

**НЕКОММЕРЧЕСКОЕ АККРЕДИТОВАННОЕ ЧАСТНОЕ
ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«НЕВИННОМЫССКИЙ ЭКОНОМИКО-ПРАВОВОЙ ТЕХНИКУМ»**

МЕТОДИЧЕСКОЕ ПОСОБИЕ

**ОРГАНИЗАЦИЯ
САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ
По дисциплине ОП.11 Компьютерные сети
для студентов специальности 09.02.07 Информационные системы и
программирование**

АВТОР- СОСТАВИТЕЛЬ: Александров А.В., преподаватель НАЧ ПОУ НЭПТ

Организация самостоятельной работы обучающихся в контексте реализации ФГОС нового поколения по дисциплине «Компьютерные сети»: методическое пособие / авт.-сост.: Александров А.В.

Методические рекомендации предназначены для студентов с целью сопровождения и рекомендаций по организации самостоятельной работы обучающихся, ее назначению, планированию, форм организации и видов контроля.

ВВЕДЕНИЕ

1. Общие положения

Под самостоятельной работой студентов (СРС) понимается планируемая учебная, учебно-исследовательская, а также научно-исследовательская работа студентов, которая выполняется во внеаудиторное время по инициативе студента или по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Целью самостоятельной работы студентов: является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;
- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений;
- использование материала, собранного и полученного в ходе самостоятельных занятий на семинарах, на практических и лабораторных занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к итоговым зачетам и экзаменам.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы.

1. Подготовительный этап включает определение целей, задач, составление программы (плана) с указанием видов работы, её сроков, результатов и форм контроля, подготовку методического обеспечения, согласование самостоятельной работы с преподавателем.

2. Основной этап состоит в реализации программы УД в части самостоятельной работы, использовании приемов поиска информации, усвоении, переработке, применении и передаче знаний, фиксировании результатов работы. На основном этапе студент может получить консультации и рекомендации у преподавателя, руководящего его самостоятельной работой.

3. Заключительный этап означает анализ результатов и их систематизацию, контроля качества, продуктивности и эффективности проделанной работы, формулирование выводов о дальнейших направлениях работы.

Компетенции обучающегося, формируемые в результате выполнения самостоятельной работы:

- организация собственной деятельности, определение методов и способов выполнения профессиональных задач, оценивание их эффективности и качества;
- осуществление поиска, анализа и оценки информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного

развития;

- использование информационно-коммуникационных технологий для совершенствования профессиональной деятельности;
- работа в коллективе и команде, обеспечение ее сплочения, эффективное общение с коллегами;
- самостоятельное определение задач профессионального и личностного развития, самообразование;
- подготовка к смене технологий в профессиональной деятельности.

Формы контроля:

В качестве форм и методов контроля внеаудиторной самостоятельной работы студентов могут быть использованы семинарские занятия, тестирование, контрольные работы, защита творческих работ и электронных презентаций, проверка выполнения самостоятельной работы преподавателем, отчет о проделанной работе, защита рефератов.

Критериями оценок результатов внеаудиторной самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- умения студента активно использовать электронные образовательные ресурсы, находить требующуюся информацию, изучать ее и применять на практике;
- обоснованность и четкость изложения ответа;
- оформление материала в соответствии с требованиями;
- умение ориентироваться в потоке информации, выделять главное;
- умение четко сформулировать проблему, предложив ее решение, критически оценить решение и его последствия;
- умение показать, проанализировать альтернативные возможности, варианты действий;
- умение сформировать свою позицию, оценку и аргументировать ее.

2. Методические указания к выполнению самостоятельной работы

Работа с книгой.

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Методические рекомендации по составлению конспекта:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта;
2. Выделите главное, составьте план;

3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора;
4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

Практические занятия.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Самопроверка.

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется, используя лист опорных сигналов, воспроизвести по памяти определения, выводы формул, формулировки основных положений и доказательств.

В случае необходимости нужно еще раз внимательно разобраться в материале.

Консультации

Если в процессе самостоятельной работы над изучением теоретического материала или при решении задач у студента возникают вопросы, разрешить которые самостоятельно не удастся, необходимо обратиться к преподавателю для получения у него разъяснений или указаний. В своих вопросах студент должен четко выразить, в чем он испытывает затруднения, характер этого затруднения. За консультацией следует обращаться и в случае, если возникнут сомнения в правильности ответов на вопросы самопроверки.

Подготовка к экзамену.

Изучение дисциплины завершается экзаменом. Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На экзамене студент демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине.

Вначале следует просмотреть весь материал по сдаваемой дисциплине, отметить для себя трудные вопросы. Обязательно в них разобраться. В заключение еще раз целесообразно повторить основные положения, используя при этом листы опорных сигналов.

Систематическая подготовка к занятиям в течение семестра позволит использовать время экзаменационной сессии для систематизации знаний.

Правила написания научных текстов (рефератов, курсовых и дипломных работ):

- важно разобраться сначала, какова истинная цель научного текста;
- важно разобраться, кто будет «читателем» работы;
- писать следует ясно и понятно, основные положения необходимо формулировать четко и недвусмысленно (чтобы и самому понятно было), а также стремясь структурировать свой текст
- объем текста и различные оформительские требования во многом зависят от принятых в колледже требований.

**Таблица 1 - Технологическая карта самостоятельной работы студента по дисциплине «Компьютерные сети»
специальность 09.02.07 -Информационные системы и программирование**

Наименование темы	Тематика самостоятельной работы	Кол-во часов	Виды самостоятельной работы		Информационное обеспечение	Форма контроля
			Обязательная	По выбору студента		
Тема 7. Адресация в сетях	Доклад на темы: «Преобразование IP-адресов», «Определение маски подсети», «Статическая и динамическая маршрутизация».	4	Подготовка доклада	презентация	Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2023. — 333 с. — (Профессиональное образование). — ISBN 978-5-534-04638-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/513518	Защита доклада/ презентации

Курс лекций

Лекция 1-2

Спецификации и топологии сети

1. Топологии сети.
2. Полносвязная топология.
3. Шинная топология.
4. Звездообразная топология.
5. Кольцеобразная топология.
6. Коммутирующая топология.
7. Выбор топологии.
8. Вопросы и задания

1. Топология сети

Сетевая технология – это согласованный набор стандартных протоколов и реализующих их программно-аппаратных средств (например, сетевых адаптеров, драйверов, кабелей и разъемов), достаточный для построения вычислительной сети.

Иногда сетевые технологии называют базовыми технологиями, имея в виду, что на их основе строится базис любой сети. При построении сети в первую очередь необходимо выбрать способ организации физических связей, т.е. топологию.

Под *топологией* вычислительной сети понимается конфигурация графа, вершинам которого соответствуют компьютеры сети (иногда другое оборудование), а ребрам – физические связи между ними. Компьютеры, подключенные к сети, часто называют станциями или узлами сети. Конфигурация физических связей определяется электрическими соединениями компьютеров между собой и может отличаться от логических связей. Логические связи образуются путем соответствующей настройки оборудования. Рассмотрим наиболее часто встречаемые топологии.

2. Полносвязная топология — топология компьютерной сети, в которой каждая рабочая станция подключена ко всем остальным. Этот вариант является громоздким и неэффективным, несмотря на свою логическую простоту. Для каждой пары должна быть выделена независимая линия, каждый компьютер должен иметь столько коммуникационных портов сколько компьютеров в сети. По этим причинам сеть может иметь только сравнительно небольшие конечные размеры. Чаще всего эта топология используется в многомашинных комплексах или глобальных сетях при малом количестве рабочих станций.

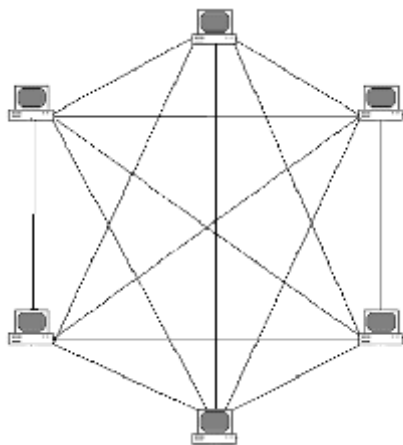


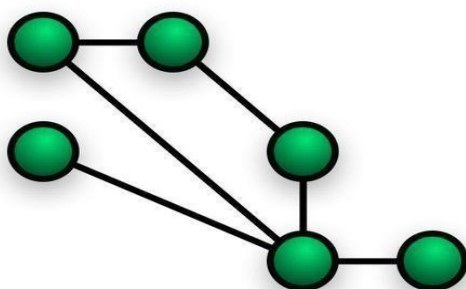
Рис. 1. Полносвязная топология

Недостатки

□ Очень много проводки Все другие варианты основаны на неполносвязных топологиях, когда для обмена данными между двумя компьютерами сети могут понадобиться промежуточные передачи данных через другие компьютеры сети.

Ячеистая топология — базовая полносвязная топология компьютерной сети, в которой каждая рабочая станция сети соединяется со всеми другими рабочими станциями этой же сети. Характеризуется высокой отказоустойчивостью, сложностью настройки и преизбыточным расходом кабеля. Каждый компьютер имеет множество возможных путей соединения с другими компьютерами. Обрыв кабеля не приведёт к потере соединения между двумя компьютерами.

Ячеистая топология



MyShared

Рис. 2. Ячеистая топология

Ячеистая топология (mesh) получается из полносвязной путем удаления некоторых возможных связей. В сети с ячеистой топологией непосредственно связывают только те компьютеры, которые ведут интенсивный обмен данными. Эта топология используется, как правило, в глобальных сетях.

3. Общая шина является очень распространенной, а до недавнего времени самой распространенной, топологией для локальных сетей. В этом случае компьютеры последовательно соединяются разомкнутым коаксиальным кабелем, образуя длинную

цепочку. Передаваемая информация может распространяться в обе стороны. Применение общей шины снижает стоимость проводки, унифицирует подключение различных модулей, обеспечивает возможность широковещательного обращения ко всем станциям сети. Таким образом, основным *преимуществом* такой топологии является дешевизна и простота разводки кабеля по помещениям.

Самый серьезный *недостаток* общей шины заключается в ее низкой надежности: любой дефект кабеля или какого-либо из многочисленных разъемов парализует всю сеть. Общий кабель является узким местом сети не только по надежности. Но и по производительности, так как он разделяется всеми станциями сети. Топология типа шина, представляет собой общий кабель (называемый шина или магистраль), к которому подсоединены все рабочие станции. На концах кабеля находятся терминаторы, для предотвращения отражения сигнала.

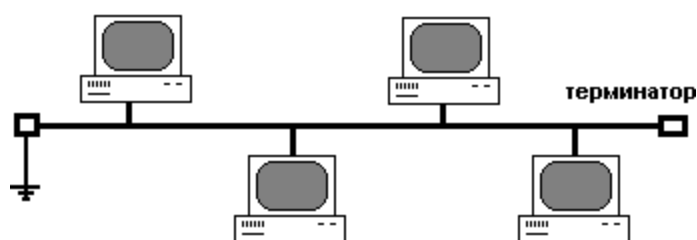


Рис. 3. Шинная топология

Работа в сети

Отправляемое рабочей станцией сообщение распространяется на все компьютеры сети. Каждая машина проверяет — кому адресовано сообщение и если ей, то обрабатывает его. Для того, чтобы исключить одновременную посылку данных, применяется либо «несущий» сигнал, либо один из компьютеров является главным и «даёт слово» остальным станциям. Шина своей структурой допускает идентичность сетевого оборудования компьютеров, а также равноправие всех абонентов. При таком соединении компьютеры могут передавать только по очереди, потому что линия связи единственная. В противном случае переданная информация будет искажаться в результате наложения (конфликту, коллизии).

Таким образом, в шине реализуется режим полудуплексного (half duplex) обмена (в обоих направлениях, но по очереди, а не одновременно). В топологии «шина» отсутствует центральный абонент, через которого передается вся информация, которая увеличивает ее надежность (ведь при отказе любого центра перестает функционировать вся управляемая этим центром система). Добавление новых абонентов в шину достаточно простое и обычно возможно даже во время работы сети. В большинстве случаев при использовании шины нужно минимальное количество соединительного кабеля по сравнению с другой топологией. Правда, нужно учесть, что к каждому компьютеру (кроме двух крайних) подходит два кабеля, что не всегда удобно.

Шине не страшны отказы отдельных компьютеров, потому что все другие компьютеры сети могут нормально продолжать обмен. Может показаться, что шине не страшен и обрыв кабеля, поскольку в этом случае мы одержимо две полностью работоспособных шины. Однако из-за особенности распространения электрических сигналов по длинным линиям связи необходимо предусматривать включение на концах шины специальных устройств — *терминаторов* (Терминатор (электроника) — поглотитель энергии (обычно резистор) на конце длинной линии, сопротивление которого равно волновому сопротивлению линии.). Без включения терминаторов сигнал отражается от конца линии и искажается так, что связь по сети становится невозможной. Так что при разрыве или повреждении кабеля нарушается согласование

линии связи, и прекращается обмен даже между теми компьютерами, которые остались соединенными между собой. Короткое замыкание в любой точке кабеля шины выводит из строя всю сеть. Любой отказ сетевого оборудования в шине очень трудно локализовать, потому что все адаптеры включены параллельно, и понять, который из них вышел из строя, не так-то просто. При построении больших сетей возникает проблема ограничения на длину связи между узлами, в таком случае сеть разбивают на сегменты. Сегменты соединяются различными устройствами — повторителями, концентраторами или хабами. Например, технология Ethernet позволяет использовать кабель длиной не более 185 метров.



Рис. 4. Соединение сегментов в шинной топологии

Сравнение с другими топологиями Достоинства

- Небольшое время установки сети;
- Дешевизна (требуется меньше кабеля и сетевых устройств);
- Простота настройки;
- Выход из строя рабочей станции не отражается на работе сети.

Недостатки

- Любые неполадки в сети, как обрыв кабеля, выход из строя терминатора полностью уничтожают работу всей сети;
- Сложная локализация неисправностей;
- С добавлением новых рабочих станций падает производительность сети.

Шинная топология представляет собой топологию, в которой все устройства локальной сети подключаются к линейной сетевой среде передачи данных. Такую линейную среду часто называют каналом, шиной или трассой. Каждое устройство, например, рабочая станция или сервер, независимо подключается к общему шинному кабелю с помощью специального разъема. Шинный кабель должен иметь на конце согласующий резистор, или терминатор, который поглощает электрический сигнал, не давая ему отражаться и двигаться в обратном направлении по шине.

Преимущества и недостатки шинной топологии

Типичная шинная топология имеет простую структуру кабельной системы с короткими отрезками кабелей. Поэтому по сравнению с другими топологиями стоимость ее реализации невелика. Однако низкая стоимость реализации компенсируется высокой стоимостью управления. Фактически, самым большим недостатком шинной топологии является то, что диагностика ошибок и изолирование сетевых проблем могут быть довольно сложными, поскольку здесь имеются несколько

точек концентрации. Так как среда передачи данных не проходит через узлы, подключенные к сети, потеря работоспособности одного из устройств никак не сказывается на других устройствах. Хотя использование всего лишь одного кабеля может рассматриваться как достоинство шинной топологии, однако оно компенсируется тем фактом, что кабель, используемый в этом типе топологии, может стать критической точкой отказа. Другими словами, если шина обрывается, то ни одно из подключенных к ней устройств не сможет передавать сигналы.

Примеры

Сегмент компьютерной сети, использующей коаксиальный кабель в качестве носителя и подключенных к этому кабелю рабочих станций. В этом случае шиной будет являться отрезок коаксиального кабеля, к которому подключены компьютеры.

4. Звезда – это вариант топологии, когда каждый компьютер подключается отдельным кабелем к общему устройству, называемому концентратором, который находится в центре воображаемой звезды. В функции концентратора входит обеспечение доступа станциям к среде передачи данных. Для подсоединения компьютера к концентратору используется, как правило, витая пара.

Главное *преимущество* этой топологии перед общей шиной – значительное увеличение надежности. Любые неприятности с кабелем касаются лишь того компьютера, к которому этот кабель подсоединен, и только неисправность концентратора может вывести из строя всю сеть.

К *недостаткам* топологии типа звезда относится более высокая стоимость сетевого оборудования из-за необходимости приобретения концентратора.

Звезда — базовая топология компьютерной сети, в которой все компьютеры сети присоединены к центральному узлу (обычно сетевой концентратор), образуя физический сегмент сети. Подобный сегмент сети может функционировать как отдельно, так и в составе сложной сетевой топологии (как правило "дерево"). Весь обмен информацией идет исключительно через центральный компьютер, на который таким способом ложится очень большая нагрузка, потому ничем другим, кроме сети, оно заниматься не может. Как правило, именно центральный компьютер является самым мощным, и именно на него возлагаются все функции по управлению обменом. Никакие конфликты в сети с топологией звезда в принципе невозможны, потому что управление полностью централизовано.



Рис. 5. Звезда

Работа в сети

Рабочая станция, с которой нужно послать данные, отправляет их на концентратор, а тот определяет адресата и отдаёт ему информацию. В определённый момент времени только одна машина в сети может пересылать данные, если на концентратор одновременно приходят два пакета, обе посылки оказываются не принятыми и отправителям нужно будет подождать случайный промежуток времени,

чтобы возобновить передачу данных. Этот недостаток отсутствует на сетевом устройстве более высокого уровня - коммутаторе, который, в отличие от концентратора, подающего пакет на все порты, подает лишь на определенный порт - получателю. Одновременно может быть передано несколько пакетов.

Сколько - зависит от коммутатора

Активная звезда

В центре сети содержится компьютер, который выступает в роли сервера.

Пассивная звезда

В центре сети с данной топологией содержится не компьютер, а концентратор, или хаб (hub), что выполняет ту же функцию, что и репитер. Он возобновляет сигналы, которые поступают, и пересылает их в другие линии связи.

Сравнение с другими типами сетей Достоинства

- выход из строя одной рабочей станции не отражается на работе всей сети в целом; хорошая масштабируемость сети;
- лёгкий поиск неисправностей и обрывов в сети;
- высокая производительность сети (при условии правильного проектирования);
- гибкие возможности администрирования.

Недостатки

- выход из строя центрального концентратора обернётся неработоспособностью сети (или сегмента сети) в целом;
- для прокладки сети зачастую требуется больше кабеля, чем для большинства других топологий;
- конечное число рабочих станций в сети (или сегменте сети) ограничено количеством портов в центральном концентраторе.

Применение

Одна из наиболее распространённых топологий, поскольку проста в обслуживании. В основном используется в сетях, где носителем выступает кабель витая пара.

5. Кольцевая технология предусматривает передачу сигналов по кольцу от одной станции к другой, как правило, в одном направлении. Если станция не распознает пакет как —свой, то она передает его следующей в кольце станции. В сети с этой топологией необходимо принимать специальные меры, чтобы в случае выхода из строя или отключения какойлибо станции не прервался канал связи между остальными станциями.

Топология типа кольцо применяется, в основном, в локальных сетях.

