Министерство образования и науки Российской Федерации

**Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Тамбовский государственный технический университет»**

СЕТИ ЭВМ И СРЕДСТВА КОММУНИКАЦИЙ

*Методические указания для студентов,
обучающихся по направлениям 221400, 190600, 190700*

Тамбов
•Издательство ФГБОУ ВПО «ТГТУ»•
2012

УДК 004.7(076)
ББК з973.202я73-5
Б20

Р е ц е н з е н т
Доктор технических наук, профессор ФГБОУ ВПО «ТГТУ»,
и.о. заведующего кафедрой УКиС
С.В. Пономарев

С о с т а в и т е л ь
П.В. Балабанов

Б20 Сети ЭВМ и средства коммуникаций : методические указания / сост. П.В. Балабанов. – Тамбов : Изд-во ФГБОУ ВПО «ТГТУ», 2012. – 44 с. – 80 экз.

Содержат указания к выполнению 23 практических работ, направленных на изучение аппаратных и программных средств современных вычислительных сетей.

Предназначены для студентов, обучающихся по направлениям 221400, 190600, 190700.

УДК 004.7(076)
ББК з973.202я73-5

ПРАКТИЧЕСКИЕ РАБОТЫ

Практическая работа 1

ТЕСТИРОВАНИЕ АППАРАТНЫХ СРЕДСТВ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ

Цель работы: научиться определять основные технические характеристики аппаратных средств современного персонального компьютера.

Задание

1. Изучить методические указания и рекомендуемую литературу.
2. При помощи программы «Everest» собрать данные о технических характеристиках персонального компьютера.

Методические указания

К основным составным частям персонального компьютера относят: системный блок, монитор, клавиатуру, мышь. В свою очередь, системный блок состоит из материнской (системной) платы на которой установлены центральный процессор, оперативная память, платы расширения (звуковой адаптер, видеоадаптер, сетевой адаптер и т.д.), блока питания, жесткого диска, оптического привода и др.

Рассмотрим состав, назначение и характеристики некоторых основных компонентов системного блока.

Системная плата (рис. 1) – это сложная многослойная печатная плата, на которой устанавливаются основные компоненты персонального компьютера (центральный процессор ЦП, контроллер оперативного запоминающего устройства ОЗУ и собственно ОЗУ, загрузочное постоянное запоминающее устройство ПЗУ, контроллеры базовых интерфейсов ввода-вывода).

Быстродействие различных компонентов компьютера (процессора, оперативной памяти и контроллеров периферийных устройств) может существенно различаться. Для согласования быстродействия на системной плате устанавливаются специальные микросхемы (чипсеты), включающие в себя контроллер оперативной памяти (так называемый северный мост) и контроллер периферийных устройств (южный мост).

Северный мост обеспечивает обмен информацией между процессором и оперативной памятью по системной шине. В процессоре используется внутреннее умножение частоты, поэтому частота процессора в несколько раз больше, чем частота системной шины. В современных компьютерах частота процессора может превышать частоту системной шины в 10 раз (например, частота процессора 1 ГГц, а частота шины – 100 МГц).

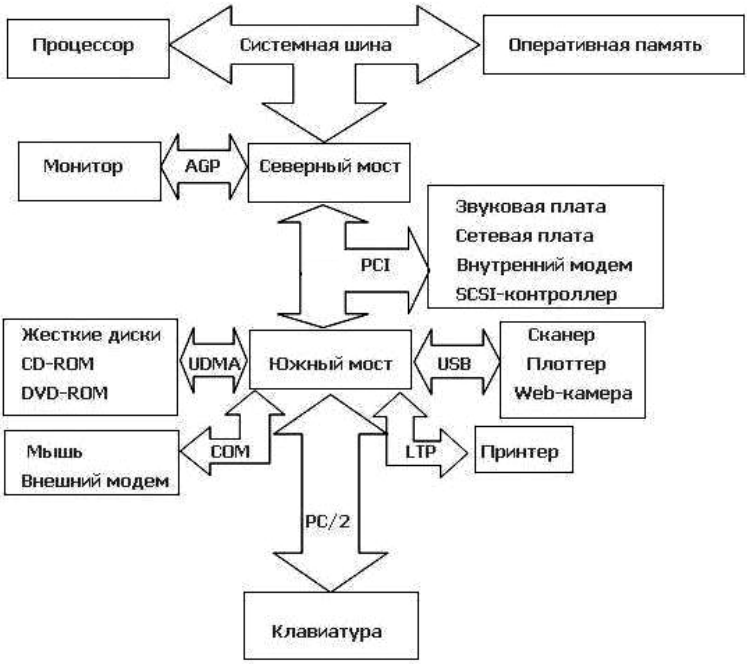


Рис. 1. Логическая схема системной платы

К северному мосту подключается шина PCI (Peripherial Component Interconnect bus – шина взаимодействия периферийных устройств), которая обеспечивает обмен информацией с контроллерами периферийных устройств. Частота контроллеров меньше частоты системной шины, например, если частота системной шины составляет 100 МГц, то частота шины PCI обычно в три раза меньше – 33 МГц. Контроллеры периферийных устройств (звуковая плата, сетевая плата, SCSI-контроллер, внутренний модем) устанавливаются в слоты расширения системной платы.

По мере увеличения разрешающей способности монитора и глубины цвета требования к быстродействию шины, связывающей видеоплату с процессором и оперативной памятью, возрастают. На рисунке 1 для подключения видеоплаты используется специальная шина AGP (Accelerated Graphic Port – ускоренный графический порт), соединенная с северным мостом и имеющая частоту, в несколько раз большую, чем шина PCI.

Южный мост обеспечивает обмен информацией между северным мостом и портами для подключения периферийного оборудования.

Устройства хранения информации (жесткие диски, CD-ROM, DVD-ROM) подключаются к южному мосту по шине UDMA (Ultra Direct Memory Access – прямое подключение к памяти).

Мышь и внешний модем подключаются к южному мосту с помощью последовательных портов, которые передают электрические импульсы, несущие информацию в машинном коде, последовательно один за другим. Обозначаются последовательные порты как COM1 и COM2, а аппаратно реализуются с помощью 25-контактного и 9-контактного разъемов, которые выведены на заднюю панель системного блока.

Принтер подключается к параллельному порту, который обеспечивает более высокую скорость передачи информации, чем последовательные порты, так как передает одновременно 8 электрических импульсов, несущих информацию в машинном коде. Обозначается параллельный порт как LTP, а аппаратно реализуется в виде 25-контактного разъёма на задней панели системного блока.

Для подключения сканеров и цифровых камер обычно используется порт USB (Universal Serial Bus – универсальная последовательная шина), который обеспечивает высокоскоростное подключение к компьютеру сразу нескольких периферийных устройств. Клавиатура подключается обычно с помощью порта PS/2.

Системные платы классифицируются по форм-фактору.

Форм-фактор материнской платы – стандарт, определяющий размеры материнской платы для персонального компьютера, места ее крепления к корпусу, расположение на ней интерфейсов шин, портов ввода/вывода, сокета центрального процессора и слотов для оперативной памяти, а также тип разъема для подключения блока питания.

Примерами обозначения форм-факторов могут быть:

- устаревшие: Baby-AT; Mini-ATX; полноразмерная плата AT; LPX;
- современные: ATX; microATX; Flex-ATX; NLX; WTX, CEB;
- внедряемые: Mini-ITX и Nano-ITX; Pico-ITX; BTX, MicroBTX и PicoBTX.

Центральный процессор – центральное вычислительное устройство, исполнитель машинных инструкций, часть аппаратного обеспечения компьютера или программируемого логического контроллера, отвечающая за выполнение операций, заданных программами.

В настоящее время используются многоядерные процессоры на одном или нескольких кристаллах.

Для повышения быстродействия используют так называемое кэширование. Кэширование – это использование дополнительной быстродействующей памяти (кеш-памяти) для хранения копий блоков информации из основной (оперативной) памяти, вероятность обращения к которым в ближайшее время велика.

Оперативная память – это рабочая область для процессора компьютера. В ней во время работы хранятся программы и данные. Оперативная память часто рассматривается как временное хранилище, потому что данные и программы в ней сохраняются только при включенном компьютере или до нажатия кнопки сброса (reset). Перед выключением или нажатием кнопки сброса все данные, подвергнутые изменениям во время работы, необходимо сохранить на запоминающем устройстве, которое может хранить информацию постоянно (обычно это жесткий диск). При новом включении питания сохраненная информация вновь может быть загружена в память.

Устройства оперативной памяти иногда называют запоминающими устройствами с произвольным доступом. Это означает, что обращение к данным, хранящимся в оперативной памяти, не зависит от порядка их расположения в ней.

В современных компьютерах используются запоминающие устройства трех основных типов.

- **ROM (Read Only Memory)**. Постоянное запоминающее устройство – ПЗУ, не способное выполнять операцию записи данных.
- **DRAM (Dynamic Random Access Memory)**. Динамическое запоминающее устройство с произвольным порядком выборки.
- **SRAM (Static RAM)**. Статическая оперативная память.

В памяти типа ROM данные можно только хранить. Именно поэтому такая память используется только для чтения данных. ROM также часто называется *энергонезависимой памятью*, потому что любые данные, записанные в нее, сохраняются при выключении питания. Поэтому в ROM помещаются команды запуска персонального компьютера, т.е. программное обеспечение, которое загружает систему.

Основной код BIOS содержится в микросхеме ROM на системной плате, но на платах адаптеров также имеются аналогичные микросхемы. Они содержат вспомогательные подпрограммы базовой системы ввода-вывода и драйверы, необходимые для конкретной платы, особенно для тех плат, которые должны быть активизированы на раннем этапе начальной загрузки, например видеоадаптер.

Динамическая оперативная память DRAM используется в большинстве систем оперативной памяти современных персональных компьютеров. Основное преимущество памяти этого типа состоит в том, что ее ячейки упакованы очень плотно, т.е. в небольшую микросхему можно упаковать много битов, а значит, на их основе можно построить память большой емкости.

