МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

ОП.16 КОМПЬЮТЕРНЫЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ

Специальность:
09.02.01 Компьютерные системы и комплексы
Квалификация выпускника: техник по компьютерным системам
(Базовая подготовка)

Разработчик: Молочков В. П., преподаватель

Методические рекомендации приняты на заседании предметной (цикловой) комиссии дисциплин профессионального цикла специальности 09.02.01 Компьютерные системы и комплексы колледжа протокол № 1 от 04.09.2017 г.

Председатель предметной (цикловой) комиссии _____ Л. Н. Цымбалюк

Содержание

Пояснительная записка

Методические рекомендации по практическим занятиям, являющиеся частью учебно-методического комплекса по дисциплине «Компьютерные и телекоммуникационные сети», составлены в соответствии с:

- Федеральным государственным образовательным стандартом по специальности: 09.02.01 «Копьютерные системы и комплексы»
- Рабочей программой учебной дисциплины;
- Положением о планировании, организации и проведении лабораторных работ и практических занятий студентов, осваивающих основные профессиональные образовательные программы среднего профессионального образования в колледжах НовГУ.

Методические рекомендации включают 10 практических занятий, предусмотренные рабочей программой учебной дисциплины в объёме 30 часов.

В результате выполнения практических заданий обучающийся должен:

Знать/понимать

- Программное и аппаратное обеспечение локальных и глобальных сетей;
- Модели и структуры компьютерных сетей;
- Основные типы сетевых топологий, приемы работы в компьютерных сетях; информационные ресурсы компьютерных сетей;
- Технологии передачи и обмена данными в компьютерных сетях;
- Теоретические основы современных информационных сетей;
- Принципы построения и организацию функционирования вычислительных сетей, их функциональную и структурную организацию;
- Базовую эталонную модель Международной организации стандартов;
- Компоненты информационных сетей;
- Методы коммутации информации;
- Методы маршрутизации информационных потоков;
- Базовые функциональные профили сетей;
- Стандарты в области построения вычислительных управляющих сетей и протоколов передач данных;

Уметь

- Оценивать технико-эксплуатационные возможности сетей, разрабатывать программные средства передачи, приема, формирования и обработки информации;
- Разрабатывать коммуникационных программ обмена информацией;
- Осуществлять планирование информационных сетей;
- Использовать приобретённые знания и умения в практической деятельности и повседневной жизни.

Владеть

- Специальной терминологией, основами построения компьютерных сетей;
- Стандартами в области построения вычислительных управляющих сетей и протоколов передач данных;
- Приемами планирования корпоративных информационных сетей;
- Приемами разработки программных средств передачи данных с использованием протоколов TCP/IP и других.

В практических работах предлагаемые задания носят репродуктивный, частично-поисковый характер и поисковый характер. Основные теоретические положения даются студентам на лекциях. Перед проведением практического занятия проводится инструктаж,

выдается индивидуальное задание для самостоятельного выполнения. Во время проведения практической работы решение индивидуального задания проверяется, корректируется, проводится анализ решения, подводятся итоги.

Степень овладения студентами запланированных умений оценивается во время защиты практической работы. Критерием оценки практических работ является качество выполненных заданий, правильность ответов во время защиты.

- Оценка «5» ставится в случае, когда результатом работы является полностью выполненная работа, даны ответы на поставленные контрольные вопросы.
- Оценка «4» ставится, когда итогом работы является правильно выполненная практическая работа, но могут быть небольшие неточности при выполнении.
- Оценка «3» - не выполнено до конца одно из заданий, даны ответы не на все контрольные вопросы.
- Оценка «2» ставится в случае неподготовленности студента к защите практической работы.

Возможным вариантом защиты практических работ, может быть защита электронного отчёта, структура которого содержит титульный лист, цели выполнения практической работы, краткое описание работы и выводы.

Тематический план и содержание учебной дисциплины «Компьютерные и телекоммуникационные сети»

Наименование Разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	**2**	**3**	**4**
Введение	Содержание учебного материала	8	1
	Что такое компьютерная сеть. Обзор аппаратного и программного обеспечения КС		
Раздел 1. Сетевое оборудование			
Тема 1.1. Сетевое оборудование -Сетевая карта, Концентратор (хаб), Коммутатор (свитч), Маршрутизатор (роутер)	Содержание учебного материала	10	1
	Сетевые кабели. Витая пара, Коаксиальный кабель, Оптоволоконный кабель		
	Самостоятельная работа обучающихся Самостоятельная работа № 1. Сетевые адаптеры. Задание 1. Изучение сетевой карты, вынутой из ПК. Задание 2. Изучение сетевой карты, вставленной в ПК	5	
Тема 1.2. Опрессовка витой пары и розеток	Содержание учебного материала	4	1
	Обжимаем витую пару ПК (PC)-ХАБ (HUB)-Получаем прямой провод по стандарту T568B. Контроль результата. Базовые термины компьютерных сетей. Изучение сетевых протоколов - TCP/IP, ARP, http, FTP, POP, SMTP. Задание 1. Определить IP адрес вашего ПК. Задание 2. Перевод чисел из двоичной системы в десятичную и наоборот. Задание 3. Определение маски сети. Задание 4. Задание диапазона IP-адресов. IP калькуляторы. Задание 5. Определить MAC-адрес ПК		
Раздел 2. Прямое соединение узлов сети. Сетевой мост			
Тема 2.1. Для прямого соединения двух ПК (или HUB-HUB) обжимаем перекрестный	Содержание учебного материала	4	2
	Обжимаем розетку категории 5 под разъем RJ45. Обжим розетки и контроль результата. Ситуация 1. Розетка с одним гнездом на 8 проводов.		

кабель (кроссовер). Проверка правильности обжима витой пары ПК-ПК.	Ситуация 2. Розетка на 2 гнезда по 8 проводов		
	Самостоятельная работа обучающихся. Самостоятельная работа № 2. Доступ в Интернет для нескольких ПК через одно подключение. Вариант 1. Раздаем компьютерам Интернет через сетевой мост. Вариант 2. Раздаем компьютерам Интернет без создания сетевого моста	8	
	Практическая работа № 1. Сетевая карта	3	
Тема 2.2 IP адрес по протоколу IPv4. Перевод чисел из двоичной системы в десятичную и наоборот. Маска подсети (сети). Классы сетей. Задание диапазона IP-адресов. IP калькуляторы. Понятия MAC-адрес и DNS-сервер. Настройка IPv4 адресов. DNS-сервер	Содержание учебного материала		1
	Программа для изучения и моделирования компьютерных сетей NetEmul. Интерфейс программы. Пример 1. Строим сеть из двух ПК и коммутатора. Задание 1. Построить сеть из двух ПК и свитча, изучить таблицу коммутации. Пример 2. Изучаем сеть из двух подсетей и маршрутизатора. Тестирование сети (Отправка пакетов). Задание 2. Построить сеть из восьми ПК, хаба, коммутатора и роутера. Настроить ее правильную работу	4	
	Практическая работа № 2. Обжимаем витую пару	3	
	Самостоятельная работа обучающихся: Самостоятельная работа № 3. Сетевые программы для создание схем локальных сетей, администрирования, мониторинга и инвентаризации компьютерных сетей. Создание схем локальных сетей в программе 10 Страйк: Схема Сети. Практика работы в программе. Трассировка. Задание 1. Нарисовать в программе 10 Страйк Схема Сети схему сети предприятия как на рис. 13. Поясните, что за устройства присутствуют в данной сети и как они работают.	8	
Раздел 3. Сетевые программы для администраторов сетей			
Тема 3.1. Построение локальной сети на ОС Windows	Содержание учебного материала		2
	Программа построения диаграмм сети EDraw Network Diagrammer. Задание 2. В программе EDraw Network Diagrammer повторите схему, показанную на рис. 17. Поясните, что за устройства присутствуют в данной сети и как они работают. Задание 3. Повторите рисунок, изображающих расположение компьютеров в компьютерном классе.	4	
	Самостоятельная работа обучающихся: Самостоятельная работа № 4. Создание и настройка сети на базе VMware	8	

	Workstation с операционной системой Windows XP. Установка виртуальной машины на ПК. Настройка виртуальной машины.		
	Практическая работа № 3. Основы сетей (глоссарий). IP калькуляторы	3	
Раздел 4. Организация общего доступа к ресурсам сети			
Тема 4.1 Обеспечение безопасности виртуальной сети (настройка политики безопасности)	Содержание учебного материала	4	2
	Обеспечение безопасности локальной сети. Шаг. 1. Меняем учетную запись администратора (Пользователь Администратор с пустым паролем - это уязвимость). Шаг 2. Делаем окно приветствия пустым (убираем уязвимость 2). Выявление сетевых уязвимостей сканированием портов ПК. Просмотр активных подключений утилитой Netstat. Пример 1. Обнаружение открытых на ПК портов утилитой Netstat. Программа NetStat Agent. Сканер портов Nmap (Zenmap). Монитор портов TCPView. Образец офисной политики безопасности		
	Практическая работа № 4. Программа для изучения компьютерных сетей NetEmul	3	
Тема 4.2 Сетевые программы и утилиты	Содержание учебного материала	4	2
	Radmin - программа удаленного управление ПК по сети. Знакомство с системой моделирования (имитации) реальной сетевой среды S2 Netest. Сетевое оборудование эмулятора сети S2 Netest. Главное окно программы (Интерфейс). Примеры выполнения тестов. Сетевые решения оптимальные и неудачные. Задание 1. Посмотрите на рис. 14 и назовите эти устройства и их характеристики. Задание 2. Постройте следующую схему (рис. 15) и кнопкой Проверка убедитесь в том, что она работает верно. Задание 3. Проверка оптимальности построения сети		
	Практическая работа № 5. Сетевые программы для создания схем локальных сетей, администрирования, мониторинга и инвентаризации компьютерных сетей.	3	
	Практическая работа № 6. Создание виртуальной машины VMware Workstation 6 с операционной системой Windows	3	
	Практическая работа № 7. Настройка связи между ПК в виртуальной сети.	3	
	Самостоятельная работа обучающихся: Самостоятельная работа № 5. Создание и настройка локальной сети	10	

Раздел 5. Построение локальной сети на ОС Windows 7			
Тема 5.1. Домашняя группа	Содержание учебного материала	6	2
	Основные элементы управления сетью в интерфейсе Windows 7. Создание общего доступа к ресурсам сети в ОС Windows 7. Центр управления сетями и общим доступом и сетевое размещение. Карта сети и просмотр сетевых подключений. Сведения о сетевом подключении. Сетевые профили и сетевое обнаружение . Подключение общего доступа к папкам. Общий доступ с парольной защитой. Задание 1. Произведите отключение пользователя от папки с общим доступом		
	Практическая работа № 8. Создаем общий доступ к ресурсам сети	3	
	Практическая работа № 9. Обеспечение (настройка) безопасности локальной сети	3	
	Практическая работа № 10. Программа для изучения компьютерных сетей S2 Netest	3	
	Всего	**117**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

Содержание практических занятий

Раздел 2. Прямое соединение узлов сети. Тема 2.1. Для прямого соединения двух ПК (или HUB-HUB) обжимаем перекрестный кабель (кроссовер). Проверка правильности обжима витой пары ПК-ПК. Практическая работа № 1. Сетевые карты. Объём учебного времени – 3 ч.