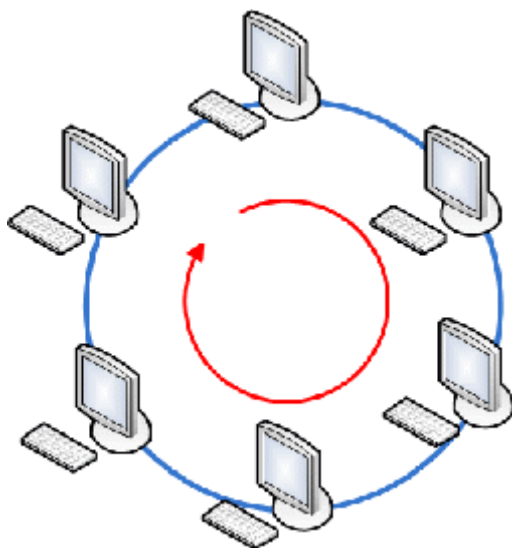


Рис. 6. Кольцо

Кольцо — это топология, в которой каждый компьютер соединен линиями связи только с двумя другими: от одного он только получает информацию, а другому только передает. На каждой линии связи, как и в случае звезды, работает только один передатчик и один приемник. Это позволяет отказаться от применения внешних терминаторов.

Работа в сети

Важна особенность кольца заключается в том, что каждый компьютер ретранслирует (возобновляет) сигнал, то есть выступает в роли репитера, потому затухание сигнала во всем кольце не имеет никакого значения, важно только затухание между соседними компьютерами кольца. Четко выделенного центра в этом случае нет, все компьютеры могут быть одинаковыми. Однако достаточно часто в кольце выделяется специальный абонент, который управляет обменом или контролирует обмен. Понятно, что наличие такого управляющего абонента снижает надежность сети, потому что выход его из строя сразу же парализует весь обмен. Компьютеры в кольце не являются полностью равноправными (в отличие, например, от шинной топологии). Одни из них обязательно получают информацию от компьютера, который ведет передачу в этот момент, раньше, а другие — позже.

Именно на этой особенности топологии и строятся методы управления обменом по сети, специально рассчитанные на «кольцо». В этих методах право на следующую передачу (или, как еще говорят, на захват сети) переходит последовательно к следующему по кругу компьютеру. Подключение новых абонентов в «кольцо» обычно совсем безболезненно, хотя и требует обязательной остановки работы всей сети на время подключения. Как и в случае топологии «шина», максимальное количество абонентов в кильке может быть достаточно большая (до тысячи и больше).

Кольцевая топология обычно является самой стойкой к перегрузкам, она обеспечивает уверенную работу с самими большими потоками переданной по сети информации, потому что в ней, как правило, нет конфликтов (в отличие от шины), а также отсутствует центральный абонент (в отличие от звезды). В кольце, в отличие от других топологий (звезда, шина), не используется конкурентный метод послышки данных, компьютер в сети получает данные от стоящего предыдущим в списке адресатов и перенаправляет их далее, если они адресованы не ему. Список адресатов генерируется компьютером, являющимся генератором маркера. Сетевой модуль генерирует маркерный сигнал (обычно порядка 2-10 байт во избежание затухания) и передает его следующей системе (иногда по возрастанию MAC-адреса). Следующая система, приняв сигнал, не анализирует его, а просто передает дальше. Это так

называемый нулевой цикл. Последующий алгоритм работы таков — пакет данных GRE, передаваемый отправителем адресату начинает следовать по пути, проложенному маркером. Пакет передаётся до тех пор, пока не доберётся до получателя.

Сравнение с другими топологиями Достоинства

- Простота установки;
- Практически полное отсутствие дополнительного оборудования;
- Возможность устойчивой работы без существенного падения скорости передачи данных при интенсивной загрузке сети, поскольку использование маркера исключает возможность возникновения коллизий.

Недостатки

- Выход из строя одной рабочей станции, и другие неполадки (обрыв кабеля), отражаются на работоспособности всей сети; □ Сложность конфигурирования и настройки;
- Сложность поиска неисправностей.

Применение

Наиболее широкое применение получила в оптоволоконных сетях. Используется в стандартах FDDI, Token ring.

Двойное кольцо - это сеть построенная на двух оптоволоконных кольцах, соединяющих компьютеры с двумя сетевыми картами кольцевой топологией. Для повышения отказоустойчивости, сеть строится на оптоволоконных кольцах образующих основной и резервный путь для передачи данных. Первое кольцо используется для передачи данных, а второе не используется. При выходе из строя 1-го кольца оно объединяется со 2-м и сеть продолжает функционировать. Данные при этом по первому кольцу передаются в одном направлении, а по второму в обратном. Используется маркерный метод доступа. Примером может быть сеть двойного кольца FDDI.

6. Коммутируемая топология

Коммутатор (switch) является многопортовым устройством канального уровня (второй уровень справочной модели OSI). Коммутатор «изучает» MAC-адреса и накапливает данные о них во внутренней таблице. Между автором кадра и предполагаемым получателем коммутатор создает временное соединение, по которому и передается кадр. В стандартной локальной сети, реализующей коммутируемую топологию, все соединения устанавливаются через коммутирующий концентратор (switching hub), что и проиллюстрировано на рисунке 8.

Каждому порту, а, следовательно, и подключенному к порту устройству, выделена собственная полоса пропускания. Первоначально принцип действия коммутаторов основывался на передаче кадров в соответствии с MAC-адресами, однако технологический прогресс внес свои коррективы. Современные устройства в состоянии коммутировать ячейки (пакеты кадров, имеющие фиксированную длину и соответствующие второму уровню структуры передачи данных). Кроме того, коммутаторы поддерживают протоколы третьего уровня, а также распознают IP-адреса и физические порты коммутатора-концентратора.

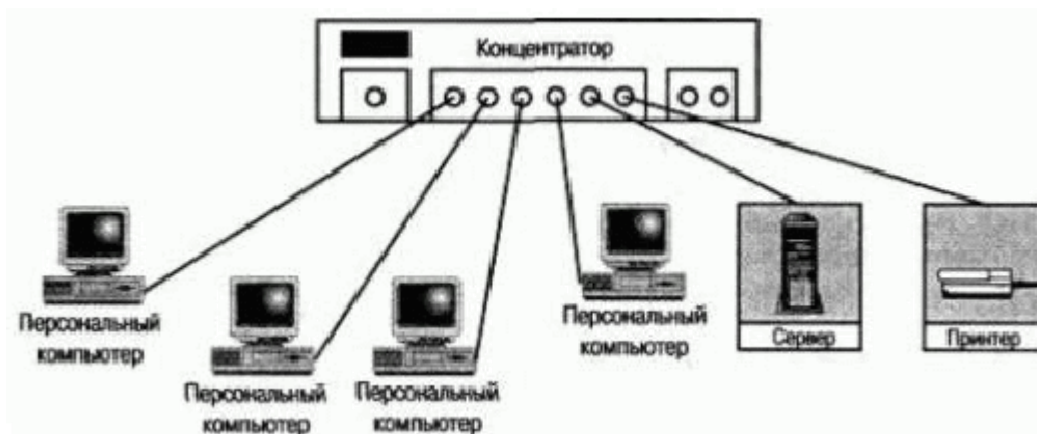


Рис. 7. Звездообразная топология.

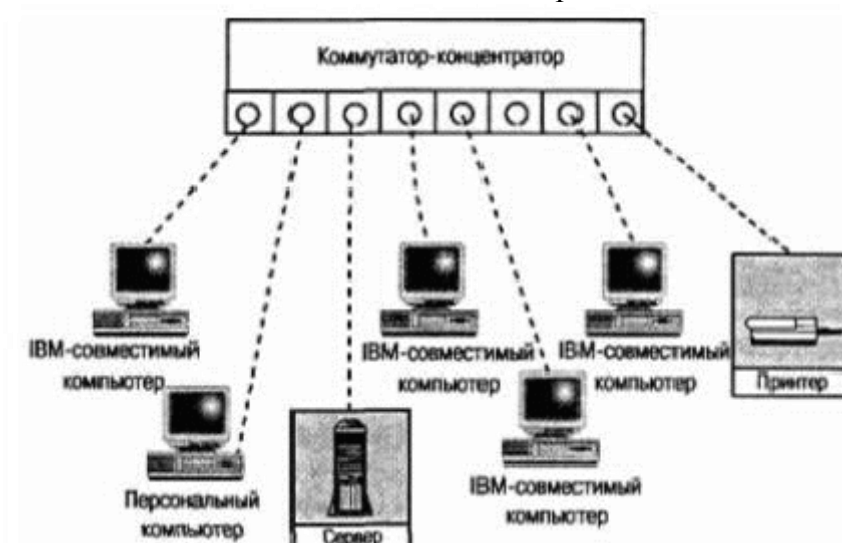


Рис. 8. Коммутируемая топология.

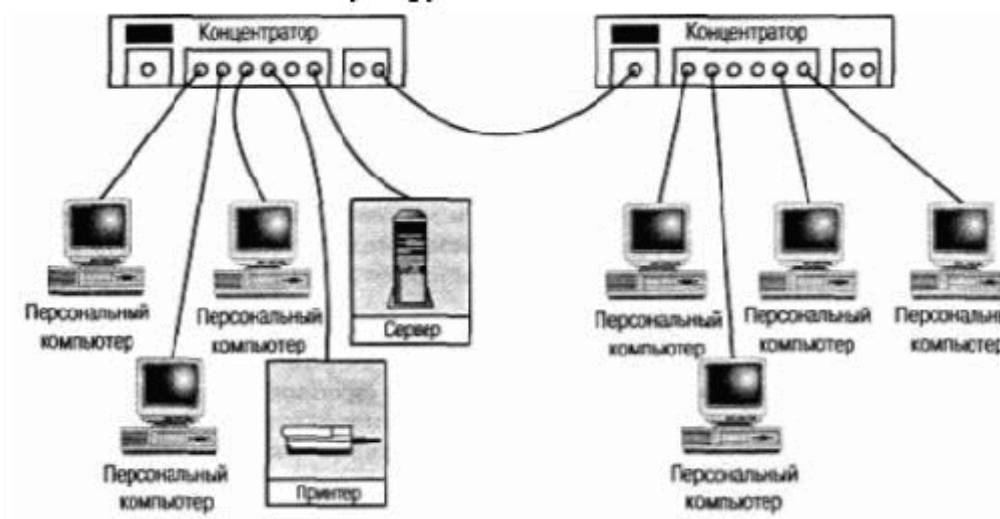


Рис. 9. Объединенные в последовательную цепочку концентраторы.

Коммутаторы повышают производительность локальной сети двумя способами. Первый способ заключается в расширении полосы пропускания, доступной сетевым устройствам. Например, коммутатор-концентратор Ethernet с восемью портами обладает таким же количеством отдельных доменов по 10 Мбит/с каждый,

обеспечивая суммарную пропускную способность 80 Мбит/с. Второй способ повышения производительности локальной сети сводится к уменьшению количества устройств, которые вынуждены использовать все сегменты полосы пропускания. В каждом выделенном коммутатором домене находятся только два устройства: собственно сетевое устройство и порт коммутатора-концентратора, к которому оно подключено. Вся полоса пропускания 10 Мбит/с принадлежит двум устройствам сегмента.

В сетях, которые не поддерживают конкурирующие методы доступа к среде передачи, например, в Token Ring или FDDI, область циркуляции маркера будет ограничена меньшим количеством сетевых устройств. Открытым вопросом остается изоляция трафика в больших сетях. Приемлемая производительность поддерживается исключительно сегментацией конфликтных, но не передающих доменов. Чрезмерно насыщенный трафик в значительной степени снижает производительность локальной сети.

7. Выбор подходящей топологии

Четыре рассмотренные топологии можно считать элементарными блоками для построения локальных сетей. Их можно комбинировать всевозможными способами и расширять. При выборе топологии следует учитывать в первую очередь требования к производительности сети конкретных приложений клиентов. Вполне вероятно, что идеальным вариантом окажется комбинация основных топологий, или так называемые сложные топологии.

Сложные топологии являются расширениями и/или комбинациями основных физических топологий. Сами по себе основные топологии целесообразно использовать только в небольших локальных сетях. Возможность расширения сетей основных топологий чрезвычайно ограничена. Гораздо выгоднее оказывается создать сложную топологию, объединив для этого в одну локальную сеть сегменты различных топологий.

При выборе топологии локальной сети учитывается множество других критериев, как технических, так и финансовых. Общая топология должна быть определена с точки зрения требований пользователя к производительности. При выборе и/или доработке топологии следует учитывать максимальное количество критериев.

Стоимость

Придумать топологию сети с абсолютно фантастической стоимостью не составит никакого труда. Но даже очень богатые компании выделяют на развертывание сети фиксированную сумму. Реализуемая топология должна иметь оптимальное соотношение стоимость/соответствие требованиям пользователей.

Использование устаревшего оборудования

Множество причин могут помешать воплотить идеальную во всех отношениях топологию. Физическая проводка и расположение рабочих станций в здании вполне могут оказаться причинами отказа от развертывания планируемой топологии. Замена проводки в значительной степени увеличит стоимость проекта. Аналогично если компания имеет значительные вложения в устаревшие технологии, вряд ли удастся развернуть «идеальную сеть» и топологию. И наконец, недостаточное финансирование также сведет на нет все старания проектировщиков сети. Все перечисленные причины вносят свою лепту в постепенный отказ от идеальной топологии. Именно поэтому они должны быть тщательно проанализированы и учтены перед приобретением необходимого оборудования.

Виды на будущее

Было бы глупо разрабатывать сеть, не учитывая при этом обстоятельства, которые могут возникнуть в обозримом будущем. Новинки сетевых и компьютерных технологий, изменение трафика и/или расположения сетевых устройств и миллионы других факторов могут в значительной степени изменить представления пользователей о должной производительности сети. Сеть и ее топология должны быть достаточно гибкими для реагирования на будущие изменения.

Выводы

Топология локальной сети является одним из самых критичных факторов, влияющих на производительность. В случае необходимости четыре основные топологии (коммутируемую, звездообразную, кольцевую и шинную) можно комбинировать произвольным образом. Возможные комбинации неограничены рассмотренными в этой лекции. Большинство современных технологий локальных сетей не только приветствуют, но даже обязывают использовать творческий подход. Очень важно разбираться в преимуществах и недостатках топологий, влияющих на производительность сети. Кроме того, следует учитывать и такие казалось бы необъективные факторы, как расположение рабочих станций в здании, пригодность кабеля, а также даже тип и способ проводки.

В конечном счете основным критерием выбора удачной топологии являются *требования пользователей к производительности*. Такие факторы, как стоимость, предполагаемая модернизация и ограничения существующих технологий, играют второстепенную роль. Сложнее всего будет перевести устные пожелания пользователей в мегабиты в секунду (Мбит/с) и другие характеристики производительности сети.

Вопросы и задания

1. Что такое «сетевая технология»?
2. Что такое «топология»?
3. Перечислите и кратко охарактеризуйте основные топологии.
4. Опишите коммутируемую топологию.
5. Приведите пример сложной топологии.
6. Какие критерии следует учитывать при выборе топологии сети?

Лекция 3-4 Модель OSI 1. Модели межсетевого взаимодействия 2. Модель OSI 3. Модель TCP/IP 4. Вопросы Модели межсетевого взаимодействия (модель OSI, модель TCP/IP) Модели межсетевого взаимодействия предназначены для формального и в то же время наглядного описания взаимодействия сетевых узлов между собой. В настоящее время наибольшее распространение получили и являются стандартами для описания межсетевого взаимодействия две сетевые модели: модель OSI и модель TCP/IP. Обе модели разбивают процесс взаимодействия сетевых узлов на несколько уровней, каждый конкретный уровень одного узла обменивается информацией с соответствующим уровнем другого узла. Каждую из этих моделей можно представлять как объединение двух моделей: □ горизонтальная модель (на базе протоколов, обеспечивающая обмен данными одного типа между программами и процессами,

работающими на одном и том же уровне на различных сетевых узлах); □ вертикальная модель (на основе услуг, предоставляемых соседними уровнями друг другу на одном сетевом узле). В горизонтальной модели двум программам, работающими на различных сетевых узлах, требуется общий протокол для обмена данными. В

вертикальной — соседние уровни обмениваются данными, выполняя необходимые преобразования с использованием соответствующих программных интерфейсов. Модель OSI В 1983 году с целью упорядочения описания принципов взаимодействия устройств в сетях Международная организация по стандартизации (International Organization for Standardization, ISO) предложила семиуровневую эталонную коммуникационную модель "Взаимодействие Открытых Систем", модель OSI (Open System Interconnection). Эталонная модель OSI сводит передачу информации в сети к семи относительно простым подзадачам. Модель OSI стала основой для разработки стандартов на взаимодействие систем. Она определяет только схему выполнения необходимых задач, но не дает конкретного описания их выполнения. Это описывается конкретными протоколами или правилами, разработанными для определенной технологии с учетом модели OSI. Уровни OSI могут реализовываться как аппаратно, так и программно. Основная идея модели OSI в том, что одни и те же уровни на разных системах, не имея возможности связываться непосредственно, должны работать абсолютно одинаково. Одинаковым должен быть и сервис между соответствующими уровнями различных систем. Нарушение этого принципа может привести к тому, что информация, посланная от одной системы к другой, после всех преобразований не будет идентична исходной. Существует семь основных уровней модели OSI (табл. 1.1). Они начинаются с физического уровня и заканчиваются прикладным. Каждый уровень предоставляет услуги для более высокого уровня. Седьмой уровень обслуживает непосредственно пользователей. ПМ.01. УЧАСТИЕ В ПРОЕКТИРОВАНИИ СЕТЕВОЙ

ИНФРАСТРУКТУРЫ ОГАПОУ БПК, Н.С.Пыхтина Таблица 1.1. 7.

Прикладной (Application) 6. Представления (Presentation) 5. Сеансовый (Session) 4. Транспортный (Transport) 3. Сетевой (Network) 2. Канальный (Data Link) 1. Физический (Physical) Модель OSI описывает путь информации через сетевую среду от одной прикладной программы на одном компьютере до другой программы на другом компьютере. При этом пересылаемая информация проходит вниз через все уровни системы. Уровни на разных системах не могут общаться между собой напрямую. Это умеет только физический уровень. По мере прохождения информации вниз внутри системы она преобразуется в вид, удобный для передачи по физическим каналам связи. Для указания адресата к этой преобразованной информации добавляется заголовок с адресом. После получения адресатом этой информации, она проходит через все уровни вверх. По мере прохождения информация преобразуется в первоначальный вид. Каждый уровень системы должен полагаться на услуги, предоставляемые ему смежными уровнями. 1. Физический уровень. На данном уровне выполняется передача битов по физическим каналам (коаксиальный кабель, витая пара, оптоволокно). 2. Канальный уровень. Данный уровень определяет методы доступа к среде передачи данных и обеспечивает передачу кадра данных между любыми узлами в сетях с типовой топологией по физическому адресу сетевого устройства. Адреса, используемые на канальном уровне в локальных сетях, часто называют MACадресами (MAC — media access control, управление доступом к среде передачи данных). 3. Сетевой уровень. Обеспечивает доставку данных между любыми двумя узлами в сети с произвольной топологией, при этом не гарантируется надежная доставка данных от узлаотправителя к узлу-получателю. На этом уровне выполняются такие функции как маршрутизация логических адресов сетевых узлов, создание и ведение таблиц маршрутизации, фрагментация и сборка данных. 4. Транспортный уровень. Обеспечивает передачу данных между любыми узлами сети с требуемым уровнем надежности. Для выполнения этой задачи на транспортном уровне имеются механизмы установления соединения между сетевыми узлами, нумерации, буферизации и упорядочивания пакетов, передаваемых между узлами сети. 5.