Ячейки памяти в микросхеме DRAM – это крошечные конденсаторы, которые удерживают заряды. Именно так (наличием или отсутствием зарядов) и кодируются биты. Проблемы, связанные с памятью этого типа, вызваны тем, что она динамическая, т.е. должна постоянно

регенерироваться, так как в противном случае электрические заряды в конденсаторах памяти будут «стекать» и данные будут потеряны.

Статическая оперативная память SRAM названа так потому, что, в отличие от динамической оперативной памяти, для сохранения ее содержимого не требуется периодической регенерации. Но это не единственное её преимущество. SRAM имеет более высокое быстродействие, чем динамическая оперативная память, и может работать на той же частоте, что и современные процессоры.

Однако для хранения каждого бита в конструкции SRAM используется кластер из шести транзисторов. Использование транзисторов без каких-либо конденсаторов означает, что нет необходимости в регенерации. Почему же тогда микросхемы SRAM не используются для всей системной памяти? Ответ прост. По сравнению с динамической оперативной памятью быстродействие SRAM намного выше, но плотность её гораздо ниже, а цена довольно высока. Более низкая плотность означает, что микросхемы SRAM имеют большие габариты, хотя их информационная ёмкость намного меньше. Все это не позволяет использовать память типа SRAM в качестве оперативной памяти в персональных компьютерах.

Жёсткий диск – энергонезависимое перезаписываемое компьютерное запоминающее устройство. Является основным накопителем данных практически во всех компьютерах. Жёсткий диск состоит из гермозоны и блока электроники.

Гермозона включает в себя корпус из прочного сплава, собственно диски (пластины) с магнитным покрытием, блок головок с устройством позиционирования, электропривод шпинделя.

Блок головок – пакет рычагов из пружинистой стали (по паре на каждый диск). Одним концом они закреплены на оси рядом с краем диска. На других концах (над дисками) закреплены головки.

Диски (пластины), как правило, изготовлены из металлического сплава. Хотя были попытки делать их из пластика и даже стекла, но такие пластины оказались хрупкими и недолговечными. Обе плоскости пластин, подобно магнитофонной ленте, покрыты тончайшей пылью ферромагнетика – окислов железа, марганца и других металлов. Точный состав и технология нанесения держатся в секрете.

Диски жёстко закреплены на шпинделе. Во время работы шпиндель вращается со скоростью несколько тысяч оборотов в минуту (4200, 5400, 7200, 10 000, 15 000). При такой скорости вблизи поверхности пластины создаётся мощный воздушный поток, который приподнимает головки и заставляет их парить над поверхностью пластины. Форма головок рассчитывается так, чтобы при работе обеспечить оптимальное расстояние от пластины. Пока диски не разогнались до скорости, необходимой для «взлёта» головок, парковочное устройство

удерживает головки в зоне парковки. Это предотвращает повреждение головок и рабочей поверхности пластин.

Устройство позиционирования головок состоит из неподвижной пары сильных, как правило неодимовых, постоянных магнитов и катушки на подвижном блоке головок.

Блок электроники обычно содержит: управляющий блок, постоянное запоминающее устройство (ПЗУ), буферную память, интерфейсный блок и блок цифровой обработки сигнала.

Интерфейсный блок обеспечивает сопряжение электроники жёсткого диска с остальной системой.

Блок управления представляет собой систему управления, принимающую электрические сигналы позиционирования головок, и вырабатывающую управляющие воздействия приводом типа «звуковая катушка», коммутации информационных потоков с различных головок, управления работой всех остальных узлов (к примеру, управление скоростью вращения шпинделя).

Блок ПЗУ хранит управляющие программы для блоков управления и цифровой обработки сигнала, а также служебную информацию винчестера.

Буферная память сглаживает разницу скоростей интерфейсной части и накопителя (используется быстродействующая статическая память). Увеличение размера буферной памяти в некоторых случаях позволяет увеличить скорость работы накопителя.

Блок цифровой обработки сигнала осуществляет очистку считанного аналогового сигнала и его декодирование (извлечение цифровой информации).

Сетевая плата (адаптер) – периферийное устройство, позволяющее компьютеру взаимодействовать с другими устройствами сети.

Звуковая карта – плата, которая позволяет работать со звуком на компьютере. В настоящее время звуковые карты бывают как встроенными в материнскую плату, так и отдельными платами расширения или как внешними устройствами.

Видеокарта (**видеоадаптер**) – устройство, преобразующее изображение, находящееся в памяти компьютера, в видеосигнал для монитора.

Более полную информацию по компонентам компьютера и, в частности, системного блока можно найти на сайтах сети Интернет [1, 2, 3, 4].

Порядок выполнения работы

1. Запустить программу Everest на тестируемом компьютере и с помощью мастера отчетов (меню «Отчёт») сформировать отчет об аппаратном обеспечении.

2. Заполнить табл. 1.

1. Результаты выполнения работы

№	Наименование компонента системного блока или характеристика	Найденное обозначение или характеристика
1	Тип ЦП, частота	
2	Тип системной платы, форм-фактор	
3	Чипсет системной платы	
4	Тип жесткого диска, объем	
5	Тип сетевого адаптера	
6	Тип видеоадаптера	
7	Тип звукового адаптера	
8	Разъемы ОЗУ	
9	Разъемы расширения системной платы	
10	Объем кэш-памяти процессора	

Контрольные вопросы

1. Назначение и компоненты системной платы.
2. Что такое северный мост? Его назначение.
3. Что такое южный мост? Его назначение.
4. Что такое форм-фактор материнской платы?
5. Назначение центрального процессора.
6. Что такое многоядерный процессор?
7. Что такое кэширование?
8. Оперативное запоминающее устройство. Его назначение.
9. Что такое энергозависимые и энергонезависимые запоминающие устройства?
10. Универсальная последовательная шина USB.
11. Шина ввода-вывода PCI и PCI-Express.
12. Шина AGP.
13. Видеокарта. Назначение и устройство.
14. Сетевой адаптер. Назначение, типы, параметры и функции.
15. Назначение и типы оптических приводов.
16. Жёсткий диск. Назначение и устройство.

Практическая работа 2

СЕТЕВЫЕ ТОПОЛОГИИ

Цель работы: изучить правила организации физического расположения в пространстве компьютеров, объединенных в сеть.

Задание

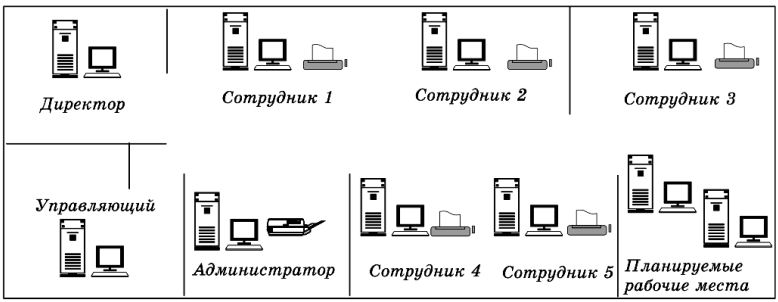
1. Подготовьте доклад с презентацией на одну из тем, приведенных ниже. Тему утвердите у преподавателя.
2. Выполните практическое задание.

Список тем доклада:

1. Базовые сетевые топологии. Шина. Преимущества и недостатки.
2. Базовые сетевые топологии. Кольцо. Преимущества и недостатки.
3. Базовые сетевые топологии. Звезда. Преимущества и недостатки.
4. Топология «дерево».
5. Сеть с сетчатой топологией.
6. Доступ к среде передачи.

Практическое задание

Вам поручено установить сеть для небольшой, но развивающейся компании, занимающей половину этажа. В состав компании входят директор, управляющий, администратор и пять сотрудников. Планируется принять на работу еще двух сотрудников. У каждого сотрудника есть компьютер. Если необходимо обменяться информацией приходится делать это устно или с использованием съемных носителей, что неудобно. Лазерный принтер имеются у администратора. У каждого сотрудника имеется сканер. Какую топологию вы предложите для компании? Оцените суммарную длину кабеля в каждом из предложенных случаев и выберите оптимальный вариант.



Контрольные вопросы

1. Нарисуйте схему сети, построенной по топологии типа шина. Сеть должна включать 5 компьютеров.
2. Имеются 3 компьютера, расположенных на расстоянии 200 м друг от друга. Какую топологию вы выберете для создания сети?

3. Имеется комната площадью 20 м^2. В ней необходимо поставить 10 компьютеров, объединенных сетью. Нарисуйте схему сети.

4. Нарисуйте схему сети, построенной по топологии типа звезда. Сеть должна включать 5 компьютеров.

5. В организации имеется 3 отдела. В каждом отделе по 8 компьютеров. Все отделы расположены на одном этаже здания. Зарисуйте схему сети.

Практическая работа 3

ЛИНИИ СВЯЗИ

Цель работы: изучить типовые линии связи, применяемые в компьютерных сетях.

Задание

1. Подготовьте доклад с презентацией на одну из тем, приведенных ниже.

2. Выполните практическое задание.

Список тем доклада:

1. Коаксиальный кабель (тонкий и толстый). Терминаторы. Примеры сетей на тонком и толстом коаксиальном кабеле.

2. Витая пара. Категории. Разводка проводников в коннекторах RJ-45.

3. Оптоволоконные кабели. Коннекторы для оптоволоконных кабелей.

4. Беспроводные линии.

Практическое задание

Для ранее разработанной сети (см. практическое занятие 2) составить проект прокладки кабеля витая пара категории 5 в кабельных каналах, согласно выбранной вами сетевой топологии.

Контрольные вопросы

1. В чем отличия тонкого и толстого коаксиального кабеля?
2. Зачем нужны терминаторы?
3. Что такое витая пара?
4. Зачем необходимо экранировать витую пару?
5. В чем преимущество оптоволоконного кабеля по сравнению с витой парой?

