано в разделе «Необходимо» работа выполняется с некой условностью. Все компьютеры будут подключены к одной локальной сети, а в ней организуются изолированные по адресам IP сети. Одновременная работа одного сетевого интерфейса в разных IP сетях достигается назначением двух и более IP адресов одному сетевому интерфейсу (Свойства сетевого соединения Свойства TCP\IP \ Дополнительно).

2. На первом этапе вам необходимо составить план сети (заранее выбрать IP-адреса для сетей, рабочих станций и портов маршрутизаторов). Определить на каком компьютере будет запущен какой виртуальный компьютер. Выбрать уникальное имя для каждого виртуального компьютера.
3. Установить при необходимости программу VMWare. В ней запустить необходимую виртуальную машину из папки C:\VM
4. В виртуальной операционной системе:

- поменять MAC адрес сетевой платы на новый уникальный (Свойства сетевого соединения \ Настройка сетевого адаптера \ Сетевой адрес). Делать это необходимо из-за того что виртуальные машины созданы из одной копии, и, следовательно, обладают идентичными MAC адресами, что приводит к неправильной работе коммутатора локальной сети.
- Изменить имя компьютера (панель управления \ свойства системы \ имя)
- Установить все необходимые IP адреса.

На рабочих станциях необходимо указывать шлюз по умолчанию – IP адрес порта маршрутизатора из IP сети.

На маршрутизаторах делать этого не следует – маршрута по умолчанию нет. Адреса DNS остаются пустыми.

5. обязательно с помощью команды PING проверить видимость ближайших соседей по локальной сети.
6. На маршрутизаторах запустите службу Routing and Remote Access (Панель управления \ Администрирование \ Routing and Remote Access). С помощью мастера сконфигурируйте службу как LAN Router.
7. С помощью консольной команды ROUTE изучите таблицу маршрутизации по умолчанию.
8. С помощью консольной команды ROUTE (рекомендуемый способ) или с помощью графической консоли службы Routing and Remote Access дополните таблицу необходимыми записями.
9. С помощью команды ping проверьте достижимость рабочих станций друг с друга, а с использованием команд tracert и pathping проверьте путь следования IP пакетов.
10. Сохраните таблицы маршрутизации в текстовом файле.
11. Удалите созданные в ручную записи в таблицах маршрутизации. Убедитесь, что рабочие станции перестали «видеть друг-друга».
12. Добавьте в консоли службы Routing and Remote Access добавьте на маршрутизаторах протокол RIP2 (General \ Add new routing protocol). В нем добавьте интерфейс, через который будет происходить обмен векторами маршрутизации. Установите интервал обмена 60 секунд.
13. обновляя консоль убедитесь что пошли рассылки таблицы. После получения чужих таблиц выведите таблицу динамической маршрутизации (IP-routing \ Routing tables)
14. после того, как будут получены все необходимые записи с помощью команды ping проверьте достижимость рабочих станций друг с друга, а с использованием команд tracert и pathping проверьте путь следования IP пакетов.

15) отключите службу Routing and Remote Access, установите автоматическое получение

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 12

«Настройка DHCP-сервера»

Цель: Изучение особенностей установки и управления DHCP-сервером в сетях Windows

.

Время выполнения: 4 часа.

- Оборудование:
- аппаратные: ПК;
- программные: установленная ОС Windows 7, Windows 10**Ход работы:**

Теоретические сведения:

DHCP (Dynamic Host Configuration Protocol) – это протокол, позволяющий компьютерам динамически получать ip адреса и другие сетевые параметры.

Для работы протокола DHCP требуется сервер и клиент.

DHCP сервер – это сервер который раздает IP-адреса и параметры компьютерам в сети, соответственно на нем и задаются настройки раздачи IP-адресов и сетевых параметров.

DHCP клиент – это приложение, установленное на клиентских компьютерах, которое обращается к DHCP серверу для получения IP-адреса и соответствующих параметров. Во всех операционных системах по умолчанию установлен клиент DHCP, например - в Windows он выглядит в виде службы с логичным названием DHCP-клиент.

DHCP доступен как для IPv4 (DHCPv4) (версии 4), так и для IPv6 (DHCPv6) (версии 6).

Каждому устройству, подключенному к сети, нужен уникальный IP-адрес. Сетевые администраторы назначают статические IP-адреса маршрутизаторам, серверам, принтерам и другим сетевым устройствам, местоположение которых (физическое и логическое) вряд ли изменится. Обычно это устройства, предоставляющие услуги пользователям и устройствам в сети, поэтому назначенные им адреса должны оставаться постоянными. Кроме того, статические адреса позволяют администраторам удаленно управлять этими устройствами – до них проще получить доступ к устройству, когда они могут легко определить его IP- адрес.

Однако компьютеры и пользователи в организации часто меняют места, физически и логически. Это может быть сложно и долго назначать новые IP-адреса каждый раз, когда сотрудник перемещается. А для мобильных сотрудников, работающих из удаленных мест, вручную настройка правильных параметров сети может быть весьма непростой задачей.

Использование DHCP в локальной сети упрощает назначение IP-адресов как на настольных, так и на мобильных устройствах. Использование централизованного DHCP-сервера позволяет администрировать все назначения динамических IP-адресов с одного сервера. Эта практика делает управление IP-адресами более эффективным и обеспечивает согласованность внутри организации, включая филиалы.

DHCPv4 динамически назначает адреса IPv4 и другую информацию о конфигурации сети. Отдельный сервер DHCPv4 является масштабируемым и относительно простым в управлении. Однако в небольшом офисе маршрутизатор может быть настроен для предоставления услуг DHCP без необходимости выделенного сервера.

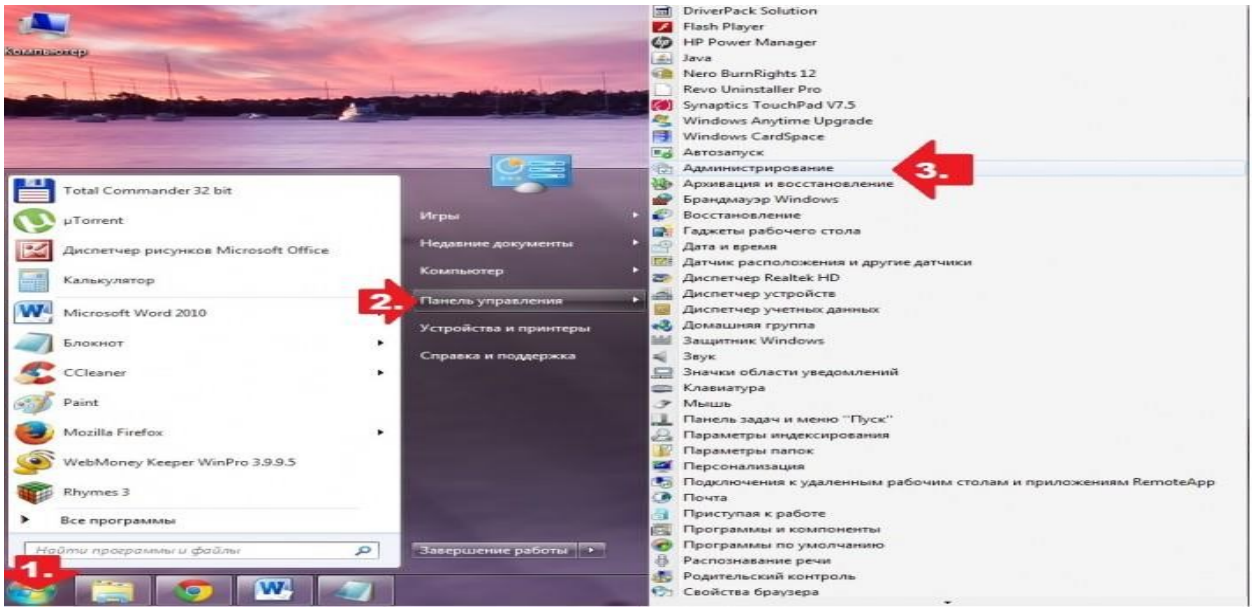
Перед тем, для подключения компьютера к интернету через сеть TCP/IP, предварительно необходимо настроить сетевой протокол DHCP. Именно он отвечает за то, чтобы ПК автоматически получил IP-адрес и прочие необходимые параметры для полноценного пользования интернетом. По умолчанию такой протокол в системе Windows активизируется автоматически. Правда, срабатывает он не всегда. В этом случае приходится думать над тем, как вручную включить DHCP в ОС Windows 7. А сделать это на самом деле несложно.

Задание:

1. В практической части необходимо выполнить установку и настройку DHCP-сервера способом – через опцию «Службы». Отталкиваясь от модели действия DHCP «клиент – сервер», включить этот сетевой протокол в Windows 7 можно через сервис «Службы».

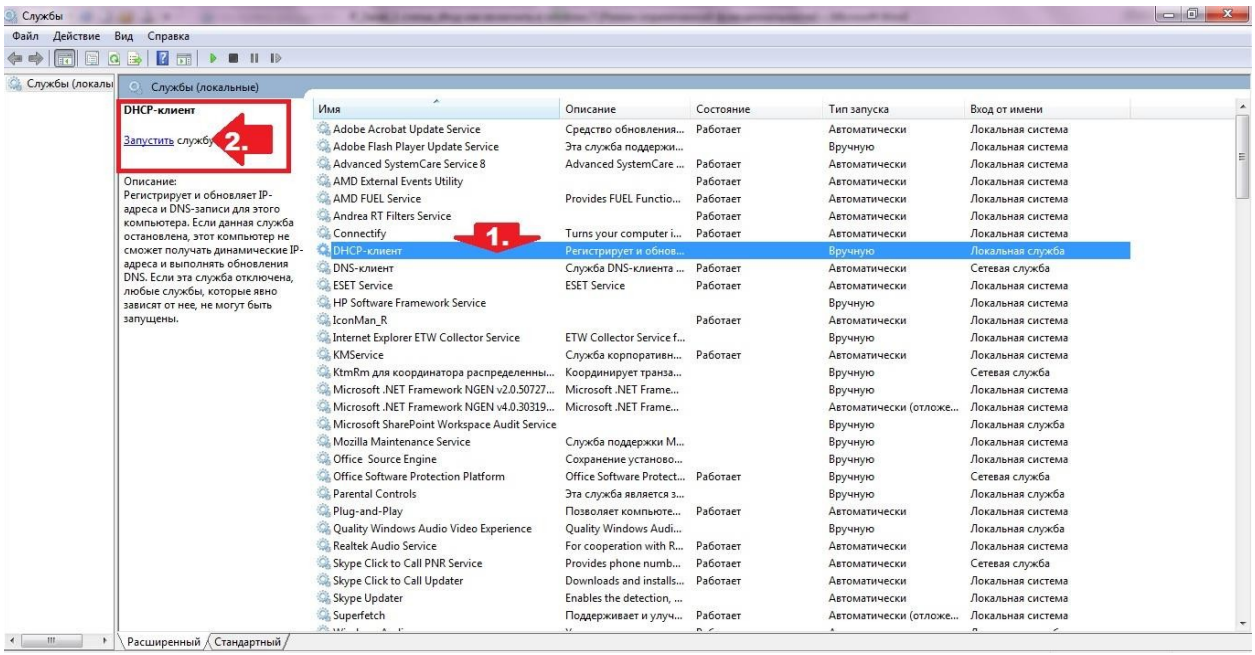
Используется следующий порядок:

2. Необходимо войти в меню «Пуск», перейти в раздел «Панель управления», а в нем выбрать вкладку «Администрирование»:



Панель управления - Администрирование

3. Далее в открывшемся списке находим и кликаем пункт «Службы», чтобы появилось окошко соответствующего сервиса. После того как оно открылось, ищем в нем службу DHCP-клиент и запускаем ее нажатием соответствующей кнопки в меню слева:



Запуск DHCP-клиента

4. Следующий шаг – проверяем тип запуска службы. В идеале запускаться она должна автоматически. Если это не так, кликаем правой кнопкой мышки по пункту DHCP-клиент, выбираем в появившемся меню вкладку «Свойства», выставляем автоматический тип запуска и сохраняем настройки нажатием кнопки ОК:

5. Установка автоматического типа запуска

В результате таких действий сетевой протокол в OS Windows 7 будет срабатывать автоматически, не требуя дополнительных настроек.

Контрольные вопросы

1. Дайте определение DHCP.

2. Что собой представляет DHCP-сервер, в чем его функции?

3. Дайте определение DHCP-клиента.

4. В чем преимущества использования DHCP?

5. Для чего необходима настройка DHCP в сети?

Содержание отчета

1. Наименование и цель лабораторной работы

2. Скриншоты выполнения лабораторной работы в соответствии с порядком выполнения практической части работы.

3. Выводы по лабораторной работе.

4. Ответы на контрольные вопросы.

Критерии оценивания
Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 13

«Настройка DNS-сервера»

Цель: Ознакомиться с принципами работы DNS (Domain Name System), изучить назначение и функции DNS-сервера. Научиться устанавливать, настраивать и проверять работу DNS-сервера для преобразования доменных имен в IP-адреса в локальной сети.

Время выполнения: 4 часа.

Ход работы:

Задание:

На этой странице мы выбираем из списка DNS-сервер и нажимаем кнопку "Далее". Появится страница "Сводка выбранных параметров", представленная на рисунке 58, на которой можно просмотреть и подтвердить выбранные параметры.

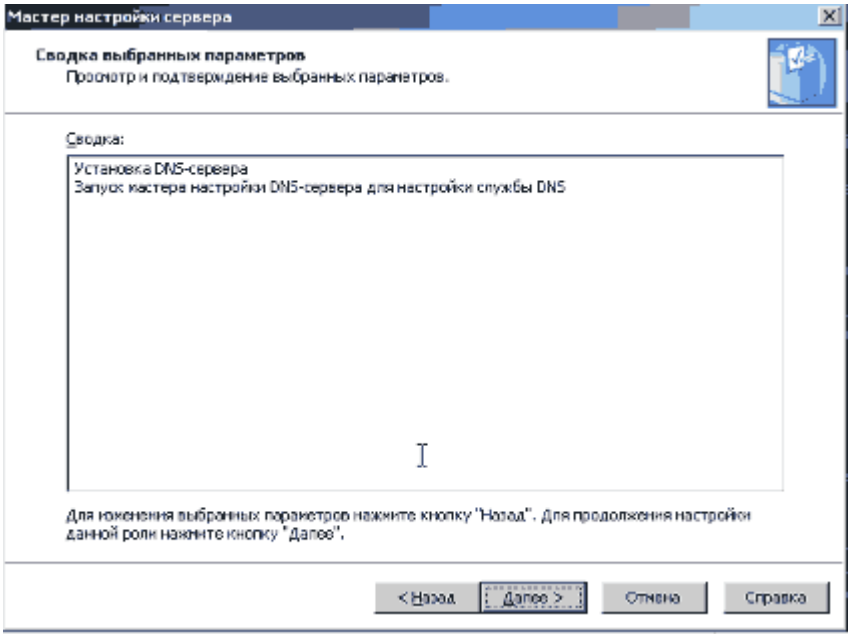


Рис. 58. Сводка выбранных параметров

Для применения параметров, выбранных на странице "Сводка выбранных параметров", нажимаем кнопку "Далее". Появится страница "Применение выбранных параметров" (рис. 59), которая будет находиться на экране всё время до окончания установки и настройки DNS-сервера.

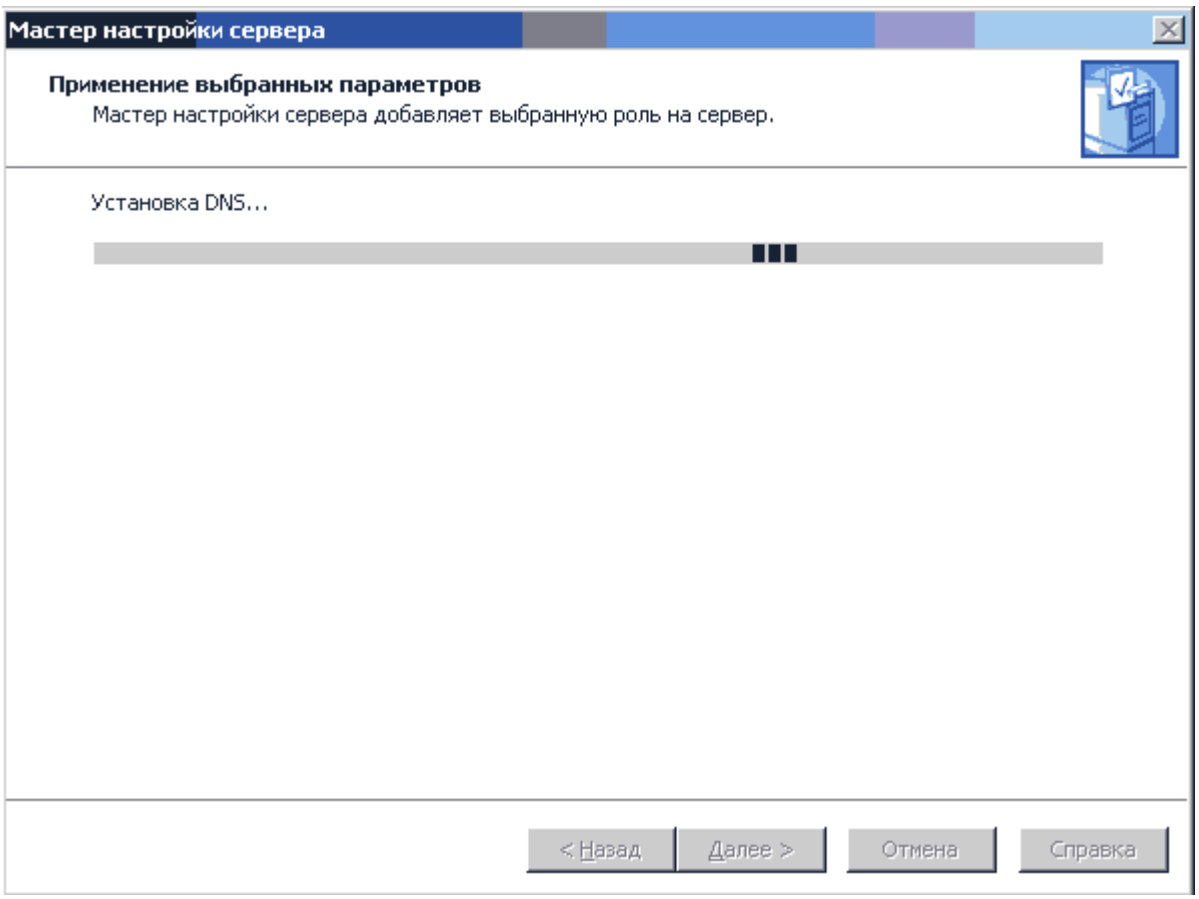


Рис. 59. Применение выбранных параметров

Мастер настройки сервера установит службу DNS-сервер. В процессе установки службы DNS-сервера мастер настройки сервера определяет, является ли IP-адрес для этого сервера статическим или настраивается автоматически. Клиенты DNS находят DNS-серверы при помощи автоматически настраиваемых статических IP-адресов. Это может создавать трудности для клиентов DNS при изменении IP-адресов.

Если этот сервер настроен для автоматического получения IP-адреса, то появляется окно "Настройка компонентов" мастера компонентов Windows и предлагает настроить этот сервер для использования статического IP-адреса.

