**Филиал федерального государственного бюджетного образовательного учреждение высшего образования «Университет «Дубна» -**

**Лыткаринский промышленно-гуманитарный колледж**

УТВЕРЖДАЮ

Зам. директора филиала

по учебно-методической работе

\_\_\_\_\_\_\_\_\_\_\_\_ Аникеева О.Б.

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2024г

**Фонд оценочных средств**

по учебной дисциплине

**ОПЦ.17 ОТРАБОТКА ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ**

Специальности

**09.02.06 Сетевое и системное администрирование**

Квалификация выпускника - **системный администратор**

Форма обучения - очная

Лыткарино, 2024

Составители (разработчики) фонда оценочных средств:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / ***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

*подпись*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / ***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

*подпись*

Фонд оценочных средств рассмотрен на заседании цикловой методической (предметной) комиссии технологических дисциплин.

Протокол заседания № \_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_ 2024г.

Председатель цикловой методической (предметной) комиссии Силяева Н.П. \_\_\_\_\_\_\_\_\_\_\_\_

*подпись*

Представитель работодателя

М.А. Непомнящий,

директор по программному обеспечению,

ООО Фирма «Рассвет Гагаринское Отделение» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(подпись) М.П.*

«\_\_\_» \_\_\_\_\_\_\_\_ 2024г.

1. **ПАСПОРТ КОМПЛЕКТА ОЦЕНОЧНЫХ СРЕДСТВ**

Фонд оценочных средств (ФОС) разработан с целью установления соответствия образовательных достижений обучающихся требованиям программы подготовки специалистов среднего звена по учебной дисциплине **ОПЦ.17 «Отработка профессиональных компетенций»** основной профессиональной образовательной программы по специальности СПО **09.02.06 Сетевое и системное администрирование.**

|  |  |  |
| --- | --- | --- |
| ***Результаты обучения*** | ***Критерии оценки*** | ***Формы и методы оценки*** |
| *Перечень знаний, осваиваемых в рамках дисциплины:* | «Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко.  «Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками.  «Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки.  «Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки. | Оценка в рамках текущего контроля результатов выполнения индивидуальных контрольных заданий, результатов выполнения практических работ, устный индивидуальный опрос.  Письменный опрос в форме тестирования |
| - настраивать сетевую адресацию  - настраивать статическую  и динамическую маршрутизацию сетей  - устанавливать и настраивать сетевые протоколы и сетевое оборудование в соответствии с конкретной задачей  - фильтровать, контролировать и обеспечивать безопасность сетевого трафика  - оценивать качество и соответствие требованиям проекта сети  - оформлять техническую документацию  - планировать и внедрять инфраструктуру развертывания серверов  - планировать и внедрять файловые хранилища и системы хранения данных  - проектировать и внедрять  инфраструктуру лесов и доменов  - осуществлять сбор данных для анализа использования и функционирования программно- технических средств  компьютерных сетей  - сопровождать и контролировать использование почтового сервера, SQL-сервера  - устанавливать Web-сервер  - осуществлять удаленное администрирование и восстановление работоспособности сетевой инфраструктуры  - внедрять механизмы сетевой безопасности с помощью межсетевых экранов  -организовывать бесперебойную работу системы по резервному копированию и восстановлению Информации  - проводить мониторинг работы оборудования после ремонта |
| *Перечень умений, осваиваемых в рамках дисциплины:* |  |
| - рассчитывать основные параметры локальной сети  - настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети  - применять программно- аппаратные средства для обеспечения целостности  резервирования данных  - регистрировать подключение к домену, вести отчетную документацию  -описывать концепции сетевой безопасности  - устанавливать, тестировать и эксплуатировать информационные системы, согласно технической  документации, обеспечивать антивирусную защиту  -выполнять замену устаревшего оборудования  и замену расходных материалов | Экспертное наблюдение и оценивание выполнения практических работ.  Текущий контроль в форме защиты практических работ |

|  |  |
| --- | --- |
| **Результаты освоения программы** | **Критерии оценок (шкала оценок)** |
| ВД.1 Настройка сетевой инфраструктуры | Выполнение проектирования кабельной структуры компьютерной сети |
| Осуществление выбора технологии, инструментальных средств и средств вычислительной техники при организации процесса разработки и исследования объектов профессиональной деятельности |
| Обеспечение защиты информации в сети с использованием программно-аппаратных средств |
| Перенимание участия в приемо-сдаточных испытаниях компьютерных сетей и сетевого оборудования различного уровня и в оценке качества и экономической эффективности сетевой топологии |
| Выполнение требований нормативно-технической документации, иметь опыт оформления проектной документации |
| ВД.2 Организация сетевого администрирования | Администрирование локальных вычислительных сетей и принятие мер по устранению возможных сбоев |
| Администрирование сетевых ресурсов в информационных системах |
| Обеспечение сбора данных для анализа использования и функционирования программно- технических средств компьютерных сетей |
| Взаимодействие со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности |
| ВД.3 Эксплуатация объектов сетевой инфраструктуры | Установка, настройка, эксплуатация и обслуживание технических и программно-аппаратных средств компьютерных сетей |
| Проведение профилактических работ на объектах сетевой инфраструктуры и рабочих станциях |
| Установка, настройка, эксплуатация и обслуживание сетевых конфигураций |
| Участие в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнение восстановления и резервного копирования информации |
| Организация инвентаризации технических средств сетевой инфраструктуры, осуществление контроля оборудования после его ремонта |
| Выполнение замены расходных материалов и мелкий ремонт периферийного оборудования, определение устаревшего оборудования и программных средств сетевой инфраструктуры |

**II. Комплект материалов для текущего контроля успеваемости**

# Практическая работа 1

**Тема:** Выполнение проектирования кабельной структуры компьютерной сети

# Цели:

1. Получение практического навыка проектирования кабельной структуры с учетом планировки помещения, количества необходимых рабочих мест и имеющегося оборудования.
2. Изучение методики проектирования локальной сети в пределах горизонтальной структурированной кабельной системы.
3. Формирование профессиональной компетенции ПК.3.2 Проводить системотехническое обслуживание компьютерных систем и комплексов и общих компетенций: ОК.1 Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес; ОК.2 Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество; ОК.3 Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность; ОК.4 Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития; ОК.5 Использовать информационно-коммуникационные технологии в профессиональной деятельности.

**Оборудование:** персональный компьютер, подключенный к сети интернет и с установленной программой Discord, любой графический редактор (Компас, Adobe Photoshop, Gimp и т.п.)

# Теоретический материал:

* 1. **Подготовка к проектированию ЛВС**

Проектирование ЛВС СКС (структурированной кабельной системы) представляет собой разработку документации, в которой описывается структура сети, ее топология, расположение конечных пользовательских устройств, компьютерных розеток и характеристики оборудования для построения ЛВС.

До начала проектирования в организации собирают и анализируют такую информацию:

* сколько единиц техники будет объединять ЛВС. Учитываются ПК, печатные устройства, АТС и другое оборудование. Это позволит рассчитать в проекте

нагрузку, которую будет испытывать локальная вычислительная сеть в штатном режиме работы;

* физические характеристики помещений, по которым будет проложена ЛВС. Учитывают площадь комнат, высоту потолков, максимальное расстояние между устройствами. От последнего параметра обратно пропорционально зависит скорость передачи данных в ЛВС;
* расположение компонентов, которые чаще других нуждаются в сервисном обслуживании. Чем проще получить к ним доступ, тем меньше времени сеть будет недоступна и рабочий процесс не нарушится. Инженеры смогут быстро выполнить основные этапы ремонта или профилактики.

Основные принципы проектирования ЛВС — обеспечение высокой скорости и безопасности передачи данных. В зависимости от критичности этих требований инженеры-проектировщики выбирают подходящее оборудование и ОС для сервера и пользовательских устройств.

# Этапы проектирования ЛВС

* **Составление ТЗ на проектирование ЛВС.** Содержит общие требования к вычислительной сети, количество автоматизированных рабочих мест, максимальную длину кабеля от порта на конечном устройстве до коммутационной панели. В техзадании указывают технологию, по которой рабочие компьютеры подключаются к ЛВС, требования к их размещению, характеристики сервера и способ его подключения, топологию сети, перечисляют средства защиты от несанкционированного доступа к ресурсам ЛВС. Прилагают планы помещений, перечень ИБП с указанием их мощности, описывают принципы прокладки кабельных трасс.
* **Согласование технического задания между подрядчиком (исполнителем) и заказчиком проекта**. После согласования исполнители приступают к составлению проектной документации и реализации проекта. Вносить кардинальные изменения в уже готовый проект (или имеющуюся ЛВС) приводит к дополнительным затратам или ограничениям. **Разработка проекта ЛВС**. При создании вычислительной локальной сети составляют детальные планы помещений. На них указывают расположение

розеток и количество портов в них, обозначают коммутационный центр, отмечают линии прокладки кабелей (в коробках и под фальшполом). К проекту прилагают расчет количества материалов и схему взаимодействия с другими видами связи в организации — например, мини-АТС.

# Программы для проектирования ЛВС

Разработка проекта будущей ЛВС — сложная задача, которая требует профессиональных знаний и опыта. Но упростить эту задачу можно, в этом помогут программы для проектирования ЛВС.

* **AutoCAD** — популярная система автоматизированного проектирования. Универсальная (подходит для многих сфер), но не адаптированная под проектирование ЛВС, поэтому для этой задачи у нее избыточный функционал и завышенная стоимость лицензии.
* **CAD5D** — онлайн-сервис для проектирования. Поддерживает поэтажные планы, размещение абонентских устройств и ключевых узлов, создание пакета проектной документации, учитывает спецификации материалов и оборудования.
* **ZWCAD** претендует на звание бюджетного аналога AutoCAD и предлагает широкий выбор инструментов для работы в двумерном и трехмерном пространстве. Позволяет организовывать элементы ЛВС в виде блоков, поддерживает параллельную работу с графикой и текстом. Для расширения базовой функциональности используются дополнительные модули.

# Порядок выполнения работы:

* 1. Повторить теоретический материал по теме: «Проектирование ЛВС»;
  2. Изучить планировку помещения (приложение А) в соответствии со своим вариантом;
  3. Спланировать размещение рабочих мест в соответствии со следующими требованиями:
     1. Необходимо разместить 59 работников фирмы, которая занимается разработкой программного обеспечения:
        + директор фирмы – 1чел;
        + секретарь директора – 1 чел;
        + гл. бухгалтер – 1 чел;
        + расчетчики и бухгалтера – 5 чел;
        + администратор локальной сети – 1чел;
        + программисты- 20 чел;
        + операторы ПК – 15 чел;
        + группа по техническому обслуживанию и ремонту офисной техники – 5 чел;
        + группа поддержки и сопровождения программного обеспечения – 10 чел.
     2. Планировку необходимо осуществить с учетом санитарных норм. В соответствии с **СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы»**, расстояние между двумя боковыми стенками компьютеров должно быть не менее 1,2 м., если компьютеры располагаются друг за другом, то расстояние между двумя компьютерами должно быть не менее 2м. Кроме того, на один компьютер должно быть выделено определенная площадь помещения:
* если компьютер снабжен монитором на базе электронно-лучевой трубки, площадь должна быть не менее 6 кв. м;
* если компьютер снабжен жидкокристаллическим или плазменным монитором, площадь может составлять 4,5 кв. м.
  + 1. Необходимо учитывать имеющийся ассортимент оборудования (например, при выборе коммутатора, необходимо учитывать количество портов).
  1. На чертеже изобразить разводку локальной сети (расположение рабочих станций, расположение сервера, концентраторов, протяжку кабеля (если он используется)).

Оборудование на чертеже должно быть показано условно:

* компьютер
  + коммутатор/концентратор
  + сервер

- провод

**Отчет должен содержать:** тему, цели, перечень оборудования, чертеж расположения рабочих мест, описание использованного при проектировании сети оборудования (количество серверов, количество коммутаторов/концентраторов, вид и количество провода, либо описание оборудования для организации беспроводной сети).

# Контрольные вопросы:

1. Как определить количество компьютеров, которое можно разместить в помещении?
2. Какой тип кабеля предпочтительнее использовать в горизонтальных подсистемах?
3. Какую топологию сети вы выбрали при проектировании и почему?

# Критерии оценки:

**Оценка «отлично»** выставляется, если задание выполнено полностью, правильно. Возможна одна неточность или описка, не являющаяся следствием незнания или непонимания учебного материала. Работа выполнена самостоятельно. Работа сдана с соблюдением сроков. Соблюдены все правила оформления отчета.

**Оценка «хорошо»** выставляется, если задание выполнено правильно, но недостаточно обоснования, рассуждения, допущены одна ошибка или два – три недочета. Работа сдана в срок (либо с опозданием на одно занятие). Есть некоторые недочеты в оформлении отчета.

**Оценка «удовлетворительно»** выставляется, если в заданиях допущены более одной ошибки или более трех недочетов, но обучающийся владеет обязательными умениями по проверяемой теме. Обучающийся многократно обращается за помощью преподавателя. Работа сдана с опозданием более одного занятия. В оформлении отчета есть отклонения и не во всем соответствует предъявляемым требованиям.

**Оценка «неудовлетворительно»** - выставляется, если выполнено меньше половины задания, допущены существенные ошибки, показавшие, что обучающийся не владеет обязательными умениями по данной теме в полном объеме. Обучающийся выполняет работу с помощью преподавателя. Работа сдана с нарушением всех сроков. Много нарушений правил оформления.

# Библиография

1. СТЕК: новости в мире ИТ: [сайт]. – Москва, 2018 – Обновляется в течение суток. – URL: https://[www.stekspb.ru/blog/it/proektirovanie-lvs](http://www.stekspb.ru/blog/it/proektirovanie-lvs) - Текст: электронный.
2. **Олифер В.** Проектирование компьютерной сети / В. Олифер, Н. Олифер. – Текст: электронный // Компьютерные сети. Принципы, технологии, протоколы: учебное пособие/ ООО «Издательство Питер». – Санккт-Петербург: Питер, 2020. - ISBN 978-5-4461-1426-9 – URL: https://studylib.net/doc/25373612/v.-olifer--n.-olifer--- komp.\_yuternye-seti.-principy--tehno...

**Практическая работа №2**

Тема: Осуществление выбора технологии, инструментальных средств и средств вычислительной техники при организации процесса разработки и исследования объектов профессиональной деятельности

Цель: Изучение состава аппаратного обеспечения компьютерных сетей. Изучение [программного обеспечения](http://www.pandia.ru/text/category/programmnoe_obespechenie/) компьютерных сетей. Приобретение умения предоставлять общий доступ к принтеру локальной сети.

Программное обеспечение:

Операционная система, текстовый редактор, браузер

Список литературы: Архитектура ЭВМ и вычислительных систем: Учебник. – М.: ФОРУМ: ИНФРА-М, 2019.

Задание к работе:

       Изучить теоретический материал. Письменно ответить на контрольные вопросы.

Теоретический материал:

При физическом соединении двух или более компьютеров образуется компьютерная сеть. Компьютерная сеть представляет собой комплекс технических, коммуникационных и программных средств, обеспечивающих эффективное распределение вычислительных ресурсов.

Уже сейчас есть сферы человеческой деятельности, которые принципиально не могут существовать без сетей (например, работа банков, крупных библиотек и т. д.) Сети используются при управлении крупными автоматизированными производствами, газопроводами, электростанциями и т. п.

В общем случае, для создания компьютерных сетей необходимо специальное аппаратное обеспечение - сетевое оборудование и специальное программное обеспечение - сетевые программные средства. Назначение всех видов компьютерных сетей определяется двумя функциями:

- обеспечение совместного использования аппаратных и программных ресурсов сети;

- обеспечение совместного доступа к ресурсам данных.

Например, все участники локальной сети могут совместно использовать одно общее устройство печати - сетевой принтер или, например, ресурсы жестких дисков одного выделенного компьютера - файлового сервера. Аналогично можно совместно использовать и программное обеспечение. Если в сети имеется специальный компьютер, выделенный для совместного использования участниками сети, он называется файловым сервером. Основными компонентами сети являются рабочие станции, серверы, передающие среды (кабели) и сетевое оборудование.

Рабочими станциями называются компьютеры сети, на которых пользователями сети реализуются прикладные задачи.

Серверы сети - это аппаратно-программные системы, выполняющие функции управления распределением сетевых ресурсов общего доступа. Сервером может быть это любой подключенный к сети компьютер, на котором находятся ресурсы, используемые другими устройствами локальной сети. В качестве аппаратной части сервера используется достаточно мощные компьютеры.

Аппаратура локальной сети обычно состоит из кабеля, разъемов, Т-коннекторов (рис. 1), терминаторов и сетевых адаптеров. Кабель, очевидно, используется для передачи данных между рабочими станциями. Для подключения кабеля используются разъемы. Эти разъемы через Т-коннекторы подключаются к сетевым адаптерам - специальным платам, вставленным в слоты расширения материнской платы рабочей станции. Терминаторы подключаются к открытым концам сети.

|  |  |
| --- | --- |
| https://pandia.ru/text/81/534/images/img1_142.png  Рис. 1. Т-коннектор | https://pandia.ru/text/81/534/images/img2_87.png  Рис. 2. T-коннектор, присоединенный к сетевой карте |

Для Ethernet (Ethernet  — пакетная технология передачи данных преимущественно локальных компьютерных сетей) могут быть использованы кабели разных типов: тонкий коаксиальный кабель, толстый коаксиальный кабель и неэкранированная витая пара. Для каждого типа кабеля используются свои разъемы и свой способ подключения к сетевому адаптеру.

Сети можно создавать с любым из типов кабеля.

|  |  |
| --- | --- |
| 1. Витая пара (TP - Twisted Pair)– это кабель, выполненный в виде скрученной пары проводов (рис. 3). Он может быть экранированным и неэкранированным. Экранированный кабель более устойчив к электромагнитным помехам. Витая пара наилучшим образом подходит для малых учреждений. Недостатками данного кабеля является высокий коэффициент затухания сигнала и высокая чувствительность к электромагнитным помехам, поэтому максимальное расстояние между активными устройствами в ЛВС при использовании витой пары должно быть не более 100 метров.  2. Коаксиальный кабель (рис. 4) состоит из одного цельного или витого центрального проводника, который окружен слоем диэлектрика. Проводящий слой [алюминиевой](http://www.pandia.ru/text/category/alyuminij/) фольги, металлической оплетки или их комбинации окружает диэлектрик и служит одновременно как экран против наводок. Общий изолирующий слой образует внешнюю оболочку кабеля.  Коаксиальный кабель может использоваться в двух различных системах передачи данных: без модуляции сигнала и с модуляцией. В первом случае цифровой сигнал используется в таком виде, в каком он поступает из ПК и сразу же передается по кабелю на приемную станцию. Он имеет один канал передачи со скоростью до 10 Мбит/сек и максимальный радиус действия 4000 м. Во втором случае цифровой сигнал превращают в аналоговый и направляют его на приемную станцию, где он снова превращается в цифровой. Операция превращения сигнала выполняется модемом; каждая станция должна иметь свой модем. Этот способ передачи является многоканальным (обеспечивает передачу по десяткам каналов, используя для этого всего лишь один кабель). Таким способом можно передавать звуки, видео сигналы и другие данные. Длина кабеля может достигать до 50 км.  3. Оптоволоконный кабель (рис. 5) является более новой технологией, используемой в сетях. Носителем информации является световой луч, который модулируется сетью и принимает форму сигнала. | https://pandia.ru/text/81/534/images/img3_74.png  Рис. 3 Кабель на основе витой пары |
| https://pandia.ru/text/81/534/images/img4_68.png  Рис. 4. Устройство коаксиального кабеля  1 — внутренний проводник (медная проволока),  2 — изоляция (сплошной полиэтилен),  3 — внешний проводник (оплётка из меди),  4 — оболочка (светостабилизированный полиэтилен). |  |
| https://pandia.ru/text/81/534/images/img5_67.png  Рис. 5. Оптоволоконный кабель | Такая система устойчива к внешним электрическим помехам и таким образом возможна очень быстрая, секретная и безошибочная передача данных со скоростью до 2 Гбит/с. Количество каналов в таких кабелях огромно. Передача данных выполняется только в симплексном режиме, поэтому для организации обмена данными устройства необходимо соединять двумя оптическими волокнами (на практике оптоволоконный кабель всегда имеет четное, парное кол-во волокон). К недостаткам оптоволоконного кабеля можно отнести большую стоимость, а также сложность подсоединения. |

4. Радиоволны в микроволновом диапазоне используются в качестве передающей среды в беспроводных локальных сетях, либо между мостами или шлюзами для связи между локальными сетями. В первом случае максимальное расстояние между станциями составляет 200 - 300 м, во втором - это расстояние прямой видимости. Скорость передачи данных - до 2 Мбит/с.

Выделяют следующие виды сетевого оборудования.

1. Сетевые карты – это контроллеры, подключаемые в слоты расширения материнской платы компьютера, предназначенные для передачи сигналов в сеть и приема сигналов из сети (рис. 6).

2. Терминаторы - это резисторы номиналом 50 Ом, которые производят затухание сигнала на концах сегмента сети.

3. Концентраторы (Hub) – это центральные устройства кабельной системы или сети физической топологии "звезда", которые при получении пакета на один из своих портов пересылает его на все остальные (рис. 7). В результате получается сеть с логической структурой общей шины. Различают концентраторы активные и пассивные. Активные концентраторы усиливают полученные сигналы и передают их. Пассивные концентраторы пропускают через себя сигнал, не усиливая и не восстанавливая его.

|  |  |
| --- | --- |
| https://pandia.ru/text/81/534/images/img6_56.png  Рис. 6. Сетевая карта в виде платы расширения, устанавливаемой в PCI-слот | https://pandia.ru/text/81/534/images/img7_46.png  Рис. 7. Концентратор с фиксированным количеством портов |

4. Повторители (Repeater)- устройства сети, усиливает и заново формирует форму входящего аналогового сигнала сети на расстояние другого сегмента (рис. 8). Повторитель действует на электрическом уровне для соединения двух сегментов. Повторители ничего распознают сетевые адреса и поэтому не могут использоваться для уменьшения трафика.

Повторители (repeater) представляют собой сетевые устройства, функционирующие на первом (физическом) уровне эталонной модели OSI. Для того чтобы понять работу повторителя, необходимо знать, что по мере того, как данные покидают устройство отправителя и выходят в сеть, они преобразуются в электрические или световые импульсы, которые после этого передаются по сетевой передающей среде. Такие импульсы называются сигналами (signals). Когда сигналы покидают передающую станцию, они являются четкими и легко распознаваемыми. Однако чем больше длина кабеля, тем более слабым и менее различимым становится сигнал по мере прохождения по сетевой передающей среде.

|  |  |
| --- | --- |
| https://pandia.ru/text/81/534/images/img8_47.png  Рис. 8. Повторители (Repeater) | Целью использования повторителя является регенерация и ресинхронизация сетевых сигналов на битовом уровне, что позволяет передавать их по среде на большее расстояние. Термин повторитель (repeater) первоначально означал отдельный порт «на входе» некоторого устройства и отдельный порт на его «выходе». В настоящее время используются также повторители с несколькими портами. В эталонной модели OSI повторители классифицируются как устройства первого уровня, поскольку они функционируют только на битовом уровне и не просматривают другую содержащуюся в пакете информацию. |

5. Коммутаторы (Switch) - управляемые программным обеспечением центральные устройства кабельной системы, сокращающие сетевой трафик за счет того, что пришедший пакет анализируется для выяснения адреса его получателя и соответственно передается только ему (рис.9).Использование коммутаторов является более дорогим, но и более производительным решением. Коммутатор обычно значительно более сложное устройство и может обслуживать одновременно несколько запросов. Если по какой-то причине нужный порт в данный момент времени занят, то пакет помещается в [буферную](http://www.pandia.ru/text/category/bufer/) память коммутатора, где и дожидается своей очереди. Построенные с помощью коммутаторов сети могут охватывать несколько сотен машин и иметь протяженность в несколько километров.

|  |
| --- |
| https://pandia.ru/text/81/534/images/img9_47.png  Рис. 9. Коммутатор |

6. Маршрутизаторы (Router) - стандартные устройства сети, работающие на сетевом уровне и позволяющее переадресовывать и маршрутизировать пакеты из одной сети в другую, а также фильтровать широковещательные сообщения (рис. 10).

7. Мосты (Bridge)- устройства сети, которое соединяют два отдельных сегмента, ограниченных своей физической длиной, и передают трафик между ними (рис.11). Мосты также усиливают и конвертируют сигналы для кабеля другого типа. Это позволяет расширить максимальный размер сети, одновременно не нарушая ограничений на максимальную длину кабеля, количество подключенных устройств или количество повторителей на сетевой сегмент.

|  |  |
| --- | --- |
| https://pandia.ru/text/81/534/images/img10_40.png  Рис. 10. Беспроводной маршрутизатор | https://pandia.ru/text/81/534/images/img11_39.png  Рис. 11. Мосты (Bridge)- |

8. Шлюзы (Gateway) - программно-аппаратные комплексы, соединяющие разнородные сети или сетевые устройства. Шлюзы позволяет решать проблемы различия протоколов или систем адресации. Они действует на сеансовом, представительском и прикладном уровнях модели OSI.

9. Мультиплексоры – это устройства центрального офиса, которое поддерживают несколько сотен цифровых абонентских линий. Мультиплексоры посылают и получают абонентские данные по телефонным линиям, концентрируя весь трафик в одном высокоскоростном канале для передачи в Internet или в сеть компании.

10. Межсетевые экраны (firewall, брандмауэры) - это сетевые устройства, реализующие контроль за поступающей в локальную сеть и выходящей из нее информацией и обеспечивающие защиту локальной сети посредством фильтрации информации. Большинство межсетевых экранов построено на классических моделях разграничения доступа, согласно которым субъекту (пользователю, программе, процессу или сетевому пакету) разрешается или запрещается доступ к какому-либо объекту (файлу или узлу сети) при предъявлении некоторого уникального, присущего только этому субъекту, элемента. В большинстве случаев этим элементом является пароль. В других случаях таким уникальным элементом является микропроцессорные карточки, биометрические характеристики пользователя и т. п. Для сетевого пакета таким элементом являются адреса или флаги, находящиеся в заголовке пакета, а также некоторые другие параметры. Таким образом, межсетевой экран - это программный и/или аппаратный барьер между двумя сетями, позволяющий устанавливать только авторизованные межсетевые соединения. Обычно межсетевые экраны защищают соединяемую с Internet корпоративную сеть от проникновения извне и исключает возможность доступа к конфиденциальной информации.

Беспроводные локальные сети считаются перспективным направлением развития ЛС. Их преимущество - простота и мобильность. Также исчезают проблемы, связанные с прокладкой и монтажом кабельных соединений - достаточно установить интерфейсные платы на рабочие станции, и сеть готова к работе.

Сердцем любой беспроводной сети является точка доступа (рис. 12), через которую конечные устройства по радио связываются с корпоративной сетью. Она определяет не только радиус действия и скорость передачи данных, но и решает элементарные задачи управления и обеспечения безопасности.

Хорошие точки доступа оснащаются двумя антеннами, причем в каждый момент времени работает антенна с лучшим качеством приема. Переключение антенн уже на удалении в несколько метров дает повышение качества и, соответственно, скорости передачи по сравнению с «однорукими» точками доступа. Обычно используемые ненаправленные антенны жестко крепятся к корпусу.

|  |  |
| --- | --- |
| Радиохарактеристики точки доступа во многом определяются тем, какие антенны используются. Так, одну и ту же точку доступа с разными антеннами можно использовать для решения разных задач. Если, к примеру, точка доступа применяется в качестве радиомоста между зданиями, удаленными на 2 км или более (до 25 км), то предпочтительнее установить направленную антенну. | https://pandia.ru/text/81/534/images/img12_35.png  Рис. 12. Точка доступа |

Программное обеспечение локальных сетей.

После подключения компьютеров к сети необходимо установить на них специальное сетевое программное обеспечение. Существует два подхода к организации сетевого программного обеспечения:

сети с централизованным управлением; одно-ранговые сети. Сети с централизованным управлением.

В сети с централизованным управлением выделяются одна или несколько машин, управляющих обменом данными по сети. Диски выделенных машин, которые называются файл-серверами, доступны всем остальным компьютерам сети. На файл-серверах должна работать специальная сетевая операционная система. Обычно это мультизадачная ОS, использующая защищенный режим работы процессора.

Остальные компьютеры называются рабочими станциями. Рабочие станции имеют доступ к дискам файл-сервера и совместно используемым принтерам, но и только. С одной рабочей станции нельзя работать с дисками других рабочих станций. С одной стороны, это хорошо, так как пользователи изолированы друг от друга и не могут случайно повредить чужие данные. С другой стороны, для обмена данными пользователи вынуждены использовать диски файл-сервера, создавая для него дополнительную нагрузку.

Есть, однако, специальные программы, работающие в сети с централизованным управлением и позволяющие передавать данные непосредственно от одной рабочей станции к другой минуя файл-сервер. Пример такой программы - программа NetLink. После ее запуска на двух рабочих станциях можно передавать файлы с диска одной станции на диск другой, аналогично тому, как копируются файлы из одного каталога в другой при помощи программы Norton Commander.

На рабочих станциях должно быть установлено специальное программное обеспечение, часто называемое сетевой оболочкой. Это обеспечение работает в среде той ОS, которая используется на данной рабочей станции, - DOS, OS/2 и т. д.

Файл-серверы могут быть выделенными или невыделенными. В первом случае файл-сервер не может использоваться как рабочая станция и выполняет только задачи управления сетью. Во втором случае параллельно с задачей управления сетью файл-сервер выполняет обычные пользовательские программы в среде MS-DOS. Однако при этом снижается производительность файл-сервера и надежность работы всей сети в целом, так как ошибка в пользовательской программе, запущенной на файл-сервере, может привести к остановке работы всей сети. Поэтому не рекомендуется использовать невыделенные файл-серверы, особенно в ответственных случаях.