АДРЕСАЦИЯ В КОМПЬЮТЕРНОЙ СЕТИ

Цель работы: Изучить способы адресации в IP-сетях.

Задание

1. Изучить методические указания и рекомендуемую литературу.
2. Начертить схему локальной сети компьютерного класса.

Методические указания

В компьютерной сети передача информации от одного узла (компьютера) к другому узлу осуществляется посредством пакетов. Пакет можно рассматривать как набор битов служебной информации и информации, подлежащей передаче. К служебной информации относятся адрес узла источника пакета и адрес узла назначения, длина пакета и др., а в качестве примера информации, подлежащей передаче, можно указать часть текста электронного письма.

Пакет должен быть доставлен из пункта отправки в пункт назначения. Для этого используется адресация TCP/IP.

TCP/IP – Transmission Control Protocol/Internet Protocol (протокол управления передачей/межсетевой протокол). TCP/IP часто называют протоколом открытых систем.

TCP/IP представляет собой набор (стек) протоколов, обеспечивающих связь компьютеров (и других устройств) в сети Internet. Семейство TCP/IP состоит из многих протоколов (более двух десятков), и каждый занят своим делом. Каждый переносит сетевые данные в различных форматах и обладает различными возможностями. В зависимости от требований приложения для передачи данных по Internet используется определенный протокол из семейства TCP/IP. Семейство включает в себя протокол контроля транспортировки (TCP), адресный протокол Internet (IP) и множество других протоколов. Все они предназначены для передачи сообщений в сети Internet.

Адрес IP – это 32-разрядное значение, которое используется для правильной идентификации источника и адреса пункта назначения. Адрес IP обычно представляется в следующем виде 204.107.2.100. Адрес можно разбить на четыре позиции по восемь битов каждая, а можно представить в двоичном коде. Эти позиции называют октетами. В приведенном примере IP-адреса число 204 – значение первого октета, а 100 – четвертого. Приведенный в примере IP-адрес можно легко записать в двоичном виде (для преобразования десятичной системы

счисления в двоичную можно воспользоваться утилитой «Калькулятор» операционной системы Windows)

11001100.01101011.00000010.01100100

IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором сети произвольно, либо назначен по рекомендации специального подразделения Internet (Network Information Center, NIC), если сеть должна работать как составная часть Internet. Обычно провайдеры услуг Internet получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами.

Номер узла в протоколе IP назначается независимо от локального адреса узла. Деление IP-адреса на поле номера сети и номера узла – гибкое, и граница между этими полями может устанавливаться весьма произвольно. Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

Для того чтобы в IP-адресе различить номер сети и номер узла используют **маску подсети**. Маска подсети важна для разделения назначения адресов IP на классы. Существуют классы A, B, C, D, E. В табл. 1 приведены стандартные значения маски подсети и соответствующие им классы сети.

В табл. 2 обобщены сведения по классам и узлам сети.

В табл. 3 приведены допустимые диапазоны частного сетевого адреса.

1. Классы адресов Internet на примере адреса IP 204.107.2.100

Класс	Адрес сети	Адрес узла	Стандартное значение маски подсети
A	204	107.2.100	255.0.0.0
B	204.107	2.100	255.255.0.0
C	204.107.2	100	255.255.255.0

2. Обобщение классов A, B, C сетей и узлов

Класс	Действительное количество возможных сетей	Действительное количество возможных узлов в сети
A	126	16 777 214
B	16 384	65 534
C	2 097 151	254

3. Допустимые диапазоны частного сетевого адреса

Класс	Начало диапазона адреса в первом октете	Конец диапазона адреса в первом октете
A	001	126
B	128	191
C	192	221

Таблица 3 показывает, например, что в сетях класса C в первом октете адреса IP не может быть цифры 191 или 222, т.е. адрес IP: 191.107.1.190 будет ошибочным, если указана маска подсети 255.255.255.0.

Кроме IP-адреса существует **локальный адрес узла**, определяемый технологией, с помощью которой построена отдельная сеть, в которую входит данный узел. Для узлов, входящих в локальные сети – это MAC-адрес сетевого адаптера или порта маршрутизатора, например, 11-A0-17-3D-BC-01. Эти адреса назначаются производителями оборудования и являются уникальными адресами, так как управляются централизовано. Для всех существующих технологий локальных сетей MAC-адрес имеет формат 6 байтов: старшие 3 байта – идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем.

На рисунке 2 приведен пример схемы локальной компьютерной сети из четырёх узлов PC1, PC2, PC3, PC4 и сервера, работающего под управлением операционной системы Windows 2000 Server.

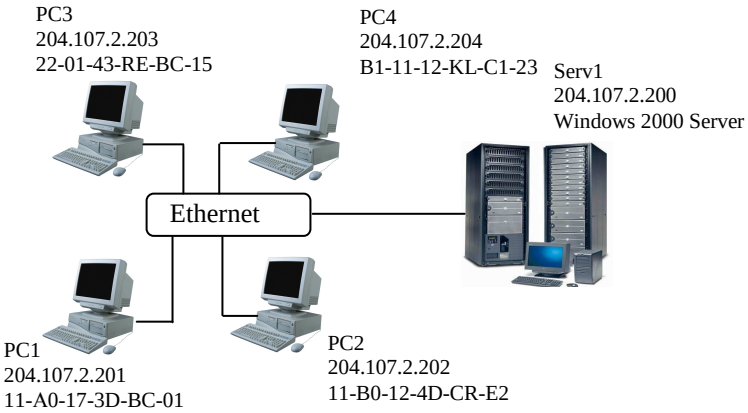


Рис. 2. Схема локальной компьютерной сети

Для определения адреса IP любого узла локальной сети достаточно знать его символьное имя и воспользоваться командой *ping*. Например, в результате выполнения команды *net view* было определено, что в компьютерной сети имеется 3 узла с именами PC1, PC2 и PC2

>*net view*

PC1

PC2

PC3

Теперь достаточно задать команду *ping Имя_узла* чтобы получить адрес IP заданного узла

>*ping PC1*

Достаточно полезной для отображения параметров TCP/IP может оказаться утилита *ipconfig*, которая отображает, в том числе, имя узла, MAC-адрес и IP-адрес.

Для её использования достаточно ввести следующую команду

> *ipconfig /all*

Более полную информацию по адресации узлов в IP-сетях можно найти на сайтах сети Интернет [5, 6, 7].

Порядок выполнения работы

1. Вызвать командную строку для выполнения вводимых с клавиатуры команд (Пуск->Выполнить->*cmd*).
2. В командной строке выполнить команду *net view* в результате выполнения которой определить символьные имена узлов локальной сети, а также имя сервера.
3. Выполнив команды *ping* и *ipconfig* определить адрес IP и MAC-адрес каждого узла.
4. Определить версию операционной системы, под управлением которой работает сервер.
5. Начертить схему локальной сети с указанием для каждого узла и сервера символьного имени, адреса IP, MAC-адреса. Для сервера указать версию операционной системы.

Контрольные вопросы

1. Что такое адрес IP?
2. Что такое MAC-адрес?
3. Что такое маска подсети?
4. На какие классы делятся сети IP?
5. Даны адрес узла и маска подсети. Что здесь не верно?

Адрес узла в частной сети: 131.107.2.100

Маска подсети: 255.255.255.0

6. Дана маска подсети 255.255.0.0. К какому классу относится сеть? Каково максимальное количество узлов в сети?

7. Дана маска подсети 255.255.255.0. Число узлов в сети 255. Что здесь не верно?

8. Дан IP-адрес узла в частной сети: 221.101.2.150. Задайте правильную маску подсети.

Практическая работа 5

СРЕДСТВА УСТРАНЕНИЯ НЕИСПРАВНОСТЕЙ В TCP/IP

Цель работы: ознакомиться со средствами поиска неисправностей TCP/IP.

Задание

1. Изучить методические указания и рекомендуемую литературу.

2. Применить утилиты *ipconfig* и *ping* для поиска неисправностей в настройке TCP/IP.

Методические указания

Целью устранения неисправностей в настройке TCP/IP является восстановление нормальной работы сети. Для поиска неисправностей можно использовать специальные диагностические утилиты, список некоторых из которых приведен в табл. 1.

1. Средства и утилиты поиска неисправностей в TCP/IP

Утилита или средство	Описание
IPConfig	Выводит текущую информацию о TCP/IP. Переключатели командной строки позволяют изменять IP-адрес узла
Ping	Проводит тестирование соединений и проверяет настройки
Hostname	Введение этой команды в командной строке приводит к возвращению имени текущего узла
Route	Отображает или изменяет таблицу маршрутизации
ARP	Позволяет просмотреть таблицы ARP локального компьютера, чтобы обнаружить повреждённые записи

Рассмотрим более подробно применение двух утилит из табл. 1. Утилита IPConfig обеспечивает отображение информации о TCP/IP. Эту утилиту хорошо применять в самом начале тестирования системы, т.к. она дает полную информацию о конфигурации TCP/IP. Существуют различные варианты команды IPConfig. Они задаются с помощью переключателей командной строки. Например, команда

>ipconfig /?

позволяет вызвать справку о команде.

Ниже приведены некоторые возможные варианты переключателей и их описание

/all	Вызов полных сведений о конфигурации
/release	Отображение адреса IP для указанного адаптера
/renew	Обновление адреса IP указанного адаптера

Чаще всего используется команда *ipconfig /all.* По этой команде отображается информация о каждом физически присутствующем сетевом адаптере, соединениях модема и виртуальных соединениях.

Команда *ping* передает пакеты протокола контроля сообщений в Internet между двумя узлами TCP/IP. Пример вызова справки о команде приведен ниже

>ping /?

Рассмотрим пример поиска неисправностей в настройках TCP/IP. Пусть известна схема сети. Специалист, выполняющий поиск неисправностей в настройках TCP/IP работает на рабочей станции (узле) PC3. Тогда, при выполнении тестирования на первом шаге на локальном рабочем узле (узел PC3) выполняется команда *IPCondig* для просмотра настроек TCP/IP.