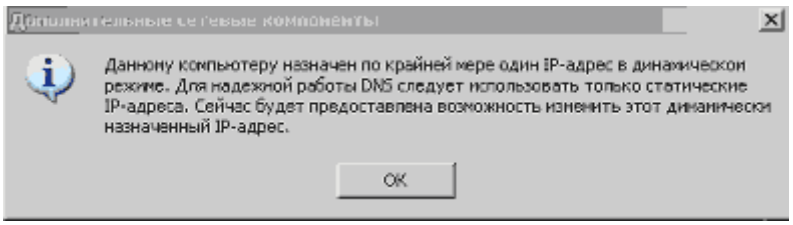


Рис. 60. Дополнительные сетевые компоненты

На странице "Подключение по локальной сети - свойства" (рис. 61) мы выбираем вариант "Протокол Интернета (TCP/IP)" и нажимаем кнопку "Свойства" (или дважды щелкаем по нему левой кнопкой мыши).

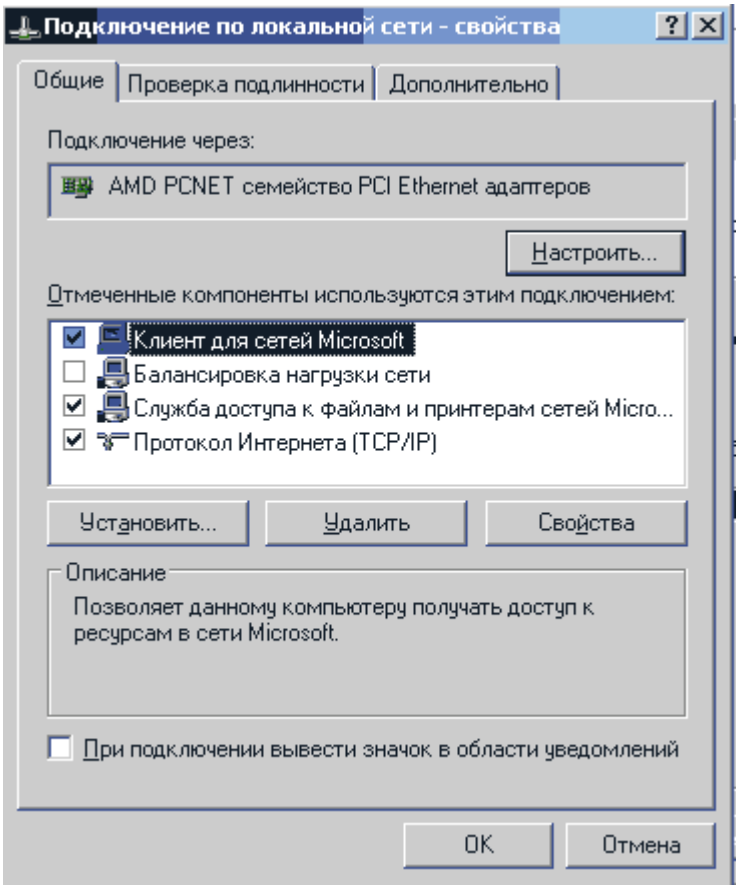


Рис. 61. Подключение по локальной сети - свойства

В диалоговом окне "Свойства: Протокол Интернета (TCP/IP)" (рис. 62) выбираем "Использовать следующий IP-адрес" и вводим статический IP-адрес, маску подсети и основной шлюз для этого сервера:

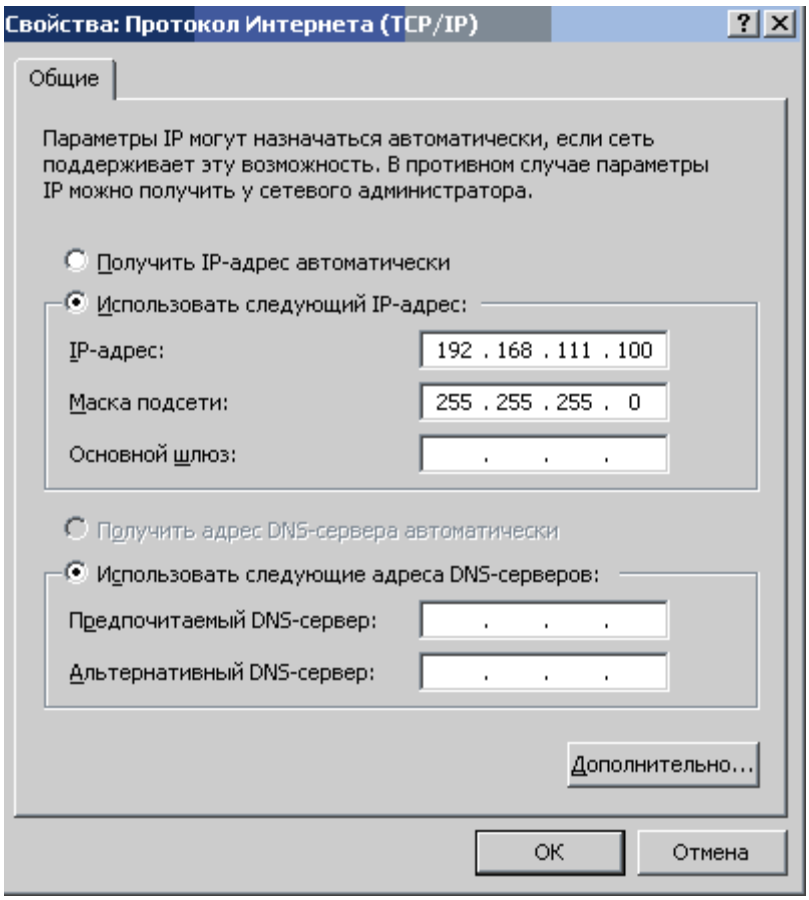


Рис. 62. Свойства: Протокол Интернета (TCP/IP)

В строке "Предпочитаемый DNS-сервер" вводим IP-адрес этого сервера, а в строке "Дополнительный DNS-сервер" - IP-адрес DNS-сервера, находящегося в центральном офисе или у поставщика услуг Интернета. После настройки статических IP-адресов для DNS-сервера нужно нажать кнопку OK, а затем - кнопку "Закрыть".

Для небольшой организации статический IP-адрес сервера будет использоваться для регистрации DNS-имени домена авторизованным регистратором Интернета. Регистратор Интернета сопоставит DNS-имя домена организации с IP-адресом, и компьютерам в Интернете при поиске компьютеров из сети организации будет известен IP-адрес DNS-сервера этой сети.

Для подразделения статический IP-адрес сервера будет использоваться при делегировании имени домена, настроенного на DNS-сервере в центральном офисе организации. Компьютеры в организации и в Интернете при поиске компьютеров из сети будут использовать IP-адрес DNS-сервера этой сети. Поэтому очень важно не изменять IP-адрес этого сервера после добавления роли DNS-сервера.

После нажатия кнопки "Закрыть" запускается "Мастер настройки DNS-сервера", представленный на рисунке 63.

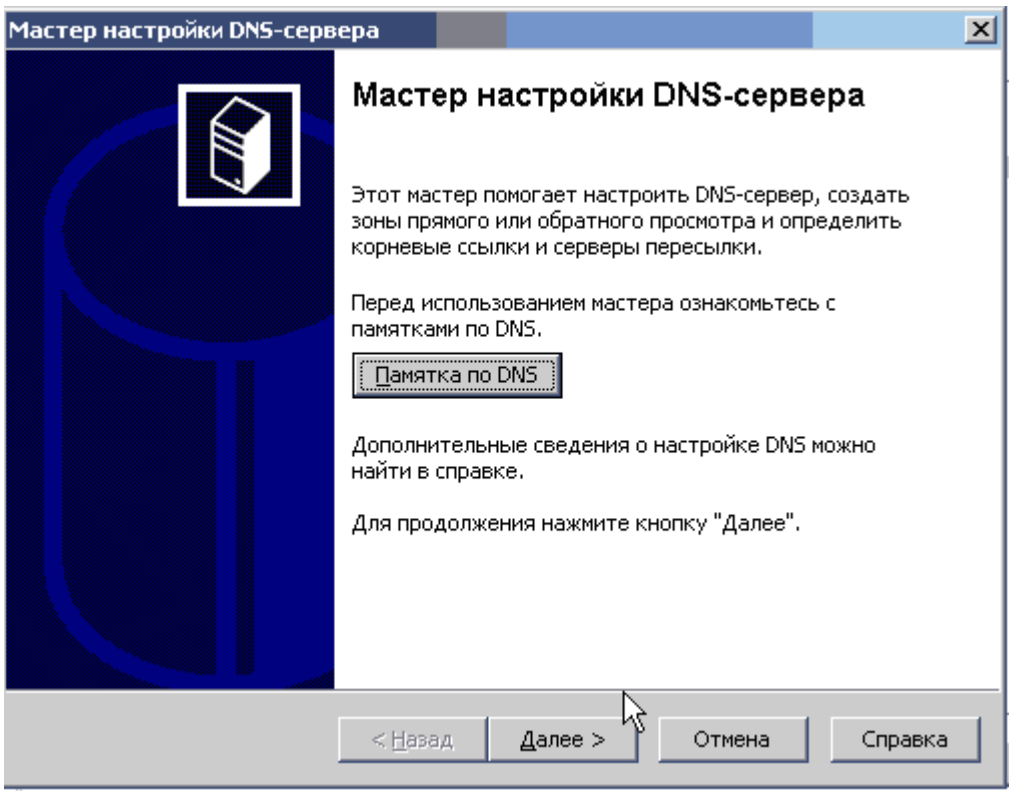


Рис. 63. Мастер настройки DNS-сервера

Если отменить работу мастера настройки DNS-сервера, служба DNS-сервера останется установленной, но не сможет рассылать клиентам IP-адреса, пока не будет создана область. Создать область позже можно при помощи консоли DNS. Для продолжения нужно нажать "Далее".

На странице "Выбор действия по настройке" (рис. 64) выбираем вариант "Создать зону прямого просмотра" и нажимаем кнопку "Далее".

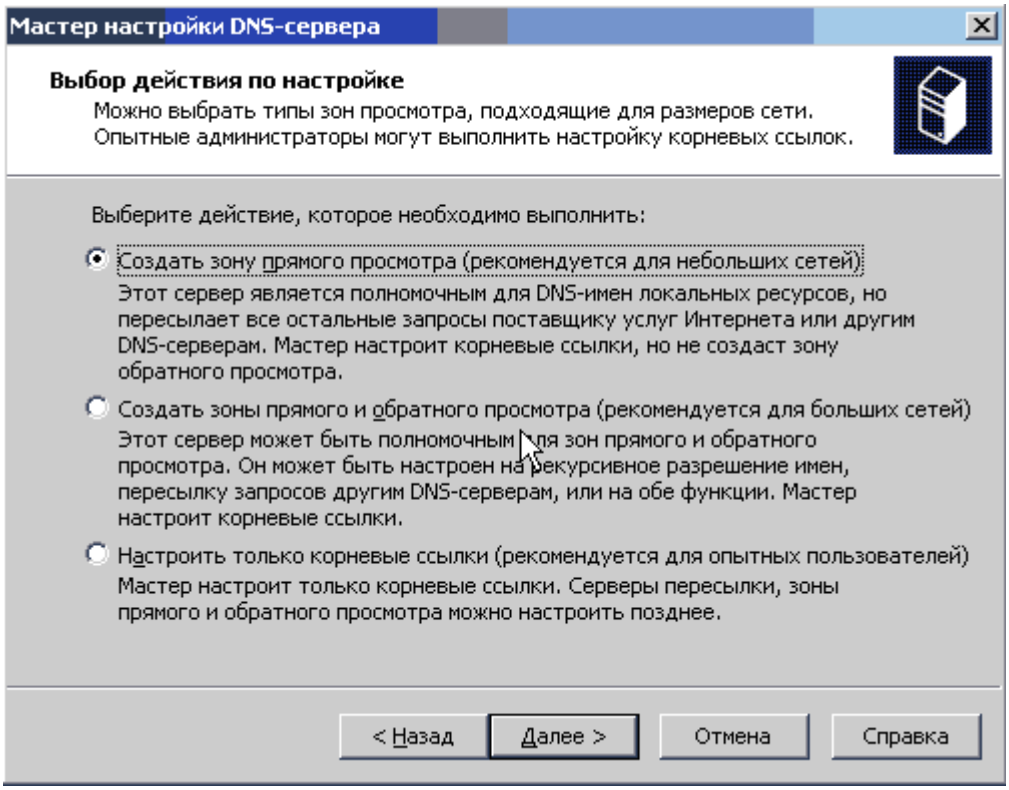


Рис. 64. Выбор действия по настройке

Чтобы задать, что этот DNS-сервер будет содержать зону DNS, в которую входят записи ресурсов DNS для ресурсов сети, на странице "Размещение основного сервера" мы выбираем "Управление зоной выполняется этим сервером" и нажимаем кнопку "Далее" (рис. 65).

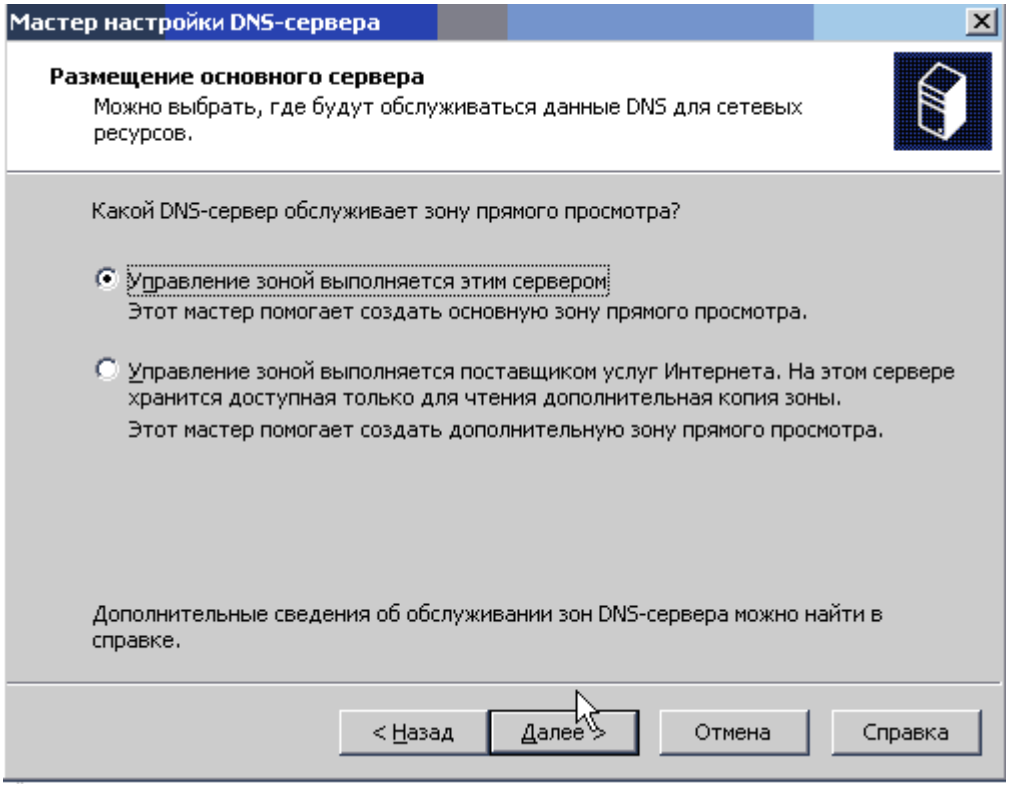


Рис. 65. Размещение основного сервера

На странице "Имя зоны" (рис. 66) в строке "Имя зоны" задаём имя зоны DNS для сети и нажимаем кнопку "Далее".

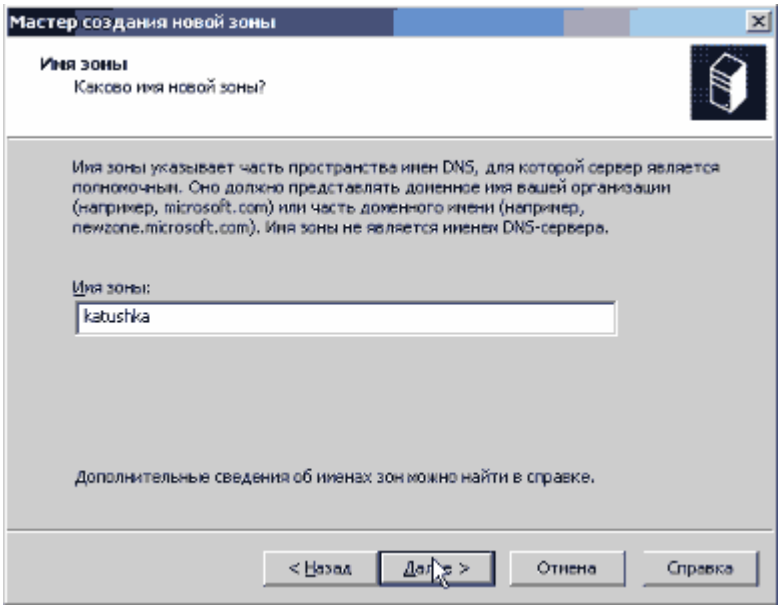


Рис. 66. Задаем имя зоны

Имя зоны совпадает с именем DNS-домена для небольшой организации или подразделения.

На странице "Файл зоны" (рис. 67) будет предложено создать новый файл зоны или скопировать существующий с другого DNS-сервера.

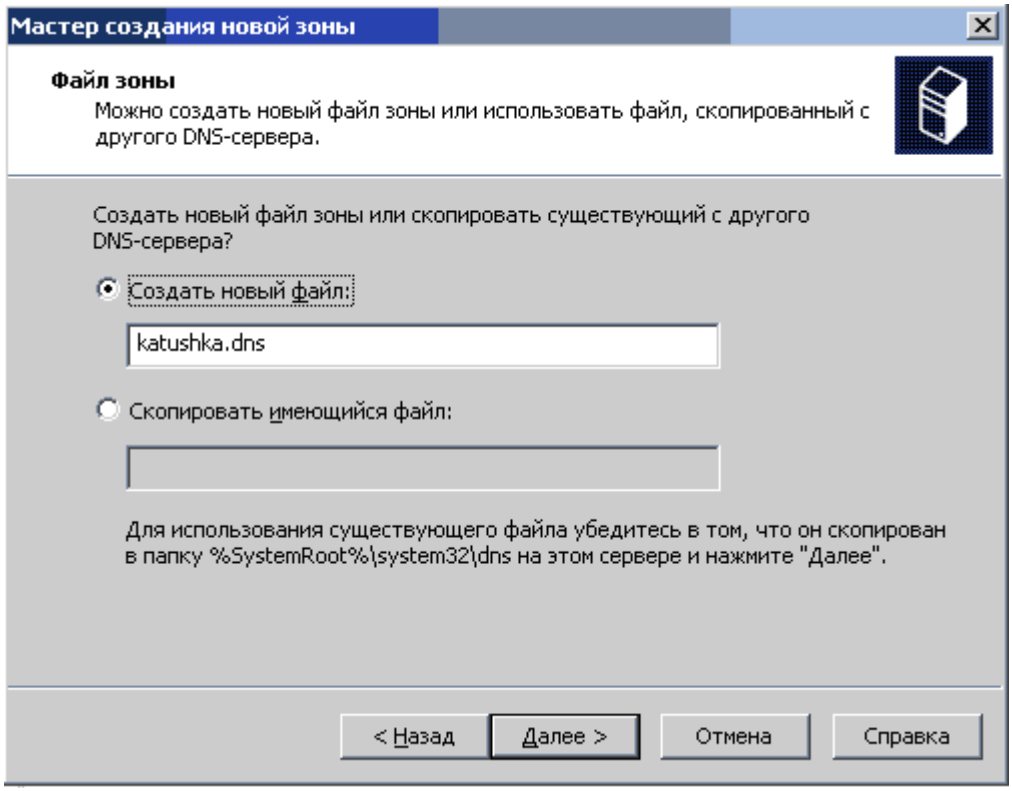


Рис. 67. Файл зоны

Выбираем "Создать новый файл" и нажимаем "Далее".