1. Цель занятия:

- изучить устройство сетевой карты

2. Перечень необходимых средств обучения (оборудование, материалы)

– технические средства обучения: персональные компьютеры, локальная сеть, Internet

Используемое программное обеспечение:

Операционная система Microsoft Windows XP/7

3. Содержание заданий

Подробно описано здесь: http://www.intuit.ru/department/network/baslocnet/1/

Сетевая карта — это часть аппаратной конфигурации компьютера. Данное устройство позволяет нам подключать компьютер к сети и обеспечивает с ней взаимодействие. Сетевые карты часто называют сетевыми интерфейсными картами, сетевыми адаптерами или LAN-адаптерами.

Сетевые карты изначально являлись дополнительным компонентом, который можно было приобрести и установить на компьютер не сразу, а спустя какое-то время. Однако на сегодняшний день стало очевидным то, что сетевые карты являются стандартным компонентом компьютера, который устанавливают в большинство продаваемых ноутбуков и компьютеров.

Зачастую, их интегрируют в материнские платы или другие устройства еще в процессе изготовления. Если карту устанавливают в компьютерную систему, то она обнаруживает себя при подключении к сети небольшими мерцающими светодиодами, которые располагаются у сетевого разъема.

Идентификация сетевой карты

Любая сетевая карта должна быть уникальной, поэтому их оснащают адресом, который сокращенно принято называть MAC. С помощью него можно провести идентификацию любого компьютера, передающего данные через сеть.

Что такое беспроводная сетевая карта

В наше время, при помощи сетевых карт, можно подключать компьютеры, используя кабельное (физическое) подключение или же и вовсе обойтись без него, воспользовавшись, так называемым, беспроводным интерфейсом. Используя кабельное подключение, обычно выбирают стандартный сетевой порт, который имеет разъем формата «RJ-45». Для беспроводного подключения к сети использование различных физических портов и интерфейсов не требуется.

Принцип работы беспроводной карты довольно прост. За прием и передачу данных из сети Интернет отвечает беспроводной модем. Данные от вашего провайдера поступят на внешний порт (кабельный вход) беспроводного роутера, после чего они будут преобразованы в радиосигнал, который будет передан в эфир через антенну. Если беспроводные сетевые карты находятся в поле действия передатчика роутера, то они получат сигнал, после чего преобразуют его в электронный, понятный компьютеру сигнал.

В любом случает, кроме того, что беспроводная сетевая карта не требует физического контакта с ней, настройка ее ничем не отличается от обычной. Как

беспроводные, так и проводные карты в настоящее время позволяют развивать практически одинаковую скорость передачи данных.

4. Содержание отчёта:

- постановка задачи;
- электронная версия выполненного задания;
- ответы на вопросы;

5. Контрольные вопросы

- Назначение индикаторов адаптера
- Мас адрес сетевой карты
- Интерфейсы сетевых карт

6. Список рекомендуемой литературы:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб. Питер, 2015.

2. Шурыгин В.Н., Ковалев И.В. Информационные сети. Методические указания по выполнению лабораторных работ. МГУП 2014

3. Основы построения телекоммуникационных систем и сетей: Учебник для вузов / В.В. Крухмалев, В.Н. Гордиенко, А.Д. Моченов и др.; Под ред. В.Н. Гордиенко и В.В. Крухмалева. – 2-е изд., испр. – М.: Горячая линия – Телеком, 2016. - 424 с.

Раздел 2. Прямое соединение узлов сети. Тема 2.2. IP адрес по протоколу IPv4. Перевод чисел из двоичной системы в десятичную и наоборот. Маска подсети (сети). Классы сетей. Задание диапазона IP-адресов. IP калькуляторы. Понятия MAC-адрес и DNS-сервер. Настройка IPv4 адресов. DNS-сервер. Практическая работа № 2. Обжимаем витую пару. Объём учебного времени – 3 ч.

1. Цель занятия:

- научиться монтировать разъем и розетку на кабель 5й категории.

2. Перечень необходимых средств обучения (оборудование, материалы):

– технические средства обучения: персональные компьютеры, локальная сеть, Internet

Используемое программное обеспечение:

Операционная система Microsoft Windows XP/7

3. Содержание заданий

Подробно описано здесь: http://www.intuit.ru/department/network/baslocnet/2/

Для обжима кабеля потребуется:

Обжимной инструмент

Коннекторы RJ 45 Как правило, используются 3'й категории (самые обычные), хотя, понятия "категория" к коннекторам на самом деле не применяется. Просто бывают коннекторы разной конструкции.

Кабель (желательно 5'ой категории. Категория указывается рядом с маркировкой производителя на самом кабеле через каждый метр). По стандарту T568B:

Оранжево-белый
Оранжевый
Зелено-белый
Синий
Сине-белый
Зеленый

Коричнево-белый
Коричневый
5. Контрольные вопросы

- Какой порядок обжима проводов для прямого и перекрестного кабеля?
- Каковы правила монтажа розеток 5й категории?

6. Список рекомендуемой литературы:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб. Питер, 2015.
2. Шурыгин В.Н., Ковалев И.В. Информационные сети. Методические указания по выполнению лабораторных работ. МГУП 2014
3. Основы построения телекоммуникационных систем и сетей: Учебник для вузов / В.В. Крухмалев, В.Н. Гордиенко, А.Д. Моченов и др.; Под ред. В.Н. Гордиенко и В.В. Крухмалева. – 2-е изд., испр. – М.: Горячая линия – Телеком, 2016. - 424 с.

Раздел 3. Сетевые программы для администраторов сетей. Тема 3.1. Построение локальной сети на ОС Windows. Практическая работа № 3. Основы сетей (глоссарий). IP калькуляторы. Объём учебного времени – 3 ч.

1. Цель занятия:
- научиться определять основные характеристики сетей
2. Перечень необходимых средств обучения (оборудование, материалы):
– технические средства обучения: персональные компьютеры, локальная сеть, Internet

Используемое программное обеспечение:
Операционная система Microsoft Windows XP/7

3. Содержание заданий

Подробно описано здесь: http://www.intuit.ru/department/network/baslocnet/5/

Компьютерная сеть – это совокупность компьютеров, объединенных каналами передачи данных. В зависимости от расстояния между компьютерами различают следующие вычислительные сети:

Локальные вычислительные сети - LAN;

Территориальные вычислительные сети, к которым относятся региональные MAN и глобальные WAN сети;

Корпоративные сети.

Локальная сеть - это ЛВС, в которой ПК и коммуникационное оборудование находится на небольшом расстоянии друг от друга. ЛВС обычно предназначена для сбора, хранения, передачи, обработки и предоставления пользователям распределенной информации в пределах подразделения или фирмы. Кроме того, ЛВС, как правило, имеет выход в Интернет.

Локальные сети можно классифицировать по:

Уровню управления;

Назначению;

Однородности;

Административным отношениям между компьютерами;

Топологии;

Архитектуре.

По уровню управления выделяют следующие ЛВС:

ЛВС рабочих групп, которые состоят из нескольких ПК, работающих под одной операционной системой. В такой ЛВС, как правило, имеется несколько выделенных серверов: файл-сервер, сервер печати;

ЛВС структурных подразделений (отделов). Данные ЛВС содержат несколько десятков ПК и серверы типа: файл-сервер, сервер печати, сервер баз данных;

ЛВС предприятий (фирм). Эти ЛВС могут содержать свыше 100 компьютеров и серверы типа: файл-сервер, сервер печати, сервер баз данных, почтовый сервер и другие серверы.

По назначению сети подразделяются на:

Вычислительные сети, предназначенные для расчетных работ;

Информационно-вычислительные сети, которые предназначены, как для ведения расчетных работ, так и для предоставления информационных ресурсов;

Информационно-советующие, которые на основе обработки данных вырабатывают информацию для поддержки принятия решений;

Информационно-управляющие сети, которые предназначены для управления объектов на основе обработки информации.

По типам используемых компьютеров можно выделить:

Однородные сети, которые содержат однотипные компьютеры и системное программное обеспечение;

Неоднородные сети, которые содержат разнотипные компьютеры и системное программное.

По административным отношениям между компьютерами можно выделить:

ЛВС с централизованным управлением (с выделенными серверами);

ЛВС без централизованного управления (децентрализованные) или одноранговые (одноуровневые) сети.

По топологии (основным топологиям) ЛВС делятся на:

Топологию "шина";

Топологию "звезда";

Топологию "кольцо".

По архитектуре (основным типам архитектур) ЛВС делятся на:

Ethernet;

Arcnet;

Token ring;

FDDI.