> IPCondig /all

Результат выполнения данной команды показан ниже

Настройка Windows 2000 IP

Имя узла……	PC3
Имя основного домена……	Main.local
Тип узла……	Broadcast
Включение маршрутизации IP……	No
Физический адрес……..	22-01-43-RE-BC-15
Адрес IP	204.107.2.203
Маска подсети	255.255.255.0
Шлюз по умолчанию	204.107.2.200

Просмотрев выведенную информацию определяем IP адрес шлюза по умолчанию 204.107.2.200 (это сервер).

На втором этапе выполняется команда *ping* для внутреннего адреса обратной связи, чтобы проверить, что TCP/IP установлен и сконфигурирован правильно на локальном компьютере узла. Этот адрес – 127.0.0.1, выделенный адрес, который не может использоваться как реальный IP-адрес

>*ping 127.0.0.1*

На третьем этапе выполняется команда *ping* для локального удаленного узла (например, узел PC1), чтобы гарантировать, что TCP/IP работает правильно

> *ping* 204.107.2.201

На последнем этапе выполняется команда *ping* для адреса IP маршрутизатора или шлюза, используемого по умолчанию. Это позволит убедиться в правильном функционировании маршрутизатора или шлюза по умолчанию.

Для шлюза по умолчанию

> *ping* 204.107.2.200

Схема, отражающая порядок тестирования в приведенном примере, показана на рис. 1.

Более полную информацию по способам поиска неисправностей в настройках TCP/IP можно найти в литературе [8].

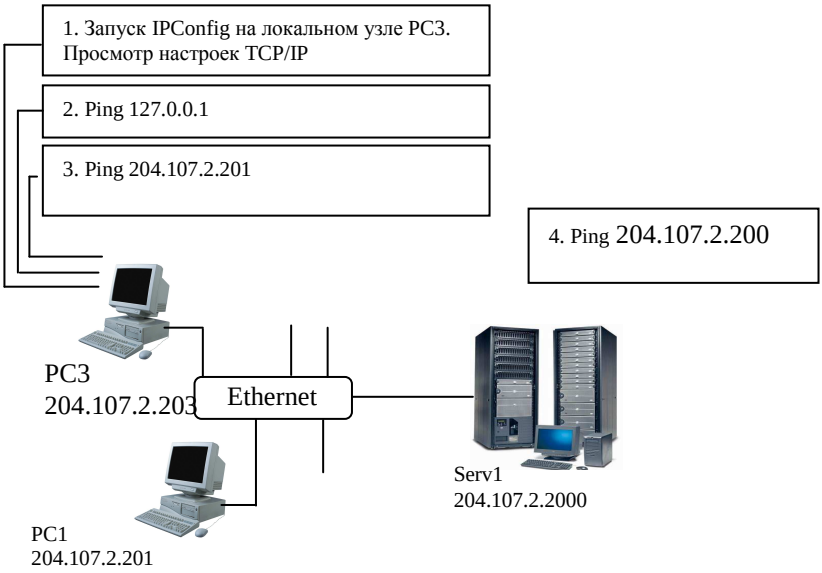


Рис. 1. Порядок совместного использования утилит IPConfig и Ping

Порядок выполнения работы

1. Выполнить команду *IPCondig* на локальном рабочем узле и просмотреть информацию о конфигурации TCP/IP.
2. Выполнить команду *ping* для внутреннего адреса обратной связи.
3. Выполнить команду *ping* для локального удаленного узла.
4. Выполнить команду *ping* для адреса IP-маршрутизатора или шлюза, используемого по умолчанию.
5. Разработать схему, отражающую порядок выполнения тестирования TCP/IP утилитами *IPConfig* и *ping*.

Контрольные вопросы

1. Перечислите утилиты, которые можно использовать для поиска неисправностей в настройках TCP/IP. Каковы их возможности?
2. Утилита IPConfig. Назначение, параметры, результаты применения.
3. Утилита Ping. Назначение, параметры, результаты применения.
4. Порядок совместного применения утилит IPConfig и Ping.
5. Назначение утилиты ARP.
6. Какую утилиту можно применить для получения имени узла?
7. Для чего используется команда Route?
8. Поясните полученные в лабораторной работе результаты.

Практическая работа 6

УСТРОЙСТВА СВЯЗИ. ПРОЕКТИРОВАНИЕ СЕТИ КРУПНОЙ ФИРМЫ

Цель работы: научиться осуществлять подбор сетевого оборудования, требуемого для создания сети организации.

Задание

Спроектируйте в виде примерной структурной схемы сеть крупной фирмы, состоящей из трех подразделений:

Офис администрации (отдельный этаж здания в центре Москвы, 10 рабочих мест).

Склад (отдельное здание за пределами МКАД), оснащен 5 стационарными рабочими станциями.

Торговый центр (рынок стройматериалов большой площади и автостоянка для покупателей), персонал которого при работе с клиентами использует КПК, свободно перемещаясь по территории торгового центра и стоянок на расстоянии до 2 км.

В пределах офиса и склада подсети должны иметь звездообразную структуру. Для офиса администрации необходимо обеспечить возможность выхода в Интернет по каналу ADSL, а связь между подразделениями фирмы осуществляется по оптоволоконному кабелю. Считать определяющими показатели надежности и скорости, пренебрегая стоимостью оборудования.

Результаты выполнения работы: схема сети, перечень необходимого оборудования.

Практическая работа 7

ИСПОЛЬЗОВАНИЕ УДАЛЁННЫХ СЕТЕВЫХ РЕСУРСОВ

Цель работы: изучить способы подключения удаленных ресурсов общего доступа.

Задание

1. Изучить методические указания.
2. Выполнить лабораторную работу в соответствии с порядком, изложенным в методических указаниях.

Методические указания

Одним из ощутимых преимуществ компьютерной сети является совместное использование таких ресурсов, как диски, папки, принтеры физически находящихся на различных узлах. Для реализации этого преимущества с компьютера, на котором установлен ресурс, необходимо разрешить к нему доступ, а на компьютере клиента необходимо подключить этот ресурс. Пусть на компьютере с именем Serv 1 (рис. 1) на диске D содержится папка Inform. Предположим, что пользователю узла PC2 во время работы требуется получить доступ к содержимому папки Inform. В этом случае для пользователя PC2 папка Inform будет являться удаленным ресурсом.

Для подключения удаленного ресурса можно использовать три основных подхода: метод «выбрать и подключить», метод с использованием графического пользовательского интерфейса GUI, метод командной строки.

Подключение сетевого диска с помощью метода «выбрать и подключить» осуществляется в следующей последовательности:

1) открыть диалоговое окно «Сетевое окружение»;
2) раскрыть элемент «Вся сеть»;
3) открыть компьютер, с которым требуется установить связь;
4) выбрать совместно используемый ресурс, которому требуется поставить в соответствие сетевой диск;
5) выбрать свободную букву сетевого диска.

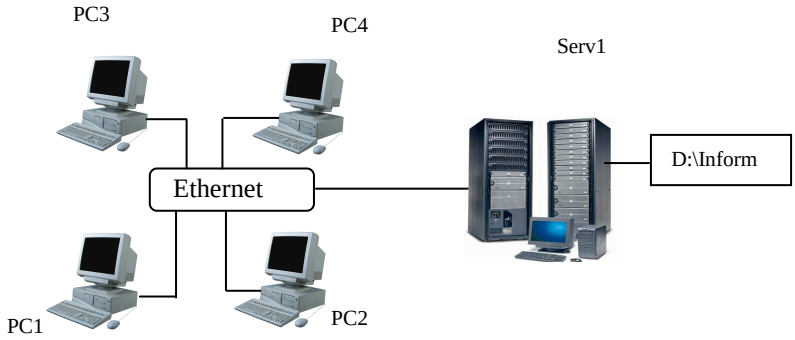


Рис. 1. К понятию о удаленном ресурсе

Подключение сетевого диска методом GUI осуществляется в следующей последовательности:

1) вызвать меню «Подключить сетевой диск…» щелчком правой кнопкой мыши на ярлыке «Мой компьютер» или ярлыке «Сетевое окружение» (рис. 2);

2) выбрать команду «Подключить сетевой диск»;

3) выбрать букву диска и имя подключаемого ресурса (имя папки), указав путь к этому ресурсу.

Рассмотрим третий способ подключения удаленных ресурсов – метод командной строки. Описание некоторых полезных команд приведено ниже.

Для просмотра удаленных компьютеров и доступных на них ресурсов в командной строке используется команда NET VIEW.

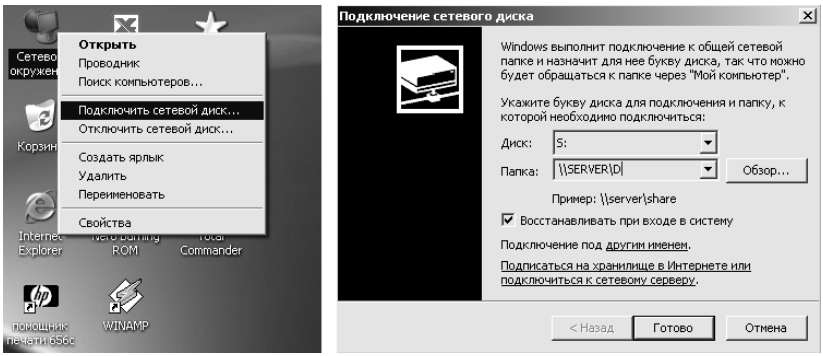


Рис. 2. Подключение удаленного ресурса методом GUI

Например, следующая команда показывает символьные имена всех доступных в данный момент компьютеров локальной сети

> NET VIEW

Для отображения всех доступных ресурсов компьютера с именем, например PC1, используется команда

> NET VIEW \\PC1

Для подключения ресурсов через командную строку используется команда

>NET USE *ДИСК*: *ИМЯ_КОМПЬЮТЕРА**РЕСУРС*

где *ДИСК* – буква диска, к которой подключается удаленный ресурс,

ИМЯ_КОМПЬЮТЕРА – имя удаленного компьютера (либо символьное, либо IP-адрес),

РЕСУРС – подключаемый ресурс удаленного компьютера.