На странице "Динамическое обновление" (рис. 68) можно определить, будет ли данный DNS-сервер принимать динамические обновления. Если выбрать вариант "Разрешить любые динамические обновления", можно автоматизировать процесс обновления записей ресурсов DNS для ресурсов сети, но этот вариант опасен, так как обновления могут быть получены от источников, не заслуживающих доверия. Мы выбираем "Запретить динамическое обновление" и нажимаем "Далее".

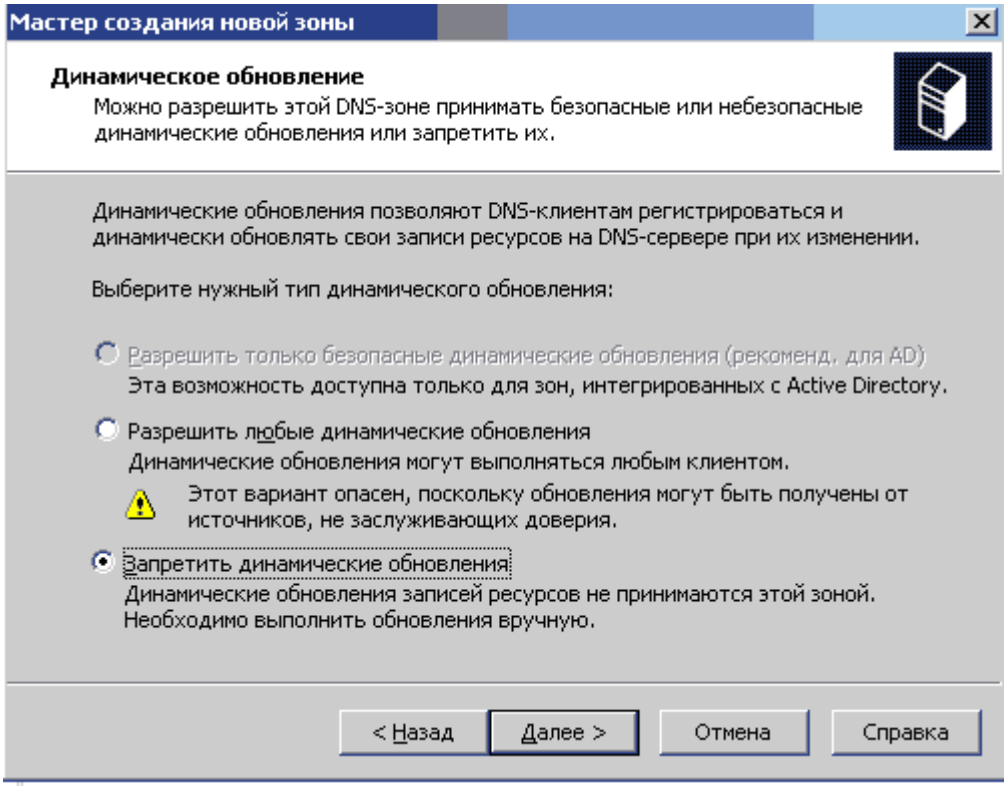


Рис. 68. Динамическое обновление

На странице "Серверы пересылки", представленной на рисунке 69, будет предложено указать IP-адреса DNS-серверов, которым данный DNS-сервер будет пересылать запросы, на которые он сам не в состоянии ответить.

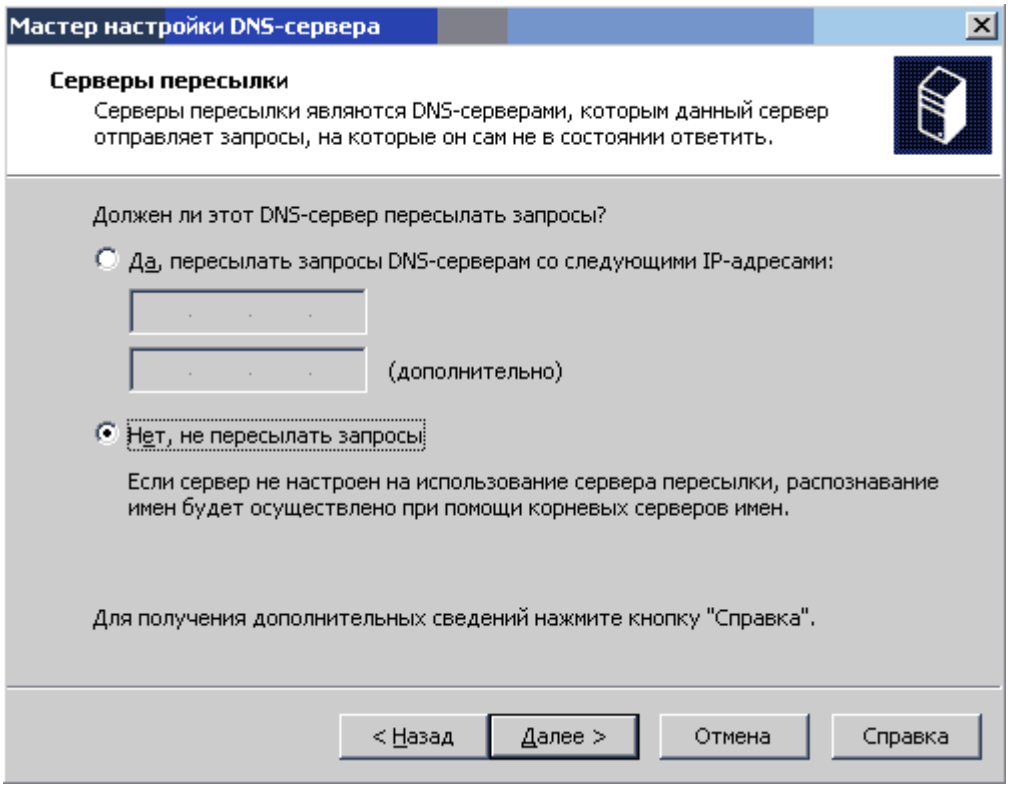


Рис. 69. Серверы пересылки

Выбор конфигурации позволит пересылать запросы DNS для DNS-имен вне сети на DNS-сервер центрального офиса или поставщика услуг Интернета. Введите один или несколько IP-адресов, используемых DNS-серверами центрального офиса или поставщика услуг Интернета. Мы выбираем "Нет, не пересылать запросы" и нажимаем "Далее". Мастер настройки DNS-сервера осуществит поиск корневых ссылок и выведет на экран страницу "Завершение работы мастера настройки DNS-сервера" (рис. 70).

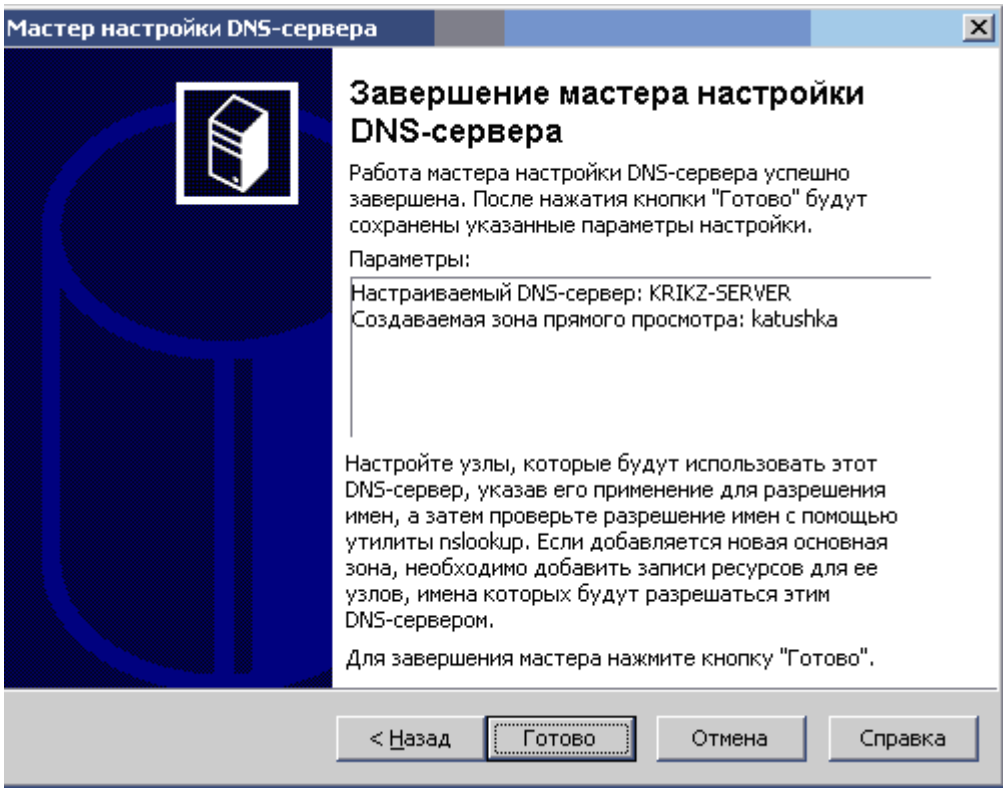


Рис. 70. Завершение работы мастера настройки DNS-сервера

На этой странице можно нажать кнопку "Назад" для изменения любого параметра. Для применения выбранных нами параметров нажимаем кнопку "Готово". После завершения работы мастера настройки DNS-сервера на экране будет отображена страница "Этот сервер теперь является DNS-сервером" (рис. 71).

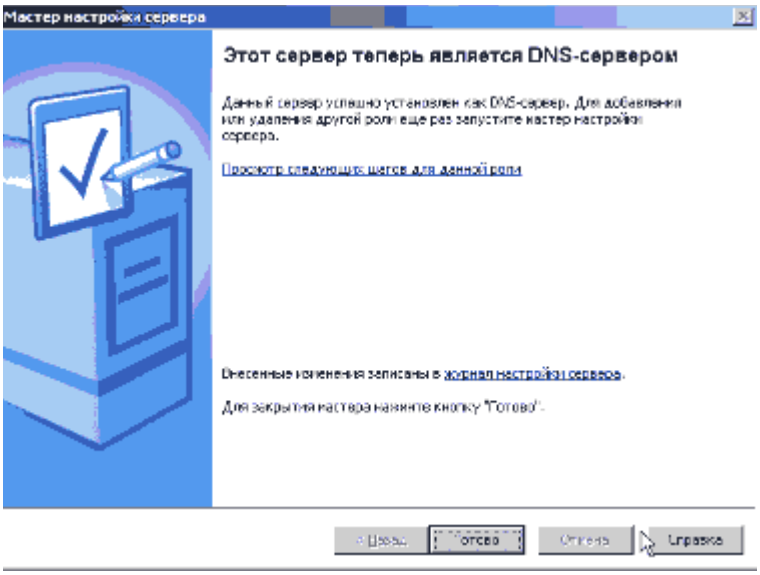


Рис. 71. Этот сервер теперь является DNS-сервером

После завершения работы мастера настройки сервера и мастера настройки DNS-сервера DNS-сервер готов к использованию.

При завершении работы мастера настройки сервера автоматически устанавливается консоль DNS, которая используется для управления DNS-сервером. Чтобы открыть компонент "DNS" (рис. 72), нужно нажать кнопку "Пуск", выбрать команду "Программы - Администрирование", а затем - "DNS".

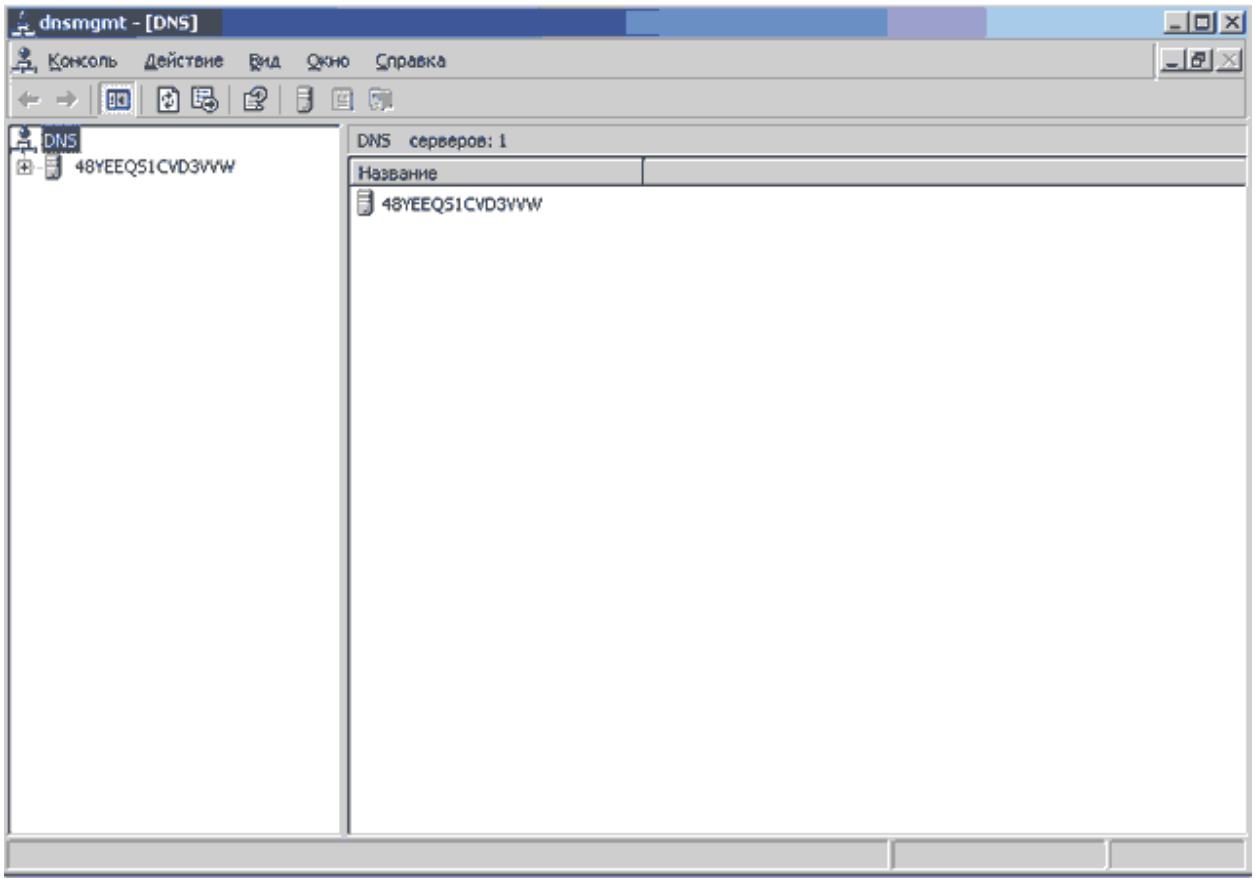


Рис. 72. Компонент DNS

Критерии оценивания
Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 14

«Настройка управляемого коммутатора L2/L3»

Цель: Ознакомиться с принципами работы и функциональными возможностями управляемых коммутаторов второго (L2) и третьего (L3) уровней. Научиться настраивать базовые параметры, VLAN, маршрутизацию и другие сетевые функции для оптимизации работы локальной сети.

Время выполнения: 8 часов.

Оборудование:

- Управляемый коммутатор (Cisco, MikroTik, HP и др.).
- Компьютер для настройки.
- Подключение через консольный порт (PuTTY, Tera Term) или Web-интерфейс.

Ход работы:

Теоретические сведения:

1. Что такое управляемый коммутатор?

Управляемый коммутатор — это сетевое устройство, которое позволяет администрировать, настраивать и управлять трафиком в сети.

2. Разница между L2 и L3 коммутаторами

Тип коммутатора	Описание
L2 (Канальный уровень)	Передает кадры на основе MAC-адресов, поддерживает VLAN.
L3 (Сетевой уровень)	Выполняет маршрутизацию на основе IP-адресов, поддерживает статическую и динамическую маршрутизацию.

3. Функции управляемого коммутатора

- Настройка VLAN.
- Управление портами (скорость, режим работы).
- Маршрутизация (для L3).
- Безопасность (ACL, фильтрация по MAC-адресам).
- Мониторинг (SNMP, логирование).

Задание:

1. Подключение к коммутатору

Через консольный порт:

Подключить кабель (RJ-45 или USB-C → COM).
Открыть PuTTY (9600 бод, 8N1, без контроля потока).
Через Web-интерфейс:

Подключиться к коммутатору по IP (по умолчанию 192.168.1.1).
Войти через браузер (admin/admin или указанный логин).

2. Базовая настройка коммутатора (CLI)

2.1. Настройка IP-адреса

```perl
enable
configure terminal
interface vlan 1
ip address 192.168.1.2 255.255.255.0
no shutdown
exit
write memory
```

2.2. Настройка VLAN

Создание VLAN 10 и VLAN 20:

```pgsql
enable
configure terminal
vlan 10
name OFFICE
exit
vlan 20
name IT
exit
```

2.3. Назначение портов в VLAN

```pgsql
interface FastEthernet0/1
switchport mode access
switchport access vlan 10
exit

interface FastEthernet0/2
switchport mode access
switchport access vlan 20
exit
write memory
```

2.4. Включение межвлановой маршрутизации (L3-коммутатор)

```nginx
ip routing
interface vlan 10
ip address 192.168.10.1 255.255.255.0
exit
interface vlan 20
ip address 192.168.20.1 255.255.255.0
exit
write memory
```

3. Проверка работоспособности сети
Проверить доступность коммутатора

```
ping 192.168.1.2
```

Проверить VLAN:

```
show vlan brief
```

Проверить маршрутизацию:

```
show ip route
```

Критерии оценивания
Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 15

«Виртуальные локальные сети VLAN, настройка»

Цель: Ознакомиться с концепцией виртуальных локальных сетей (VLAN), изучить их преимущества и области применения. Научиться настраивать VLAN на управляемом коммутаторе, конфигурировать порты, назначать VLAN-метки и проверять работоспособность сегментированной сети.

Время выполнения: 8 часов.

Оборудование:

- Управляемый коммутатор. Пример: коммутатор Cisco, HP, MikroTik или другой с поддержкой VLAN.
- Компьютеры/устройства для тестирования.
- Консольный кабель или доступ через Web-интерфейс.
- Терминальная программа (PuTTY, Tera Term) или веб-браузер для доступа к интерфейсу коммутатора.

Ход работы:

Теоретические сведения:

1. Что такое VLAN?