Сетевой калькулятор. Необходим IT-специалистам для корректного расчёта маски подсети. Введите IP-адрес (можно вводить как адрес сети, так и хост внутри неё), и получите требуемый результат

4. Содержание отчёта:

- постановка задачи;
- электронная версия выполненного задания;
- ответы на вопросы;

5. Контрольные вопросы

1. Определите адрес сети и адрес узла, если:

IP-адрес: 00001100 00100010 00111000 01001110 (12.34.56.78)

Маска подсети: 11111111 11111111 11100000 00000000 (255.255.224.0)

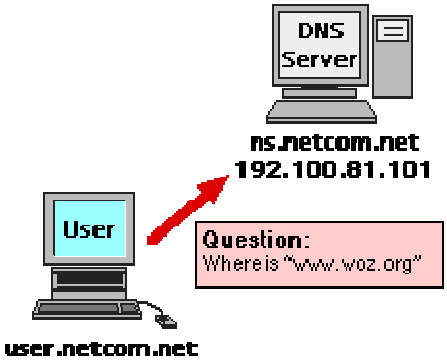
3. Подтвердите или опровергните следующие вычисления путем выполнения логического И:

ip адрес	129.64.134.5	10000001. 01000000.10000110. 00000101
маска подсети	255.255.128.0	11111111.11111111.10000000. 00000000
номер сети	129.64.128.0	10000001.01000000.10000000. 00000000
номер узла	0.0.6.5	00000000.00000000.00000110.00000101

ip адрес	12.34.56.78	00001100 00100010 00111000 01001110
маска подсети	255.255.255.224	11111111 11111111 11111111 11100000
адрес сети	12.34.48.64	00001100 00100010 00110000 01000000
адрес узла	0.0.0.224	0.0.0.11100000

IP-адрес	169.234.93.171	10101001.11101010.01011101.10101011
Маска подсети	255.255.0.0	11111111.11111111.00000000.00000000
Адрес сети	169.234.0.0	10101001.11101010.00000000.00000000
Адрес узла	0.0.93.171	00000000.00000000.01011101.10101011

Поясните картинку ниже:



Список рекомендуемой литературы:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб. Питер, 2015.
2. Шурыгин В.Н., Ковалев И.В. Информационные сети. Методические указания по выполнению лабораторных работ. МГУП 2014
3. Основы построения телекоммуникационных систем и сетей: Учебник для вузов / В.В. Крухмалев, В.Н. Гордиенко, А.Д. Моченов и др.; Под ред. В.Н. Гордиенко и В.В. Крухмалева. – 2-е изд., испр. – М.: Горячая линия – Телеком, 2016. - 424 с.

Раздел 4. Организация общего доступа к ресурсам сети. Тема 4.1. Обеспечение безопасности виртуальной сети (настройка политики безопасности). Практическая работа № 4. Программа для изучения компьютерных сетей NetEmul. Объём учебного времени – 3 ч.

1. Цель занятия:

- научиться моделировать работу локальной сети.

2. Перечень необходимых средств обучения (оборудование, материалы):

– технические средства обучения: персональные компьютеры, локальная сеть, Internet

Используемое программное обеспечение:

Операционная система Microsoft Windows XP/7

3. Содержание заданий

Подробно описано здесь: http://www.intuit.ru/department/network/baslocnet/5/

Бесплатная программа NetEmul была создана для визуализации работы компьютерных сетей, для облегчения понимания происходящих в ней процессов.

Сайт проекта: http://netemul.sourceforge.net. Руководство пользователя Netemul расположено здесь: http://netemul.sourceforge.net/help/ru/index.html.

Для начала установим программу, запустим и русифицируем ее.

Построим простейшую локальную сеть и посмотрим, как она работает. Для этого выполните команду Файл > Новый и нарисуйте схему сети как на рисунке.

После рисования двух ПК и концентратора создадим их соединение.

В процессе рисования связей между устройствами вам потребуется выбрать соединяемые интерфйсы и нажать на кнопку Соединить.

Теперь добавляем сетевую карту (интерфейс) и настраиваем ее.

Сеть создана и настроена. Отравляем данные по протоколу TCP.

Если вы где-то ошиблись, то появиться соответствующее сообщение, а если все верно – то анимация движущихся по сети пакетов.

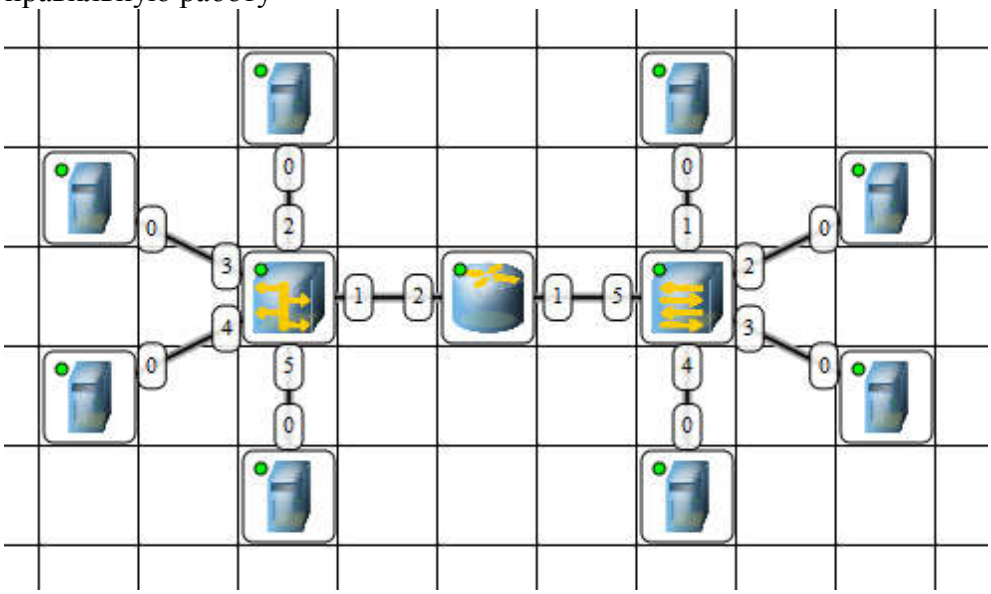
Само собой, что в программе можно строить сети более сложные, чем мы рассмотрели выше.

4. Содержание отчёта:

- постановка задачи;
- электронная версия выполненного задания;
- ответы на вопросы;

5. Контрольные вопросы

Построить сеть из восьми ПК, хаба, коммутатора и роутера. Настроить ее правильную работу



Список рекомендуемой литературы:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб. Питер, 2015.
2. Шурыгин В.Н., Ковалев И.В. Информационные сети. Методические указания по выполнению лабораторных работ. МГУП 2014
3. Основы построения телекоммуникационных систем и сетей: Учебник для вузов / В.В. Крухмалев, В.Н. Гордиенко, А.Д. Моченов и др.; Под ред. В.Н. Гордиенко и В.В. Крухмалева. – 2-е изд., испр. – М.: Горячая линия – Телеком, 2016. - 424 с.

Раздел 4. Организация общего доступа к ресурсам сети. Тема 4.2 Сетевые программы и утилиты. Практическая работа № 5. Сетевые программы для создания схем локальных сетей, администрирования, мониторинга и инвентаризации компьютерных сетей. Объём учебного времени – 3 ч.

1. Цель занятия:

- научиться работе со шрифтом и текстом в среде графического редактора

2. Перечень необходимых средств обучения (оборудование, материалы):

– технические средства обучения: персональные компьютеры, локальная сеть, Internet

Используемое программное обеспечение:

Операционная система Microsoft Windows XP/7

3. Содержание заданий

Подробно описано здесь: http://www.intuit.ru/department/network/baslocnet/6/

CADE (бесплатная)

Векторный 2D-редактор CADE для Windows разработан компанией, специализирующейся на работе с САПР. Программа позволяет с легкостью составить подробную схему сети. Одна из самых полезных, на мой взгляд, функций — возможность подписать IP-адрес, серийный номер и название фирмы-производителя для каждого устройства в сети. CADE включает все необходимые для составления схемы шаблоны и распространяется абсолютно бесплатно.

Concept Draw Pro

Concept Draw Pro — один из наиболее мощных бизнес-инструментов для составления диаграмм, причем не только сетевых. На освоение программы требуется минимум времени — все операции осуществляются простым перетаскиванием. В состав Concept Draw Pro входит полный набор сетевых символов, а все аспекты диаграммы можно персонализировать. Стоимость приложения — 249 долларов.

Dia (бесплатная)

Dia — открытое ПО для составления диаграмм, главным недостатком которого является устаревший интерфейс и примитивный набор символов. Зато программу очень легко использовать, не отвлекаясь ни на какие посторонние задачи. Dia распространяется бесплатно и работает практически во всех настольных дистрибутивах Linux.

Diagram Designer (бесплатная)

Diagram Designer — еще одна бесплатная утилита с устаревшим интерфейсом, зато очень простая в обращении, благодаря чему наверняка придется по вкусу многим пользователям. В отличие от Dia, программа предлагает куда более широкий выбор символов и значков. Единственное, что мне не понравилось в Diagram Designer, — это необходимость рисовать соединения между компьютерами вручную, потому что для этого в программе используется произвольная форма. За исключением этого небольшого недостатка, DD — вполне достойное решение.

eDraw Max

eDraw Max — один из лучших инструментов в этом списке, за исключением, разумеется, Visio. Программа проста в освоении, обладает удобным, и притом наиболее современным пользовательским интерфейсом из всех перечисленных вариантов. eDraw Max представляет собой полофункциональное средство для составления бизнес-диаграмм любого назначения, а не только сетевых схем. Стоимость решения составляет 99,95 долларов за одну лицензию, причем чем больше лицензий, тем дешевле стоит каждая из них.

GoVisual Diagram Editor (бесплатная)

Бывают на редкость неудачные программы, и GoVisual Diagram Editor — одна из них. Это сложный в обращении инструмент, обеспечивающий далеко не удовлетворительные результаты. Хотя с его помощью все-таки можно составить схему сети, она будет не особенно удобна для чтения, поскольку в GoVisual Diagram Editor отсутствуют некоторые полезные функции — в частности, значки сетевых устройств. Но если кому-то нужна бесплатная программа для составления диаграмм любого назначения, GoVisual — как раз подходящий вариант, потому что распространяется даром.

LanFlow

LanFlow я бы включил в число лучших. Программа обладает превосходным интерфейсом, предлагает богатый выбор сетевых объектов и позволяет с легкостью создавать схемы локальной, телекоммуникационной, внешней сети, а также диаграммы компьютеров. В LanFlow даже предусмотрено два разных шаблона сетевых диаграмм: 3D-схема и черно-белая. Чтобы создать схему, достаточно выбрать шаблон и перетащить на него подходящие объекты, которые можно группировать, удалять и так далее. Однопользовательская лицензия на программу стоит 89 долларов, так что LanFlow по праву может называться одной из лучших бюджетных альтернатив Visio.