Например следующая команда позволит подключить ресурс Inform сервера Serv1 (рис. 1) используя букву диска H

>NET USE H: \\Serv1\Inform

Следующая команда отображает все подключенные к данному компьютеру удаленные ресурсы.

> NET USE

Отключение подключенного ранее ресурса производится при помощи команды

> NET USE *ДИСК*: /D

Подключение сетевого принтера производится аналогичным образом, только вместо буквы диска пишется порт (например, LPT1):

>NET USE LPT1 *ИМЯ_КОМПЬЮТЕРА**ИМЯ_ПРИНТЕРА*

Чтобы обеспечить возможность создания общих (общим называется ресурс, к которому разрешен доступ с других компьютеров сети) ресурсов в операционной системе Windows XP необходимо отключить режим **простого общего доступа к папкам**. Для этого необходимо выбрать в окне «Мой компьютер» меню «Сервис» – «Свойства папки…».

Затем в открывшемся окне выбрать вкладку «Вид» и снять отметку в пункте «Использовать простой общий доступ к файлам».

Для открытия общего доступа к папке необходимо на выбранной папке щелкнуть правой кнопкой мыши и выбрать пункт меню «Общий доступ и безопасность…».

В открывшемся окне во вкладке «Доступ» необходимо выбрать кнопку «Открыть общий доступ к этой папке» и определить «Разрешения».

Под разрешениями понимается перечень пользователей, которым разрешен доступ к данной папке, а также определенные им права доступа (чтение, запись и др.).

Чтобы добавить в список разрешений того или иного пользователя, необходимо щелкнуть на кнопке «Добавить», затем в открывшемся окне ввести имя пользователя.

Порядок выполнения работы

1. Просмотреть через командную строку список всех доступных компьютеров в локальной сети.
2. Просмотреть через командную строку список всех доступных ресурсов сервера.
3. Подключить ресурс сервера “NetShare” (тремя способами).
4. Просмотреть через командную строку список всех подключенных ресурсов к данному компьютеру.
5. Отключить все подключенные ранее ресурсы.
6. Создать в папке C:\TEMP\ папку с именем DISK *№Компьютера*, например, DISK1 или DISK12.
7. Открыть общий доступ к этой папке.
8. Для пользователей группы "Все" запретить все виды доступа (на чтение, на запись и др.).
9. Добавить в список разрешений одного пользователя (например ah08-01). Определить ему права полного доступа.

Контрольные вопросы

1. Что представляет собой удаленный ресурс? Примеры.
2. Какие способы подключения удаленных ресурсов вам известны?
3. Что такое общий ресурс? Приведите примеры.
4. Как создать общий ресурс?
5. Как подключить удаленный принтер, используя командную строку?
6. Как просмотреть список удаленных ресурсов узла?
7. Как удалить подключенный ранее сетевой диск?
8. Как добавить в список разрешений заданного пользователя?

Практическая работа 8

МЕТОДЫ ЗАЩИТЫ КОМПЬЮТЕРА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ИЗ ВНЕШНЕЙ СЕТИ И ПОИСК УЯЗВИМОСТЕЙ В СИСТЕМЕ ЗАЩИТЫ

Цель работы: 1. Изучить возможности брандмауэра Windows и обозревателя Internet Explorer в защите от несанкционированного доступа. 2. Изучить методы анализа защищенности информационных ресурсов.

Задание

1. Определить все доступные узлы в локальной сети.
2. Просканировать порты сервера компьютерной сети.

Методы защиты компьютера от несанкционированного доступа из внешней сети

Брандмауэр – сочетание программного и аппаратного обеспечения, образующее систему защиты от несанкционированного доступа из внешней глобальной сети во внутреннюю сеть (интрасеть). Брандмауэр предотвращает прямую связь между внутренней сетью и внешними компьютерами, пропуская сетевой трафик через прокси-сервер, находящийся снаружи сети. Прокси-сервер определяет, следует ли разрешить файлу попасть во внутреннюю сеть. Брандмауэр называется также шлюзом безопасности.

Можно считать брандмауэр пограничным постом, на котором проверяется информация (часто называемая *трафик*), приходящая из Интернета или локальной сети. В ходе этой проверки брандмауэр отклоняет или пропускает информацию на компьютер в соответствии с установленными параметрами.

Когда к компьютеру пытается подключиться кто-то из Интернета или локальной сети, такие попытки называют «непредусмотренными запросами». Когда на компьютер поступает непредусмотренный запрос, брандмауэр Windows блокирует подключение. Если на компьютере используются такие программы, как программа передачи мгновенных сообщений или сетевые игры, которым требуется принимать информацию из Интернета или локальной сети, брандмауэр запрашивает пользователя о блокировании или разрешении подключения. Если пользователь разрешает подключение, брандмауэр Windows создает *исключение*, чтобы в будущем не тревожить пользователя запросами по поводу поступления информации для этой программы.

Если идёт обмен мгновенными сообщениями с собеседником, который собирается прислать файл (например фотографию), брандмауэр Windows запросит подтверждение о снятии блокировки подключения и разрешении передачи фотографии на компьютер. А при желании участвовать в сетевой игре через Интернет с друзьями пользователь может добавить эту игру как исключение, чтобы брандмауэр пропускал игровую информацию на компьютер.

Хотя имеется возможность отключать брандмауэр Windows для отдельных подключений к Интернету или локальной сети, это повышает вероятность нарушения безопасности компьютера.

Чтобы открыть компонент «Брандмауэр Windows», нажмите кнопку **Пуск**, выберите пункты **Настройка**, **Панель управления**, **Сеть и подключения к Интернету** и **Брандмауэр Windows**.

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 веб-узлы используют эти данные, а также задать значения параметров конфиденциальности, которые будут определять, разрешено ли веб-узлам сохранять файлы «cookie» на компьютере.

В число параметров конфиденциальности Internet Explorer входят следующие.

- Параметры конфиденциальности, определяющие обработку на компьютере файлов «cookie». Файлы «cookie» – это созданные веб-узлом объекты, которые сохраняют на компьютере определенные сведения, например о предпочтениях пользователя при посещении данного узла. Кроме того, эти файлы могут также сохранять личные данные пользователя, такие, как имя и адрес электронной почты.
- Оповещение безопасности, выдаваемые пользователю при попытке получить доступ к веб-узлу, не соответствующему заданным параметрам конфиденциальности.
- Возможность просмотра политики конфиденциальности P3P для веб-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. Эти средства безопасности могут также защитить компьютер от небезопасного программного обеспечения.

В число параметров безопасности Internet Explorer входят следующие.

- Возможность блокирования большинства всплывающих окон.
- Возможность обновления, отключения или повторного включения надстроек для веб-обозревателя.
- Средства повышения безопасности, предупреждающие пользователя о попытке веб-узла загрузить файлы или программы на компьютер.
- Цифровые подписи, которые подтверждают, что файл поступил действительно от указанного лица или издателя и с момента включения цифровой подписи в этот файл никем не внесены изменения.
- Безопасное подключение с использованием 128-разрядного ключа, которое применяется для связи с безопасными веб-узлами.

Поиск уязвимостей в системе защиты

Противостояние атакам – важное свойство защиты. Казалось бы, если в сети установлен межсетевой экран (firewall), то безопасность гарантирована, но это распространенное заблуждение может привести к серьёзным последствиям.

Например, межсетевой экран (МЭ) не способен защитить от пользователей, прошедших аутентификацию. А квалифицированному хакеру не составляет труда украсть идентификатор и пароль авторизованного пользователя. Кроме того, межсетевой экран не только не защищает от проникновения в сеть через модем или иные удалённые точки доступа, но и не может обнаружить такого злоумышленника.

При этом система защиты, созданная на основе модели адаптивного управления безопасностью сети (Adaptive Network Security, ANS), способна решить все или почти все перечисленные проблемы. Она позволяет обнаруживать атаки и реагировать на них в режиме реального времени, используя правильно спроектированные, хорошо управляемые процессы и средства защиты.

Компания Yankee Group опубликовала в июне 1998 г. отчёт, содержащий описание процесса обеспечения адаптивной безопасности сети. Этот процесс должен включать в себя анализ защищённости, т.е. поиск уязвимостей, обнаружение атак, а также использовать адаптивный (настраиваемый) компонент, расширяющий возможности двух первых функций, и управляющий компонент.

Анализ защищённости осуществляется на основе поиска уязвимых мест во всей сети, состоящей из соединений, узлов (например, коммуникационного оборудования), хостов, рабочих станций, приложений и баз данных. Эти элементы нуждаются как в оценке эффективности их защиты, так и в поиске в них неизвестных уязвимостей. Процесс анализа защищённости предполагает исследование сети для выявления в ней слабых мест и обобщение полученных сведений, в том числе в виде отчёта. Если система, реализующая данную технологию, содержит адаптивный компонент, то устранение найденной уязвимости будет осуществляться автоматически. При анализе защищённости обычно идентифицируются:

- люки в системах (back door) и программы типа «троянский конь»;
- слабые пароли;
- восприимчивость к проникновению из внешних систем и к атакам типа «отказ в обслуживании»;
- отсутствие необходимых обновлений (parch, hotfix) операционных систем;
- неправильная настройка межсетевых экранов, WEB-серверов и баз данных.

Обнаружение атак – это процесс оценки подозрительных действий в корпоративной сети, реализуемый посредством анализа журналов регистрации операционной системы и приложения (log-файлов) либо сетевого трафика. Компоненты ПО обнаружения атак размещаются на узлах или в сегментах сети и оценивают различные операции, в том числе с учётом известных уязвимостей.