- **VLAN (Virtual Local Area Network)** – это логически выделенная группа устройств внутри одной физической сети, объединённых по функциональному, организационному или другому признаку.
- VLAN позволяет сегментировать сеть, изолируя трафик между различными группами, даже если они физически подключены к одному коммутатору.

2. Зачем используются VLAN?

- **Сегментация трафика:** уменьшение широковещательной нагрузки, разделение трафика между отделами (например, бухгалтерия, IT, отдел продаж).
- **Повышение безопасности:** изоляция трафика позволяет ограничить доступ между сегментами сети.
- **Упрощение управления сетью:** логическое разделение позволяет проще администрировать и настраивать политику безопасности, применять ACL (списки контроля доступа) и другие средства защиты.
- **Оптимизация использования ресурсов:** VLAN позволяют эффективно использовать один физический коммутатор для создания нескольких виртуальных сетей.

3. Основные принципы работы VLAN

- **Access-порты:** порты коммутатора, настроенные для работы с одним VLAN. Обычно подключают конечные устройства (ПК, принтеры).
- **Trunk-порты:** порты, способные передавать трафик нескольких VLAN посредством тегирования кадров (обычно используют протокол IEEE 802.1Q). Такие порты используются для соединения между коммутаторами или между коммутатором и маршрутизатором.
- **Нативный VLAN:** специальный VLAN для trunk-порта, для которого теги отсутствуют (необязателен, но часто используется в настройках).

4. Примеры использования VLAN

- Разделение трафика между офисами (например, отдел продаж и технический отдел).
- Создание гостевых сетей, изолированных от основной корпоративной сети.
- Разделение трафика для IP-телефонии и передачи данных для обеспечения качества обслуживания (QoS).

Задание:

1. Подключение к коммутатору

Через консоль:

Подключитесь к консольному порту коммутатора с помощью консольного кабеля и запустите терминальную программу (например, PuTTY) с параметрами (9600 бод, 8 бит, без контроля четности, 1 стоп-бит).

Через Web-интерфейс:

Если коммутатор имеет встроенный веб-сервер, откройте браузер и введите IP-адрес устройства (по умолчанию, например, 192.168.1.1). Авторизуйтесь, используя учётные данные (логин/пароль).

2. Базовая настройка IP-адреса для управления

Пример для CLI (на примере Cisco IOS):

```
enable
configure terminal
interface vlan 1
 ip address 192.168.1.2 255.255.255.0
 no shutdown
exit
write memory
```

Эта команда задаёт IP-адрес для управления коммутатором через VLAN 1.

3. Создание и настройка VLAN

Рассмотрим создание двух VLAN для разделения сети на два сегмента (например, VLAN 10 – отдел продаж, VLAN 20 – технический отдел).

3.1. Создание VLAN

```
configure terminal
vlan 10
 name SALES
exit
vlan 20
 name IT
exit
write memory
```

3.2. Назначение портов в соответствующие VLAN

Настроим порты, подключенные к ПК, чтобы они относились к нужным VLAN.

Для VLAN 10 (отдел продаж):

```
configure terminal
interface FastEthernet0/1
 switchport mode access
 switchport access vlan 10
exit
```

Для VLAN 20 (технический отдел):

```
configure terminal
interface FastEthernet0/2
 switchport mode access
 switchport access vlan 20
exit
write memory
```

Примечание: Если требуется настроить несколько портов, повторите команды для каждого соответствующего порта.

4. Настройка trunk-порта для передачи трафика нескольких VLAN

Если необходимо передать трафик с нескольких VLAN между коммутаторами или на маршрутизатор (router-on-a-stick), настройте trunk-порт. Например, порт FastEthernet0/24:

```
configure terminal
interface FastEthernet0/24
 switchport mode trunk
 switchport trunk encapsulation dot1q  ! (если требуется, указываем тип инкапсуляции)
 switchport trunk allowed vlan 10,20
exit
write memory
```

Эта команда позволяет передавать трафик VLAN 10 и VLAN 20 по trunk-порту.

5. Тестирование и проверка настройки VLAN

5.1. Проверка конфигурации VLAN

Используйте команду для отображения списка настроенных VLAN:

```
show vlan brief
```

В выводе вы увидите порты, назначенные каждой VLAN.

5.2. Тестирование связи между устройствами

Изолированность VLAN:

Подключите ПК к порту, назначенному VLAN 10, и другой ПК – к порту VLAN 20.

Попробуйте выполнить команду ping между ПК – если настройка выполнена правильно и отсутствует межвлановая маршрутизация, пинги не должны проходить.

Если требуется межвлановая маршрутизация:

Настройте маршрутизатор или включите маршрутизацию на L3-коммутаторе для связи между VLAN. Пример (на L3-коммутаторе):

```
configure terminal
interface vlan 10
 ip address 192.168.10.1 255.255.255.0
exit
interface vlan 20
 ip address 192.168.20.1 255.255.255.0
exit
ip routing
write memory
```

После этого, ПК из разных VLAN смогут обмениваться данными через маршрутизатор.

5.3. Дополнительные проверки

Проверьте состояние trunk-порта:

```
show interfaces trunk
```

Проверьте таблицу MAC-адресов

```
show mac address-table
```

Критерии оценивания

Оценка «5» ставится, если выполнены все задания

Оценка «4» ставится, если выполнено не менее 80% заданий

Оценка «3» ставится, если выполнено не менее 60% заданий

Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 16

«Мониторинг состояния элементов сети»

Цель: Ознакомиться с методами мониторинга состояния элементов сети, изучить основные инструменты и протоколы (например, SNMP, ICMP). Научиться настраивать и использовать средства мониторинга для контроля работоспособности сетевого оборудования и выявления возможных неисправностей.

Время выполнения: 4 часа.

Оборудование:

- Устройства сети: Сервер, маршрутизатор, коммутатор или рабочая станция с поддержкой SNMP.
- Программное обеспечение мониторинга:
- Локальный компьютер с установленными утилитами (например, ping, snmpwalk, snmpget)
- Система мониторинга (опционально – Zabbix, Nagios, Cacti или MRTG для централизованного контроля).
- Доступ к устройствам: Настроенные SNMP-сервисы на сетевых устройствах (например, SNMP-агент на сервере или коммутаторе).

Ход работы:

Теоретические сведения:

1. Понятие и задачи мониторинга сети

Мониторинг сети – это процесс постоянного наблюдения за состоянием и работой сетевых устройств и сервисов с целью своевременного обнаружения и устранения сбоев, оптимизации производительности и обеспечения безопасности.

Задачи мониторинга:

Контроль работоспособности узлов (серверов, маршрутизаторов, коммутаторов, рабочих станций).

Отслеживание пропускной способности, задержек, потерь пакетов и загрузки каналов связи.

Сбор статистики по использованию ресурсов (CPU, память, дисковое пространство).

Выявление аномалий, перегрузок и сбоев в работе оборудования.

Автоматизация уведомлений и создание отчётов для оперативного реагирования.

2. Основные элементы и протоколы мониторинга

Управляющее программное обеспечение: Системы мониторинга, такие как Zabbix, Nagios, PRTG, Cacti, MRTG и др.

Протокол SNMP (Simple Network Management Protocol):

Позволяет опрашивать сетевые устройства и получать их статус и статистику.

Работает по принципу запроса (polling) или уведомления (traps).

ICMP (Internet Control Message Protocol):

Используется утилитой ping для проверки доступности устройств.

Syslog:

Сбор и анализ системных логов для выявления ошибок и аномальных событий.

3. Основные показатели для мониторинга

Доступность узлов: Время отклика, процент недоступности (uptime/downtime).

Нагрузка на процессор и память: Использование CPU, объем свободной/занятой оперативной памяти.

Состояние сетевых интерфейсов: Скорость передачи данных, количество ошибок, потерь пакетов.

Пропускная способность каналов: Использование трафика, задержки, пиковые значения нагрузки.

События и логи: Фиксирование критических ошибок, сбоев питания, входов/выходов.

Задание:

1. Проверка доступности устройств с помощью ICMP (ping)

Откройте терминал или командную строку.

Выполните команду:

```
ping 192.168.1.1
```

Если устройство отвечает, то базовая связь установлена.

В случае отсутствия ответа проверьте физическое соединение и настройки брандмауэра.

2. Использование SNMP для получения информации об устройстве

2.1. Настройка SNMP на целевом устройстве (пример для Linux-сервера):

Установите SNMP-агент (если не установлен)

```
sudo apt-get install snmpd
```

Отредактируйте файл конфигурации SNMP (/etc/snmp/snmpd.conf), например, разрешив чтение для сообщества public (для тестовых целей):

```
rocommunity public  default    -V systemonly
```

Перезапустите сервис SNMP:

```
sudo systemctl restart snmpd
```

2.2. Получение данных с помощью snmpwalk:

Выполните команду, чтобы получить информацию о системе:

```
snmpwalk -v2c -c public 192.168.1.100 system
```

Где:

-v2c – используется версия SNMP 2c,

-c public – строка сообщества,

192.168.1.100 – IP-адрес целевого устройства.

В результате вы получите перечень параметров, таких как название системы, информация о процессоре, время работы и т.д.

2.3. Пример получения конкретного параметра:

Для запроса информации о загрузке системы можно использовать определённый OID (например, если устройство поддерживает нужный OID):

```
snmpget -v2c -c public 192.168.1.100 1.3.6.1.4.1.x.x.x
```

(Значение OID зависит от производителя и конфигурации устройства.)

3. Мониторинг состояния через системы централизованного контроля (опционально)

Если у вас есть система мониторинга (например, Zabbix или Nagios), настройте следующие шаги:

3.1. Установка агента мониторинга на сервере:

Для Zabbix, например, установите агент:

```
sudo apt-get install zabbix-agent
```

Отредактируйте конфигурационный файл /etc/zabbix/zabbix_agentd.conf, указав адрес сервера мониторинга и необходимые параметры.

Перезапустите агент:

```
sudo systemctl restart zabbix-agent
```

3.2. Добавление устройства в систему мониторинга:

В веб-интерфейсе Zabbix или Nagios добавьте новое устройство, укажите IP-адрес, SNMP-сообщества и выберите шаблоны мониторинга (например, шаблон для Linux-сервера или сетевого устройства).

После настройки система будет собирать данные, отображать графики загрузки, пропускной способности, ошибок интерфейсов и уведомлять о сбоях.

4. Анализ и интерпретация полученных данных

Проверка логов:

Системные логи (например, syslog) могут дополнительно информировать о сбоях, перегрузках или ошибках.

Сравнение показателей:

Сравните полученные данные с установленными пороговыми значениями. Например, если загрузка процессора превышает 80% в течение длительного времени, это может указывать на перегрузку.

Планирование действий:

На основе данных мониторинга примите меры по оптимизации сети: настройте балансировку нагрузки, распределите трафик или обновите оборудование.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания

Оценка «4» ставится, если выполнено не менее 80% заданий

Оценка «3» ставится, если выполнено не менее 60% заданий

Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 17

«Работа с серверами HTTP и FTP»

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

Время выполнения: 2 часа.

Оборудование:

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

Ход работы:

Теоретические сведения:

Сервер - в локальных вычислительных сетях - специализированная ЭВМ, управляющая использованием разделяемых между терминалами сети дорогостоящих ресурсов системы.

Сервер (англ. *server* от англ. *to serve* — служить) — в информационных технологиях — программный компонент вычислительной системы, выполняющий сервисные функции по запросу клиента, предоставляя ему доступ к определённым ресурсам.

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. Виды серверов: FTP; Файловый; Web; Телефонный; Терминальный; Факс; Суперсервер и т.д.

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,
- архивирование данных,
- 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. Администраторы узла (сервера). Имеют те же привилегии, что и разработчики, но могут также реконфигурировать сервер и определять категорию доступа.
5. Системные администраторы. Имеют идентичные привилегии с администраторами сервера.

Оснастка Internet Information Service (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 **Internet Information Services** 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. при желание вы можете что-нибудь новое добавить в эту программу самостоятельно);
- **RigthFTP, CuteFTP** – графические ftp-клиенты;
- **Total commander** (или любой другой с интерфейсом **Norton Commander**)– имеет встроенный ftp клиент;
- **Explorer.exe** – стандартное приложение **Windows**;
- Любой браузер.

Задание 1. Подготовьте файловый сервер.

1. Подключите к виртуальной машине **VM-2** образ установочного диска ***win2003-2.iso***.
2. Запустите виртуальную машину **VM-2**.
3. Добавьте новую **роль** серверу – *Файл-сервер*:
   - откройте диалоговое окно **Управление данным сервером (*Пуск/дминистрирование/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***.
4. Перезагрузите виртуальный компьютер кнопкой ***Перезегрузить***.
5. Откройте диалоговое окно **Настройки файлового сервера (*Пуск/дминистрирование/Управление Данным Сервером/Управление этим файловым сервером*)**.
6. 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***.
7. Откажитесь от включения службы индексирования.
8. Укажите папку на сервере, для хранения файлов, например ***C:\Documents and settings\Администратор\Рабочий стол\PUB***.

9. 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.

1. Установите **Internet Information Service (IIS) (*Пуск/администрирование/Управление Данным Сервером/Сервер приложений IIS*)**:
2. Подготовьте тестовую страницу:
- создайте временную страницу, вызываемую по умолчанию: наберите в **Блокноте** и сохраните в файле с именем ***Default.html*** в каталоге ***\Inetpub\wwwroot***.

-
3. 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***);

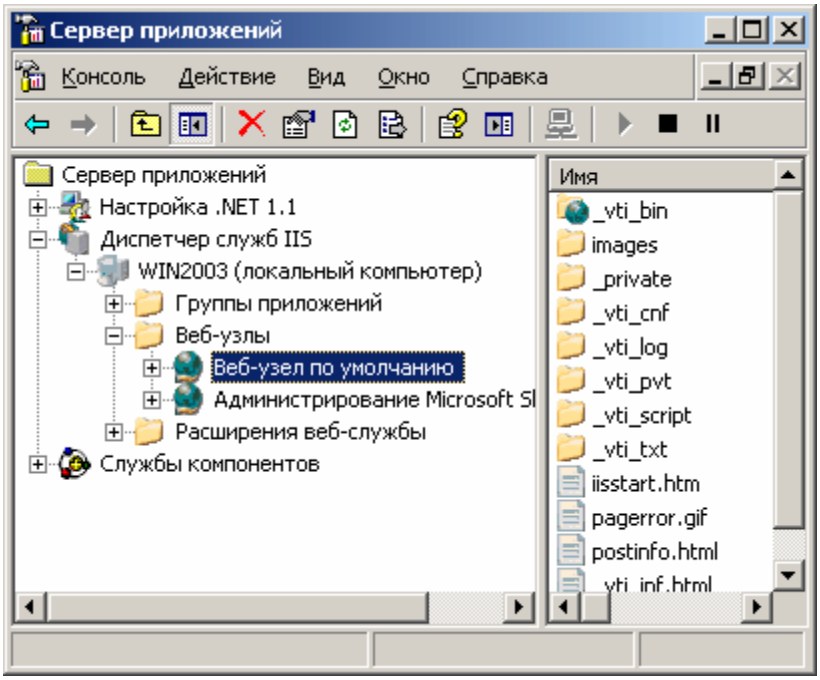


Рисунок 1. Консоль управления сервером приложений (IIS).

- откройте диалоговое окно **Свойства узла 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 ***OK***.
- закройте окно свойств кнопкой ***OK***.
4. Проверьте настройку **Web-сервера**:

- на вашем компьютере откройте **Internet Explorer (*Пуск/Программы/Internet Explorer*)**;
- наберите в адресной строке **http://127.0.0.1/**;
- сделайте скриншот происходящего на экране и сохраните его в своей папке.

Задание 3. Установите и настройте сервер FTP

1. Установите сервер **FTP - FileZilla**.
2. Запустите **FileZilla Server Interface**.

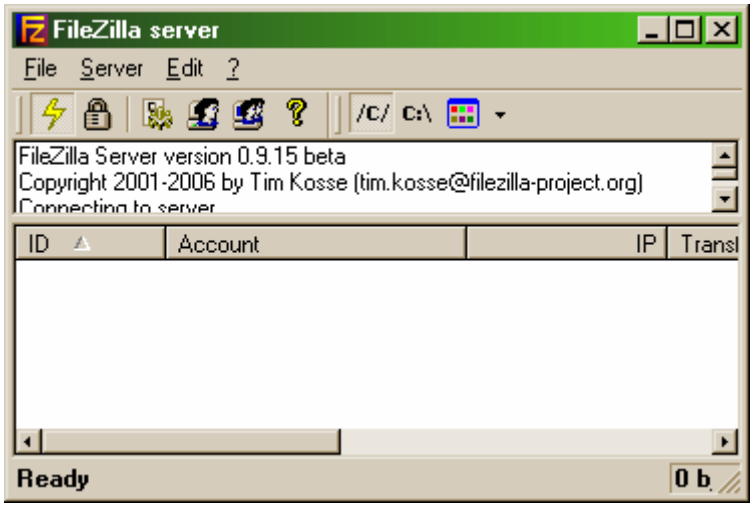


*Рисунок 2. Интерфейс управления FTP-сервером **FileZilla***

3. Ограничьте количество одновременных подключений к серверу:
- откройте окно настройки сервера (***Edit/Settings***);

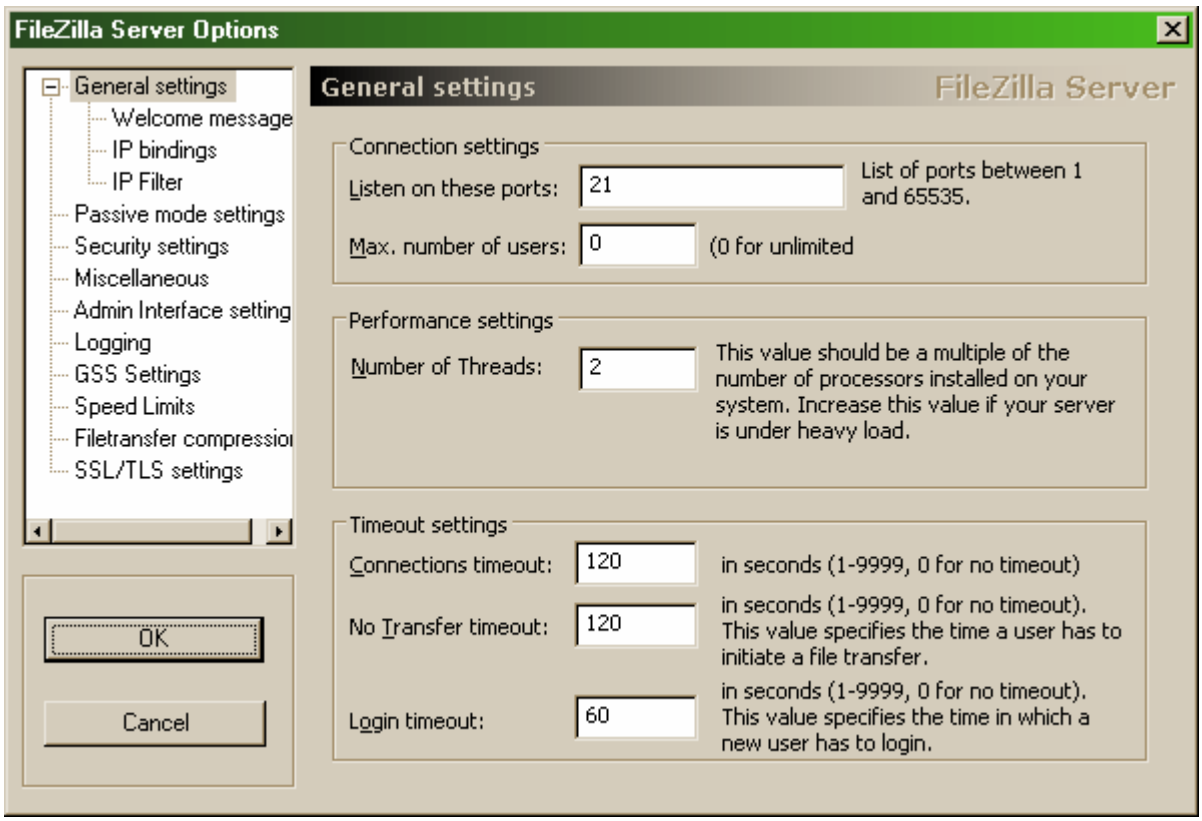


Рисунок 3. Настройки FTP-сервера

- перейдите в раздел **General Settings** (общие настройки);
- введите в поле **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 ***OK***;
- примените параметры кнопкой ***OK***.
- 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* (***OK***);
- задайте общую папку для созданной группы:
- перейдите в раздел **Shared Folders** (Общие папки);
- активируйте добавление папок кнопкой ***Add*** (Добавить);
- укажите общую папку, например ***C:\Documents and settings\Администратор\Рабочий стол*** и подтвердите выбор кнопкой ***OK***;
- разрешите чтение и удаление содержимого общей папки – установите флажок *Write u Delete*;
- завершите добавление групп пользователей кнопкой ***OK***.
- 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 ***OK***;
- установите пароль для созданного пользователя:
- перейдите на вкладку **General** (Общие);
- введите в поле **Password** новый пароль, например *123*;
- завершите добавление групп пользователей кнопкой ***OK***.
- 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**.