Существуют различные сетевые ОS, ориентированные на сети с централизованным управлением. Самые известные из них - Novell NetWare, [Microsoft](http://www.pandia.ru/text/category/microsoft/" \o "Microsoft) Lan Manager (на базе OS/2), а также выполненная на базе UNIX System V сетевая ОS VINES.

Порядок [выполнения работы](http://www.pandia.ru/text/category/vipolnenie_rabot/):

Изучите теоретический материал;

Письменно ответьте на контрольные вопросы первой части;

Письменно ответьте на контрольные вопросы второй части;

Составьте отчет о проделанной работе.  
  
Контрольные вопросы:

Основная часть

Что такое компьютерная сеть? Что необходимо для создания компьютерных сетей? Какова основная задача, решаемая при создании компьютерных сетей? Что такое протоколы? Для чего они предназначены? По какому принципу компьютерные сети делятся на локальные и глобальные? Что такое интерфейсы? Что такое серверы сети? Какие сети называются одноранговыми? Что такое рабочие станции? Какие кабели можно использовать в качестве передающей среды в проводных сетях? Что используются в качестве передающей среды в беспроводных локальных сетях? Что представляет технология Ethernet? Что такое сетевой адаптер? Какие вы знаете топологии сетей? Каковы преимущества беспроводных локальных сетей? Каково назначение точки доступа? Чем отличаются сети с выделенным сервером от одноранговых сетей? Что такое технология клиент-сервер? Приведите примеры сетевых операционных систем.

Дополнительная часть

Что такое топология сети? Что представляет собой проводник витая пара? Каково устройство коаксиального кабеля? Почему оптоволоконный кабель является приоритетным для проводных сетей? В чем его недостатки? Что такое шлюзы? Какими могут быть шлюзы? Зачем нужны повторители? В чем состоят преимущества использования коммутаторов? Для чего служит межсетевой экран (брандмауэр)? Что такое концентратор? Что такое маршрутизатор? В чем заключаются преимущества и недостатки сетей с выделенным сервером? Для чего предназначена программа NetLink? Чем отличается выделенные файл-серверы от невыделенных?  
Содержание отчета:

Оформить отчет следующего содержания:

наименование работы; цель работы; задание; последовательность выполнения работы; вывод о проделанной работе.

# Практическая работа №3

Тема: Обеспечение защиты информации в сети с использованием программно-аппаратных средств

**Цель:** изучить возможности защиты архива паролем, научиться использовать программу вскрытия паролей Advanced ZIP Password Recovery

# Проблема: забытые пароли

Если вы будете честно следовать правилам установки паролей, то вскоре начнёте их путать и забывать. Windows берёт часть работы на себя. Он запомнит, если вы захотите, логины и пароли на веб-сайтах, сохранит ключи шифрования, электронные сертификаты. Единственное, что вам необходимо помнить — это ваши имя пользователя и пароль. Пользователь в Windows сам управляет своими паролями. При утере пароля администратор, конечно, может присвоить новый пароль. Но при этом вы потеряете доступ ко всем вашим зашифрованным данным и сертификатам.

Если требуется восстановить утерянный пароль (либо проверить насколько уязвимым по отношению к атакам является компьютер), можно воспользоваться программами восстановления паролей. Они различаются по методам взлома (атаки со словарём, извлечение хэшей паролей из базы данных SAM или, что ещё лучше, извлечение подобной информации из памяти, грубый перебор всех вариантов) и способом работы (после загрузки с диска, после загрузки в другой операционной системе, с другого компьютера, подключённого к сети, с другого рабочего стола).

Рассмотрим пример программы для восстановления паролей

**Advanced Office Password Recovery (AOPR)** - программа для восстановления забытых паролей к документам Microsoft Office.

**Advanced Office Password Recovery** позволяет восстанавливать пароли либо обходить парольную защиту файлов и документов, созданных в продуктах семейства MS Office всех версий. В данный момент поддерживаются версии с

2.0 по 2010 включительно. Программа поддерживает документы, созданные MS Word, Excel, Access, Outlook, Project, Money, PowerPoint, Publisher, а также OneNote. Кроме перечисленного, программа позволяет получить доступ к исходным текстам VBA макросов, защищенных паролем.

# Возможности Advanced Office Password Recovery

* + Поддержка всех версий Microsoft Office с 2.0 по 2010
  + Мгновенное восстановление отдельных паролей
  + Изменение пароля на указанный пользователем
  + Мгновенное снятие защиты с документов, для которых когда-либо были подобраны пароли
  + Использование всех обнаруженных уязвимостей продуктов семейства MS Office для восстановления доступа к документам
  + Предварительная атака с набором типичных параметров для восстановления стойких паролей
  + Поддержка атаки по словарю и прямого перебора паролей с использованием шаблонов масок
  + Аппаратное ускорение (подана заявка на патент) уменьшает время перебора паролей в 50 раз
  + Технология аппаратного ускорения с использованием видеокарт NVIDIA или ATI
  + Поддержка одновременно до 32 центральных процессоров или ядер и до 8 графических процессоров
  + Оптимизация кода под современные процессоры позволяет достичь максимальной в данном классе продуктов скорости перебора паролей **Мгновенное восстановление доступа к защищенным документам**

Во многих случаях **Advanced Office Password Recovery** позволяет восстановить доступ к защищенным документам в ту же секунду. Например, старые версии MS Office используют очень простую систему шифрования, которая позволяет вычислить пароль. Также в некоторых версиях Office используются алгоритмы с ограничением длины ключа

Помимо указанных приложений, с помощью **Advanced Office Password Recovery** возможно мгновенное восстановление доступа к документам, защищенным другими версиями продуктов семейства MS Office. В частности, поддерживается возможность восстановления сохраненных паролей, используемых для авторизации через MS Passport (LiveID).

# Методы восстановления пароля Предварительная атака

Если документ защищен стойким паролем, его расшифровка может занять

много времени. Для удобства пользователей в программе предусмотрена предварительная атака, которая автоматически перебирает все типичные пароли и использует атаку по словарю. Также производится поиск среди паролей, которые когда-либо были восстановлены для других документов.

# Перебор по маске

В случае наличия дополнительной информации о пароле (известна длина пароля в символах или любая часть пароля, либо есть информация об использовании или отсутствии в пароле определенных символов и цифр) скорость восстановления может быть существенно увеличена методом перебора по заданной маске.

# Атака по словарю

Согласно статистике, существенная часть паролей, используемых для защиты офисных документов, содержит одно или несколько слов из словаря. Метод подбора паролей по словарю позволяет в десятки раз сократить время, требуемое для восстановления пароля. **Advanced Office Password Recovery** поддерживает атаку по словарю, перебирая пароли, состоящие из слов и их возможных комбинаций в разных регистрах и на нескольких языках. Поддерживается возможность подключения дополнительных словарей.

# Прямой перебор

В случае полного отсутствия информации о пароле осуществляется перебор всех возможных вариантов пароля определенной длинны для восстановления доступа к документу. В **Advanced Office Password Recovery** используются новейшие методы низкоуровневой оптимизации кода под современные процессоры, позволяющие достичь высокой производительности перебора по сравнению с конкурирующими продуктами.

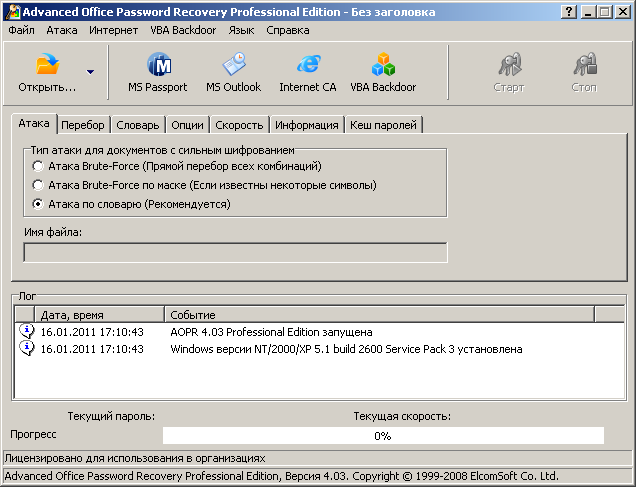


Рис. 3 Интерфейс программы

# Выполнить практическое задание:

**Задание 1. Восстановление пароля в документах MS Office**

**Указание:** при выполнении задания используйте документы MS Word, MS Excel, MS Access, защищенные паролем

* + Откройте программу **Advanced Office Password Recovery (AOPR)**
  + В панели инструментов окна программы выберите **Открыть**
  + В окне открытия файла выберите защищенный файл MS Word
  + Просмотрите результат: пароль восстановлен?
  + Аналогично выберите документ MS Excel, затем файл базы данных MS Access
  + Изучите возможности программы

# Выполнить конспект задания в тетради

**Задание 2**

1. Выполните поиск в сети Internet специализированных программных средств для создания, а также для восстановления паролей
2. Подготовьте сообщение по данной теме

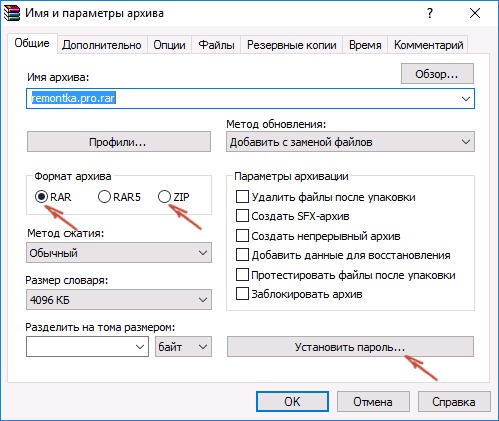
# Установка пароля на архив

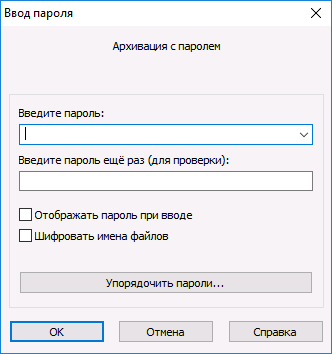
Создание архива с паролем, при условии, что этот пароль достаточно сложен — очень надежный способ защитить свои файлы от просмотра посторонними. Несмотря на обилие разнообразных программ **Password Recovery** для подбора паролей архивов, если он будет достаточно сложным, взломать его не получится.

**Установка пароля на архивы ZIP и RAR в программе WinRAR**

В WinRAR вы можете создавать архивы RAR и ZIP, и устанавливать пароли на оба типа архива. Однако, шифрование имен файлов доступно только для RAR (соответственно, в ZIP, чтобы извлечь файлы понадобится ввести пароль, однако имена файлов будут видны и без него).

**Первый способ** создать архив с паролем в WinRAR — выделить все файлы и папки для помещения в архив в папке в Проводнике или на Рабочем столе, кликнуть по ним правой кнопкой мыши и выбрать пункт контекстного меню **Добавить в архив…** с иконкой WinRAR.

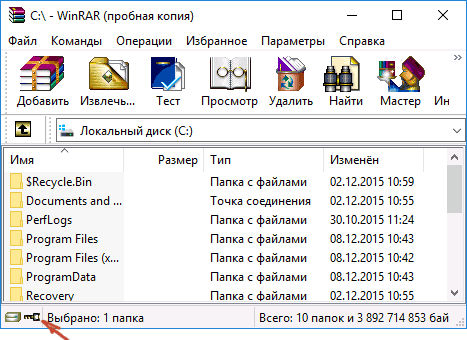


Откроется окно создания архива, в котором, помимо выбора типа архива и места его сохранения, вы можете нажать кнопку **Установить пароль**, после чего дважды ввести его, при необходимости включить шифрование имен файлов (только для RAR). После этого нажмите ОК, и еще раз ОК в окне создания архива — архив будет создан с паролем.

Если в контекстном меню по правому клику нет пункта для добавления в архив WinRAR, то вы можете просто запустить архиватор, выбрать файлы и папки для архивации в нем, нажать кнопку **Добавить** в панели сверху, после чего проделать те же действия по установке пароля на архив.

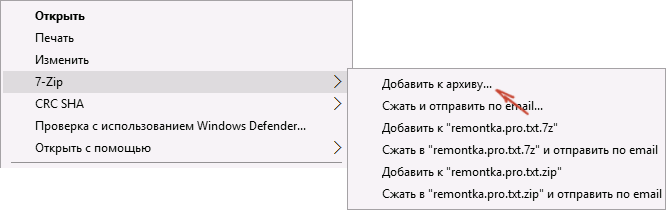
**Второй способ** поставить пароль на архив или все архивы, в дальнейшем создаваемые в WinRAR — нажать по изображению ключа слева внизу в строке

состояния и задать необходимые параметры шифрования. При необходимости установите отметку **Использовать для всех архивов**.

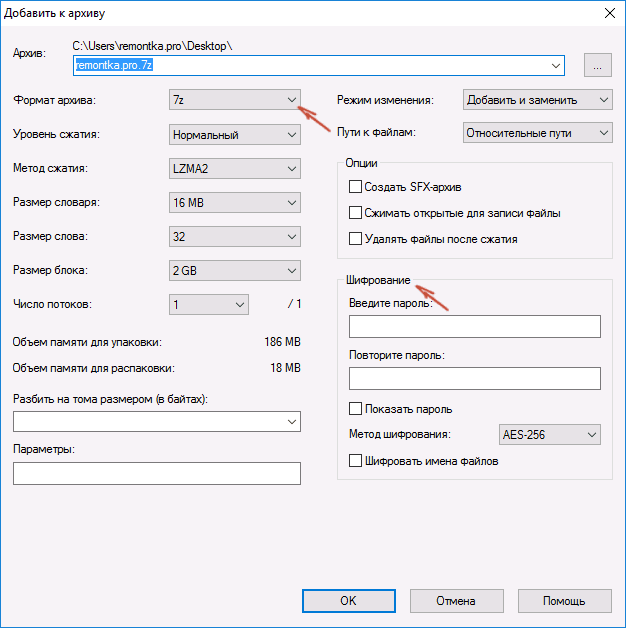


**Создание архива с паролем в 7-ZIP**

С помощью бесплатного архиватора 7-Zip можно создавать архивы 7z и ZIP, устанавливать на них пароль и выбирать тип шифрования (а распаковывать можно и RAR). Точнее, можно создавать и другие архивы, но установить пароль возможно лишь на два указанных выше типа.



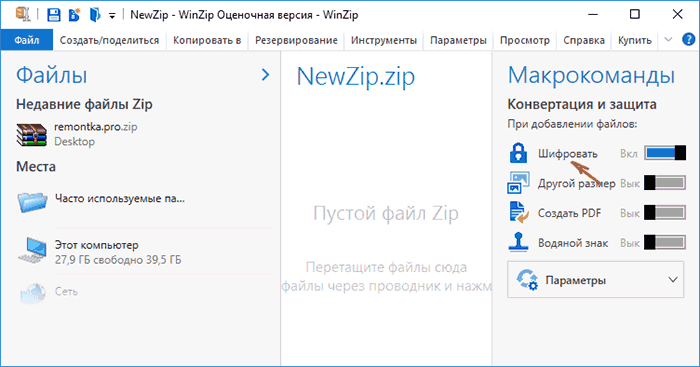
Так же, как и в WinRAR, в 7-ZIP создание архива возможно с помощью пункта контекстного меню **Добавить к архиву** в разделе **7-ZIP** или из главного окна программы с помощью кнопки **Добавить**.

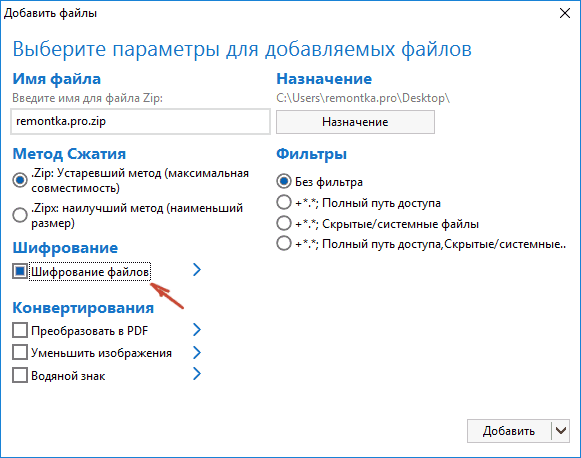


В обоих случаях вы увидите одинаковое окно добавления файлов в архив, в котором, при выборе форматов 7z (по умолчанию) или ZIP будет доступно включение шифрования, при этом для 7z доступно также и шифрование файлов. Просто задайте желаемый пароль, при желании включите скрытие имен файлов и нажмите ОК. В качестве метода шифрования рекомендованы AES-256 (для ZIP имеется также ZipCrypto).

**В WinZip**

С помощью WinZIP можно создать архивы ZIP (или Zipx) с шифрованием AES-256 (по умолчанию), AES-128 и Legacy (тот самый ZipCrypto). Сделать это можно в главном окне программы, включив соответствующий параметр в правой панели, а затем задав параметры шифрования ниже (если вы их не зададите, то при добавлении файлов в архив вас просто попросят указать пароль).



При добавлении файлов в архив с помощью контекстного меню проводника, в окне создания архива просто отметьте пункт **Шифрование файлов**, нажмите кнопку **Добавить** внизу и установите пароль на архив после этого.

# Выполнить практическое задание:

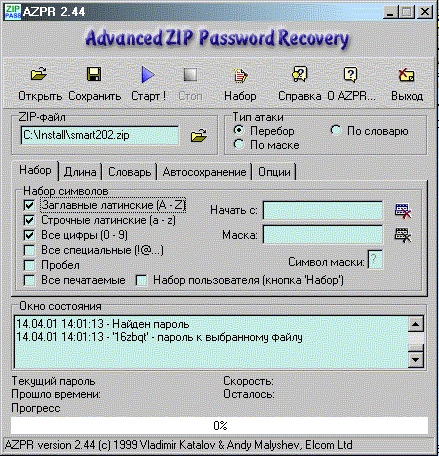
**Задание 3.** Создайте 2 архива, содержащие по 3 файла. Установите пароль на каждый архив

# Работа с программами взлома на примере AZPR

Программа AZPR используется для восстановления забытых паролей ZIP- архивов. На сегодняшний день существует два способа вскрытия паролей: перебор (brute force) и атака по словарю (dictionary-based attack).

# Панель управления:

* кнопки **Открыть** и **Сохранить** позволяют работать с проектом, в котором указан вскрываемый файл, набор символов, последний протестированный пароль. Это позволяет приостанавливать и возобновлять вскрытие.
* кнопки **Старт** и **Стоп** позволяют соответственно начинать и заканчивать подбор пароля.
* кнопка **Набор** позволяет задать свое множество символов, если известны символы, из которых состоит пароль.
* кнопка **Справка** выводит помощь по программе.
* кнопка **O AZPR** выводит информацию о программе.
* кнопка **Выход** позволяет выйти из программы



Рассмотрим возможности программы:

# Выбирается архив для вскрытия и тип атаки (см. рис).

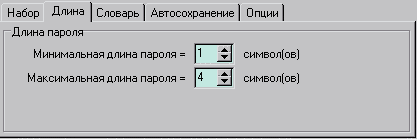
https://studfiles.net/html/2706/601/html_k8lrK7nHjh.fK4x/img-qQRSsM.png

**Выбираются параметры работы:**

* Закладка **Набор**

Программа позволяет выбрать область перебора (набор символов). Это значительно сокращает время перебора. Можно использовать набор пользователя, заданный с помощью кнопки Набор. Можно ограничить количество тестируемых паролей, задав начальный пароль. В случае если известна часть пароля, очень эффективна атака по маске. Нужно выбрать соответствующий тип атаки, после этого станет доступным поле маска. В нем нужно ввести известную часть пароля в виде **P?s?W?r?** , где на месте неизвестных символов нужно поставить знак вопроса. Можно использовать любой другой символ, введя его в поле символ маски.

* Закладка **Длина -** позволяет выбрать длину пароля



* Закладка **Словарь**

Позволяет выбрать файл-словарь. Выбирайте файл **English.dic**, он содержит набор английских слов и наборы символов, наиболее часто использующиеся в качестве паролей.

* Закладка **Автосохранение**

Можно выбрать имя файла для сохранения результатов работы и интервал автосохранения.

* Закладка **Опции**

Выбирается приоритет работы (фоновый или высокий), интервал обновления информации о тестируемом в данный момент пароле. Увеличение интервала повышает быстродействие, но снижает информативность. Также можно установить режим ведения протокола работы и возможность минимизации программы в **tray** (маленькая иконка рядом с часами).

# Выполнить практическое задание:

**Задание 4. Вскрытие пароля архива**

Используются архивы с паролями из задания 3.

# Проведение атаки перебором (bruteforce attack)

1. Используя программу для вскрытия паролей произвести атаку на зашифрованные архивный файлы созданный вами ( не менее 5 файлов). Используйте при создания паролей разное сочетание допустимых символов алфавита, но не более 4 символов. Зафиксируйте время нахождения пароля в каждом случае. Сделайте выводы, как от сложности пароля зависит время вскрытия пароля.
2. Выполнив пункт 1, сократить область перебора до фактически используемого (например если пароль 6D1A – то выбрать прописные английские буквы и цифры). Провести повторное вскрытие. Сравнить затраченное время.

# Проведение атаки по словарю (dictionary attack)

1. Сжать какой-либо небольшой файл, выбрав в качестве пароля английское слово длиной до 5 символов (например love, god, table, admin и т.д.). Провести атаку по словарю. Для этого выбрать вид атаки и в закладке Словарь выбрать файл English.dic. Он содержит набор английских слов и наборы символов, наиболее часто использующиеся в качестве паролей.
2. Попытаться определить пароль методом прямого перебора. Сравнить затраченное время.

# Оформить конспект работы в тетради Контрольные вопросы:

1. Какие виды атак на пароль Вы знаете?
2. Что такое плохой пароль?
3. Как можно противостоять атаке полным перебором?
4. Как длина пароля влияет на вероятность раскрытия пароля?
5. Какие рекомендации по составлению паролей Вы можете дать?

**Практическая работа № 4**

Тема: Перенимание участия в приемосдаточных испытаниях компьютерных сетей и сетевого оборудования различного уровня и в оценке качества и экономической эффективности сетевой топологии

Цель работы: получить практические навыки работы с онлайн калькуляторами: тестирования СКС и расчет стоимости монтажа компьютерной сети

**Задание 1** Расчет стоимости монтажа компьютерной сети

Используя Онлайн калькулятор рассчитайте стоимость монтажа компьютерной сети <http://net-services.ru/calc2.php> (необходимые данные возьмите из практической работы № 10)

**Задание 2** Тестирование СКС

Используя Онлайн калькулятор рассчитайте стоимость тестирования СКС <http://www.stroi-tk.ru/price/calculator_test_sks/> (необходимые данные возьмите из практической работы № 10)

**Задание 3** Онлайн сервис цены на монтаж и тестирование скс, локальной сети Используя Онлайн сервис просчитайте монтаж и тестирование скс, локальной сети (необходимые данные так же возьмите из практической работы № 10) https://comdas.ru/up/lvs/tsenyi-na-montazh-sks-lokalnoy-seti/

и сравните результаты с предыдущими сайтами (задание 1 и 2)

Для отчета предоставьте скрины выполненных работ.

**Практическая работа №5**

**Выполнение требований нормативно-технической документации, иметь опыт оформления проектной документации**

Цель занятия: Изучить основные стадии разработки конструкторской документации.

Теоретические положения:

Основными стадиями опытно-конструкторских работ являются:

* техническое задание;
* техническое предложение;
* эскизный проект;
* технический проект;
* разработка рабочей документации опытного образца;
* изготовление и предварительные (заводские) испытания опытного образца;
* приемочные испытания опытных образцов;
* разработка рабочей документации установочной серии;
* разработка рабочей документации установившегося серийного производства;
* авторский надзор.

Исходным документом для проектирования любых изделий является **техническое задание (ТЗ)**, разрабатываемое совместно научно-исследовательскими и проектно-конструкторскими организациями с привлечением заводов-изготовителей, заказчиков. ТЗ может разрабатываться заказчиком и самостоятельно.

Научно-исследовательские организации обеспечивают научное обоснование показателей разрабатываемого изделия, а проектно-конструкторские – разрабатывают его схемное решение, принципиальную конструкцию узлов и изделия в целом.

Техническое задание устанавливает основное назначение техническую и тактико-техническую характеристику, технико-экономические требования, предъявляемые к новому изделию, сроки выполнения работ, объемы изготовления, показатели качества, требования технической эстетики, техники безопасности и гигиены труда, а также дается оценка перспективности разработки. В ТЗ отражают вопросы целесообразности создания модификаций нового изделия, особенности управления и регулирования рабочих органов, унификации узлов машины, сезонности работ, особенности облуживания и состава персонала, а также ценообразования.

В ТЗ следует устанавливать количество опытных образцов или объем опытной партии, которые должны быть достаточными для получения достоверной оценки свойств в предусмотренных условиях ее эксплуатации (или имитации этих условий).

В ТЗ указывают порядок сдачи и приемки результатов разработки, который в общем случае содержит:

* виды изготовленных образцов (экспериментальные, опытные, головные);
* категории испытаний;
* место проведения испытаний;
* необходимость рассмотрения результатов на приемочной комиссии и ее состав;
* документы, предъявляемые на приемку.

Наряду со стандартами ЕСКД, разработка технических заданий регламентируется еще целым рядом других стандартов, как отраслевых, так и государственных, различными руководящими материалами по проектированию и т.д. ГОСТ 15.001-88 «Система разработки и поставки продукции на производство. Продукция производственно-технического назначения» устанавливает общий порядок разработки ТЗ, их согласование и утверждение. ГОСТ 15.150-69 регламентирует условия эксплуатации, климатическое исполнение. ГОСТ 16.263-70 устанавливает термины и определения метрологических характеристик. ГОСТ 27.003-89 нормирует показатели качества. В отраслевом стандарте ОСТ 41.01.93-83 «Система разработки и постановки продукции на производство. Изделия геологоразведочной техники» приводятся все требования к структуре проектных работ на новую технику геологоразведочного сортамента.

ТЗ после его согласования и утверждения является основанием для выполнения проектных работ.

Первой стадией разработки проектной документации является **техническое предложение (ТП)**, выполняемое в соответствие с ГОСТ 2.118-73. Этот документ является как бы ответом проектанта на полученное им техническое задание. Он содержит технические и технико-экономические обоснования целесообразности разработки документации на изделие. Обоснование производится на основе анализа технического задания заказчика, существующих изделий аналогичного назначения, различных вариантов возможных решений изделий, сравнительной оценки решений с учетом конструктивных и эксплуатационных особенностей разрабатываемого и существующих изделий, патентных материалов. ТП должно содержать: обзор существующих образцов аналогичных или близких по назначению изделий отечественного и зарубежного производства, оценку их конструктивных особенностей и эксплуатационных показателей, варианты процессов работы, варианты компоновок будущего изделия, расчет производительности по каждому варианту.

В ТП должны быть указаны преимущества и недостатки каждого варианта, даны технико-экономические показатели изделия в оптимальном варианте (сравнительные данные по производительности, срокам окупаемости), общий вид изделия оптимального варианта, краткое описание его конструкции и принципа действия.

Возможны случаи, когда в ТЗ дается четкое решение какого-то вопроса, например оптимальный вариант буровой установки – самоходный. В этом случае проектанту в ТП не требуется разрабатывать варианты компоновки и указывать оптимальный вариант.

После согласования и утверждения ТП является основанием для разработки эскизного проекта.

**Эскизный проект (ЭП)**– это совокупность конструкторских документов, которые должны содержать принципиальные конструкторские решения, дающие общее представление об устройстве и принципе работы изделия. Кроме того, ЭП определяет назначение, основные параметры и габаритные размеры разрабатываемого изделия. Структура ЭП и порядок его разработки регламентируется ГОСТ 2.119-73. При выполнении ЭП производится следующая работа:

* конструкторская проработка оптимального варианта;
* выполняются в эскизном исполнении основные сборочные единицы изделия;
* уточняется общий вид изделия;
* разрабатывается кинематическая схема;
* разрабатывается циклограмма или предварительная принципиальная электрическая схема и другие основные конструкторские документы в зависимости от специфики изделия;
* производится краткое описание конструкции и принципа работы изделия;
* указывается уточненная производительность, дается технико-экономический расчет.

На стадии эскизного проектирования могут разрабатываться и изготавливаться макеты отдельных сборочных единиц изделия или изделия в целом для проверки новых или наиболее важных конструкторских решений.

ЭП после согласования и утверждения служит основанием для разработки технического проекта.

**Технический проект**– это совокупность конструкторских документов, которые должны содержать окончательные технические решения, дающие полное представление об устройстве разрабатываемого изделия и исходные данные для разработки рабочей документации. Основное содержание и порядок выполнения технического проекта определяется ГОСТ 2.120-73.

В техническом проекте содержится:

* описание окончательной конструкции изделия и принципа его действия (работы);
* обоснование выбора материалов и видов защитных покрытий;
* требования к точности сборки отдельных сборочных единиц и всего изделия;
* описание всех схем;
* окончательный технико-экономический расчет.

Технический проект после согласования и утверждения служит основанием для разработки рабочей конструкторской документации, т.е. рабочего проекта.

Разработка **рабочей документации**осуществляется проектной организацией обычно совместно с заводом-изготовителем на основе ТЗ и технического проекта в соответствии с требованиями государственных и отраслевых стандартов, которые устанавливают следующие виды рабочей конструкторской документации:

* конструкторская документация на опытный образец (опытную партию), имеющая литеру **О1, О2, О3**и т.д.;
* конструкторская документация на установочную (головную) серию (литера **А**);
* конструкторская документация для установившегося серийного или массового производства (литера **Б**).