Сеансовый уровень. Реализует средства управления сессией, диалогом, а также предоставляет средства синхронизации в рамках процедуры обмена сообщениями, контроля над ошибками, обработки транзакций, поддержки вызова удаленных процедур RPC. 6. Уровень представления. На этом уровне могут выполняться различные виды преобразования данных, такие как компрессия и декомпрессия, шифровка и дешифровка данных. 7. Прикладной уровень. Набор сетевых сервисов, предоставляемых конечным пользователям и приложениям. Примеры таких сервисов — обмен сообщениями электронной почты, передача файлов между узлами сети, приложения управления сетевыми узлами. Функционирование первых трех уровней, физического, канального и сетевого, обеспечивается, в основном, активным сетевым оборудованием и, как правило, реализуются следующими компонентами: сетевыми адаптерами, репитерами, мостами, концентраторами, коммутаторами, маршрутизаторами. Модель TCP/IP Модель TCP/IP называют также моделью DARPA (сокращение от Defense Advanced Research Projects Agency, организация, в которой в свое время разрабатывались сетевые проекты, в том числе протокол TCP/IP, и которая стояла у истоков сети Интернет) или моделью Министерства обороны США (модель DoD, Department of Defense, проект DARPA работал по заказу этого ведомства). Историческая справка: Впервые о TCP/IP было сказано в 1973 году на заседании International Network Working Group, прошедшем в Великобритании. Здесь Роберт Кан и Винт Серф выступили с проектом статьи, которая позже, в мае 1974 года, была опубликована в одном из самых престижных журналов Transactions on Communications. В статье были изложены основы будущего протокола TCP/IP. Главная идея, предложенная авторами, состояла в том, чтобы перенести обеспечение надежности коммуникаций из сети в подключенные к ней серверы. Идея оказалась блестящей, она пришлась по вкусу и либерально настроенным ученым, и военным одновременно. После этого протокол начал жить своей жизнью, пока еще под названием TCP. К совершенствованию нового протокола приложили руку многие инженеры и ученые, и к октябрю 1977 года его работу удалось продемонстрировать не только в ARPAnet, но и в пакетной радиосети и спутниковой сети SATNET. Чуть позже инженеры пришли к выводу о необходимости разделить протокол на две части: так появились "близнецы-братья" TCP и IP. Часть TCP отвечает за разбиение сообщения на дейтаграммы на стороне отправителя, за сборку их на стороне получателя, обнаружение ошибок и восстановление порядка пакетов, если он был нарушен в процессе передачи. IP, или Internet Protocol, отвечает за маршрутизацию отдельных дейтаграмм. История создания TCP/IP ведет свое начало с момента, когда министерство обороны США столкнулось с проблемой объединения большого числа компьютеров с различными ОС. В 1970 г. был разработан необходимый набор стандартов. Протоколы, разработанные на базе этих стандартов, получили обобщенное название TCP/IP. К 1978 году окончательно оформилось то, что сегодня мы называем TCP/IP. Позже стек адаптировали для использования в локальных сетях. В начале 1980 г. протокол стал составной частью ОС UNIX. В том же году появилась объединенная сеть Internet. Переход к технологии Internet был завершен в 1983 г., когда министерство обороны США решило, что все компьютеры, присоединенные к глобальной сети, будут использовать стек протоколов TCP/IP. Модель TCP/IP разрабатывалась для описания стека протоколов TCP/IP (Transmission Control Protocol/Internet Protocol). Она была разработана значительно раньше, чем модель OSI. Формальные правила, определяющие последовательность и формат сообщений на одном уровне, называются протоколами. Иерархически организованная совокупность протоколов называется стеком коммуникационных протоколов. Модель состоит из четырех уровней, представленных в табл. 1.2. Таблица 1.2. 1. Прикладной уровень (Application) WWW, FTP, TFTP, SNMP, Telnet, SMTP, DNS, DHCP, WINS 2. Транспортный уровень (Transport) TCP, UDP 3. Уровень межсетевого взаимодействия

(Internet) ARP, IP, ICMP, RIP, OSPF ПМ.01. УЧАСТИЕ В Уровне сетевого интерфейса (Network Interface) Не регламентируется спецификациями стека TCP/IP (Ethernet, Token Ring, FDDI, ATM, X.25, Frame Relay, SLIP, PPP) Приближенное соответствие между моделями OSI и TCP/IP представлено в табл. 1.3. Таблица 1.3. 7. Прикладной (Application) 1. Прикладной уровень (Application) 6. Представления (Presentation) 5. Сеансовый (Session) 4. Транспортный (Transport) 2. Транспортный уровень (Transport) 3. Сетевой (Network) 3. Уровень межсетевого взаимодействия (Internet) 2. Канальный (Data Link) 4. Уровень сетевого интерфейса (Network Interface) 1. Физический (Physical) Преимущества стека протоколов TCP/IP

- Основное достоинство стека протоколов TCP/IP в том, что он обеспечивает надежную связь между сетевым оборудованием от различных производителей.

- Независимость от сетевой технологии — стек только определяет элемент передачи, дейтаграмму, и описывает способ ее движения по сети.

- Всеобщая связанность — стек позволяет любой паре компьютеров, которые его поддерживают, взаимодействовать друг с другом. Каждому компьютеру назначается логический адрес, а каждая передаваемая дейтаграмма содержит логические адреса отправителя и получателя. Промежуточные маршрутизаторы используют адрес получателя для принятия решения о маршрутизации.

- Подтверждения. Протоколы стека обеспечивают подтверждения правильности прохождения информации при обмене между отправителем и получателем.

- Стандартные прикладные протоколы. Протоколы стека TCP/IP включают в свой состав средства поддержки основных приложений, таких как электронная почта, передача файлов, удаленный доступ и т.д. Кратко опишем уровни модели TCP/IP. 1. Уровень сетевого интерфейса не регламентирован спецификациями стека TCP/IP и фактически к стеку TCP/IP относят уровни с 1-го по 3-й модели TCP/IP. Данный уровень соответствует физическому и канальному уровням модели OSI. 2. Уровень межсетевого взаимодействия. На данном уровне функционирует целое семейство протоколов. Основная задача данного уровня — доставка пакетов от одного узла-отправителя к узлу-получателю. Эту задачу выполняет протокол IP (Internet Protocol, протокол межсетевого взаимодействия). Протокол IP — базовый протокол стека TCP/IP и основной протокол сетевого уровня. Отвечает за передачу информации по сети. В его основе заложен дейтаграммный метод, который не гарантирует доставку пакета. о Протокол

ARP (Address Resolution Protocol, протокол разрешения физических адресов) — служит связующим звеном между уровнем межсетевого взаимодействия и уровнем сетевого интерфейса. Он преобразует IP-адреса сетевых узлов в физические MAC-адреса соответствующих сетевых адаптеров. Протокол ARP предполагает, что каждое устройство знает как свой IP-адрес, так и свой физический адрес. ARP динамически связывает их и заносит в специальную таблицу, где хранятся пары "IP-адрес – физический адрес" (обычно каждая запись в ARP-таблице имеет время жизни 10 мин.). о Протокол ICMP (Internet Control Message Protocol, протокол межсетевых управляющих сообщений) — служит для обмена информацией об ошибках. помощью специальных пакетов ICMP сообщает сетевым узлам информацию о невозможности доставки пакета, о превышении времени жизни пакета и др. о Протоколы RIP (Routing Internet Protocol) и OSPF (Open Shortest Path First) служат для построения таблиц маршрутизации и вычисления маршрутов при отправке пакетов между различными IP-сетями. 3. Транспортный уровень. о Протокол TCP (Transmission Control Protocol, протокол управления передачей) обеспечивает, базируясь на услугах протокола IP,

надежную передачу сообщений между сетевыми узлами с помощью образования соединений (сеансов) между данными узлами. Такие протоколы прикладного уровня, как HTTP и FTP, передают протоколу TCP свои данные для транспортировки. Поэтому скоростные характеристики TCP оказывают непосредственное влияние на производительность приложений. Кроме того, протокол TCP используется для обработки запросов на вход в сеть, разделения ресурсов и т.д. На протокол TCP, в частности, возложена задача управления потоками и перегрузками. Он отвечает за согласование скорости передачи данных с техническими возможностями рабочей станции-получателя и промежуточных устройств в сети. о Протокол UDP (User Datagram Protocol, протокол дейтаграмм пользователя) обеспечивает передачу прикладных пакетов дейтаграммным способом (т.е. не гарантирующим доставку пакетов). Работа этого протокола аналогична IP, но основной его задачей является связь сетевого протокола и различных приложений. 4. Прикладной уровень. Приложения, перечисленные в табл. 1.2, специально разрабатывались для функционирования в сетях TCP/IP. о Протоколы для формирования сетевой инфраструктуры (DNS, DHCP, WINS) будут рассмотрены в следующих разделах данного курса. о Приложения WWW (World Wide Web, Всемирная паутина) — основа для работы сегодняшней сети Интернет. Протокол FTP (File Transfer Protocol, протокол передачи файлов) реализует удаленную передачу файлов между узлами сети. о Протокол TFTP (Trivial File Transfer Protocol, простейший протокол пересылки файлов) — более простой передачи файлов, в отличие от FTP не требующий аутентификации пользователя на удаленном узле и использующий протокол UDP для передачи информации. о Протокол SNMP (Simple Network Management Protocol, простой протокол управления сетью) используется для организации управления сетевыми узлами. Вопросы 1. Поясните, для чего предназначена модель OSI? Где она применяется? 2. Назовите функции канального, сетевого и транспортного уровней модели OSI. 3. Чем отличается модель TCP/IP (DoD) от модели OSI? Как вы думаете, почему? 4. Перечислите функции уровней модели TCP/IP. 5. Опишите преимущества стека протоколов TCP/IP.

Лекция 5-6

Типовые элементы структурированной кабельной системы

1. Структурированная кабельная система
2. Подсистемы СКС
3. Вопросы

Структурированная кабельная система (СКС)- основа информационной инфраструктуры предприятия, позволяющая свести в единую систему множество информационных сервисов разного назначения: локальные вычислительные и телефонные сети, системы безопасности, видеонаблюдения и т.д.

СКС представляет собой иерархическую кабельную систему здания или группы зданий, разделенную на структурные подсистемы. Она состоит из набора медных и оптических кабелей, кросс-панелей, соединительных шнуров, кабельных разъемов, модульных гнезд, информационных розеток и вспомогательного оборудования. Все перечисленные элементы интегрируются в единую систему и эксплуатируются согласно определенным правилам.

Кабельная система - это система, элементами которой являются кабели и компоненты, которые связаны с кабелем. К кабельным компонентам относится все пассивное коммутационное оборудование, служащее для соединения или физического окончания (терминирования) кабеля - телекоммуникационные розетки на рабочих

местах, кроссовые и коммутационные панели в телекоммуникационных помещениях, муфты и сплайсы.

Термин «структурированная» означает, с одной стороны, способность системы поддерживать различные телекоммуникационные приложения (передачу речи, данных и видеоизображений), с другой - возможность применения различных компонентов и продукции различных производителей, и с третьей - способность к реализации так называемой мультимедийной среды, в которой используются несколько типов передающих сред - коаксиальный кабель, UTP, STP и оптическое волокно. Структуру кабельной системы определяет инфраструктура информационных технологий, IT (Information Technology), именно она диктует содержание конкретного проекта кабельной системы в соответствии с требованиями конечного пользователя, независимо от активного оборудования, которое может применяться впоследствии.

Подсистемы СКС

В структуре СКС существует несколько подсистем, каждая из которых выполняет свои функции. Для каждой из подсистем существуют правила физических конструкций, топология, способы физических соединений линий. Благодаря этому облегчается администрирование и обслуживание сети, и появляется возможность неограниченно увеличивать как объем сети, так и усложнять ее структуру.

Структурированная кабельная система состоит из нескольких уровней. Уровни отличаются по функциям, расположению и составу компонентов (регламентированных стандартами на кабельную разводку в зданиях (американским EIA/TIA-568A, европейским EN-50173 и международным ISO/IEC 11801).

Пример СКС



Структура СКС согласно международному стандарту ISO 11801

В самом общем случае СКС включает в себя три подсистемы: внешних магистралей, внутренних магистралей и горизонтальную.

Подсистема внешних магистралей состоит из

- внешних магистральных кабелей между кроссовой внешних

магистралей и кроссовыми зданиям,

- коммутационного оборудования в этих служебных помещениях, к которому подключаются внешние коммутационные кабели,

- коммутационных шнуров и/или перемычек в кроссовой внешних магистралей.

С помощью подсистемы внешних магистралей связываются в единую сеть здания, расположенные рядом. В случае создания сети в пределах одного здания необходимости в подсистеме внешних магистралей нет. Подсистема внешних магистралей чаще всего имеет топологию "кольцо" или "двойное кольцо".

Подсистема **внутренних магистралей** состоит из

- внутренних магистральных кабелей, положенных между кроссовой здания и кроссовыми этажей,

- коммутационное оборудование в данных кроссовых помещениях, - коммутационные шнуры и/или перемычки в кроссовой здания.

Посредством подсистемы внутренних магистралей соединяются отдельные этажи здания. Если СКС создается в пределах этажа, то подсистема внутренних магистралей может отсутствовать.

Горизонтальная, или третичная подсистема состоит из

- внутренних горизонтальных кабелей между кроссовой этажа и информационными розетками рабочих мест,

- информационных розеток,

- коммутационного оборудования в кроссовой этажа, к которому подключены горизонтальные кабели,

- коммутационных шнуров и/или перемычек в кроссовой этажа.

Горизонтальная подсистема имеет топологию типа "звезда", в которой каждая информационная розетка соединена своим кабелем с этажным коммутационным оборудованием. При использовании в горизонтальном тракте медного кабеля необходимо, чтобы все четыре пары были подключены к одной информационной розетке. Максимальная длина горизонтального проброса медного кабеля (экранированная или неэкранированная витая пара) не должна превышать 90 м.

Деление на перечисленные три подсистемы принципиально одинаково и для офисной, и для производственной сети. Иногда для удобства проектирования и обслуживания применяется более мелкое дробление на подсистему рабочего места, подсистему оборудования и административную подсистему.

Подсистема рабочего места - это соединение между информационной розеткой и компьютером/ телефоном/ принтером и т. д. К ней относятся соединительные шнуры, адаптеры, а также устройства передачи, позволяющие подключать перечисленные устройства к сети через информационную розетку.

Подсистема оборудования состоит из активного сетевого оборудования и компонентов, обеспечивающих подключение этого оборудования к коммутационным панелям: соединительных шнуров, разъемов и элементов их фиксации.

Административная подсистема состоит из соединительных проводов и шнуров, с помощью которых производится физическое соединение линий подсистем, подключенных к коммутационным панелям.

Типовые работы по монтажу СКС включают:

установку кабельных каналов (в коробах, лотках, гофротрубе, трубах и т.п.); пробивку отверстий в стенах; прокладку кабеля в кабельных каналах; установку розеток и заделку кабеля модули розетки; сборку и установку монтажного шкафа; установку и набивку патч-панелей и органайзеров.

Вопросы

1. Что такое СКС?
2. Охарактеризуйте кабельную систему.
3. Из каких подсистем состоит СКС?
4. Перечислите основные стандарты, регламентирующие кабельную разводку в зданиях.
5. Охарактеризуйте подсистемы СКС согласно международному стандарту ISO 11801.
6. Что включают в себя типовые работы по монтажу СКС?

Лекция 7-8

Планирование структуры сети

1. Методика и начальные этапы проектирования сети
2. Исходные данные
3. Выбор размера и структуры сети
4. Вопросы

Методика и начальные этапы проектирования сети

Любое планирование, как известно, представляет собой сильно упрощенное моделирование еще не наступившей действительности. Именно поэтому предусмотреть все возможные факторы, учесть все потребности, которые могут возникнуть в будущем, практически невозможно. Однако общие подходы к проектированию локальных компьютерных сетей все-таки могут быть сформулированы, некоторые полезные принципы такого проектирования предлагаются и с успехом используются. Не стоит только воспринимать их как нечто пригодное для любых практических случаев и учитывающее все возможные ситуации.