Критерии оценивания
Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 18

«Работа по протоколу передачи файлов FTP»

Цель: Изучить работу FTP – протокола (протокола передачи файлов). Получить представление о программе Telnet.

Время выполнения: 2 часа.

Ход работы:

Теоретические сведения:

На языке Internet'a FTP означает интерфейс пользователя, реализующий ARPANET стандартный протокол передачи файлов. Эта программа позволяет пользователю передавать файлы между двумя компьютерами, связанными между собой локальной (LAN) или глобальной (WAN) сетью. При этом компьютерные платформы могут быть различных типов. В этом и заключается главная особенность FTP в сети.

FTP-server - 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. Вообще, практически любой компьютер с операционной системой UNIX позволяет подключаться к нему по FTP протоколу. Соединение выполняется с помощью FTP клиента.

Команды FTP: [команда[аргументы]]

Выход в shell - интерпретатор на локальной системе.

dir [удаленная_директория] [локальный_файл]

ls [удаленная_директория] [локальный_файл] Выводит список файлов в директории либо не стандартный вывод, либо, если указано имя локального файла, в этот файл.

get [удаленный_файл] [локальный_файл] Вызывает передачу копии удаленного файла на ваш компьютер. В случае, если имя локального файла не было задано, то оно совпадает с именем удаленного файла.

mget [удаленные_файлы] Для получения нескольких файлов

hash Служит переключателем для индикации каждого полученного блока данных в 1024 байта, повышает наглядность процедуры.

cd [удаленная_директория] Сменить директорию. Существуют также 'cdup' или 'cd' для возврата на один или выше

lcd Меняет рабочую директорию на локальной машине (без аргумента - переход в домашнюю директорию пользователя)

bin (или binary) Переключает в режим передачи двоичных файлов

ascii Переключает в режим передачи текстовых файлов (обычно по умолчанию).

prompt Переключает интерактивную подсказку. Часто при использовании команды 'mget' желательно предварительно набрать 'prompt', чтобы не давать многократные подтверждения.

pwd Выводит имя удаленной рабочей директории.

mkdir [имя_директории] Создает директорию на удаленной машине

open хост [порт] Устанавливает соединение с заданным FTP сервером

put [локальный_файл] [удаленный_файл] Пересылает файл на удаленную систему. Если имя удаленного файла не указано, то оно совпадает с именем на локальной системе.

quit Синоним для 'bye'

recv [удаленный_файл] [локальный_файл] Синоним для команды 'get'

reget [удаленный_файл] [локальный_файл] "Дополучение" удаленного файла в том случае, когда часть его уже есть на локальной машине. Команда особенно полезна для получения больших файлов при возможных резервах соединения.

delete [удаленный_файл] Стирает удаленный файл

close Обрывает FTP сеанс с удаленным сервером и возвращает к командному интерпретатору

bye Оканчивает работу с FTP сервером и приводит к выходу и из интерпретатора.

NCSA Telnet версии 2.3 для PC обеспечивает интерактивный доступ с IBM PC к машинам, объединенным TCP/IP сетью. Команда telnet позволяет вам войти в терминальный сеанс работы с удаленным компьютером. Чтобы из командной строки запустить NCSA Telnet , введите C:\>telnet имя_компьютера Эта команда инициирует соединение с другим компьютером, чье имя дано в качестве параметра "имя_компьютера". Обычно этот компьютер (хост) сразу запрашивает у Вас регистрационное имя и пароль для создания новой сессии.

Задание:

Работа в режиме FTP.

1. Откройте Far (Пуск>Программы>Far manager).

2. Нажмите одновременно клавиши ALT F1. В появившемся окне выберите опцию FTP.

3. В командной строке наберите FTP://FTP2.KBSU.RU и нажмите ввод. В левой панели менеджера файлов появится корневой каталог сервера KBSU.RU.

4. Зайдите в каталог INCOMING, выберите любой подкаталог, и любой файл из этого подкаталога и скопируйте этот файл в папку STUDENT. Это можно сделать с помощью клавиши F5.

5. Повторите копирование любого файла с сервера FTP://FTP.MICROSOFT.COM. Копирование с удаленного сервера занимает больше времени, чем копирование с FTP://FTP2.KBSU.RU.

6. Откройте броузер Internet Explorer (Пуск>Программы>Internet Explorer).

7. В строке универсально адреса ресурса введите FTP://FTP2.KBSU.RU. В окне броузера появится корневой каталог сервера.

8. Скопируйте один из файлов в каталог STUDENT. Сравните копирование файлов по протоколу FTP с помощью программы Far и Internet Explorer. Где вы получаете больше информации о передаваемом файле?

9. Проверьте копирование файла по FTP с сервера FTP://FTP.MICROSOFT.COM с помощью броузера Internet Explorer.

Работа команд FTP.

1. Откройте КОМАНДНУЮ СТРОКУ (Пуск>Программы>Командная строка).

2. Анонимные FTP серверы позволяют вам войти в них под именем пользователя 'anonymous' или 'ftp', наберите: ftp ftp.microsoft.com.

3. Когда появится подсказка с именем системы, напечатайте следующее ftp .microsoft.com > login: anonymous или ftp. На появившуюся подсказку о пароле вводите: Password: ваш_адрес_электронной_почты.

4. После этого вы входите в систему и можете выполнять в ней различные команды в пределах интерпретатора FTP. Вместо имени FTP сервера вы можете использовать его IP адрес, например 198.105.232.1 для того же ftp.microsoft.com.

5. Наберите в командной строке DIR. На экране появится список доступных директорий. Справа будут обозначены названия директорий.

6. Введите следующую команду: CD BUSSYS. После успешного выполнения этой команды введите PWD. Вы увидите имя текущей директории.

7. Введите LS. Появится список файлов текущей директории. В этой директории будет присутствовать файл README.TXT. Скопируйте его с помощью команды GET README.TXT и этот файл будет скопирован в текущую директорию, т.е. D:\. Проверьте наличие файла в директории.

8. Введите LCD. На экране появится текущая локальная директория, именно в нее и будет скопирован файл.

9. Закончите работу с удаленным сервером набрав команду: CLOSE.

10.Выйдите из интерпретатора, используя команду: BYE.

Работа в режиме Telnet.

1. Откройте программу Telnet (Пуск>Программы>Стандартные>Telnet).

2. В главном меню выберите ПОДКЛЮЧЕНИЕ, Удаленная система. В появившемся окне Подключение, в опции Главный компьютер введите IP – адрес 192.168.0.1 и нажмите на кнопку Подключить. При подключении должен появится запрос на логин и пароль. Запишите имя подключенной системы.

3. Отключите подключенную систему (Подключение>Отключить).

4. Зайдите в параметры: (Терминал>Параметры). В появившемся окне поставьте флажки напротив опций Отображение ввода, Мерцающий курсор.

5. В этом же окне нажмите кнопку Шрифты. Измените шрифт, цвет, размер, атрибуты шрифта

6. Нажмите кнопку Цвет фона, выберите любой цвет фона. Как изменился вид программы?

7. Выйдите из программы Telnet (Подключение>Выход).

Контрольные вопросы:

1. Команды FTP, назначение, характеристика.

2. Назначение команды Telnet.

Отчет должен содержать:

1. Тему, цель работы, ответы на контрольные вопросы и на вопросы хода выполнения работы, выводы.

2. Описание выполненных действий по пунктам.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 19

«Соединение с сервером в безопасном режиме»

Цель: Ознакомиться с методами безопасного подключения к серверу, изучить принципы аутентификации и шифрования данных. Научиться устанавливать и настраивать защищенные соединения с сервером с использованием протоколов SSH, VPN или других технологий безопасности.

Время выполнения: 2 часа.

Ход работы:

Теоретические сведения:

1. Понятие безопасного соединения с сервером

Безопасное соединение с сервером – это установление защищённого канала передачи данных между клиентом и сервером с использованием технологий шифрования и аутентификации. Оно предотвращает перехват информации и несанкционированный доступ.

2. Методы безопасного соединения

SSH (Secure Shell) – защищённый протокол для удалённого управления сервером, обеспечивающий шифрование и защиту от атак (замена Telnet).

RDP (Remote Desktop Protocol) – протокол удалённого рабочего стола для соединения с Windows-серверами.

VPN (Virtual Private Network) – создание зашифрованного туннеля между клиентом и сервером.

HTTPS (HyperText Transfer Protocol Secure) – безопасное соединение для веб-сервисов.

3. Протокол SSH (основной метод соединения)

SSH – это наиболее распространённый и надёжный способ безопасного подключения к серверу. Он использует симметричное и асимметричное шифрование, аутентификацию с помощью паролей или ключей.

Основные команды SSH:

Подключение к серверу:

```
ssh user@server_ip
```

Подключение с нестандартным портом:

```
ssh -p 2222 user@server_ip
```

Использование ключей для аутентификации:

```
ssh -i /path/to/private_key user@server_ip
```

Копирование файлов через SCP (Secure Copy)

```
scp file.txt user@server_ip:/home/user/
```

4. Двухфакторная аутентификация и защита SSH

Для повышения безопасности применяют:

Аутентификацию по ключу вместо пароля
Ограничение доступа по IP-адресу
Изменение стандартного порта SSH (22 → другой)
Fail2Ban для защиты от брутфорса

Задание:
1. Настройка безопасного соединения с сервером через SSH
1.1. Подключение к серверу по SSH
Откройте терминал.
Введите команду:

```
ssh user@server_ip
```

Введите пароль (если используется парольная аутентификация).
1.2. Использование SSH-ключей для безопасного соединения
Создайте SSH-ключ (на клиенте)

```
ssh-keygen -t rsa -b 4096 -C "your_email@example.com"
```

Ключи будут сохранены в ~/.ssh/id_rsa (закрытый) и ~/.ssh/id_rsa.pub (открытый).
Скопируйте открытый ключ на сервер:

```
ssh-copy-id user@server_ip
```

(или вручную добавьте содержимое id_rsa.pub в ~/.ssh/authorized_keys на сервере)
Проверка подключения:

```
ssh user@server_ip
```

Теперь доступ без пароля возможен только с доверенного устройства.
1.3. Изменение порта SSH для защиты
Откройте файл конфигурации SSH на сервере

```
sudo nano /etc/ssh/sshd_config
```

Найдите строку #Port 22 и замените её, например, на

```
Port 2222
```

Перезапустите SSH-сервис:

```
sudo systemctl restart ssh
```

Подключение теперь выполняется так

```
ssh -p 2222 user@server_ip
```

2. Настройка безопасного соединения с сервером через VPN
(Опционально, если сервер предоставляет VPN-доступ)

Установите OpenVPN

```
sudo apt-get install openvpn
```

Скопируйте VPN-конфигурационный файл (*.ovpn) на клиент.
Подключитесь

```
sudo openvpn --config /path/to/config.ovpn
```

Проверьте соединение

```
ip a
```

3. Настройка безопасного соединения через RDP (для Windows-серверов)

Откройте Подключение к удалённому рабочему столу (mstsc.exe).

Введите IP-адрес сервера.

Включите Network Level Authentication (NLA) для дополнительной защиты.

Настройте VPN перед подключением, чтобы исключить открытый доступ в интернет.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания

Оценка «4» ставится, если выполнено не менее 80% заданий

Оценка «3» ставится, если выполнено не менее 60% заданий

Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 20

«Установка и настройка HTTP-сервера»

Цель: Получить теоретические и практические навыки по работе с веб-сервером.

Время выполнения: 6 часов.

Ход работы:

Теоретические сведения:

Основа Интернета известна всем – это сервера. Именно на них размещены домашние страницы рядовых пользователей, состоящие из нескольких страничек, тематические ресурсы, состоящие из сотен страниц, часто генерируемых динамически и в большинстве своем поддерживаемые группой людей, а также коммерческие проекты и вполне настоящие, несмотря на свою виртуальность, магазины. Большинству рядовых пользователей свой сервер совершенно не нужен. Посудите сами: даже если не выключать домашний компьютер круглосуточно, установив серверное ПО, то для доступа к нему также необходимо круглосуточное соединение с провайдером. Соединение по телефонной линии слишком медленное, чтобы обслуживать хотя бы десять клиентов одновременно. А выделенная линия стоит дорого. Намного проще разместить свою страничку на сервере провайдера. Другое дело – корпоративные пользователи. Как правило, у них уже есть выделенная линия, соединяющая с Интернетом локальную сеть, и выделенный компьютер, выполняющий роль шлюза между локальной и глобальной сетями. На нем-то и можно установить веб-сервер. Или для того, чтобы отдать дань моде, или развернуть крупный проект, приносящий прибыль.

Для того чтобы в Интернете появился сайт, он должен быть размещен на сервере хостера или вашем собственном, подключенном к Сети и имеющем выделенный IP-адрес. Сервер представляет собой компьютер, на котором установлено специальное программное обеспечение, которое тоже называют "веб-сервером".

Веб-сервер — это сервер, принимающий HTTP-запросы от клиентов, обычно веббраузеров, и выдающий им HTTP-ответы, обычно вместе с HTML-страницей, изображением, файлом, медиа-потоком или другими данными.

Веб-серверы — основа Всемирной паутины.

Клиенты получают доступ к веб-серверу по URL адресу нужной им веб-страницы или другого ресурса.

Дополнительными функциями многих веб-серверов являются:

• ведение журнала обращений пользователей к ресурсам,

• аутентификация пользователей,

• поддержка динамически генерируемых страниц,

• поддержка HTTPS для защищённых соединений с клиентами.

Что должен делать Web-сервер?

Основное действие конечного пользователя в Интернете – это "переход на Webстраницу". На самом общем уровне это предполагает совместную работу пары

приложений:

• Web-браузера, такого как Firefox или Internet Explorer, который показывает в удобной для человеческого восприятия форме запрашиваемую страницу, которую он получает от…

• Web-сервера, находящегося, как правило, на удалённой машине, который отвечает на запрос страницы потоком данных в формате HTML или аналогичном.

С браузерами имеют дело Web-пользователи, которые подходят к их выбору и анализу с надлежащей тщательностью. Напротив, серверы видны только техническому персоналу сайтов.

Web-сервер оценивается по целому ряду важнейших параметров:

• Эффективность: как быстро он отвечает на запрос?

• Масштабируемость: продолжает ли сервер работать надёжно, когда к нему одновременно обращаются много пользователей?

• Безопасность: совершает ли сервер только те операции, которые должен? Какие возможности он предлагает для аутентификации пользователей и шифрования потока обмена информацией? Делает ли его использование более уязвимыми соседние приложения или хосты?

• Работоспособность: какие у сервера режимы отказа и аварийные ситуации?

• Соответствие стандартам: поддерживает ли сервер соответствующие RFC?

• Гибкость: можно ли настроить сервер для принятия большого количества запросов или динамических страниц, требующих значительных вычислений, или сложной аутентификации, или ...?

• Требования к платформе: на каких платформах возможно использование сервера? Предъявляет ли он особые требования к аппаратной платформе?

• Управляемость: легко ли установить и обслуживать сервер? Совместим ли он с организационными стандартами по ведению журналов, аудиту, оценке затрат и т.д.?

2. Обзор наиболее распространенных веб-серверов

В мире существует огромное множество веб-серверов. Они отличаются друг от друга по функциональности и по предназначению.

Обзорная таблица

Название	Автор и год создания	Распространение	Open Source	Лицензия	Особенности
Apache HTTP Server	Apache Software Foundation, 1995	бесплатно	Да	Apache License	Упор на надёжность и гибкость.
HTTP File Server	Massimo Melina, 2002	бесплатно	Да	GNU GPL	Простой сервер для выкладывания файлов в сети.
Internet Information Services	Microsoft, 1995	вкл. в Win NT	Нет	Microsoft EULA	Является частью пакета IIS.
Jetty	Mort Bay	бесплатно	Да	Apache	Реализован

	Consulting, 1995			License	полностью на Java.
lighttpd	Jan Kneschke	бесплатно	Да	Вариант BSD	Использование на сильно нагруженных серверах обеспечивая быстроту и защищённость.
nginx	Игорь Сысоев для Рамблера, 2002	бесплатно	Да	Вариант BSD	Разрабатывался для испытывающих большую нагрузку серверов. Включает в себя почтовый прокси-сервер.

Поддержка платформ

Название	Windows	Mac OS X	Linux	BSD	Solaris
Apache HTTP Server	Да	Да	Да	Да	Да
HTTP File Server	Да	Нет	Нет	Нет	Нет
Internet Information Services	Да	Нет	Нет	Нет	Нет
Jetty	Да	Да	Да	Да	Да
lighttpd	Да	Да	Да	Да	Да
nginx	Нет	Да	Да	Да	Да

Около 90% всех сайтов, согласно недавним исследованиям Netcraft, работают всего на двух из них - Apache и Internet Information Server (IIS). Оба эти сервера – тщательно проработанные продукты, обладающие не только очень длинным списком встроенных возможностей, но и процветающим "вторичным рынком" книг, дополнений, консультаций, провайдеров и т.д. IIS — это монстроподобный гигант великой компании Microsoft. Установив этакую "штуковину", Вы сразу получаете FTP сервер, WEB сервер, Сервер Почты и многое другое.