Отдельным пунктом выступает разработка рабочей документации для индивидуального производства (литера **И**), когда изделие изготавливается в 1 – 2-х экземплярах, например экспериментальная установка специального назначения.

В комплект рабочей документации должны входить следующие конструкторские документы:

* чертежи всех деталей (кроме стандартных) с простановкой всех размеров с допусками, степенью обработки и другой информацией, необходимой для изготовления;
* чертеж общего вида изделия;
* чертежи подузлов, узлов и групп для слесарей-сборщиков;
* сборочные чертежи изделия;
* технические условия на изготовление, в которых даются допуски на взаимные перекосы, допустимые несоосности, люфты и т.д.;
* технические условия на поставку с учетом комплектации установок;
* программы стендовых (заводских) и промышленных испытаний;
* спецификация (ведомость) материалов, готовых изделий, необходимых для изготовления данного изделия;
* дополнительные расчеты, необходимость которых возникает при разработке рабочей документации;
* эксплуатационные документы (инструкции по эксплуатации, смазке, ремонту и т.д.);
* патентный формуляр.

В рабочем проекте дается предписание о количестве опытных образцов. Их может быть один или несколько. Количество опытных образцов зависит от назначения оборудования, его сложности и возможности получения исчерпывающих и достоверных данных о работоспособности и долговечности нового оборудования или инструмента.

Рабочая документация согласовывается с заказчиком, заводом-изготовителем, утверждается в установленном порядке и передается на завод-изготовитель.

В данной главе рассмотрены все проектные стадии разработки конструкторской документации. Однако наличие всех стадий в процессе разработки того или иного изделия не обязательно. Определяющим фактором в этом случае является степень **новизны**и **сложности** разрабатываемого изделия.

С точки зрения **новизны** все изделия делят на пять групп.

К Iгруппе относятся изделия, которые являются воспроизведением существующих образцов, без существенных переделок или с небольшими переделками.

Ко IIгруппе относятся конструктивные модификации существующих базовых моделей с использованием унифицированных узлов и механизмов.

К III группе относятся изделия, отличающиеся от существующих моделей и типов размерными параметрами.

К IVгруппе относятся изделия новые по конструктивному оформлению, но предназначенные для выполнения распространенных в практике операций.

К Vгруппе относятся изделия новые по конструктивному оформлению, основанные на принципиально новых конструкторских решениях.

**По сложности** все изделия можно разделить также на пять групп:

* группа **А**– изделия с простой кинематикой, с нерегулируемыми скоростями главных движений;
* группа **Б**– изделия со ступенчатым переключением скоростей подач;
* группа **В**– изделия, кинематика которых предусматривает ступенчатое или бесступенчатое регулирование скоростей при централизованном, но не автоматизированном управлении;
* группа **Г**– изделия автоматического или полуавтоматического типа;
* группа **Д**– изделия, в которых автоматизация операций осуществляется с применением электроники или специальных электрических и гидравлических схем.

*Соответствующее сочетание групп новизны и сложности должно быть решающим аргументом при определении необходимых стадий разработки конструкторской документации. Если предстоит разработка документации на новое и сложное изделие, то предусматриваются все стадии разработки.*

*Контрольные вопросы:*

*1.Назовите* основные стадии опытно-конструкторских документов?

2.Техническое задание содержит?

3. Какие задачи выполняет техническое предложение?

4.Эскизный проект-это?

5.Какие функции выполняет эскизный проект?

6.Технический проект– это?

7. В техническом проекте содержится?

8. Виды рабочей конструкторской документации?

# Практическая работа № 6

**Администрирование локальных вычислительных сетей и принятие мер по устранению возможных сбоев**

**Цель работы:** находить и подключать к своему компьютеру сетевые принтеры, измерять скорость Интернета и определять IP-адрес компьютера**.**

## Теоретические сведения к практической работе

Локальные сети в последнее время из модного дополнения к компьютерам все более превращаются в обязательную принадлежность любой организации, имеющей более одного компьютера.

**Локальные компьютерные сети –** это сложные структурированные кабельные системы, в составе которых функционирует множество компонентов. Именно поэтому крайне важен квалифицированный подход к проектированию сети и монтажу.

### Внедрение локальных компьютерных сетей осуществляется в несколько этапов.

1. *Разработка технического задания*. Определение технических требований и разработка технического задания. На данном этапе специалист выезжает к заказчику для проведения анализа его компьютерной сети.
2. *Обследование локальной компьютерной сети и сетевого оборудования.* Учитываются все пожелания заказчика, оговаривается такой немаловажный вопрос, как использование пассивного и активного сетевого оборудования. Предварительно определяется расположение кабельных каналов.
3. *Проектирование сети.* С клиентом уточняются последние детали проекта, учитываются упущенные пожелания, дорабатывается список оборудования. На основании технического задания составляется технико-коммерческое предложение, с учетом которого формируется список различного пассивного и активного сетевого оборудования, определяется его стоимость. Обговариваются сроки выполнения работ. Составляется договор и устанавливается порядок расчетов.
4. *Поставка оборудования*. Комплексная поставка оборудования в рамках реализации проекта, специальных программ замены устаревшего оборудования.
5. *Монтаж локальной сети и пусконаладочные работы*. Выполняется комплекс монтажных и пусконаладочных работ на объекте заказчика.
6. *Монтаж пассивного сетевого оборудования*. Установка кабельных каналов, укладка кабеля, монтаж розеток, монтаж коммутационных шкафов.
7. *Настройка локальной компьютерной сети*. Подключение и наладка активного сетевого оборудования (маршрутизаторы, KVM- переключатели, серверы, источники бесперебойного питания, фильтры, системы оптимизации трафика).
8. *Тестирование.* Выполненные работы проходят многоуровневое тестирование с выявлением и устранением возможных неисправностей. Тестирование осуществляется с помощью как тестового, так и компьютерного оборудования для выявления возможных ошибок в разводке кабельных систем.
9. *Сдача локальной компьютерной сети в эксплуатацию*. Подписание акта приемки-сдачи выполненных работ.

### Преимущества использования локальной компьютерной сети:

* оперативная передача файлов;
* разделение и совместное использование файлов, программ, принтеров и другого оборудования;
* электронная почта;
* координация совместной работы (взаимодействие территориально разнесенных сотрудников организации);
* упорядочивание делопроизводства, контроль доступа к информации, защита информации.

## Организация локальных компьютерных сетей

Существует разнообразные варианты организации локальных компьютерных сетей.

***Вариант 1***. Сеть без сервера с организацией выхода в Интернет для малых организаций от трех рабочих мест. Организация подключения корпоративной сети к Интернету посредством одного из рабочих компьютеров показана на рис.1.

***Вариант 2***. Сеть с выделенными файловым и интернет-серверами для компаний среднего масштаба с числом компьютеров от 10 и более. Данная конфигурация (рис.2) подходит для организации сетевых ресурсов на выделенном сервере в сети, а также для организации безопасного выхода в Интернет.

|  |  |
| --- | --- |
| Рис.1. Пример построения сети без выделенным сервером | Рис.2. Пример построения сети с выделенным сервером |
| Рис.3. Пример построения сети с выделенным сервером и безопасным выходом в Интернет | Рис.4. Пример построения сети с выделенным файловым, интернет- и SQL-серверами |

***Вариант 3.*** Сеть с выделенным сервером для организаций среднего масштаба с числом компьютеров от 10 и более. Данная конфигурация (рис. 3) подходит для организации сетевых ресурсов (общих документов, принтеров, баз данных) на выделенном сервере в сети.

***Вариант 4.*** Сеть с выделенными файловым, интернет- и SQL-серверами для средних и крупных компаний с числом компьютеров от 20 и более. Данная конфигурация (рис. 4) подходит для организации сетевых ресурсов на выделенном сервере в сети. Имеется возможность «жесткого» контроля доступа к интернет-ресурсам. SQL-сервер позволяет ускорить работу объемных баз данных (например, 1С).

# СОДЕРЖАНИЕ РАБОТЫ:

**Задание № 1.**

Измерить скорость Интернета и определить IP-адрес компьютера.

1. Запустите браузер.
2. Зайдите на сайт [http://www.speedtest.net](http://www.speedtest.net/) (это онлайн-сервис измерения скорости Интернета)
3. Нажмите кнопку **НАЧАТЬ**.
4. Через некоторое время в окне появится *СКАЧАТЬ (Входящая скорость)* и *ЗАГРУЗИТЬ (Исходящая скорость).* Скорость измеряется в кбайт/с (рис.5). В этом окне можно увидеть не только входящую и исходящую скорость, но и IP-адрес компьютера и название провайдера.
5. Определите IP-адрес вашего компьютера, название вашего провайдера. Запишите в тетрадь.

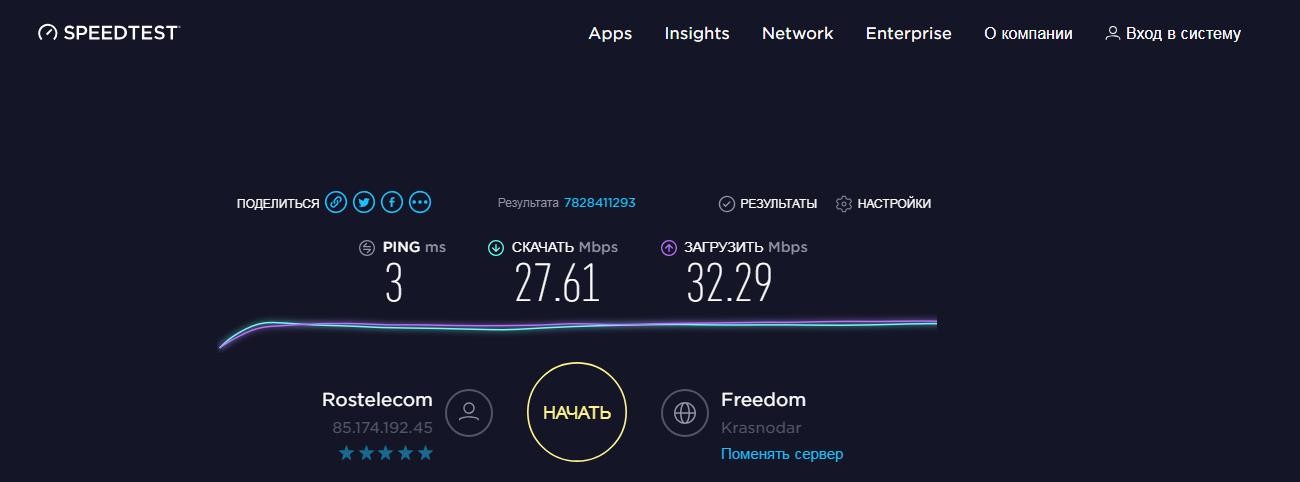


Рис.5. Измерение скорости.

**Задание № 2.**

Определить вариант организации локальной сети в компьютерном классе.

* 1. Выполните команду **Пуск-Панель управления-Центр управления сетями и общим доступом**

(рис. 6)

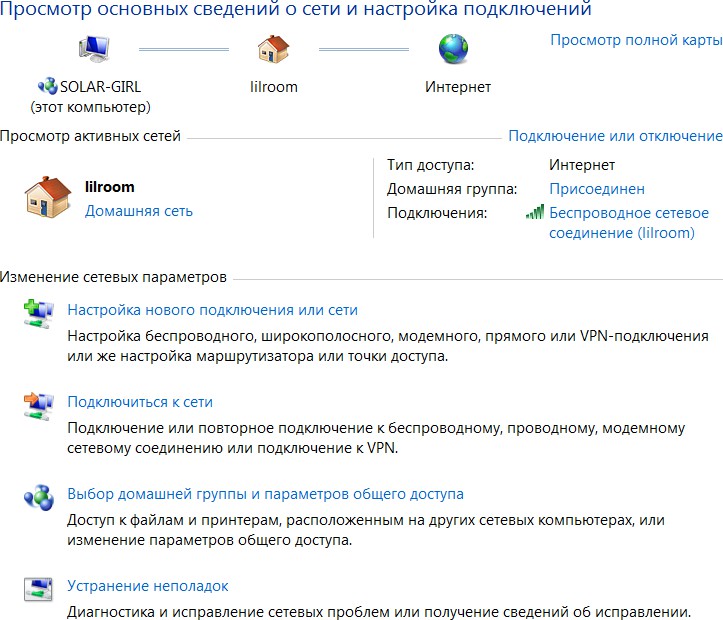


Рис. 6. Окно Центра управления сетями и общим доступом

* 1. Продемонстрируйте преподавателю результат работы.
  2. Определить вариант организации локальной сети, используя теоретические сведения к практической работе.
  3. Вариант организации локальной сети запишите в тетрадь.

**Задание № 3.**

Предоставить общий доступ к принтеру в локальной сети.

1. Для предоставления общего доступа к принтеру по локальной сети, необходимо на компьютере с подключенным принтером (компьютер преподавателя) выполнить команду **Пуск - Панель управления - Устройства и принтеры.**
2. Найти подключенный к компьютеру принтер, щелкнуть по нему правой клавишей мыши и в контекстном меню выбрать **Свойства принтера.** На вкладке **Доступ** выбрать **Общий доступ к данному компьютеру** и нажать кнопку **ОК.** После этого данный принтер автоматически определится на других компьютерах, подключенных к этой локальной сети.
3. Для установки принтера, который находится в общем доступе в локальной сети, на других компьютерах (компьютер ученика) зайдите в **Пуск - Панель управления - Устройства и принтеры.**
4. Выберите пункт **Установка принтер**а, после чего выберите **Добавить сетевой, беспроводной или Bluetooth-принтер,** далее следуйте указаниям **Мастера установки** принтера.
5. Сделайте обзор принтеров в локальной сети (рис. 7) и выберите необходимый.
6. Завершите процесс установки принтера.
7. Если принтер установлен, верно, распечатайте пробную страницу нажав на кнопку **Печать пробной страницы.**

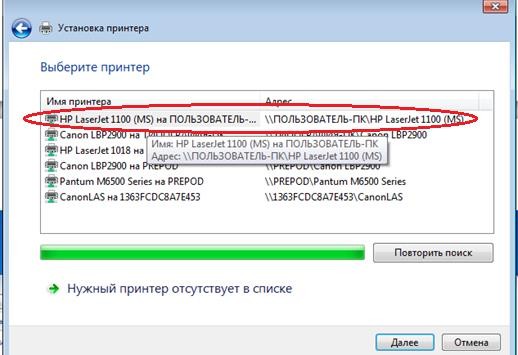


Рис. 7. Обзор имеющихся принтеров

1. Для частого использования данного принтера, зайдите **Пуск-Панель управления - Устройства и принтеры.** Найдите подключенный к компьютеру принтер, щелкните по нему правой клавишей мыши и в контекстном меню выберете **Использовать по умолчанию.**

## Задание № 4.

Выяснить название рабочей группы, в которую входят компьютеры, а так же найти имя вашего персонального компьютера.

1. Чтобы выяснить название рабочей группы, в которую входят персональные компьютеры, необходимо посмотреть свойства **Компьютера** (на рабочем столе найдите значок **Компьютер** и правой кнопкой мыши вызовите контекстное меню и выберите **Свойства**.
2. Название рабочей группы записать в тетрадь.
3. Там же найти имя вашего персонального компьютера и записать в тетрадь.
4. Методом подсчета выяснить, какие имена присвоены каждому из компьютеров, входящих в локальную сеть. Результаты записать в тетрадь.

## Задание № 5.

Решите задачу.

Максимальная скорость передачи данных в локальной сети 100 Мбит/с. Сколько страниц текста можно передать за 1 сек, если 1 страница текста содержит 50 строк и на каждой строке - 70 символов?

## Задание № 6.

Сделать вывод о проделанной практической работе.

**Практическая работа № 7**

**Тема:** Администрирование сетевых ресурсов в информационных системах

**Цели занятия:**

– Познакомиться с работой глобальной сетью Интернет, изучить основные возможности сетевого программирования.

**Методические указания**

Компьютерной сетью, или сетью ЭВМ, называется комплекс территориально рассредоточенных ЭВМ, связанных между собой каналами передачи данных. Объединенные в сеть компьютеры обладают существенным суммарным вычислительным потенциалом и обеспечивают повышение надежности работы всей системы в целом за счет дублирования ресурсов. Целесообразность создания компьютерной сети обуславливается следующим: возможностью использования территориально распределенного программного обеспечения, информационных баз данных и баз знаний, находящихся у различных пользователей; возможностью организации распределенной обработки данных путем привлечения ресурсов многих вычислительных машин; оперативному перераспределению нагрузки между компьютерами, включенными в сеть и ликвидации пиковой нагрузки за счет перераспределения ее с учетом часовых поясов; специализацией отдельных машин на работе с уникальными программами, которые нужны ряду пользователей сети; коллективизации ресурсов, в особенности дорогостоящего периферийного оборудования, которым экономически нецелесообразно укомплектовывать каждую ЭВМ.

Локальная сеть – это компьютерная сеть небольшой протяженности: в пределах комнаты, этажа, здания. Обычно такие сети действуют в пределах одного учреждения и имеют небольшой радиус действия: 1-10 км.

Локальная сеть обеспечивает высокие скорости передачи данных. А так как в этих сетях среда обычно контролируема, линии связи короткие, элементы структуры однородные, то частота ошибок в них низкая и протоколы обмена упрощены. В локальных сетях обычно не используются средства коммуникации общего назначения (телефонные линии) для организации обмена информацией.

Глобальная вычислительная сеть объединяет абонентов, расположенных в различных странах, на различных континентах. Взаимодействие между абонентами такой сети может осуществляться на базе телефонной линии связи, радиосвязи и систем спутниковой связи. Глобальные вычислительные сети позволяют решить проблему объединения информационных ресурсов всего мира и организации доступа к этим ресурсам.

Глобальные сети, в основном, используют в качестве каналов связи телефонные линии – это медленные каналы с высоким уровнем ошибок. Однако в настоящее время все более внедряются высокоскоростные оптоволоконные и радиоспутниковые каналы связи.

Примером глобальной сети является сеть Internet.

Возможности сети Internet определяются ее тремя основными функциями. Электронная почта (e-mail) – позволяет отправлять сообщения одному или нескольким адресатам; пересылать файлы, получать информацию от компьютерных программ. Передача файлов – это доступ к материалам, переведенным к разделу общедоступных. Эта процедура позволяет заходить на удаленные компьютеры и использовать источники информации в тех каталогах, которые администраторы системы открыли для общего доступа. Удаленный доступ позволяет подключиться к удаленному компьютеру и работать с ним в режиме диалога. Можно входить в любые компьютеры, которые включены в состав Internet, находить разнообразную информацию, работать с удаленным персональным компьютером как с собственным. Наличие трех указанных функций (базовых видов услуг) дает возможность организовать в Internet и предоставить пользователю много различных видов сетевых услуг. Электронная почта. С помощью почтовых программ Outlook Express, Netscape Messenger и др. Чтение и посылка текстов в Usenet. Отправка и получение файлов с помощью FTP (File Transfer Protocol)/ Поиск информации через WWW (World Wide Web) и через Gopher. Удаленное управление – запрос и запуск программ на удаленном компьютере. Chat-разговор с помощью сети IRC и электронной почты. Игры через Internet. Программы Outlook Express, Gopher, Netscape Messenger, обеспечивающие отдельные функции Internet, называют клиентами. Они удобны в использовании и предоставляют дружественный интерфейс для пользователей Internet.

В Internet очень популярен сервис UseNet – телеконференции. По своему характеру телеконференции близки к сообщением электронной почты и представляют собой электронные форумы. Пользователи Internet посылают туда свои сообщения, в которых высказываются по определенной интересующей их теме. Эти сообщения, называемые статьями, адресуются не отдельным пользователям, как в электронной почте, а в специальные дискуссионные группы – телеконференции. Для работы с телеконференциями существуют специальные программы чтения сообщений телеконференций – News Readers.

 Примеры сетевых информационных систем для различных направлений профессиональной деятельности (система электронных билетов, банковские расчеты, регистрация автотранспорта, электронное голосование, система медицинского страхования, дистанционное обучение и тестирование, сетевые конференции и форумы и пр.).

Бухгалтерский учет является самым сложным и трудоемким процессом учета, поэтому использование компьютерных технологий при обработке информации просто необходимо. Современные информационные системы предназначены для повышения эффективности работы предприятия.

**Автоматизация бухучета** – это процесс, при котором в результате перевода бухгалтерии на компьютер повышается эффективность и улучшается качество ведения бухучета на предприятии.

Выделяют следующие причины перехода к автоматизированным бухгалтерским информационным системам:

— облегчение работы при обработке документов, снижение трудоемкости

— снижение ошибок

— облегчение процесса подготовки баланса

— повышение эффективности и достоверности учета

— повышение оперативности

**Электронный билет**—**это особенная форма авиа- (в основном) или железнодорожного билета**, отличающаяся от обычной тем, что вся информация о рейсе (или поезде), пассажире и другие необходимые данные печатаются не на бумажном бланке, а хранятся в недрах специализированной компьютерной системы.

**Система расчетов по банковским картам** — платёжная система, объединяющая банкоматы различных банков.

Обычно банкоматы банка, выпустившего платежную банковскую карту, предоставляют расширенную функциональность, в то время как при работе с банкоматами других банков, объединённых системой расчёта, предоставляются только базовые услуги: просмотр баланса и получение наличных.

Системы расчётов бывают глобальные, которые охватывают большинство стран, и национальные, действующие в рамках одной страны.  
К глобальным системам относятся:

· PLUS, VISA,

· Cirrus, Maestro.

· China UnionPay

К национальным системам относятся:

· Cartes Bancaires или «СВ» — Франция,

· Quick и Bancjmat — Австрия,

· Multibanco — Португалия,

· Армениан Кард — Армения,

· Белкарт — Беларусь,

· НСМЭП — Украина,

· Золотая Корона — Россия и другие страны СНГ.

При безналичной форме расчетов проводятся записи по счетам в банках, когда деньги списываются со счета плательщика и зачисляются на счет получателя. Естественно, что широкому распространению такой формы денежных расчетов может способствовать только разветвленная сеть банков.

 Необходимо отметить, что проведение мероприятий по регистрации автотранспортных средств в органах Госавтоинспекции в соответствии с законодательствами о бухгалтерском учете и о налогах и сборах не оказывает никакого влияния на отражение в бухгалтерском и налоговом учетах хозяйственной операции по приобретению (реализации) этих автотранспортных средств.

В соответствии с Законом N 129-ФЗ от 21.11.96 «О бухгалтерском учете» все хозяйственные операции, проводимые организацией, должны оформляться оправдательными документами. Эти документы служат первичными учетными документами, на основании которых ведется бухгалтерский учет.

Автотранспортные средства, в соответствии с Положением по бухгалтерскому учету «Учет основных средств» ПБУ 6/01, утвержденному Приказом Минфина РФ от 30.03.01 N 26н, относятся к объектам основных средств.

Первичные документов по учету основных средств оформляются по формам ОС-1, ОС-2, ОС-3, ОС-4а, ОС-6, ОС-6а (б), утвержденным Постановлением Госкомстата РФ от 21.01.03 N 7 «Об утверждении унифицированных форм первичной учетной документации по учету основных средств». Указанные формы распространяются на юридические лица всех форм собственности (за исключением кредитных организаций и бюджетных учреждений).

Принятие автотранспорта к учету оформляется актом приема-передачи объекта основных средств составленным по форме N ОС-1. Одновременно с этим, организация-продавец оформляет покупателю счет-фактуру на реализуемое автотранспортное средство.

Для учета наличия автотранспорта, а также для учета его перемещения между структурными подразделениями организации в бухгалтерии ведутся: на каждый объект автотранспорта — по форме N ОС-6, на группу объектов — по форме N ОС-6а, для объектов основных средств малых предприятий — по форме N ОС-6б. Записи при приеме-передаче производятся на основании актов о приеме-передаче (форма N ОС-1) и сопроводительных документов.

Прием, перемещение автотранспорта внутри организации, включая проведение реконструкции, модернизации, капитального ремонта, а также их выбытие или списание отражаются в инвентарной карточке (книге) на основании соответствующих документов, в том числе:

— формы N ОС-2, применяемой для оформления и учета перемещения автотранспорта внутри организации из одного структурного подразделения (цеха, отдела, участка и др.) в другой;

— формы N ОС-3, применяемой для оформления и учета приема-сдачи автотранспорта из ремонта, реконструкции, модернизации, которая подписывается членами приемочной комиссии или лицом, уполномоченным на приемку, а также представителем организации (структурного подразделения), проводившей ремонт, реконструкцию, модернизацию;

— формы N ОС-4а, применяемой для оформления и учета списания пришедших в негодность автотранспортных средств, которая подписывается членами комиссии, назначенной руководителем организации, утверждаются руководителем или уполномоченным им лицом, и передается в бухгалтерию вместе с документом, подтверждающий снятие его с учета в Госавтоинспекции.

При списании у владельцев автотранспорта снова возникает вопрос о том, что следует делать раньше: списывать транспортное средство или снимать его с учета в Госавтоинспекции?

Несмотря на то, что в акте о списании автотранспортного средства реквизит «дата снятия с учета в ГИБДД (ГАИ)» предусмотрен, но нормативными документами конкретный срок для проведения этой процедуры в случае утилизации не установлен. Законодательства о бухгалтерском учете и о налогах и сборах также не содержат запрета на списание автотранспорта, который еще не снят с учета в ГИБДД. Предварительно снимать транспорт с учета нужно лишь перед заключением договоров, которые предполагают переход права собственности, например купли-продажи, мены.

В том случае, если автотранспортное средство находится в угоне, то организация, на балансе которой находится это автотранспортное средство, обязана в соответствии с действующим законодательством провести инвентаризацию имущества и списать убыток на виновных лиц. Если виновные лица не установлены или суд отказал во взыскании убытков с них, то убытки от хищения автотранспорта списываются на финансовые результаты организации.

**Содержание работы:**

**Задание 1**

С помощью сети Интернет создайте таблицу в MS Word и заполните ее

|  |  |
| --- | --- |
| **Понятие о дистанционном обучении** | |
| Дистанционное образование – |  |
| Дистанционное обучение – |  |
| Система ДО – |  |
| Информационно-образовательная среда ДО – |  |
| Педагогические технологии ДО — |  |
| Кейс-технологии – |  |
| ТВ-технология — |  |
| Сетевая технология – |  |
| Учебно-методическое обеспечение ДО – |  |
| Система средств обучения в ДО – |  |
| Основные причины активно развивающихся дистанционных технологий в России |  |
|  |
|  |
|  |
|  |
|  |
| Признаки дистанционной системы обучения |  |
|  |
|  |
|  |
|  |
|  |
| Средства и методы дистанционного обучения |  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

**Задание 2**

**Сделайте вывод о проделанной работе**

**Практическая работа 8.**

**Тема:** Обеспечение сбора данных для анализа использования и функционирования программно- технических средств компьютерных сетей

**Цель занятия:** Получить навыки использования стандартных сетевых утилит ОС Windows.

Постоянный контроль за работой локальной сети, составляющей основу любой корпоративной сети, необходим для поддержания ее в работоспособном состоянии.

Контроль – это необходимый первый этап, который должен выполняться при управлении сетью. Ввиду важности этой функции ее часто отделяют от других функций систем управления и реализуют специальными средствами.

Такое разделение функций контроля и собственно управления полезно для небольших и средних сетей, для которых установка интегрированной системы управления экономически нецелесообразна. Использование автономных средств контроля помогает администратору сети выявить проблемные участки и устройства сети, а их отключение или реконфигурацию он может выполнять в этом случае вручную.

Процесс контроля работы сети обычно делят на два этапа – мониторинг и анализ.

На этапе **мониторинга** выполняется более простая процедура – процедура сбора первичных данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов и т.п.

Далее выполняется этап **анализа**, под которым понимается более сложный и интеллектуальный процесс осмысления собранной на этапе мониторинга информации, сопоставления ее с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадежной работы сети.

Задачи мониторинга решаются программными и аппаратными измерителями, тестерами, сетевыми анализаторами, встроенными средствами мониторинга коммуникационных устройств, а также агентами систем управления.

Задача анализа требует более активного участия человека и использования таких сложных средств, как экспертные системы, аккумулирующие практический опыт многих сетевых специалистов.

Все многообразие средств, применяемых для анализа и диагностики вычислительных сетей, можно разделить на несколько крупных классов.

**Агенты систем управления,**поддерживающие функции одной из стандартных MIB и поставляющие информацию по протоколу SNMP или CMIP. Для получения данных от агентов обычно требуется наличие системы управления, собирающей данные от агентов в автоматическом режиме.

**Встроенные системы диагностики и управления** (Embedded systems)

Эти системы выполняются в виде программно-аппаратных модулей, устанавливаемых в коммуникационное оборудование, а также в виде программных модулей, встроенных в операционные системы. Они выполняют функции диагностики и управления только одним устройством, и в этом их основное отличие от централизованных систем управления. Примером средств этого класса может служить модуль управления многосегментным повторителем Ethernet, реализующий функции автосегментации портов при обнаружении неисправностей, приписывания портов внутренним сегментам повторителя и некоторые другие. Как правило, встроенные модули управления “по совместительству” выполняют роль SNMP-агентов, поставляющих данные о состоянии устройства для систем управления.

**Анализаторы протоколов** (Protocol analyzers)

Представляют собой программные или аппаратно-программные системы, которые ограничиваются в отличие от систем управления лишь функциями мониторинга и анализа трафика в сетях. Хороший анализатор протоколов может захватывать и декодировать пакеты большого количества протоколов, применяемых в сетях, – обычно несколько десятков. Анализаторы протоколов позволяют установить некоторые логические условия для захвата отдельных пакетов и выполняют полное декодирование захваченных пакетов, т.е. показывают в удобной для специалиста форме вложенность пакетов протоколов разных уровней друг в друга с расшифровкой содержания отдельных полей каждого пакета.