NetProbe

Хотя NetProbe можно использовать и для составления схем, основное назначение программы — это мониторинг сетевых устройств в режиме реального времени. Но главное достоинство NetProbe как средства для построения диаграмм заключается в том, что сетевые устройства можно добавлять на схему по мере необходимости, причем даже заранее. Делать это вручную не обязательно — встроенный компонент NetProbe автоматически сканирует сеть и составляет список всех доступных в сети устройств. Версия Standard бесплатна, но может отслеживать всего восемь хостов. Версия Pro стоит всего 40 долларов и рассчитана на 20 хостов, а версия Enterprise, позволяющая вести мониторинг 400 хостов, предлагается по цене 295 долларов.

Network Notepad (бесплатная)

Network Notepad (буквально «сетевой блокнот») представляет собой именно то, что следует из названия — блокнот для составления сетевых диаграмм. Но несмотря на кажущуюся простоту, программа обладает богатыми возможностями, включая интерактивные функции (Telnet, просмотр сети, пингование и т. д.). Network Notepad имеет простой интерфейс с поддержкой перетаскивания и умеет автоматически обнаруживать устройства Cisco. Распространяется программа бесплатно.

Microsoft Visio

Visio — это, конечно, фактический стандарт на рынке приложений для составления диаграмм в Windows. Программа позволяет с легкостью создавать красивые схемы сети и обеспечивать к ним общий доступ через веб-браузер. Visio включает богатый набор шаблонов, в том числе для центров обработки данных, служб помощи, сетевых стоек; для консолидации офиса, планирования сети в масштабах предприятия, ЦОД или домашнего офиса; для составления дерева неисправностей, плана отопления, вентиляции, кондиционирования и т. п. Visio — лучшее решение для составления сетевых схем, а потому и стоит оно недешево: 249,99 долларов за версию Standard, 559,99 за Professional и 999,99 за Premium 2010.

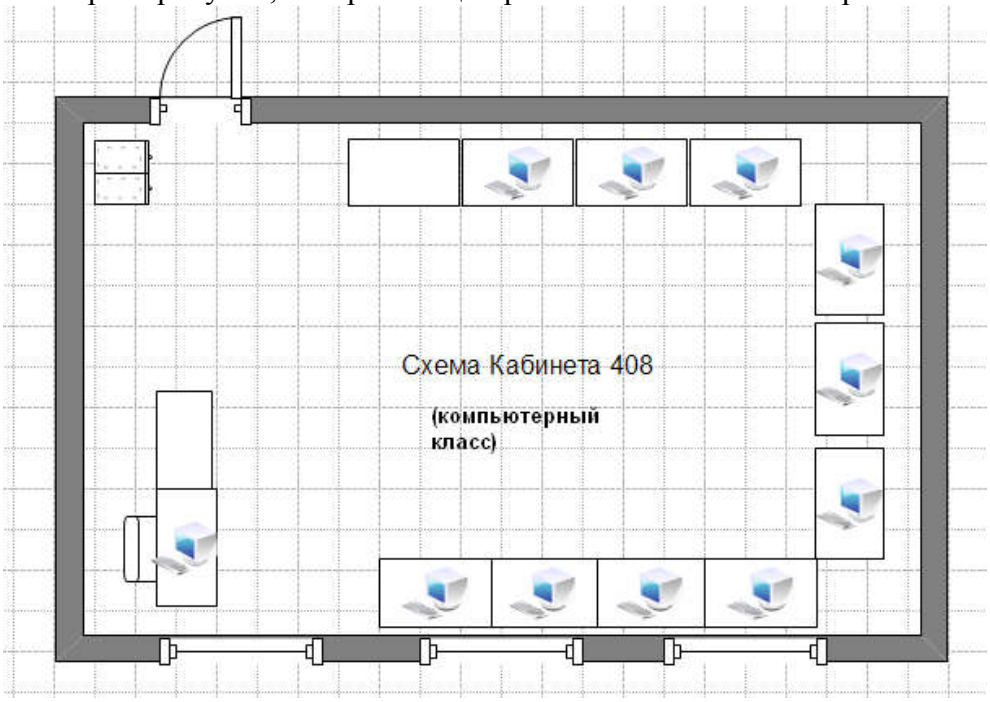
4. Содержание отчёта:

- постановка задачи;
- электронная версия выполненного задания;
- ответы на вопросы;

5. Контрольные вопросы

В программе EDraw Network Diagrammer повторите схему, показанную на рис. ниже. Поясните, что за устройства присутствуют в данной сети и как они работают.

Повторите рисунок, изображающих расположение компьютеров в компьютерном классе



Список рекомендуемой литературы:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб. Питер, 2015.
2. Шурыгин В.Н., Ковалев И.В. Информационные сети. Методические указания по выполнению лабораторных работ. МГУП 2014
3. Основы построения телекоммуникационных систем и сетей: Учебник для вузов / В.В. Крухмалев, В.Н. Гордиенко, А.Д. Моченов и др.; Под ред. В.Н. Гордиенко и В.В. Крухмалева. – 2-е изд., испр. – М.: Горячая линия – Телеком, 2016. - 424 с.

Раздел 4. Организация общего доступа к ресурсам сети. Тема 4.2 Сетевые программы и утилиты. Практическая работа № 6.

Создание виртуальной машины VMware Workstation 6 с операционной системой Windows. Объём учебного времени – 3 ч.

1. Цель занятия:

- научиться создавать рамочки для фотоснимков.

2. Перечень необходимых средств обучения (оборудование, материалы):

– технические средства обучения: персональные компьютеры, локальная сеть, Internet

Используемое программное обеспечение:

Операционная система Microsoft Windows XP/7

3. Содержание заданий

Подробно описано здесь: http://www.intuit.ru/department/network/baslocnet/7/

VMware Workstation v11.0.0 Build 2305329 Final for Windows & Linux

Год/Дата Выпуска: 2014

Разрядность: ТОЛЬКО 64bit

Язык интерфейса: Английский

Системные требования:

Windows - 7, 8, Server 2008, Server 2012

VMware Workstation — известная программа для виртуализации систем. VMware Workstation является мощным решением для разработчиков программного обеспечения и системных администраторов, создающих и тестирующих полно-комплексные сетевые приложения класса серверов, работающие в различных средах. Уникальная технология VMware MultipleWorlds позволяет изолировать операционные системы и приложения в пределах создаваемых виртуальных машин, причем в распоряжении каждой виртуальной машины оказывается стандартный компьютер x86, с собственным процессором и памятью. С помощью данного решения вы сможете на одном компьютере вести процессы разработки, тестирования, отладки и запуск многоуровневых браузерных приложений, эксплуатировать новые операционные системы и унаследованные приложения на одном компьютере, устанавливать новые или обновлять имеющиеся операционные системы без выполнения операций с разделами дисков и перезагрузки компьютера.

Основные возможности:

▪ Одновременный запуск нескольких гостевых операционных систем на одном компьютере

▪ Запуск виртуальной машины в окнах рабочего стола основной операционной системы и на полный экран

▪ Установка виртуальных машин без переразбиения дисков

▪ Запуск уже установленных на компьютере ОС без их переустановки или переконфигурирования

▪ Запуск приложений операционной системы Windows на компьютере с ОС Linux и наоборот

▪ Создание и тестирование приложений одновременно для разных систем

▪ Запуск непротестированных приложений без риска нарушить устойчивую работу системы или потерять критичные данные

▪ Совместное использование файлов и приложений разными виртуальными машинами за счет использования виртуальной сети

▪ Запуск клиент-серверных и веб-приложений на одном ПК

▪ Запуск на одном ПК нескольких виртуальных компьютеров и моделирование работы локальной сети

4. Содержание отчёта:

- постановка задачи;

- электронная версия выполненного задания;

- ответы на вопросы;

5. Контрольные вопросы

- Назначение виртуальной машины
- Как настроить виртуальную машину
- Как установить на виртуальную машину ОС Windows XP, используя ISO образ этой операционной системы
- Зачем необходимо клонирование виртуальной машины

6. Список рекомендуемой литературы:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб. Питер, 2015.
2. Шурыгин В.Н., Ковалев И.В. Информационные сети. Методические указания по выполнению лабораторных работ. МГУП 2014
3. Основы построения телекоммуникационных систем и сетей: Учебник для вузов / В.В. Крухмалев, В.Н. Гордиенко, А.Д. Моченов и др.; Под ред. В.Н. Гордиенко и В.В. Крухмалева. – 2-е изд., испр. – М.: Горячая линия – Телеком, 2016. - 424 с.

Раздел 4. Организация общего доступа к ресурсам сети. Тема 4.2 Сетевые программы и утилиты. Практическая работа № 7. Настройка связи между ПК в виртуальной сети. Объём учебного времени – 3 ч.

1. Цель занятия:

- научиться настраивать обмен данными в сети.

2. Перечень необходимых средств обучения (оборудование, материалы):

– технические средства обучения: персональные компьютеры, локальная сеть, Internet

Используемое программное обеспечение:

Операционная система Microsoft Windows XP/7

3. Содержание заданий

Подробно описано здесь: http://www.intuit.ru/department/network/baslocnet/8/

Запускаем обе, ранее созданные нами виртуальные машины командой ВМ - Питание Power On. Для работы в сети настроем сначала первую машину. Для этого в Панели управления найдем Сетевые подключения-Подключение по локальной сети-Свойства, затем находим свойства Протокола Интернет (TCP/IP) и пишем IP-адрес и Маску подсети.

Совет

Вам придется периодически переходить от окна физического ПК к окну виртуального ПК. Для этого нажимайте на сочетания клавиш Ctrl+Alt.

Аналогично включим и настроим вторую машину/ Затем настраиваем виртуальную сеть.

Для настройки сети выполним команду Сетевое окружение-Установить домашнюю или малую сеть.

Выбираем переключатель Другое. Присвоим машине сетевое имя и описание.

На следующем шаге (нажав Далее) создадим рабочую группу 110.

Устанавливаем первый переключатель снизу. Теперь машина настроена для работы в сети, перезагружаем ее и аналогично настроим другой виртуальный ПК, также включив его в рабочую группу 110. Перезагружаем.