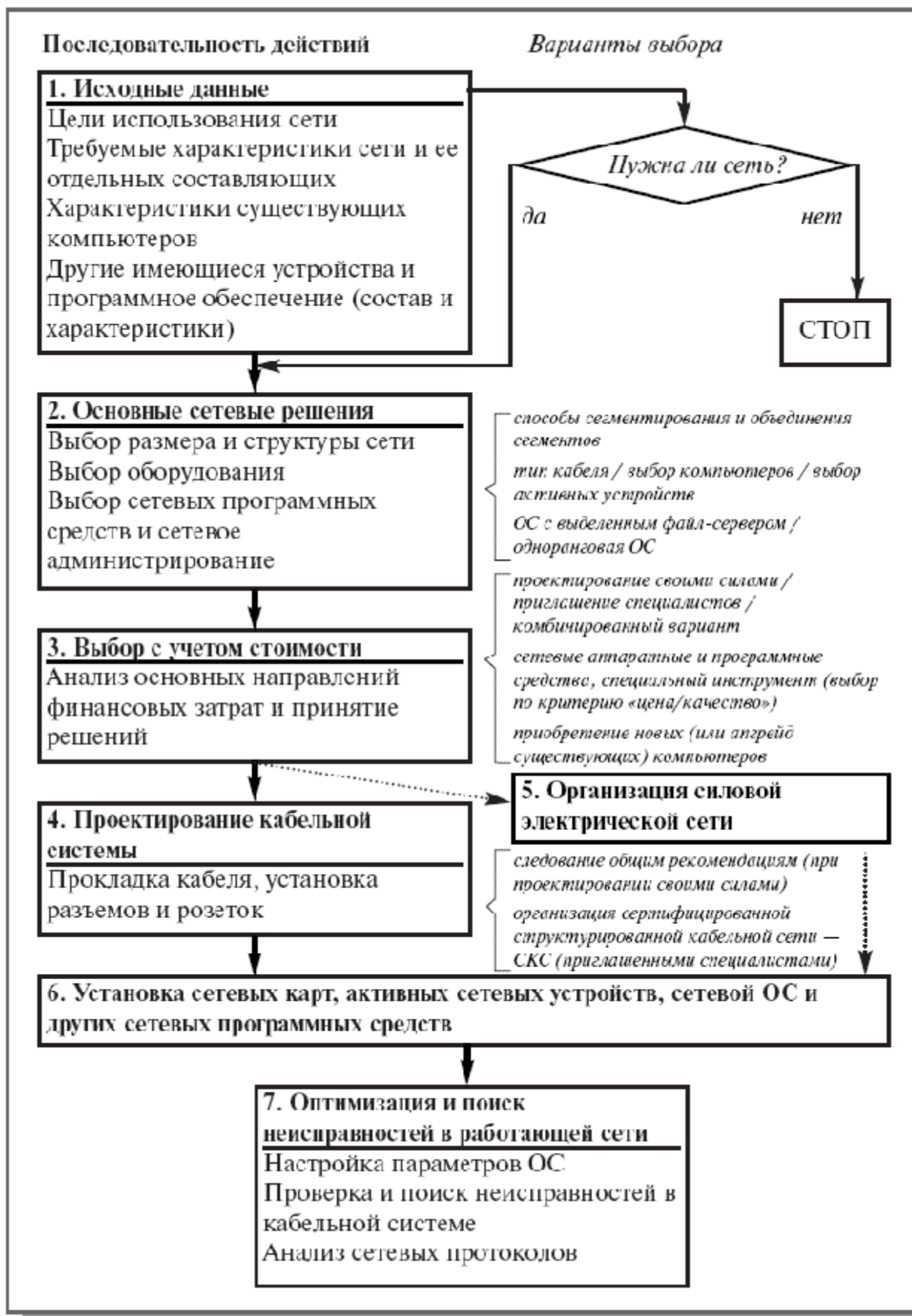


Рис. 1. Примерная последовательность этапов и варианты выбора при проектировании ЛС

На рисунке 1 приведена примерная последовательность этапов и варианты выбора при проектировании локальной сети. Вообще, проблема выбора одного из многочисленных вариантов при проектировании ЛС является основной для данного раздела. Выбор затрудняет необходимость учета множества требований, иногда противоречивых (например, обеспечение высоких технических характеристик сети при доступной стоимости), а также настойчивая, порой агрессивная реклама отдельных решений. Последнее часто относится к новейшим вариантам сетевого оборудования и/или программного обеспечения, отнюдь не самым доступным по цене и не всегда имеющим значительные преимущества по техническим характеристикам перед опробованными вариантами.

Не все этапы проектирования, перечисленные на рисунке 1, будут далее рассматриваться. Так, организация силовой электрической сети, актуальна в относительно редких случаях. Например, если сеть размещается в новом здании или производится капитальный ремонт, то возникает необходимость организации силовой электрической сети "по всем правилам". Многие из этих правил в отечественных условиях реализуются нечасто (или возможность их реализации ограничена по техническим причинам).

Не вдаваясь в излишние подробности, следует упомянуть необходимость организации полноценной системы заземления оборудования (что означает использование не двух-, а трехполюсных розеток, причем один из полюсов должен быть подключен к шине физического заземления) и обеспечение мер электробезопасности. Другой этап, который также не будет далее детализироваться, это этап 6 (установка сетевых карт, активных сетевых устройств, сетевой ОС и других сетевых программных средств).

С одной стороны, усилиями разработчиков компьютерного оборудования и программных средств, процедура их инсталляции максимально упрощена (режим plug-and-play, пошаговые инструкции по инсталляции). С другой же, в особо сложных случаях (например, при установке, настройке и последующей поддержке сети на основе выделенного сервера) может потребоваться либо приглашение стороннего специалиста, либо (что предпочтительнее) работа штатного системного администратора.

Исходные данные

Важность этого этапа связана как с необходимостью упорядочивания требований к создаваемой ЛС и ее отдельным составляющим для обеспечения возможности принятия в будущем взвешенных конкретных решений, так и с ее обоснованием. При создании новой сети для какого-нибудь предприятия желательно учитывать следующие факторы: Требуемый размер сети (в настоящее время, в ближайшем будущем и по прогнозу на перспективу).

- Структура, иерархия и основные части сети (по подразделением предприятия, а также по комнатам, этажам и зданиям предприятия).
- Основные направления и интенсивность информационных потоков в сети (в настоящее время, в ближайшем будущем и в дальней перспективе).
- Характер передаваемой по сети информации (данные, оцифрованная речь, изображения), который непосредственно сказывается на требуемой скорости передачи (до нескольких сотен Мбит/с для телевизионных изображений высокой четкости).
- Технические характеристики оборудования (компьютеров, адаптеров, кабелей, репитеров, концентраторов, коммутаторов) и его стоимость.

- Возможности прокладки кабельной системы в помещениях и между ними, а также меры обеспечения целостности кабеля.
- Обслуживание сети и контроль ее безотказности и безопасности.
- Требования к программным средствам по допустимому размеру сети, скорости, гибкости, разграничению прав доступа, стоимости, по возможностям контроля обмена информацией и т.д.
- Необходимость подключения к глобальным или к другим локальным сетям.

Сеть по сравнению с автономными компьютерами порождает множество дополнительных проблем: от простейших механических (компьютеры, подключенные к сети, труднее перемещать с места на место) до сложных информационных (необходимость контролировать совместно используемые ресурсы, предотвращать заражение сети вирусами). К тому же пользователи сети уже не так независимы, как пользователи автономных компьютеров, им надо придерживаться определенных правил, подчиняться установленным требованиям, которым их необходимо научить.

Наконец, сеть остро ставит вопрос о безопасности информации, защиты от несанкционированного доступа, ведь с любого компьютера сети можно считать данные с общих сетевых дисков. Защитить один компьютер или даже несколько одиночных гораздо проще, чем целую сеть. Поэтому приступать к установке сети целесообразно только тогда, когда без сети работа становится невозможной, непроизводительной, когда отсутствие межкомпьютерной связи сдерживает развитие дела.

В начале проектирования сети необходимо провести полную "инвентаризацию" имеющихся компьютеров и их программного обеспечения, а также периферийных устройств (принтеров, сканеров и т.д.). Это позволит при организации сети исключить ненужное дублирование (оборудование и программное обеспечение теперь могут быть разделяемыми ресурсами), а также поставить задачи модернизации (апгрейда) как аппаратных, так и программных средств.

Для корректного определения характеристик компьютеров целесообразно использовать специальные диагностические программы или встроенные программы ОС. Следует выбирать такие варианты программ, которые обеспечивают получение правильных данных ("старые" диагностические программы могут неверно указать тип процессора и версию ОС), а также сохранение данных в файле (это особенно ценно при большом числе компьютеров). Кроме того, следует уделить внимание наличию встроенной сетевой карты или сетевого контроллера на системной плате, а также типу поддерживаемых ими сетевых стандартов (как правило, поддерживается сеть Ethernet на витой паре, но принципиально знать ее разновидность – 10/100/1000 Мбит/с).

Не все характеристики компьютеров, которые важны при их объединении в сеть, могут быть определены описанными выше способами. Из сопроводительной документации к компьютеру или после вскрытия системного блока можно и нужно определить число и тип свободных слотов (разъемов) расширения, а также максимальную мощность блока питания. Это необходимо для оценки возможности установки в компьютер новых плат.

Выбор размера и структуры сети.

Под размером сети в данном случае понимается как количество объединяемых в сеть компьютеров, так и расстояния между ними. Надо четко представлять себе, сколько компьютеров (минимально и максимально) нуждается в подключении к сети. При этом необходимо оставлять возможность для дальнейшего роста количества компьютеров в сети, хотя бы процентов на 20–50.

Кстати, совсем не обязательно раз и навсегда включать в сеть все компьютеры предприятия. Иногда имеет смысл оставить некоторые из них автономными, например, из соображений безопасности информации на их дисках. Количество подключенных к сети компьютеров сильно влияет как на производительность, так и на сложность ее обслуживания. Оно также определяет стоимость требуемых программных средств, поэтому просчеты могут иметь довольно серьезные последствия.

Требуемая длина линий связи сети также играет не малую роль в проектировании сети. Например, если расстояния очень большие, может понадобиться использование дорогого оборудования. К тому же с увеличением расстояния резко возрастает значимость защиты линий связи от внешних электромагнитных помех. От расстояния зависит и скорость передачи информации по сети (выбор между Ethernet и Fast Ethernet). Целесообразно при выборе расстояний закладывать небольшой запас (хотя бы процентов 10) для учета непредвиденных обстоятельств. Преодолеть ограничения по длине иногда можно путем выбора структуры сети, разбиения ее на отдельные части.

Под структурой сети понимается способ разделения сети на части (сегменты), а также способ соединения этих сегментов между собой. Сеть предприятия может включать в себя рабочие группы компьютеров, сети подразделений, опорные сети, средства связи с другими сетями. Для объединения частей сети могут использоваться репитеры, репитерные концентраторы, коммутаторы, мосты и маршрутизаторы. Причем в ряде случаев стоимость этого объединительного оборудования может даже превысить стоимость компьютеров, сетевых адаптеров и кабеля, поэтому выбор структуры сети исключительно важен.

В идеале структура сети должна соответствовать структуре здания или комплекса зданий предприятия. Рабочие места группы сотрудников, занимающихся одной задачей (например, бухгалтерия, отдел продаж, инженерная группа), должны размещаться в одной или рядом расположенных комнатах. Тогда можно компьютеры этих сотрудников объединить в один сегмент, в единую рабочую группу и установить вблизи их комнат сервер, с которым они будут работать, а также концентратор или коммутатор, связывающий все их машины. Точно так же рабочие места сотрудников подразделения, занимающихся комплексом близких задач, лучше расположить на одном этаже здания, что существенно упростит их объединение в сегмент и дальнейшее его администрирование. На этом же этаже удобно расположить коммутаторы, маршрутизаторы и серверы, с которыми работает данное подразделение.

Как и в других случаях, при выборе структуры разумно оставлять возможности для дальнейшего развития сети. Например, лучше приобретать коммутаторы или маршрутизаторы с количеством портов, несколько большим, чем требуется в настоящий момент (хотя бы на 10—20 процентов). Это позволит при необходимости легко включить в сеть один или несколько сегментов. Ведь любое предприятие всегда стремится к росту (порой совершенно напрасно), и этот рост не должен каждый раз приводить к необходимости проектировать сеть предприятия заново.

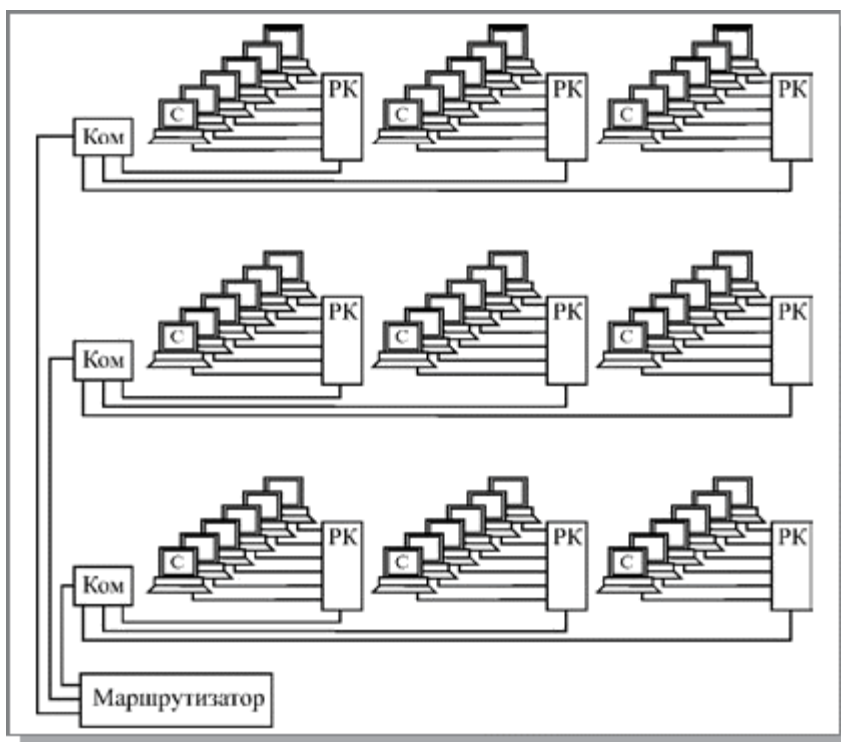


Рис. 2. Структура сети предприятия (С – серверы рабочих групп, РК – репитерные концентраторы, Ком – коммутаторы)

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

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

В рассмотренной ситуации области коллизий (зоны конфликта) сети будут включать в себя сегменты, расположенные в комнатах каждой рабочей группы, плюс сегмент, связывающий концентратор рабочей группы с коммутатором подразделения. Всего таких областей коллизий будет девять. Именно для них необходимо проводить расчеты работоспособности сети в соответствии с предыдущей темой.

Широковещательные области будут включать в себя все сегменты сети каждого подразделения плюс сегмент, связывающий коммутатор подразделения с маршрутизатором предприятия. Таких широковещательных областей будет всего три.

Если предполагаемая интенсивность обмена по проектируемой сети не достаточно велика, компьютеров не слишком много, и размеры здания позволяют, то

вполне возможно обойтись без маршрутизаторов, довольно сложных и сравнительно дорогих устройств.

Тогда сети подразделений будут связаны концентраторами, а между собой они будут соединяться коммутаторами.

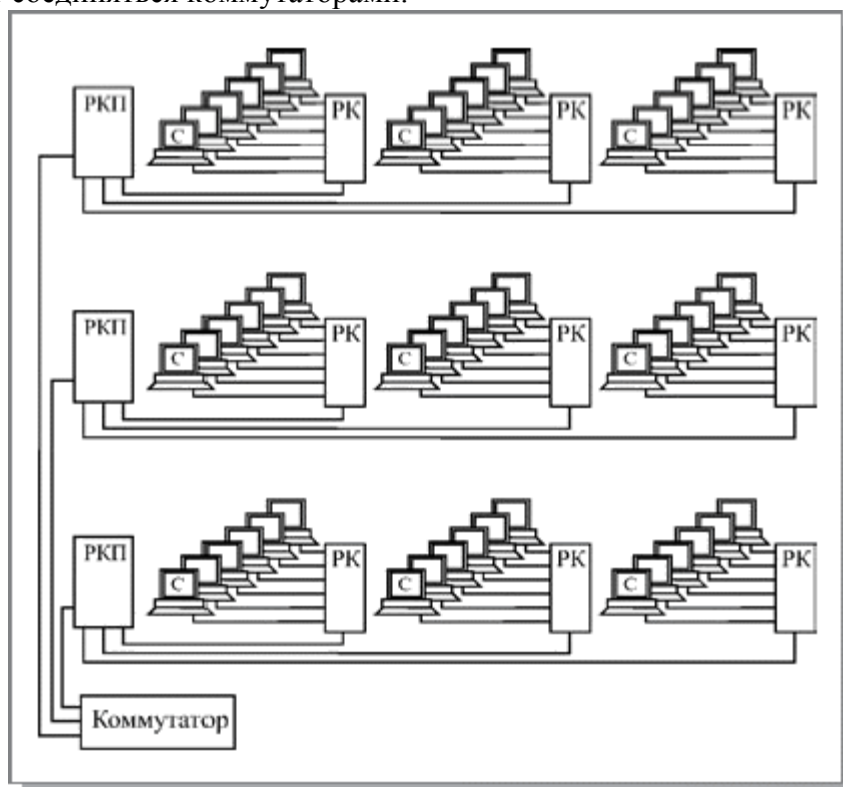


Рис. 3. Структура сети предприятия (С – серверы рабочих групп, РК – репитерные концентраторы, РКП – концентраторы подразделений)

Области коллизий в данном случае будут включать в себя все сегменты сети каждого подразделения плюс сегмент, соединяющий концентратор подразделения и коммутатор предприятия. Таких областей коллизий всего три. Для них надо проводить расчет работоспособности сети. В единственную широковещательную область войдет вся сеть предприятия.

В ситуации, когда компьютеров на предприятии немного (до 50), имеет смысл отказаться не только от маршрутизаторов, но и от коммутаторов, оставив только репитерные концентраторы. Более того, при такой малой сети и низкой интенсивности обмена вполне может оказаться подходящей сеть Ethernet на тонком коаксиальном кабеле (сегменты 10BASE2) без концентраторов или с 1–2 простейшими репитерами. Правда, в последнем случае придется компьютеры каждого сегмента разместить на одном этаже из-за ограничений на длину кабеля сегмента 10BASE2. Следует учитывать, что во вновь создаваемых сетях использование коаксиального кабеля не рекомендуется.

Конечно, такая идиллическая картина, как рассмотренная выше, наблюдается далеко не всегда. В реальности все бывает гораздо сложнее. Например, структура подразделений может вообще не соответствовать структуре комнат и этажей. Предприятие может занимать два разнесенных друг от друга помещения в одном здании или даже три—четыре удаленных здания. Тогда может понадобиться применение оптоволоконных сегментов (в том числе и полнодуплексных, которые обеспечивают максимальную длину кабеля). А структура сети при этом обычно чрезвычайно сложна, с множеством областей коллизий и широковещательных областей.

Вопросы

1. Что такое планирование?
2. Перечислите примерную последовательность этапов при проектировании ЛС.
3. Какие факторы нужно учитывать при создании новой сети для какого-нибудь предприятия?
4. Сколько процентов необходимо оставлять для расширения сети?
5. Чему должна соответствовать структура сети?
6. Что понимается под структурой сети?

Лекция 9-10

Проектирование локальной сети

1. Выбор с учетом стоимости
2. Проектирование кабельной системы
3. Вопросы

Выбор с учетом стоимости

При формулировании критериев выбора сетевых аппаратных и программных средств в качестве одного из главных критериев называлась их стоимость. Очевидно, что простой констатации важности учета уровня цен недостаточно. Тем не менее, анализ текущего уровня абсолютных цен на сетевую аппаратуру и программное обеспечение, пусть даже на основе представительного обзора, имеет сам по себе малую ценность и очень быстро устаревает.

Уровень абсолютных цен зависит от множества факторов, причем не всегда определяющим среди них является совокупность характеристик аппаратуры или ПО (далее для краткости называемая качеством). На него влияют также такие рыночные факторы, как конъюнктура (текущий спрос), уровень наценки, устанавливаемый дилерами или продавцами, ценовая политика самого производителя, уровень национальной валюты по отношению к евро и динамика его изменения.

В этих условиях вместо абсолютных правильнее оперировать относительными ценами в координатах "цена-качество" для однородной (имеющей одинаковое или сходное назначение) продукции. Относительные цены меньше подвержены изменениям, а базовый, принимаемый за единицу отсчета уровень, всегда может быть скорректирован на основании анализа свежих данных из сети Интернет или прайс-листов отдельных фирмпродавцов.