**Экспертные системы**

Этот вид систем аккумулирует знания технических специалистов о выявлении причин аномальной работы сетей и возможных способах приведения сети в работоспособное состояние. Экспертные системы часто реализуются в виде отдельных подсистем различных средств мониторинга и анализа сетей: систем управления сетями, анализаторов протоколов, сетевых анализаторов. Простейшим вариантом экспертной системы является контекстно-зависимая система помощи. Более сложные экспертные системы представляют собой т.н. базы знаний, обладающие элементами искусственного интеллекта. Примерами таких систем являются экспертные системы, встроенные в систему управления Spectrum компании Cabletron и анализатора протоколов Sniffer компании Network General. Работа экспертных систем состоит в анализе большого числа событий для выдачи пользователю краткого диагноза о причине неисправности сети.

**Оборудование для диагностики и сертификации кабельных систем**

Условно это оборудование можно поделить на четыре основные группы: сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.

* **Сетевые мониторы**(называемые также сетевыми анализаторами) предназначены для тестирования кабелей различных категорий. Сетевые мониторы собирают также данные о статистических показателях трафика – средней интенсивности общего трафика сети, средней интенсивности потока пакетов с определенным типом ошибки и т.п. Эти устройства являются наиболее интеллектуальными устройствами из всех четырех групп устройств данного класса, т.к. работают не только на физическом, но и на канальном, а иногда и на сетевом уровнях.
* **Устройства для сертификации кабельных систем**выполняют сертификацию в соответствии с требованиями одного из международных стандартов на кабельные системы.
* **Кабельные сканеры**используются для диагностики медных кабельных систем.
* **Тестеры**предназначены для проверки кабелей на отсутствие физического разрыва.
* **Многофункциональные портативные устройства анализа и диагностики**. В связи с развитием технологии больших интегральных схем появилась возможность производства портативных приборов, которые совмещали бы функции нескольких устройств: кабельных сканеров, сетевых мониторов и анализаторов протоколов.

**Анализаторы протоколов**

Анализатор протоколов представляет собой либо специализированное устройство, либо персональный компьютер, обычно переносной, класса Notebook, оснащенный специальной сетевой картой и соответствующим программным обеспечением. Применяемые сетевая карта и программное обеспечение должны соответствовать технологии сети (Ethernet, Token Ring, FDDI, Fast Ethernet). Анализатор подключается к сети точно так же, как и обычный узел. Отличие состоит в том, что анализатор может принимать все пакеты данных, передаваемые по сети, в то время как обычная станция – только адресованные ей. Для этого сетевой адаптер анализатора протоколов переводится в режим “беспорядочного” захвата – promiscuous mode.

Программное обеспечение анализатора состоит из ядра, поддерживающего работу сетевого адаптера и программного обеспечения, декодирующего протокол канального уровня, с которым работает сетевой адаптер, а также наиболее распространенные протоколы верхних уровней, например IP, TCP, ftp, telnet, HTTP, IPX, NCP, NetBEUI, DECnet и т.п. В состав некоторых анализаторов может входить также экспертная система, которая позволяет выдавать пользователю рекомендации о том, какие эксперименты следует проводить в данной ситуации, что могут означать те или иные результаты измерений, как устранить некоторые виды неисправности сети.

Анализаторы протоколов имеют некоторые общие свойства.

* Возможность (кроме захвата пакетов) измерения среднестатистических показателей трафика в сегменте локальной сети, в котором установлен сетевой адаптер анализатора. Обычно измеряется коэффициент использования сегмента, матрицы перекрестного трафика узлов, количество хороших и плохих кадров, прошедших через сегмент.
* Возможность работы с несколькими агентами, поставляющими захваченные пакеты из разных сегментов локальной сети. Эти агенты чаще всего взаимодействуют с анализатором протоколов по собственному протоколу прикладного уровня, отличному от SNMP или CMIP.
* Наличие развитого графического интерфейса, позволяющего представить результаты декодирования пакетов с разной степенью детализации.
* Фильтрация захватываемых и отображаемых пакетов. Условия фильтрации задаются в зависимости от значения адресов назначения и источника, типа протокола или значения определенных полей пакета. Пакет либо игнорируется, либо записывается в буфер захвата. Использование фильтров значительно ускоряет и упрощает анализ, т.к. исключает захват или просмотр ненужных в данный момент пакетов.
* Использование триггеров. Триггеры в данном случае – это задаваемые администратором некоторые условия начала и прекращения процесса захвата данных из сети. Такими условиями могут быть: время суток, продолжительность процесса захвата, появление определенных значений в кадрах данных. Триггеры могут использоваться совместно с фильтрами, позволяя более детально и тонко проводить анализ, а также продуктивнее расходовать ограниченный объем буфера захвата.
* Многоканальность. Некоторые анализаторы протоколов позволяют проводить одновременную запись пакетов от нескольких сетевых адаптеров, что удобно для сопоставления процессов, происходящих в разных сегментах сети.

Возможности анализа проблем сети на физическом уровне у анализаторов протоколов минимальные, поскольку всю информацию они получают от стандартных сетевых адаптеров. Поэтому они передают и обобщают информацию физического уровня, которую сообщает им сетевой адаптер, а она во многом зависит от типа сетевого адаптера. Некоторые сетевые адаптеры сообщают более детальные данные об ошибках кадров и интенсивности коллизий в сегменте, а некоторые вообще не передают такую информацию верхним уровням протоколов, на которых работает анализатор протоколов.

**Сетевые анализаторы**

Сетевые анализаторы представляют собой эталонные измерительные приборы для диагностики и сертификации кабелей и кабельных систем. Они могут с высокой точностью измерить все электрические параметры кабельных систем, а также работают на более высоких уровнях стека протоколов. Сетевые анализаторы генерируют синусоидальные сигналы в широком диапазоне частот, что позволяет измерять на приемной паре амплитудно-частотную характеристику и перекрестные наводки, затухание и суммарное затухание. Сетевой анализатор представляет собой лабораторный прибор больших размеров, достаточно сложный в обращении.

**Кабельные сканеры и тестеры**

Основное назначение кабельных сканеров – измерение электрических и механических параметров кабелей: длины кабеля, параметра NEXT, затухания, импеданса, схемы разводки пар проводников, уровня электрических шумов в кабеле. Точность измерений, произведенный этими устройствами, ниже, чем у сетевых анализаторов, но вполне достаточна для оценки соответствия кабеля стандарту.

Для определения местоположения неисправности кабельной системы (обрыва, короткого замыкания, неправильно установленного разъема и т.д.) используется метод “отраженного импульса” (Time Domain Reflectometry, TDR). Суть этого метода состоит в том, что сканер излучает в кабель короткий электрический импульс и измеряет время задержки до прихода отраженного сигнала. По полярности отраженного импульса определяется характер повреждения кабеля (короткое замыкание или обрыв). В правильно установленном и подключенном кабеле отраженный импульс почти отсутствует.

Точность измерения расстояния зависит от того, насколько точно известна скорость распространения электромагнитных волн в кабеле.

Кабельные сканеры – это портативные приборы, которые обслуживающий персонал может постоянно носить с собой.

Кабельные тестеры – наиболее простые и дешевые приборы для диагностики кабеля. Они позволяют определить непрерывность кабеля, однако, в отличие от кабельных сканеров, не дают ответа на вопрос о том, в каком месте произошел сбой.

**Многофункциональные портативные приборы мониторинга**

В последнее время начали выпускаться многофункциональные портативные приборы, которые объединяют в себе возможности кабельных сканеров, анализаторов протоколов и даже некоторые функции систем управления, сохраняя в то же время такое важное свойство, как портативность. Многофункциональные приборы мониторинга имеют специализированный физический интерфейс, позволяющий выявлять проблемы и тестировать кабели на физическом уровне, который дополняется микропроцессором с программным обеспечением для выполнения высокоуровневых функций.

**Функции проверки аппаратуры и кабелей**

многофункциональные приборы сочетают наиболее часто используемые на практике функции кабельных сканеров с рядом новых возможностей тестирования.  
**● Сканирование**[***кабеля***](http://teacherbox.ru/kompseti/pm01/lessonpm01/provodkisks/.html)Функция позволяет измерять длину кабеля, расстояние до самого серьезного дефекта и распределение импеданса по длине кабеля. При проверке неэкранированной витой пары могут быть выявлены следующие ошибки: расщепленная пара, обрывы, короткое замыкан е и другие виды нарушения соединения. Для сетей Ethernet на коаксиальном кабеле эти проверки могут быть осуществлены на работающей сети.

* **Функция определения распределения кабельных жил**Осуществляет проверку правильности подсоединения жил, наличие промежуточных разрывов и перемычек на витых парах. На дисплей выводится перечень связанных между собой контактных групп.
* **Функция определения карты кабелей**

Используется для составления карты основных кабелей и кабелей, ответвляющихся от центрального помещения.

* **Автоматическая проверка кабеля**

В зависимости от конфигурации возможно определить длину, импеданс, схему подключения жил, затухание и параметр NEXT на частоте до 100 МГц. Автоматическая проверка выполняется для коаксиальных кабелей, экранированной витой пары с импедансом 150 Ом, неэкранированной витой пары с сопротивлением 100 ОМ.  
**● Целостность цепи при проверке постоянным током**

Эта функция используется при проверке коаксиальных кабелей для верификации правильности используемых терминаторов и их установки.  
**● Определение номинальной скорости распространения**

Функция вычисляет номинальную скорость распространения (Nominal Velocity of Propagation, NVP) по кабелю известной длины и дополнительно сохраняет полученные результаты в файле для определяемого пользователем типа кабеля (User Defined Cable Type) или стандартного кабеля.  
**● Комплексная автоматическая проверка пары “сетевой адаптер-концентратор”**Этот комплексный тест позволяет последовательно подключить прибор между конечным узлом сети и концентратором. Тест дает возможность автоматически определить местонахождение источника неисправности – кабель, концентратор, сетевой адаптер или программное обеспечение станции.  
**● Автоматическая проверка сетевых адаптеров**

Проверяет правильность функционирования вновь установленных или “подозрительных” сетевых адаптеров. Для сетей Ethernet по итогам проверки сообщаются: MAC-адрес, уровень напряжения сигналов (а также присутствие и полярность импульсов Link Test для 10Base-T). Если сигнал не обнаружен на сетевом адаптере, то тест автоматически сканирует соединительный разъем и кабель для их диагностики.

**Функции сбора статистики**

Эти функции позволяют в реальном масштабе времени проследить за изменением наиболее важных параметров, характеризующих “здоровье” сегментов сети. Статистика обычно собирается с разной степенью детализации по разным группам.  
**● Сетевая статистика**  
В этой группе собраны наиболее важные статистические показатели – коэффициент использования сегмента (utilization), уровень коллизий, уровень ошибок и уровень широковещательного трафика. Превышение этими показателями определенных порогов в первую очередь говорят о проблемах в том сегменте сети, к которому подключен многофункциональный прибор.  
**● Статистика ошибочных кадров**

Эта функция позволяет отслеживать все типы ошибочных кадров для определенной технологии. Например, для технологии Ethernet характерны следующие типы ошибочных кадров.

* Укороченные кадры (Short Frames).Это кадры, имеющие длину, меньше допустимой, т.е. меньше 64 байт. Иногда этот тип кадров дифференцируют на два класса – просто короткие кадры (short), у которых имеется корректная контрольная сумма, и “коротышки” (runts), не имеющие корректной контрольной суммы. Наиболее вероятными причинами появления укороченных кадров являются неисправные сетевые адаптеры и их драйверы.  
  Удлиненные кадры (Jabbers). Это кадры, имеющие длину, превышающую допустимое значение в 1518 байт с хорошей или плохой контрольной суммой. Удлиненные кадры являются следствием затянувшейся передачи, которая появляется из-за неисправностей сетевых адаптеров.
* Кадры нормальных размеров, но с плохой контрольной суммой (Bad FCS) и кадры с ошибками выравнивания по границе байта. Кадры с неверной контрольной суммой являются следствием множества причин – плохих адаптеров, помех на кабелях, плохих контактов, некорректно работающих портов повторителей, мостов, коммутаторов и маршрутизаторов. Ошибка выравнивания всегда сопровождается ошибкой по контрольной сумме, поэтому некоторые средства анализа трафика не делают между ними различий. Ошибка выравнивания может быть следствием прекращения передачи кадра при распознавании коллизии передающим адаптером.  
  Кадры-призраки (ghosts) являются результатом электромагнитных наводок на кабеле. Они воспринимаются сетевыми адаптерами как кадры, не имеющие нормального признака начала кадра – 10101011. Кадры-призраки имеют длину более 72 байт, в противном случае они классифицируются как удаленные коллизии. Количество обнаруженных кадров-призраков в большой степени зависит от точки подключения сетевого анализатора. Причинами их возникновения являются петли заземления и другие проблемы с кабельной системой.

Знание процентного распределения общего количества ошибочных кадров по их типам может многое подсказать администратору о возможных причинах неполадок в сети. Даже небольшой процент ошибочных кадров может привести к значительному снижению полезной пропускной способности сети, если протоколы, восстанавливающие искаженные кадры, работают с большими тайм-аутами ожидания квитанций. Считается, что в нормально работающей сети процент ошибочных кадров не должен превышать 0,01% , т.е. не более 1 ошибочного кадра из 10000.

**● Статистика по**[***коллизиям***](http://teacherbox.ru/kompseti/pm01/lessonpm01/nettopolog/.html)Эта группа характеристик дает информацию о количестве и видах коллизий, отмеченных на сегменте сети, позволяет определить наличие и местонахождение проблемы. Анализаторы протоколов обычно не могут дать дифференцированной картины распределения общего числа коллизий по их отдельным типам, в то же время знание преобладающего типа коллизий может помочь понять причину плохой работы сети. Ниже приведены основные типы коллизий сети Ethernet.

* Локальная коллизия (Local Collision). Является результатом одновременной передачи двух или более узлов, принадлежащих к тому сегменту, в котором производятся измерения. Если многофункциональный прибор не генерирует кадры, то в сети на витой паре или волоконно-оптическом кабеле локальные коллизии не фиксируются. Слишком высокий уровень локальных коллизий является следствием проблем с кабельной системой.
* Удаленная коллизия (Remote Collision). Эти коллизии происходят на другой стороне повторителя (по отношению к тому сегменту, в котором установлен измерительный прибор). В сетях, построенных на многопортовых повторителях (10Base-T, 10Base-FL/FB, 100Base-TX/FX/T4, Gigabit Ethernet), все измеряемые коллизии являются удаленными (кроме тех случаев, когда анализатор сам генерирует кадры и может быть виновником коллизии). Не все анализаторы протоколов и средства мониторинга одинаковым образом фиксируют удаленные коллизии. Это происходит из-за того, что некоторые измерительные средства и системы не фиксируют коллизии, происходящие при передаче преамбулы.
* Поздняя коллизия (Late Collision). Это коллизия, которая происходит после передачи первых 64 байт кадра (по протоколу Ethernetколлизия должна обнаруживаться при передаче первых 64 бай кадра). Результатом поздней коллизии будет кадр, который имеет длину более 64 байт и содержит неверное значение контрольной суммы. Чаще всего это указывает на то, что сетевой адаптер, являющийся источником конфликта, оказывается не в состоянии правильно прослушивать линию и поэтому не может вовремя остановить передачу. Другой причиной поздней коллизии является слишком большая длина кабельной системы или слишком большое количество промежуточных повторителей, приводящее к превышению максимального значения времени двойного оборота сигнала.Средняя интенсивность коллизий в нормально работающей сети должна быть меньше 5%. Большие всплески (более 20%) могут быть индикатором кабельных проблем.
* **Распределение используемых сетевых протоколов**Эта статистическая группа относится к протоколам сетевого уровня. На дисплее отображается список основных протоколов в убывающем порядке относительно процентного соотношения кадров, содержащих пакеты данного протокола к общему числу кадров в сети.

**● Основные отправители (Top** **Sendes)**Функция позволяет отслеживать наиболее активные передающие узлы локальной сети. Прибор можно настроить на фильтрацию по единственному адресу и выявить список основных отправителей кадров для данной станции. Данные отражаются на дисплее в виде диаграммы вместе с перечнем основных отправителей кадров.

**● Основные получатели (Top** **Receivers)**Функция позволяет следить за наиболее активными узлами-получателями сети. Информация отображается в виде, аналогичном приведенному выше.

**● Основные генераторы широковещательного трафика (Top** **Broadcasters)**Функция выявляет станции сети, которые больше остальных генерируют кадры с широковещательными и групповыми адресами.

**● Генерирование трафика (Traffic** **Generation)**Прибор может генерировать трафик для проверки работы сети при повышенной нагрузке. Трафик может генерироваться параллельно с активизированными функциями Сетевая статистика, Статистика ошибочных кадрови Статистика по коллизиям.

Пользователь может задать параметры генерируемого трафика, такие как интенсивность и размер кадров. Для тестирования мостов и маршрутизаторов прибор может автоматически создавать заголовки IP- и IPX-пакетов, и все что требуется от оператора – это внести адреса источника и назначения.

В ходе испытаний пользователь может увеличить на ходу размер и частоту следования кадров с помощью клавиш управления курсором. Это особенно ценно при поиске источника проблем производительности сети и условий возникновения отказов.

**Функции анализа**[**протокол**](http://teacherbox.ru/kompseti/pm02/lesson2/protokolyimarshrutizatsii/.html)**ов**

Обычно портативные многофункциональные приборы поддерживают декодирование и анализ только основных протоколов локальных сетей, таких как протоколы стековTCP/IP, Novell NetWare, NetBIOS и Banyan VINES.

В некоторых многофункциональных приборах отсутствует возможность декодирования захваченных пакетов, как в анализаторах протоколов, а вместо этого собирается статистика о наиболее важных пакетах, свидетельствующих о наличии проблем в сетях. Например, при анализе протоколов стека TCP/IP собирается статистика по пакетам протокола ICMP, с помощью которого маршрутизаторы сообщают конечным узлам о возникновении разного рода ошибок. Для ручной проверки достижимости узлов сети в приборы включается поддержка утилиты IP Ping, а также аналогичных по назначению утилит NetWare Ping и NetBIOS Ping.

**Мониторинг локальных сетей на основе коммутаторов**

**Наблюдение за трафиком**

Так как перегрузки процессоров портов и других обрабатывающих элементов коммутатора могут приводить к потерям кадров, то функция наблюдения за распределением трафика в сети, построенной на основе коммутаторов, очень важна.

Однако если сам коммутатор не снабжен встроенным агентом SNMP для каждого своего порта, то задача слежения за трафиком, традиционно решаемая в сетях с разделяемыми средами с помощью установки в сеть внешнего анализатора протоколов, очень усложняется.

Обычно в традиционных сетях анализатор протоколов или многофункциональный прибор подключался к свободному порту концентратора, что позволяло ему наблюдать за всем трафиком, передаваемым между любыми узлами сети.

Если же анализатор протокола подключить к свободному порту коммутатора, то он не зафиксирует почти ничего, т.к. кадры ему передавать никто не будет, а чужие кадры в его порт также направляться не будут. Единственный вид трафика, который будет фиксировать анализатор, – это трафик широковещательных пакетов, которые будут передаваться всем узлам сети, а также трафик кадров с неизвестными коммутатору адресами назначения. В случае когда сеть разделена на виртуальные сети, анализатор протоколов будет фиксировать только широковещательный трафик своей виртуальной сети, чтобы анализаторами протоколов можно было по-прежнему пользоваться и в коммутируемых сетях, производители коммутаторов снабжают свои устройства функцией зеркального отображения трафика любого порта на специальный порт. К специальному порту подключается анализатор протоколов, а затем на коммутатор подается команда через его модульSNMP-управления для отображения трафика какого-либо порта на специальный порт.

Наличие функции зеркализации портов частично снимает проблему, но оставляет некоторые вопросы. Например, как просматривать одновременно трафик двух портов или трафик порта, работающего в полнодуплексном режиме.

Более надежным способом слежения за трафиком, проходящим через порты коммутатора, является замена анализатора протокола на агенты RMON MIB для каждого порта коммутатора.

Агент RMON выполняет все функции хорошего анализатора протокола для протоколов Ethernet и Token Ring, собирая детальную информацию об интенсивности трафика, различных типах плохих кадров, о потерянных кадрах, причем самостоятельно строя временные ряды для каждого фиксируемого параметра. Кроме того, агент RMON может самостоятельно строить матрицы перекрестного трафика между узлами сети, которые очень нужны для анализа эффективности применения коммутатора.

Так как агент RMON, реализующий все 9 групп объектов Ethernet, стоит весьма дорого, то производители для снижения стоимости коммутатора часто реализуют только первые несколько групп объектов RMON MIB. Другим приемом снижения стоимости коммутатора является использование одного агента RMON для нескольких портов. Такой агент по очереди подключается к нужному порту, позволяя снять с него требуемые статистические данные.

**Управление виртуальными сетями**

Виртуальные локальные сети VLAN порождают проблемы для традиционных систем управления на платформе SNMP как при их создании, так и при наблюдении за их работой.

Как правило, для создания виртуальных сетей требуется специальное программное обеспечение компании-производителя, которое работает на платформе системы управления, например, HP Open View. Сами платформы систем управления этот процесс поддержать не могут в основном из-за долгого отсутствия стандарта на виртуальные сети. Можно надеяться, что появление стандарта 802.1Q изменит ситуацию в этой области.

Наблюдение за работой виртуальных сетей также создает проблемы для традиционных систем управления. При создании карты сети, включающей виртуальные сети, необходимо отображать как физическую структуру сети, так и ее логическую структуру, соответствующую связям отдельных узлов виртуальной сети. При этом по желанию администратора система управления должна уметь отображать соответствие логических и физических связей в сети, т.е. на одном физическом канале должны отображаться все или отдельные пути виртуальных сетей.

К сожалению, многие системы управления либо вообще не отображают виртуальные сети, либо делают это очень неудобным для пользователя способом, что вынуждает обращаться к менеджерам компаний-производителей для решения этой задачи.

# Контрольныевопросы

1. Какой протокол необходим для работы с утилитой ***ping***? Найти описание и характеристики протокола.
2. Можно ли утилитой ***tracert*** задать максимальное число ретрансляций?
3. Какой результат выдаст утилита ***netstat*** с параметрами ***-a-s-r?*** Поясните полученный результат.
4. Что такое localhost? Найти самостоятельно любую стандартную сетевую утилиту Windows.

**Практическая работа №9**

**Взаимодействие со специалистами смежного профиля при создании информационной системы**

**Цель:** *определить состав и функции персонала информационной системы на этапах ее создания.*

**Задачи:**

*Дать определение информационной системе;*

*Выделить типы информационных систем;*

*Разобрать основные этапы создания информационной системы;*

*Определить состав и функции персонала ИС;*

*Описать уровни представлений об информации в информационных системах.*

1. **Информационная система**

***Система****(system – целое, составленное из частей; греч.) – это совокупность элементов,  взаимодействующих друг с другом, образующих определенную целостность, единство.*

***Структура системы****– состав, порядок и принципы взаимодействия элементов системы, определяющие основные свойства системы*. Если отдельные элементы системы разнесены по разным уровням и характеризуются внутренними связями, то говорят об иерархической структуре системы.

Добавление к понятию система слова информационная отражает цель ее создания и функционирования. *Информационные системы обеспечивают сбор, хранение, обработку, поиск, выдачу информации, необходимой в процессе принятия решений задач из любой области.* Они помогают анализировать проблемы и создавать новые информационные продукты.

***Информационная система****— это взаимосвязанная совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации в интересах достижения поставленной цели.*  
Современное понимание информационной системы предполагает использование в качестве основного технического средства переработки информации компьютера. Кроме того, тех­ническое воплощение информационной системы само по себе ничего не будет значить, если не учтена роль человека, для которого предназначена производимая информация и без кото­рого невозможно ее получение и представление.

Необходимо понимать разницу между компьютерами и информационными система­ми. *Компьютеры, оснащенные специализированными программными средствами, являются технической базой и инструментом для информационных систем. Информационная система немыслима без персонала, взаимодействующего с компьютерами и телекоммуникациями.*

1. **Типы информационных систем**

*Тип информационной системы зависит от того, чьи интересы она обслуживает и на каком уровне управления. По характеру представления и логической организации хранимой информации информационные системы подразделяются на фактографические, документальные и геоинформационные.*

***Фактографические информационные системы****накапливают и хранят данные в виде множества экземпляров одного или нескольких типов структурных элементов (информационных объектов).* Каждый из таких экземпляров или некоторая их совокупность отражают сведения по какому-либо факту, событию отдельно от всех прочих сведений и фактов.

*Структура каждого типа информационного объекта состоит из конечного набора реквизитов, отражающих основные аспекты и характеристики объектов данной предметной области.* Комплектование информационной базы в фактографических информационных системах включает, как правило, обязательный процесс  структуризации входной информации.  
*Фактографические информационные системы предполагают удовлетворение информационных потребностей непосредственно, т.е. путем представления потребителям самих сведений (данных, фактов, концепций).*

***В******документальных (документированных)информационных системах****единичным элементом информации является нерасчлененный на более мелкие элементы документ и информация при вводе (входной документ), как правило, не структурируется, или структурируется в ограниченном виде.* Для вводимого документа могут устанавливаться некоторые формализованные позиции (дата изготовления, исполнитель, тематика).

*Некоторые виды документальных информационных систем обеспечивают установление логической взаимосвязи вводимых документов – соподчиненность по смысловому содержанию, взаимные отсылки по каким-либо критериям и т.д.*Определение и установление такой взаимосвязи представляет собой сложную многокритериальную и многоаспектную аналитическую задачу, которая не может быть формализована в полной мере.

***В геоинформационных системах****данные организованы в виде отдельных информационных объектов (с определенным набором реквизитов), привязанных к общей электронной топографической основе (электронной карте). Геоинформационные системы применяются для информационного обеспечения в тех предметных областях, структура информационных объектов и процессов в которых имеет пространственно-географический компонент (маршруты транспорта, коммунальное хозяйство).*

**3.Основные этапы создания информационной системы**

Создание информационной системы начинается с момента первых переговоров Заказчика и потенциального Исполнителя и может никогда не закончиться, поскольку хорошие и полезные системы постоянно совершенствуются и развиваются.

**Предварительный этап**

*На данном этапе необходимо осознать основные цели и задачи будущего проекта.* Для этого ключевые представители Заказчика и Исполнителя организуют встречи, на которых обсуждают концепцию информационной системы, ключевые технические моменты, сроки и объемы выполняемых работ, а также стоимость и источники финансирования. *Итогом предварительного этапа, помимо согласованных условий будущего договора, должен стать первый и самый фундаментальный проектный документ –****устав проекта****.*

*Устав проекта определяет следующие принципиальные моменты, связанные с процессом разработки и внедрения информационной системы:*

* Краткое описание проекта, цели и задачи создания информационной системы.
* Общее описание состава работ.
* Границы проекта: сроки, бюджет, перечень объектов автоматизации.
* Описание продукта: перечень поставляемого аппаратного и программного обеспечения, тип и количество лицензий и т.д.
* Организационная структура проекта: список и роли участников проектной группы со стороны Исполнителя и Заказчика, их ответственность и обязанности, система документооборота проекта.
* Основные этапы разработки и внедрения информационной системы, укрупненный план-график их реализации.
* Наиболее значимые риски невыполнения обязательств по проекту, а также способы минимизации рисков.

Другими словами, *устав проекта – это именно устав, который разрабатывается руководителем проекта совместно с основными участниками проектной группы, утверждается руководством Исполнителя и Заказчика и не должен корректироваться в течение всего времени создания информационной системы.*

Завершением предварительного этапа можно считать момент, когда подписан договор на услуги по разработке и внедрению информационной системы и утвержден устав проекта.

**Сбор требований**

К этому моменту все ключевые фигуры – участники проекта определены, и ничто не мешает начать собирать и утверждать требования к будущей информационной системе. Представители исполнителя общаются с будущими пользователями и администраторами системы, а также с их руководством. В ходе обследования не только систематизируются требования и пожелания к внедряемому решению, но и анализируется документация, которая должна стать источником исходных данных системы, или формирование которой должно быть в результате автоматизировано.

*Результатом данного этапа должно стать появление****технического задания****на разработку и внедрение информационной системы. Техническое задание должно базироваться на условиях договора и требованиях, изложенных в уставе проекта и содержать следующие разделы (для России структура технического задания регламентируется ГОСТ 34.602 89):*

* Назначение и цели создания системы.
* Описание объекта автоматизации и основных автоматизируемых бизнес-процессов.
* Требования к системе: требования к структуре; функциям (задачам), решаемым системой; требования к техническому и организационному обеспечению; требования к надежности, безопасности и т.д. и т.п.
* Состав и содержание работ по созданию информационной системы.
* Порядок контроля и приемки результатов работ.
* Требования к составу работ по подготовке объекта автоматизации для запуска информационной системы в эксплуатацию.
* Требования к составу проектной и пользовательской документации.

*Завершение этапа сбора требований – это утверждение Заказчиком Технического задания.* В некоторых случаях у Заказчика до начала работ по проекту уже существует техническое задание (входит в состав конкурсной документации). В этом случае результаты обследования и сбора требований фиксируются в частных технических заданиях, детализирующих и конкретизирующих общие требования к информационной системе, представленные в исходном техническом задании.

**Проектирование**

На этом этапе усилиями Исполнителя детально проектируются все сценарии, связанные с разработкой и внедрением информационной системы на территории Заказчика. Делается это в соответствии с условиями информационной среды (системного ландшафта) Заказчика и требованиями к интеграции создаваемой системы с уже имеющимися и эксплуатируемыми Заказчиком прочими программными продуктами. *Результатом этапа проектирования должно стать оформление следующих разделов****технического (концептуального) проекта****:*

* Архитектура информационной системы.
* Описание структур информационного хранилища (базы данных).
* Проектные решения, представленные детальным описанием сценариев автоматизации всех, затрагиваемых внедрением системы бизнес процессов.
* Сценарии интеграции разрабатываемой информационной системы с внешними программными продуктами.
* Источники исходных данных и варианты первоначального информационного наполнения системы.
* Концепция разграничения прав доступа к данным на основе ролей пользователей, определяющих, в том числе, их полномочия.
* Концепция обучения пользователей информационной системы.