4. Содержание отчёта:

- постановка задачи;
- электронная версия выполненного задания;
- ответы на вопросы;

5. Контрольные вопросы

- Настраиваем виртуальный ПК для работы в сети
- Настраиваем рбч группу, маску подсети, IP адрес
- Проверяем работу виртуальных машин в сети
- Установка средств Wmware

6. Список рекомендуемой литературы:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб. Питер, 2015.
2. Шурыгин В.Н., Ковалев И.В. Информационные сети. Методические указания по выполнению лабораторных работ. МГУП 2014
3. Основы построения телекоммуникационных систем и сетей: Учебник для вузов / В.В. Крухмалев, В.Н. Гордиенко, А.Д. Моченов и др.; Под ред. В.Н. Гордиенко и В.В. Крухмалева. – 2-е изд., испр. – М.: Горячая линия – Телеком, 2016. - 424 с.

Раздел 5. Построение локальной сети на ОС Windows 7 Ultimate (Максимальная). Тема 5.1. Домашняя группа. Практическая работа № 8. Создаем общий доступ к ресурсам сети. Объём учебного времени – 3 ч.

1. Цель занятия:

- научиться коррекции цифровых изображений.

2. Перечень необходимых средств обучения (оборудование, материалы):

– технические средства обучения: персональные компьютеры, локальная сеть, Internet

Используемое программное обеспечение:

Операционная система Microsoft Windows XP/7

3. Содержание заданий

Подробно описано здесь: http://www.intuit.ru/department/network/baslocnet/11/

Для работы в локальной сети служит системная папка Сетевое окружение, в которой отображаются все доступные ресурсы ЛВС.

Для отображения списка всех компьютеров, входящих в рабочую группу, необходимо щелкнуть мышью на пункте "Отобразить компьютеры рабочей группы" в командной панели "Сетевые задачи" окна "Сетевое окружение".

Дважды щелкнув мышью на значке любого из удаленных компьютеров в окне "Сетевое окружение", можно увидеть, какие его ресурсы доступны для работы. С этими удаленными ресурсами можно работать так же, как с файлами локальных дисков в программе Проводник.

Управление сетевым доступом к дискам, папкам, принтеру

Для того чтобы другие пользователи ЛВС могли обращаться к ресурсам вашего ПК, таким как принтер, логические диски, папки и файлы, необходимо открыть сетевой доступ к этим ресурсам и установить права пользователей для работы с каждым из этих ресурсов.

Доступ к дискам

Можно открыть пользователям локальной сети доступ к дискам ПК, что позволяет им просматривать, редактировать и сохранять файлы на этих дисках. Чтобы открыть пользователям доступ к дисковым ресурсам вашего ПК, необходимо выполнить следующее:

Откройте системную папку "Мой компьютер" и выберите требуемый диск, например диск Е.

Щелкните на значке диска правой кнопкой мыши и выберите из контекстного меню команду "Общий доступ и безопасность... "

В появившемся окне диалога "Свойства: Локальный диск (Е)" установите переключатель в положение "Открыть общий доступ к этой папке". В текстовой строке "Общий ресурс" появится надпись "Е"

Установите предельное число пользователей

Для выбора прав доступа к общему диску нажмите кнопку "Разрешение"

В открывшемся окне диалога "Разрешение для Е" установите пользователей и права пользователей.

Доступ к папкам

Чтобы настроить сетевой доступ к какой-либо папке на жестком диске компьютера, необходимо выполнить:

Щелкните на значке требуемой папки правой кнопкой мыши и выберите из контекстного меню команду "Общий доступ и безопасность... "

Далее выполнить все действия аналогичные действиям при назначении общего доступа к диску.

Доступ к принтеру

Для того чтобы открыть пользователям ЛВС доступ к принтеру, который подключен к вашему ПК, необходимо выполнить следующее:

Выполните команду "Пуск" - "Настройка" - "Панель управления" - "Принтеры и факсы"

Щелкните на значке локального принтера, подключенного к этому компьютеру, правой кнопкой мыши и выберите из контекстного меню команду "Общий доступ"

На вкладке "Доступ" установите переключатель в положение "Общий доступ к данному принтеру "

Щелкните на кнопках "Применить" и "ОК" в окне, чтобы сохранить внесенные изменения.

Подключение сетевого принтера

Принтер, подключенный к одному из компьютеров локальной сети, можно использовать для распечатки документа с любого компьютера сети. Для этого компьютер локальной сети, к которому подключен принтер, должен разрешить доступ к принтеру другим пользователям сети, т.е. должен быть установлен режим "Общий доступ к данному принтеру ".

Далее необходимо выполнить настройку ПК, с которого будет осуществляться распечатка документа:

Выполните команду "Пуск" - "Настройка" - "Панель управления" - "Принтеры и факсы"

Выберите команду "Файл" - "Установить принтер"

В появившемся окне "Мастер установки принтеров" нажмите на кнопке "Далее"

В следующем окне выберите пункт "Сетевой принтеров или принтер, подключенный к другому компьютеру" и щелкните "Далее"

В следующем окне установите переключатель в положение "Обзор принтеров" и щелкните "Далее"

В предложенном списке принтеров, доступных для работы в локальной сети, выберите требуемый принтер и нажмите на кнопке "Далее"

В окне "Использовать этот принтер по умолчанию" установите переключатель в положение "Да".

4. Содержание отчёта:

- постановка задачи;
- электронная версия выполненного задания;
- ответы на вопросы;

5. Контрольные вопросы

- Как произвести поиск других ПК в сети?
- Настройка общего доступа к сетевым ресурсам
- Простой общий доступ к файлам
- Расширенный общий доступ к файлам
- Возможные проблемы с общим доступом к ресурсам сети
- Как создать сетевой диск Z, общий для всех ПК
- Как настроить доступ к принтеру в локальной сети

6. Список рекомендуемой литературы:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб. Питер, 2015.
2. Шурыгин В.Н., Ковалев И.В. Информационные сети. Методические указания по выполнению лабораторных работ. МГУП 2014
3. Основы построения телекоммуникационных систем и сетей: Учебник для вузов / В.В. Крухмалев, В.Н. Гордиенко, А.Д. Моченов и др.; Под ред. В.Н. Гордиенко и В.В. Крухмалева. – 2-е изд., испр. – М.: Горячая линия – Телеком, 2016. - 424 с.

Раздел 5. Построение локальной сети на ОС Windows 7 Ultimate (Максимальная). Тема 5.1. Домашняя группа. Практическая работа № 9. Обеспечение (настройка) безопасности локальной сети. Объём учебного времени – 3 ч.

1. Цель занятия:

- научиться настраивать безопасную работу в сетях

2. Перечень необходимых средств обучения (оборудование, материалы):

– технические средства обучения: персональные компьютеры, локальная сеть, Internet

Используемое программное обеспечение:

Операционная система Microsoft Windows XP/7

3. Содержание заданий

Подробно описано здесь: http://www.intuit.ru/department/network/baslocnet/9/

Идеальная безопасность — недостижимый миф, который могут реализовать, в лучшем случае, только несколько профессионалов. Есть один фактор, который невозможно преодолеть на пути к идеальной безопасности — это человек.

Часть 1. Основные цели сетевой безопасности

Цели сетевой безопасности могут меняться в зависимости от ситуации, но основных целей обычно три:

Целостность данных.

Конфиденциальность данных.

Доступность данных.

Рассмотрим более подробно каждую из них.

Целостность данных

Одна из основных целей сетевой безопасности — гарантированность того, чтобы данные не были изменены, подменены или уничтожены. Целостность данных должна гарантировать их сохранность как в случае злонамеренных действий, так и случайностей. Обеспечение целостности данных является обычно одной из самых сложных задач сетевой безопасности.

Конфиденциальность данных

Второй главной целью сетевой безопасности является обеспечение конфиденциальности данных. Не все данные можно относить к конфиденциальной информации. Существует достаточно большое количество информации, которая должна быть доступна всем. Но даже в этом случае обеспечение целостности данных, особенно открытых, является основной задачей. К конфиденциальной информации можно отнести следующие данные:

Личная информация пользователей.

Учетные записи (имена и пароли).

Данные о кредитных картах.

Данные о разработках и различные внутренние документы.

Бухгалтерская информация.

Доступность данных

Третьей целью безопасности данных является их доступность. Бесполезно говорить о безопасности данных, если пользователь не может работать с ними из-за их недоступности. Вот приблизительный список ресурсов, которые обычно должны быть «доступны» в локальной сети:

Принтеры.

Серверы.

Рабочие станции.

Данные пользователей.

Любые критические данные, необходимые для работы.

Рассмотрим угрозы и препятствия, стоящие на пути к безопасности сети. Все их можно разделить на две большие группы: технические угрозы и человеческий фактор.

Технические угрозы:

Ошибки в программном обеспечении.

Различные DoS- и DDoS-атаки.

Компьютерные вирусы, черви, троянские кони.

Анализаторы протоколов и прослушивающие программы («снифферы»).

Технические средства съема информации.

Ошибки в программном обеспечении

Самое узкое место любой сети. Программное обеспечение серверов, рабочих станций, маршрутизаторов и т. д. написано людьми, следовательно, оно практически всегда содержит ошибки. Чем выше сложность подобного ПО, тем больше вероятность обнаружения в нем ошибок и уязвимостей. Большинство из них не представляет никакой опасности, некоторые же могут привести к трагическим последствиям, таким, как

получение злоумышленником контроля над сервером, неработоспособность сервера, несанкционированное использование ресурсов (хранение ненужных данных на сервере, использование в качестве плацдарма для атаки и т.п.). Большинство таких уязвимостей устраняется с помощью пакетов обновлений, регулярно выпускаемых производителем ПО. Своевременная установка таких обновлений является необходимым условием безопасности сети.

DoS- и DDoS-атаки

Denial Of Service (отказ в обслуживании) — особый тип атак, направленный на выведение сети или сервера из работоспособного состояния. При DoS-атаках могут использоваться ошибки в программном обеспечении или легитимные операции, но в больших масштабах (например, посылка огромного количества электронной почты). Новый тип атак DDoS (Distributed Denial Of Service) отличается от предыдущего наличием огромного количества компьютеров, расположенных в большой географической зоне. Такие атаки просто перегружают канал трафиком и мешают прохождению, а зачастую и полностью блокируют передачу по нему полезной информации. Особенно актуально это для компаний, занимающихся каким-либо online-бизнесом, например, торговлей через Internet.