IIS поддерживает удаленное администрирование, для этого существует специальный web интерфейс. Программа имеет красивый и интуитивно понятный графический интерфейс для контроля и настройки. Несколько разновидностей логов. IIS нуждается в минимальной настройке. Большинству пользователей вполне подойдут настройки по умолчанию. IIS работает только под ОС Windows. Создавая IIS, Microsoft хотела втолкнуть Windows NT на рынок веб-серверов. Если имеется необходимость поставить сервер для большого предприятия, и исторически сложилось так, что сервер работает под Windows NT/2000 - в этом случае IIS для Вас. IIS входит в стандартную поставку Windows 2000 Server и Windows 2000 Advanced Server. Из поддерживаемых технологий следует отметить ASP и работу с ODBC (различные базы данных).

Другой, не менее распространенный сервер - Apache удовлетворяет практически всем потребностям современных веб-разработок, но в то же время он достаточно прост, чтобы его устанавливали программисты для отладки своих программ.

В 1994 году сотрудник Национального центра приложений для суперкомпьютеров в Университете Иллинойса США (NCSA) Роб Маккул выложил в общее пользование первый веб-сервер, который так и назывался — NCSA HTTP daemon. Сервер получил

популярность в узких кругах, но в середине 1994 года Маккул покинул университет, и разработки прекратились.

Небольшая группа заинтересованных веб-мастеров начала совместную работу над продуктом. Общаясь в дискуссионном листе по электронной почте, они разрабатывали «заплатки» и нововведения для сервера. Именно они и создали Apache Group, разработавшую первую версию Apache-сервера. Произошло это в апреле 1995 года, когда на основу (NCSA Server 1.3) были наложены все существующие «заплатки». Так появился первый официальный публичный релиз Apache 0.6.2.

Итак, что же такое Apache? Это полнофункциональный, расширяемый веб-сервер, полностью поддерживающий протокол HTTP/1.1 и распространяющийся с открытым исходным кодом. Сервер может работать практически на всемх распространенных платформах. Существуют готовые исполняемые файлы сервера для Windows NT, Windows 9x, OS/2, Netware 5.x и нескольких UNIX-систем.

Apache настраивается с помощью текстовых конфигурационных файлов. Основные параметры уже настроены «по умолчанию» и будут работать в большинстве случаев. Если вам не хватает функциональности штатного «Апача», то стоит присмотреться к распространяемым модулям, написанным Apache Group и сторонними разработчиками. Немаловажным преимуществом является то, что создатели активно общаются с пользователями и реагируют на все сообщения об ошибках. Самая простая функция, которую может выполнять Apache – стоять на сервере и обслуживать обычный HTML-сайт. При получении запроса на определенную страницу сервер отправляет в ее ответ браузеру. Набираете адрес, открывается страница — все просто.

Если на одном сервере с установленной операционной системой семейства Unix и сервером Apache заведено несколько пользователей, то каждому из них можно создать отдельную директорию. Точнее, она будет создаваться автоматически вместе с псевдонимом. Это делается с помощью модуля mod_userdir и директивы UserDir. Так, например, можно папке public_html в домашней папке пользователя сопоставить адрес www.site.ru/~user. В общем-то, так и делается на серверах большинства сайтов, предоставляющих бесплатный хостинг. Администратор сервера может разрешить или запретить определенным пользователям создавать домашние страницы, использовать SSI и другие функции сервера. Полноценный же хостинг обычно предусматривает создание отдельного виртуального сервера для каждого пользователя.

Сервер Apache был одним из первых серверов, которые начали поддерживать виртуальные сервера (хосты). Эта возможность позволяет размещать на одном физическом сервере несколько полноценных сайтов. У каждого из них может быть свой домен, администратор, IP-адрес и так далее.

Если вам нужно разместить на вашем сервере домены domain.ru и domain.com, то для начала надо сделать так, чтобы в системе DNS им был сопоставлен ваш IP-адрес. После этого в конфигурационном файле Apache создаете две директивы , где описываете каждый виртуальный хост. Таким образом, сервер будет знать, на какую папку «отправлять» пришедший запрос. В данный момент большинство интернет-страниц являются динамическими. Это значит, что их внешний вид и наполнение формируется с помощью программного скрипта, написанного на одном из «языков» (их нельзя в полной мере назвать языками, определение достаточно условно).

В данный момент наиболее сильно распространены технологии CGI и PHP. Разумеется, в Apache существует поддержка и того, и другого, плюс возможность подключать другие языки.

Модуль mod_cgi позволяет вам размещать на сервере CGI-скрипты. Вообще, это всегонавсего исполняемые файлы, написанные на одном из допустимых языков программирования. Они могут содержаться как в откомпилированном виде (например, так делают, если пишут CGI на языке C++), так и в виде исходного текста (если на сервере

установлен Perl, то программист может помещать и такие файлы. Иногда они имеют расширение .pl).

Что касается PHP, то возможность интеграции его в Apache предусмотрена разработчиками самого PHP. Apache же выполняет только функции посредника между скриптом и компилятором. Существует два способа интеграции PHP в Apache. Первый – установка специального модуля, расширяющего возможности сервера, и тогда он сам становится способным «компилировать» скрипты. И второй – установка в конфигурационных файлах связей между php-файлами и самим компилятором (он находится на диске в виде файлов .cgi или .exe). На основе сервера Apache можно создавать не только простые любительские сайты, но и ресурсы, требующие серьезной криптографической защиты передаваемых данных. Специально для этого был разработан протокол SSL/TLS, а его поддержка была встроена в Apache 2.0. С помощью специального модуля можно осуществлять аутентификацию на основе именных сертификатов, что позволяет практически наверняка гарантировать подлинность пользователя.

Ну и, разумеется, сервер Apache может вести протокол всех действий, совершаемых с ним. Причем администратор может сам выбрать степень подробности протокола. Протоколы ведутся отдельно для ошибок, для успешных операций и для каждого виртуального хоста. Словом, полный набор для тщательного анализа появляющихся ошибок.

3. Организация локального веб-сервера.

Content Manage System позволяет четко разделить обязанности. Пользователю, остается лишь выбрать специальный пункт меню, дождаться загрузки визуального редактора (аналога Word`a), заполнить поле требуемым материалом и сохранить. Сразу же новость становится доступной для всеобщего обозрения (Примечание: в зависимости от прав, материал может публиковаться не сразу, а после проверки ответственным за это человеком). И совершенно не требуется никаких знаний HTML кода!

Для того, чтобы данные системы функционировали, одного HTML недостаточно. По сути это всего лишь язык разметки, который сообщает браузеру(IE, Opera, Mozilla) как 6 отобразить информацию загруженную с сервера на компьютер пользователя – это так называемая клиентская сторона. Кроме того, сюда относятся CSS, Javascript.

Существует еще так называемая «серверная» сторона выполнения кода. Главная идея – пользователь посылает запрос на сервер (например, кликает по пункту меню «Наши выпускники» сайта кафедры) и получает готовый результат на своем компьютере (в нашем примере сервер генерирует html-страницу и выдает ее пользователю). Возможность генерации страниц «на лету» с серверной стороны позволяет существенно расширить реализацию различных «примочек».

Рассмотрим поподробнее этот вопрос. Пользователь привыкает еще с первых моментов работы за компьютером что каждый файл имеет свой адрес. Например,

C:\Program Files\Mozilla Firefox\firefox.exe

Отсюда четко становится понятным, где находится файл firefox.exe Что представляет собой сайт? В простейшем случае, это набор связанных html страниц (т.е. файлов с расширением .html). Поэтому набирая в адресной строке что-то вроде

http://physics.volsu.ru/feskov/index.html

мы уверены, что в папке /feskov находится файл index.html, который подгружается с сервера на компьютер пользователя и лишь потом отображается на в браузере. Поэтому содержимое данной страницы можно изменить лишь только изменив сам файл index.html Рассмотрим теперь другой случай. Набрав адрес

http://physics.volsu.ru/nashi-vypyskniki.html

нам кажется что в корневой директории на сервере должен быть файл nashivypyskniki.html. Но его там нет физически. И не должно быть. Этот файл генерирует сервер на своей стороне и в готовом виде выдает компьютеру пользователя. Чтобы изменить текст на странице, достаточно изменить параметры обработки и выдачи

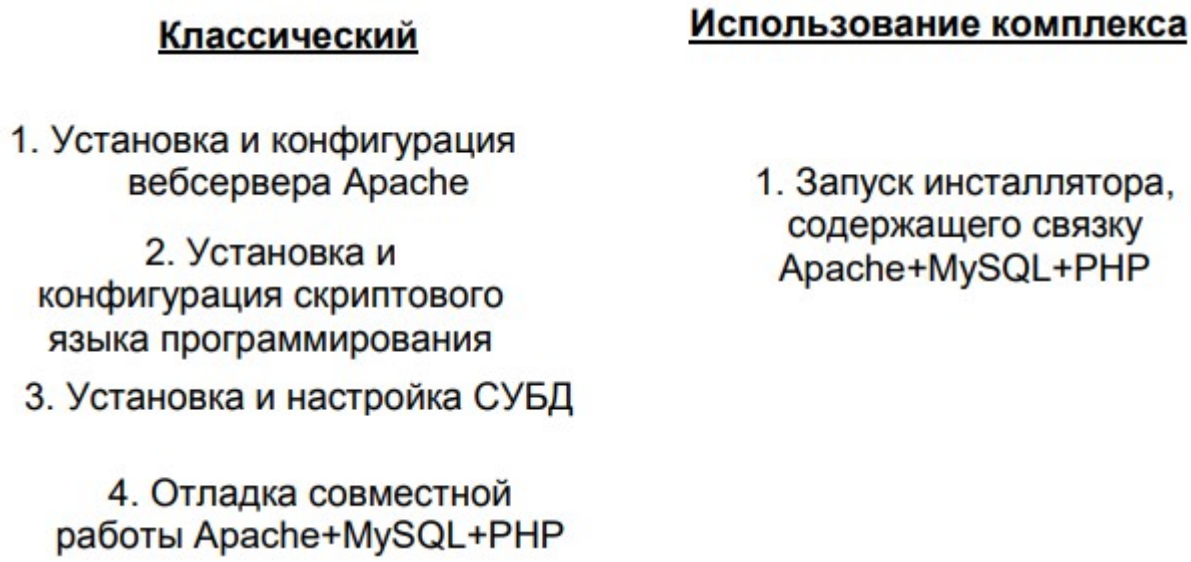
информации(с помощью визуального редактора). Никакого знания кода, никакого доступа к файлам – отличное решение в плане безопасности! Для веб-приложений используются специальные языки, которые предназначены для выполнения на стороне сервера(ASP, JAVA, PHP и т.д). Мы будем рассматривать только PHP.

Для его функционирования также используется база данных MySQL. Этому есть несколько причин: быстродействие (снижается нагрузка на сервер), безопасность (например, возможность скрытия и шифрования паролей) и многое другое. Пользователь видит только результат, выдаваемый сервером, содержимое php файла или базы данных он не увидит. Поэтому, если написать и разместить скрипт на сайте (программа на серверном языке), то «утащить» его можно будет лишь в случае непосредственного доступа к файлам (например, по FTP)

Итак, подведем итог. Что нам требуется для функционирования сайта?

1. Веб-сервер(Apache) для обработки http запросов
2. PHP – скриптовый язык программирования
3. MySQL – СУБД

Что необходимо, чтобы создать локальный веб сервер на персональном компьютере? Рассмотрим два варианта: установка компонентов по отдельности и установка комплексом.



Таким образом, использование сборок позволяет существенно сократить время и требует меньших знаний о каждом составляющем компоненте. Готовые решения уже можно найти в сети Интернет. Одно из таких решений – Денвер (denwer.ru) Таким образом, характерными особенностями «хороших» комплексов по созданию локального веб-сервера являются:

1. Русификация
2. Виртуальный диск
3. Минимальные знания и требования для установки
4. Автоматическое добавление новых сайтов
5. Графическая оболочка для настроек
6. Небольшой вес дистрибутива
7. Самостоятельное обновление
8. Тестовые и обучающие программы

Задание:

1. Установка Денвера

Для установки веб-сервера требуется полноценный доступ к изменению файла hosts, расположенному в папке: C:\WINDOWS\system32\drivers\etc (разумеется, диск и название папки WINDOWS могут быть другими)

1. Запускаем инсталляционный файл Денвера.

2. Указываем, в какой каталог требуется установить комплекс (по умолчанию, все файлы загрузятся в папку C:\WebServers). Все файлы Денвера будут находиться только в этой папке (за исключением трех ярлыков на рабочем столе)

3. Следующий шаг заключается в создании виртуального диска. Придумываем ему имя (например Server) и оставляем умолчание Z:/

4. После копирования файлов дистрибутива будет задан вопрос, каким образом запускать и останавливать комплекс. Пользователю предлагается два варианта

а) создание виртуального диска и запуск Денвера при загрузке компьютера

б) создание виртуального диска и запуск Денвера вручную при щелчке ярлыка запуска (Start Servers) на рабочем столе.

5. Установка комплекса завершена.

Обращаем внимание, что, если установка производится под логином «Администратор» (записанном кириллицей), ярлыки на Рабочем столе не создаются. В этом случае они могут быть созданы вручную, используя папку C:\WebServers\etc. При возникновении проблем с установкой системы Денвер, рекомендуется обратиться за дополнительной информацией на сайт разработчика: http://www.denwer.ru/base.html

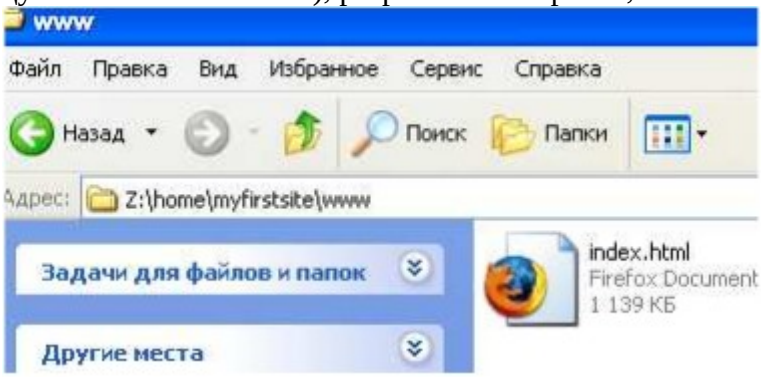
3. Работа с Денвером. Создание нового домена.

Для тестирования работы установленного комплекса используем готовый html-сайт (или отдельную страницу index.html).

1. Запускаем Денвер (если он не запустился сам при загрузке компьютера). Примечание: комплексу требуется полноценный доступ к изменению файла hosts, расположенному в папке: C:\WINDOWS\system32\drivers\etc.

2. Для проверки работоспособности запущенного комплекса откройте любой из имеющихся в системе Интернет-браузеров (IE, Opera, Firefox и др.) и в адресной строке наберите http://localhost. Если установка была завершена успешно, в окне браузера появится стартовая страница Денвера, показанная ниже.

3. На диске Z: (виртуальный диск, создаваемый Денвером при запуске) найдите папку Z:\home, в которой создайте новую директорию (например, myfirstsite). После этого зайдите в эту папку и создайте в ней еще одну папку www. Поместите готовый сайт (или страницу с именем index.html), разработанные ранее, в этот каталог (см. рис. ниже).



4. После того, как все файлы скопированы, перезапустите веб-сервер, кликнув по ярлыку «Restart Servers».

5. В адресной строчке веб-браузера наберите в http://myfirstsite. Если все этапы установки комплекса и локального размещения сайта выполнены правильно, в окне браузера отобразится содержимое файла index.html.

3. Работа с Денвером. Создание поддоменов.

1. В директории домена создайте новую папку (subdomain). Разместите в ней файл index.html.

2. Перезапустите Денвер. Проверьте работу поддомена, набрав в адресной строчке браузера адрес вида: http://subdoman.domain

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 21

«Настройка свойств и параметров безопасности Интернет браузера »

Цель: Научиться настраивать параметры безопасности в современных Интернет браузерах.

Время выполнения: 2 часа.

- Оборудование:
- аппаратные: компьютер;
- программные: ОС Windows XP или Windows 2000; браузеры: Internet Explorer; Firefox, Opera.

Ход работы:

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 1.

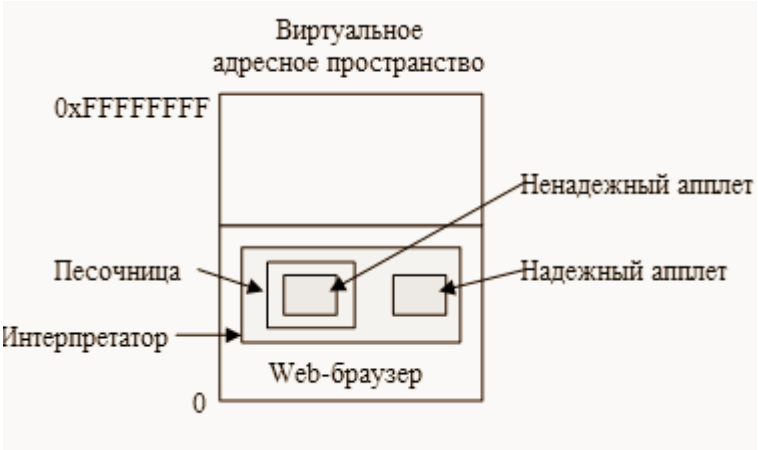


Рисунок 1. Обработка апплетов браузером

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 в данном случае сводится к вопросу о том, 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 сначала 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, в противном случае 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 метода 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 части. 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.

Задание: 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*;
6. Отключите *Использование элементов ActiveX не помеченных как безопасные*;
7. Отключите загрузку *Неподписанных элементов ActiveX*;
8. Примените параметры кнопкой ***OK***;
9. Установите параметры конфиденциальности:
    - перейдите на вкладку **Конфиденциальность**;
    - установите регулятор на уровень *Умеренно высокий*;
    - разрешите загружать файлы ***cookie*** с узла **www.mail.ru**:
        - щелкните по кнопке ***Узлы***;
        - введите в поле *www.mail.ru* и щелкните по кнопке ***Разрешить***;
    - аналогично разрешите загружать cookie со следующих узлов: **www.yandex.ru, www.pochta.ru**;
    - примените параметры кнопкой ***OK***;
10. 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 ***OK***.
    - перейдите на вкладку **Оценки** и установите уровни **Службы оценки 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**.

Критерии оценивания
Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 22

«Настройка брандмауэра»

Цель: Ознакомиться с принципами работы брандмауэра (firewall), изучить его роль в обеспечении безопасности сети. Научиться настраивать брандмауэр для контроля и фильтрации сетевого трафика, а также создавать правила для защиты сети от несанкционированного доступа.

Время выполнения: 4 часа.