**Реализация**

*Этап реализации всех требований к информационной системе, изложенных в Техническом задании и Техническом проекте.* В этот период Исполнитель разрабатывает все необходимые программные компоненты, создает структуры базы данных, производит установку, настройку и тестирование всех компонентов информационной системы на своей территории, имитирует сценарии интеграции и т.д. и т.п. *Завершение этапа реализации подтверждается появлением таких проектных документов, как руководство по установке и настройке системы,****программа и методика испытаний****системы, а также шаблон базы данных и реестр всех выполненных программных разработок.*

**Подготовка информационной системы к эксплуатации**

Все работы данного этапа уже проводятся на территории Заказчика и включают в себя установку и настройку всех компонентов системы в информационной среде Заказчика, проведение предварительного тестирования, разработку пользовательской документации, обучение пользователей, загрузку исходных данных, проведение [испытаний системы](http://itconcord.ru/articles/testing/) в соответствии с программой и методикой испытаний и прочие подготовительные работы.

*К моменту окончания всех подготовительных работ должен быть разработан и утвержден регламент эксплуатации системы. Регламент, в частности, должен определять пользователей и их роли в системе, в соответствии с их должностными обязанностями.*

**Опытно-промышленная эксплуатация**

*Последний этап в рамках разработки и первоначального внедрения информационной системы, задачей которого является успешное проведение опытной эксплуатации системы в течение определенного времени, а целью – подтвердить, что созданная информационная система – это ровно тот результат, который и ожидал Заказчик.*

В этот период пользователи начинают эксплуатировать систему в соответствии с разработанным на предыдущем этапе регламентом. В ходе опытно-промышленной эксплуатации фиксируются ошибки и согласовываются необходимые доработки. Исполнитель устраняет ошибки, выполняет доработки и при условии, что система начинает функционировать в соответствии со всеми, предъявленными к ней ранее требованиями, в конце установленного периода получает протокол об успешном завершении опытно-промышленной эксплуатации.

С завершением опытно-промышленной эксплуатации, как правило, завершается действие договора на создание информационной системы. Сама система переходит в режим промышленной эксплуатации, а Исполнитель, если в этом заинтересован Заказчик, заключает отдельный договор на ее сопровождение, на период установленного условиями договора срока.

**Сопровождение и развитие системы**

Промышленная эксплуатация может выявить то, что некоторые требования к созданной информационной системе содержали неточности и требуют иной формулировки или дополнений, а сама система требует доработки. Не каждый Заказчик имеет в своем штате персонал, который способен самостоятельно внести в работу системы все, диктуемые реальной обстановкой изменения, поэтому заключает с Исполнителем отдельный договор на сопровождение информационной системы.

Пользователи информационной системы начинают общаться с представителями службы поддержки Заказчика, которые принимают от них заявки на доработку функционала и устранение дефектов, передают заявки в работу и периодически оповещают пользователей о статусе их запроса. Перечень возможных доработок и регламент обработки заявок определяется условиями договора. Если появляется потребность в работах, которые не укладываются в суть договора на сопровождение, то Заказчик и Исполнитель составляют отдельный договор на данный вид работ, который уже можно отнести к работам по модернизации и развитию эксплуатируемой информационной системы.

1. **Состав и функции персонала ИС - информационных систем:**

***Аналитики***- это специалисты, которые строит математическую модель предметной области, исходя из информационных потребностей конечных пользователей; ставит задачи для прикладных программистов. На практике персонал небольших ИС часто состоит из одного - двух специалистов, которые выполняют все перечисленные функции.

***Администратор***- это специалист (или группа специалистов), который понимает потребности конечных пользователей, работает с ними в тесном контакте и отвечает за определение, загрузку, защиту и эффективность работы банка данных. Он должен координировать процесс сбора информации, проектирования и эксплуатации БД, учитывать текущие и перспективные потребности пользователей.

***Системные программисты***- это специалисты, которые занимаются разработкой и сопровождением базового математического обеспечения ЭВМ (ОС, СУБД, трансляторов, сервисных программ общего назначения).

***Прикладные программисты***- это специалисты, которые разрабатывают программы для реализации запросов к БД.

|  |  |
| --- | --- |
| Для разных классов пользователей можно выделить несколько уровней представлений об информации в ИС, которые обусловлены потребностями различных групп пользователей и уровнем развития инструментальных средств создания ИС. Классификация по уровням позволяет разделить работу по созданию и обслуживанию ИС на относительно независимые части. |  |



1. **Уровни представлений об информации в информационных системах**

* **Внешнее представление**данных - это описание информационных потребностей конечного пользователя и прикладного программиста. Связь между этими двумя видами внешнего представления осуществляет аналитик;
* **Концептуальное представление**данных - отображение знаний обо всей предметной области ИС. Это наиболее полное представление, отражающее смысл информации, оно может быть только одно и не должно содержать противоречий и двусмысленностей. Концептуальное представление - это сумма всех внешних представлений, которое учитывает перспективы развития ИС, знания о методах обработки информации, знания о структуре самой ИС и др. Существует две формы концептуального представления информации:
  + *инфологическая*(информационно-логическая) модель, которая не привязана к конкретной реализации и ориентирована на пользователя;
  + *даталогическая*модель, которая учитывает требования конкретной СУБД.
* **Внутреннее** (физическое) представление - это организация данных на физическом носителе информации. Этот уровень характеризует представления системных программистов и практически используется только тогда, когда СУБД не обеспечивает требуемого быстродействия или специфического режима обработки данных.

Методы разработки ИС: при традиционном подходе сначала выявлялись информационные потоки на предприятии, а затем к этой структуре привязывалась ИС, повторяя и закрепляя тем самым недостатки организации бизнеса. Таким образом, современная ИС должна создаваться как часть предприятия, включающая бизнес-архитектуру, персонал и ИТ.

**Практическая работа № 10**

**Установка, настройка, эксплуатация и обслуживание технических и программно-аппаратных средств компьютерных сетей**

**Цель работы:** ознакомиться с установкой, настройкой, эксплуатацией и обслуживанием технических и программно-аппаратных средств компьютерных сетей

Оборудование: учебный персональный компьютер.

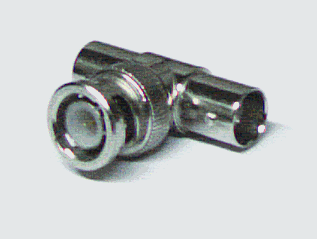
Программное обеспечение: операционная система, презентация.

**Теоретические основы**

Ознакомиться с презентацией "[Аппаратные средства и оборудование ЛВС](http://khpi-iip.mipk.kharkiv.edu/library/net/prezent/aparat_net.ppt)".   
Рассмотреть следующие аппаратные средства и оборудование ЛВС:   
1. Виды кабелей для сетей ( коаксиальный , неэкранированная витая пара, оптоволокно).   
2. Устройства соединения BNC, RJ -45, настенные и модульные розетки, терминаторы.   
3. Элементы ЛВС: монтажные короба, патч-панели , патч-корды , абонентские шнуры. Разделение кабеля UTP по стандартам TIA / EIA -568 A / B .   
4. Варианты исполнения активных концентраторов ( хабы , комутаторы , MAU).

**Коаксиальные кабели**

В начале развития локальных сетей коаксиальный кабель как среда передачи был наиболее распространен. Он использовался и используется преимущественно в сетях Ethernet и отчасти ARCnet . Различают "толстый" и "тонкий" кабели.   
" Толстый Ethernet ", как правило, используется следующим образом. Он прокладывается по периметру помещения или здания, и на его концах устанавливаются 50-омные терминаторы. Из-за своей толщины и жесткости кабель не может подключаться непосредственно к сетевой плате. Поэтому на кабель в нужных местах устанавливаются "вампиры" - специальные устройства, прокалывающие оболочку кабеля и подсоединяющиеся к его оплетке и центральной жиле. "Вампир" настолько прочно сидит на кабеле, что после установки его невозможно снять без специального инструмента. К "вампиру", в свою очередь, подключается трансивер - устройство, согласовывающее сетевую плату и кабель. И, наконец, к трансиверу подключается гибкий кабель с 15-контактными разъемами на обоих концах - вторым концом он подсоединяется к разъему AUI ( attachment unit interface ) на сетевой плате.   
Все эти сложности были оправданы только одним - допустимая максимальная длина "толстого" коаксиального кабеля составляет 500 метров . Соответственно одним таким кабелем можно обслужить гораздо большую площадь, чем "тонким" кабелем, максимально допустимая длина которого составляет, как известно, 185 метров . При наличии некоторого воображения можно представить себе, что "толстый" коаксиальный кабель - это распределенный в пространстве Ethernet-концентратор, только полностью пассивный и не требующий питания. Других преимуществ у него нет, недостатков же хоть отбавляй - прежде всего высокая стоимость самого кабеля (порядка 2,5 долл. за метр), необходимость использования специальных устройств для монтажа (25-30 долл. за штуку), неудобство прокладки и т.п. Это постепенно привело к тому, что "толстый Ethernet " медленно, но верно сошел со сцены, и в настоящее время мало где применяется.   
"Тонкий Ethernet " распространен значительно шире, чем его "толстый" собрат. Принцип использования у него тот же, но благодаря гибкости кабеля он может присоединяться непосредственно к сетевой плате. Для подключения кабеля используются разъемы BNC ( bayonet nut connector ), устанавливаемые собственно на кабель, и T-коннекторы , служащие для отвода сигнала от кабеля в сетевую плату. Разъемы типа BNC бывают обжимные и разборные (пример разборного разъема - отечественный разъем СР-50-74Ф).

  
Т-коннектор   
Для монтажа разъема на кабель вам потребуется либо специальный инструмент для обжимки, либо паяльник и плоскогубцы.   
Кабель необходимо подготовить следующим образом:

1. Аккуратно отрежьте так, чтобы его торец был ровным. Наденьте на кабель металлическую муфту (отрезок трубки), который поставляется в комплекте с BNC-разъемом.   
2. Снимите с кабеля внешнюю пластиковую оболочку на длину примерно 20 мм .

Будьте аккуратны, чтобы не повредить по возможности ни один проводник оплетки.   
3. Оплетку аккуратно расплетите и разведите в стороны. Снимите изоляцию с центрального проводника на длину примерно 5 мм .

4. Установите центральный проводник в штырек, который также поставляется в комплекте с разъемом BNC. Используя специальный инструмент, надежно обожмите штырек, фиксируя в нем проводник, либо впаяйте проводник в штырек. При пайке будьте особенно аккуратны и внимательны - плохая пайка через некоторое время станет причиной отказов в работе сети, причем локализовать это место будет достаточно трудно.

5. Вставьте центральный проводник с установленным на него штырьком в тело разъема до щелчка. Щелчок означает, что штырек сел на свое место в разъеме и зафиксировался там.   
6. Равномерно распределите проводники оплетки по поверхности разъема, если необходимо, обрежьте их до нужной длины. Надвиньте на разъем металлическую муфту.   
7. Специальным инструментом (или плоскогубцами) аккуратно обожмите муфту до обеспечения надежного контакта оплетки с разъемом. Не обжимайте слишком сильно - можно повредить разъем или пережать изоляцию центрального проводника. Последнее может привести к неустойчивой работе всей сети. Но и обжимать слишком слабо тоже нельзя - плохой контакт оплетки кабеля с разъемом также приведет к отказам в работе.

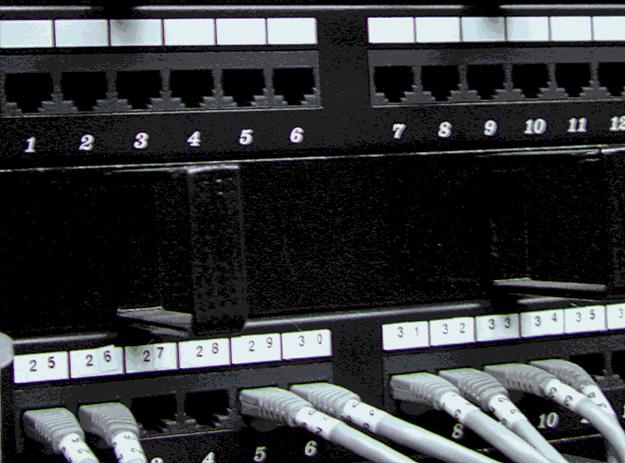
Отмечу, что отечественный разъем СР-50 монтируется примерно так же, за исключением того, что оплетка в нем заделывается в специальную разрезную втулку и закрепляется гайкой. В некоторых случаях это может оказаться даже удобнее.

**Кабели на основе витой пары**

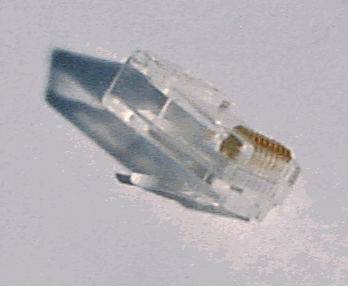
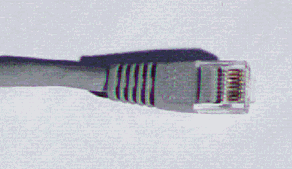
Витая пара (UTP/STP, unshielded / shielded twisted pair ) в настоящее время является наиболее распространенной средой передачи сигналов в локальных сетях. Кабели UTP/STP используются в сетях Ethernet , Token Ring и ARCnet . Они различаются по категориям (в зависимости от полосы пропускания) и типу проводников (гибкие или одножильные) . В кабеле 5-й категории, как правило, находится восемь проводников, перевитых попарно (то есть четыре пары).   
  
Кабель UTP   
Структурированная кабельная система, построенная на основе витой пары 5-й категории, имеет очень большую гибкость в использовании. Ее идея заключается в следующем.   
На каждое рабочее место устанавливается не менее двух (рекомендуется три) четырехпарных розеток RJ-45. Каждая из них отдельным кабелем 5-й категории соединяется с кроссом или патч-панелью , установленной в специальном помещении, - серверной. В это помещение заводятся кабели со всех рабочих мест, а также городские телефонные вводы, выделенные линии для подключения к глобальным сетям и т.п. В помещении, естественно, монтируются серверы, а также офисная АТС, системы сигнализации и прочее коммуникационное оборудование.   
Благодаря тому что кабели со всех рабочих мест сведены на общую панель, любую розетку можно использовать как для подключения рабочего места к ЛВС, так и для телефонии или вообще чего угодно. Допустим, две розетки на рабочем месте были подключены к компьютеру и принтеру, а третья - к телефонной станции. В процессе работы появилась необходимость убрать принтер с рабочего места и установить вместо него второй телефон. Нет ничего проще - патч-корд соответствующей розетки отключается от концентратора и переключается на телефонный кросс, что займет у администратора сети никак не больше нескольких минут.   
  
Розетка на 2 порта

Патч-панель , или панель соединений, представляет собой группу розеток RJ-45, смонтированных на пластине шириной 19 дюймов . Это стандартный размер для универсальных коммуникационных шкафов - рэков ( rack ), в которых устанавливается оборудование (концентраторы, серверы, источники бесперебойного питания и т.п.). На обратной стороне панели смонтированы соединители, в которые монтируются кабели.

Кросс в отличие от патч-панели розеток не имеет. Вместо них он несет на себе специальные соединительные модули. В данном случае его преимущество перед патч-панелью в том, что при его использовании в телефонии вводы можно соединять между собой не специальными патч-кордами , а обычными проводами. Кроме того, кросс можно монтировать прямо на стену - наличия коммуникационного шкафа он не требует. В самом деле, нет смысла приобретать дорогостоящий коммуникационный шкаф, если вся ваша сеть состоит из одного-двух десятков компьютеров и сервера.

Кабели с многожильными гибкими проводниками используются в качестве патч-кордов , то есть соединительных кабелей между розеткой и сетевой платой, либо между розетками на панели соединений или кроссе. Кабели с одножильными проводниками - для прокладки собственно кабельной системы. Монтаж разъемов и розеток на эти кабели совершенно идентичен, но обычно кабели с одножильными проводниками монтируются на розетки рабочих мест пользователей, панели соединений и кроссы, а разъемы устанавливают на гибкие соединительные кабели.   
  
Патч-панель   
Как правило, применяются следующие виды разъемов:   
S110 - общее название разъемов для подключения кабеля к универсальному кроссу " 110" или коммутации между вводами на кроссе;

RJ-11 и RJ-12 - разъемы с шестью контактами. Первые обычно применяются в телефонии общего назначения - вы можете встретить такой разъем на шнурах импортных телефонных аппаратов. Второй обычно используется в телефонных аппаратах, предназначенных для работы с офисными мини-АТС, а также для подключения кабеля к сетевым платам ARCnet ;

RJ-45 - восьмиконтактный разъем, использующийся обычно для подключения кабеля к сетевым платам Ethernet либо для коммутации на панели соединений.   
  
Разъем RJ-45   
В зависимости от того, что с чем нужно коммутировать, применяются различные патч-корды : "45- 45" (с каждой стороны по разъему RJ-45), "110- 45" (с одной стороны S110, с другой - RJ-45) или "110- 110" .

Для монтажа разъемов RJ-11, RJ-12 и RJ-45 используются специальные обжимочные приспособления, различающиеся между собой количеством ножей (6 или 8) и размерами гнезда для фиксации разъема. В качестве примера рассмотрим монтаж кабеля 5-й категории на разъем RJ-45.

1. Аккуратно обрежьте конец кабеля. Торец кабеля должен быть ровным.   
2. Используя специальный инструмент, снимите с кабеля внешнюю изоляцию на длину примерно 30 мм и обрежьте нить, вмонтированную в кабель (нить предназначена для удобства снятия изоляции с кабеля на большую длину). Любые повреждения (надрезы) изоляции проводников абсолютно недопустимы - именно поэтому желательно использовать специальный инструмент, лезвие резака которого выступает ровно на толщину внешней изоляции.

* 1. Аккуратно разведите, расплетите и выровняйте проводники. Выровняйте их в один ряд, при этом соблюдая цветовую маркировку. Существует два наиболее распространенных стандарта по разводке цветов по парам: T568A ( рекомендуемый компанией Siemon ) и T568B (рекомендуемый компанией AT&T и фактически наиболее часто применяемый).

  
На разъеме RJ-45 цвета проводников располагаются так:

  
Проводники должны располагаться строго в один ряд, без нахлестов друг на друга. Удерживая их одной рукой, другой ровно обрежьте проводники так, чтобы они выступали над внешней обмоткой на 8- 10 мм .

4. Держа разъем защелкой вниз, вставьте в него кабель. Каждый проводник должен попасть на свое место в разъеме и упереться в ограничитель. Прежде чем обжимать разъем, убедитесь, что вы не ошиблись в разводке проводников. При неправильной разводке помимо отсутствия соответствия номерам контактов на концах кабеля, легко выявляемого с помощью простейшего тестера, возможна более неприятная вещь - появление "разбитых пар" ( splitted pairs ).

Для выявления этого брака обычного тестера недостаточно, так как электрический контакт между соответствующими контактами на концах кабеля обеспечивается и с виду все как будто бы нормально. Но такой кабель никогда не сможет обеспечить нормальное качество соединения даже в 10-мегабитной сети на расстояние более 40- 50 метров . Поэтому нужно быть внимательным и не торопиться, особенно если у вас нет достаточного опыта.

5. Вставьте разъем в гнездо на обжимочном приспособлении и обожмите его до упора-ограничителя на приспособлении. В результате фиксатор на разъеме встанет на свое место, удерживая кабель в разъеме неподвижным . Контактные ножи разъема врежутся каждый в свой проводник, обеспечивая надежный контакт.   
Аналогичным образом можно осуществить монтаж разъемов RJ-11 и RJ-12, используя соответствующий инструмент.

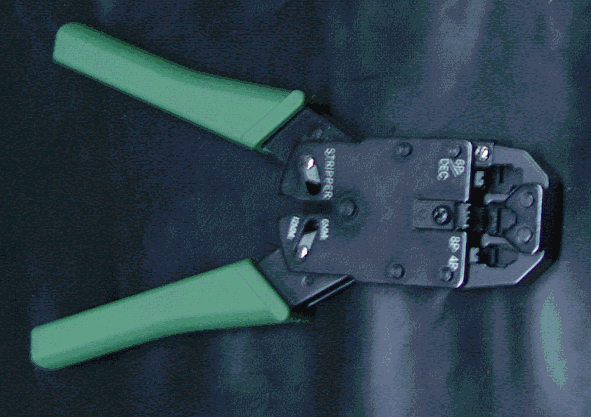
Для монтажа разъема S110 специального обжимочного инструмента не требуется. Сам разъем поставляется в разобранном виде. Кстати, в отличие от "одноразовых" разъемов типа RJ разъем S110 допускает многократную разборку и сборку, что очень удобно. Последовательность действий при монтаже следующая:   
1. Снимите внешнюю изоляцию кабеля на длину примерно 40 мм , разведите в стороны пары проводников, не расплетая их.   
2. Закрепите кабель (в той половинке разъема, на которой нет контактной группы) с помощью пластмассовой стяжки и отрежьте получившийся "хвост".   
3. Аккуратно уложите каждый проводник в органайзер на разъеме. Не расплетайте пару на большую, чем требуется, длину - это ухудшит характеристики всего кабельного соединения. Последовательность укладки пар обычная - синяя-оранжевая-зеленая-коричневая; при этом светлый провод каждой пары укладывается первым.

4. Острым инструментом ( бокорезами или ножом) обрежьте каждый проводник по краю разъема.

5. Установите на место вторую половинку разъема и руками обожмите ее до защелкивания всех фиксаторов. При этом ножи контактной группы врежутся в проводники, обеспечивая контакт.

**Оптоволоконный кабель**

Оптоволоконные кабели - наиболее перспективная и обеспечивающая наибольшее быстродействие среда распространения сигналов для локальных сетей и телефонии. В локальных сетях оптоволоконные кабели используются для работы по протоколам ATM и FDDI.

  
Приспособление для снятия изоляции и обжимки разъема   
Оптоволокно, как понятно из его названия, передает сигналы при помощи импульсов светового излучения. В качестве источников света используются полупроводниковые лазеры, а также светодиоды. Оптоволокно подразделяется на одно- и многомодовое .

Одномодовое волокно очень тонкое, его диаметр составляет порядка 10 микрон. Благодаря этому световой импульс, проходя по волокну, реже отражается от его внутренней поверхности, что обеспечивает меньшее затухание. Соответственно одномодовое волокно обеспечивает большую дальность без применения повторителей. Теоретическая пропускная способность одномодового волокна составляет 10 Гбит/с. Его основные недостатки - высокая стоимость и высокая сложность монтажа. Одномодовое волокно применяется в основном в телефонии.   
Многомодовое волокно имеет больший диаметр - 50 или 62,5 микрона. Этот тип оптоволокна чаще всего применяется в компьютерных сетях. Большее затухание во многомодовом волокне объясняется более высокой дисперсией света в нем, из-за которой его пропускная способность существенно ниже - теоретически она составляет 2,5 Гбит/с.

Для соединения оптического кабеля с активным оборудованием применяются специальные разъемы. Наиболее распространены разъемы типа SC и ST.   
Монтаж соединителей на оптоволоконный кабель - очень ответственная операция, требующая опыта и специального обучения, поэтому не стоит заниматься этим в домашних условиях, не будучи специалистом. Если уж вам " приспичило " строить сеть с использованием оптоволокна, легче приобрести кабели с соединителями. Впрочем, учитывая стоимость кабеля, соединителей, а также активного оборудования для оптики, можно предположить, что в домашних и небольших ЛВС это оборудование будет использоваться еще нескоро.

**Порядок выполнения работы**

Рассмотреть следующие аппаратные средства и оборудование ЛВС:   
1. Исполнение сетевых адаптеров Ethernet и Token Ring для шин ISA, PCI, MCA.   
2. Виды кабелей для сетей ( коаксиальный , неэкранированная витая пара, оптоволокно).   
3. Устройства соединения BNC, RJ -45, настенные и модульные розетки, терминаторы.   
4. Элементы ЛВС: монтажные короба, патч-панели , патч-корды , абонентские шнуры. Разделение кабеля UTP по стандартам TIA / EIA -568 A / B .   
5. Варианты исполнения активных концентраторов ( хабы , комутаторы , MAU).   
6. Протестировать сетевой адаптер с помощью утилит настройки.

**Содержание отчета.**

 Отчет должен содержать:

* цель работы;
* индивидуальное задание;
* описание выполнения индивидуального задания;
* ответы на контрольные вопросы;
* выводы.

**Контрольные вопросы**

1. Дать определение компьютерной сети и ее назначения.
2. По какому принципу строится архитектура сетей?
3. Как классифицируются компьютерные сети по территориальному признаку?
4. Какие существуют разновидности корпоративных сетей.
5. Дайте определение понятиям "клиент", "сервер".
6. Какие задачи решаются рабочими станциями, а какие сервером?
7. Перечислите топологии компьютерных сетей. Назовите достоинства и недостатки.

**Практическая работа №11**

**Проведение профилактических работ на объектах сетевой инфраструктуры и рабочих станциях**

**Обслуживание сетей**- перечень работ направленных на обеспечение безотказной работы сетевой инфраструктуры компании.

* Анализ текущего состояния сети
* Профилактические работы
* Устранения неисправностей в сети
* Подбор и установка сетевого оборудования
* Прокладка новых сетевых и телефонных линий
* Проектирование сетевой инфраструктуры

Рекомендуются следующие методы технического обслуживания объектов ТЭ:

**профилактическое ТО**, выполняемое через определенные интервалы времени или в соответствии с заранее установленными критериями и направленное на своевременное предупреждение возможности появления отказа или ухудшения функционирования объектов;

**корректирующее ТО**, выполняемое после обнаружения состояния неработоспособности объектов и направленное на его восстановление в состояние, когда параметры качества объектов находятся в пределах установленных допусков;

**управляемое ТО,**выполняемое путем систематического применения методов анализа состояния объектов и направленное на минимизацию работ по профилактическому и корректирующему ТО

Проверка физических компонентов

Проверка документации и требований

Проверка списка совместимого оборудования

**Процедуры по обслуживанию ИС**

Цель: обеспечить целостность и доступность информационных сервисов.

Существует великое множество обязательных для исполнения ежедневных операций. Например, проверка правильности функционирования электронной почты и телеконференций, просмотр регистрационных файлов на предмет наличия ранних признаков неисправностей, контроль за подключением локальных сетей и за наличием системных ресурсов. Рассмотрим некоторые из них.

**Ведение журналов регистрации событий**

Операторы компьютеров должны вести журнал регистрации всех выполняемых заданий. Этот журнал должен по необходимости включать:

* время запуска и останова систем;
* подтверждение корректного оперирования с файлами данных и выходной информацией от компьютеров.

В журнал регистрации следует заносить зафиксированные пользователями сбои, касающиеся проблем с компьютерными и коммуникационными системами.

В связи с появлением проблемы ( как сбойной ситуации) выделяют несколько областей:

***Определение проблемы*.**- Выявляется проблема и выполняются шаги, необходимые для начала диагностики проблемы. Назначение этой области - изолировать проблему в конкретной подсистеме, например, в каком-нибудь аппаратном устройстве, программном изделии, компоненте микрокода или сегменте носителя.

***Диагноз проблемы.***- Определяется точная причина проблемы и воздействие, необходимое для решения этой проблемы.

***Обход проблемы и восстановление.***- Осуществляются попытки обойти проблему либо частично, либо полностью. Обычно эта операция является временной.

***Решение проблемы.***- Включает усилия, необходимые для устранения проблемы, которые должны быть занесены в график; например, это может быть замена отказавшего дисковода.

***Отслеживание и управление проблемой.****-* Отслеживается проблема до ее полного решения. В частности, если для решения проблемы необходимо внешнее воздействие, то жизненно важная информация, описывающая эту проблему (такая, как информация контролирования состояния и отчеты о состоянии проблемы), включается в запись управления проблемой, которая вводится в базу данных этой проблемы.

**Слежение за окружающей средой**

Для определения условий, которые могут неблагоприятно сказаться на работе компьютерного оборудования и для принятия корректирующих мер, необходимо постоянно следить за окружающей средой, в том числе за влажностью, температурой и качеством источников электропитания.

**Практическая работа№ 11**

**Установка, настройка, эксплуатация и обслуживание сетевых конфигураций**

Часть 1. Определение емкости устройства хранения данных

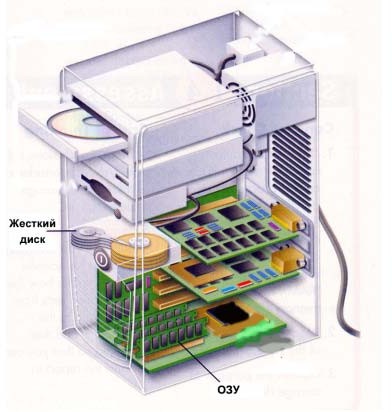


Рис. 1. Основные компоненты компьютерной системы внутри системного блока.

Задачи

* Определить объем установленного в ПК ОЗУ (в МБ).
* Определить размер установленного в ПК жесткого диска (в ГБ).
* Определить используемое и доступное пространство на жестком диске (в ГБ).
* Проверить другие типы устройств хранения (дискеты, компакт-диски, DVD-диски).