Компьютерные вирусы, троянские кони

Вирусы — старая категория опасностей, которая в последнее время в чистом виде практически не встречается. В связи с активным применением сетевых технологий для передачи данных вирусы все более тесно интегрируются с троянскими компонентами и сетевыми червями. В настоящее время компьютерный вирус использует для своего распространения либо электронную почту, либо уязвимости в ПО. А часто и то, и другое. Теперь на первое место вместо деструктивных функций вышли функции удаленного управления, похищения информации и использования зараженной системы в качестве плацдарма для дальнейшего распространения. Все чаще зараженная машина становится активным участником DDoS-атак. Методов борьбы достаточно много, одним из них является все та же своевременная установка обновлений.

Анализаторы протоколов и «снифферы»

В эту группу входят средства перехвата передаваемых по сети данных. Такие средства могут быть как аппаратными, так и программными. Обычно данные передаются по сети в открытом виде, что позволяет злоумышленнику внутри локальной сети перехватить их. Некоторые протоколы работы с сетью (POPS, FTP) не используют шифрование паролей, что позволяет злоумышленнику перехватить их и использовать самому. При передаче данных по глобальным сетям эта проблема встает наиболее остро. По возможности следует ограничить доступ к сети неавторизированным пользователям и случайным людям.

Технические средства съема информации

Сюда можно отнести такие средства, как клавиатурные жучки, различные мини-камеры, звукозаписывающие устройства и т.д. Данная группа используется в повседневной жизни намного реже вышеперечисленных, так как, кроме наличия спецтехники, требует доступа к сети и ее составляющим.

Человеческий фактор:

Уволенные или недовольные сотрудники.

Промышленный шпионаж.

Халатность.

Низкая квалификация.

Уволенные и недовольные сотрудники

Данная группа людей наиболее опасна, так как многие из работающих сотрудников могут иметь разрешенный доступ к конфиденциальной информации. Особенную группу составляют системные администраторы, зачастую недовольные своим материальным положением или несогласные с увольнением, они оставляют «черные ходы» для

последующей возможности злонамеренного использования ресурсов, похищения конфиденциальной информации и т. д.

Промышленный шпионаж

Это самая сложная категория. Если ваши данные интересны кому-либо, то этот кто-то найдет способы достать их. Взлом хорошо защищенной сети — не самый простой вариант. Очень может статься, что уборщица «тетя Глаша», моющая под столом и ругающаяся на непонятный ящик с проводами, может оказаться хакером весьма высокого класса.

Халатность

Самая обширная категория злоупотреблений: начиная с не установленных вовремя обновлений, неизмененных настроек «по умолчанию» и заканчивая несанкционированными модемами для выхода в Internet, — в результате чего злоумышленники получают открытый доступ в хорошо защищенную сеть.

Низкая квалификация

Часто низкая квалификация не позволяет пользователю понять, с чем он имеет дело; из-за этого даже хорошие программы защиты становятся настоящей морокой системного администратора, и он вынужден надеяться только на защиту периметра. Большинство пользователей не понимают реальной угрозы от запуска исполняемых файлов и скриптов и считают, что исполняемые файлы -только файлы с расширением «exe». Низкая квалификация не позволяет также определить, какая информация является действительно конфиденциальной, а какую можно разглашать. В крупных компаниях часто можно позвонить пользователю и, представившись администратором, узнать у него учетные данные для входа в сеть. Выход только один -обучение пользователей, создание соответствующих документов и повышение квалификации.

Часть 2. Методы защиты

Согласно статистике потерь, которые несут организации от различных компьютерных преступлений, львиную долю занимают потери от преступлений, совершаемых собственными нечистоплотными сотрудниками. Однако в последнее время наблюдается явная тенденция к увеличению потерь от внешних злоумышленников. В любом случае необходимо обеспечить защиту как от нелояльного персонала, так и от способных проникнуть в вашу сеть хакеров. Только комплексный подход к защите информации может внушить уверенность в ее безопасности.

Однако в связи с ограниченным объемом данной статьи рассмотрим только основные из технических методов защиты сетей и циркулирующей по ним информации, а именно — криптографические алгоритмы и их применение в данной сфере.

Защита данных от внутренних угроз

Для защиты циркулирующей в локальной сети информации можно применить следующие криптографические методы:

шифрование информации;

электронную цифровую подпись (ЭЦП).

Шифрование

Шифрование информации помогает защитить ее конфиденциальность, т.е. обеспечивает невозможность несанкционированного ознакомления с ней. Шифрование — это процесс преобразования открытой информации в закрытую, зашифрованную (что называется «зашифрование») и наоборот («расшифрование»). Это преобразование выполняется по строгим математическим алгоритмам; помимо собственно данных в преобразовании также участвует дополнительный элемент — «ключ». В ГОСТ 28147-89 дается следующее определение ключа: «Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований». Иными словами, ключ представляет собой уникальный элемент,

позволяющий зашифровать информацию так, что получить открытую информацию из зашифрованной можно только определенному пользователю или группе пользователей.

Шифрование можно выразить следующими формулами:

C=Ek1 (M) — зашифрование,

M'=Dk2(C) — расшифрование.

Функция E выполняет зашифрование информации, функция D – расшифрование. В том случае, если ключ k2 соответствует ключу k1, примененному при зашифровании, удается получить открытую информацию, т.е. получить соответствие M' = M.

При отсутствии же правильного ключа k2 получить исходное сообщение практически невозможно.

По виду соответствия ключей k1 и k2 алгоритмы шифрования разделяются на две категории:

1) Симметричное шифрование: k1 = k2. Для зашифрования и расшифрования информации используется один и тот же ключ. Это означает, что пользователи, обменивающиеся зашифрованной информацией, должны иметь один и тот же ключ. Более безопасный вариант — существует уникальный ключ шифрования для каждой пары пользователей, который неизвестен остальным. Ключ симметричного шифрования должен храниться в секрете: его компрометация (утеря или хищение) повлечет за собой раскрытие всей зашифрованной данным ключом информации.

2) Асимметричное шифрование. Ключ k1- в данном случае называется «открытым», а ключ k2 — «секретным». Открытый ключ вычисляется из секретного различными способами (зависит от конкретного алгоритма шифрования). Обратное же вычисление k2 из k1 является практически невозможным. Смысл асимметричного шифрования состоит в том, что ключ k2 хранится в секрете у его владельца и не должен быть известен никому; ключ k1, наоборот, распространяется всем пользователям, желающим отправлять зашифрованные сообщения владельцу ключа k2; любой из них может зашифровать информацию на ключе k1, расшифровать же ее может только обладатель секретного ключа k2.

Оба ключа: ключ симметричного и секретный ключ асимметричного шифрования должны быть абсолютно случайными — в противном случае злоумышленник теоретически имеет возможность спрогнозировать значение определенного ключа. Поэтому для генерации ключей обычно используют датчики случайных чисел (ДСЧ), лучше всего — аппаратные.

Стоит сказать, что все государственные организации РФ и ряд коммерческих обязаны для защиты данных использовать отечественный алгоритм симметричного шифрования ГОСТ 28147-89. Это сильный криптографический алгоритм, в котором пока еще не найдено недостатков за более чем 12 лет применения.

ЭЦП

ЭЦП позволяет гарантировать целостность и авторство информации (схема 2). Как видно из схемы, ЭЦП также использует криптографические ключи: секретный и открытый. Открытый ключ вычисляется из секретного по достаточно легкой формуле, например: y=ax mod p (где x — секретный ключ, y — открытый ключ, a и p- параметры алгоритма ЭЦП), обратное же вычисление весьма трудоемко и считается неосуществимым за приемлемое время при современных вычислительных мощностях.

Схема 2. Схема применения ЭЦП

Схема распространения ключей ЭЦП аналогична схеме асимметричного шифрования: секретный ключ должен оставаться у его владельца, открытый же распространяется всем пользователям, желающим проверять ЭЦП владельца секретного ключа. Необходимо обеспечивать недоступность своего секретного ключа, ибо злоумышленник легко может подделать ЭЦП любого пользователя, получив доступ к его секретному ключу.

Электронной подписью можно подписать любую информацию. Предварительно информацию обрабатывают функцией хэширования, цель которой — выработка последовательности определенной длины, однозначно отражающей содержимое подписываемой информации. Данная последовательность называется «хэш», основное свойство хэша таково, что исключительно сложно модифицировать информацию так, чтобы ее хэш остался неизменным. Отечественный стандарт хэш-функций ГОСТ Р 34.11-94 предусматривает хэш размером 256 бит.

На основе хэша информации и секретного ключа пользователя вычисляется ЭЦП. Как правило, ЭЦП отправляется вместе с подписанной информацией (ЭЦП файла чаще всего просто помещают в конец файла перед его отправкой куда-либо по сети). Сама ЭЦП, как и хэш, является бинарной последовательностью фиксированного размера. Однако, помимо ЭЦП, к информации обычно добавляется также ряд служебных полей, прежде всего, идентификационная информация о пользователе, поставившем ЭЦП; причем, данные поля участвуют в расчете хэша. При проверке ЭЦП файла в интерактивном режиме результат может выглядеть так:

«Подпись файла „Document.doc“ верна: Иванов А.А. 25.02.2003».

Естественно, в случае неверной ЭЦП выводится соответствующая информация, содержащая причину признания ЭЦП неверной. При проверке ЭЦП также вычисляется хэш информации; если он не совпадает с полученным при вычислении ЭЦП (что может означать попытку модификации информации злоумышленником), ЭЦП будет неверна.

Наряду с ГОСТ 28147-89 существует отечественный алгоритм ЭЦП: ГОСТ Р 34.10-94 и его более новый вариант ГОСТ Р 34.10-2001. Государственные организации РФ и ряд коммерческих обязаны использовать один из этих алгоритмов ЭЦП в паре с алгоритмом хэширования ГОСТ Р 34.11 -94.

Существует и более простой способ обеспечения целостности информации — вычисление имитоприставки. Имитоприставка — это криптографическая контрольная сумма информации, вычисляемая с использованием ключа шифрования. Для вычисления имитоприставки используется, в частности, один из режимов работы алгоритма ГОСТ 28147-89, позволяющий получить в качестве имитоприставки 32-битную последовательность из информации любого размера. Аналогично хэшу информации имитоприставку чрезвычайно сложно подделать. Использование имитоприставок более удобно, чем применение ЭЦП: во-первых, 4 байта информации намного проще добавить, например, к пересылаемому по сети IP-пакету, чем большую структуру ЭЦП, во-вторых, вычисление имитоприставки существенно менее ресурсоемкая операция, чем формирование ЭЦП, поскольку в последнем случае используются такие сложные операции, как возведение 512-битного числа в степень, показателем которой является 256-битное число, что требует достаточно много вычислений. Имитоприставку нельзя использовать для контроля авторства сообщения, но этого во многих случаях и не требуется.