Ход работы:

Задание:

Брандмауэр Windows препятствует несанкционированному доступу вредоносных программ из Интернета и локальной сети. Общий вид брандмауэра операционной системы Windows 7 изображен на рисунке 4.8

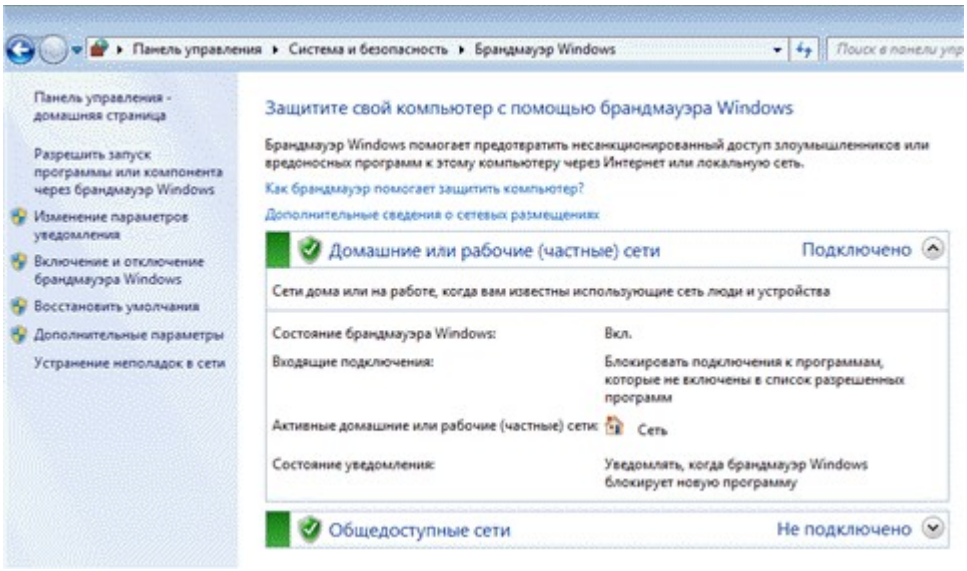


Рисунок 4.8 – Окно брандмауэра Windows 7

Для запуска из командной строки используется команда: control.exe/name Microsoft.WindowsFirewall.

В брандмауэре Windows 7 произошел ряд изменений, в первую очередь функциональных. Основным нововведением в брандмауэре Windows 7 является одновременная работа нескольких сетевых профилей:

- общий – публичные (общедоступные) сети, например, в кафе или аэропорту;
- частный – домашние или рабочие сети;
- доменный – доменная сеть в организации, определяемая автоматически.

В предыдущих версиях только один профиль мог быть активен в любой момент времени, Windows 7 все три профиля могут быть активны одновременно, обеспечивая соответствующий уровень безопасности для каждой сети.

Настройка параметров брандмауэра заключается в изменении двух параметров: изменение параметров уведомления, а также включение и отключение брандмауэра Windows

Обе ссылки открывают окно настройки параметров (Рисунок 4.9).

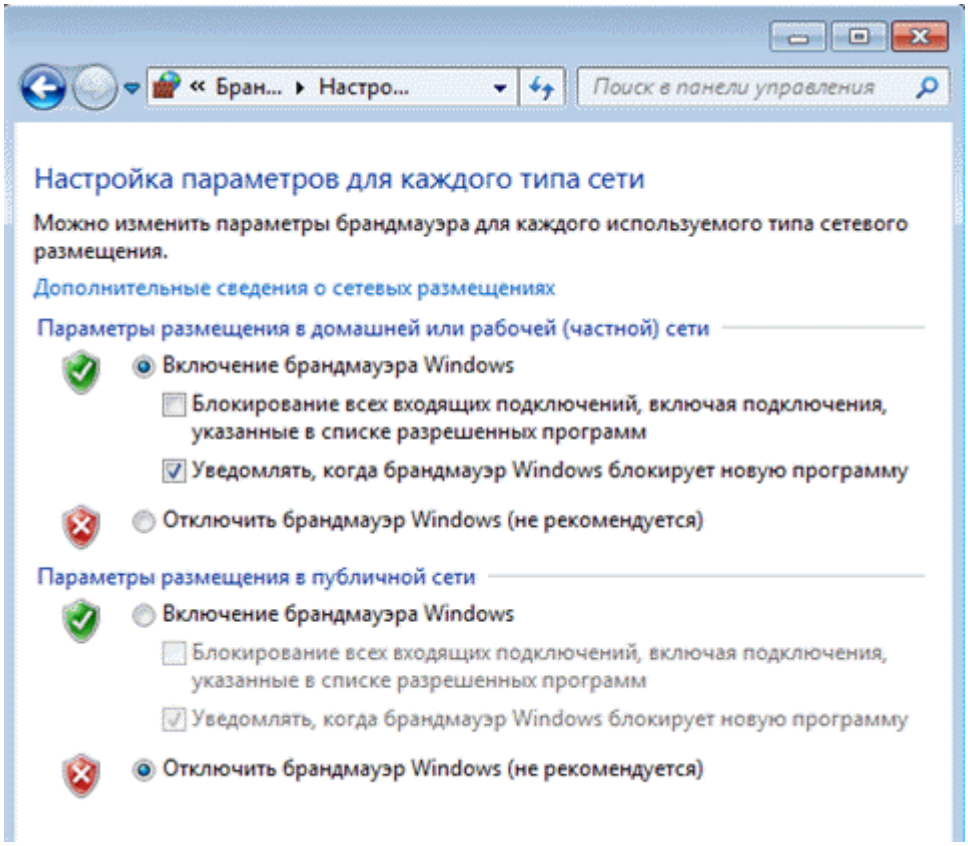


Рисунок 4.9 – Настройка параметров для каждого вида сети

Для каждого профиля можно задать собственный набор параметров. При включении брандмауэра рекомендуется включить уведомления о блокировке новой программы. В диалоговом окне блокировки также имеется возможность разрешить или заблокировать программу для каждого профиля.

В случае необходимости существует возможность сброса настроек брандмауэра. Для этого необходимо выбрать опцию Восстановить умолчания в левой панели. В открывшемся окне подтверждаем выбранное действие.

Для настройки разрешения для конкретной программы или компонента операционной системы необходимо выбрать опцию Разрешить запуск программы или компонента через брандмауэр Windows в левой панели и в открывшемся окне нажмите кнопку Изменить (Рисунок 4.10).

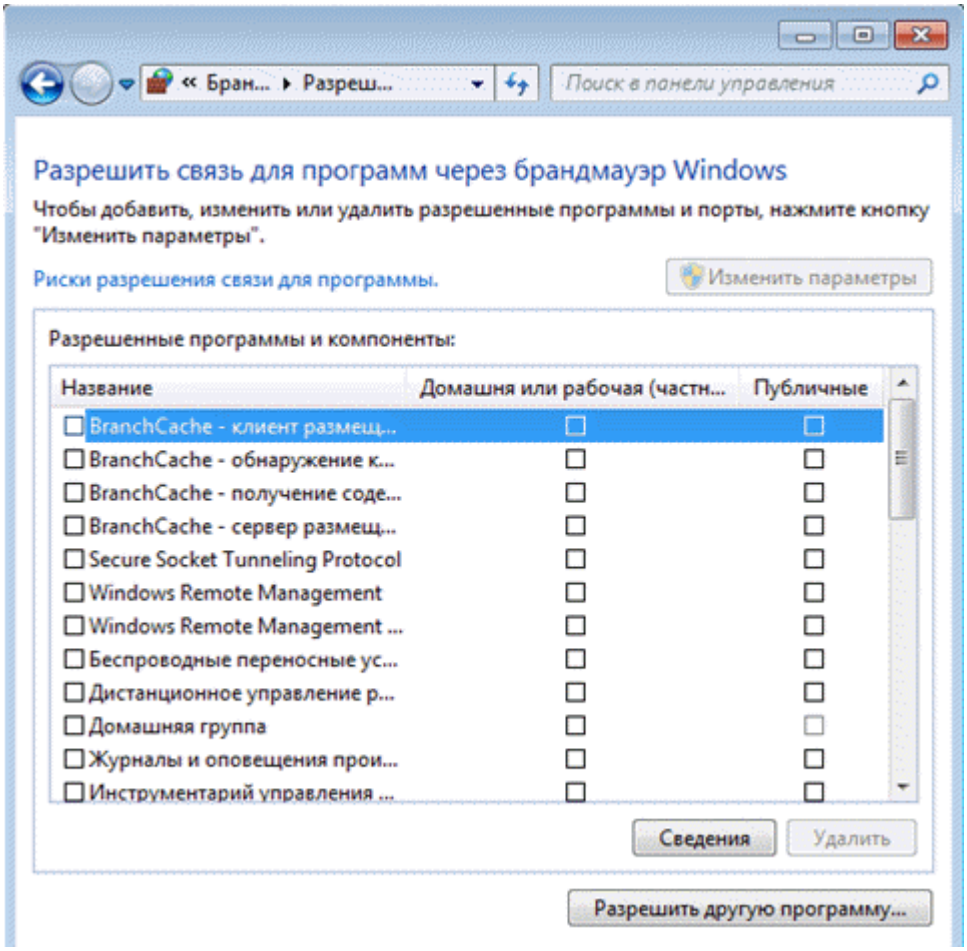


Рисунок 4.10 – Окно Разрешить связь программ через Брандмауэр Windows

Для добавления в список конкретной программы, необходимо выбрать Разрешить другую программу.

У брандмауэра Windows есть расширенный режим, который реализован с помощью оснастки консоли управления Microsoft (MMC). В левой панели щелкните Дополнительные параметры и перед вами предстанет Брандмауэр Windows в режиме повышенной безопасности (Рисунок 4.11).

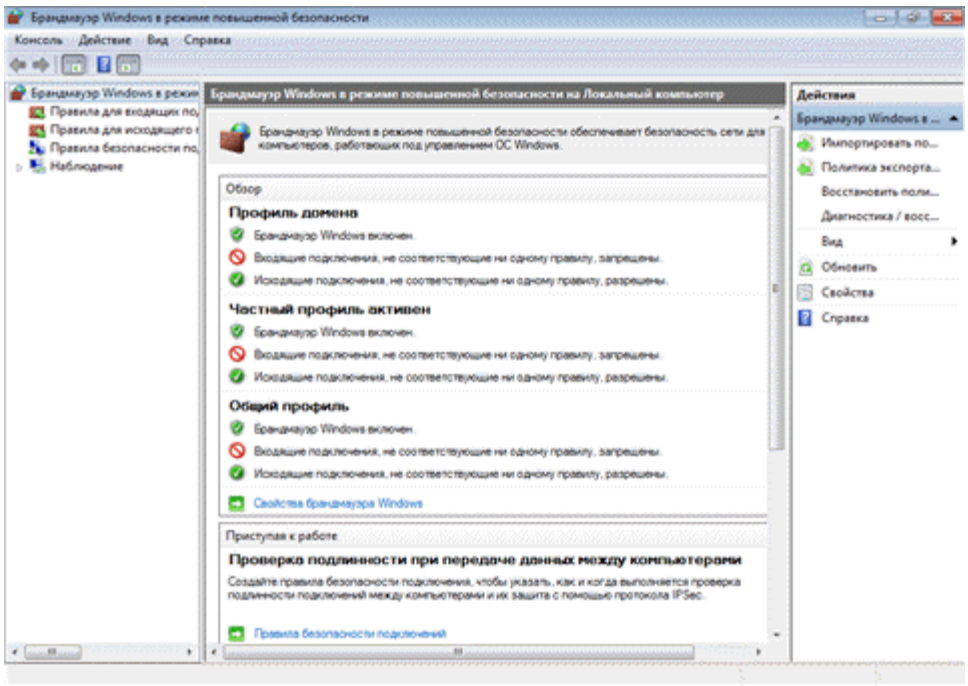


Рисунок 4.11 – Брандмауэр Windows в режиме повышенной безопасности

В брандмауэре Windows 7 произошло много изменений по сравнению с предыдущими версиями. Например, для каждого профиля фильтрация трафика возможна на основе:

- пользователей и групп службы каталогов Active Directory
- исходным и целевым IP-адресам
- IP-портам
- параметрам IPsec
- типам сетевых интерфейсов
- служб и т. д.

Рекомендация по использованию брандмауэра Windows 7 очень проста. Брандмауэр должен быть включен всегда, если вы не используете стороннее решение для защиты периметра. В большинстве случаев домашним пользователям подойдут стандартные параметры брандмауэра. Если же вы используете стороннее программное обеспечение, то при его установке встроенный брандмауэр, скорее всего, будет отключен, во избежание конфликтов между двумя программами, выполняющими одинаковую функцию.

Критерии оценивания
Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 23

«Работа с программой электронной почты»

Цель: Ознакомиться с основами работы с программами электронной почты, изучить настройку учетных записей, отправку и получение сообщений, организацию папок и управление контактами. Научиться эффективно использовать функции программы для работы с электронной почтой в рамках корпоративной или личной сети.

Время выполнения: 2 часа.

Оборудование:

- Компьютер или мобильное устройство с доступом в интернет.
- Программа для работы с электронной почтой (например, Microsoft Outlook, Mozilla Thunderbird или веб-клиент Gmail).

Ход работы:

Теоретические сведения:

1. Понятие электронной почты

Электронная почта (E-mail) – это способ передачи сообщений и файлов через сеть Интернет или локальные сети. Она используется для личной и деловой переписки, отправки уведомлений, обмена документами и прочего взаимодействия между пользователями.

2. Программы для работы с электронной почтой

Существует два основных способа работы с электронной почтой:

Веб-интерфейсы (Gmail, Яндекс.Почта, Mail.ru, Outlook.com и др.).

Клиентские программы (Microsoft Outlook, Mozilla Thunderbird, The Bat!, Apple Mail и др.).

3. Основные почтовые протоколы

При работе с почтовыми программами используются следующие протоколы:

SMTP (Simple Mail Transfer Protocol) – отправка почты.

POP3 (Post Office Protocol v3) – загрузка писем с сервера на локальный компьютер.

IMAP (Internet Message Access Protocol) – работа с почтой на сервере без её удаления (рекомендуется для многопользовательской работы).

4. Основные функции почтовых программ

Отправка и получение сообщений.

Создание и управление контактами.

Настройка фильтров и автоматической сортировки писем.

Работа с вложениями (файлы, изображения и др.).

Настройка электронной подписи и шифрования.

Использование папок для организации писем (входящие, отправленные, архив и т. д.).

5. Организация почтового ящика

Папки: Для удобства организации писем почтовые клиенты поддерживают создание папок (входящие, отправленные, черновики, спам и т.д.).

Подписи: Почтовые клиенты позволяют добавлять подписи в сообщения, что может быть полезно для создания фирменного стиля или автоматического добавления контактной информации.

Задание:

1. Настройка почтового клиента

В этом примере будет рассматриваться настройка почтового клиента Mozilla Thunderbird для работы с почтовым сервером Gmail.

Шаг 1. Установка почтового клиента

Скачайте и установите почтовый клиент Mozilla Thunderbird.

Запустите программу и выберите «Создать новый аккаунт».

Шаг 2. Ввод данных для настройки аккаунта

Введите имя, адрес электронной почты (например, username@gmail.com) и пароль.

Нажмите «Продолжить». Почтовый клиент автоматически определит параметры для подключения (для Gmail это будет сервер входящей почты imap.gmail.com и исходящей почты smtp.gmail.com).

Шаг 3. Завершение настройки

Введите пароль для вашего почтового ящика.

Завершите настройку, выбрав «Готово».

Шаг 4. Проверка подключения

После настройки почтовый клиент подключится к серверу, загрузит последние сообщения и синхронизирует почтовый ящик.

2. Отправка и получение сообщений

Отправка письма

Откройте почтовый клиент.

Нажмите на кнопку «Создать сообщение» или «Написать».

В поле "Кому" введите адрес получателя.

Введите тему письма в поле "Тема".

В основном поле сообщения напишите текст письма.

Если нужно, прикрепите файл (кнопка «Прикрепить файл»).

Нажмите «Отправить».

Получение письма

Нажмите кнопку "Получить почту" или дождитесь автоматического обновления почтового ящика.

Программа загрузит новые сообщения с почтового сервера.

Откройте письмо для чтения.

Ответ на письмо

Откройте полученное письмо.

Нажмите кнопку «Ответить» или «Ответить всем», если хотите ответить сразу нескольким получателям.

Напишите свой ответ в поле сообщения и нажмите «Отправить».

3. Организация почтового ящика

Создание папок

Для организации писем можно создавать новые папки (например, "Работа", "Личные").

В меню почтового клиента выберите «Папки» и нажмите «Создать папку».

Назовите папку и подтвердите создание.

Перемещение писем в папки

Перетащите письмо в нужную папку или используйте функцию «Переместить».

Таким образом, можно сортировать письма по категориям.

Использование фильтров и меток

Почтовые клиенты позволяют настроить автоматическую сортировку входящих писем по меткам или фильтрам.

Например, все письма от определённого отправителя могут автоматически перемещаться в папку «Работа».

4. Работа с вложениями

Отправка вложений

При написании письма нажмите кнопку «Прикрепить файл».

Выберите файл на вашем компьютере для отправки.

Вложения можно отправлять в различных форматах (например, документы, изображения, архивы).

Скачивание вложений

При открытии письма с вложением нажмите на иконку вложения.

Выберите, куда сохранить файл.

5. Безопасность работы с электронной почтой

Проверка на вирусы

Почтовые клиенты часто автоматически проверяют вложения на наличие вирусов.

При получении письма с вложением всегда проверяйте его на наличие вирусов, прежде чем открывать файл.

Использование шифрования

Для защиты личной переписки можно настроить шифрование с использованием PGP или S/MIME.

Шифрование доступно в некоторых почтовых клиентах, например, в Thunderbird.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания

Оценка «4» ставится, если выполнено не менее 80% заданий

Оценка «3» ставится, если выполнено не менее 60% заданий

Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 24

«Поиск информации в сети Интернет»

Цель: Ознакомиться с методами поиска информации в сети Интернет, изучить использование поисковых систем, фильтрацию результатов и оценку достоверности источников. Научиться эффективно находить необходимую информацию для решения различных задач и исследований.

Время выполнения: 2 часа.

Ход работы:

Задание:

Упражнение 1. Освоение элементарных приемов поиска информации в сети Интернет.
Цель упражнения: Изучение интерфейса, назначения и особенностей популярных поисковых систем («Яндекс» (www.yandex.ru), «Бинг» (www.bing.com), «Google» (www.google.ru). Разъяснение понятия «запрос», отличие запроса от вопроса.
Порядок выполнения:

1. Запустить браузер, установленный на компьютере.
2. В адресной строке окна браузера набрать адрес поисковой системы. Повторить п.п. 2 не менее трех раз, так чтобы были загружены все три поисковые системы.
3. Сравнить интерфейсы поисковых систем.
4. Организовать поиск следующей информации: **какое количество людей проживает в настоящее время на планете Земля.**
5. Данные поиска внести в таблицу:

	Yandex	Google	Bing
Запрос			
Количество ссылок			
Ответ (+ адрес сайта, номер ссылки)			

6. Сравнить результаты поиска, выбрать достоверный ответ.

Упражнение 2. Поиск в каталогах.
Цель упражнения: Освоение приёмов поиска информации через каталоги и применения средств простого поиска.
Задание:
Найти с помощью тематического поискового каталога:

1. Характеристики последней модели мобильного телефона известной фирмы (по вашему выбору);
2. Долгосрочный прогноз погоды в вашем регионе (не менее чем на 10 дней);
3. Информацию о вакансиях на должность учителя в вашем регионе.

Порядок выполнения:

1. Выберите любую поисковую систему.
2. В интерфейсе поисковой системы найти список тематических категорий и, продолжая погружаться в тему поиска, дойти до списка конкретных Web-страниц.
3. Если список страниц небольшой, выбрать среди них те ресурсы, которые лучше подходят для решения поставленной задачи. Если список ресурсов достаточно велик, необходимо в форме для поиска в строку ввода внести список ключевых слов, для уточнения поиска.