Исходные данные / подготовка

Устройства хранения многих компонентов ПК измеряется в мегабайтах (МБ) - 2 в 20-ой степени байт и гигабайтах (ГБ) - 2 в 30-ой степени байт. Эти значения несколько больше, чем 1 миллион байт и 1 миллиард байт, соответственно. К таким компонентам относятся ОЗУ, жесткие диски и оптические носители, такие как компакт-диски и DVD-диски. В данной работе требуется определить емкость и доступное пространство для различных компонентов компьютера.

Необходимо использовать следующие ресурсы:

* компьютер с установленной ОС Windows XP.

Шаг 1. Идентификация ОЗУ компьютера

а. В ОС Windows XP существуют два способа просмотра панели управления: классический вид и вид по категориям. Эти возможности доступны в зависимости от того, какой из двух видов используется. Если слева видна опция «Переключение к виду по категориям», то в настоящее время используется классический вид. Если отображается опция «Переключение к классическому виду», то в настоящее время используется вид по категориям. На этом шаге необходимо переключиться к классическому виду.

б. В меню «Пуск» выберите пункт «Панель управления». В окне «Панель управления» выберите значок «Система», чтобы открыть диалоговое окно «Свойства системы». Другой способ: эту информацию можно получить, нажав кнопку «Пуск» и правой кнопкой щелкнув значок «Мой компьютер». Затем в раскрывающемся меню выберите пункт «Свойства».

Информация об операционной системе и пакете обновлений компьютера указана в верхней части данного диалогового окна. Тип процессора, тактовая частота и объем памяти компьютера указаны в нижней части.

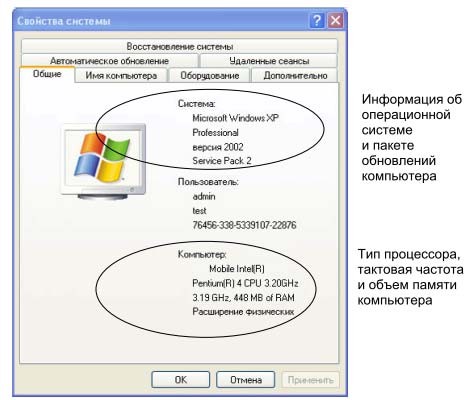


Рис. 2. Информация о характеристиках процессора, оперативной памяти и версии ОС.

в. В данном примере процессор компьютера – Pentium 4 с тактовой частотой 3,2 гигагерц (ГГц). Тактовая частота соответствует числу циклов тактового генератора в секунду, синхронизирующего работу процессора. Число циклов влияет на количество выполняемых процессором за секунду команд. Более высокая тактовая частота означает, что процессор способен выполнять больше инструкций за секунду.

На данном компьютере для ЦП доступно 448 МБ ОЗУ.

г. Проверьте свой компьютер и определите объем ОЗУ, доступного ЦП. Укажите объем ОЗУ вашего компьютера.

Шаг 2. Определение объема жесткого диска \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

а. Дважды щелкните значок «Мой компьютер» на рабочем столе компьютера. Если значка «Мой компьютер» нет, нажмите кнопку «Пуск» и выберите пункт «Мой компьютер».

б. Правой кнопкой мыши щелкните значок локального жесткого диска в разделе «Жесткие диски» (обычно это диск C) и выберите пункт «Свойства». В результате откроется диалоговое окно «Свойства: Локальный диск (С:)». Общая емкость жесткого диска отображается над значком «Диск C».

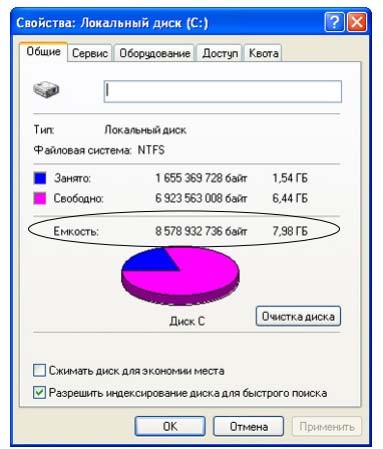


Рис. 3. Объем жесткого диска.

в. Определите объем жесткого диска своего компьютера. Укажите общий объем жесткого диска в ГБ.

г. Оставьте диалоговое окно «Свойства: Локальный диск (С:)» для выполнения следующего шага.

Шаг 3. Определение свободного и используемого пространства на жестком диске а. В диалоговом окне «Свойства: Локальный диск (С:)» используемое и свободное пространство указывается в байтах и ГБ над разделом «Емкость».

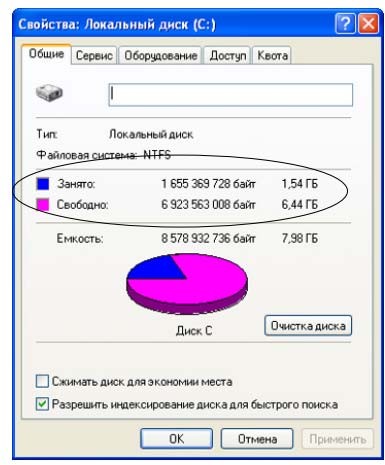


Рис. 4. Распределение занятого и свободного пространства на жестком диске.

б. Какой объем жесткого диска в ГБ используется?

в. Какой объем свободного пространства на жестком диске в ГБ?

Шаг 4. Проверка других устройств хранения

а. Правой кнопкой мыши щелкните кнопку «Пуск» и выберите пункт «Проводник». В левой панели выберите ветку «Мой компьютер».

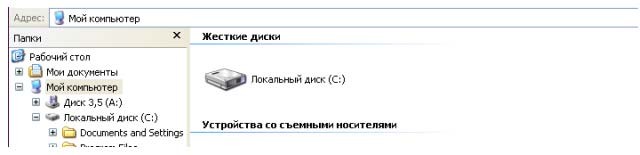


Рис. 5. Логические жесткие диски в ОС Windows.

б. Сколько букв дисков отображается в открывшемся окне?

в. Правой кнопкой мыши щелкните значок другого диска, не C:, и выберите пункт «Свойства».

Откроется диалоговое окно «Свойства: Съемный диск».

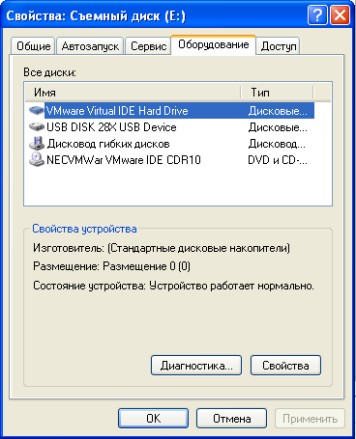
г. Перейдите на вкладку «Оборудование», на которой представлена информация о каждом устройстве и его состоянии работоспособности.

Рис. 6. Связь между логическими дисками и физическими устройствами.

Шаг 5. Вопросы для обсуждения

а. Почему важно знать объем ОЗУ компьютера?

б. Почему важно знать объем жесткого диска, а также объем используемого пространства?

Часть 2. Определение разрешения экрана компьютера

Задачи

* Определить текущее разрешение экрана монитора ПК.
* Определить максимальное разрешение для самого высокого качества цветопередачи.
* Вычислить число пикселей, необходимых для настройки разрешения.
* Определить тип монитора и установленной графической платы.

Исходные данные / подготовка

Разрешение монитора определяет качество изображения на экране монитора. Разрешение определяется числом горизонтальных и вертикальных элементов изображения (пикселей), которые используются для формирования изображения на экране монитора. Обычно число пикселей предопределяется производителем графических плат и мониторов ПК. Самое больше число пикселей, поддерживаемое монитором и графической платой, называется максимальным разрешением. Пример максимального разрешения – 1280 x1024, которое означает, что экран состоит из 1280 горизонтальных пикселей и 1024 вертикальных пикселей. Чем более высокое разрешение задано, тем четче отображается на экране изображение. Максимальное разрешение монитора ПК и число цветов, которое может отобразить монитор, определяется двумя факторами:

* возможностями монитора;
* возможностями графической платы, особенно объемом встроенной памяти.

Необходимо использовать следующие ресурсы:

* компьютер с установленной ОС Windows XP.

Шаг 1. Определение текущего разрешения экрана

а. Чтобы узнать текущее разрешение экрана и настройки качества цветопередачи, правой кнопкой мыши щелкните в пустом месте рабочего стола и выберите в контекстном меню пункт

«Свойства». В окне «Свойства: Экран» перейдите на вкладку «Параметры».

Окно «Свойства: Экран» также можно открыть из панели управления, щелкнув значок «Экран».

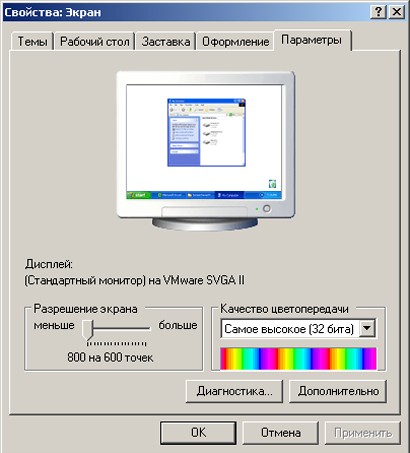


Рис. 7. Настройка разрешения экрана.

б. Запишите текущие параметры ПК, представленные на вкладке «Параметры» окна «Свойства:

Экран»

Разрешение экрана (Г x В) Разрешение по горизонтали: Разрешение по вертикали: Значение качества цветопередачи:

Шаг 2. Определение максимального разрешения для самого высокого качества цветопередачи Ползунок в разделе «Разрешение экрана» используется для настройки требуемого разрешения.

а. Подвигайте ползунок, чтобы просмотреть диапазон разрешений экрана, доступных на данном ПК. (Данный диапазон определяется операционной системой, если та распознает графическую плату и монитор.)

б. На основе текущих параметров ПК, представленных на вкладке «Параметры» окна

«Свойства: Экран», заполните следующую таблицу.

Минимальное разрешение экранаМаксимальное разрешение экранаДоступные значения параметра качества цветопередачи

Шаг 3. Вычисление числа пикселей для настроек текущего и максимального разрешений

Экран монитора состоит из рядов пикселей. Число пикселей в каждом ряду – это разрешение по горизонтали. Число рядов – это разрешение по вертикали. Чтобы определить общее число пикселей при некотором разрешении экрана, разрешение по горизонтали умножается на разрешение по вертикали. Например, если текущее разрешение – 1280 x 1024, то общее число пикселей равно 1280 умножить на 1024, или 1 310 720.

а. Вычислите общее число пикселей при минимальном разрешении.

б. Вычислите общее число пикселей при максимальном разрешении.

Шаг 4. Определение типа установленной графической платы

Подробную информацию о графической плате (также называется адаптером дисплея) можно получить в окне «Свойства: Экран».

а. В окне «Свойства: Экран» нажмите кнопку «Дополнительно».

б. Перейдите на вкладку «Адаптер».

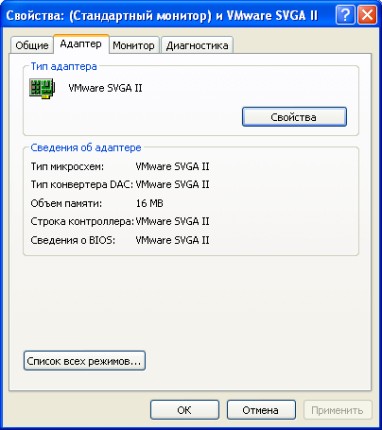


Рис. 8. Характеристики адаптера видеокарты.

в. На основе информации, представленной на вкладке «Адаптер», заполните следующую таблицу.

|  |  |
| --- | --- |
| Производитель и модель графической платы (тип адаптера) |  |
| Объем графической памяти на плате (объем памяти) |  |

Шаг 5. Определение типа монитора и доступных частот обновления

Подробную информацию о мониторе можно получить в окне «Свойства: Экран». Частота обновления экрана определяет, сколько раз за секунду экран облучается или перерисовывается. Частота обновления 60 герц означает, что экран облучается 60 раз в секунду. Более высокие частоты обновления снижают мерцание экрана, что уменьшает напряжение глаз, однако может негативно повлиять на монитор. Следует устанавливать максимальную частоту обновления, которую монитор может безопасно поддерживать.

а. Перейдите на вкладку «Монитор», чтобы узнать тип монитора и текущую частоту обновления.

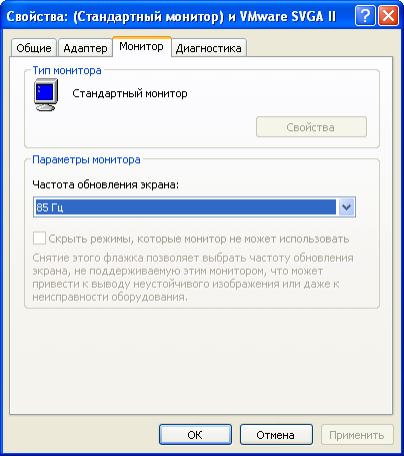


Рис. 9. Настройка частоты обновления экрана.

Б Что может случиться, если выбрать частоту обновления выше той, которую монитор может безопасно поддерживать?

**Практическая работа №12**

**Участие в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнение восстановления и резервного копирования информации**

Часть 1 Соединение двух персональных компьютеров без промежуточных устройств.



Рис. 1. Прямое соединение двух компьютеров сетевым кабелем.

Задачи

* Построить простую одноранговую сеть и проверить физическое подключение.
* Назначить узлам разные IP-адреса и пронаблюдать за их влиянием на сетевое взаимодействие.

Исходные данные / подготовка

В первой части лабораторной работы требуется построить простую одноранговую сеть с помощью двух компьютеров и перекрестного кабеля Ethernet. Потребуется назначать узлам различные совместимые и несовместимые IP-адреса и отслеживать их влияние на возможность взаимодействия.

Для проведение работы потребуются следующие ресурсы:

* два ПК с Windows XP Professional, на каждом из которых установлена и функционирует сетевая интерфейсная плата;
* перекрестный кабель Ethernet для соединения ПК (предоставляется преподавателем);

Шаг 1. Соединение ПК для создания одноранговой сети

а. Возьмите у преподавателя перекрестный кабель Ethernet для соединения двух ПК.

б. Вставьте один конец кабеля в сетевую плату Ethernet компьютера PC1. Другой конец кабеля вставьте в сетевую плату Ethernet компьютера PC2. При подключении конца кабеля должен быть слышен щелчок, указывающий на то, что кабель вставлен в порт правильно.

Шаг 2. Проверка физического соединения

а. После подключения перекрестного кабеля Ethernet к обоим ПК, внимательно осмотрите каждый порт Ethernet. Световая индикация канала (обычно зеленого или желтого цвета) означает, что между двумя сетевыми платами установлено физическое соединение. Попробуйте отключить кабель от одного из ПК, а затем снова подключить, чтобы проверить, как световая индикация отключается и снова включается.

б. Перейдите в «Панель управления», дважды щелкните значок «Сетевые подключения» и убедитесь, что подключение по локальной сети установлено. На рисунке 2 показан пример активного подключения по локальной сети. При наличии неполадок физического подключения

на значке «Подключение по локальной сети» виден знак X и сообщение: «Сетевой кабель не подключен».

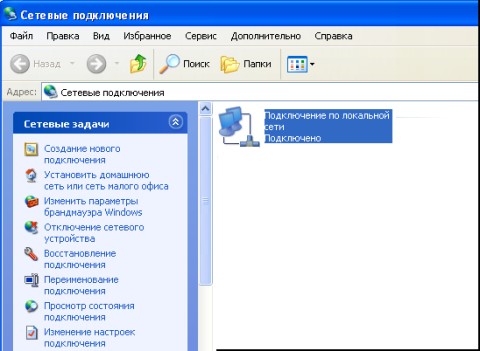


Рис. 2 Состояние сетевого подключения.

в. Если в значке «Подключение по локальной сети» не указывается, что соединение установлено, устраните неполадки, повторив шаги 1 и 2. Можно также попросить преподавателя подтвердить, что используется перекрестный кабель Ethernet.

Шаг 3. Настройка параметров IP для двух ПК

а. Настройте логические IP-адреса двух ПК, чтобы они могли связываться по протоколу TCP/IP. На компьютере PC1 перейдите в панель управления, дважды щелкните значок «Сетевые подключения» и правой кнопкой мыши щелкните значок установленного подключения по локальной сети. В раскрывающемся меню выберите пункт «Свойства».

б. С помощью полосы прокрутки в окне «Подключение по локальной сети – свойства», прокрутите список до элемента «Протокол Интернета (TCP/IP)». Нажмите кнопку «Свойства».

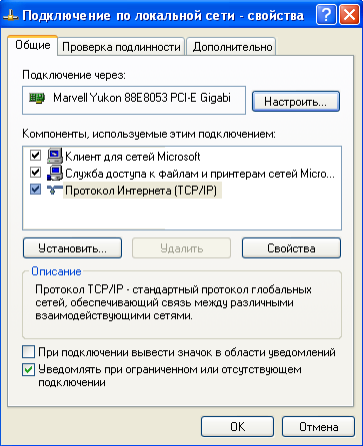
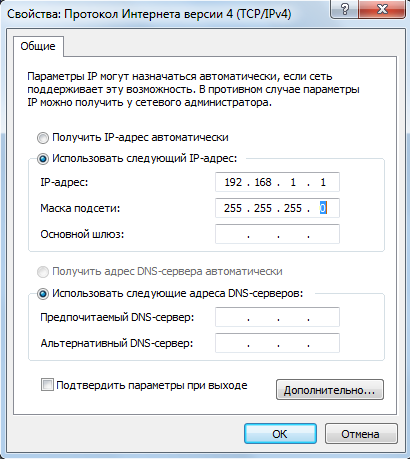


Рис. 3. Настройка свойств протокола Интернета.

в. Установите переключатель «Использовать следующий IP-адрес» и введите IP-адрес 192.168.1.1 и маску подсети 255.255.255.0. С данными IP-адресом и маской подсети номер сети узла – 192.168.1.0, а 192.168.1.1 – это первый узел в сети 192.168.1.0:



-адрес 192.168.1.1 Маска подсети 255.255.255.0 Рис. 4. Настройка статического IP-адреса на сетевом интерфейсе

г. Нажмите кнопку «ОК», чтобы закрыть окно «Свойства: Протокол Интернета (TCP/IP)».

Нажмите кнопку «Закрыть», чтобы закрыть окно «Подключение по локальной сети – свойства».

д. Повторите шаги 3a – 3d для компьютера PC2, используя IP-адрес 192.168.1.2 и маску подсети 255.255.255.0. Номер сети данного ПК – 192.168.1.0, а 192.168.1.2 – это второй узел в сети 192.168.1.0.

|  |  |
| --- | --- |
| I P-а д р е с | 192.168.1.2 |
| Ма с к а  п о д с е т и | 255.255.255.0 |

Шаг 4. Проверка IP-соединения между двумя ПК

ПРИМЕЧАНИЕ. Для проверки соединения TCP/IP на обоих ПК необходимо временно отключить межсетевой экран Windows либо разрешить прохождение эхо-пакетов протокола ICMP. После завершения проверки межсетевой экран Windows следует снова включить.

а. На рабочем столе Windows XP обоих ПК нажмите кнопку «Пуск». В меню «Пуск» выберите пункт «Панель управления» и дважды щелкните значок «Сетевые подключения».

б. Правой кнопкой мыши щелкните значок «Подключение по локальной сети» и выберите пункт

«Свойства». Перейдите на вкладку «Дополнительно». Найдите и нажмите кнопку «Параметры».

в. Проверьте, какие у межсетевого экрана настройки: «ВКЛЮЧЕН (ВКЛ.) для порта Ethernet»

или «ВЫКЛЮЧЕН (ВЫКЛ.) для порта Ethernet».

г. Если межсетевой экран включен, установите переключатель «Выключить (не рекомендуется)», чтобы отключить межсетевой экран. В дальнейшем межсетевой экран будет снова включен. Нажмите кнопку «ОК» в данном диалоговом окне и в следующем, чтобы применить изменения. Повторите шаги 4a – 4d на втором ПК.

д. Теперь, когда два ПК физически соединены и в них правильно настроены IP-адреса, необходимо убедиться в их способности связываться друг с другом. Команда ping – самый простой способ выполнения этой задачи. Команда ping включена в операционную систему Windows XP:

е. На компьютере PC1 нажмите кнопку «Пуск», а затем выберите команду «Выполнить». Введите команду cmd, а затем нажмите кнопку «ОК». Откроется окно командной строки Windows (см. рисунок ниже).

ж. В командной строке > введите ping 192.168.1.2 и нажмите клавишу ВВОД. Успешное выполнение команды ping подтверждает IP-подключение. Пример выходных данных представлен ниже.

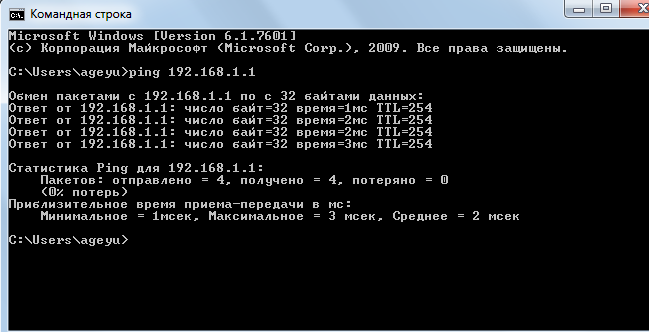


Рис. 5. Проверка состояния сетевого соединения.

**Практическая работа № 13**

**Организация инвентаризации технических средств сетевой инфраструктуры, осуществление контроля оборудования после его ремонта**

Часть 1. Настройка точки беспроводного доступа Задача

* Настроить точку беспроводного доступа, являющуюся компонентом многофункционального устройства, чтобы разрешить доступ беспроводным клиентам.

Исходные данные / подготовка

Устройство Linksys WRT54G2 совмещает в себе встроенный коммутатор на 4 порта, маршрутизатор и точку беспроводного доступа. В этой лабораторной работе необходимо настроить один из компонентов этого многофункционального устройства, а именно точку беспроводного доступа, чтобы разрешить доступ беспроводным клиентам. Будут настроены основные беспроводные возможности многофункционального устройства, но это не будет безопасная беспроводная сеть. Настройка безопасной беспроводной сети будет выполнена в следующей лабораторной работе.

Требуются следующие ресурсы:

* компьютер с ОС Windows XP, подключенный через кабель к многофункциональному устройству;
* устройство Linksys WRT54G2.

Шаг 1. Проверка соединения между компьютером и многофункциональным устройством

а. Компьютер, используемый для настройки точки доступа, должен быть подключен к одному из портов коммутатора многофункционального устройства.

б. На компьютере щелкните кнопку «Пуск» и выберите «Выполнить». Введите команду cmd и нажмите кнопку «OK» или клавишу ВВОД.

в. Используя командную строку, отправьте эхо-запрос на многофункциональное устройство, используя IP-адрес по умолчанию (192.168.1.1) или IP-адрес, настроенный для порта многофункционального устройства. Ничего не предпринимайте, пока эхо-запрос не будет успешным.

г. Запишите команду, использованную для отправки эхо-запроса на многофункциональное устройство.

ПРИМЕЧАНИЕ. Если эхо-запрос выполнить не удалось, попробуйте следующие способы

устранения неполадок.

* Убедитесь, что IP-адрес компьютера находится в сети 192.168.1.0. Для успешного выполнения эхо-запроса компьютер должен находиться в той же сети, что и многофункциональное

устройство. Служба DHCP многофункционального устройства включена по умолчанию. Если компьютер настроен как клиент DHCP, он должен иметь правильный IP-адрес и маску подсети. Если компьютер использует статический IP-адрес, он должен находиться в сети 192.168.1.0,

а его маска подсети должна быть 255.255.255.0.

* Убедитесь, что используется гарантированно работоспособный прямой кабель. Протестируйте его, чтобы убедиться в этом.
* Проверьте, что индикатор связи порта, к которому подключен компьютер, горит.
* Проверьте, подается ли на многофункциональное устройство электропитание. Если эти шаги не помогли решить проблему, обратитесь к преподавателю.

Шаг 2. Вход в систему многофункционального устройства и настройка беспроводной сети

а. Откройте веб-обозреватель. В строке адреса наберите http://ip\_address, где ip\_address – IP- адрес беспроводного маршрутизатора (по умолчанию 192.168.1.1). В запросе оставьте поле ввода имени пользователя пустым, но введите пароль, назначенный маршрутизатору. Пароль по умолчанию: admin. Щелкните кнопку «OK».

б. В главном меню щелкните параметр «Wireless» (беспроводная сеть).



Рис. 1. Интерфейс окна настроек многофункционального устройства Linksys.

в. В окне «Basic Wireless Settings» (основные настройки беспроводной сети) в списке «Network Mode» (сетевой режим) по умолчанию выбрано значение «Mixed» (смешанный), поскольку точка доступа поддерживает беспроводные устройства 802.11b, g, и n. Можно использовать любой из этих стандартов для подключения к точке доступа. Если беспроводная часть многофункционального устройства НЕ используется, в качестве сетевого режима можно установить «Disabled» (отключено). Оставьте выбранным значение по умолчанию «Mixed» (смешанный).

г. Удалите SSID по умолчанию (linksys) из поля ввода «Network Name (SSID)» (сетевое Имя (SSID)). Введите новый SSID, используя свою фамилию или имя, указанное преподавателем. SSID задаются с учетом регистра.

д. Запишите точное имя SSID, которое будет использоваться.

е. Щелкните по раскрывающемуся меню «Radio Band» (радиодиапазон) и запишите два

предлагаемых параметра.

ж. Для беспроводной сети, в которой можно использовать клиентские устройства 802.11b, g

или n, значение по умолчанию – «Auto» (автоматически). Значение «Auto» (автоматически)» позволяет выбрать параметр «Wide Channel» (широкий канал) и обеспечивает наилучшие параметры работы. Параметр «Standard Channel» (стандартный канал) используется, если устройства беспроводных клиентов имеют типы 802.11b или/и g. Параметр «Wide Channel» (широкий канал) используется, если используются только клиентские устройства 802.11n.

Оставьте выбор значения по умолчанию «Auto» (авто).

з. Для параметра «SSID Broadcast» (широковещательная рассылка SSID) по умолчанию выбрано значение «Enabled» (включить), это позволяет точке доступа регулярно посылать SSID, используя беспроводную антенну. Все беспроводные устройства поблизости могут обнаружить этот сигнал. Таким способом клиенты обнаруживают находящуюся поблизости беспроводную сеть.

и. Щелкните кнопку «Save Settings» (сохранить настройки), находящуюся в самом низу веб- страницы. После успешного сохранения настоек щелкните «Continue» (продолжить).

к. Теперь точка доступа настроена для беспроводной сети с присвоенным ей именем (SSID). Необходимо записать эту информацию до начала следующей лабораторной работы или до подключения любых беспроводных сетевых интерфейсных плат к беспроводной сети.

Вопросы для обсуждения

1. Сколько беспроводных устройств по вашему мнению можно настроить в одном помещении? Что может ограничить это число?
2. Какую потенциальную угрозу безопасности при широковещательной рассылке вашего SSID с

точки доступа вы можете назвать?

Часть 2. Настройка беспроводного клиента

Задачи

* Установите и настройте на клиентском компьютере драйвер для беспроводной сетевой интерфейсной платы, подключаемой к USB.
* Определите версию установленного драйвера и проверьте обновления в Интернете.

Исходные данные / подготовка

В этой лабораторной работе необходимо установить на компьютере драйвер для беспроводной сетевой интерфейсной платы, подключаемой к USB. Драйвер – это вид программного обеспечения, который управляет беспроводной сетевой интерфейсной платой. Драйвер можно найти на CD-диске, поставляемом вместе с сетевой интерфейсной платой, или он может быть загружен из Интернета.

Многие производители требуют установить драйвер до подключения адаптера. Процедура, описанная в этой лабораторной работе, предназначена для беспроводной сетевой интерфейсной платы Linksys USB 802.11g, но она будет аналогична и для других плат. Всегда выполняйте процедуру, рекомендованную производителем беспроводной сетевой интерфейсной платы.

Требуются следующие ресурсы:

* компьютер с ОС Windows XP и со свободным USB портом;
* беспроводная сетевая интерфейсная плата и соответствующий драйвер;
* права администратора для установки драйвера;
* устройство Linksys WRT54G2 с беспроводным доступом, настроенное в предыдущей лабораторной работе.

Шаг 1. Установка драйвера беспроводной сетевой интерфейсной платы

а. Вставьте компакт-диск, на котором находится драйвер беспроводной сетевой интерфейсной платы, в дисковод CD/DVD и установите драйвер в соответствии с рекомендациями производителя. Для большинства USB-устройств необходимо установить драйвер до физического подключения самого устройства. Обратите внимание, что можно выполнить часть процесса установки сейчас, а закончить после установки беспроводной сетевой интерфейсной платы.



Рис. 2. Окно программы настройки беспроводного USB-интерфейса.

б. Кто производитель беспроводной сетевой интерфейсной платы?

в. Опишите процесс установки драйвера беспроводной сетевой интерфейсной платы.

Шаг 2. Установка беспроводной сетевой интерфейсной платы

а. При запросе подсоедините USB-кабель беспроводной сетевой интерфейсной платы к свободному USB-порту. Для продолжения нажмите кнопку «Next» (далее).



Рис. 3. Подключение беспроводного USB-адаптера.

Шаг 3. Выполнение подключения к беспроводной сети

а. Большинство адаптеров беспроводных сетевых интерфейсных плат имеют клиентское программное обеспечение для управления сетевой интерфейсной платой. Это программное обеспечение отображает все обнаруженные беспроводные сети. Выберите SSID беспроводной сети, настроенной на точке доступа в предыдущей лабораторной работе.

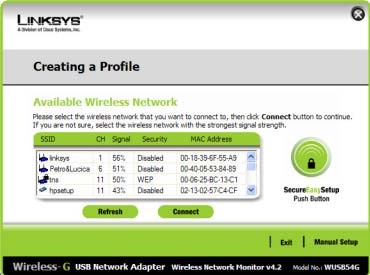


Рис. 4. Обнаружение беспроводных сетей в радиусе действия адаптера.