Комплексное применение криптографических алгоритмов

Для безопасной передачи по сети каких-либо файлов, их достаточно подписать и зашифровать. На схеме 3 представлена технология специализированного архивирования, обеспечивающая комплексную защиту файлов перед отправкой по сети.

Схема 3. Технология специализированного архивирования

Прежде всего, файлы подписываются секретным ключом отправителя, затем сжимаются для более быстрой передачи. Подписанные и сжатые файлы шифруются на случайном ключе сессии, который нужен только для зашифрования этой порции файлов - ключ берется с датчика случайных чисел, который обязан присутствовать в любом шифраторе. После этого к сформированному таким образом спецархиву добавляется заголовок, содержащий служебную информацию.

Заголовок позволяет расшифровать данные при получении. Для этого он содержит ключ сессии в зашифрованном виде. После зашифрования данных и записи их в архив, ключ сессии, в свою очередь, зашифровывается на ключе парной связи (DH-ключ), который вычисляется динамически из секретного ключа отправителя файлов и открытого ключа получателя по алгоритму Диффи-Хеллмана. Ключи парной связи различны для каждой пары «отправитель-получатель». Тот же самый ключ парной связи может быть вычислен только тем получателем, открытый ключ которого участвовал в вычислении ключа парной связи на стороне отправителя. Получатель для вычисления ключа парной связи использует свой секретный ключ и открытый ключ отправителя. Алгоритм Диффи-Хеллмана позволяет при этом получить тот же ключ, который сформировал отправитель из своего секретного ключа и открытого ключа получателя.

Таким образом, заголовок содержит копии ключа сессии (по количеству получателей), каждая их которых зашифрована на ключе парной связи отправителя для определенного получателя.

После получения архива получатель вычисляет ключ парной связи, затем расшифровывает ключ сессии, и наконец, расшифровывает собственно архив. После расшифрования информация автоматически разжимается. В последнюю очередь проверяется ЭЦП каждого файла.

Защита от внешних угроз

Методов защиты от внешних угроз придумано немало — найдено противодействие практически против всех опасностей, перечисленных в первой части данной статьи. Единственная проблема, которой пока не найдено адекватного решения, — DDoS-атаки. Рассмотрим технологию виртуальных частных сетей (VPN — Virtual Private Network), позволяющую с помощью криптографических методов как защитить информацию, передаваемую через Internet, так и пресечь несанкционированный доступ в локальную сеть снаружи.

Виртуальные частные сети

На наш взгляд, технология VPN является весьма эффективной защитой, ее повсеместное внедрение — только вопрос времени. Доказательством этого является хотя бы внедрение поддержки VPN в последние операционные системы фирмы Microsoft — начиная с Windows 2000.

Суть VPN состоит в следующем:

На все компьютеры, имеющие выход в Internet (вместо Internet может быть и любая другая сеть общего пользования), ставится средство, реализующее VPN. Такое средство обычно называют VPN-агентом. VPN-агенты обязательно должны быть установлены на все выходы в глобальную сеть.

VPN-агенты автоматически зашифровывают всю информацию, передаваемую через них в Internet, а также контролируют целостность информации с помощью имитоприставок.

Технология VPN

Как известно, передаваемая в Internet информация представляет собой множество пакетов протокола IP, на которые она разбивается перед отправкой и может многократно переразбиваться по дороге. VPN-агенты обрабатывают именно IP-пакеты, ниже описана технология их работы.

1. Перед отправкой IP-пакета VPN-агент выполняет следующее:

Анализируется IP-адрес получателя пакета. В зависимости от адреса и другой информации (см. ниже) выбираются алгоритмы защиты данного пакета (VPN-агенты могут, поддерживать одновременно несколько алгоритмов шифрования и контроля целостности) и криптографические ключи. Пакет может и вовсе быть отброшен, если в настройках VPN-агента такой получатель не значится.

Вычисляется и добавляется в пакет его имитоприставка.

Пакет шифруется (целиком, включая заголовок IP-пакета, содержащий служебную информацию). Формируется новый заголовок пакета, где вместо адреса получателя указывается адрес его VPN-агента. Это называется инкапсуляцией пакета. При использовании инкапсуляции обмен данными между двумя локальными сетями снаружи представляется как обмен между двумя компьютерами, на которых установлены VPN-агенты. Всякая полезная для внешней атаки информация, например, внутренние IP-адреса сети, в этом случае недоступна.

2. При получении IP-пакета выполняются обратные действия:

Из заголовка пакета получается информация о VPN-агенте отправителя пакета. Если такой отправитель не входит в число разрешенных в настройках, то пакет отбрасывается. То же самое происходит при приеме пакета с намеренно или случайно поврежденным заголовком.

Согласно настройкам выбираются криптографические алгоритмы и ключи.

Пакет расшифровывается, затем проверяется его целостность. Пакеты с нарушенной целостностью также отбрасываются.

В завершение обработки пакет в его исходном виде отправляется настоящему адресату по локальной сети.

Все перечисленные операции выполняются автоматически, работа VPN-агентов является незаметной для пользователей. Сложной является только настройка VPN-агентов, которая может быть выполнена только очень опытным пользователем. VPN-агент может находиться непосредственно на защищаемом компьютере (что особенно полезно для мобильных пользователей). В этом случае он защищает обмен данными только одного компьютера — на котором установлен.

VPN-агенты создают виртуальные каналы между защищаемыми локальными сетями или компьютерами (к таким каналам обычно применяется термин «туннель», а технология их создания называется «туннелировани-ем»). Вся информация идет по туннелю только в зашифрованном виде. Кстати, пользователи VPN при обращении к компьютерам из удаленных локальных сетей могут и не знать, что эти компьютеры реально находятся, может быть, в другом городе, — разница между удаленными и локальными компьютерами в данном случае состоит только в скорости передачи данных.

Как видно из описания действий VPN-агентов, часть IP-пакетов ими отбрасывается. Действительно, VPN-агенты фильтруют пакеты согласно своим настройкам (совокупность настроек VPN-агента называется «Политикой безопасности»). То есть VPN-агент выполняет два основных действия: создание туннелей и фильтрация пакетов

IP-пакет отбрасывается или направляется в конкретный туннель в зависимости от значений следующих его характеристик:

IP-адрес источника (для исходящего пакета — адрес конкретного компьютера защищаемой сети).

IP-адрес назначения.

Протокол более верхнего уровня, которому принадлежит данный пакет (например, TCP или UDP для транспортного уровня).

Номер порта, с которого или на который отправлен пакет (например, 1080).

4. Содержание отчёта:

- постановка задачи;
- электронная версия выполненного задания;
- ответы на вопросы;

5. Контрольные вопросы

- Как поменять учетную запись администратора (Пользователь Администратор с пустым паролем - это уязвимость)
- Как сделать окно приветствия пустым
- Выявление сетевых уязвимостей сканированием портов ПК

- Перечислите основные положения офисной политики безопасности

6. Список рекомендуемой литературы:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб. Питер, 2015.
2. Шурыгин В.Н., Ковалев И.В. Информационные сети. Методические указания по выполнению лабораторных работ. МГУП 2014
3. Основы построения телекоммуникационных систем и сетей: Учебник для вузов / В.В. Крухмалев, В.Н. Гордиенко, А.Д. Моченов и др.; Под ред. В.Н. Гордиенко и В.В. Крухмалева. – 2-е изд., испр. – М.: Горячая линия – Телеком, 2016. - 424 с.

Раздел 5. Построение локальной сети на ОС Windows 7 Ultimate (Максимальная). Тема 5.1. Домашняя группа. Практическая работа № 10. Программа для изучения компьютерных сетей S2 Netest. Объём учебного времени – 3 ч.

1. Цель занятия:

- научиться исправлению дефектов на изображениях людей.

2. Перечень необходимых средств обучения (оборудование, материалы):

– технические средства обучения: персональные компьютеры, локальная сеть, Internet

Используемое программное обеспечение:

Операционная система Microsoft Windows XP/7

3. Содержание заданий

Подробно описано здесь: http://www.intuit.ru/department/network/baslocnet/15/

Ход выполнения:

Включить компьютер.

Осуществить идентификацию пользователя в системе.

Подготовительный этап.

Запуск программы. Для этого необходимо запустить программу через Пуск – Программы - S2 Netest.

В результате на экране появится диалоговое окно программы, которое содержит строки выбора режима работы в программе:

Стандартный тест

Тест из файла.

Режим тренировки

Первый режим предоставляет возможность выйти в режим тестовой работы со стандартным набором тестовых заданий.

Второй режим позволяет выбрать тесты, из какой-либо директории или на носителе информации.

В диалоговом окне присутствуют две кнопки – ПРАВИЛА и СТАРТ.

Кнопка ПРАВИЛА дает возможность прочитать инструкцию по использованию программы (смотрите и читайте ниже). Кнопка СТАРТ – запускает режим тестирования.

Управление.

На моделирующей площадке могут находиться компьютеры, принтеры и сетевое оборудование (Рис.4). Ваша задача, перетаскивая мышью элементы сети, находящиеся справа от площадки, объединить все компьютеры в одну локальную сеть.

В начале нужно установить в каждый компьютер сетевую карту. Перетащите мышью сетевую карту на компьютер, и она появится слева от компьютера на площадке.

Затем возьмите необходимое количество хабов (учитывая количество портов на каждом хабе и количество соединений).

Если прокладка кабеля затруднена, т.е. имеются препятствия в виде серых клеток (стен), то необходимо воспользоваться беспроводным решением.

Чтобы объединить два компьютера между собой в сеть дополнительных устройств, кроме сетевых карт, не требуется. Достаточно соединить компьютеры так называемым перекрестным (реверсным) кабелем (его еще называют «перевернутая витая пара»). В программе такой кабель имеет фиолетовый цвет.

Если же компьютеров три и более, то необходимо использовать хаб. В этом случае используется прямой кабель. В программе такой кабель имеет серый цвет.

Хаб имеет ограниченное количество портов для подключения компьютеров, поэтому реализована возможность создания сети с использованием нескольких хабов.