Прежде всего следует определить возможные направления финансовых затрат (к данному этапу проектирования необходимые предпосылки для решения этой задачи уже имеются):

- Дополнительные компьютеры и апгрейд существующих компьютеров. Необязательное направление затрат: при достаточном количестве и качестве существующих компьютеров их апгрейд не требуется (или требуется в минимальном объеме – например, для установки более современных сетевых карт); в одноранговой сети не нужен (хотя и желателен) также специальный файл-сервер.
- Сетевые аппаратные средства (кабели и все, что необходимо для организации кабельной системы, сетевые принтеры, активные сетевые устройства – повторители, концентраторы, маршрутизаторы и т.д.).
- Сетевые программные средства, прежде всего, сетевая ОС на необходимое число рабочих станций (с запасом).

- Оплата работы приглашенных специалистов при организации кабельной системы, установке и настройке сетевой ОС, при проведении периодической профилактики и срочного ремонта. Необязательное направление затрат: для небольших сетей со многими из этих работ может и должен справляться штатный сетевой администратор (возможно, с помощью других сотрудников данного предприятия).

Несколько лет назад, когда вместе с появлением ОС типа Windows 95 появилась также возможность организовывать простые одноранговые сети, довольно популярным за рубежом средством упрощения проектирования (но не экономии денежных средств!) было использование так называемых стартовых наборов (starter kit). Типовой стартовый набор включал 2 сетевые карты, 2 копии сетевой ОС и коаксиальный кабель длиной футов (около 7,6 м) с установленными на нем разъемами для объединения в сеть двух компьютеров. За возможность включения в сеть каждого дополнительного компьютера нужно было платить цену, равную половине цены стартового набора.

Вскоре после перехода на сети на основе витой пары, произошла трансформация подобного набора. Он стал включать концентратор (возможен выбор концентратора на разное число выходов), необходимое число сетевых карт и сетевых кабелей (витых пар) нужной длины (выбор из нескольких вариантов стандартных длин) с предустановленными на них разъемами типа RJ45, а также инструкцию по установке сетевой ОС и организации сетевой печати. Подобные подходы на основе наборов типа "сеть в одной коробке" предназначены, в основном, для неопытных пользователей.

В настоящее время они мало популярны, так как установка новых сетей стала массовым явлением и происходит часто на основе передачи опыта предыдущей установки, да и число полностью неопытных пользователей становится все меньше. Следует помнить, что кроме жесткости любого готового набора сетевых средств, в котором невозможно учесть специфику данной проектируемой сети, его недостатком является и явно завышенная цена – при том же или лучшем качестве оборудования и ОС их предпочтительнее приобретать по отдельности.

Следует отметить, что погонная цена кабеля зависит от его типа и характеристик (кабель для внутренней или внешней проводки, категория витой пары или тип оптического волокна ВОЛС, число витых пар или волокон в одной оболочке, наличие и разновидность экранов в витой паре). Инструменты, используемые для работы с кабелем, значительно дороже, если это оптоволокно.

Активное сетевое оборудование, включая сетевые адаптеры, повторители, концентраторы, маршрутизаторы и т.д., для сетей семейства Ethernet при прочих равных условиях (прежде всего, при том же типе кабеля и скорости передачи) доступнее по цене, чем оборудование для сетей другого типа. Это одно из объяснений популярности сетей семейства Ethernet на практике у нас в стране и за рубежом. Фактически сети данного типа легли в основу стандарта структурированных кабельных систем.

На отечественном рынке сетевого оборудования преобладают средства для построения сетей Ethernet и беспроводных сетей, но последние требуют значительных финансовых затрат.

Проектирование кабельной системы

Считается, что к данному этапу проектирования тип кабеля определен. Более того, предполагается, что тип локальной сети (Ethernet, Fast Ethernet, FDDI или др.) также выбран. Далее рассматриваются рекомендации по организации кабельной системы для сетей на основе проводных соединений (витых пар и оптоволокон). При

этом учитывается преобладание в настоящее время на практике сетей данного типа и их заметное отличие от сетей на основе беспроводных соединений с точки зрения особенностей организации кабельной системы.

При выборе кабеля в первую очередь надо учитывать требуемую длину, а также защищенность от внешних помех и уровень собственных излучений. При большой длине сети и необходимости обеспечить секретность передаваемых данных или высоком уровне помех в помещении незаменим оптоволоконный кабель. Следует отметить, что применение оптоволоконных вместо электрических кабелей даже при достаточно комфортных условиях позволяет существенно (на 10-50 процентов) поднять производительность сети за счет снижения доли искаженных информационных пакетов.

При проектировании кабельных систем для локальных сетей накоплен большой опыт, на основе которого могут быть сформулированы общие рекомендации по организации таких систем. Более того, существуют стандарты под общим названием "структурированные кабельные системы (СКС)", которые особенно актуальны для вновь создаваемых или реконструируемых относительно больших локальных сетей на уровне предприятия. Для сравнительно небольших локальных сетей создание сертифицированной СКС, которое предполагает работу приглашенных специалистов, резонно рассматривается как излишняя роскошь.

Ниже перечислены общие рекомендации по созданию кабельных систем, являющиеся фактически "подмножеством" не детализированных требований стандартов СКС.

1. Составить план размещения компьютеров и других сетевых устройств в помещении (или помещениях). Этот план следует рассматривать как детализацию принятого ранее решения относительно размера и структуры сети.

Провести анализ возможности перемещения всех или большей части компьютеров в одно или несколько соседних помещений. Это существенно упростит организацию кабельной системы и исключит необходимость использования излишних активных сетевых устройств. Следует также принять во внимание расширение сети в будущем, для чего предусмотреть наличие точек подключения к сети даже в тех помещениях, где сетевые компьютеры пока отсутствуют. План размещения не должен быть абстрактным, не учитывающим хотя бы в эскизном варианте ограничения, накладываемые конкретным типом выбранной локальной сети. Так, например, нельзя рассчитывать в сети типа 100BASE-T4 или 100BASE-TX (Fast Ethernet на витой паре) на расстояние от абонента (сетевого компьютера или другого сетевого устройства) до концентратора, превышающее 100 м.

2. Оценить соответствие длины кабельной системы и ее отдельных частей (сегментов, соединений между данным абонентом и концентратором и т.д.) требованиям выбранной разновидности локальной сети. Для сетей семейства Ethernet необходимо учитывать ограничения на длины сегментов на разных типах кабелей и задержки сигналов в кабельной системе в соответствии с правилами модели 1 или 2. Для сетей другого типа (Token Ring, FDDI и т.д.) действуют абсолютные ограничения на длины отдельных участков кабельной системы. В случае если рассчитанная таким образом длина кабельной системы в целом или на отдельных участках превышает предельно допустимую или близка к ней, следует выбрать одно или несколько из следующих решений (в порядке предпочтения по простоте, стоимости и эффективности реализации):

о перейти к более качественному типу кабеля во всей сети или только на критичных участках (переход от неэкранированной витой пары к экранированной или оптоволокну);
о использовать дополнительные репитеры или репитерные

концентраторы, позволяющие восстановить амплитуду и форму сигналов, тем самым повысить длину кабельной системы;

О применять модемы для связи данной локальной сети из относительно близко расположенных абонентов с одним или несколькими удаленными абонентами, если снижение скорости передачи на данном участке (или участках) допустимо; о перейти к другому типу сети, имеющему меньшие ограничения на длину кабельной системы (то есть от сетей на витой паре к сетям на оптоволокне).

Таким образом, выбор конфигурации кабельной системы на данном и предыдущем этапах – итерационный процесс, который может затронуть и более ранние этапы проектирования (вплоть до выбора типов локальной сети и кабеля), если выбор на этих этапах был некорректным.

3. Кабельная система должна быть устойчива к внешним электромагнитным помехам и, по возможности, не генерировать заметные собственные излучения. В противном случае снижается фактическая скорость работы сети (из-за необходимости повторной передачи искаженных помехами пакетов), а также нарушаются требования защиты информации.

Большой уровень помех может быть вызван наличием в помещении предприятия мощного электрического оборудования (например, металлообрабатывающих станков, физических установок). Он может быть также связан с близким расположением (до 100-200 метров) высоковольтных линий электропередачи и мощных радиопередатчиков (радиостанций, ретрансляционных антенн сотовой телефонии). Иногда высокий уровень помех вызван всего лишь неправильным размещением кабеля сети. Например, при прокладке кабеля вдоль силовых проводов 220 вольт или вдоль рядов светильников с лампами дневного света количество ошибок передачи резко возрастает (кстати, последнее решение кажется многим очень удобным, так как кабель никому не мешает).

4. Кабельная система должна быть защищена от механических повреждений.

Для прокладки кабелей сети лучше всего использовать специальные подвесные кабельные короба, настенные кабелепроводы или фальшполы. В этом случае кабели надежно защищены от механических воздействий. Самое дорогое решение – это фальшпол, представляющий собой металлические панели, установленные на подставках, и покрывающие весь пол помещения. Зато фальшпол позволяет легко и безопасно проложить огромное количество проводов, что особенно ценно в научных лабораториях, где помимо кабелей локальной сети существует множество других проводов.

Для прокладки кабеля между комнатами или этажами обычно пробиваются отверстия в стенах или перекрытиях. По сравнению с прокладкой кабеля через двери комнат и стены коридоров это позволяет существенно сократить общую длину кабелей. Однако надо учитывать, что такое решение усложняет любые дальнейшие изменения в кабельной системе (замену кабелей, прокладку дополнительных кабелей, изменение расположения компьютеров сети и т.д.).

Кабели ни в коем случае не должны самостоятельно удерживать свой вес, так как со временем это может вызвать их обрыв. Их следует подвешивать на стальных тросах, причем для эксплуатации на открытом воздухе необходимы специально предназначенные для этого кабели с оболочкой, устойчивой к атмосферным воздействиям. По возможности надо использовать для соединения далеко разнесенных зданий подземные коллекторы. Но при этом необходимо предпринимать меры по защите кабелей от воздействия влаги.

Следует также избегать чрезмерно малых радиусов изгиба кабелей (особенно это важно в случае коаксиальных и оптоволоконных кабелей), чтобы не вызвать разрушения изоляции или обрыва центральной жилы. По этой же причине крепежные элементы не должны чересчур пережимать кабель. Известны случаи, когда подобные

нарушения вызывали полное прекращение связи через недели или даже месяцы после начала эксплуатации сети.

Часть из перечисленных в данном пункте мер способствует также защите от помех и защите информации (из-за ограничения непосредственного доступа к кабельной системе).

5. Кабельная система должна иметь "прозрачную" и документированно оформленную структуру. Это необходимо как для обеспечения возможности внесения изменений в эту структуру, так и для поиска неисправностей.

Для объединения концов кабелей часто используются специальные распределительные шкафы, доступ к которым должен быть ограничен. Конечно, их применение оправдано только в том случае, если кабелей много (несколько десятков). Располагать распределительные шкафы целесообразно рядом с концентраторами, коммутаторами или маршрутизаторами. Отдельные кабели в жгутах, располагающихся в коробах, под вторым полом и т.д., должны быть одинаковым образом промаркированы с помощью специальных цветных наклеек.

6. Необходимо проверить целостность кабельной системы.

В сети на коаксиальном кабеле для этого можно было использовать непосредственные измерения омметром сопротивления при наличии и отсутствии согласующих нагрузок. В более современных сетях на витой паре и оптоволокне о целостности кабельной системы можно судить по показаниям индикаторов, расположенных на сетевых картах вблизи сетевых разъемов. Возможно также использование для этой цели специальных приборов – кабельных сканеров.

Стандарты на "Структурированные кабельные системы (СКС)" представляют собой объемные документы, детально описывающие и регламентирующие процесс создания кабельных соединений локальных сетей. Как и в случае сетевого администрирования, целесообразно рассмотреть лишь общие принципы создания СКС. Конечно, отдельные рекомендации стандартов СКС могут быть с успехом использованы при создании кабельной системы собственными силами (но без возможности официальной сертификации такой системы).

Структурированная кабельная система (СКС) представляет собой иерархическую кабельную систему здания или группы зданий, разделенную на структурные подсистемы. СКС состоит из набора медных и оптических кабелей, кросс-панелей, соединительных шнуров, кабельных разъемов, модульных гнезд, информационных розеток и вспомогательного оборудования. Все перечисленные элементы интегрируются в единую систему и эксплуатируются согласно определенным правилам.

Основные преимущества (или принципы) СКС:

- Универсальность: передача данных в ЛВС, видеоинформации или сигналов от датчиков пожарной безопасности либо охранных систем по единой кабельной системе, организация локальной телефонной сети.
- Гибкость: простота изменения конфигурации кабельной системы и управления перемещениями внутри и между зданиями.
- Устойчивость: тщательно спланированная СКС устойчива к внештатным ситуациям и гарантирует высокую надежность и защиту данных в течение многих лет. Так большинство ведущих производителей дают гарантию на поставляемые ими СКС (при выполнении требуемых процедур сертификации) до 25 лет.

Основным препятствием широкого внедрения СКС является, как уже отмечалось, их высокая стоимость, что делает приемлемым это решение для

относительно масштабных локальных сетей уровня предприятия. Действительно, стандарты на СКС предусматривают проведение, наряду с прочими, комплекса дорогостоящих строительных работ.

Основными стандартами на СКС являются:

- Международный стандарт ISO/IEC 11801 Generic Cabling for Customer Premises.
- Европейский стандарт EN 50173 Information technology– Generic cabling systems.
- Американский стандарт ANSI/TIA/EIA 568-B Commercial Building Telecommunication Cabling Standard.

Стандарты на СКС периодически (примерно раз в пять лет) пересматриваются в связи с развитием аппаратных средств локальных сетей (включая совершенствование медных и оптоволоконных кабелей).

Согласно стандартам, СКС включает следующие три подсистемы:

- магистральная подсистема комплекса;
- магистральная подсистема здания;
- горизонтальная подсистема.

Распределительные пункты (РП) обеспечивают возможность создания топологии каналов типа "шина", "звезда" или "кольцо".

Магистральная подсистема комплекса включает магистральные кабели комплекса, механическое окончание кабелей (разъемы) в РП комплекса и РП здания и коммутационные соединения в РП комплекса. Магистральные кабели комплекса также могут соединять между собой распределительные пункты зданий.

Магистральная подсистема здания включает магистральные кабели здания, механическое окончание кабелей (разъемы) в РП здания и РП этажа, а также коммутационные соединения в РП здания. Магистральные кабели здания не должны иметь точек перехода, электропроводные кабели не следует соединять сплайсами (тип непосредственного соединения кабелей без разъемов).

Горизонтальная подсистема включает горизонтальные кабели, механическое окончание кабелей (разъемы) в РП этажа, коммутационные соединения в РП этажа и телекоммуникационные разъемы. В горизонтальных кабелях не допускается разрывов. При необходимости возможна одна точка перехода. Точка перехода – это место горизонтальной подсистемы, в котором выполняется соединение двух кабелей разных типов (например, круглого кабеля с плоским) или разветвление многопарного кабеля на несколько четырехпарных. Все пары и волокна телекоммуникационного разъема должны быть подключены. Телекоммуникационные разъемы не являются точками администрирования. Не допускается включения активных элементов и адаптеров в состав СКС.

Абонентские кабели для подключения терминального оборудования не являются стационарными и находятся за рамками СКС. Однако стандарты определяют параметры канала, в состав которого входят абонентские и сетевые кабели.

В целом соединения в СКС образуют систему интерфейсов СКС.

Интерфейсы СКС – это гнездовые разъемы каждой из подсистем, обеспечивающие постоянное или коммутируемое подключение оборудования и кабелей внешних служб. На рисунке 1 показаны интерфейсы в виде линий в пределах распределительных пунктов, схематически обозначающих блоки гнезд на панелях.

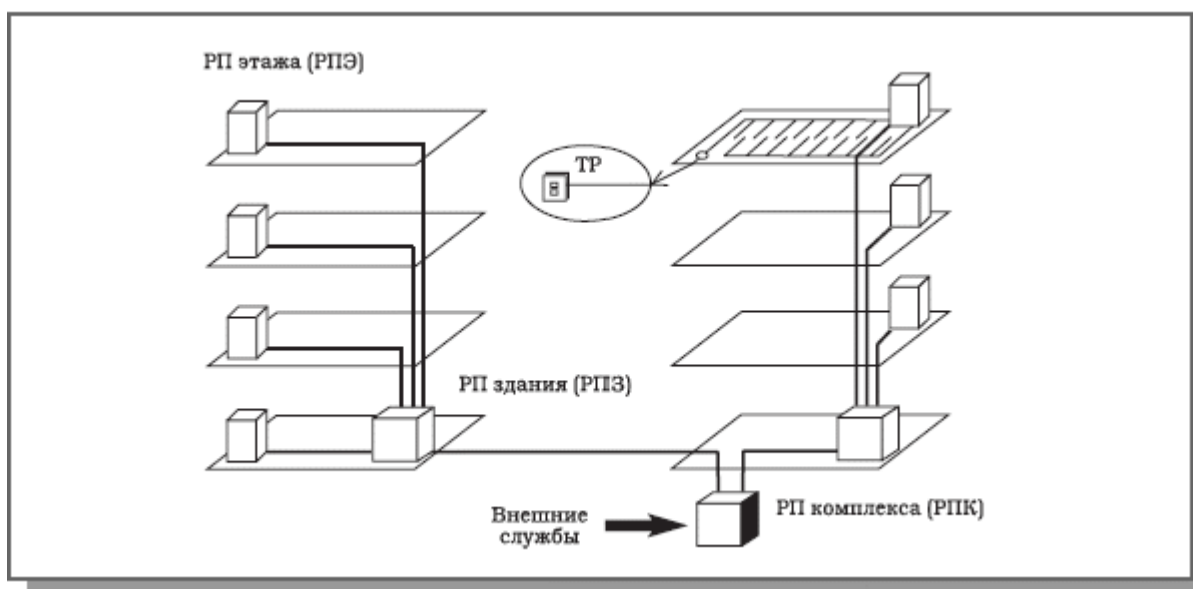


Рисунок 1. Система интерфейсов СКС

Для подключения к СКС достаточно одного сетевого кабеля. В варианте коммутации используют сетевой и коммутационный кабель и дополнительную панель.

Стандарты на СКС по содержанию можно разделить на три группы – стандарты проектирования, монтажа и администрирования. Пожалуй, наиболее полезная в практическом плане группа стандартов монтажа включает рекомендуемые типы и длины отдельных сегментов кабелей в различных подсистемах. В настоящее время во вновь создаваемых кабельных системах рекомендуется использовать только витую пару (симметричный кабель в соответствии с терминологией стандартов) и оптоволоконный кабель, причем, чем выше уровень подсистемы, тем предпочтительнее использование оптоволокна.

Наиболее серьезной проблемой при создании СКС для работы высокоскоростных приложений (категория 3 и выше) является качество монтажа. По данным BICSI (Building Industry Consulting Service International) – международной ассоциации профессионалов телекоммуникационной промышленности, 80% всех структурированных кабельных систем США, построенных на компонентах категории 5, не могут быть квалифицированы как системы категории 5 вследствие нарушения правил монтажа.