Упражнение 3. Освоение приемов поиска с помощью языка запросов.
Цель упражнения: Освоение приёмов поиска информации с помощью языка запросов поисковой системы Яндекс, формирование группы слов для организации простого поиска.
Задание:
1.Изучите правила формирования запросов в Яндексе, используя Яндекс.Помощь.
2. Составьте запрос на поиск информации по уходу за домашними кошками. Исключите из поиска крупных кошек (например, львов), а также предложения о покупке, продаже, фотографии для обоев и т. п.
Текст запроса и результат поиска оформите в виде таблицы:

Оператор	Текст запроса	Результат поиска

3.Найдите с помощью языка запросов **биографию** следующих людей (номер человека совпадает с номером компьютера):

1. Автора учебника информатики Семакина И.Г.
2. Автора учебника информатики Босовой Л.Л.
3. Изобретателя первой вычислительной машины Чарльза Беббиджа.
4. Ученого Джона фон Неймана.
5. Основателя теории информации Клода Шеннона.
6. Основателя Microsoft Билла Гейтса.
7. Изобретателя всемирной паутины Тимоти Бернерса-Ли.
8. Создателя антивирусной программы Евгения Касперского.
9. Основателя Apple Стива Джобса.
10. Разработчика поисковой машины Google Сергея Брина.

Биографию оформить в отдельном текстовом документе (шрифт Times New Roman, 12) под названием «*Биография …* (указать ФИО, например, «Биография Касперского Е.В.»)».
В биографии обязательно должны содержаться следующие сведения:

- Дата и место рождения,
- Сведения о родителях,
- Образование,
- Профессиональные труды и достижения,
- Фотография.

Критерии оценивания
Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 25

«Сетевая защита»

Цель: Ознакомиться с основными принципами и методами сетевой защиты, изучить различные инструменты и технологии для предотвращения угроз, таких как фаерволы, системы обнаружения вторжений (IDS), шифрование данных и аутентификация. Научиться применять средства защиты для обеспечения безопасности сети и предотвращения несанкционированного доступа.

Время выполнения: 4 часа.

Оборудование:

- Сетевое оборудование: Коммутатор, маршрутизатор, сервер (или виртуальные машины) с установленными ОС Linux или Windows.
- ПО для практики:
- Фаервол: iptables (Linux) или встроенный Windows Firewall.
- IDS/IPS: Snort (для Linux) или аналогичные решения.
- VPN-сервер: OpenVPN.
- Утилиты для тестирования: nmap, Wireshark.

Ход работы:

Теоретические сведения:

1. Понятие и задачи сетевой защиты

Сетевая защита – это совокупность мер, процедур и технологий, направленных на обеспечение безопасности информационных ресурсов сети. Основной целью является предотвращение несанкционированного доступа, защита данных от утечек, вирусных атак, DDoS-атак и других угроз.

Задачи сетевой защиты:

Обеспечение конфиденциальности, целостности и доступности данных.

Контроль доступа к ресурсам сети.

Обнаружение и предотвращение вторжений.

Мониторинг и анализ трафика для своевременного выявления аномалий.

Управление уязвимостями и реагирование на инциденты.

2. Основные методы и технологии сетевой защиты

Фаерволы (межсетевые экраны)

Назначение: Фаерволы фильтруют входящий и исходящий трафик согласно заданным политикам, блокируя подозрительные соединения.

Типы: Аппаратные (специальные устройства) и программные (например, iptables в Linux, Windows Firewall).

Системы обнаружения и предотвращения вторжений (IDS/IPS)

IDS (Intrusion Detection System): Обнаруживает подозрительные активности в сети и генерирует оповещения.

IPS (Intrusion Prevention System): Помимо обнаружения, активно блокирует атаки, фильтруя нежелательный трафик.

VPN (виртуальные частные сети)

Назначение: Обеспечивают защищённый туннель для передачи данных через публичные сети с использованием шифрования (протоколы IPSec, OpenVPN, SSL VPN).

Применение: Дистанционное подключение сотрудников к корпоративной сети, безопасный обмен данными между филиалами.

Антивирусы и системы предотвращения утечек данных (DLP)

Обеспечивают защиту конечных точек и анализируют сетевой трафик для обнаружения вредоносного кода и утечек информации.

Шифрование и аутентификация

Шифрование данных: Использование протоколов SSL/TLS, SSH для защиты передаваемой информации.

Многофакторная аутентификация: Повышает безопасность доступа к ресурсам сети.

Политики безопасности и мониторинг

Регулярный анализ логов, аудит конфигураций, обновление программного обеспечения и установка патчей.

Использование SIEM-систем (Security Information and Event Management) для централизованного мониторинга и корреляции событий.

Задание:

1. Настройка базового фаервола (на примере iptables в Linux)

Просмотр текущих правил

```
sudo iptables -L -n -v
```

Добавление правил для блокировки нежелательного трафика:

Блокировка входящего трафика по умолчанию:

```
sudo iptables -P INPUT DROP
sudo iptables -P FORWARD DROP
sudo iptables -P OUTPUT ACCEPT
```

Разрешение входящего трафика для уже установленных соединений:

```
sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Разрешение SSH-доступа (порт 22)

```
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

Сохранение правил (в зависимости от дистрибутива, например, для Ubuntu):

```
sudo sh -c "iptables-save > /etc/iptables/rules.v4"
```

2. Настройка системы обнаружения вторжений (Snort)

Установка Snort:

На Ubuntu

```
sudo apt-get update
sudo apt-get install snort
```

Первичная настройка Snort:

При установке укажите сеть, которую необходимо мониторить (например, 192.168.1.0/24).

Отредактируйте основной конфигурационный файл /etc/snort/snort.conf для корректного определения сети и путей к правилам.

Запуск Snort в режиме прослушивания:

```
sudo snort -A console -q -c /etc/snort/snort.conf -i eth0
```

Опция -A console выводит оповещения в консоль, -q – тихий режим, -i – интерфейс для мониторинга.

3. Настройка VPN-соединения с использованием OpenVPN

Установка OpenVPN (на сервере Ubuntu):

```
sudo apt-get update
sudo apt-get install openvpn easy-rsa
```

Настройка PKI (Public Key Infrastructure):

Скопируйте пример конфигурационных файлов и инициализируйте PKI

```
make-cadir ~/openvpn-ca
cd ~/openvpn-ca
source vars
./clean-all
./build-ca
./build-key-server server
./build-dh
./build-key client1
```

Настройка конфигурационного файла сервера:

Скопируйте пример конфигурации:

```
cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz ~/openvpn-ca/
gunzip server.conf.gz
```

Отредактируйте server.conf, указав пути к сертификатам и ключам, настройте диапазон IP-адресов для клиентов.

Запуск OpenVPN-сервера

```
sudo openvpn --config /path/to/server.conf
```

Настройка клиента:

Скопируйте на клиентскую машину соответствующие сертификаты, ключи и пример конфигурационного файла клиента, отредактируйте его для подключения к VPN-серверу.

4. Тестирование настроек сетевой защиты

Проверка работы фаервола:

Используйте утилиту nmap с другого компьютера для сканирования открытых портов

```
nmap -Pn 192.168.1.X
```

Убедитесь, что нежелательные порты закрыты.

Мониторинг событий IDS/IPS:

Запустите Snort и сгенерируйте тестовый трафик (например, с помощью утилиты nmap или специальных скриптов) для проверки срабатывания правил.

Проверка VPN-соединения:

Подключитесь с клиентского устройства к VPN-серверу и убедитесь, что весь трафик проходит через VPN (проверьте IP-адрес, доступность внутренних ресурсов).

Критерии оценивания

Оценка «5» ставится, если выполнены все задания

Оценка «4» ставится, если выполнено не менее 80% заданий

Оценка «3» ставится, если выполнено не менее 60% заданий

Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 26

«Брэндмауэры, антивирусное ПО»

Цель: Изучение вредоносных программ и антивирусного программного обеспечения.

Время выполнения: 6 часов.

Ход работы:

Теоретические сведения:

Вредоносная программа — компьютерная программа или переносной код, предназначенный для реализации угроз информации, хранящейся в компьютерной системе, либо для скрытого нецелевого использования ресурсов системы, либо иного воздействия, препятствующего нормальному функционированию компьютерной системы. К вредоносному программному обеспечению относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

Независимо от типа, вредоносные программы способны наносить значительный ущерб, реализуя любые угрозы информации — угрозы нарушения целостности, конфиденциальности, доступности.

1. Сетевые черви. К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

- ✓ проникновения на удаленные компьютеры;
- ✓ запуска своей копии на удаленном компьютере;
- ✓ дальнейшего распространения на другие компьютеры в сети.

Для своего распространения сетевые черви используют разнообразные компьютерные и мобильные сети: электронную почту, системы обмена мгновенными сообщениями, файлообменные (P2P) и IRC-сети, LAN, сети обмена данными между мобильными устройствами (телефонами, карманными компьютерами) и т. д.

Некоторые черви обладают свойствами других разновидностей вредоносного программного обеспечения. Например, некоторые черви содержат троянские функции или способны заражать выполняемые файлы на локальном диске, т. е. имеют свойство троянской программы и/или компьютерного вируса.

2. Классические компьютерные вирусы. К данной категории относятся программы, распространяющие свои копии по ресурсам локального компьютера с целью:

- ✓ последующего запуска своего кода при каких-либо действиях пользователя;
- ✓ дальнейшего внедрения в другие ресурсы компьютера.

В отличие от червей, вирусы не используют сетевых сервисов для проникновения на другие компьютеры. Копия вируса попадает на удалённые компьютеры только в том случае, если зараженный объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например:

✓ при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;
✓ вирус скопировал себя на съёмный носитель или заразил файлы на нем;
✓ пользователь отослал электронное письмо с зараженным вложением.

3. Троянские программы. В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера (например, троянские программы, разработанные для массированных DoS-атак на удалённые ресурсы сети).

4. Хакерские утилиты и прочие вредоносные программы. К данной категории относятся:

✓ утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);
✓ программные библиотеки, разработанные для создания вредоносного ПО;
✓ хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
✓ «злые шутки», затрудняющие работу с компьютером;
✓ программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
✓ прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удалённым компьютерам.

Руткит (Rootkit) - программа или набор программ, использующих технологии сокрытия системных объектов (файлов, процессов, драйверов, сервисов, ключей реестра, открытых портов, соединений и пр.) посредством обхода механизмов системы.

В системе Windows под термином руткит принято считать программу, которая внедряется в систему и перехватывает системные функции, или производит замену системных библиотек. Перехват и модификация низкоуровневых API функций в первую очередь позволяет такой программе достаточно качественно маскировать свое присутствие в системе, защищая ее от обнаружения пользователем и антивирусным ПО. Кроме того, многие руткиты могут маскировать присутствие в системе любых описанных в его конфигурации процессов, папок и файлов на диске, ключей в реестре. Многие руткиты устанавливают в систему свои драйверы и сервисы (они естественно также являются «невидимыми»).

В последнее время угроза руткитов становится все более актуальной, т.к. разработчики вирусов, троянских программ и шпионского программного обеспечения начинают встраивать руткит-технологии в свои вредоносные программы. Одним из классических примеров может служить троянская программа Trojan-Spy.Win32.Qukart, которая маскирует свое присутствие в системе при помощи руткит-технологии. Ее RootKit-механизм прекрасно работает в Windows 95, 98, ME, 2000 и XP.

Современные антивирусные программы обеспечивают комплексную защиту программ и данных на компьютере от всех типов вредоносных программ и методов их проникновения на компьютер (Интернет, локальная сеть, электронная почта, съемные

носители информации). Большинство антивирусных программ сочетает в себе функции постоянной защиты (антивирусный монитор) и функции защиты по требованию пользователя (антивирусный сканер).

Межсетевой экран — это программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа к компьютеру. Другое распространенное название сетевого экрана — файервол от английского термина firewall. Иногда сетевой экран называют еще брандмауэром (нем. brandmauer) — это немецкий эквивалент слова firewall. Основная задача сетевого экрана — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации сетевого экрана. Межсетевой экран позволяет:

- ✓ Блокировать хакерские атаки;
- ✓ Не допускать проникновение сетевых червей;
- ✓ Препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере.

Задание. В операционной системе Windows проверить выбранные объекты на наличие вредоносных объектов, выполнить лечение или удаление зараженных объектов

Порядок работы

1) Запустить на выполнение антивирусную программу.
2) Запустить обновление из контекстного меню.
3) Выполнить проверку съемного носителя.
4) Выполнить проверку локального диска.
5) Отчет о работе антивирусной содержит информацию о результатах проверки.

Контрольные вопросы

1. Дайте понятие компьютерного вируса.
2. Какие угрозы информации способны нанести вредоносные программы?
3. Для чего предназначены антивирусные программы?
4. Каковы функции брандмауэра?
5. В чем разница между антивирусными сканерами и мониторами?
6. Какие существуют признаки заражения компьютерным вирусом?
7. Что необходимо сделать в первую очередь в случае заражения компьютерным вирусом?
8. Каковы характерные особенности компьютерных вирусов как типа вредоносных программ?
9. Какие существуют типы компьютерных вирусов?
10. Как сетевые черви проникают на компьютер?
11. Какие вредоносные действия выполняют троянские программы?
12. Какие типы хакерских атак и методы защиты от них существуют?
13. К какому типу вредоносных программ относятся руткиты?
14. Приведите классификацию антивирусных программ. Приведите примеры.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания
Оценка «4» ставится, если выполнено не менее 80% заданий
Оценка «3» ставится, если выполнено не менее 60% заданий
Оценка «2» ставится, если выполнено менее 60% заданий

Практическая работа № 27

«Защита от шпионского ПО»

Цель: Ознакомиться с методами защиты от шпионского ПО (spyware), изучить способы его обнаружения и предотвращения. Научиться использовать антивирусные и антишпионские программы, а также настраивать систему безопасности для защиты личных данных и предотвращения утечек информации.

Время выполнения: 6 часов.

Оборудование:

- Компьютер под управлением ОС (Windows, Linux или macOS).
- Программное обеспечение:
- Антивирусное ПО с функциями обнаружения шпионского ПО (например, Windows Defender, Malwarebytes, Spybot Search & Destroy).
- Обновлённые базы данных антивируса/антишпионского ПО.
- Доступ к интернету для обновления программного обеспечения и загрузки обновлений.

Ход работы:

Теоретические сведения:

1. Определение шпионского ПО

Шпионское ПО (Spyware) – это тип вредоносного программного обеспечения, которое тайно устанавливается на компьютер пользователя с целью сбора информации, мониторинга активности, перехвата личных данных (паролей, финансовой информации и т.д.) и передачи их злоумышленнику.

Шпионские программы могут работать в фоновом режиме, оставаясь незаметными для пользователя.

2. Основные цели и последствия работы шпионского ПО

Сбор личной и конфиденциальной информации: пароли, банковские данные, историю браузера, личные сообщения.

Нарушение конфиденциальности: передача данных без ведома пользователя.

Снижение производительности системы: потребление системных ресурсов и замедление работы компьютера.

Финансовые потери и кража личных данных: риск несанкционированных переводов, мошеннических операций и утечки коммерческой тайны.

3. Методы распространения шпионского ПО

Фишинговые рассылки и вредоносные ссылки: получение доступа через электронную почту или социальные сети.

Уязвимости в программном обеспечении: использование эксплойтов для установки вредоносного кода.

Скачивание программ с ненадежных источников: установка «бесплатных» программ, в которых скрыт шпионский модуль.

Использование пиратского программного обеспечения: нелегальные копии программ могут содержать встроенное шпионское ПО.

4. Методы защиты от шпионского ПО

Антивирусные и антишпионские программы: регулярное обновление антивирусных баз, использование специализированных средств (например, Malwarebytes, Spybot Search & Destroy, Windows Defender).

Обновление программного обеспечения: своевременное обновление операционной системы и установленных программ для устранения известных уязвимостей.

Бдительность пользователя: осторожность при открытии вложений, переходе по ссылкам, скачивании программ из недоверенных источников.

Использование сетевых фильтров и брандмауэров: блокирование подозрительного трафика и предотвращение несанкционированного доступа.

Настройка политики безопасности: ограничение прав пользователей, контроль за установкой программ и регулярный аудит системы.

Задание:

1. Подготовительный этап

1.1. Обновление операционной системы и программного обеспечения

Убедитесь, что установлены все актуальные обновления ОС и используемых приложений.

Проверьте настройки автоматического обновления, чтобы своевременно получать патчи безопасности.

1.2. Установка и обновление антивирусного/антишпионского ПО

Если на компьютере ещё не установлено специальное ПО для защиты от шпионского ПО, скачайте и установите его с официального сайта.

Запустите программу и обновите вирусные базы (обычно функция обновления доступна в главном меню).

2. Сканирование системы на наличие шпионского ПО

2.1. Полное сканирование системы

Откройте установленное антивирусное/антишпионское приложение.

Выберите режим «Полное сканирование» или «Глубокое сканирование».

Запустите процесс сканирования и дождитесь его завершения.

Просмотрите отчёт сканирования – если найдены подозрительные или вредоносные файлы, программа предложит варианты удаления или помещение в карантин.

2.2. Пример работы с Malwarebytes (Windows)

Запуск программы:

Откройте Malwarebytes через ярлык на рабочем столе или из меню «Пуск».

Обновление базы данных:

Нажмите кнопку «Обновить» и дождитесь окончания процесса.

Запуск сканирования:

Выберите «Сканирование системы» или «Полное сканирование».

Дождитесь завершения сканирования – это может занять от нескольких минут до получаса в зависимости от объёма данных.

Анализ результатов:

После завершения сканирования программа отобразит найденные угрозы.

Выберите действие для каждого найденного объекта (удаление, помещение в карантин или игнорирование, если объект оказался ложным срабатыванием).

Перезагрузка компьютера (при необходимости):

Если программа рекомендует перезагрузку системы для завершения удаления угроз, сохраните все данные и перезагрузите компьютер.

3. Дополнительные меры по защите системы

3.1. Настройка брандмауэра

Проверьте настройки встроенного брандмауэра Windows или другого используемого решения.

Убедитесь, что в правилах брандмауэра нет исключений для подозрительных программ или портов.

3.2. Ограничение прав пользователя

Создайте учетную запись с ограниченными правами для повседневной работы (без прав администратора), чтобы снизить риск установки шпионского ПО через уязвимости.

Используйте учетную запись администратора только для установки и обновления программного обеспечения.

3.3. Контроль установленных программ

Регулярно проверяйте список установленных программ и удаляйте неиспользуемые или подозрительные приложения.

Используйте инструменты типа «Программы и компоненты» в Windows для анализа установленных приложений.

4. Тестирование эффективности защиты

После выполнения вышеуказанных шагов рекомендуется провести повторное сканирование системы для подтверждения отсутствия шпионского ПО.

Можно также использовать онлайн-сервисы проверки (например, VirusTotal) для анализа подозрительных файлов:

Сохраните файл с обнаруженной угрозой (если он не был автоматически удалён).

Загрузите его на VirusTotal для многоплатформенного сканирования.

Критерии оценивания

Оценка «5» ставится, если выполнены все задания

Оценка «4» ставится, если выполнено не менее 80% заданий

Оценка «3» ставится, если выполнено не менее 60% заданий

Оценка «2» ставится, если выполнено менее 60% заданий