Адаптивный компонент ANS позволяет модифицировать процесс анализа защищенности, предоставляя самую последнюю информацию о новых уязвимостях. Он также модифицирует компонент обнаружения атак, дополняя его последней информацией о подозрительных действиях и атаках. Примером адаптивного компонента может служить механизм обновления баз данных антивирусных программ, которые являются частным случаем систем обнаружения атак.

Управляющий компонент предназначен для анализа тенденций, связанных с формированием системы защиты организации и генерацией отчётов.

К сожалению, эффективно реализовать все описанные технологии в одной системе пока не удаётся, поэтому пользователям приходится применять совокупность систем защиты, объединённых единой концепцией безопасности. Пример таких систем – семейство продуктов SAFEsuite, разработанных американской компанией Internet Security Systems (ISS). В настоящее время комплект ПО SAFEsuite поставляется в новой версии SAFEsuite Enterprise, в которую входит также ПО SAFEsuite Decisions, обеспечивающее принятие решений по проблемам безопасности.

Система анализа защищённости Internet Scanner предназначена для проведения регулярных всесторонних или выборочных тестов сетевых служб, операционных систем, используемого прикладного ПО, маршрутизаторов, межсетевых экранов, WEB-серверов и т.п.

Другим примером системы анализа защищенности является программа SuperScan, позволяющая сканировать открытые порты узлов с известными IP-адресами.

Для начала сканирования достаточно в поле Start указать IP-адрес сканируемого узла. Для более глубокого сканирования необходимо указать минимальную скорость сканирования, передвинув движок на отметку Min. Запустите программу SuperScan на своем компьютере и просканируйте порты сервера с именем queen. Результаты занесите в табл. 1.

Результаты выполнения лабораторной работы

Результаты поиска уязвимостей в системе защиты
узла _____ IP: ___ . ___ . ___ . ___
Символьное имя узла IP адрес узла

1. Результаты сканирования

№ п.п	№ порта	Наименование	№ п.п	№ порта	Наименование
1			7		
2			8		
3			9		
4			10		
5			11		
6			12		

Контрольные вопросы

1. Может ли брандмауэр блокировать компьютерным вирусам и «червям» доступ на компьютер?
2. Может ли брандмауэр обнаружить или обезвредить компьютерных вирусов и «червей», если они уже попали на компьютер?
3. Может ли брандмауэр запретить пользователю открывать сообщения электронной почты с опасными вложениями?
4. Может ли брандмауэр блокировать спам или несанкционированные почтовые рассылки?
5. Может ли брандмауэр запросить пользователя о выборе блокировки или разрешения для определённых запросов на подключение?
6. Для чего нужен журнал безопасности брандмауэра?
7. Сколько параметров определяет работу брандмауэра?
8. Перечислите параметры, определяющие работу брандмауэра.
9. Какой параметр брандмауэра обеспечивает наивысшую защиту компьютера?
10. Что такое брандмауэр, его назначение.
11. Как работает брандмауэр?
12. Какими возможностями обладает Интернет-обозреватель для защиты личных данных пользователей?
13. Перечислите параметры безопасности Internet Explorer.
14. Перечислите параметры конфиденциальности Internet Explorer.
15. Для чего нужно проводить анализ защищенности сети?
16. Перечислите наиболее уязвимые «места» сети.
17. Приведите примеры систем анализа уязвимостей.

Практическая работа 9

МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО СЕТИ

Цель работы: изучить метод перестановки для шифрования открытого текста.

Задание

1. Изучить теоретические основы метода перестановки.
2. Зашифровать (расшифровать) одно слово открытого текста ключом, длина которого равна длине шифруемого слова.
3. Придумать символьный пароль, преобразовать его в ключ и зашифровать (расшифровать) фразу открытого текста с помощью этого ключа.

Методические указания

Шифрование является одним из эффективных способов защиты текстовой информации. При шифровании существуют следующие понятия.

Открытый текст – информация, содержание которой может быть понятно любому субъекту.

Шифрование – процесс преобразования открытого текста в шифротекст или криптограмму с целью сделать его содержание непонятным для посторонних лиц. В общем виде процесс шифрования описывается выражением вида $C = E_k(P)$, где C – шифротекст; E – функция шифрования; k – ключ шифрования; P – открытый текст.

Расшифрование – процесс обратного преобразования шифротекста в открытый текст. В общем виде процесс расшифрования описывается выражением вида $P = D_{k'}(C)$, где D – функция расшифрования; k' – ключ расшифрования.

Криптосистема – совокупность алгоритмов, реализуемых функциями E и D, множества ключей k, k' и шифротекстов.

Криптограмма (загадочное письмо или тайнопись) – наука о защите информации с помощью шифрования.

Криптоанализ – наука о методах дешифрования.

Криптостойкость – характеристика надёжности шифротекста от вскрытия.

Криптостойкость шифра характеризуют двумя величинами:

1) минимальным объёмом шифротекста, статическим анализом которого можно его вскрыть и получить открытый текст без знания ключа;

2) числом MIPS-часов (лет) – временем работы условного криптоаналитического компьютера производительностью 1 000 000 операций в секунду, необходимым для вскрытия шифротекста.

В настоящее время известно множество методов шифрования, одним из которых является метод перестановки.

В соответствии с этим методом биты (или символы) открытого текста переставляются в соответствии с задаваемым ключом шифрования правилом

$$1 \le i \le n,\ C_i = P_{k[i]}, \qquad (1)$$

где $P = \{P_1, P_2, P_3, ...P_i, ...P_n\}$ – открытый текст; n – длина открытого текста (количество символов текста); $C = \{C_1, C_2, C_3, ...C_i, ...C_n\}$ – шифротекст; $k = \{k_1, k_2, k_3, ...k_i, ...k_n\}$ – ключ шифрования.

При расшифровании используется обратная перестановка:

$$P_{k[i]} = C_i. \qquad (2)$$

Как видно из приведенных выражений, ключ должен удовлетворять условиям: $k_i \ne k_j$, $1 \le k_i \le n$.

Рассмотрим пример шифрования слова «Пример» методом перестановки (табл. 1). Зададим ключ, который должен быть равен 6-ти символам (количеству символов в шифруемом слове) в виде $k = \{1, 4, 6, 2, 3, 5\}$.

1. Данные для шифрования

Символы открытого текста	П	р	и	м	е	р
	P_1	P_2	P_3	P_4	P_5	P_6
Цифровые символы ключа	1	4	6	2	3	5
	k_1	k_2	k_3	k_4	k_5	k_6

Применим формулу (1) с выбранным ключом k к слову «Пример». Получим следующие выражения:

$$C_1 = P_{k[1]} = P_1 = \text{'П'};\ C_2 = P_{k[2]} = P_4 = \text{'м'};\ C_3 = P_{k[3]} = P_6 = \text{'р'};$$
$$C_4 = P_{k[4]} = P_2 = \text{'р'};\ C_5 = P_{k[5]} = P_3 = \text{'и'};\ C_6 = P_{k[6]} = P_5 = \text{'е'}.$$

В конечном итоге получим шифротекст $C =$ Пмррие.

Очевидно, что применив другой ключ, получим другой вид шифрованного текста.

При дешифровании используем обратную операцию по формуле (2):

$$P_{k[1]} = P_1 = C_1 = \text{'П'};\ P_{k[2]} = P_4 = C_2 = \text{'м'};\ P_{k[3]} = P_6 = C_3 = \text{'р'};$$
$$P_{k[4]} = P_2 = C_4 = \text{'р'};\ P_{k[5]} = P_3 = C_5 = \text{'и'};\ P_{k[6]} = P_5 = C_6 = \text{'е'}.$$

Таким образом, получим $P = \{P_1, P_2, P_3, P_4, P_5, P_6\} = \{\text{Пример}\}$.

Если требуется зашифровать достаточно длинный текст длиной *n*, то его можно разбить на блоки, длина которых равна длине ключа *m*. Открытый текст записывают в таблицу с числом столбцов, равным

длине ключа (каждый блок открытого текста записывается в столбец таблицы). Затем столбцы полученной таблицы переставляются в соответствии с ключом перестановки, а шифротекст считывается из строк таблицы последовательно.

Пусть требуется зашифровать открытый текст «этот пример шифрования». Длина текста (вместе с пробелами n = 22). Выберем ключ шифрования в виде $k = \{3, 5, 4, 2, 1\}$ $(m = 5)$.

Разбиваем строку «этот пример шифрования» на пять блоков, каждый из который располагаем в таблицу:

э	п	р	р	и
т	р		о	я
о	и	ш	в	
т	м	и	а	
	е	ф	н	

Переставляем столбцы полученной таблицы в соответствии с ключом $k = \{3, 5, 4, 2, 1\}$. Получим

р	и	р	п	э
	я	о	р	т
ш		в	и	о
и		а	м	т
ф		н	е	

Считываем последовательно текст из строк таблицы. Получим следующий шифр: рирпэ яортш виои амтф не.

Для расшифрования шифротекст записывают в таблицу того же размера по строкам, затем производится обратная перестановка столбцов в соответствии с ключом, после чего расшифрованный текст считывается из таблицы по столбцам. Ниже приведены этапы расшифровывания: а) запись шифротекста в таблицу; б) перестановка столбцов в соответствии с ключом; в) считывание символов по столбцам.

Этап а)

р	и	р	п	э
	я	о	Р	т
ш		в	и	о
и		а	м	т
ф		н	е	

Этап б)

э	п	р	р	и
т	р		о	я
о	и	ш	в	
т	м	и	а	
	е	ф	н	

Результатом считывания данных таблицы этапа б) будет фраза «этот пример шифрования».

Если в качестве ключа перестановки использовать последовательность не цифр, а произвольных символов (например пароль пользователя), то его необходимо предварительно преобразовать в последовательность целых чисел от 1 до *m*.

Например, пользователь ввел пароль «Петров».

Отсортируем символы в алфавитном порядке.

Получим Петров=>веопрт. Каждому символу присвоим порядковый номер:

в е о п р т
1 2 3 4 5 6

Заменим символы введённого пароля цифрами и получим ключ: 426531.