Существуют специальные требования и рекомендации по монтажу СКС, выполнение которых гарантирует сохранение исходных рабочих характеристик отдельных компонентов, собранных в линии, каналы и системы. Стандарты ISO/IEC 11801 и ANSI/TIA/EIA-568A устанавливают в качестве требований несколько основных правил монтажа, предусматривающих методы и аккуратность выполнения соединения компонентов и организации кабельных потоков, которые в значительной степени повышают производительность системы и облегчают администрирование установленных кабельных систем.

Вопросы

1. Перечислите возможные направления финансовых затрат.
2. Что нужно учитывать при выборе кабеля?
3. Перечислите общие рекомендации по созданию кабельных систем.
4. Перечислите основные преимущества (или принципы) СКС.
5. Перечислите основные стандарты на СКС.
6. Дайте определение интерфейсам СКС.

Лекция 10-12

Ввод в эксплуатацию компьютерных систем

- 1 Введение
- 2 Общая часть
- 3 Порядок ввода в эксплуатацию и перемещение компьютерного оборудования
- 4 Меры безопасности
- 5 Порядок работы в информационной сети
- 6 Ответственность
- 7 Вопросы

1. Введение

Эксплуатация локальной сети – это непрерывный процесс, для упрощения которого, в частности, можно составить план замены устаревающих устройств, чтобы их обновление происходило раньше, чем они начнут усложнять эксплуатацию сети.

Ввод в эксплуатацию ЛВС предполагает следующие этапы реализации:

Получение технического задания.

Разработка проекта локальной вычислительной сети.

Организация подготовительных строительно-монтажных работ.

Приведение монтажа оборудования структурированных кабельных систем.

Установка вычислительной техники и подключение её и СКС.

Проведение пуско-наладочных работ.

Сдача в эксплуатацию ЛВС.

Организация работ по обслуживанию ЛВС.

При эксплуатации локальной компьютерной сети обязательно должна быть составлена и доведена до пользователей сети инструкция по эксплуатации компьютерной сети.

2. Общая часть

2.1 Вид оборудования, для которого составлена инструкция.

Инструкция по эксплуатации применяется для персональных компьютеров, принтеров, серверов, сетевых коммутаторов (далее - компьютерное оборудование).

2.2 Функции, реализуемые компьютерным оборудованием.

На персональных компьютерах осуществляются работы с электронными документами, ввод и вывод данных в информационных базах данных.

Серверы обеспечивают централизованное хранение, обработку и выдачу информации, ограничение прав доступа к базам данных на уровне пользователей, а так же резервное копирование баз данных.

Сетевые коммутаторы обеспечивают физическое соединение между компьютерами, подключенными к информационной сети, пересылку пакетов между компьютерами и серверами.

2.3 Регламент и режимы работы компьютерного оборудования.

Пользователь автоматизированного рабочего места (АРМ) несет ответственность за сохранность и правильную эксплуатацию компьютерного оборудования.

Установка и изменение конфигурации операционной системы и состава программного обеспечения производятся специалистами отдела технического

обслуживания информационных систем (ТОИС) и отдела прикладного программирования (ПП) Организации.

В случае неисправности компьютерного оборудования об этом необходимо сообщить в отдел ТОИС Организации

3. Порядок ввода в эксплуатацию и перемещение компьютерного оборудования

3.1 Для приобретения нового компьютерного оборудования руководитель подразделения подает заявку по установленной форме. Конфигурация компьютерного оборудования согласовывается с отделом ТОИС.

3.2 Вводимое в эксплуатацию компьютерное оборудование доставляется со склада Организации материально ответственным лицом подразделения в отдел ТОИС для установки лицензионных программных продуктов из перечня разрешенных к использованию в информационной системе Организации.

3.3 Перемещение компьютерного оборудования между подразделениям Организации производится только после проверки его технического состояния и установленных программных продуктов в отделе ТОИС.

3.4 Вынос за территорию Организации компьютерного оборудования и его частей на ремонт производится с оформлением материального пропуска, в исключительных случаях, для проведения срочного ремонта, допускается вынос без оформления материального пропуска работникам отдела ТОИС, включенных в список лиц, имеющих разрешение на перемещение компьютерного оборудования.

4. Меры безопасности

4.1 Требования безопасности.

Компьютерное оборудование, приобретаемое для использования в Организации, должно иметь сертификат соответствия требованиям следующих нормативных документов:

ГОСТ Р МЭК 60950-2002 - Безопасность оборудования информационных технологий;

ГОСТ 26329-84 - Машины вычислительные и системы обработки данных. Допустимые уровни шума технических средств и методы их определения;

ГОСТ Р 51318.22-2006 - Совместимость технических средств электромагнитная. Оборудование информационных технологий. Радиопомехи промышленные. Нормы и методы измерений;

ГОСТ Р 51318.24-99 - Совместимость технических средств электромагнитная. Устойчивость оборудования информационных технологий к электромагнитным помехам. Требования и методы испытаний;

ГОСТ Р 51317.3.2-2006 - Совместимость технических средств электромагнитная. Эмиссия гармонических составляющих тока техническими средствами с потребляемым током не более 16 А (в одной фазе). Нормы и методы испытаний;

ГОСТ Р 51317.3.3-2008 - Совместимость технических средств электромагнитная. Ограничение изменений напряжения, колебаний напряжения и фликера в низковольтных системах электроснабжения общего назначения. Технические средства с потребляемым током не более 16 А (в одной фазе), подключаемые к электрической сети при несоблюдении определенных условий подключения. Нормы и методы испытаний;

Санитарно-эпидемиологические правила и нормативы СанПиН 2.2.2/2.4.1340-03 "Гигиенические требования к персональным электронно вычислительным машинам и организации работы" (в редакции СанПиН 2.2.2/2.4.2198-07. Изменение N 1 к СанПиН 2.2.2/2.4.1340-03).

Для подключения к сети электропитания необходимо использовать только исправные силовые кабели, поставляемые с компьютерным оборудованием.

Любые ремонтные работы необходимо производить только при полном отключении электропитания.

4.2 Подготовка компьютерного оборудования к эксплуатации.

До включения компьютерного оборудования пользователь обязан:
проверить правильность расположения компьютерного оборудования: кабели электропитания оборудования должны находиться с тыльной стороны рабочего места;
проверить надежность подключения к компьютеру разъемов периферийного оборудования; убедиться в отсутствии засветок, отражений и бликов на экране монитора; убедиться в отсутствии пыли на экране монитора и клавиатуре, при необходимости, протереть их специальной салфеткой.

Размещение компьютерного оборудования, обеспечение температурных режимов внутри помещений и организация рабочих мест должны быть выполнены в соответствии с Санитарно-эпидемиологическим правилам и нормативам СанПиН 2.2.2/2.4.1340-03 "Гигиенические требования к персональным электронно-вычислительным машинам и организации работы" (в редакции СанПиН 2.2.2/2.4.2198-07. Изменение N 1 к СанПиН 2.2.2/2.4.1340).

4.3 Эксплуатация компьютерного оборудования.

Пользователь АРМ во время работы обязан:

не закрывать вентиляционные отверстия компьютерного оборудования; при необходимости временного прекращения работы корректно закрыть все активные программы; соблюдать требования настоящей инструкции.

Включение компьютерного оборудования производить в следующей последовательности:

- принтер
- монитор
- компьютер

Начинать работу можно только после полной загрузки операционной системы и появления сообщения о вводе имени и пароля пользователя.

Во время работы запрещается:

- прикасаться к задней панели компьютерного оборудования;
- переключать разъемы кабелей периферийного оборудования;
- производить самостоятельный ремонт компьютерного оборудования
- удалять с корпуса наклейки с заводскими и лицензионными номерами.

При печати на лазерном принтере необходимо использовать только бумагу для лазерных принтеров плотностью не ниже 80 г/м². Использование менее плотной бумаги ведет к повреждению принтера. Вытягивание бумаги во время печати из выходного отверстия принтера недопустимо и ведет к повреждению механизма печати.

Для корректного выключения компьютера необходимо закрыть все работающие программы, выбрать в меню "Пуск" команду "Завершение работы" и в появившемся меню выбрать пункт "Завершение работы" и нажать кнопку "ОК". Дождаться отключения питания системного блока, выключить монитор и принтер.

5. Порядок работы в информационной сети

5.1 Порядок доступа в информационную сеть Организации:

доступ пользователей в информационную сеть производится по служебной записке адресованной директору Организации. Служебная записка должна содержать информацию о пользователе, месте расположения автоматизированного рабочего места (АРМ), перечня выполняемых задач и режимов доступа к ним (полный доступ или только просмотр баз данных). При необходимости доступа к бухгалтерским базам данных служебная записка адресуется главному бухгалтеру Организации;

администратор сети присваивает имя АРМ, однозначно определяющее пользователя в информационной сети, и устанавливает первоначальный пароль пользователя, необходимый в дальнейшем для определения подлинности доступа АРМ к сетевым ресурсам; пользователь при первом входе в информационную сеть обязан заменить пароль, установленный администратором, на личный пароль. Передача имени пользователя и пароля другим лицам категорически запрещается, при запросе системы о смене пароля необходимо заменить его новым; при увольнении или смене места работы работника руководитель подразделения ставит в известность администратора сети для отключения учетной записи пользователя.

5.2 При запросе установки обновлений операционной системы пользователь обязан разрешить системе автоматическую установку.

6 Ответственность

Работники, нарушившие требования настоящей инструкции, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами Организации.

Вопросы

1. Какие этапы предполагает ввод в эксплуатацию компьютерной локальной сети?
2. Требованиям каких нормативных документов должна соответствовать компьютерная сеть, вводимая в эксплуатацию?
3. Какие санитарно-гигиенические нормы и требования следует соблюдать при введении компьютерной сети в эксплуатацию?

Лекция 12-14

Программно-аппаратные средства защиты информации в сети

1. Аппаратные средства защиты информации
2. Программные средства защиты информации
3. Сервисы безопасности
4. Вопросы

Аппаратные средства защиты информации

Программно-аппаратные средства защиты информации — это сервисы безопасности, встроенные в сетевые операционные системы.

К **аппаратным средствам защиты информации** относятся электронные и электронно-механические устройства, включаемые в состав технических средств КС и выполняющие (самостоятельно или в едином комплексе с программными средствами) некоторые функции обеспечения информационной безопасности. Критерием отнесения устройства к аппаратным, а не к инженерно-техническим средствам защиты является обязательное включение в состав технических средств КС.

К основным **аппаратным средствам** защиты информации относятся: устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т. п.); устройства для шифрования информации; устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы).

Примеры вспомогательных аппаратных средств защиты информации: устройства уничтожения информации на магнитных носителях; устройства сигнализации о попытках несанкционированных действий пользователей КС и др.

Программные средства защиты информации

Под **программными средствами защиты информации** понимают специальные программы, включаемые в состав программного обеспечения КС исключительно для выполнения защитных функций. К основным **программным средствам** защиты информации относятся:

программы идентификации и аутентификации пользователей КС; программы разграничения доступа пользователей к ресурсам КС; программы шифрования информации; программы защиты информационных ресурсов (системного и прикладного программного обеспечения, баз данных, компьютерных средств обучения и т. п.) от несанкционированного изменения, использования и копирования.

Примеры вспомогательных программных средств защиты информации: программы уничтожения остаточной информации (в блоках оперативной памяти, временных файлах и т. п.); программы аудита (ведения регистрационных журналов) событий, связанных с безопасностью КС, для обеспечения возможности восстановления и доказательства факта происшествия этих событий; программы имитации работы с нарушителем (отвлечения его на получение якобы конфиденциальной информации); программы тестового контроля защищенности КС и др.

Сервисы безопасности

К **сервисам безопасности** относятся: идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография, экранирование.

Под **идентификацией**, применительно к обеспечению информационной безопасности компьютерной сети, понимают однозначное распознавание уникального имени субъекта компьютерной сети. Идентификация предназначена для того, чтобы пользователь или вычислительный процесс, действующий по команде определенного пользователя, могли идентифицировать себя путем сообщения своего имени.

Аутентификация означает подтверждение того, что предъявленное имя соответствует данному субъекту (подтверждение подлинности субъекта). С помощью аутентификации вторая сторона убеждается, что пользователь, пытающийся войти в операционную систему, действительно тот, за кого себя выдает.

Средства управления доступом позволяют специфицировать и контролировать действия, которые пользователи и вычислительные процессы могут выполнять над информацией и другими компьютерными ресурсами, то есть речь идет о логическом управлении доступом, который реализуется программными средствами.

Логическое управление доступом обеспечивает конфиденциальность и целостность объектов путем запрещения обслуживания неавторизованных пользователей. Контроль прав доступа осуществляется посредством различных компонент программной среды — ядром сетевой операционной системы,

дополнительными средствами безопасности, системой управления базами данных, посредническим программным обеспечением.

Протоколированием называется процесс сбора и накопления информации о событиях, происходящих в компьютерной сети.

Возможные события принято делить на три группы:

внешние события, вызванные действиями других сервисов; внутренние события, вызванные действиями самого сервиса; клиентские события, вызванные действиями пользователей и

администраторов.

Аудитом называется процедура анализа накопленной в результате протоколирования информации. Этот анализ может осуществляться оперативно в реальном времени или периодически.

Экран это средство разграничения доступа клиентов из одного сетевого множества к серверам, принадлежащим другому сетевому множеству. Функция экрана заключается в контроле всех информационных потоков между двумя множествами систем. Примерами экранов являются межсетевые экраны (брандмауэры (firewalls)), устанавливаемые для защиты локальной сети организации, имеющей выход в открытую среду.

Метод криптографии — одно из наиболее мощных средств обеспечения конфиденциальности и контроля целостности информации. Основным элементом криптографии шифрование (или преобразование данных в нечитабельную форму ключей шифрования расшифровки). В состав криптографической системы входят: один или нескольких алгоритмов шифрования, ключи, используемые этими алгоритмами шифрования, подсистемы управления ключами, незашифрованный и зашифрованный тексты.

При использовании метода криптографии на первом этапе к тексту, который необходимо шифровать, применяются алгоритм шифрования и ключ для получения из него зашифрованного текста. На втором этапе зашифрованный текст передается к месту назначения, где тот же самый алгоритм используется для его расшифровки.

Ключом называется число, используемое криптографическим алгоритмом для шифрования текста.

В криптографии используется два **метода шифрования** симметричное и асимметричное.

При **симметричном шифровании** для шифрования и для расшифровки отправителем и получателем применяется один и тот же ключ, об использовании которого они договариваются заранее. Основным недостаток симметричного шифрования состоит в том, что ключ должен быть известен как отправителю, так и получателю, откуда возникает новая проблема безопасной рассылки ключей.

Существует также вариант симметричного шифрования, основанный на использовании составных ключей, когда секретный ключ делится на две части, хранящиеся отдельно. Таким образом, каждая часть сама по себе не позволяет выполнить расшифровку.

Асимметричное шифрование характеризуется тем, что при шифровании используются два ключа: первый ключ делается общедоступным (публичным) и используется для шифровки, а второй является закрытым (секретным) и используется для расшифровки

Дополнительным методом защиты шифруемых данных и проверки их целостности является **цифровая подпись**.

Вопросы

1. Что относится к сервисам безопасности?

2. Что является наиболее эффективным средством для защиты от сетевых атак?
3. Что называется утечкой информации?
4. Защита информации обеспечивается применением антивирусных средств?
5. В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на ...
6. Сервисы безопасности, встроенные в сетевые операционные системы, это...
7. Устройства для ввода идентифицирующей пользователя информации, устройства для шифрования информации; устройства для воспрепятствования несанкционированному включению рабочих станций и серверов, относятся к ...
8. Устройства уничтожения информации на магнитных носителях; устройства сигнализации о попытках несанкционированных действий пользователей компьютерных сетей относятся к...
9. Программы идентификации и аутентификации пользователей КС; программы разграничения доступа пользователей к ресурсам КС; программы шифрования информации; программы защиты информационных от несанкционированного изменения, использования и копирования относятся к ...
10. Программы уничтожения остаточной информации; программы аудита событий, связанных с безопасностью КС, для обеспечения возможности восстановления и доказательства факта происшествия этих событий; программы имитации работы с нарушителем программы тестового контроля защищенности КС относятся к...
11. Однозначное распознавание уникального имени субъекта компьютерной сети – это...
12. Подтверждение подлинности субъекта – это...
13. Процесс сбора и накопления информации о событиях, происходящих в компьютерной сети – это...
14. Процедура анализа накопленной в результате протоколирования информации – это...
15. Средство разграничения доступа клиентов из одного сетевого множества к серверам, принадлежащим другому сетевому множеству – это...
16. Число, используемое криптографическим алгоритмом для шифрования текста – это...
17. Назовите дополнительный метод защиты шифруемых данных и проверки их целостности.
18. Назовите вид шифрования, при котором используются два ключа, один ключ.

Тест для самоконтроля

1. Кто руководил разработкой протокола TCP/IP, который до сих пор используется для передачи данных по сети?
 - a. Винтон Серф
 - b. Рей Томлинсон
 - c. Пол Бэрэн

- d. Роберт Кан
- 2. Линии связи - это...
 - a. передающая среда
 - b. станции
 - c. абоненты сети
 - d. режим передачи
- 3. Режим передачи, когда приемник и передатчик последовательно меняются местами...
 - a. дуплексный
 - b. симплексный
 - c. полудуплексный
 - d. передающий
- 4. Конфигурация (топология) локальной компьютерной сети, в которой все рабочие станции соединены с сервером, называется:
 - a. кольцевой
 - b. звезда
 - c. шинной
 - d. радиально-кольцевой
- 5. Компьютер, предоставляющий свои ресурсы другим компьютерам при совместной работе, называется:
 - a. адаптером
 - b. коммутатором
 - c. станцией
 - d. сервером
- 6. Какой вид топологии представлен на рисунке?
 - a. шинная
 - b. кольцевая
 - c. звездообразная
 - d. иерархическая
- 7. Укажите обязательную характеристику компьютерной сети, созданной на основе топологии «звезда»:
 - a. Компьютерная сеть - несколько компьютеров, используемых для схожих операций
 - b. Компьютерная сеть - группа компьютеров, соединенных с помощью специальной аппаратуры
 - c. Обязательное наличие сервера
 - d. Компьютеры должны соединяться непосредственно друг с другом
- 8. Пакет содержит:
 - a. Адрес только компьютера, которому он послан
 - b. Адрес компьютера-получателя и адрес компьютера – отправителя
 - c. Информацию без адресов
 - d. Заголовок сообщения
- 9. Сетью называется:
 - a. Совокупность компьютеров, находящихся в одном помещении
 - b. Совокупность компьютеров, соединенных линиями связи
 - c. Совокупность всего коммуникационного оборудования, находящегося в одном помещении

- d. Совокупность компьютеров, соединенных линиями связи для решения каких-либо задач
10. Небольшая организация (5 сотрудников) собирается построить сеть. Какой тип сети является для нее наиболее приемлемым?
- a. Одноранговая сеть
 - b. Сеть с выделенным сервером
 - c. Сеть на основе топологии «звезда»
 - d. Сеть на основе топологии «кольцо»
11. В каком типе сетей безопасность находится на более высоком уровне?
- a. В одноранговых сетях
 - b. В сетях на основе сервера
 - c. В сетях на основе топологии «шина»
 - d. В сетях на основе топологии «кольцо»
12. Коаксиальный кабель имеет жилу, изготовленную из:
- a. Меди
 - b. Стекла
 - c. Пластика
 - d. Стали
13. Какой тип коаксиального кабеля не существует?
- a. Тонкий
 - b. Средний
 - c. Толстый
 - d. Среди предложенных вариантов нет верного.
14. Для подключения витой пары к компьютеру используется вилка и гнездо:
- a. RG-44
 - b. RG-45
 - c. RG-54
 - d. RG-55
15. Кабель, способный передавать большие объемы данных на большие расстояния, - это:
- a. Коаксиальный кабель
 - b. Витая пара
 - c. Оптоволоконный кабель
 - d. Медный кабель
16. Выберите правильное утверждение:
- a. Технология Bluetooth работает на дальних расстояниях
 - b. Для работы технологии Bluetooth наличие прямой видимости обязательно
 - c. Для работы технологии Bluetooth наличие прямой видимости необязательно
 - d. Среди предложенных вариантов нет верного
17. В каком поколении семейства компьютеров появились терминалы?
- a. I
 - b. II
 - c. III
 - d. IV
18. Кто автор идеи связать несколько компьютеров в одну сеть?