б. Какой SSID вы используете? в. Если беспроводная сетевая интерфейсная плата не подключилась к беспроводной сети, выполните соответствующие действия по поиску и устранению неполадок.

г. Укажите силу сигнала для беспроводной сетевой интерфейсной платы.

д. Обнаружила ли беспроводная сетевая интерфейсная плата другие беспроводные сети? Почему? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

е. Покажите свое активное сетевое подключение другому учащемуся или лаборанту.

ж. Как по-другому называется беспроводной узел? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

з. Что лучше: использовать клиентское программное обеспечение от производителя беспроводной сетевой интерфейсной платы или разрешить управлять беспроводной сетевой интерфейсной платой Windows XP?

Шаг 4. Определение версии драйвера сетевой платы

а. Производители оборудования постоянно обновляют драйверы. Драйвер, поставляемый в комплекте с сетевой интерфейсной платой или другим оборудованием, часто является не самым последним.

б. Чтобы узнать версию установленного вами драйвера сетевой интерфейсной платы, щелкните

«Пуск», выберите «Панель управления» и далее «Сетевые подключения». Щелкните правой кнопкой мыши по беспроводному соединению и выберите пункт «Свойства». Щелкните кнопку

«Настройка» для сетевой интерфейсной платы, а затем вкладку «Драйвер». Как называется установленный драйвер и какая его версия установлена?

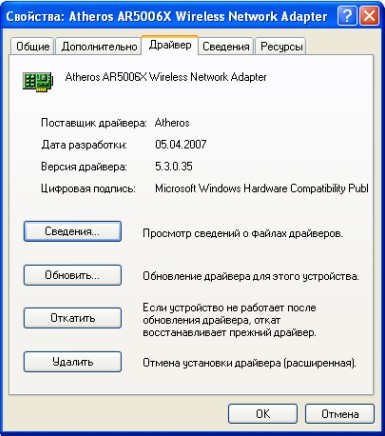


Рис. 5. Определение версии драйвера для установленной беспроводной сетевой карты.

Шаг 5. Определение текущей версии драйвера сетевой интерфейсной платы

а. Выполните поиск драйверов, поддерживающих вашу беспроводную сетевую интерфейсную плату, на веб-узле производителя. Предлагает ли производитель более новые версии драйвера?

б. Какая из перечисленных версий самая новая?

в. Если есть более новый драйвер, что с ним следует сделать?

Шаг 6. Проверка подключения.

а. После установки сетевой интерфейсной платы необходимо проверить возможность соединения с Linksys WRT300N.

б. Откройте веб-обозреватель (например, Windows Internet Explorer или Mozilla Firefox).

в. В строке адреса введите [http://192.168.1.1.](http://192.168.1.1/) Это адрес по умолчанию точки доступа.

г. В диалоговом окне «Подключение к 192.168.1.1» ничего не вводите в поле ввода имени пользователя, а в поле ввода пароля введите admin. Не устанавливайте флажок «Сохранить пароль». Нажмите кнопку «ОК».

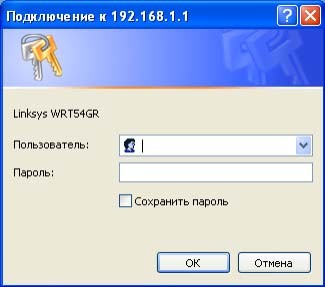


Рис. 6. Подключение к многофункциональному устройству по беспроводной сети.

д. Если вы увидите экран настройки Linksys, то вы успешно соединились с точкой доступа. Если соединение не установлено, следует устранить неполадки в соединении, убедившись что устройства включены и IP-адреса всех устройств верны. Какой IP-адрес должен быть настроен для беспроводной сетевой интерфейсной платы?

Вопросы для обсуждения

1. Будет ли, по вашему мнению, отличаться процесс установки беспроводной сети в продуктовом или книжном магазине от только что выполненного? Почему?

б. Будет ли, по вашему мнению, использованная модель точки доступа достаточна для

продуктового магазина в вашем районе? Поясните свой ответ.

Часть 3. Настройка безопасности беспроводной сети

Задачи

* Разработать план обеспечения безопасности для домашней сети.
* Настроить точку беспроводного доступа, являющуюся компонентом многофункционального устройства, используя лучшие методы обеспечения безопасности.

Исходные данные / подготовка

Хорошо продуманная реализация системы безопасности крайне важна для безопасной работы беспроводной сети. В этой лабораторной работе демонстрируются действия, которые необходимо предпринять, чтобы гарантировать безопасность сети, используя следующий сценарий:

Вы только что приобрели беспроводной маршрутизатор Linksys WRT54G2 и хотите настроить небольшую сеть у себя дома. Вы выбрали этот маршрутизатор, поскольку согласно спецификации IEEE 802.11n он в 12 раз превосходит 802.11g по скорости и в 4 раза по дальности. Поскольку в стандарте 802.11n используется частота 2,4 ГГц, он обратно совместим как с 802.11b, так и с 802.11g и использует технологию MIMO (много входов, много выходов).

Механизмы безопасности следует включить перед подключением беспроводного устройства к Интернету или проводной сети. Также следует изменить значения по умолчанию, поскольку они широко известны и могут быть получены из Интернета.

Требуются следующие ресурсы:

* компьютер с ОС Windows;
* устройство Linksys WRT54G2;
* прямой кабель Ethernet.

Шаг 1. Разработка плана обеспечения безопасности для домашней сети

а. Укажите как минимум шесть лучших методов, которые следует использовать, чтобы защитить многофункциональное устройство и беспроводную сеть.

1)

2)

3)

4)

5)

6)

б. Укажите, какие существуют угрозы безопасности для каждого из элементов.

1)

2)

3)

4)

5)

6)

Шаг 2. Подключение компьютера к многофункциональному устройству и вход на веб-утилиту а. Подключите ваш компьютер (сетевую интерфейсную плату Ethernet) к многофункциональному устройству (порт 1 на Linksys WRT54G2), используя прямой кабель. б. IP-адрес Linksys WRT54G2 по умолчанию: 192.168.1.1, маска подсети по умолчанию: 255.255.255.0. Для возможности обмена данными компьютер и устройство Linksys должны находиться в одной сети. Измените IP-адрес компьютера на 192.168.1.2 и убедитесь, что в

качестве маски подсети указано 255.255.255.0. Введите в качестве основного шлюза внутренний адрес устройства Linksys (192.168.1.1). Для этого щелкните «Пуск» > «Панель управления» >

«Сетевые подключения». Щелкните правой кнопкой мыши по беспроводному подключению и выберите пункт «Свойства». Выберите протокол Интернета (TCP/IP) и введите адреса, как указано ниже.

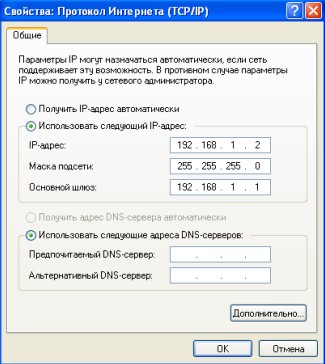


Рис. 7. Настройка сетевого адреса на компьютере клиента сети.

в. Откройте веб-обозреватель (например, Internet Explorer, Netscape или Firefox), введите в поле адреса IP-адрес по умолчанию устройства Linksys (192.168.1.1) и нажмите клавишу ВВОД.

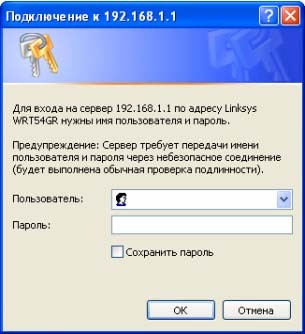
г. Отображается экран с запросом имени пользователя и пароля.

Рис. 8. Проверка пользователя при попытке доступа к устройству.

д. Оставьте поле имени пользователя пустым, а в поле пароля введите admin. Это пароль по умолчанию для устройства Linksys. Щелкните кнопку «ОК». Пароли задаются с учетом регистра.

е. После выполнения всех необходимых изменений в устройстве Linksys нажмите «Save Settings» (сохранить настройки) на каждом экране, чтобы сохранить изменения, или «Cancel Changes» (отменить изменения) для сохранения значений по умолчанию.

Шаг 3. Изменение пароля устройства Linksys

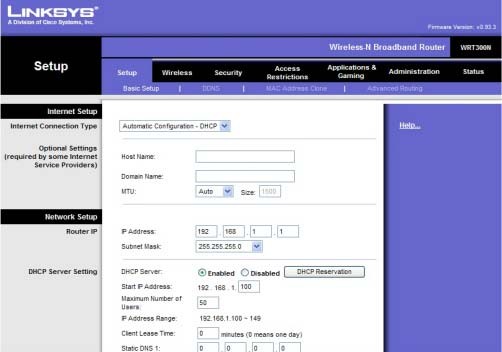
а. Изображенный здесь начальный экран – это экран «Setup» (настройки) > «Basic Setup» (основные настройки).

Рис. 9. Изменение пароля доступа к устройству.

б. Щелкните вкладку «Administration» (администрирование). Вкладка «Management» (управление) выбрана по умолчанию.

в. Введите новый пароль для устройства Linksys, а затем подтвердите его. Новый пароль должен состоять не более чем из 32 символов и не должен содержать пробелов. Пароль необходим для доступа к веб-утилите устройства Linksys и к мастеру установки.

г. Возможность доступа к веб-утилите через беспроводную сеть включена по умолчанию. Эту функцию можно отключить для повышения уровня безопасности.

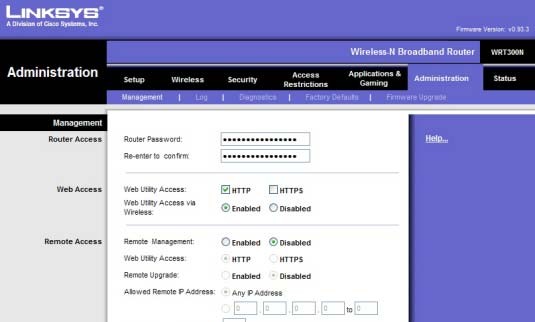


Рис. 10. Настройка ограничений доступа.

д. Щелкните кнопку «Save Settings» (сохранить настройки), чтобы сохранить информацию. ПРИМЕЧАНИЕ. Если вы забудете свой пароль, можно восстановить заводские настройки устройства Linksys по умолчанию, нажав кнопку RESET и удерживая ее в течение 5 секунд. Пароль по умолчанию: admin.

Шаг 4. Настройка параметров безопасности беспроводной сети

а. Щелкните вкладку «Wireless» (беспроводная). Вкладка «Basic Wireless Settings» (основные настройки беспроводной сети) выбрана по умолчанию. «Network Name» (сетевое имя) – это SSID, общее для всех устройств сети. Оно должен быть одинаковым для всех устройств в беспроводной сети. Оно задается с учетом регистра, и его длина не может превышать 32 символов.

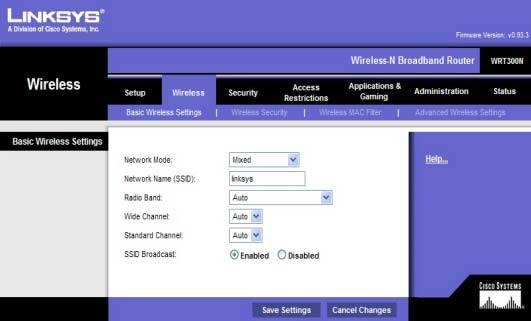


Рис. 11. Настройка параметров защиты беспроводной сети.

б. Измените значение SSID с linksys на уникальное имя. Запишите выбранное имя.

в. Оставьте в качестве значения параметра «Radio Band (Радиодиапазон)» – «Auto»

(автоматически). Это позволяет сети использовать все устройства: 802.11n, g и b.

г. Для параметра «SSID Broadcast» (широковещательная рассылка SSID) выберите переключатель «Disabled» (отключить), чтобы отключить широковещательную рассылку SSID. Беспроводные клиенты выполняют поиск сети в зоне своего доступа и обнаруживают широковещательную рассылку SSID устройства Linksys. Для большей безопасности отключите широковещательную рассылку SSID.

д. Сохраните изменения перед переходом на следующий экран.

Шаг 5. Настройка шифрования и аутентификации

а. Выберите вкладку «Wireless Security» (безопасность беспроводной сети) на экране

«Wireless» (беспроводная сеть).

б. Этот маршрутизатор поддерживает четыре типа настроек режима безопасности:

* WEP (обеспечение конфиденциальности, сопоставимой с проводными сетями);
* WPA (защищенный доступ к Wi-Fi), использующий предварительно согласованный ключ

(PSK);

* WPA Enterprise, использующий службу удаленной аутентификации пользователей с коммутируемым доступом (RADIUS);
* RADIUS.

в. Выберите Security Mode (режим безопасности) WPA Personal.

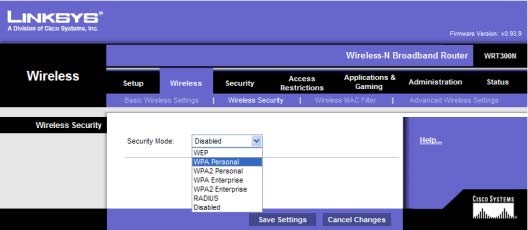


Рис. 12. Выбор криптографического протокола для беспроводной сети. г. На следующем экране выберите алгоритм шифрования (строка Encryption).

Чтобы защитить сеть, используйте самый высокий уровень шифрования из предложенных для выбранного режима безопасности. Далее перечислены режимы безопасности и уровни шифрования от наименее защищенного (WEP) к наиболее защищенному (WPA2 с AES)

* WEP;
* WPA
* WPA2
* TKIP (Temporal Key Integrity Protocol);
* AES (Advanced Encryption System - расширенный стандарт шифрования); ;

AES поддерживается только новыми устройствами, содержащими специальный криптографический сопроцессор. Чтобы обеспечить совместимость со всеми устройствами, выберите протокол TKIP.

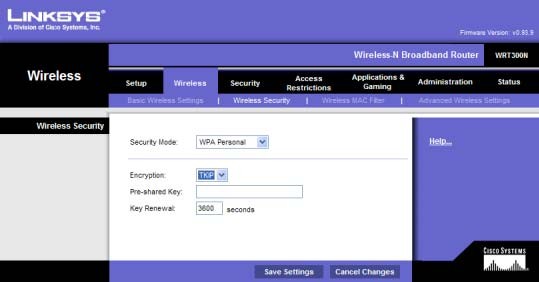


Рис. 13. Выбор алгоритма шифрования.

д. Для аутентификации введите предварительно согласованный ключ длиной от 8 до 63 символов. Этот ключ является общим для устройства Linksys и всех подключенных устройств. е. Выберите период обновления ключа от 600 до 7 200 секунд. Период обновления – время, через которое устройство Linksys изменяет ключ шифрования.

ж. Сохраните настройки до выхода из этого экрана.

Шаг 6. Настройка фильтрации по MAC-адресам

а. Выберите вкладку «Wireless MAC Filter» (фильтр беспроводных MAC-адресов) на экране

«Wireless» (беспроводная).

б. Фильтрация по MAC-адресам позволяет только беспроводным клиентам с указанными MAC-адресами подключаться к сети. Установите переключатель «Permit PCs listed below to access the wireless network» (разрешить указанным ниже ПК получать доступ к беспроводной сети). Щелкните кнопку «Wireless Client List» (список беспроводных клиентов), чтобы отобразить список всех беспроводных клиентских компьютеров в сети.

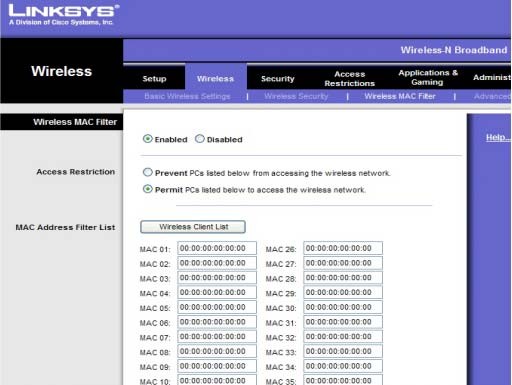


Рис. 14. Настройка фильтрации клиентских подключений по MAC-адресам.

в. На следующем экране можно указать, какие MAC-адреса могут иметь доступ к беспроводной сети. Установите флажок «Save to MAC Address Filter List» (сохранить в списке фильтра по MAC-адресам) для всех клиентских устройств, которые следует добавить, а затем щелкните кнопку «Add» (добавить). Все беспроводные клиенты, не указанные в списке, не смогут подключиться к беспроводной сети. Сохраните настройки до выхода из этого экрана.

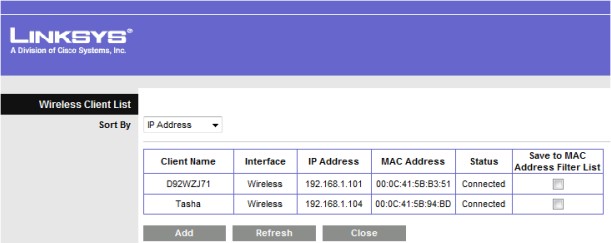


Рис. 15. Отображение подключенных клиентов.

Вопросы для обсуждения

1. Какая функция, настроенная на Linksys WRT54G2, по вашему мнению, наиболее важна для обеспечения безопасности и почему?
2. Напишите, что еще можно сделать, чтобы повысить безопасность сети.

**Практическая работа № 14**

**Выполнение замены расходных материалов и мелкий ремонт периферийного оборудования, определение устаревшего оборудования и программных средств сетевой инфраструктуры**

Часть 1. Настройка политик доступа и DMZ на многофункциональном устройстве

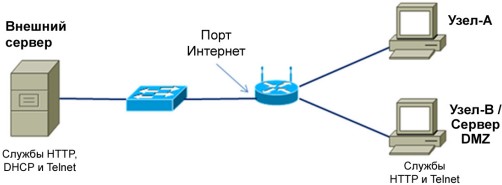


Рис. 1. Топология сети в которой установлено многофункциональное устройство.

Задачи

* Войти в систему многофункционального устройства и просмотреть настройки безопасности.
* Настроить политики доступа в Интернет на основе IP-адреса и приложения.
* Настроить DMZ для сервера открытого доступа со статическим IP-адресом.
* Настроить переадресацию портов, чтобы разрешить доступ только к портам HTTP.
* Использовать возможности справки Linksys WRT54G2.

Исходные данные / подготовка

В этой лабораторной работе содержатся инструкции по настройке параметров безопасности на Linksys WRT54G2. Linksys содержит программный межсетевой экран для защиты внутренних (принадлежащих к локальной сети) клиентов от атак с внешних узлов.

Подключения внутренних узлов к внешним адресатам могут фильтроваться в зависимости от IP-

адреса, веб-узла назначения и приложения.

Устройство Linksys также можно настроить на создание демилитаризованной зоны (DMZ) для контроля доступа к серверу с внешних узлов. Эта лабораторная работа выполняется в группах по двое, при этом две группы могут работать вместе для взаимного тестирования настроек ограничения доступа и функциональности DMZ. Работа делится на 2 части:

* + Часть 1. Настройка политик доступа.
  + Часть 2. Настройка DMZ.

Для выполнения работы требуются следующие ресурсы:

* + Linksys WRT54G2 или другое многофункциональное устройство с настройками по умолчанию;
  + идентификатор пользователя и пароль для устройства Linksys, если они отличаются от значений по умолчанию;
  + компьютер с Windows XP Professional для доступа к графическому интерфейсу пользователя Linksys;
  + внутренний ПК в качестве сервера в DMZ со службами HTTP и Telnet (заранее настроенный или сервер Discovery Live CD);
  + внешний сервер, используемый в качестве «Интернета» и поставщика услуг Интернета, на котором заранее настроены службы DHCP, HTTP и Telnet (это может быть реальный сервер или сервер Discovery Live CD);
  + кабели для соединения ПК, Linksys WRT54G2 или другого многофункционального устройства и коммутаторов.

Часть 1. Настройка политик доступа Шаг 1. Создание сети и настройка узлов

а. Присоедините узлы к портам коммутатора многофункционального устройства, как показано на схеме топологии рис. 1. Узел-А – это консоль, используемая для доступа к графическому интерфейсу пользователя Linksys. Узел-B сначала выполняет роль тестовой машины, а затем используется как сервер DMZ.

б. Настройте IP-конфигурацию для обоих узлов, используя сетевые подключения Windows XP и свойства TCP/IP. Убедитесь, что узел-А настроен как клиент DHCP. Присвойте узлу-В статический IP-адрес в диапазоне 192.168.1.x с маской подсети 255.255.255.0. В качестве основного шлюза следует задать внутренний локальный сетевой адрес устройства Linksys.

ПРИМЕЧАНИЕ. Если узел-В уже является клиентом DHCP, можно сохранить его текущий адрес и сделать его статическим, используя возможность сохранения DHCP на экране основных настроек Linksys.

в. Используйте команду ipconfig для отображения IP-адреса, маски подсети и основного шлюза для узла-А и узла-В и запишите их в таблицу. Узнайте у преподавателя IP-адрес и маску подсети внешнего сервера и запишите их в таблицу.

Табл. 1

|  |  |  |  |
| --- | --- | --- | --- |
| Узел | IP-адрес | Маска подсети | Основной шлюз |
| Узел А |  |  |  |
| Узел В/Сервер DMZ |  |  |  |
| Внешний сервер |  |  |  |

Шаг 2. Вход в интерфейс пользователя

а. Для доступа к веб-интерфейсу пользователя устройства Linksys откройте обозреватель и введите IP-адрес устройства по умолчанию 192.168.1.1.

б. Войдите в систему, используя идентификатор пользователя и пароль по умолчанию admin. На рис. 2 показано окно аутентификации.

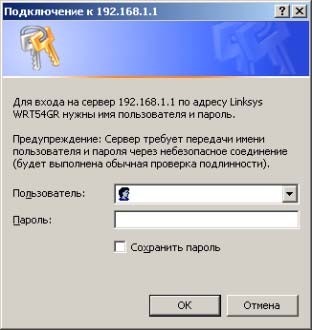


Рис. 2. Окно аутентификации на многофункциональном устройстве.

в. Многофункциональное устройство должно быть настроено для получения IP-адреса с внешнего сервера DHCP. При входе на устройство Экран по умолчанию после входа в систему многофункционального устройства:

«Setup» (настройки) > «Basic Setup» (основные настройки), как показано на рис. 3.

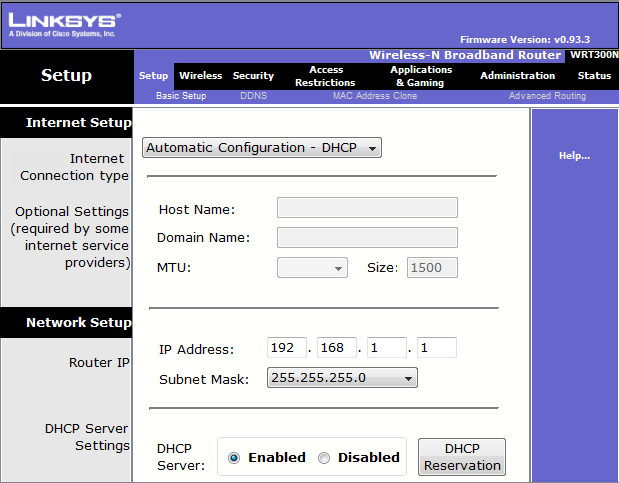


Рис. 3. Окно базовых настроек многофункционального устройства Ответьте на следующие вопросы:

Какой используется тип подключения к Интернету?

г. Какой IP-адрес и маска подсети маршрутизатора по умолчанию (внутреннего) используется для многофункционального устройства?

д. Убедитесь, что многофункциональное устройство получило внешний IP-адрес с сервера

DHCP. Для этого щелкните «Status» (статус) > вкладка «Router» (маршрутизатор).

е. Какой внешний IP-адрес и маска подсети присвоены многофункциональному устройству?

Шаг 3. Просмотр настроек межсетевого экрана многофункционального устройства

а. Linksys WRT54G2 содержит простой межсетевой экран (рис. 4), который использует преобразование сетевых адресов (NAT). Кроме того, он имеет дополнительные возможности межсетевого экрана с использованием функции динамического анализа пакетов (SPI) для обнаружения и блокирования запросов, поступающих из Интернета.

б. На главном экране щелкните вкладку «Security» (безопасность) для просмотра состояния параметров «Firewall» (межсетевой экран) и «Internet Filter» (интернет-фильтр). Укажите статус защиты межсетевого экрана SPI.

в. Какие флажки установлены для «Internet Filter» (интернет-фильтр)?

г. Щелкните «Help» (справка), чтобы больше узнать об этих настройках. Какие преимущества

дает фильтрация IDENT?

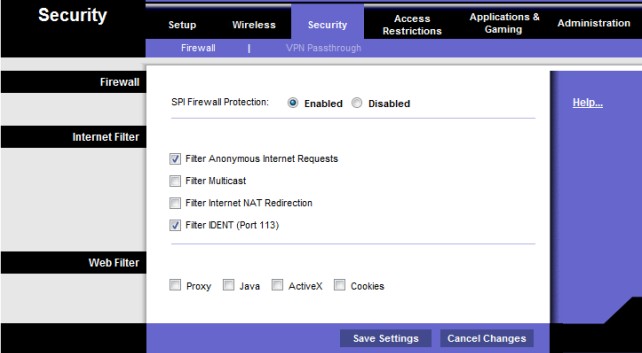


Рис. 4. Настройки межсетевого экрана многофункционального устройства.

Шаг 4. Настройка ограничений доступа в Интернет на основе IP-адреса

В лабораторной работе №5 было продемонстрировано, что для указания того, какие клиентские компьютеры могут получать доступ к многофункциональному устройству в зависимости от их MAC-адреса, можно использовать возможности беспроводной безопасности. Это предотвращает подключение не авторизованных компьютеров к точке беспроводного доступа и получение ими доступа к внутренней локальной сети и Интернету.

Многофункциональное устройство также позволяет указать, какие внутренние пользователи могут выйти в Интернет из локальной сети. Можно создать политику доступа в Интернет, разрешающую или запрещающую определенным внутренним компьютерам доступ в Интернет в зависимости от их IP-адреса, MAC-адреса и других критериев.

а. На главном экране многофункционального устройства щелкните вкладку «Access Restrictions» (ограничения доступа) и задайте параметр «Access Policy 1» (политика доступа 1).

б. Введите в качестве названия политики «Block-IP» (блокировка IP). Выберите «Enabled» (включено), чтобы включить политику, а затем выберите «Deny» (запретить), чтобы предотвратить доступ в Интернет с указанного IP-адреса (рис. 5).

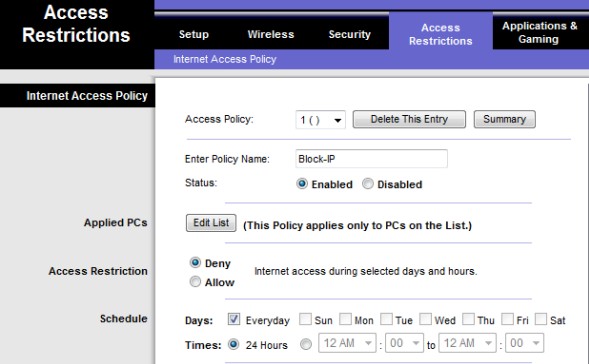


Рис. 5. Настройка политики ограничения доступа в Интернет.

в. Щелкните кнопку «Edit List» (редактировать список) и введите IP-адрес узла-В. Щелкните

«Save Settings» (сохранить настройки), а затем «Close» (закрыть)». Щелкните «Save Settings» (сохранить настройки)» для сохранения политики доступа в Интернет 1 – «Блокировка IP». г. Протестируйте политику, попробовав подключиться к внешнему веб-серверу с узла-В. Откройте обозреватель и введите IP-адрес внешнего сервера в поле адреса. Можете ли вы подключиться к серверу?

д. Измените статус политики «Block-IP» (блокировка IP) на «Disabled» (выключено) и щелкните «Save Settings» (сохранить настройки). Можете ли вы теперь подключиться к серверу?

е. Какие еще можно использовать политики доступа для блокировки доступа в Интернет?

Шаг 5. Настройка политики доступа в Интернет на основе приложений

Можно создать политику доступа в Интернет, не позволяющую некоторым компьютерам использовать определенные приложения или протоколы Интернета.

а. На главном экране графического интерфейса пользователя Linksys щелкните вкладку «Access Restrictions» (ограничение доступа) и определите политику доступа в Интернет.

б. Введите в качестве названия политики «Block-Telnet» (блокировка Telnet). Выберите

«Enabled» (включено) для включения политики, а затем щелкните «Allow to permit Internet access from a specified IP address as long as it is not one of the applications that is blocked» (разрешить доступ в Интернет с заданного IP-адреса, если это не одно из заблокированных приложений).

в. Щелкните кнопку «Edit List» (редактировать список) и введите IP-адрес узла-В. Щелкните

«Save Settings» (сохранить настройки), а затем «Close» (закрыть). Какие другие интернет- приложения и протоколы можно заблокировать?

г. Выберите приложение Telnet из списка приложений, которые можно заблокировать, а затем

щелкните двойную стрелку вправо, чтобы добавить его к списку «Blocked List» (список заблокированных), как показано на рисунке 6. Щелкните «Save Settings» (сохранить настройки).