Выберите предложение открытого текста для шифрования в соответствии с номером своего варианта (табл. 2).

2. Таблица выбора заданий по вариантам

Вариант №	№ шифруемой строки	Вариант №	№ шифруемой строки	Вариант №	№ шифруемой строки
1	1	7	7	13	13
2	2	8	8	14	14
3	3	9	9	15	15
4	4	10	10	16	16
5	5	11	11	17	17
6	6	12	12	18	18

1. Существует три разновидности угроз.

2. Угроза нарушения конфиденциальности заключается в следующем.

3. Информация становится известной тому, кто не располагает полномочиями доступа к ней.

4. Она имеет место всякий раз, когда получен доступ к некоторой секретной информации.

5. Информация хранится в вычислительной системе или передается от одной системы к другой.

6. В связи с угрозой нарушения конфиденциальности, используется термин «утечка».

7. Угроза нарушения целостности включает в себя любое умышленное изменение информации.

8. Когда злоумышленники преднамеренно изменяют информацию, говорится, что целостность информации нарушена.

9. Целостность также будет нарушена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения.

10. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью.

11. Целостность информации это существование информации в неискаженном виде.

12. Чаще субъектов интересует обеспечение более широкого свойства – достоверности информации.

13. Угроза отказа служб возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы.

14. Реально блокирование может быть постоянным – запрашиваемый ресурс никогда не будет получен.

15. Или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того чтобы он стал бесполезным.

16. В этих случаях говорят, что ресурс исчерпан.

17. Естественные угрозы – угрозы, вызванные воздействиями на АС и её компоненты объективных физических процессов или стихийных природных явлений, независящих от человека.

18. Искусственные угрозы – это угрозы информационной безопасности АС, вызванные деятельностью человека.

Результаты выполнения лабораторной работы

Исходное слово для шифрования:

Ключ шифрования:

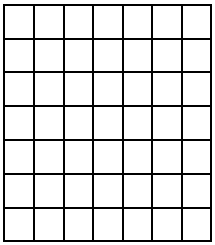
Результат шифрования

Символьный пароль

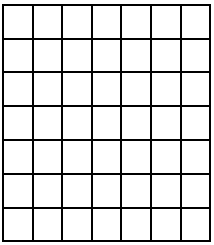
Цифровой пароль _ _ _ _ _ _ _ _ _ _

Фраза для шифрования

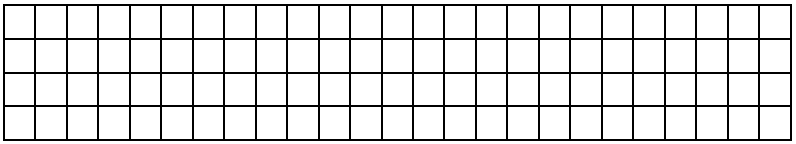
Этап а)



Этап б)



Результат шифрования



Контрольные вопросы

1. Охарактеризовать информацию и её свойства.
2. Что является предметом и объектом защиты информации?
3. Чем определяется ценность информации? Приведите классификацию конфиденциальной информации.
4. Охарактеризовать свойства достоверности и своевременности информации.
5. Что понимается под угрозой информации? Назвать разновидности угроз информации.
6. Привести классификацию угроз информации.
7. Какие основные направления и методы реализации угроз вам известны?
8. Пояснить классификацию злоумышленников.
9. Охарактеризовать причины и виды утечки информации.
10. Назвать и привести примеры каналов утечки информации.
11. Перечислить задачи государства в области безопасности информации.
12. Охарактеризовать основные законы РФ, регулирующие отношения в области информационных технологий.
13. Назвать государственные органы, обеспечивающие безопасность информационных технологий, и решаемые ими задачи.
14. Пояснить, что такое шифрование и в чём заключается сущность метода перестановки.

АВТОМАТИЗАЦИЯ ШИФРОВАНИЯ МЕТОДОМ ПЕРЕСТАНОВКИ

Цель работы: разработать программу, реализующую шифрование слова методом перестановки.

Задание

1. Написать программу, позволяющую автоматически зашифровать (расшифровать) заданное в текстовом файле слово с помощью ключа, введенного с клавиатуры. Слова для шифрования выберите из табл. 1.

2. Протестировать программу, зашифровав (расшифровав) 3 – 5 слов различными ключами.

Методические указания

Для написания программы можно использовать любой из известных языков программирования. В данной работе используется встроенный язык программирования программы MatLab.

Исходное слово для шифрования помещается в текстовый файл, созданный, например, в редакторе «Блокнот».

Откроем файл из программы MatLab. Это осуществляется за счёт использования выражения **fid=fopen('nietzsche.txt','r')**. В приведенном выражении в оператор **fopen** передаются два значения: **nietzsche.txt** – имя открываемого файла, содержащего шифруемое слово; **r** – статус открытия файла, означающий, что файл будет открыт только для чтения. В переменную **fid** будет записан результат открытия файла. Если в переменную **fid** запишется число, равное –1, то это означает, что файл не был открыт. Поэтому в программу можно добавить следующий код:

```
if(fid==–1)
disp('ошибка открытия файла')
error(mes)
```

который предназначен для вывода сообщения об ошибке, возникающей в случае, если файл не был открыт.

В случае успешного открытия файла, содержащуюся в нём строку (строки) необходимо записать в некоторую переменную (переменные). Оператор MatLab **feof(fid)** позволяет определить факт достижения конца файла. Оператор **fgetl(fid)** позволяет последовательно считывать строки файла и записывать их в заданные переменные. Оператор **size(string,2)** позволяет определить длину (количество символов) строки. Ниже приведён фрагмент программы, позволяющий считать строку (или строки) из файла и определить её размер:

```
while ~(feof(fid)) % пока не конец файла
string=fgetl(fid); % запись строки из файла в переменную string
char_tek=size(string,2); % запись длины строки string
end
```

После того, как длина слова определена, пользователя программы можно попросить ввести с клавиатуры ключ шифрования и сохранить его в массив **kl** так, как показано в примере:

```
for i=1:char_tek
kl(i)=input('Введите число');
end
```

Теперь можно зашифровать слово методом перестановки. Это осуществляется в следующем коде программы:

```
for i=1:char_tek
shifr(i)=string(kl(i));
end
```

Шифр помещается в строку **shifr**, которую можно вывести на экран с помощью оператора **disp(shifr)**. После этого открытый ранее файл можно закрыть, применив оператор **fclose(fid)**.

Ниже приведён полный текст программы шифрования слова:

```
fid=fopen('nietzsche.txt','r');
if(fid==-1)
disp('ошибка открытия файла')
error(mes)
else
while ~(feof(fid))
string=fgetl(fid);
char_tek=size(string,2);
end
clc
disp('Шифруемое слово:')
disp(string)
disp('Длина ключа')
disp(char_tek)
for i=1:char_tek
kl(i)=input('Введите число');
end
for i=1:char_tek
shifr(i)=string(kl(i));
end
disp('Шифрованное слово')
disp(shifr)
fclose(fid);
end
```

1. Варианты заданий для самостоятельной работы

№ варианта	Слово	№ варианта	Слово	№ варианта	Слово
1	technical	7	simulation	13	matrix
2	Algorithm	8	standard	14	Scientific
3	matlab	9	analysis	15	complete
4	Modeling	10	logic	16	graphics
5	project	11	control	17	including
6	Interface	12	interactive	18	system

Результаты выполнения лабораторной работы

Исходное слово для шифрования

Результат шифрования Ключ шифрования

Результат шифрования Ключ шифрования

Результат шифрования Ключ шифрования

Результат шифрования Ключ шифрования

Результат шифрования Ключ шифрования

Контрольные вопросы

1. Пояснить алгоритм работы вашей программы.
2. Указать недостатки программы шифрования, приведённой в примере. Как можно их устранить?
3. Написать код для подсчёта числа символов ‘a’ в строке.
4. Написать код для подсчёта числа пустых строк в файле.
5. Написать код для подсчёта числа не пустых строк в файле.

6. Написать код для подсчёта общего числа строк в файле.
7. Написать код для преобразования пароля в ключ шифрования.
8. Написать код для подсчёта числа символов в файле.
9. Написать код для замены символов ‘р’ слова цифрой 1.
10. Написать код для сортировки букв слова в алфавитном порядке.
11. Написать код для подсчёта числа букв в первом слове предложения.
12. Написать код для подсчёта числа пробелов в предложении.
13. Написать код для замены пробелов в предложении цифрой 0.
14. Написать код для подсчёта числа слов в предложении. Слова разделены пробелами.

Практическая работа 11

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Цель работы: изучить современные достижения в области защиты компьютерной информации, получить навыки формирования политики и программы защиты информационных ресурсов.

Задание

1. Составить список фирм, специализирующихся на защите компьютерной информации.
2. Составить политику и сформировать программу защиты информационных ресурсов.

Методические указания

В поисковых системах сети Интернет (например, yandex.ru, aport.ru) найдите 3–4 фирмы, которые предлагают свои услуги по защите компьютерной информации. Просмотрите перечень услуг этих фирм и определите: объекты защиты, методы и средства защиты. Полученные данные внесите в табл. 1.

Выберите любую организацию (например, можно взять организацию – место прохождения производственной практики) и сформируйте: основные положения политики защиты информационных ресурсов; укажите компоненты программы защиты информационных ресурсов.

1. Перечень фирм, специализирующихся на защите информационных ресурсов

Наименование фирмы	Предложения по защите	
	Объекты защиты	Методы и средства

Контрольные вопросы

1. Что представляет собой политика защиты информации?
2. В чём заключается политика защиты информации верхнего уровня?
3. Какие темы освещает политика защиты информации среднего уровня?
4. Расскажите об аспектах, которые включает политика защиты информации нижнего уровня.
5. На что направлена программа защиты информации?
6. Что должна регламентировать программа защиты информации?
7. Какие компоненты входят в программу защиты информации?