- a. Пол Бэрэн
 - b. Роберт Тейлор
 - c. Рей Томлинсон
 - d. Вinton Серф
19. Как называлась первая отечественная компьютерная сеть?
- a. RELCOM
 - b. ARPANET
 - c. ИАСНЕТ
 - d. INTERNET
20. Что такое абонентская система?
- a. Абоненты сети
 - b. Станция
 - c. Абоненты сети и станции
 - d. Среди предложенных вариантов нет верного.
21. Режим передачи данных только в одном направлении...
- a. симплексный
 - b. полудуплексный
 - c. дуплексный
 - d. Среди предложенных вариантов нет верного.
22. Множество компьютеров, связанных каналами передачи информации и находящихся в пределах одного помещения, здания, называется:
- a. глобальной компьютерной сетью
 - b. информационной системой с гиперсвязями
 - c. локальной компьютерной сетью
 - d. региональной компьютерной сетью
23. В каком виде топологии выход одного из узлов сети нарушает работоспособность всей сети?
- a. шинная
 - b. звездообразная
 - c. кольцевая
 - d. иерархическая
24. В зависимости от удаленности компьютеров сети условно разделяют на:
- a. Местные и локальные
 - b. Локальные и глобальные
 - c. Домашние и глобальные
 - d. Домашние и местные
25. В каких сетях все компьютеры равноправны?
- a. в одноранговых сетях
 - b. в сетях с выделенным сервером
 - c. в электрических сетях
 - d. в глобальных сетях
26. Укажите основную характеристику локальной сети:
- a. Компьютеры расположены в одном здании, помещении
 - b. Соединение происходит с помощью высокоскоростных адаптеров
 - c. Рабочие станции могут находиться в разных городах, но обязательно на одном континенте
 - d. Соединение происходит при помощи коммуникационного

оборудования

27. Назовите совокупность правил, при помощи которых сообщение обрабатывается структурными элементами и передается по сети:

- a. Интерфейс
- b. Протокол
- c. Пакет
- d. Режим передачи

28. Каждый пользователь получил в свое распоряжение терминал после появления:

- a. систем пакетной обработки
- b. первых локальных сетей
- c. глобальных сетей
- d. многотерминальных систем

29. Можно ли назвать сетью пять компьютеров, находящихся в одном помещении?

- a. Да
- b. Нет
- c. Можно, если эти компьютеры соединены в сеть
- d. Среди предложенных вариантов нет верного.

30. Преимущества разделения аппаратных ресурсов при использовании компьютерных сетей заключается в том, что:

a. Пользователи могут совместно работать с принтером и другими периферийными устройствами, подключенными к одному из компьютеров

b. Компьютерные сети упрощают обмен информацией между пользователями

- c. Оба вышестоящих ответа верны
- d. Среди предложенных вариантов нет верного.

31. Какое устройство обязательно для подключения компьютера к сети?

- a. Сетевой адаптер
- b. Концентратор
- c. Маршрутизатор
- d. Роутер

32. Какая сеть является более дешевой?

- a. Одноранговая сеть
- b. Сеть с выделенным сервером
- c. Сеть на основе топологии «звезда»
- d. Среди предложенных вариантов нет верного.

33. Чем непосредственно окружена жила коаксиального кабеля?

- a. Слой изоляции
- b. Экраном в металлической оплетке
- c. Внешней оболочкой
- d. Ничем не окружена

34. Какие меры можно предпринять для увеличения информационной скорости сегмента?

- a. уменьшить длину кабеля
- b. выбрать кабель с меньшим сопротивлением
- c. выбрать кабель с более широкой полосой пропускания

- d. применить метод кодирования с более узким спектром
- 35. За счет какого механизма подавляются помехи в кабелях UTP?
 - a. экранирование и скручивание
 - b. увеличение длины сегмента
 - c. уменьшение длины сегмента
 - d. среди предложенных вариантов нет верного
- 36. Дайте определение понятия «бод».
 - a. скорость изменения информационного сигнала
 - b. информационная скорость
 - c. скорость передачи данных
 - d. Среди предложенных вариантов нет верного.
- 37. Что называется элементарным каналом цифровых телефонных сетей?
 - a. цифровой канал 64 Кбит/с
 - b. цифровой канал 56 Кбит/с
 - c. цифровой канал 100 Кбит/с
 - d. Среди предложенных вариантов нет верного.
- 38. OSI - это:
 - a. модель взаимодействия открытых систем
 - b. международная организация по стандартизации
 - c. сетевая операционная система
 - d. сетевое программное обеспечение
- 39. Какой уровень эталонной модели OSI обеспечивает сетевые услуги пользовательским прикладным программам?
 - a. Уровень представлений
 - b. Уровень приложений
 - c. Сеансовый
 - d. Транспортный
- 40. Какой уровень эталонной модели OSI устанавливает, обслуживает и управляет сеансами взаимодействия прикладных программ?
 - a. Сеансовый
 - b. Транспортный
 - c. Уровень приложений
 - d. Уровень представлений
- 41. Что из приведенного ниже наилучшим образом описывает дейтаграмму?
 - a. Пакет сетевого уровня
 - b. Двоичное представление информации о маршрутизации
 - c. Посылаемое источнику сообщение с подтверждением получения неповрежденных данных
 - d. Пакет данных размером менее 100 байт
- 42. Какой уровень эталонной модели OSI решает вопросы уведомления о неисправностях, учитывает топологию сети и управляет потоком данных?
 - a. Сетевой
 - b. Транспортный
 - c. Физический
 - d. Канальный
- 43. Что из приведенного ниже наилучшим образом описывает функцию уровня представлений?

- a. Он обеспечивает электрические, механические, процедурные и функциональные средства для активизации и поддержания канала связи между системами
 - b. Он предоставляет сетевые услуги пользовательским прикладным программам
 - c. Он обрабатывает уведомления об ошибках, учитывает топологию сети и управляет потоком данных
 - d. Он обеспечивает форматирование кода и представление данных
44. Наиболее защищенным от перехвата данных является:
- a. Коаксиальный кабель
 - b. Витая пара
 - c. Оптоволоконный кабель
 - d. Среди предложенных вариантов нет верного.
45. В дуплексном режиме устройства могут
- a. только передавать информацию
 - b. или передавать, или принимать информацию
 - c. и передавать, и принимать информацию
 - d. Среди предложенных вариантов нет верного.
46. В чем состоит главный отличительный признак локальной сети?
- a. площадь сети не более 1 км²
 - b. ограниченное количество пользователей, качественная связь
 - c. централизованное управление работой сети
 - d. объединение компьютеров в пределах одного здания
47. Какой тип среды передачи обеспечивает максимальную помехозащищенность и секретность передачи информации?
- a. инфракрасный канал
 - b. оптоволоконный кабель
 - c. витая пара
 - d. коаксиальный кабель
48. На каком уровне модели OSI работают маршрутизаторы?
- a. на канальном
 - b. на транспортном
 - c. на сетевом
 - d. на физическом
49. Какой уровень модели OSI определяет скорость побитовой передачи?
- a. физический
 - b. канальный
 - c. сетевой
 - d. транспортный
50. Каковы особенности одноранговой сети?
- a. исключение коллизий и гарантированное время доступа
 - b. развитая система разграничения прав доступа, необходимость администратора
 - c. централизованный контроль за обменом и эффективная защита данных
 - d. простота и низкая стоимость, небольшое количество абонентов
51. Выберите предложение, лучше других определяющее TCP/IP.

- а. Протокол, разработанный Microsoft для того, чтобы позволить маршрутизацию информации между смешанными сетями.
 - б. Протокол, разработанный IAB для того, чтобы предоставить доступ к Интернету различным производителям программного и аппаратного обеспечения
 - с. Семейство протоколов, организовывающих обмен информацией между разными типами приложений, которые работают на различных платформах и в различных сетевых окружениях.
 - д. Семейство протоколов, разработанных Microsoft и позволяющее обычным пользователям получать доступ к ресурсам Интернета.
52. MAC-адрес является
- а. 32-разрядным
 - б. 64-разрядным
 - с. 48-разрядным
 - д. 8-разрядным
53. Кто назначает физический адрес (MAC-адрес) абонентов сети Ethernet?
- а. компьютер-сервер
 - б. изготовитель сетевого адаптера
 - с. активное приложение
 - д. пользователь компьютера
54. В чем основное преимущество сети FDDI перед остальными стандартными сетями?
- а. максимальное количество абонентов
 - б. использование оптоволоконного кабеля
 - с. максимальный размер сети
 - д. использование маркерного метода управления
55. Какой уровень модели OSI задает логические адреса и определяет маршрут, по которому будет передаваться пакет:
- а. транспортный
 - б. канальный
 - с. прикладной
 - д. сетевой
56. Беспроводное подключение обеспечивает...
- а. максимальную мобильность и оперативность связи
 - б. быстрый способ организации связи, т.е. особенный эффект достигается, если прокладка кабеля связана со значительными затратами, или невозможна (например, в помещениях, имеющих железобетонные полы и стены, и т.д.) или нецелесообразна (например, в помещении, снятом на короткий срок);
 - с. полосу пропускания с ограниченным частотным ресурсом
 - д. все ответы верны
57. Виды беспроводного доступа:
- а. кабельное телевидение;
 - б. многоканальная электросвязь;
 - с. местные телефонные сети;
 - д. Среди предложенных вариантов нет верного.
58. WLAN-сети обладают рядом преимуществ перед обычными кабельными сетями:

- a. Низкая скорость работы, зато высокая устойчивость соединения и хорошее шифрование
- b. WLAN-сеть можно очень быстро развернуть, что очень удобно при проведении презентаций или в условиях работы вне офиса
- c. WLAN-сеть можно использовать там, где требуется высокая скорость работы и постоянное соединение
- d. все вышестоящие ответы верны

59. Wi-Fi сеть может использоваться:

- a. для объединения пространственно разнесенных подсетей в одну общую сеть там, где кабельное соединение подсетей невозможно или нежелательно
- b. для беспроводного подключения пользователей к сети
- c. все вышестоящие ответы верны;
- d. Среди предложенных вариантов нет верного.

60. Как называется вид беспроводной связи, обеспечивающий мобильность абонентов в пределах достаточно большой зоны обслуживания, а также проще и дешевле по принципам построения и предоставляют абонентам меньший набор услуг?

- a. персональная спутниковая связь;
- b. радиовещание;
- c. телевидение;
- d. Среди предложенных вариантов нет верного.

61. В сетях Wi-Fi:

- a. функция роуминга отсутствует, т.е. пользователи не могут перемещаться по территории покрытия сети без разрыва соединения
- b. функция роуминга существует, но ограничена только в пределах одного здания (офиса, квартиры и т.п.)
- c. существует функция роуминга, благодаря чему пользователи могут перемещаться по территории покрытия сети без разрыва соединения
- d. Среди предложенных вариантов нет верного.

62. Базовый режим точки доступа используется для:

- a. подключения к ней клиентов
- b. подключения к ней базовых станций
- c. обнаружения беспроводных сетей неизвестных стандартов
- d. все вышестоящие ответы верны;

63. Системы передачи информации, в которой сигналы электросвязи передаются посредством радиоволн в открытом пространстве, называется...

- a. системой связи;
- b. системой оптической связи;
- c. системой проводной связи;
- d. Среди предложенных вариантов нет верного.

64. На практике очень часто применяются антенны, обладающие _____ действием.

- a. всенаправленным;
- b. направленным;
- c. узко направленным;
- d. Среди предложенных вариантов нет верного.

65. Каково основное преимущество WLAN?

- a. высокая помехозащищенность передачи информации

- b. большое количество абонентов
 - c. мобильность абонентов
 - d. большие расстояния между абонентами
66. Каковы основные достоинства сети Fast Ethernet?
- a. максимальное расстояние между компьютерами, максимальное число объединяемых компьютеров
 - b. возможность применения топологий типа кольцо и шина
 - c. совместимость с Ethernet и высокая скорость передачи
 - d. возможность использования любых линий передачи (витых пар, коаксиального и оптоволоконного кабелей)
67. В современном мире телекоммуникации беспроводные системы связи применяются в..
- a. локальных сетях
 - b. корпоративных сетях;
 - c. глобальных сетях;
 - d. все вышестоящие ответы верны;
68. Назовите используемый стандарт сотовой связи...
- a. GSM
 - b. DECT
 - c. Smart-II
 - d. Среди предложенных вариантов нет верного.
69. Какому уровню модели OSI принадлежит обмен сообщениями с прикладной программой?
- a. прикладной
 - b. сеансовый
 - c. транспортный
 - d. представления
70. Как называется режим передачи данных между двумя беспроводными сетевыми адаптерами без использования Точки Доступа?
- a. HotSpot
 - b. Ad Hoc
 - c. WDS
 - d. Среди предложенных вариантов нет верного.
71. Что рекомендует стандарт, если длина линии оказалась более максимально допустимой?
- a. не допускает сертификации с целью получения гарантий
 - b. не допускает в принципе
 - c. рекомендует измерения параметров линии
 - d. нет рекомендаций
72. Горизонтальная подсистема включает в себя:
- a. фиксированные кабели, абонентские розетки и панели
 - b. фиксированные и гибкие коммутационные кабели
 - c. фиксированные и гибкие коммутационные кабели, абонентские розетки и панели для подключения перечисленных кабелей
 - d. горизонтальные кабели, механическое окончание кабелей (разъемы), коммутационные соединения в РП этажа и телекоммуникационные разъемы
73. Интерфейсами СКС являются:

- a. точки подключения активного оборудования
 - b. точки подключения активного оборудования за исключением точки перехода
 - c. любые разъемные соединения
 - d. точки подключения активного оборудования и кабелей внешних служб
74. Максимально допустимая длина магистральных подсистем здания и комплекса составляет:
- a. 2000 метров с учетом ограничений приложений и среды передачи
 - b. 2020 метров с учетом ограничений приложений и среды передачи
 - c. 2040 метров с учетом ограничений приложений и среды передачи
 - d. определяется ограничениями приложений и среды передачи
75. Телекоммуникационная розетка:
- a. является функциональным элементом СКС
 - b. не входит в состав СКС
 - c. является интерфейсом и функциональным элементом СКС
 - d. является интерфейсом СКС
76. Максимально допустимая длина линии горизонтальной подсистемы составляет:
- a. 94 метра
 - b. 90 метров
 - c. 100 метров
 - d. 95 метров
77. Параметры кабелей определяются:
- a. категорией
 - b. классом
 - c. категорией в американских стандартах и классом в международных
 - d. категорией и волновым сопротивлением для симметричных и модовым типом для оптоволоконных
78. Коммутационные кабели (patch cords) предназначены:
- a. для коммутаций типа панель - панель
 - b. для подключений к интерфейсам СКС
 - c. для подключения оборудования и коммутации на панелях
 - d. для коммутаций на панелях и кроссах
79. Что такое планирование?
- a. Усложненное моделирование уже наступившей действительности
 - b. Упрощенное моделирование еще не наступившей действительности
 - c. Усложненное моделирование еще не наступившей действительности
 - d. Среди предложенных вариантов нет верного.
80. Какой этап необязателен при проектировании сети?
- a. Организация силовой электрической сети
 - b. Основные сетевые решения
 - c. Оптимизация и поиск неисправностей в работающей сети
 - d. Исходные данные
 - e. Проектирование кабельной системы
 - f. Выбор с учетом стоимости
 - g. Установка сетевых карт, активных сетевых устройств, сетевой ОС и

других сетевых программных средств

81. Сколько процентов необходимо оставлять для расширения сети?

- a. 5-10
- b. 10-25
- c. 20-50
- d. Среди предложенных вариантов нет верного.

82. Чему должна соответствовать структура сети?

- a. Имеющемуся в наличии оборудованию
- b. Структуре здания или комплекса зданий
- c. Количеству рабочих мест
- d. Среди предложенных вариантов нет верного.

83. Уровень стандартизации оборудования, скорость передачи информации и возможные топологии сети необходимо учитывать при выборе:

- a. Компьютеров
- b. Расположения рабочих мест
- c. Сетевого оборудования
- d. Типа кабеля

84. Какой тип среды передачи обеспечивает максимальную помехозащищенность и секретность передачи информации?

- a. беспроводная связь
- b. оптоволоконный кабель
- c. витая пара
- d. коаксиальный кабель

85. Предоставление легальным пользователем дифференцированных прав доступа к ресурсам системы - это...

- a. Авторизация
- b. Идентификация
- c. Разделение доступа
- d. Среди предложенных вариантов нет верного.

86. Присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации

- a. Идентификация
- b. Аутентификация
- c. Аудит
- d. Среди предложенных вариантов нет верного.

87. Свойство, которое гарантирует, что информация не может быть доступна или раскрыта для неавторизованных личностей, объектов или процессов.

- a. Конфиденциальность
- b. Безопасность
- c. Шифрование
- d. Среди предложенных вариантов нет верного.

88. Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования.