Между собой хабы соединяются либо перевернутым кабелем через обычный порт, либо прямым кабелем через порт Up-Link (в программе применяется именно такой принцип).

С экономической точки зрения использование одного 8-портового хаба несколько дешевле, но не во всех случаях это важно.

Описание сетевых компонентов

Там, где располагаются элементы сети (сетевое оборудование и кабели двух видов), с помощью которых необходимо смонтировать локальную сеть, есть кнопки ПРАЙС.

При нажатии кнопки появляется информационный экран соответствующего сетевого компонента, который предоставляет информацию о нем:

- Наименование;
- Стоимость
- Интерфейс;
- Скорость;
- Функциональные возможности;
- Физические характеристики

Для проверки выполнения задания теста в самом низу справа расположена кнопка ПРОВЕРКА, нажатием на которую и можно проверить правильность смонтированной сети и, в случае успешного выполнения задания, перейти к следующему заданию теста.

Информация предоставляемая для пользователя в окне РУЗУЛЬТАТЫ:

- Ваши результаты, где показано количество объединенных компьютеров из имеющихся в наличии;
- Наличие ошибок прокладывания кабеля. Пока есть ошибки, их необходимо исправить, вернувшись обратно на моделируемую площадку, нажав кнопку ЗАКРЫТЬ.
- Время выполнения задания в минутах;
- Перемещений элементов сети;

- Длина используемого кабеля;
- И стоимость сети.

Если объединены все компьютеры и это выполнено без ошибок, то вы можете приступить к выполнению следующего теста, для чего необходимо нажать кнопку ДАЛЕЕ.

Структура отчета по практической работе.

В процессе выполнения работы Вам необходимо будет вести протокол выполнения заданий. Для этого необходимо будет воспользоваться программой MS WORD, в которую необходимо будет записать информацию:

В начале

Фамилия, Имя. Группа. Дата выполнения.

Далее записывается номер заданий и методом копирования активного окна, копируется окно Результат и вставляется в текстовой документ-отчет за номером соответствующего задания.

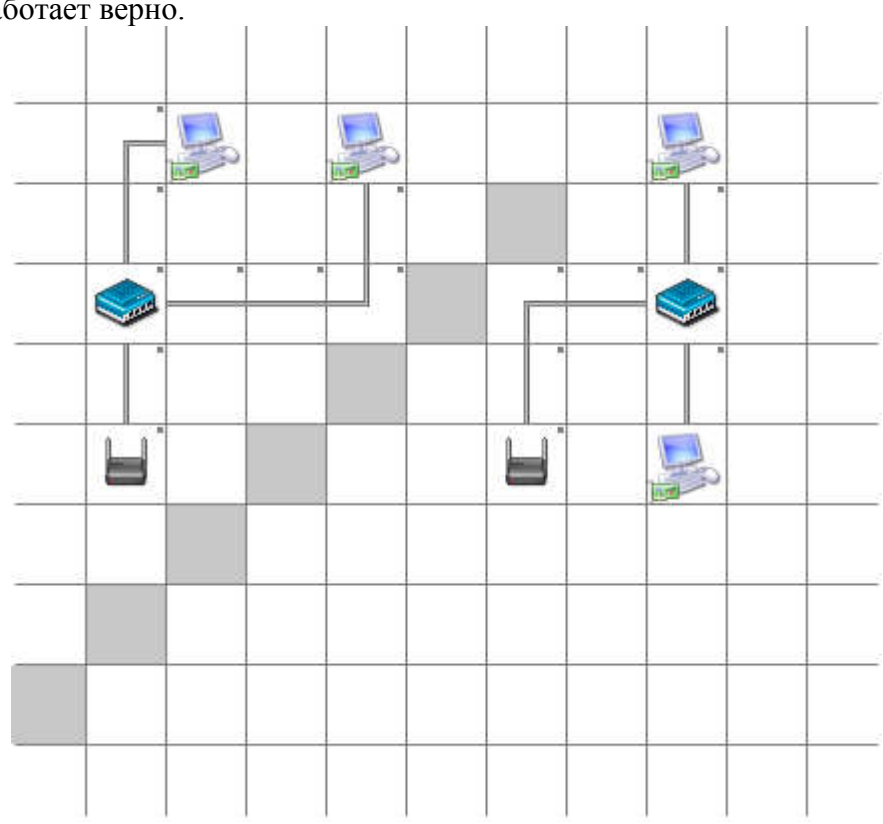
4. Содержание отчёта:

- постановка задачи;
- электронная версия выполненного задания;
- ответы на вопросы;

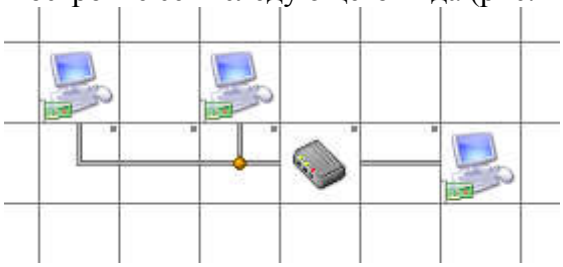
5. Контрольные вопросы

Посмотрите на рис. ниже и назовите эти устройства и их характеристики.

Постройте следующую схему (рис. ниже) и кнопкой Проверка убедитесь в том, что она работает верно.



Постройте сеть следующего вида (рис. ниже). Проверьте ее работоспособность.



Теперь хаб замените на свитч. Сеть также будет работать. Но какое из этих двух решений будет более оптимальным и почему?

6. Список рекомендуемой литературы:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб. Питер, 2015.
2. Шурыгин В.Н., Ковалев И.В. Информационные сети. Методические указания по выполнению лабораторных работ. МГУП 2014
3. Основы построения телекоммуникационных систем и сетей: Учебник для вузов / В.В. Крухмалев, В.Н. Гордиенко, А.Д. Моченов и др.; Под ред. В.Н. Гордиенко и В.В. Крухмалева. – 2-е изд., испр. – М.: Горячая линия – Телеком, 2016. - 424 с.

Информационное обеспечение обучения

Основные источники:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб. Питер, 2015.
2. Основы построения телекоммуникационных систем и сетей: Учебник для вузов / В.В. Крухмалев, В.Н. Гордиенко, А.Д. Моченов и др.; Под ред. В.Н. Гордиенко и В.В. Крухмалева. – 2-е изд., испр. – М.: Горячая линия – Телеком, 2014. - 424 с.
3. Семакин И.Г. Информатика и ИКТ. Базовый уровень: учебник для 10-11 классов /. 4-е изд., – М.: БИНОМ. Лаборатория знаний, 2014. — 234с.

Дополнительные источники:

4. Цифровые и аналоговые системы передачи: Учебник для вузов/ В.И. Иванов, В.Н. Гордиенко, Г.Н. Попов и др.; Под ред. В.Иванова. – 2-у изд.- М.: Горячая линия – Телеком, 2013. – 232 с.

5. Телекоммуникационные системы и сети: Учебное пособие для вузов / Крук Б.И., Попантонопуло В.К., Шувалов В.П., т.1.- М.: Горячая линия-Телеком, 2013.- 648с.
6. Телекоммуникационные системы и сети: Учебное пособие для вузов / Катунин Г.П., Мамчев Г.В., Попантонопуло В.К., Шувалов В.П., т.2. - М.: Горячая линия-Телеком, 2014.- 672с.
7. Телекоммуникационные системы и сети: Учебное пособие для вузов / Величко В.В., Субботин Е.А., Шувалов В.П., Ярославцев А.Ф. т.2. - М.: Горячая линия-Телеком, 2015. - 592с.
8. Основы построения систем и сетей передачи информации: Учебное пособие для вузов/ В.В. Ломовицкий, А.И. Михайлов, К.В. Шестак, В.М. Щекотихин; Под ред. В.М.Щекотихина - М.: Горячая линия – Телеком, 2014. – 382 с.
9. Кульгин М. Технологии корпоративных сетей. Энциклопедия. – СПб. Питер, 2013.
10. Майкрософт. Учебные проекты с использованием Microsoft Office. – М., 2017.
11. Уваров В.М., Силакова Л.А., Красникова Н.Е. Практикум по основам информатики и вычислительной техники: учеб. пособие. – М., 2015.
12. Угринович Н., Босова Л., Михайлова Н. Практикум по информатике и информационным технологиям, Бином. Лаборатория знаний, 2015.
13. Фуфаева Э.В., Фуфаева Л.И. Пакеты прикладных программ, 2014. Семакин И.Г., Хеннер Е.К. Информатика. Учебник 10-11 кл. – М., 2016.
14. Гагарина Л.Г. Технические средства информатизации: уч. пос. для студ. СПО. - М.: Форум, 2013. -254 с.
15. Гохберг Г.С. Информационные технологии: учебник для студ. СПО. – М.: Академия, 2016. -207 с.
16. Максимов Н.В. Архитектура ЭВМ и вычислительных систем: учеб. Для студ. СПО. - М.: Форум: Инфра-М, 2013. – 511с.
17. Максимов Н.В., Партыка Т.Л., Попов И.И. Информационные технологии в профессиональной деятельности – М.: ФОРУМ, 2013. - 496с.
18. Михеева Е.В., Информационные технологии в профессиональной деятельности. – М.: Издательский центр «Академия», 2013. — 211с.
19. Михеев Е.В. Информатика: учебн. для студ. СПО. – М.: Академия, 2017. -346 с.
20. Рудаков А.В. Технология разработки программных продуктов: уч. пос. для студ. СПО. – М.: Академия, 2013. -207 с.
21. Михеев Е.В. Информационные технологии в проф. деятельности: уч. пос. для студ. СПО. – М.: ИЦ «Академия», 2017. – 384 с
22. Шурыгин В.Н., Ковалев И.В. Информационные сети. Методические указания по выполнению лабораторных работ. МГУП 2013
23. Угринович Н.Д. Информатика и ИКТ. Базовый уровень: учебник для 10 класса/. – 4-е изд. – М.: БИНОМ, Лаборатория знаний, 2013. — 260с.

Интернет-ресурсы:
www.moodle.org
www.cor.home-edu.ru
http://school-collection.edu.ru
www.intschool.ru

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер изменения	Обозначение документа	Номер листа				Всего листов в документе	Подпись ответственного за внесение изменения	Дата внесения изменения	Дата введения изменения
		Измененного	Замененного	Нового	Изъятого				