ТЕМЫ СЕМИНАРСКИХ ЗАНЯТИЙ

Перед каждым семинарским занятием получите у преподавателя тему доклада и подготовьте презентацию, содержащую основные положения вашего доклада. Доклад должен содержать актуальные (не устаревшие) сведения по рассматриваемым вопросам. При необходимости в презентацию необходимо включать иллюстрации, таблицы и графики. Продолжительность доклада 5 – 7 минут.

В ходе семинара необходимо конспектировать основные положения доклада в рабочую тетрадь.

Тема 1. АППАРАТНЫЕ СРЕДСТВА ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ

Цель работы: изучить назначение и принципы работы основных составных частей персонального компьютера.

Задание

Подготовьте доклад с презентацией на одну из тем, приведённых ниже.

Список вопросов для обсуждения на семинаре:

1. Назначение и компоненты системной платы.
2. Что такое северный мост? Его назначение.
3. Что такое южный мост? Его назначение.
4. Что такое форм-фактор материнской платы?
5. Назначение центрального процессора.
6. Что такое многоядерный процессор?
7. Что такое кэширование?
8. Оперативное запоминающее устройство. Его назначение.
9. Что такое энергозависимые и энергонезависимые запоминающие устройства?

10. Универсальная последовательная шина USB.
11. Шина ввода-вывода PCI и PCI-Express.
12. Шина AGP.
13. Видеокарта. Назначение и устройство.
14. Сетевой адаптер. Назначение, типы, параметры и функции.
15. Назначение и типы оптических приводов.
16. Жёсткий диск. Назначение и устройство.

Тема 2. КОМПЬЮТЕРНАЯ СЕТЬ

Цель работы: изучить назначение и виды компьютерных сетей.

Задание

Подготовьте доклад с презентацией на одну из тем, приведенных ниже.

Список вопросов для обсуждения на семинаре:

1. Что такое компьютерная сеть. Ресурсы сети.
2. Локальные, региональные и глобальные сети.
3. Проводные и беспроводные сети.
4. Одноранговые и клиент-серверные сети.
5. Взаимодействие компьютеров в сети.
6. Серверы и клиенты.

Тема 3. ВЗАИМОДЕЙСТВИЕ КОМПЬЮТЕРОВ В СЕТИ

Цель работы: изучить правила взаимодействия компьютеров в сети.

Задание

Подготовьте доклад с презентацией на одну из тем, приведенных ниже.

Список вопросов для обсуждения на семинаре:

1. Что такое сетевой протокол?
2. Структура модели OSI.
3. Уровни модели OSI.
4. Структура кадра.
5. Функции сетевого адаптера при работе с кадрами.

Тема 4. СЕТЕВЫЕ АРХИТЕКТУРЫ

Цель работы: изучить типовые сетевые архитектуры, их характеристики.

Задание

Подготовьте доклад с презентацией на одну из тем, приведённых ниже. Тему утвердите у преподавателя.

Список вопросов для обсуждения на семинаре:

1. Архитектура TokenRing. Стандарты.
2. Архитектура Ethernet. Стандарты.
3. Архитектуры беспроводных сетей. Стандарты.

Тема 5. УСТРОЙСТВА СВЯЗИ

Цель работы: изучить назначение и основные характеристики сетевых устройств

Задание

Изучите рекомендуемую литературу и подготовьте доклад с презентацией на одну из тем, приведенных ниже. Тему утвердите у преподавателя.

Список вопросов для обсуждения на семинаре:

1. Сетевые адаптеры.
2. Концентраторы. Повторители.
3. Мосты. Коммутаторы.
4. Маршрутизаторы.
5. Шлюзы.

Тема 6. СТЕК TCP/IP

Цель работы: изучить назначение и основные характеристики сетевых протоколов

Задание

Подготовьте доклад с презентацией на одну из тем, приведенных ниже. Тему утвердите у преподавателя.

Список вопросов для обсуждения на семинаре:

1. Протокол NetBEUI.
2. Основные протоколы стека TCP/IP.
3. Прикладной уровень стека TCP/IP.
4. Сходство и различие между протоколами TCP и UDP.
5. Порты в TCP/IP.

Тема 7. НАСТРОЙКИ IP-АДРЕСАЦИИ И МАРШРУТИЗАЦИИ

Цель работы: изучить основы маршрутизации.

Задание

Подготовьте доклад с презентацией на одну из тем, приведенных ниже. Тему утвердите у преподавателя.

Список вопросов для обсуждения на семинаре:

1. Основы IP-маршрутизации.
2. Анализ таблицы маршрутизации.
3. Таблица маршрутизации компьютера с двумя сетевыми адаптерами.
4. Сеть с двумя маршрутизаторами.

Тема 8. СЕТЕВЫЕ СЛУЖБЫ, КЛИЕНТЫ, СЕРВЕРЫ, РЕСУРСЫ

Цель работы: изучить основы настройки сетевых служб и безопасности работы в сети

Задание

Подготовьте доклад с презентацией на одну из тем, приведенных ниже. Тему утвердите у преподавателя.

Список вопросов для обсуждения на семинаре:

1. Типы серверов.
2. Основы безопасности при работе в сетях.
3. Рабочие группы и домены.
4. Основные угрозы при работе в сети.

Тема 9. ПОДКЛЮЧЕНИЕ СЕТИ К ИНТЕРНЕТУ

Цель работы: изучить основы настройки сетевых служб и безопасности работы в сети

Задание

Подготовьте доклад с презентацией на одну из тем, приведенных ниже. Тему утвердите у преподавателя.

Список вопросов для обсуждения на семинаре:

1. Модемы, цифровые модемы.
2. Технология GPRS, Wi-Fi, WiMAX.
3. Подключение на сетевом уровне. Работа транслятора сетевых адресов при взаимодействии с Интернетом.
4. Доменная система имен.
5. Всемирная паутина.

Тема 10. ГЛОБАЛЬНЫЕ СЕТИ

Цель работы: изучить основы построения глобальных сетей

Задание

Подготовьте доклад с презентацией на одну из тем, приведенных ниже. Тему утвердите у преподавателя.

Список вопросов для обсуждения на семинаре:

1. Общая структура и функции глобальной сети.
2. Типы глобальных сетей.
3. Глобальные связи на основе выделенных линий.
4. Глобальные связи на основе сетей с коммутацией каналов.

Тема 11. ГЛОБАЛЬНЫЕ СЕТИ

Цель работы: изучить основы построения глобальных сетей

Задание

Изучите рекомендуемую литературу и подготовьте доклад с презентацией на одну из тем, приведенных ниже. Тему утвердите у преподавателя.

Список вопросов для обсуждения на семинаре:

1. Глобальные сети с коммутацией пакетов.
2. Удаленный доступ.
3. Средства анализа и управления сетями.

Тема 12. СРЕДСТВА АНАЛИЗА И УПРАВЛЕНИЯ СЕТЯМИ

Цель работы: изучить основы анализа и управления сетями

Задание

Подготовьте доклад с презентацией на одну из тем, приведенных ниже. Тему утвердите у преподавателя.

Список вопросов для обсуждения на семинаре:

1. Стандарты систем управления.
2. Мониторинг и анализ локальных сетей.
3. Многофункциональные портативные приборы мониторинга.

СПИСОК ЛИТЕРАТУРЫ

1. Бройдо, В.Л. Архитектура ЭВМ и систем : учебник для вузов / В.Л. Бройдо, О.П. Ильина. – СПб. : Питер, 2006.

2. Бройдо, В.Л. Вычислительные системы, сети и телекоммуникации : учебник для вузов / В.Л. Бройдо. – 2-е изд. – СПб. : Питер, 2005.

3. Пятибратов, А.П. Вычислительные системы, сети и телекоммуникации : учебник для вузов / А.П. Пятибратов, Л.П. Гудынов, А.А. Кириченко; под ред. проф. А.П. Пятибратова. – 3-е изд. – М. : Финансы и статистика, 2005.

4. Архитектура компьютерных систем и сетей : учебное пособие для вузов / М.И. Семенов, И.Т. Трубилин, В.И. Лойко, Т.П. Барановская. – М. : Финансы и статистика, 2004.

5. Велихов, А.В. Компьютерные сети : учебное пособие для вузов / А.В. Велихов. – М. : Новый издательский дом, 2005.

6. Воеводин, В.В. Параллельные вычисления / В.В. Воеводин, В.В. Воеводин. – СПб. : БВХ – Петербург, 2002.

7. Жмакин, А.П. Архитектура ЭВМ / А.П. Жмакин. – СПб. : БВХ – Петербург, 2006.

8. Комарцева, А.Г. Нейрокомпьютеры : учебное пособие для вузов / А.Г. Комарцева, А.В. Максимов. – М. : МГТУ им. Баумана, 2002.

9. Таненбаум, Э. Архитектура компьютера / Э. Таненбаум. – СПб. : Питер, 2002.

10. Цилькер, Б.Я. Организация ЭВМ и систем : учебник для вузов / Б.Я. Цилькер, С.А. Орлов. – СПб. : Питер, 2006.

11. Иванова, Т.Н. Корпоративные сети связи / Т.Н. Иванова. – М. : ЭкоТрендз, 2001.

12. Оливер, В.Г. Компьютерные сети: принципы, технологии, протоколы / В.Г. Оливер, Н.А. Оливер. – Питер, 2001.

13. Дебра, Л.Ш. Основы компьютерных сетей / Л.Ш. Дебра; перевод с англ. – М. : Издательский дом «Вильяме», 2003.

Учебное издание

СЕТИ ЭВМ И СРЕДСТВА КОММУНИКАЦИЙ

Составитель
БАЛАБАНОВ Павел Владимирович

Методические указания

Редактор Е.С. Мордасова

Инженер по компьютерному макетированию М.С. Анурьева

Подписано в печать 03.04.2012.
Формат 60 × 84 / 16. 2,56 усл. печ. л. Заказ № 235

Издательско-полиграфический центр ФГБОУ ВПО «ТГТУ»
392000, г. Тамбов, ул. Советская, д. 106, к. 14