- a. Безопасность информации
- b. Конфиденциальность
- c. Шифрование

- d. Среди предложенных вариантов нет верного.
- 89. Запись определенных событий в журнал безопасности сервера.
 - a. Аудит
 - b. Мониторинг
 - c. Шифрование
 - d. Среди предложенных вариантов нет верного.
- 90. Получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля.
 - a. Мониторинг
 - b. Аудит
 - c. Шифрование
 - d. Среди предложенных вариантов нет верного.
- 91. Наиболее надежный механизм для защиты содержания сообщений.
 - a. Криптография
 - b. Криптология
 - c. Шифрование
 - d. Среди предложенных вариантов нет верного.
- 92. Какой класс кабелей UTP из описываемых в стандарте EIA/TIA-568B является наиболее часто рекомендуемым и используемым при установке ЛВС?
 - a. Категории 5
 - b. Категории 6
 - c. Категории 6e
 - d. Категории 7e
- 93. Какой тип гнездового разъема должен использоваться для создания соединений с кабелем UTP категории 5 в горизонтальной кабельной системе?
 - a. RJ45
 - b. RJ12
 - c. USB
 - d. Среди предложенных вариантов нет верного.
- 94. Какой тип кабеля используется в сетях 10BaseT?
 - a. Витая пара
 - b. Оптоволокно
 - c. Коаксиальный
 - d. Среди предложенных вариантов нет верного.
- 95. Что можно сделать, если размеры здания превышают установленную максимальную длину кабеля?
 - a. Добавить повторители
 - b. Добавить сервер
 - c. Увеличить длину сегмента
 - d. Поменять кабель на другой тип
- 96. Какое преимущество дает использование топологии «звезда»?
 - a. Высокая надежность
 - b. Низкая стоимость
 - c. Необходимость в администрировании
 - d. Среди предложенных вариантов нет верного.
- 97. Что происходит с сигналом, если длина отрезка горизонтальной кабельной системы превышает размер, устанавливаемый стандартом EIA/TIA-568B?

- a. Сигнал ослабевает
- b. Сигнал усиливается
- c. Сигнал перестает транслироваться
- d. Среди предложенных вариантов нет верного.

98. Сервер, в основную задачу которого входит предоставление доступа к файлам на диске:

- a. файл-сервер
- b. контроллер домена
- c. терминальный сервер
- d. Среди предложенных вариантов нет верного.

99. Комплекс мероприятий, направленных на обеспечение информационной безопасности:

- a. защита информации
- b. информационная защита
- c. безопасность информации
- d. информационная безопасность

100. Какой стандарт регламентирует построение структурированных кабельных систем?

- a. ГОСТ Р 53246-2008
- b. IEEE 802.11
- c. OSI
- d. TSP/IP

101. Какой этап является первым при проектировании сети?

- a. Исходные данные
- b. Проектирование кабельной системы
- c. Выбор с учетом стоимости
- d. Среди предложенных вариантов нет верного.

102. Устройство для модуляции и демодуляции сигнала), используется для присоединения компьютеров к сети

- a. модем
- b. концентратор
- c. маршрутизатор
- d. прокси-сервер

103. Устройство пересылает данные, поступившие по одному из каналов связи, в каждый из присоединенных каналов

- a. модем
- b. концентратор
- c. маршрутизатор
- d. прокси-сервер

104. Устройство направляет данные только по одному каналу, определяя маршрут, по которому нужно переслать данные

- a. прокси-сервер
- b. концентратор
- c. коммутатор
- d. маршрутизатор

105. Удаленный компьютер, который, при подключении к нему вашей машины, становится посредником для выхода абонента в интернет

- a. прокси-сервер

- b. концентратор
- c. коммутатор
- d. маршрутизатор

106. Устройство соединяет несколько сетей в одну, пересылает данные из одной сети в другую

- a. модем
- b. концентратор
- c. коммутатор
- d. маршрутизатор

107. Гарантия того, что секретные данные будут доступны только тем пользователям, которым этот доступ разрешен (такие пользователи называются авторизованными).

- a. Конфиденциальность
- b. Доступность
- c. Целостность
- d. Среди предложенных вариантов нет верного.

108. Гарантия того, что авторизованные пользователи всегда получают доступ к данным.

- a. Конфиденциальность
- b. Доступность
- c. Целостность
- d. Среди предложенных вариантов нет верного.

109. Гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные.

- a. Конфиденциальность
- b. Доступность
- c. Целостность
- d. Среди предложенных вариантов нет верного.

110. Угрозы вызываются ошибочными действиями лояльных сотрудников, становятся следствием их низкой квалификации или безответственности.

- a. Умышленные
- b. Неумышленные

111. Угрозы могут ограничиваться либо пассивным чтением данных или мониторингом системы, либо включать в себя активные действия, например нарушение целостности и доступности информации, приведение в нерабочее состояние приложений и устройств.

- a. Умышленные
- b. Неумышленные

112. Совокупность мероприятий, методов и средств, обеспечивающих проверку целостности информации; исключение несанкционированного доступа к ресурсам ЭВМ и хранящимся в ней программам и данным; исключение несанкционированного использования хранящихся в ЭВМ программ.

- a. Защита информации
- b. Сетевая безопасность
- c. Среди предложенных вариантов нет верного.

113. Сервисы безопасности (выберите все правильные ответы): а.
идентификация и аутентификация
b. шифрование

- c. инверсия паролей
- d. контроль целостности
- e. регулирование конфликтов
- f. экранирование
- g. обеспечение безопасного восстановления
- h. кэширование записей

114. Наиболее эффективное средство для защиты от сетевых атак:

- a. использование сетевых экранов или «firewall»
- b. использование антивирусных программ
- c. посещение только «надёжных» Интернет-узлов
- d. использование только сертифицированных программ-броузеров при

доступе к сети Интернет

115. Утечка информации – это ...

a. несанкционированный процесс переноса информации от источника к злоумышленнику

- b. процесс раскрытия секретной информации
- c. процесс уничтожения информации
- d. непреднамеренная утрата носителя информации

116. Защита информации обеспечивается применением антивирусных средств?

- a. Да
- b. Нет

117. В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на ...

a. обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации

b. реализацию права на доступ к информации»

c. соблюдение норм международного права в сфере информационно-безопасности

d. выявление нарушителей и привлечение их к ответственности

e. соблюдение конфиденциальности информации ограниченного доступа

f. разработку методов и усовершенствование средств информационно-безопасности

118. Способ подключения к Интернет, обеспечивающий наибольшие возможности для доступа к информационным ресурсам

- a. постоянное соединение по оптоволоконному каналу
- b. удаленный доступ по телефонным каналам
- c. постоянное соединение по выделенному каналу
- d. терминальное соединение по коммутируемому телефонному каналу
- e. временный доступ по телефонным каналам

119. Для хранения Файлов, предназначенных для общего доступа пользователей сети, используется ...

- a. хост-компьютер
- b. файл-сервер
- c. рабочая станция
- d. клиент-сервер

120. Транспортный протокол (TCP) обеспечивает ...

Файлов в процессе получения

- a. разбиение файлов на IP- пакеты в процессе передачи и сборку
- b. прием, передачу и выдачу одного сеанса связи
- c. предоставление в распоряжение пользователя уже переработанную

информацию

- d. доставку информации от компьютера-отправителя к компьютеру-получателю

121. Конфигурация (топология) локальной компьютерной сети, в которой все рабочие станции соединены с Файл-сервером, называется...

- a. Кольцевой
- b. радиальной (звездообразной)
- c. шинной
- d. древовидной

122. Скорость передачи данных по каналу связи измеряется количеством передаваемых ...

- a. байтов в минуту
- b. битов информации в секунду
- c. символов в секунду
- d. слов в минуту

123. Уровень модели OSI, который обеспечивает услуги, непосредственно поддерживающие приложения пользователя называют ... уровнем.

- a. Прикладным
- b. Представительским
- c. Сеансовым
- d. Транспортным

124. Признак “Топология сети” характеризует ...

- a. схему проводных соединений в сети (сервера и рабочих станций)
- b. как работает сеть
- c. сеть в зависимости от ее размера
- d. состав технических средств

125. Сетевой протокол – это ...

сети

- a. набор соглашений о взаимодействиях в компьютерной сети
- b. последовательная запись событий, происходящих в компьютерной

- c. правила интерпретации данных, передаваемых по сети
- d. правила установления связи между двумя компьютерами в сети

126. Локальная вычислительная сеть (LAN) – это ...

или подразделений предприятия

- a. вычислительная сеть, функционирующая в пределах подразделения

- b. объединение вычислительных сетей на государственном уровне
- c. сеть, функционирующая в пределах одного субъекта федерации
- d. общепланетное объединение сетей

127. Эталонная модель обмена информацией открытой системы получила название модели ...

- a. ISO
- b. OSI
- c. OIS
- d. ОИОС

128. RAID-массив это

- a. Набор жестких дисков, подключенных особым образом
- b. Антивирусная программа
- c. Вид хакерской утилиты
- d. Брандмауэр

129. Сервисы безопасности, встроенные в сетевые операционные системы, это...

- a. Программно-аппаратные средства защиты информации в сети
- b. Программные средства защиты информации
- c. Аппаратные средства защиты информации
- d. Средства управления доступом

130. Устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т. п.), устройства для шифрования информации; устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы), относятся к ...

- a. Основным программным средствам защиты информации
- b. Основным аппаратным средствам защиты информации
- c. Вспомогательным программным средствам защиты информации
- d. Вспомогательным аппаратным средствам защиты информации

131. Устройства уничтожения информации на магнитных носителях; устройства сигнализации о попытках несанкционированных действий пользователей компьютерных сетей относятся к...

- a. Основным программным средствам защиты информации
- b. Основным аппаратным средствам защиты информации
- c. Вспомогательным программным средствам защиты информации
- d. Вспомогательным аппаратным средствам защиты информации

132. Программы идентификации и аутентификации пользователей КС; программы разграничения доступа пользователей к ресурсам КС; программы шифрования информации; программы защиты информационных ресурсов (системного и прикладного программного обеспечения, баз данных, компьютерных средств обучения и т. п.) от несанкционированного изменения, использования и копирования относятся к ...

- a. Основным программным средствам защиты информации
- b. Основным аппаратным средствам защиты информации
- c. Вспомогательным программным средствам защиты информации
- d. Вспомогательным аппаратным средствам защиты информации

133. Программы уничтожения остаточной информации; программы аудита событий, связанных с безопасностью КС, для обеспечения возможности восстановления и доказательства факта происшествия этих событий; программы имитации работы с нарушителем; программы тестового контроля защищенности КС относятся к...

- a. Основным программным средствам защиты информации
 - b. Основным аппаратным средствам защиты информации
 - c. Вспомогательным программным средствам защиты информации
 - d. Вспомогательным аппаратным средствам защиты информации
134. Однозначное распознавание уникального имени субъекта компьютерной сети – это...
- a. Идентификация
 - b. Аутентификация
 - c. Аудит
 - d. Протоколирование
135. Подтверждение подлинности субъекта – это...
- a. Идентификация
 - b. Аутентификация
 - c. Аудит
 - d. Протоколирование
136. Процесс сбора и накопления информации о событиях, происходящих в компьютерной сети – это...
- a. Идентификация
 - b. Аутентификация
 - c. Аудит
 - d. Протоколирование
137. Процедура анализа накопленной в результате протоколирования информации – это...
- a. Идентификация
 - b. Аутентификация
 - c. Аудит
 - d. Протоколирование
138. Средство разграничения доступа клиентов из одного сетевого множества к серверам, принадлежащим другому сетевому множеству – это...
- a. Экран
 - b. Ключ
 - c. Цифровая подпись
139. Число, используемое криптографическим алгоритмом для шифрования текста – это...
- a. Экран
 - b. Ключ
 - c. Цифровая подпись
140. Дополнительный метод защиты шифруемых данных и проверки их целостности:
- a. Экран
 - b. Ключ
 - c. Цифровая подпись
141. Вид шифрования, при котором используются два ключа: а.
- Симметричное
 - b. Асимметричное
142. Вид шифрования, при котором используется один ключ: а.
- Симметричное
 - b. Асимметричное

143. Автоматизированное решение для проведения полного сканирование портов, контроля необходимых обновлений ПО для защиты сети, а также проверки программного и аппаратного обеспечения

a. Сканер сетевой уязвимости

b. Цифровая подпись

c. Цифровой замок

d. Утилита жесткого диска

144. Механизмы работы сканера безопасности сети:

a. Зондирование

b. Идентификация

c. Сканирование

d. Шифрование

145. К каким средствам защиты информации относятся авторское право, документирование?

a. средства собственной защиты

b. средства защиты в составе вычислительной системы

c. средства защиты с запросом информации

d. средства активной защиты

e. средства пассивной защиты

146. К каким средствам защиты информации относятся защита магнитных дисков, специальная аппаратура?

a. средства собственной защиты

b. средства защиты в составе вычислительной системы

c. средства защиты с запросом информации

d. средства активной защиты

e. средства пассивной защиты

147. К каким средствам защиты информации относятся пароли, шифры?

a. средства собственной защиты

b. средства защиты в составе вычислительной системы

c. средства защиты с запросом информации

d. средства активной защиты

e. средства пассивной защиты

148. К каким средствам защиты относятся замки защиты, запуск по ключам?

a. средства собственной защиты

b. средства защиты в составе вычислительной системы

c. средства защиты с запросом информации

d. средства активной защиты

e. средства пассивной защиты

149. К каким средствам защиты относятся идентификация программ, антивирусное сканирование?

a. средства собственной защиты

b. средства защиты в составе вычислительной системы

c. средства защиты с запросом информации

d. средства активной защиты

e. средства пассивной защиты

150. Предварительный сбор информации о состоянии винчестера, проверка жесткого диска, исправление ошибок и восстановление данных выполняют:

- a. Антивирусные программы
- b. Утилиты жестких дисков
- c. Сетевые сканеры

Методические указания по выполнению самостоятельных работ

Рабочей программой предусмотрены следующие виды самостоятельной работы:

- выполнение домашних заданий;
- систематическая проработка конспектов занятий, учебной и справочной литературы;
- подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ;
- подготовка рефератов.

Методические рекомендации для написания рефератов

Что такое реферат

Многие обучающиеся слегка заблуждаются, когда полагают, что реферат – это самостоятельное сочинение на заданную тему.

На самом деле реферат – это не сочинение, а обзор публикаций, доступных по заданной теме. Обзор, в отличие от сочинения, не требует ни фантазии, ни оригинальности мышления, ни высказывания новых идей. Разумеется, в реферате можно приводить собственные утверждения и высказывания, но, во-первых, это совсем не обязательно, а во-вторых, уместно не во всех разделах работы.

Слово «реферат» в переводе с латинского буквально означает «пусть он доложит». Реферат при индивидуальной работе с литературой представляет собой краткую «обогащенную» запись идей, содержащихся в одном или нескольких источниках.

Создание рефератов очень похоже на коллекционирование почтовых марок. Представьте себе, что перед вами лежит десяток почтовых марок, и ваша задача – аккуратно их расположить. Один человек расположит их в хронологическом порядке, другой – по возрастанию номиналов, третий – в порядке возрастания геометрических размеров, четвертый – по странам.

Обратите особое внимание на то, что каждый проведет при этом небольшое исследование. Кто-то внимательно изучит содержимое марок, а кто-то ограничится их обмером с помощью линейки, но каждый проявит творчество и получит результат, отличный от других. По этому результату можно многое сказать об исследовательских способностях и творческом подходе автора.

Точно так же происходит и подготовка рефератов. Сначала собираются исходные материалы на заданную тему (книги, статьи, заметки, иллюстрации), а потом выдержки из них группируются в том порядке, который удобен автору. Как и во всяком деле, успех зависит от наличия исходных материалов и практических навыков.

Написать хороший реферат может лишь тот, кто овладел азбукой работы с книгой. Проще организовать подготовку, когда на тему реферата имеется всего один-два источника. Сложнее работать с большим количеством книг и статей. Во всех случаях дело облегчит рационально организованный предварительный просмотр литературы.

Виды рефератов

Существуют разные типы рефератов, и, соответственно, к ним подходят разные модели подготовки. Если говорить обобщенно, то можно выделить четыре основных типа: учебные, контрольные, служебные и творческие рефераты.

Учебные рефераты

Учебные рефераты – это, как правило, те, которые задают в качестве самостоятельных работ. У них одна цель – научить обучающихся работать эффективно. Эффективность – это не объем, а максимум результата при минимуме затрат сил и времени. Кто-то может подумать, что самый эффективный подход состоит в том, чтобы найти в Интернете готовую работу и сделать ее вместо своей. Однако это не совсем так. Если бы цель реферата состояла в том, чтобы только его сдать, то это было бы верно, но поскольку на самом деле цель состоит в том, чтобы учиться работать, то эффективность оказывается нулевой.

Творческие рефераты

Это самый интересный вид рефератов. Почему работу над творческими материалами лучше начинать с рефератов? Здесь есть, по крайней мере, четыре причины.

Первая причина состоит в том, что творческие работы лучше всего выполнять не тогда, когда дано задание, а тогда, когда есть желание. Это намного эффективнее. Работа проходит быстро, весело и интересно.

Вторая причина в целесообразности подготовки самостоятельных творческих рефератов состоит в том, что даже опытные авторы редко могут написать хорошую работу с первого раза. Обычно большинство авторов говорят, что, если бы им пришлось выполнить ту же работу еще раз, они сделали бы ее иначе. Постоянное недовольство результатами своего труда – неотъемлемая черта творчества.

Еще одна причина состоит в том, что в любой творческой деятельности есть противоречие между структурой работы и ее содержанием.

Четвертая причина желательности предварительных рефератов состоит в том, что обычный человек не может уместить в голове содержание большого труда. Работа только тогда становится творчеством, когда ее пропускают через сито строгого отбора.

Строгий отбор – это основа любого творчества, а чтобы было из чего отбирать, надо иметь исходные материалы. Творческие рефераты очень хорошо для этого подходят.

Как писать введение

Для окончательной доводки реферата в нем не хватает двух разделов: введения и заключения. У введения может быть самостоятельная тема, например, актуальность работы. Под актуальностью понимается значение того, о чем написано в реферате. Введение, основанное на актуальности, применяют в учебных рефератах.

Если действовать контрастно, тему введения можно сделать «контрастной» к теме самого реферата. Такой подход удобен для творческих рефератов.

Как писать заключение

Почти во всех видах рефератов заключение можно оформлять в виде выводов. Важно сделать их краткими и точными. Сколько выводов сделать – это не вопрос. Их никогда не бывает больше или меньше, чем это вытекает из основного текста.

О списках литературы

Реферат не может обойтись без списка литературы. Это связано с тем, что реферат – это не сочинение, и он по определению основывается на первоисточниках. Даже если вы подготовили реферат с помощью Интернета, это не меняет дела. Публикации в WWW – это те же первоисточники, и их тоже надо указывать.

Свои работы всегда надо готовить так, чтобы они могли принести как можно больше пользы другим людям, даже если вы не надеетесь, что их будет читать кто-то, кроме преподавателя.

Основные источники:

1. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2023. — 333 с. — (Профессиональное образование). — ISBN 978-5-534-04638-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/513518>
2. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2023. — 351 с. — (Профессиональное образование). — ISBN 978-5-534-04635-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/514019>
3. Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2023. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/517817>

Дополнительные источники:

1. Замятина, О. М. Инфокоммуникационные системы и сети. Основы моделирования : учебное пособие для среднего профессионального образования / О. М. Замятина. — Москва : Издательство Юрайт, 2023. — 159 с. — (Профессиональное образование). — ISBN 978-5-534-10682-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518012>
2. Методические рекомендации, для организации самостоятельной работы, обучающихся по дисциплине ОП.11 Компьютерные сети для студентов специальности 09.02.07 Информационные системы и программирование, 2023г.