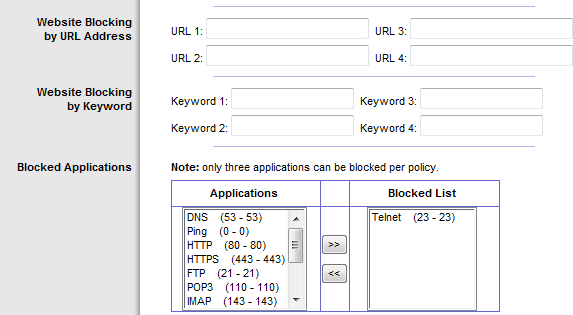


Рис. 6. Ограничение доступа для заданного приложения.

д. Протестируйте политику: откройте командную строку, используя «Пуск» > «Все программы»

> «Стандартные» > «Командная строка».

е. Отправьте эхо-запрос на IP-адрес внешнего сервера с узла-В, используя команду ping. Можете ли вы получить эхо-запрос с сервера?

ж. Подключитесь по протоколу Telnet на IP-адрес внешнего сервера с узла-В, используя команду telnet A.B.C.D (где A.B.C.D – IP-адрес сервера).

Можете ли вы получить доступ к серверу?

Часть 2. Настройка DMZ на многофункциональном устройстве Шаг 1. Настройка простой зоны DMZ

Иногда требуется разрешить доступ к компьютеру из Интернета, но защитить остальные компьютеры внутренней локальной сети. Для этого можно создать демилитаризованную зону (DMZ), которая позволяет получать доступ к любым портам и службам на указанном сервере. Любые запросы к службам по внешнему адресу многофункционального устройства будут перенаправлены указанному серверу.

а. Узел-В будет выполнять функцию сервера DMZ, и на нем необходимо запустить службы HTTP и Telnet. Убедитесь, что узел-В имеет статический IP-адрес, или, если узел-В является клиентом DHCP, можно зарезервировать его текущий адрес и сделать его статическим, используя функцию «DHCP Reservation» (резервирование DHCP) устройства Linksys на экране

«Basic Setup» (основные настройки).

б. На главном экране графического интерфейса пользователя Linksys щелкните вкладку

«Applications & Gaming» (приложения и игры), а затем щелкните «DMZ», рис. 7.

в. Щелкните ссылку «Help» (справка) для получения дополнительных сведений о DMZ. Для каких других целей может понадобиться настройка узла в DMZ?

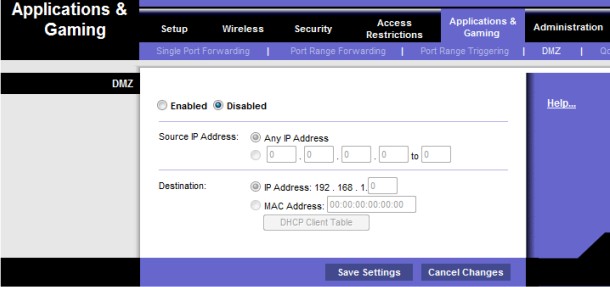


Рис. 7. Окно настроек DMZ.

г. Функция DMZ отключена по умолчанию. Выберите «Enabled» (включено), чтобы включить DMZ. Переключатель «Any IP Address» (любой IP-адрес) в поле «Source IP Address» (IP-адрес источника) должен быть выбран, а в поле в поле «Destination IP Address» (IP-адрес назначения)» введите IP-адрес узла-В. Щелкните «Save Settings» (сохранить настройки) и «Continue» (продолжить) при получении запроса.

д. Проверьте базовый доступ к серверу DMZ, отправив эхо-запрос с внешнего сервера на внешний адрес многофункционального устройства. Используйте команду ping –a, чтобы убедиться, что на запросы в действительности отвечает сервер DMZ, а не многофункциональное устройство. Можно ли получить эхо-запрос с DMZ-сервера?

е. Протестируйте HTTP-доступ к серверу DMZ: откройте обозреватель на внешнем сервере и

введите внешний IP-адрес многофункционального устройства. Попробуйте сделать то же самое из обозревателя на узле-А, используя внутренние адреса. Можно ли получить доступ к веб- странице?

ж. Протестируйте подключение по протоколу Telnet: откройте командную строку (см. шаг 5). Подключитесь по протоколу Telnet к внешнему IP-адресу многофункционального устройства, используя команду telnet A.B.C.D (где A.B.C.D – внешний IP-адрес многофункционального устройства). Можете ли вы получить доступ к серверу?

Шаг 2. Настройка узла с переадресацией одного порта

Базовые функции хостинга DMZ, настроенные на шаге 6, позволяют открыть доступ ко всем портам и службам на сервере, например, HTTP, FTP и Telnet. Если узел используется для конкретной цели (например, для служб FTP или для веб-служб), доступ должен быть ограничен указанной службой. Это можно сделать за счет переадресации одного порта. Эта функция более безопасна, чем основные функции DMZ, поскольку она открывает доступ только к необходимым портам. Перед выполнением этого шага отключите настройки DMZ для шага 1. узел-В – это сервер, на который переадресуются порты, но доступ к нему ограничен веб- протоколом (HTTP).

а. На главном экране щелкните вкладку «Applications & Gaming» (приложения и игры), а затем щелкните «Single Port Forwarding» (переадресация одного порта), чтобы указать приложения и номера портов.

б. Щелкните первое раскрывающееся меню под заголовком «Application Name» (имя приложения) и выберите HTTP. Это порт 80 протокола веб-сервера.

в. В первое поле «To IP Address» (на IP-адрес) введите IP-адрес узла-В и установите флажок

«Enabled» (включено). Щелкните кнопку «Save Settings» (сохранить настройки).

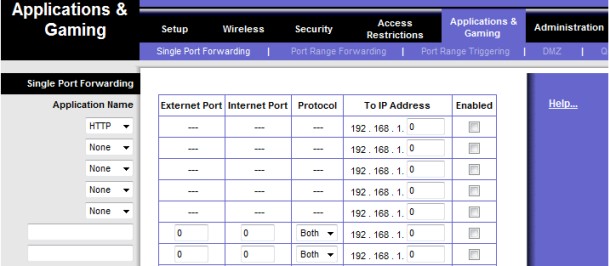


Рис. 8. Настройка перенаправления портов.

г. Протестируйте HTTP-доступ к узлу DMZ: откройте обозреватель на внешнем сервере и введите внешний IP-адрес многофункционального устройства. Попробуйте сделать то же самое из обозревателя на узле-А на узел-В. Можно ли получить доступ к веб-странице? д. Протестируйте подключение по протоколу Telnet: откройте командную строку (см. шаг 5).

Подключитесь по протоколу telnet к внешнему IP-адресу многофункционального устройства, используя команду A.B.C.D (где A.B.C.D – внешний IP-адрес многофункционального устройства). Можете ли вы получить доступ к серверу?

Шаг 3. Восстановление настроек по умолчанию многофункционального устройства

а. Чтобы восстановить заводские настройки по умолчанию устройства Linksys, щелкните вкладку «Administration» (администрирование) > «Factory Defaults» (заводские настройки по умолчанию).

б. Щелкните кнопку «Restore Factory Defaults» (восстановить заводские настройки по умолчанию), рис. 9. Все записи и изменения настроек будут потеряны.

ПРИМЕЧАНИЕ. Текущие настройки можно сохранять и загружать, используя вкладку

«Administration» (администрирование) > «Management» (управление) и кнопки «Backup Configuration» (резервное копирование конфигурации) и «Restore Configuration» (восстановить конфигурацию).



Рис. 9. Восстановление заводских настроек.

Часть 2. Выполнение анализа уязвимости системы с помощью программы MBSA

ВНИМАНИЕ! При выполнении этой лабораторной работы могут оказаться нарушенными юридические и организационные политики безопасности. Анализатор системы безопасности, загружаемый в процессе выполнения этой лабораторной работы, необходимо использовать только в целях обучения в рамках этой лабораторной работы. До использования анализатора системы безопасности в реальной сети проконсультируйтесь с преподавателем и администрацией сети относительно внутренних правил по использованию таких инструментальных средств.

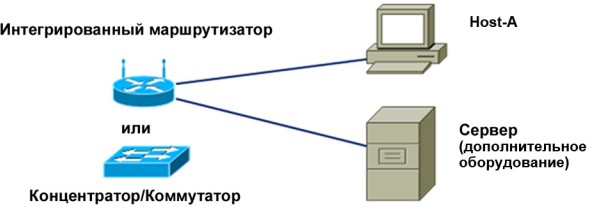


Рис. 10. Топология сети при выполнении анализа уязвимостей.

Задачи

* Загрузить и установить программный анализатор системы безопасности.
* Выполнить тестирование узла для определения потенциальных мест, уязвимых для атаки.

Исходные данные / подготовка

Анализаторы системы безопасности – ценные средства, используемые сетевыми администраторами и инспекторами для выявления уязвимых мест сети и узла. Для тестирования безопасности узла и сети разработано много инструментальных средств анализа уязвимости, также известные как сканеры безопасности. В этой лабораторной работе предлагается загрузить и установить анализатор основных элементов защиты Microsoft Baseline Security Analyzer (MBSA). Инструментальное средство MBSA специально разработано для выявления потенциальных проблем нарушения безопасности, связанных с операционными системами, обновлениями и приложениями корпорации Microsoft. Оно также выявляет ненужные службы, которые, возможно, запущены на компьютере, а также все открытые порты.

Средство MBSA запускается в системах Windows Server или Windows XP и используется для поиска распространенных ошибок при настройке системы безопасности или отсутствующих обновлений безопасности для операционной системы, а также для большинства версий Internet Information Server (IIS), SQL Server, Internet Explorer (IE) и продуктов MS Office. MBSA предлагает конкретные способы устранения потенциальных проблем.

Эту лабораторную работу можно выполнять индивидуально или в группах по двое.

Для выполнения работы требуются следующие ресурсы:

* компьютер, на котором запущена операционная система Windows XP Professional,

выполняющий функцию тестируемой станции;

* высокоскоростное подключение к Интернету для загрузки средства MBSA (если оно предварительно не установлено);
* компьютер должен быть подсоединен к интегрированному коммутатору-маршрутизатору или автономному концентратору или коммутатору;
* дополнительно можно пользоваться сервером, на котором одновременно запущены

DHCP, HTTP, FTP и Telnet (предварительно настроенные).

Шаг 1. Загрузка и установка MBSA

а. Откройте обозреватель и перейдите на веб-страницу MBSA по адресу: <http://technet.microsoft.com/en-us/security/cc184924.aspx>

б. Какая последняя версия MBSA доступна?

в. Перечислите некоторые функции, предлагаемые средством MBSA.

г. Прокрутите страницу вниз и выберите язык, чтобы начать процесс загрузки.

д. Щелкните «Continue» (продолжить) для проверки установленной на компьютере копии

Microsoft Windows.

е. Щелкните кнопку «Download Files below» (загрузить следующие файлы) и выберите файл для загрузки. (Файл установки на английском языке: MBSASetup-EN.msi). Щелкните кнопку

«Download» (загрузить) справа от этого файла. Укажите размер загружаемого файла в мегабайтах. ж. При отображении диалогового окна «Загрузка файла – Предупреждении системы

безопасности» щелкните «Сохранить» и загрузите файл в указанную папку или на рабочий стол. Можно также запустить его с веб-узла загрузки программ.

з. По завершении загрузки убедитесь, что все остальные приложения закрыты. Дважды щелкните загруженный файл. Для запуска программы установки щелкните «Выполнить», и еще раз щелкните «Выполнить» при появлении предупреждения системы безопасности. На экране установки MBSA щелкните «Next» (далее).

и. Выберите соответствующий переключатель для принятия условий лицензионного соглашения и щелкните «Next» (далее). По мере выполнения процесса установки принимайте все параметры по умолчанию, а затем щелкните «Finish» (готово). На последнем экране программы установки MBSA щелкните кнопку «OK» и закройте папку, чтобы вернуться к рабочему столу Windows.

Шаг 2. Создание сети и настройка узлов

а. Подсоедините узел (узлы) к интегрированному маршрутизатору, концентратору или коммутатору, как показано на схеме топологии. Узел Host-А – это тестируемая станция, где установлено средство MBSA. Сервер можно не использовать.

б. Задайте IP-конфигурацию узла (узлов), используя окно "Сетевые подключения" Windows XP и свойства TCP/IP. Если узел подсоединен к интегрированному маршрутизатору, настройте его как DHCP-клиент. В противном случае перейдите к шагу 2в.

в. Если узел подсоединен к концентратору или коммутатору, а DHCP-сервер не доступен, настройте его вручную, присвоив ему статический IP-адрес.

Какие IP-адрес и маску подсети имеет узел Host-А и сервер (не обязательно)?

Шаг 3. Запуск на узле программы MBSA

а. Дважды щелкните значок MBSA на рабочем столе или запустите ее из меню «Пуск» > «Все программы». Какие параметры доступны при отображении главного экрана?

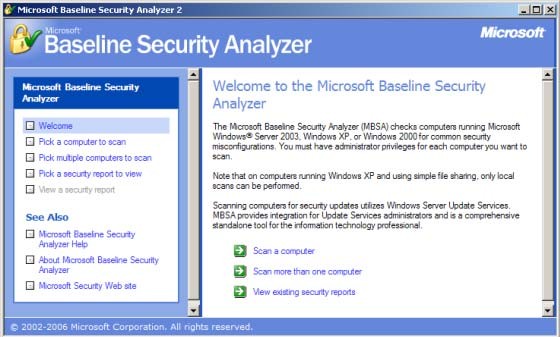


Рис. 11. Главное окно MBSA.

Шаг 4. Выбор компьютера для выполнения сканирования

а. В левой части экрана щелкните «Pick a computer to scan» (выберите компьютер для сканирования). По умолчанию отображается компьютер, на который установлена программа MBSA.

б. Какие два способа задания компьютера для сканирования существуют?

в. Укажите для выполнения сканирования компьютер по умолчанию. Снимите флажки «Check

for IIS administrative vulnerabilities» (поиск уязвимых мест IIS) и «Check for SQL administrative vulnerabilities» (поиск уязвимых мест SQL), поскольку маловероятно, что эти услуги установлены на сканируемом компьютере. Щелкните «Start Scan» (начать сканирование).

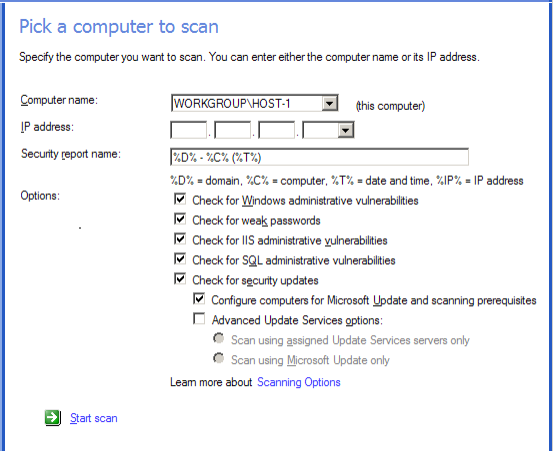


Рис. 12. Окно настройки параметров сканирования.

Шаг 5. Просмотр результатов поиска обновлений безопасности

а. Изучите отчет безопасности. Какие результаты получены в результате поиска обновлений безопасности?

б. При наличии красных или желтых символов "X" щелкните «How to correct this» (как

устранить эту проблему). Какое решение предлагается?

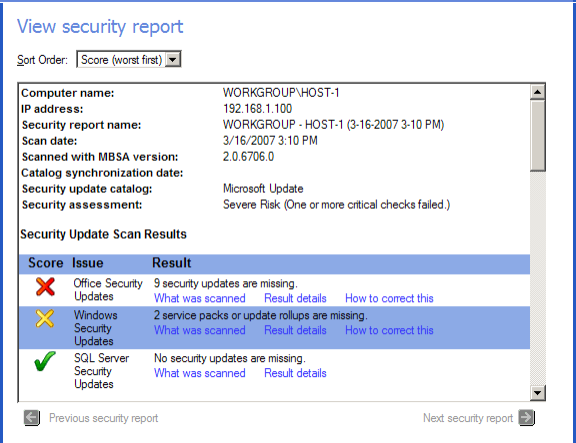


Рис. 13.

Отчет, получаем ый в результат е сканирова ния.

Шаг 6. Просмотр результат ов сканирова ния Windows в отчете безопасно сти

а.

Прокрутите отчет вниз и найдете второй раздел, содержащий результаты сканирования Windows («Windows Scan Results»). Были ли найдены какие-либо уязвимые места системы административной безопасности?

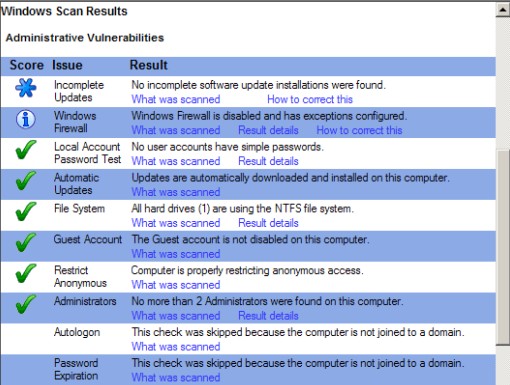


Рис. 14. Результат сканирования операционной системы.

б. В разделе «Additional System Information» (дополнительные сведения о системе) на экране (см. рис. 15) в столбце «Issue» (проблема) в строке «Services» (службы) щелкните «What was scanned» (что сканировалось) и «Result details» (подробные сведения) в столбце «Result» (результаты), чтобы прочесть описание выполненной проверки. Что вы обнаружили? По завершении закройте оба всплывающих окна и вернитесь к отчету безопасности.

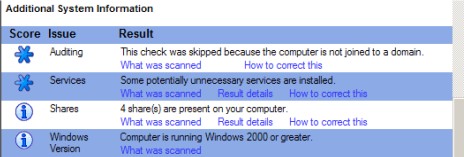


Рис. 15. Окно дополнительной информации.

Шаг 7. Просмотр результатов сканирования приложений для настольного компьютера в отчете безопасности

а. Прокрутите отчет вниз и найдите последний раздел, содержащий результаты сканирования приложений для настольного компьютера («Desktop Applications Scan Results», рис. 16). Были ли найдены какие-либо уязвимые места системы административной безопасности?

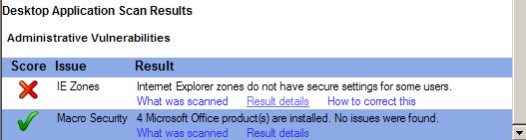


Рис. 16. Результат сканирования прикладных программ.

б. Сколько на компьютере установлено продуктов Microsoft Office? в. Были ли для какого-либо из них выявлены проблемы безопасности (см. «Macro Security» [защита от макросов])?

Шаг 8. Выполнение сканирования сервера, если он используется

а. Если в конфигурации доступен сервер с различными службами, на главном экране MBSA щелкните «Pick a computer to scan» (выберите компьютер для сканирования) и введите IP-адрес сервера, а затем щелкните «Start Scan» (начать сканирование). Какие уязвимые места в системе безопасности были выявлены?

б. Установлены ли на нем потенциально бесполезные службы? Укажите номер порта, на

котором они работают.

Шаг 9. Удаление MBSA с компьютера с использованием функции «Установка и удаление программ» на «Панели управления»

а. Этот шаг необязателен, и его выполнение зависит от того, выполняется ли в дальнейшем автоматическое восстановление узла в процессе работы сети.

б. Чтобы удалить MBSA с компьютера, щелкните «Пуск» > «Панель управления» > «Установка и удаление программ». Найдите приложение MBSA и удалите его. В списке оно отображается как Microsoft Baseline Security Analyzer 2.0.1 (или номер другой загруженной версии). Щелкните

«Удалить», а затем щелкните «Да» для подтверждения удаления приложения MBSA. По завершении закройте все окна и вернитесь к рабочему столу.

Вопросы для обсуждения

а. Инструментальное средство MBSA предназначено для поиска уязвимых мест на компьютерах, на которых установлена ОС Windows. Найдите в Интернете другие аналогичные инструментальные средства. Перечислите некоторые из найденных инструментов.

б. Какие инструментальные средства могут использоваться для компьютеров, на которых

установлена операционная система, отличная от Windows? Найдите в Интернете другие инструментальные средства и перечислите некоторые из них.

в. Какие другие шаги можно предпринять для повышения защищенности компьютера от атак из Интернета?

**III.** **Комплект материалов для промежуточной аттестации**

|  |
| --- |
| **Наименование модуля задания** |
| **Модуль 1: Настройка сетевой инфраструктуры** |
| Задание модуля 1:  Образец задания для демонстрационного экзамена по комплекту оценочной документации. |
| Предисловие: |
| Администрирование сетей и систем является одной из ключевых задач при создании и поддержке информационной инфраструктуры организации. Качественная настройка и управление сетевыми компонентами, серверами и сервисами играет важную роль в обеспечении стабильной и безопасной работы всей системы. |
| Данное задание представляет собой комплексную программу по администрированию, которая включает в себя несколько модулей. Каждый модуль охватывает различные аспекты настройки и поддержки системы, начиная с базовой конфигурации устройств и заканчивая реализацией сложных сервисов и технологий. |
| Модуль А посвящен базовой настройке устройств, включая присвоение имен, расчет IP-адресации и настройку внутренней динамической маршрутизации. Эти шаги позволяют создать основу для дальнейшего развития и масштабирования сети. |
| Модуль Б фокусируется на настройке DNS-сервера, синхронизации времени между устройствами, реализации файлового SMB(NFS)-сервера и других сервисов, таких как мониторинг и центр сертификации. Все эти шаги направлены на обеспечение безопасности, доступности и функциональности системы. |
| Модуль В включает в себя настройку защищенного туннеля между офисами, управление трафиком и конфигурирование веб- сервера. Эти меры способствуют обеспечению безопасности коммуникаций, контролю трафика и предоставлению доступа к веб-приложениям. |
| Цель данного задания состоит в том, чтобы разработать и настроить комплексную систему, которая удовлетворяет требованиям безопасности, функциональности и производительности. Работа в рамках этого задания требует глубоких знаний и навыков в области администрирования сетей и систем, а также умения применять современные технологии и методы для достижения поставленных целей.  Учтите, что в некоторых заданиях необходимо составить отчёт о проделанной работе в электронном виде. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Топология сети    **Задание 1 модуля 1**   1. Выполните базовую настройку всех устройств:    1. Присвоить имена в соответствии с топологией    2. Рассчитайте IP-адресацию IPv4 и IPv6. Необходимо заполнить таблицу №1, чтобы эксперты могли проверить ваше рабочее место.    3. Пул адресов для сети офиса BRANCH - не более 16    4. Пул адресов для сети офиса HQ - не более 64   Таблица №1   |  |  | | --- | --- | | **Имя устройства** | **IP** | | CLI |  | | ISP |  | | HQ-R |  | | HQ-SRV |  | | BR-R |  | | BR-SRV |  | | HQ-CLI |  | | HQ-AD |  | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. Настройте внутреннюю динамическую маршрутизацию по средствам FRR. Выберите и обоснуйте выбор протокола динамической маршрутизации из расчёта, что в дальнейшем сеть будет масштабироваться.    1. Составьте топологию сети L3. 2. Настройте автоматическое распределение IP-адресов на роутере HQ-R.    1. Учтите, что у сервера должен быть зарезервирован адрес. 3. Настройте локальные учётные записи на всех устройствах в соответствии с таблицей 2.   Таблица №2  **Учётная Пароль Примечание запись**  Admin P@ssw0rd CLI HQ-SRV HQ-R  Branch admin P@ssw0rd BR-SRV BR-R Network P@ssw0rd HQ-R BR-R BR- admin SRV     1. Измерьте пропускную способность сети между двумя узлами HQ-R-ISP по средствам утилиты iperf 3. Предоставьте описание пропускной способности канала со скриншотами. 2. Составьте backup скрипты для сохранения конфигурации сетевых устройств, а именно HQ-R BR-R. Продемонстрируйте их работу. 3. Настройте подключение по SSH для удалённого конфигурирования устройства HQ-SRV по порту 2222. Учтите, что вам необходимо перенаправить трафик на этот порт по средствам контролирования трафика. 4. Настройте контроль доступа до HQ-SRV по SSH со всех устройств, кроме CLI. | | | | |
| **Модуль 2:** **Организация сетевого администрирования** | | | | |
| Задание модуля 2   1. Настройте DNS-сервер на сервере HQ-SRV:    1. На DNS сервере необходимо настроить 2 зоны Зона hq.work, также не забудьте настроить обратную зону.   **Имя Тип записи Адрес**  hq-r.hq.work A, PTR IP-адрес  hq-srv.hq.work A, PTR IP-адрес  Зона branch.work | | | | |
|  | **Имя** | **Тип записи** | **Адрес** |  |
| br-r.branch.work | A, PTR | IP-адрес |
| br-srv.branch.work | A | IP-адрес |

1. Настройте синхронизацию времени между сетевыми устройствами по протоколу NTP.
   1. В качестве сервера должен выступать роутер HQ-R со стратумом 5
   2. Используйте Loopback интерфейс на HQ-R, как источник сервера времени
   3. Все остальные устройства и сервера должны синхронизировать свое время с роутером HQ-R
   4. Все устройства и сервера настроены на московский часовой пояс (UTC +3)
2. Настройте сервер домена выбор, его типа обоснуйте, на базе HQ-SRV через web интерфейс, выбор технологий обоснуйте.
   1. Введите машины BR-SRV и CLI в данный домен
   2. Организуйте отслеживание подключения к домену
3. Реализуйте файловый SMB или NFS (выбор обоснуйте) сервер на базе сервера HQ-SRV.
   1. Должны быть опубликованы общие папки по названиям:
      1. Branch\_Files - только для пользователя Branch admin;
      2. Network - только для пользователя Network admin;
      3. Admin\_Files - только для пользователя Admin;
   2. Каждая папка должна монтироваться на всех серверах в папку /mnt/<name\_folder> (например,

/mnt/All\_files) автоматически при входе доменного пользователя в систему и отключаться при его выходе из сессии. Монтироваться должны только доступные пользователю каталоги.

1. Сконфигурируйте веб-сервер LMS Apache на сервере BR- SRV:
   1. На главной странице должен отражаться номер места
   2. Используйте базу данных mySQL

Создайте пользователей в соответствии с таблицей, пароли у всех пользователей «P@ssw0rd»

|  |  |
| --- | --- |
| Пользователь | Группа |
| Admin | Admin |
| Manager1 | Manager |
| Manager2 | Manager |
| Manager3 | Manager |
| User1 | WS |
| User2 | WS |
| User3 | WS |
| User4 | WS |
| User5 | TEAM |
| User6 | TEAM |
| User7 | TEAM |

1. Запустите сервис MediaWiki используя docker на сервере HQ-SRV.
   1. Установите Docker и Docker Compose.
   2. Создайте в домашней директории пользователя файл wiki.yml для приложения MediaWiki:
   3. Средствами docker compose должен создаваться стек контейнеров с приложением MediaWiki и базой данных
   4. Используйте два сервиса;
   5. Основной контейнер MediaWiki должен называться wiki и использовать образ mediawiki;
   6. Файл LocalSettings.php с корректными настройками должен находиться в домашней папке пользователя и автоматически монтироваться в образ;
   7. Контейнер с базой данных должен называться db и использовать образ mysql;
   8. Он должен создавать базу с названием mediawiki, доступную по стандартному порту, для пользователя wiki с паролем DEP@ssw0rd;
   9. База должна храниться в отдельном volume с названием dbvolume.

MediaWiki должна быть доступна извне через порт 8080.

**Модуль 3:** **Эксплуатация объектов сетевой инфраструктуры**

Задание модуля 3:

1. Реализуйте мониторинг по средствам rsyslog на всех Linux хостах.
   1. Составьте отчёт о том, как работает мониторинг
2. Выполните настройку центра сертификации на базе HQ- SRV:
   1. Выдайте сертификаты для SSH;
   2. Выдайте сертификаты для веб серверов;
3. Настройте SSH на всех Linux хостах:
   1. Banner ( Authorized access only! );
   2. Установите запрет на доступ root;
   3. Отключите аутентификацию по паролю;
   4. Переведите на нестандартный порт;
   5. Ограничьте ввод попыток до 4;
   6. Отключите пустые пароли;
   7. Установите предел времени аутентификации до 5 минут;
   8. Установите авторизацию по сертификату выданным HQ-SRV
4. Реализуйте антивирусную защиту по средствам ClamAV на устройствах HQ-SRV и BR-SRV:
   1. Настройте сканирование системы раз в сутки с сохранением отчёта

Учтите, что сканирование должно проводится при условии, что от пользователей нет нагрузки

1. Настройте систему управления трафиком на роутере BR-R для контроля входящего трафика в соответствии со следующими правилами:
   1. Разрешите подключения к портам DNS (порт 53), HTTP (порт 80) и HTTPS (порт 443) для всех клиентов. Эти порты необходимы для работы настраиваемых служб.
   2. Разрешите работу выбранного протокола организации защищенной связи. Разрешение портов должно быть выполнено по принципу "необходимо и достаточно".
   3. Разрешите работу протоколов ICMP (протокол управления сообщениями Internet).
   4. Разрешите работу протокола SSH (Secure Shell) (SSH используется для безопасного удаленного доступа и управления устройствами).
   5. Запретите все прочие подключения.
   6. Все другие подключения должны быть запрещены для обеспечения безопасности сети.
2. Настройте виртуальный принтер с помощью CUPS для возможности печати документов из Linux-системы на сервере BR-SRV.
3. Между офисами HQ и BRANCH установите защищенный туннель, позволяющий осуществлять связь между регионами с применением внутренних адресов.
4. По средствам уже настроенного мониторинга установите следующие параметры:
   1. Warning
      1. Нагрузка процессора больше или равна 70%
      2. Заполненность оперативной памяти больше или равна 80%
      3. Заполненность диска больше или равна 85%
   2. Напишите план действия при получении Warning сообщений
5. Настройте программный RAID 5 из дисков по 1 Гб, которые подключены к машине BR-SRV.
6. Настройте Bacula на сервере HQ-SRV для резервного копирования etc на сервере BR-SRV